# Cisco Connected Factory—PROFINET Wireless Design and Implementation Guide

First Published: October 2017

Cisco Validated Design

**Cisco Systems, Inc.** www.cisco.com

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

# Contents

# Cisco Connected Factory—PROFINET Wireless Design and Implementation Guide

## Preface

This document is built on the Cisco Connected Factory vision to provide users with a plant-wide industrial wireless solution using or supporting the PROFINET IO protocol, a PROFIBUS International (PI) open Industrial Ethernet Standard for industrial automation. This solution is designed for an industrial automation application and can apply to multiple industries.

### Navigator

The document covers:

- PROFINET wireless network architectures
- PROFINET wireless use cases
- Configuration for the PROFINET wireless solution

### Audience

The primary intended audience for this document is Industrial Operations, IT, and Security teams as well as Cisco partners, SEs, and services teams.

### Document Objective and Scope

This design guide provides a comprehensive explanation of a wireless solution for PROFINET, including information about the system architecture, possible deployment models, and guidelines for implementation and configuration. This guide also recommends best practices and potential issues when deploying the reference architecture.

### Use Cases/Services/Deployment Models

This guide addresses the following technology use cases:

- Static Equipment
- Mobile equipment—Roaming within an access point (AP)
- Mobile Equipment—Roaming intra cell
- Mobile Equipment—Roaming inter cell

# System Overview

## Executive Summary

In today's world of the Industrial Internet of Things (IIoT), manufacturing industries are adopting the vision of connecting devices using a common standard, thereby realizing a converged plant floor that brings down the cost of operation and improves productivity. Several trends are also occurring in industrial automation, such as edge computing, IT/OT convergence, Big Data/Cloud, wireless access requirements, etc. To meet these trends, we need a network that supports continuous operation, automation, open standards, multi-vendor support, and high performance for real-time applications like PLC-IO, accessing data from a centralized location, and seamless roaming. There is significant interest in industrial automation to provide wireless access for industrial devices, mainly in places that are hard to reach, outdoors, airports, shipping facilities, factory floors, rough environments, monorails, and automated guided vehicles. While wired access is the preferred access method, wireless access can complement a wired deployment.

This document is written to address these trends in the manufacturing industry with a design that offers:

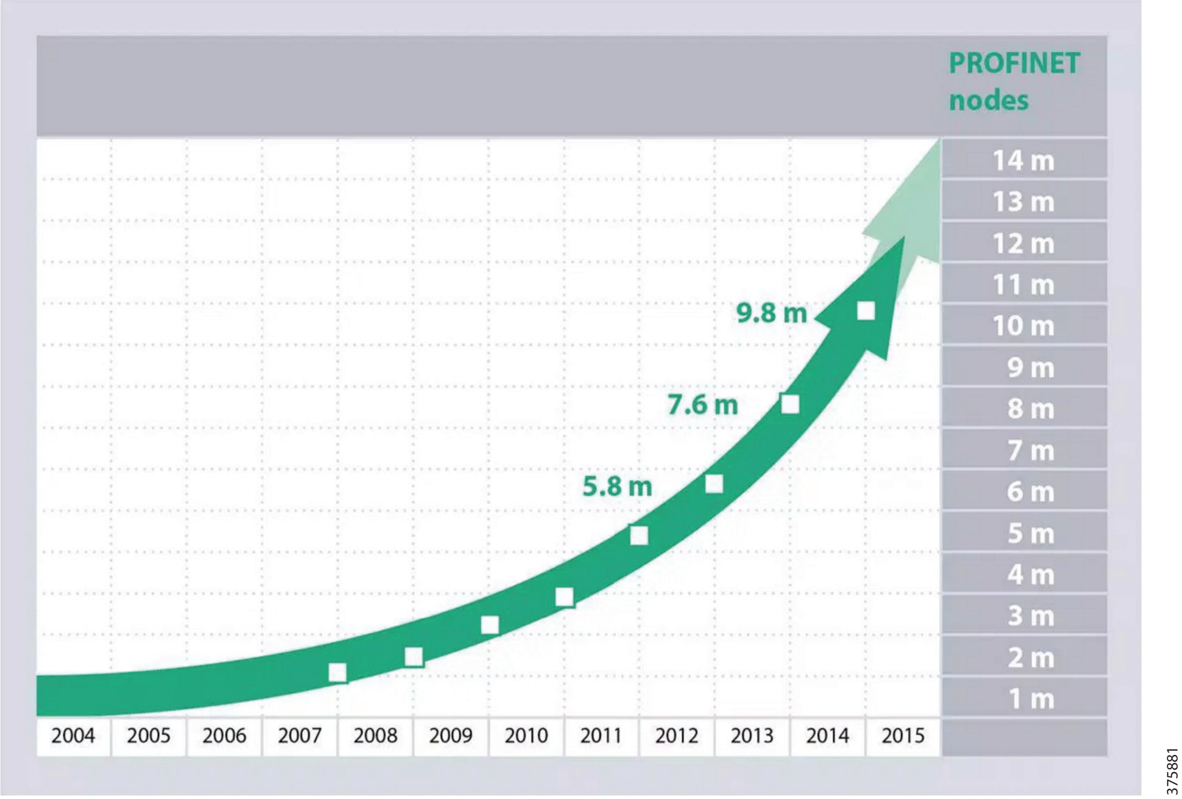
- Continuous connectivity—The design ensures that the network is resilient and converges within defined value when a failure occurs.
- Performance for real time (RT) traffic—By building a delay-constrained application, this design validated the latency variation requirement of the industrial end devices.
- Centralized management—This design configured PROFINET for both the PLC/IO and the Cisco Infrastructure by Siemens© Totally Integrated Automation Portal Version 14 (TIA Portal).
- Data Access—By integrating this design in the industrial architecture, we have ensured that different types of management, security, and automation tools can access the industrial devices for automation, management, and data collection.
- Wireless use case—This design was built to meet the standard use cases designed in manufacturing such as stationary, roaming intra-cell, and inter-cell scenarios.

## Introduction

PROFINET is a standard that allows many industrial applications to use the network for machine-to-machine communication without infrastructure modification. Because it is a standard, it allows different vendors to build inter-operable products, thereby reducing deployment and operational costs for manufacturers. Adopting PROFINET as a standard has enabled manufacturers to realize many benefits, including cost reduction through the use of Ethernet cabling, easy installation, high performance, and higher return on investment (ROI).

The PROFINET standard is being widely adopted worldwide. According to PI North America, there are 15 million PROFINET Ethernet nodes deployed in the market today and PROFINET, as a standard for industrial automation, is adopted by 30 percent of the industrial Ethernet switching market. Figure 1 illustrates the growth curve PROFINET-capable devices have experienced in the last few years.

**Figure 1 PROFINET-Capable Devices Sold Globally**



The adoption of an industrial Ethernet approach, specifically PROFINET, has grown at a rapid rate, doubling in the last five years from 4 million devices to 9+ million devices in 2015 (according to a PI survey). PROFINET supports the 802.11n wireless standard, which is part of PROFINET specification–IEC 61784-2. Also, PROFINET standard IEC 61784-3-3 supports PROFISAFE, which is a certified technology that uses PROFINET as transport. Traditional automation designs leveraged wired infrastructure to enable access to Industrial IoT devices. However, for certain uses cases, such as outdoors, large factory halls, airports, etc. it makes more sense to use wireless technology. For example, applications such as Automated Guided Vehicles can roam in a factory by using wireless technology. There are many advantages to implementing a wireless solution, including reachability, cabling cost, reduced maintenance costs, etc.

Cisco PROFINET wireless technology supports the requirements of industrial automation by providing continuous connectivity to end devices. The Cisco IOT wireless solution is fully compatible with 802.11n and meets the latency and resiliency requirements of manufacturing industries. Cisco industrial access points now support PROFINET. By using Cisco wired and wireless infrastructure, customers can not only provide basic connectivity for industrial devices, but also provide continuous connectivity for other applications related to Big Data, analytics, etc.

## Cisco Connected Factory–PROFINET Components

This section describes the components that are part of the solution. We begin by describing the physical media, wired and wireless, then describe the industrial automation system and extensively discuss the PROFINET protocol, mainly on the treatment of real time traffic.

### Physical Layer–Ethernet

Industrial Ethernet PROFINET IO is based on IEEE 802.3 Ethernet standards. It uses wired media such as twisted pair cables (copper) or single/multimode fiber optic cables. The connectors for the above two media are also standardized with RJ45 connectors for copper cables and SC/ST or LC connectors for fiber optic cables. Sealed connectors such as M12 are required for harsh environments, which require IP67 certification. An Ethernet speed of 100 Mbps is typically used in Industrial Automation System installations with 1Gbps in the industrial Ethernet backbone, which has been validated as part of this design guide. The physical layout and media choice is dependent on the industry environment and the physical layout of end devices.

## Physical Layer—Wireless

PROFINET runs over the standard wireless 802.11 (b/g/a/h/n/a/c), and is also part of the IEC 61784-2 specification. Some IO devices have wireless built-in. PROFINET transportation is supported when a Cisco autonomous AP or a Cisco unified AP in FlexConnect local switching mode communicates with a Cisco AP in workgroup bridge mode.

## Automation and Control System Devices

Different types of devices are used in Industrial Automation Systems. The range of functionality varies from simple devices like an on-off switch to a complex system like a Programmable Logic Controller (PLC). Table 1 describes the types of devices in an Industrial Automation System.

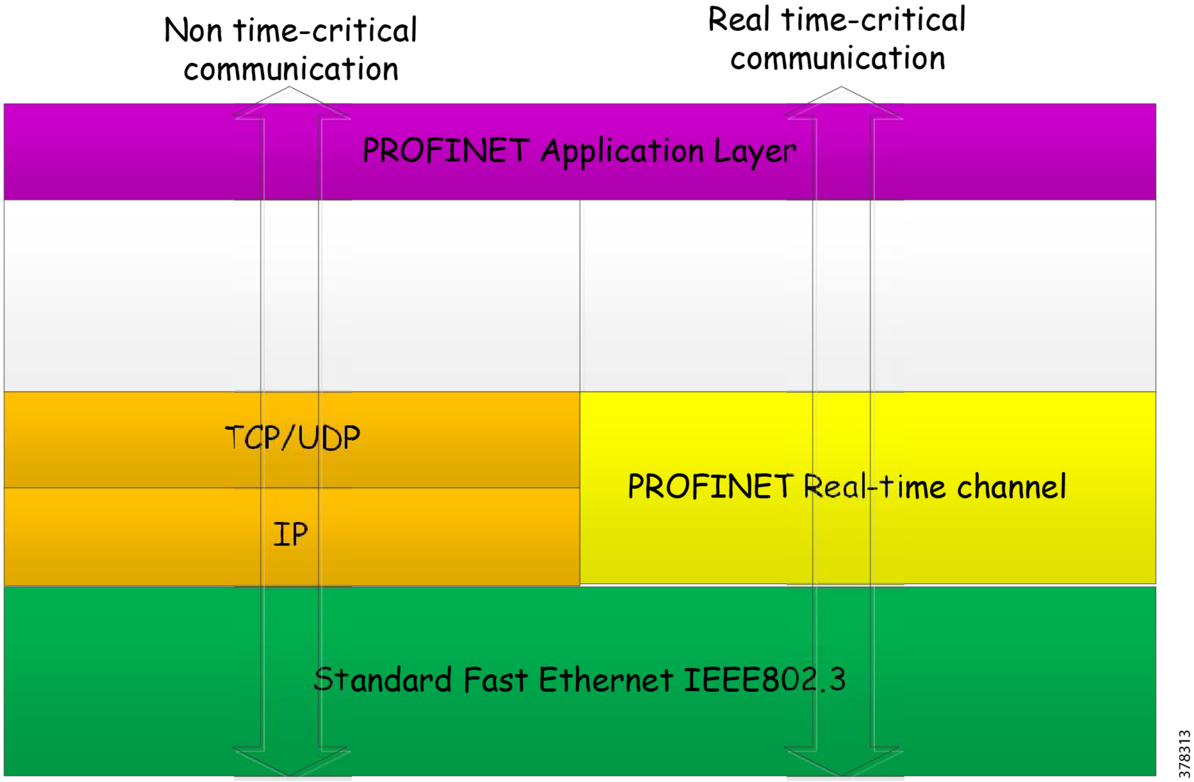
**Table 1 Third-party Devices Used in this Document**

| Components | Description |
|---|---|
| Programmable Logic Controller (PLC) | The PLC acts as the heart of the Industrial Automation System. It can perform many complex tasks, such as sending and receiving information to/from a device, and it is programmable from an automation tool like TIA Portal. |
| Human Machine Interface (HMI) | The HMI has two functions: present the complete flow of the automation process on the GUI and take or accept input from users. |
| PC Supervisor | An automation tool (TIA Portal) that provides an OT/IT person with the ability to configure and manage PROFINET applications on the industrial devices and also on the Cisco IE switches. |
| Distributed IO | The PLC manages the operation of the field IO devices through Distributed IO. By deploying Distributed IO, manufactures save the cost of running wires directly to the PLC. |

# Network Protocol—PROFINET

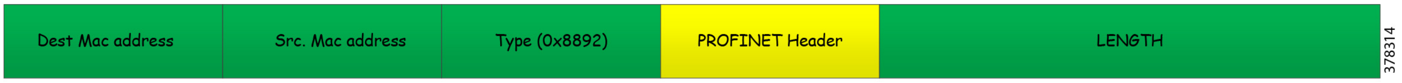
PROFINET is a PROFIBUS International (PI) open Industrial Ethernet Standard for industrial automation. It provides high-speed data exchange between Industrial Automation System devices and networking devices, allowing manufacturers to utilize future innovations as they become available. Figure 2 shows the PROFINET stack mapped to an OSI model.

**Figure 2 PROFINET Stack Mapping**


Non time-critical communication
Real time-critical communication
PROFINET Application Layer
TCP/UDP
IP
PROFINET Real-time channel
Standard Fast Ethernet IEEE802.3
378313

As shown in Figure 2, PROFINET uses a TCP/IP channel for non-time critical tasks such as downloading configurations, diagnostics, device management information, etc. PROFINET uses a real time channel for time-critical data such as cyclic data with IO devices, alarms and critical messages, and communication monitoring. Note this distinction between the communication that occurs with a TCP/IP channel and a RT channel. For the RT channel, there is no TCP/IP header inserted into the frame. The PROFINET application layer adds a PROFINET header on top of the Ethernet frame for RTP communication, which is shown in Figure 3. The next section provides more details on the different types of RT traffic.

**Figure 3 PROFINET Header RT Communication**



| Dest Mac address | Src. Mac address | Type (0x8892) | PROFINET Header | LENGTH |
|---|---|---|---|---|

## Real Time Traffic

In the PROFINET world, there are two types of real time traffic:

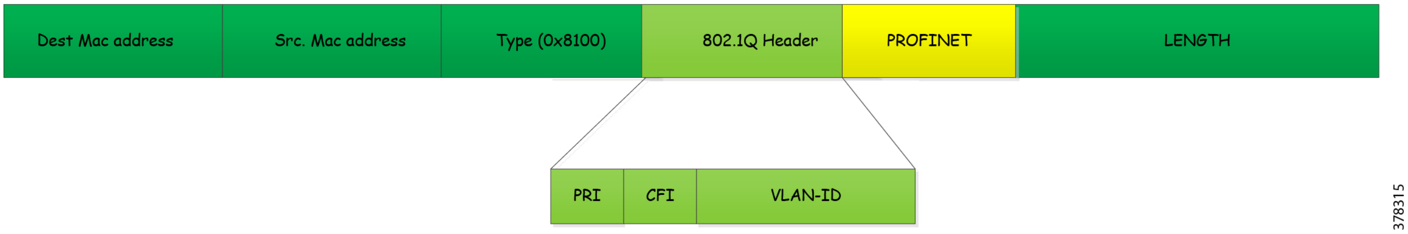
- Real Time (RT)
- Isochronous Real Time (IRT)

PROFINET applications use a RT channel for achieving cycle time up to 10 msec. with <1 msec. jitter, which is the best performance that can be accomplished by a RT channel. However, we would like to have roaming scenarios covered in this CVD; we have set the critical parameter for the delay to be between 10-100 msec. The rationale of this parameter is to ensure that when an IO device roams in the network, the end-to-end delay should be within the critical parameter. The PROFINET standard also specifies the use of an IRT channel for highly-deterministic performance with cycle times < 1 msec. with <1 sec. jitter. This design guide focused mainly on providing RT channel for the PROFINET applications. The next section describes how Cisco IE switches, access points, and WGBs identify real time traffic and prioritize it over regular traffic.

## Real Time Traffic Treatment in a Wired Environment

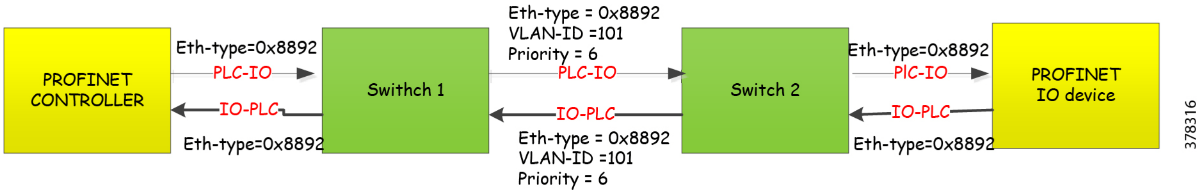
Before we begin, we briefly review how to classify and mark the real time traffic class used in a normal scenario. Ethernet frames can mark with their relative importance at Layer 2 by setting the 802.1p user priority bits (COS) of the 802.1Q header, as shown in Figure 4.

### Figure 4 802.1Q Header



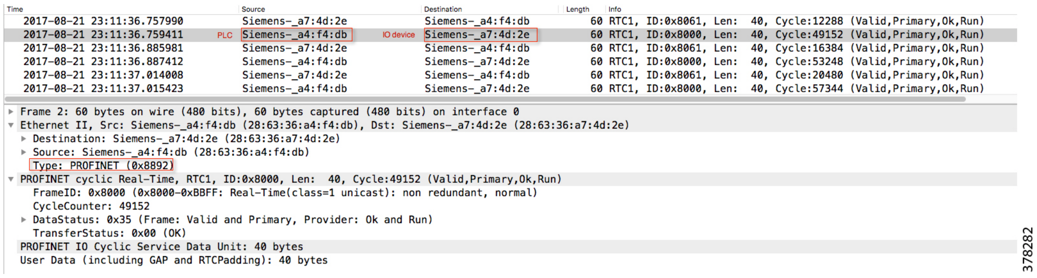
When an end host wants to send a high priority frame, it needs to use an 802.1q header because it allows the application to set the priority setting. Since the end host does not know the VLAN information, it sets the VLAN-ID value to 0. These frames are called priority tagged frames. Once a switch or an access point receives this frame, it is supposed to evaluate it and treat it based on the traffic class. In the PROFINET world, when an industrial device wants to send a packet that needs high priority treatment, it sends a frame with a VLAN- ether-type of 0x8892, as shown in Figure 5.

### Figure 5 Traffic Flow of PROFINET in Wired Switches



The PLC sends a frame to an IO device with an eth-type of 0x8992 to the switch, as shown in Figure 6.

### Figure 6 PROFINET Real Time Header



```
Time                            Source                  Destination             Length  Info
  2017-08-21 23:11:36.757990    Siemens-_a7:4d:2e       Siemens-_a4:f4:db           60 RTC1, ID:0x8061, Len:  40, Cycle:12288 (Valid,Primary,Ok,Run)
  2017-08-21 23:11:36.759411    Siemens-_a4:f4:db       Siemens-_a7:4d:2e           60 RTC1, ID:0x8000, Len:  40, Cycle:49152 (Valid,Primary,Ok,Run)
  2017-08-21 23:11:36.885981    Siemens-_a7:4d:2e       Siemens-_a4:f4:db           60 RTC1, ID:0x8061, Len:  40, Cycle:16384 (Valid,Primary,Ok,Run)
  2017-08-21 23:11:36.887412    Siemens-_a4:f4:db       Siemens-_a7:4d:2e           60 RTC1, ID:0x8000, Len:  40, Cycle:53248 (Valid,Primary,Ok,Run)
  2017-08-21 23:11:37.014008    Siemens-_a7:4d:2e       Siemens-_a4:f4:db           60 RTC1, ID:0x8061, Len:  40, Cycle:20480 (Valid,Primary,Ok,Run)
  2017-08-21 23:11:37.015423    Siemens-_a4:f4:db       Siemens-_a7:4d:2e           60 RTC1, ID:0x8000, Len:  40, Cycle:57344 (Valid,Primary,Ok,Run)

▶ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▼ Ethernet II, Src: Siemens-_a4:f4:db (28:63:36:a4:f4:db), Dst: Siemens-_a7:4d:2e (28:63:36:a7:4d:2e)
  ▶ Destination: Siemens-_a7:4d:2e (28:63:36:a7:4d:2e)
  ▶ Source: Siemens-_a4:f4:db (28:63:36:a4:f4:db)
    Type: PROFINET (0x8892)
▼ PROFINET cyclic Real-Time, RTC1, ID:0x8000, Len:  40, Cycle:49152 (Valid,Primary,Ok,Run)
    FrameID: 0x8000 (0x8000-0xBBFF: Real-Time(class=1 unicast): non redundant, normal)
    CycleCounter: 49152
  ▶ DataStatus: 0x35 (Frame: Valid and Primary, Provider: Ok and Run)
    TransferStatus: 0x00 (OK)
  PROFINET IO Cyclic Service Data Unit: 40 bytes
  User Data (including GAP and RTCPadding): 40 bytes
```

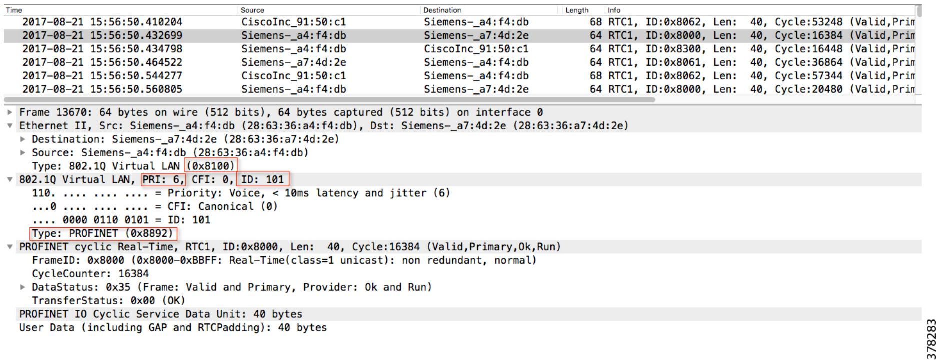
In Figure 6, PLC device - Siemens-a7:f4:db sends a frame to IO device Siemens-a4:4d:2e x8892.

The switch encodes this frame in an 802.1q trunk and prioritizes the traffic as high priority by setting the priority bits in the 802.1q header to 6. The last switch, which receives the traffic, removes the trunk information and passes the PROFINET frame to the application. We need both VLAN 0 support and PROFINET RT support because older switches did not support PROFINET RT, so by supporting both VLAN 0 and ether-type of 0x8892 we obtain backward compatibility with older switches.

Also note that for the 802.1q frame we have two fields for indicating the type of information that is present in a frame, as shown in Figure 4. The first field with a value of 0x8100 indicates that this frame is an 802.q frame. The second type value is 0x8892, which indicates that this frame is encoding RT channel information. When a Cisco IE switch receives a PROFINET RT frame it does the following:

- If the egress interface has a trunk configured, it marks the frame with the outgoing VLAN, marks the COS setting to 6, and sends the PROFINET RT frame. Figure 7 shows the details.

**Figure 7 Trunk Encoding Priority of Real Time Frame**



```
Time                              Source                   Destination              Length  Info
   2017-08-21 15:56:50.410204     CiscoInc_91:50:c1        Siemens-_a4:f4:db            68 RTC1, ID:0x8062, Len:  40, Cycle:53248 (Valid,Prim
   2017-08-21 15:56:50.432699     Siemens-_a4:f4:db        Siemens-_a7:4d:2e            64 RTC1, ID:0x8000, Len:  40, Cycle:16384 (Valid,Prim
   2017-08-21 15:56:50.434798     Siemens-_a4:f4:db        CiscoInc_91:50:c1            64 RTC1, ID:0x8300, Len:  40, Cycle:16448 (Valid,Prim
   2017-08-21 15:56:50.464522     Siemens-_a7:4d:2e        Siemens-_a4:f4:db            64 RTC1, ID:0x8061, Len:  40, Cycle:36864 (Valid,Prim
   2017-08-21 15:56:50.544277     CiscoInc_91:50:c1        Siemens-_a4:f4:db            68 RTC1, ID:0x8062, Len:  40, Cycle:57344 (Valid,Prim
   2017-08-21 15:56:50.560805     Siemens-_a4:f4:db        Siemens-_a7:4d:2e            64 RTC1, ID:0x8000, Len:  40, Cycle:20480 (Valid,Prim

▶ Frame 13670: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
▼ Ethernet II, Src: Siemens-_a4:f4:db (28:63:36:a4:f4:db), Dst: Siemens-_a7:4d:2e (28:63:36:a7:4d:2e)
  ▶ Destination: Siemens-_a7:4d:2e (28:63:36:a7:4d:2e)
  ▶ Source: Siemens-_a4:f4:db (28:63:36:a4:f4:db)
    Type: 802.1Q Virtual LAN (0x8100)
▼ 802.1Q Virtual LAN, PRI: 6, CFI: 0, ID: 101
    110. .... .... .... = Priority: Voice, < 10ms latency and jitter (6)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 0110 0101 = ID: 101
    Type: PROFINET (0x8892)
▼ PROFINET cyclic Real-Time, RTC1, ID:0x8000, Len:  40, Cycle:16384 (Valid,Primary,Ok,Run)
    FrameID: 0x8000 (0x8000-0xBBFF: Real-Time(class=1 unicast): non redundant, normal)
    CycleCounter: 16384
  ▶ DataStatus: 0x35 (Frame: Valid and Primary, Provider: Ok and Run)
    TransferStatus: 0x00 (OK)
  PROFINET IO Cyclic Service Data Unit: 40 bytes
  User Data (including GAP and RTCPadding): 40 bytes
```

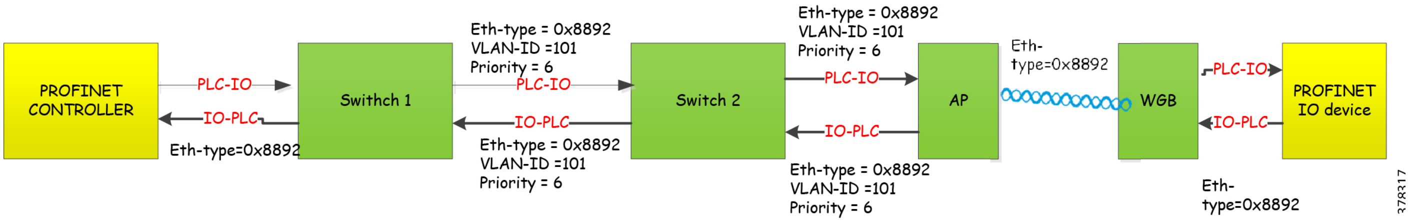
As you can see in Figure 7, the switch set the encapsulation to 0x8100 indicating a 802.1q trunk, Priority to 6 indicating Real Time traffic, ID to 101 indicating the VLAN information, and finally ether-type to 0x8892 indicating the frame encoded in the trunk is a PROFINET frame.

- If the egress interface has no trunk set, it strips the VLAN-id and sends the frame.

## Real Time Traffic Treatment in a Wireless Deployment

In a wireless deployment, access points and WGBs need to evaluate traffic that is encoded with ether-type of 0x8892 and treat this traffic higher than other types of traffic. When an IO device sends a frame with ether-type 0x8892, then the WGB sends the frame across the wireless network to the access point. The priority for this frame is carried all along the path, as shown in Figure 8. The same operation is repeated when a PLC sends RT channel traffic back to the IO controller, as shown in Figure 8.

**Figure 8 Traffic Flow of PROFINET in Wireless Switches**



# PROFINET Traffic Flow

A variety of exchanges occur in the PROFINET domain, including:

- Topology discovery by the TIA Portal
- Configurations pushed from the TIA Portal to all the devices
- Alarms between the IO device and the TIA Portal
- PLC-to-PLC communication

Figure 9 and Table 2 describe at a high level the information and types of exchanges occurring in PROFINET.

**Figure 9 High-level Overview of the Exchanges Occurring in PROFINET**

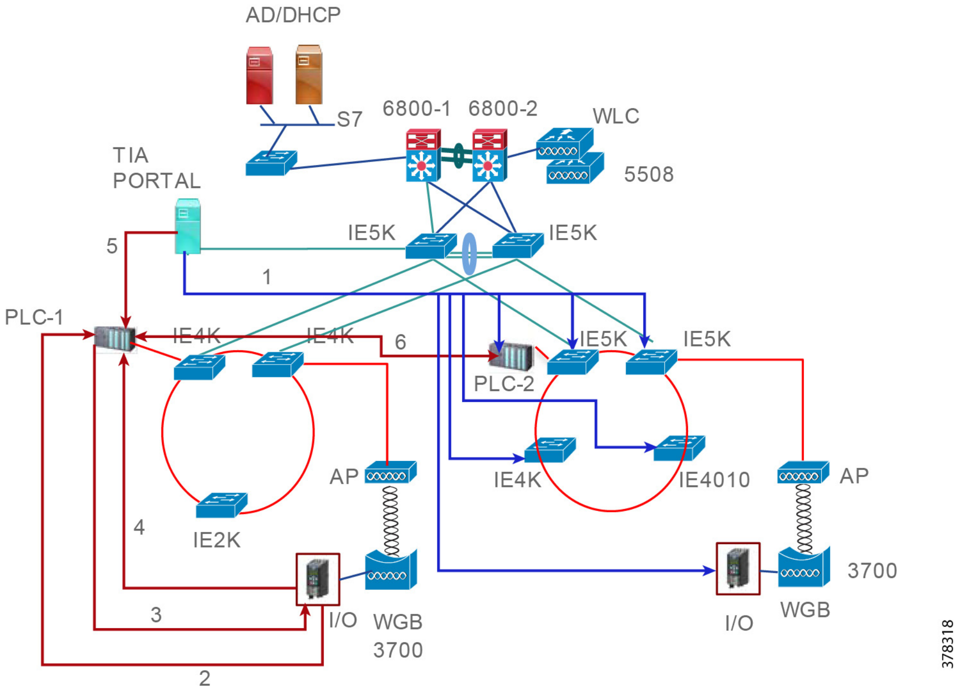


**Table 2 Exchanges in PROFINET**

| Traffic Number | Description | From | To | Protocol | Type |
|---|---|---|---|---|---|
| 1 | TIA Portal uses PN-DCP or LLDP to discover all the devices to configure the device name and the IP address. | TIA Portal | All PROFINET devices | PN-DCP/LLDP | RT/NRT |
| 2 | Alarms | Device | PLC | PROFINET | RT |
| 3 | Process data | PLC | Device | PROFINET | RT |
| 4 | Process data | Device | PLC | PROFINET | RT |
| 5 | Configuration pushed from the TIA Portal | TIA Portal | PLC | TCP/IP | NRT |
| 6 | Controller-to-controller communication | PLC | PLC | PROFINET | RT |

# Cisco Connected Factory–PROFINET Solution Benefits

The following are the operational benefits of the Cisco Connected Factory–PROFINET solution:

- Help minimize risk factors and maximize plant operation uptime with a focus on network resiliency and application availability.
- Lower Costs–Using Media Redundancy Protocol (MRP) as a resiliency protocol along with a ruggedized but standard industrial Ethernet protocol (PROFINET) increases critical information access from machines, resiliency for some applications, and bandwidth.
- Single-pane management–Using general system description (GSD) files, a single supervisor (such as TIA Portal) tool can manage Industrial Automation System devices, as well as Cisco Industrial Ethernet switches.

## Use Case Overview

As discussed in the introduction, certain industrial devices need to roam around the factory so enabling wireless access for those devices facilitates their roaming capability. This section describes different mobility scenarios that would typically occur in a factory.

- Stationary use case—As the name suggests, this use case covers the scenario where the industrial automation endpoint is at a fixed location and is accessing the network through a wireless medium. As explained in the Introduction, wireless access is preferred medium for end point devices in situations where it is difficult or nearly impossible to install wire cables.
- Roaming within an access point—This use case covers a scenario where the IO device moves within the same access point.
- Roaming within a cell zone—This use case is one of the important aspects of roaming. The IO device roams to a new access point and, during this process, the PLC should not experience any timeouts. During movement, a handoff occurs between the old access point and the new access point and the application must remain transparent throughout the process.
- Roaming inter cell—This use case covers a scenario when an IO device has to perform plant-wide roaming. In an ideal scenario, the IO device or PLC should be able to roam to a different cell and still be able to connect to the other PLC. However, this use case has limited applicability in the PROFINET space because RT channel communication uses Layer 2 technology in PROFINET. Since each ring is on a separate VLAN, when an IO device moves to another ring it will not be able to communicate with the master PLC using Layer 2 communication.

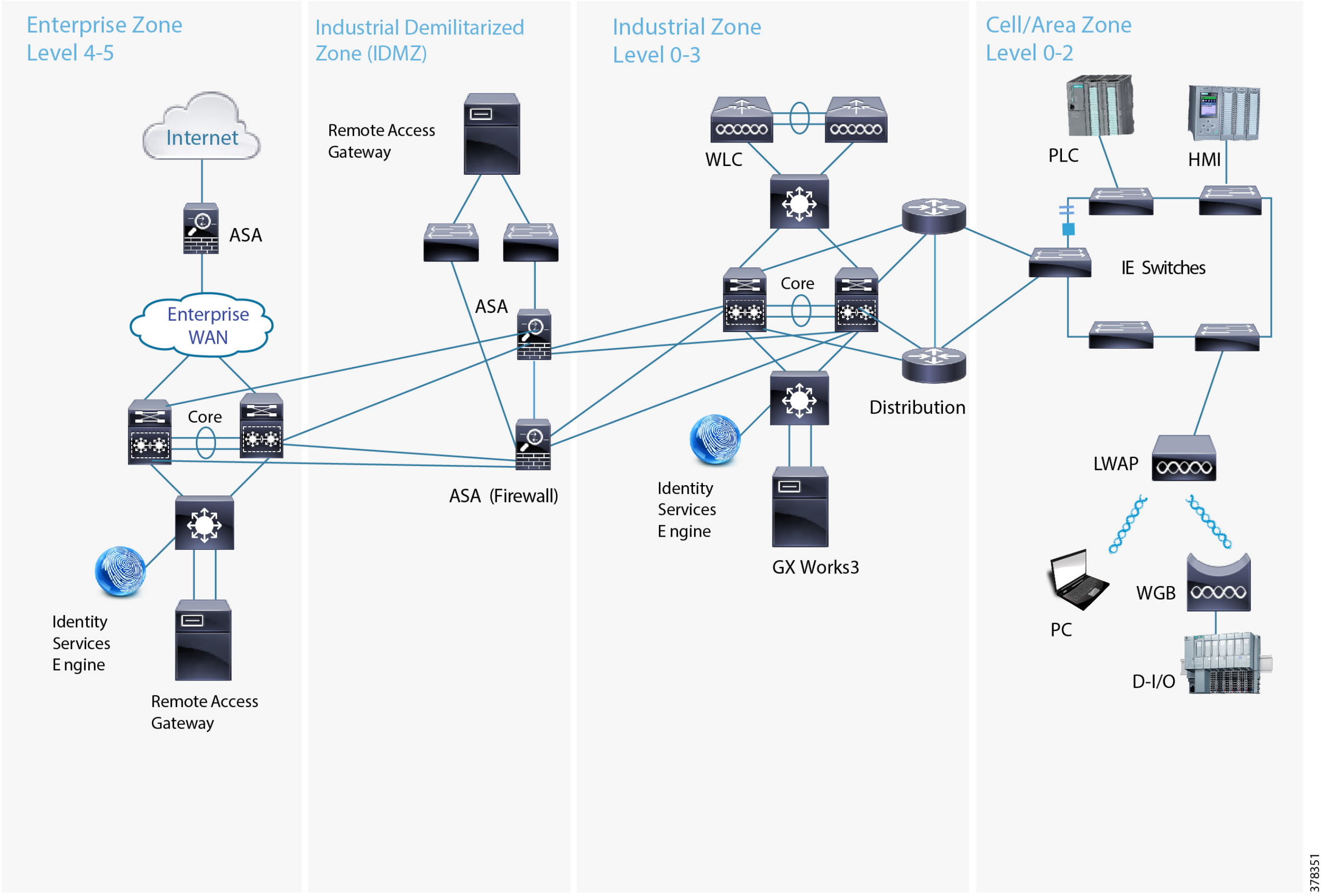
# System Design

This section covers the Cisco Connected Factory—PROFINET solution and its various systems, components, and their relation to each other. Cisco Connected Factory—PROFINET 2.0 is an architecture that provides wireless services and also network resiliency services to the devices, equipment, and applications found in an Industrial Automation System. The Cisco Connected Factory—PROFINET solution architecture overview provides the background and description of an Industrial Automation network model.

## Reference Architecture

The Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) is a common and well-understood model in the manufacturing industry that segments devices and equipment into hierarchical functions. It has been incorporated into many other models and standards in the industry. Based on this segmentation of the plant technology, the International Society of Automation ISA-99 2-2 Committee for Manufacturing and Control Systems Security has identified the levels and logical framework shown in Figure 10. Each zone and the related levels are described in detail below.

**Figure 10 Complete Network Architecture**



## Cell/Area Zone

The Cell Area zone is a functional zone where the industrial automation devices interact with each other. It can be visualized as a kitchen area where the chefs prepare the food. The network is a critical factor because all the automation devices must communicate to ensure that goods are produced. A plant factory may have one or multiple cell zones. Each cell can have the same or different topologies. In Figure 10, the diagram on the left represents the one used in this design for validating the PROFINET 2.0 solution.

## Manufacturing Zone

The Manufacturing zone comprises the Cell/Area zones (Levels 0 to 2) and site-level (Level 3) activities. The Manufacturing zone is important because all the IACS applications, devices, and controllers critical to monitoring and controlling the plant floor IACS operations are in this zone. To preserve smooth plant operations and functioning of the IACS applications and IACS network, this zone requires clear logical segmentation and protection from Levels 4 and 5 of the plant/enterprise operations.

# System Components

Table 3 lists all the Cisco components that are involved in this design.

**Table 3 Cisco Components**

| Role | Model | Software Release | Comments |
|---|---|---|---|
| Cisco Layer 2 Industrial Ethernet Switch | Cisco IE2000<br>Cisco IE4000<br>Cisco IE5000<br>Cisco IE4010 | 15.2(5.5.03i)E2<br>15.2(5)E2<br>15.2(5)E2<br>15.2(5.5.03I)E2<br>15.2(5)E2c or 15.2(6)E0a (preferred) | Provides connectivity to Level 0-2 devices.<br>If MRP ring managed by TIA Portal is desired, 15.2(6)E0a for Cisco IE4000 is required.<br>15.2(5)E2c only supports CLI MRP on Cisco IE2000, Cisco IE4000, and Cisco IE5000. |
| Cisco WLC | Cisco 5508 WLC | 8.4.1 | Supports VLAN-0 and PROFINET |
| Cisco AP | Cisco AP3700 | 15.2(4)JB6 | Supports VLAN-0 and PROFINET |
| Cisco Work Group Bridge | Cisco 2700/Cisco IW3700 | 15.3(3)JD | Supports VLAN-0 and PROFINET capability. |
| Cisco Layer 3 Distribution switches | Cisco IE5000 | 15.2(5)E2<br>15.2(5)E2c or 15.2(6)E0a (preferred) | Provides aggregation to Cell/Area zones MRP ring. |
| Core | Cisco Catalyst 6880 | 15.2(1)SY1a | Provides core functionality to the design. |

## Cisco Industrial Ethernet 2000 Series Switches

The Cisco Industrial Ethernet 2000 series switches are designed for low cost, low ports, and small sizes and offer:

- Four, eight, or 16 10/100Base-T Ethernet ports (Small Form-Factor Pluggable [SFP] downlinks on selected models); fixed configurations with a compact form factor
- Two Gigabit combo ports: SFP (100 Mbps and 1 Gbps) or RJ45 uplink
- Dual-input DC power supply, alarm relays, DIN rail mountable
- Industrial Power over Ethernet (PoE) solution
- Conformal coating available
- Swappable SD flash card and mini-USB connector
- Industrial environmental compliance and certifications
- Industrial partner applications: EtherNet/IP and PROFINET
- Support for ring protocols REP and MRP

For more details about various SKUs, refer to the data sheet at:
http://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-2000-series-switches/datasheet-c78-730729.html

## Cisco Industrial Ethernet 4000 Series Switches

The Cisco Industrial Ethernet 4000 series switches offer:

- Bandwidth and capacity to grow with your networking need: 20-Gbps nonblocking switching capacity with up to 20 Gigabit Ethernet ports per switch

- Cisco IOS Software features for smooth IT integration and policy consistency
- Robust resiliency enabled by dual ring design via 4x Gigabit Ethernet uplink ports, Resilient Ethernet Protocol (REP), Media Redundancy Protocol (MRP), Parallel Redundancy Protocol (PRP), Etherchannel and Flexlink support, and redundant power input
- True zero-touch replacement for middle-of-the-night or middle-of-nowhere situations
- Simplified software upgrade path with universal images
- Industrial environmental compliance and certifications
- Industrial partner applications: EtherNet/IP and PROFINET
- Supports MRP and MRP Automanager managed by CLI or TIA Portal

For more details about various SKUs, refer to the data sheet at:
http://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4000-series-switches/datasheet-c78-733058.html

## Cisco Industrial Ethernet 5000 Series Switches

The Cisco Industrial Ethernet 5000 series switches offer:

- Bandwidth and capacity to grow with your networking need: High performance nonblocking switch capacity with up to 24 Gigabit Ethernet downlink ports and four 10 Gigabit or four 1 Gigabit Ethernet uplink ports per switch.
- Robust resiliency enabled by features such as a dual-ring design through four 10 Gigabit Ethernet uplink ports, REP, Etherchannel, Flexlink, and redundant power input.
- Supports PROFINET MRP and MRP Auto manager (via CLI).

For more details about various SKUs, refer to the data sheet at:
http://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-5000-series-switches/datasheet-c78-734967.html

## Cisco Catalyst 6880-X Product Details

The Cisco Catalyst 6880-X provides flexibility to build the desired port density through two versions of the base chassis (C6880-X-LE with standard FIB/ACL/Netflow tables and C6880-X with larger FIB/ACL/Netflow tables) along with optional port cards. The base chassis comes with 16 10G/1G ports and each port card supports 16 additional 10G/1G ports. Each system can be built up to 80 ports in 16-port increments. The port interface on the base module and the port cards support both 10 Gigabit Ethernet and 1 Gigabit Ethernet speeds allowing customers to use their investment in 1 Gigabit Ethernet SFP and upgrade to 10 Gigabit Ethernet SFP+ when business demands change, without having to do a comprehensive upgrade of the existing deployment. The port cards are hot swappable. For further information, refer to:
http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6880-x-switch/data_sheet_c78-728228.html

## Cisco 5508 Wireless Controller

The Cisco 5500 Series Wireless Controller (WLC) is a highly-scalable and flexible platform that enables system wide services for mission-critical wireless networking in medium-sized to large enterprises and campus environments. Designed for 802.11ac and 802.11n performance and maximum scalability, the Cisco 5500 Series offers enhanced uptime with:

- RF visibility and protection
- The ability to simultaneously manage up to 500 access points
- Superior performance for reliable streaming video and toll- quality voice

- Sub-second stateful failover of all access points and clients from the primary to standby controller

For further information, refer to:
http://www.cisco.com/c/en/us/products/collateral/wireless/5500-series-wireless-controllers/data_sheet_c78-521631.html

## Cisco IW3702 Industrial Access Point

The access point is an IEEE 802.11a/b/g/n/ac compliant, dual-band WiFi access point with external antennas.

The access point is IP67 rated, ruggedized, and certified for on-board rail and outdoor use cases such as train and trackside, mining, intelligent transportation systems, and smart city applications. You can mount the access point on a DIN rail in an industrial enclosure. Its components are designed to withstand extremes in temperature, vibration, and shock common in industrial environments.

The access point features:

- IEEE 802.11a/b/g/n compliant operation
- IEEE 802.11ac Wave 1 support
- Dual-radio design for 2.4 GHz and/or 5 GHz bands
- 4x4 multiple-input multiple-output (MIMO) technology with three spatial streams
- Cisco CleanAir support for 20, 40, and 80 MHz channels
- DC input port (M12 connector)
- 2 Power over Ethernet (PoE) ports with M12 X-code connectors:
  - 1 x PoE-IN Gigabit Ethernet port compliant with IEEE 802.3at POE+ PD
  - 1 x PoE-OUT Gigabit Ethernet port compliant with IEEE 802.3af POE PSE
- RS232 console port with cover (RJ-45 connector)
- Four antenna ports (N connector-female)
- Rugged IP67 rated housing and -40 to 167° F (-40 to 75° C) operating temperature range (ambient-without solar loading or wind cooling)
- Compact size for space constrained environments

For further information, refer to:
http://www.cisco.com/c/en/us/td/docs/wireless/outdoor_industrial/iw3702/hardware/install/guide/b_iw3702_gsg.html - con_1150688

## Cisco Access Point 2700

The Cisco Aironet® 2700 Series of Wi-Fi Access Points (APs) delivers industry-leading 802.11ac performance at a price point ideal for plugging capacity and coverage gaps in dense indoor environments. The Aironet 2700 Series extends 802.11ac speed and features to a new generation of smartphones, tablets, and high-performance laptops now shipping with the faster, 802.11ac Wi-Fi radios.

The Aironet 2700 series supports 802.11ac "Wave 1" In its first implementation, providing a theoretical connection rate of up to 1.3 Gbps, which is roughly triple the rates offered by today's high-end 802.11n APs. The boost helps you stay ahead of the performance and bandwidth expectations of today's mobile worker, who usually uses multiple Wi-Fi devices rather than just one. As such, users are adding proportionally larger traffic loads to the wireless LAN, which has outpaced Ethernet as the default enterprise access network.

For further information, refer to:
http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2700-series-access-point/datasheet-c78-730593.html

# System Design Considerations—Cell Area Zone

Plant operators and control engineers must consider many factors to successfully deploy PROFINET in the cell/area zone. The PROFINET 1.0 solution (https://www.cisco.com/c/dam/en_us/solutions/industries/docs/manufacturing/profinet-implementation-guide.pdf) describes many factors that should be considered for successfully deploying PROFINET in the cell/area zone. We want to leverage the foundation work in PROFINET 1.0 and expand it by providing design/implementation guidance for wireless connectivity to some end points. To keep the design guide to a reasonable size, we do not repeat the considerations already provided in PROFINET 1.0, but rather focus on the additional factors that are required for wireless and resiliency considerations.

One of the key questions that arises when implementing the wireless solution in a cell/area zone is whether industrial applications can use wireless technology to achieve benefits related to roaming and also meet the requirements for real time communication and network availability. To achieve the objectives mentioned earlier, we need to consider the following factors:

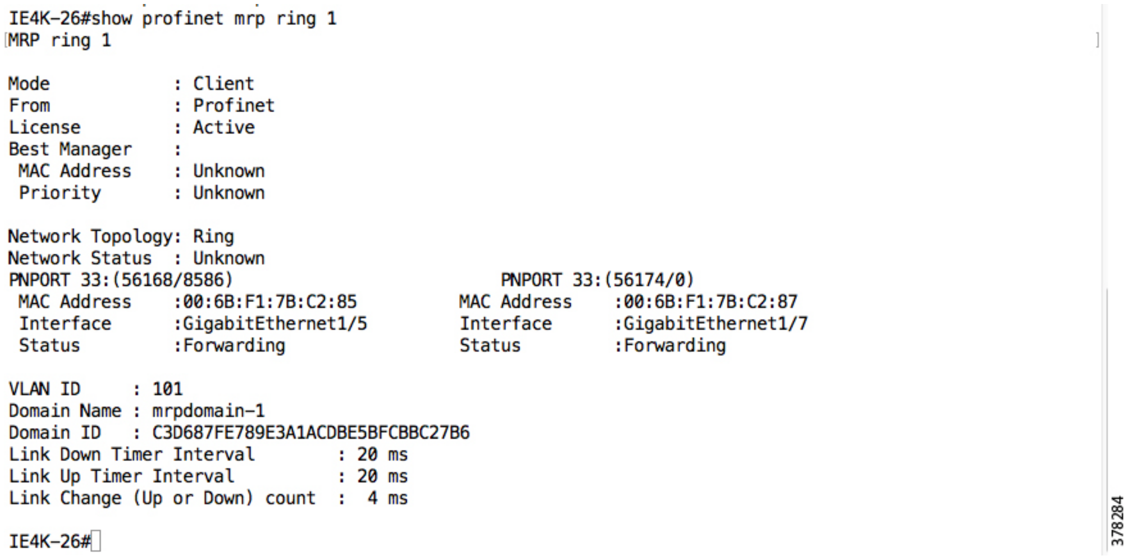
- Manageability
- Network Resiliency
- VLAN Design
- Routing Design
- Wireless Architecture

## Manageability

We discuss manageability first because many of the network architecture decisions made in this design guide are dependent on ensuring that manageability is a primary design consideration. The design goal was to ensure that we could configure all the Cisco IE switches and Siemens PLCs using a single automation tool. Research with customers indicated that TIA Portal is a standard tool that is widely used by PROFINET customers. TIA Portal is used to configure both Cisco IE switches and Siemens equipment using General Station Descriptor (GSD) files. A GSD file, which is provided by the device manufacturer, contains a description of the PROFIBUS DP/PA or PROFINET device. GSD files provide a way for an open configuration tool to obtain the device characteristics automatically. Using TIA Portal not only configures the PROFINET protocol, but it offers other benefits such as programming the PLC and managing the HMI devices.

In the PROFINET world, we group devices by a domain. When using MRP, all the devices that are part of a ring become part of a domain. Figure 11 shows a Cisco IE switch as part of a domain.

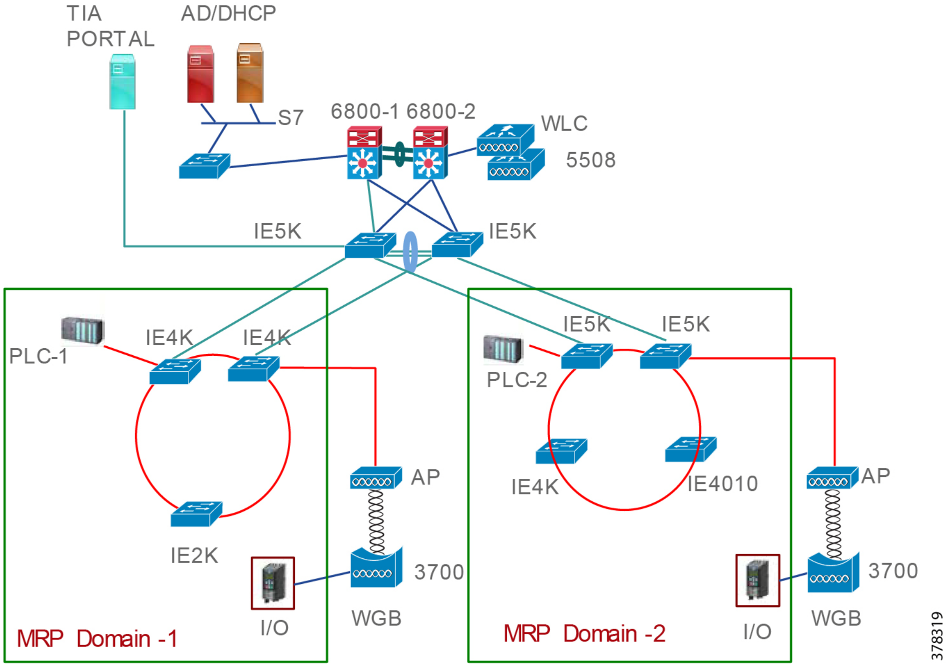
### Figure 11 MRP Domain



```
IE4K-26#show profinet mrp ring 1
MRP ring 1

Mode             : Client
From             : Profinet
License          : Active
Best Manager     :
 MAC Address     : Unknown
 Priority        : Unknown

Network Topology: Ring
Network Status  : Unknown
PNPORT 33:(56168/8586)                          PNPORT 33:(56174/0)
 MAC Address     :00:6B:F1:7B:C2:85          MAC Address     :00:6B:F1:7B:C2:87
 Interface       :GigabitEthernet1/5         Interface       :GigabitEthernet1/7
 Status          :Forwarding                 Status          :Forwarding

VLAN ID     : 101
Domain Name : mrpdomain-1
Domain ID   : C3D687FE789E3A1ACDBE5BFCBBC27B6
Link Down Timer Interval        : 20 ms
Link Up Timer Interval          : 20 ms
Link Change (Up or Down) count  :  4 ms

IE4K-26#
```

We had two choices available to integrate TIA Portal for managing the cell zones in our design. Figure 12 shows option-1.

### Figure 12 Each Cell is in a Separate Domain



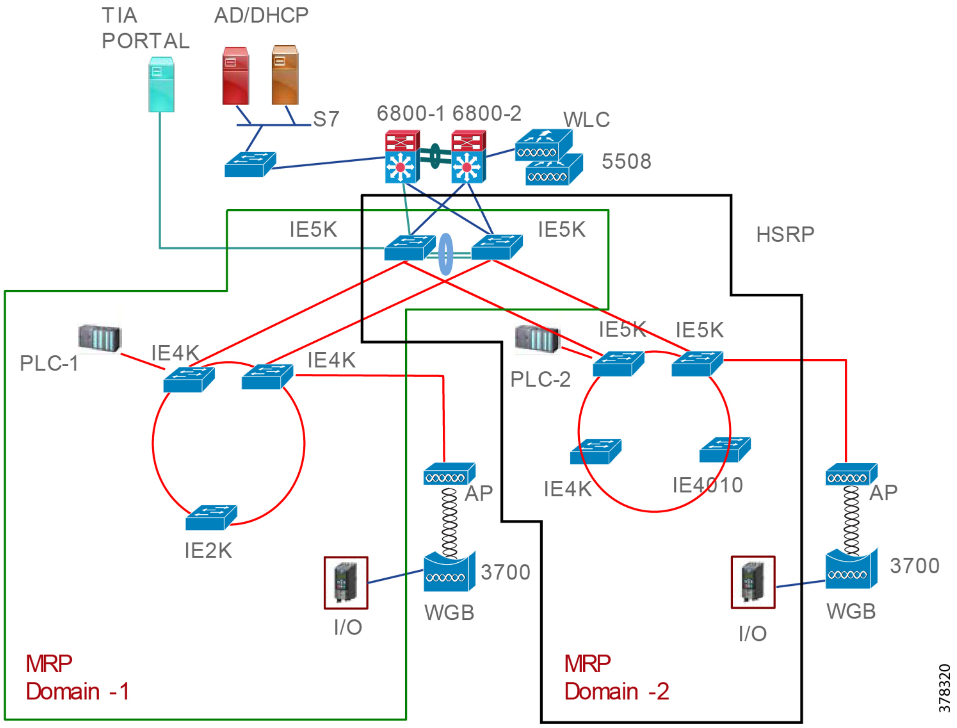
As shown in Figure 12, we have two different domains and each domain is used to manage a set of switches, PLCs, and IO devices. Each cell zone can be defined as a domain and using the above method we can connect multiple cells sharing the same distribution layer. From a TIA Portal perspective, there are two different projects and each project manages a particular domain.

We have an alternative design where we could have the individual domain extend all the way to the distribution layer, which is shown in Figure 13. The highlights of the design is that the distribution layer would become part of the access layer and each distribution switch would be part of both domains. The advantages of this design are:

- Layer 2 connectivity from the access to the distribution layer.

- Less complexity because there is no routing in the access layer.

**Figure 13 Distribution Switches Part of the Ring**



However, we observed that with the current support of Cisco IE switches we are unable to provision two domains on a single switch. As you can see in Figure 13, for multi-domain support we need Cisco IE5000 switches in the distribution layer to be part of both domains. The multi-domain support feature can be enabled with CLI option on the IOS. Since we had a goal of managing all the required equipment using a single automation portal, we have chosen design-1 as an option for this CVD.

# Network Resiliency

The primary goal of network resiliency is a network design without a single point of failure. When a failure happens at either a link level or at a device level, there must be an alternate path for communication. To achieve that goal, we have enabled the following methods:

- MRP protocol for network resiliency
- Redundant paths

## Media Redundancy Protocol

The Media Redundancy Protocol (MRP) is a data network protocol standardized by the International Electrotechnical Commission (IEC) as IEC 62439-2. The MRP operates at the MAC layer and allows rings of Ethernet switches to overcome a single failure with recovery time much faster than achievable with traditional STP. The MRP is suitable for Industrial Ethernet applications and natively supported within Cisco Connected Factory—PROFINET.

Cisco Industrial Ethernet switches support the following three roles:

- Media Redundancy Manager (MRM)—Serve as the ring manager and initiate and control the ring topology to react to network faults by sending a control packet from one ring port and receiving them on its other ring port in both directions.

- Media Redundancy Client (MRC)—Serve as member nodes of the ring, react to receive reconfiguration frames from the MRM, and detect and signal link changes on its ring ports.
- Media Redundancy Automanager (MRA)—Serve as a temporary role at device startup and a node must transition to the MRM role or the MRC role after startup.

The MRA role is not an operational MRP role like MRM or MRC. If configured to start as MRA, the node or nodes select an MRM using a voting protocol and configured priority value. The remaining MRAs transition to the MRC role.

MRA is a new released feature. As of this document's publication, it only applies to Cisco IE 4000 and Cisco IE 5000 switches through the CLI. This solution doe not implement MRA.

**Note:** At power on, all MRAs begin the manager voting process. Each MRA begins to send MRP_Test frames on both ring ports. The MRP_Test frame contains the MRA's priority value. The remote manager's priority value contained in the received MRP_Test frames are compared with the MRA's own priority. If its own priority is higher than the received priority, the MRA sends a negative test manager acknowledgment (MRP_TestMgrNAck) frame, along with the remote manager's MAC address. If the receiving MRA receives an MRP_TestMgrNAck with its own MAC address, the receiving MRA initiates the transition into the client (MRC) role. The MRP_TestPropagate frame informs other MRA devices in the client role about the role change and the new higher priority manager. The clients receiving this frame update their higher priority manager information accordingly. This ensures that clients remain in the client role if the monitored higher priority manager role changes.

Special poll packets which can traverse blocked ports are sent around the ring and monitored by the Ring Manager. If the Ring Manager does not see its poll packets come back around the ring, it knows that one of the switch nodes, or even a switch/hub that does not support MRP, has failed. The Ring Manager will then unblock its port and resume the forwarding of packets on both of its ring ports. All devices on switches, except the failed node, will again have a path to each other.

During these topology change events, the various switches on the ring will be informed to clear the MAC tables that they have built so they can re-learn the port-to-destination MAC addresses of the devices connected to the ring.

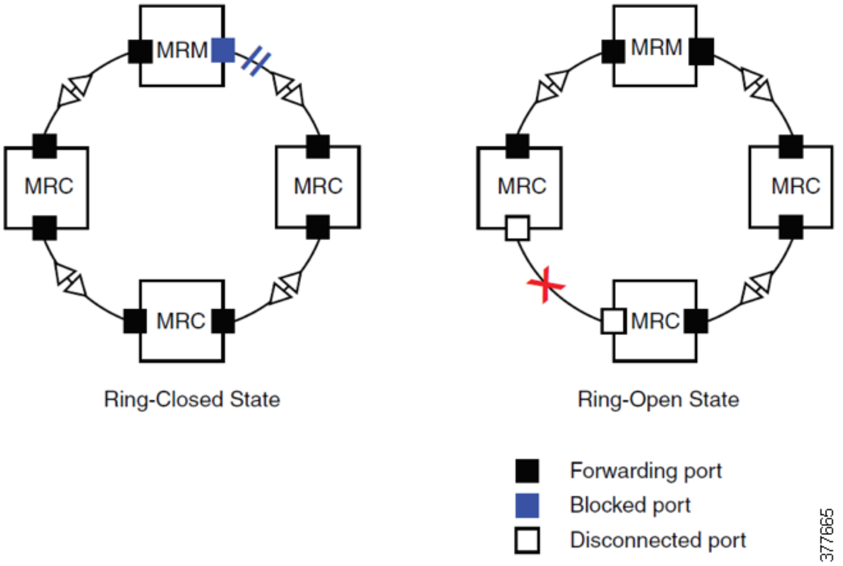
MRM and MRC ring ports support three status conditions:

- Disabled—Disabled ring ports drop all the received frames.
- Blocked—Blocked ring ports drop all the received frames except the MRP control frames.
- Forwarding—Forwarding ring ports forward all the received frames.

### Ring Status

- Closed—During normal operation, the network operates in the closed state. In this status, on MRM one ring port remains in a blocked port state and the other works in forwarding port status on all MRCs in the ring. In the ring, both ports stay in the forwarding state. The MRP protocol avoids loops because the MRP protocol reduces the physical ring topology to a logical, linear topology. Figure 14 shows the behavior.

### Figure 14 Ring–Closed State and Ring–Open State



- Open—When a network link or device fails, the ring transitions to the open status. For example, in a case of failure of a link connecting two MRCs (as shown in Figure 14), MRM will not receive the control frame and move both its ring ports to the forwarding state. The MRCs adjacent to the failure have a disconnected and a forwarding ring port, preventing traffic from attempting to utilize the failed segment.

Table 4 shows the key advantages of MRP compared to RSTP considering the roles defined in Figure 15.

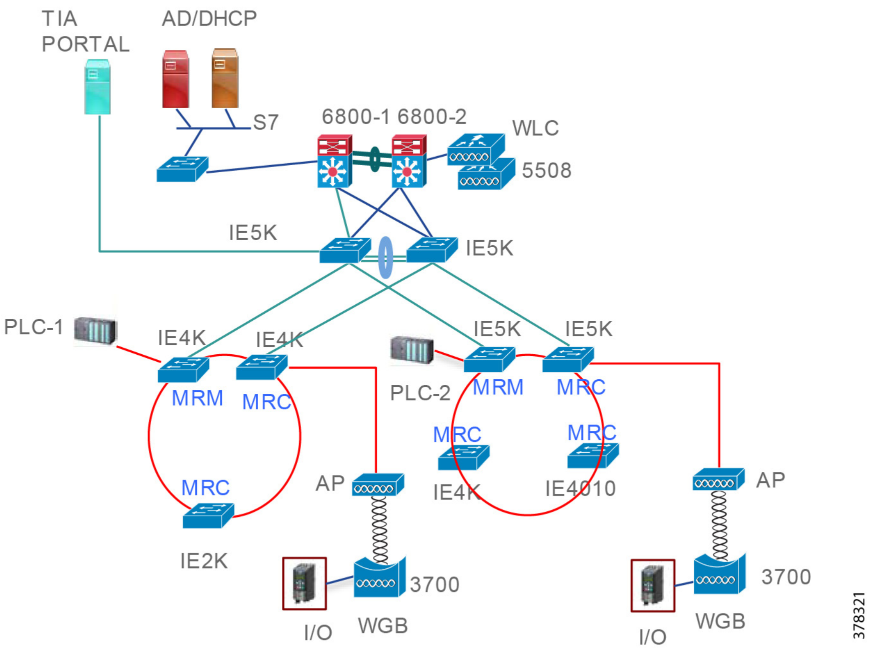
### Table 4 MRP–RSTP Comparison

| | MRP | | RSTP | |
|---|---|---|---|---|
| Loops | No | + | Possible | - |
| Duplicated packets | No | + | Possible | - |
| Deterministic failover time | Yes | + | No | - |
| Failover time versus number of switches in ring | Nearly independent | + | Increases with every additional switch | - |
| Failover control based on physical link | Yes | + | Yes | + |
| Failover control based on data layer link | Yes | + | Yes, but slow | - |
| Implementation effort and resources needed | Low | + | Medium | - |

- Fast Convergence—MRP can provide convergence times of 200ms.
- Link integrity—MRP does not use an end-to-end polling function between edge ports to verify link integrity. It implements local link failure detection.
- MRP-STP Interoperability—MRP works with STP to prevent unwanted broadcast loops in the event that a user accidentally connects a device that does not participate in the MRP ring. In a network operating with MRP and STP, spanning tree BPDUs are not sent on MRP-enabled ports. If ports are unconfigured from an MRP ring, then the ports are added to the spanning tree.
- Device level ring support—Since MRP is an inbuilt resiliency protocol for PROFINET, a Cisco Industrial Ethernet switch can form a ring with Industrial Automation System devices, such as PLC, Remote IO, etc.

In the current CVD, we have two rings and Figure 15 illustrates how we have defined the roles.

**Figure 15 Roles of Individual Switches in the Ring**



The MRP protocol is a standards-based protocol. In order to use MRP with PROFINET devices, we need to first enable MRP PROFINET mode. The switch supports one MRP ring (one VLAN) with the mrp-manager license and one MRP ring in the same VLAN. Support for multiple MRP rings is available only through the CLI or Web Device Manager tool, not in PROFINET mode. Cisco IE switches support 50 MRCs per ring. MRP cannot run on the same interface (port) as Resilience Ethernet Protocol (REP), Spanning Tree Protocol (STP), Flex Links, or Dot1X. STP does not run on MRP segments and MRP interfaces drop all STP BPDUs.

MRP Media Redundancy Manager (MRM) defines its maximum recovery times for a ring in the following range: 10 ms, 30 ms, 200 ms, and 500 ms. The default maximum recovery time on the Cisco IE switch is 200 ms for a ring composed of up to 50 nodes. You can configure the switches to use the 500 ms recovery time profile according to the size of ring.

# VLANs

The logical segmentation of a LAN in a Cell/Area Zone is driven by factors such as separation of real-time communication between Industrial Automation System devices, security, or segmentation of the network based on applications, such as IP camera and IP phones, which could be using the same network. Design subnets or VLANs to be small for easier maintenance of real-time communication and reduce the number of broadcasts in the network. VLAN segmentation also isolates faults or problems to the affected VLAN. VLANs also provide basic security by limiting the access from one VLAN to other.

Segmentation can be achieved via the following two key mechanisms in the Cell/Area network:

- Physical–Use of separate cabling and Layer 2 access switches to achieve segmentation.
- VLAN (802.1Q)–Use of the VLAN protocol to achieve a VLAN that can be implemented on the same physical infrastructure.

## VLAN Design

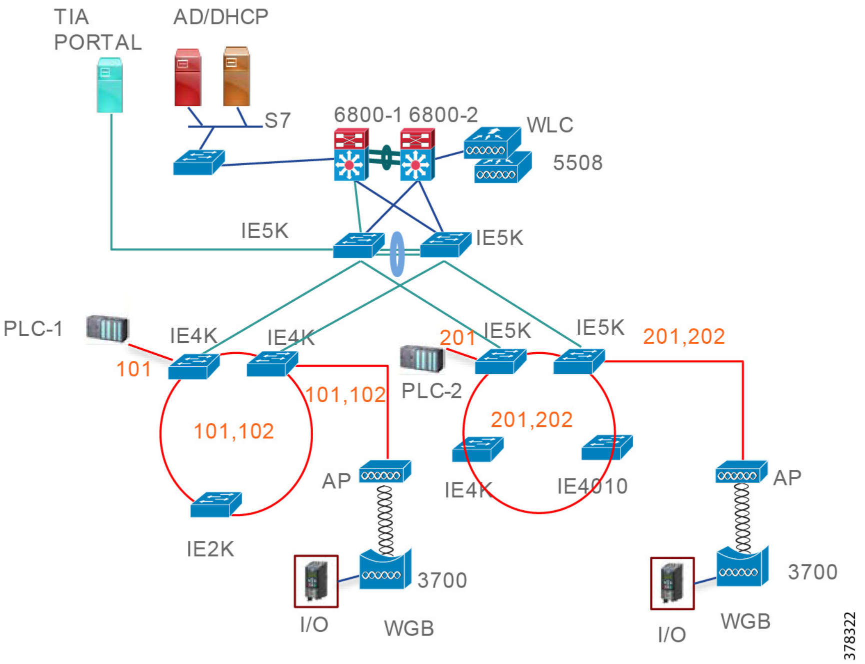
In this CVD, we have designed two different VLANs for each cell: one VLAN for PROFINET traffic for both wired and wireless and the second VLAN for management. The management VLAN was mainly for managing the wireless access points. The wireless access points use the management VLAN to connect to the Wireless LAN Controller. The WLC uses the management VLAN for all management-related operations. As illustrated in Figure 16, cell 1 has VLANs 101 and 102, where the first VLAN 101 is for the PROFINET VLAN and the second VLAN 102 is for management. VLAN 102 is a native VLAN between the switches and is also used for management of the access points. The access point would use management VLAN 102 to register to the WLC and obtain the necessary configuration information. Table 5 provides information about each VLAN and its purpose.

**Table 5 VLAN Design**

| Cell | VLAN | Purpose |
|---|---|---|
| Cell -1 | 101 | PROFINET |
| Cell -1 | 102 | Management |
| Cell -2 | 201 | PROFINET |
| Cell -2 | 202 | Management |

Figure 16 shows how VLANs are designed in the test bed.

**Figure 16 VLANs in the Test Bed**



## IP Address and Device Name Assignment

IP address planning is slightly different in a PROFINET domain because the end devices do not support DHCP. The important consideration that a network engineer should address is the fact that there is no out-of-band management for PROFINET; management is done in-band, which means that the same interface that is used for sending traffic is also used for managing the device. As mentioned in the previous section, in cell-1, for example, VLAN-101 would be used for configuring the PROFINET protocol and managing the devices. So we need to assign an IP address to each switch so that the central automation portal (TIA Portal) can use Layer 3 connectivity to manage the device. The other VLANs 102 and 202 are mainly for managing wireless access points from the WLC. Table 6 illustrates the IP address subnets for each cell.

**Table 6 Subnet Design in the Test Bed**

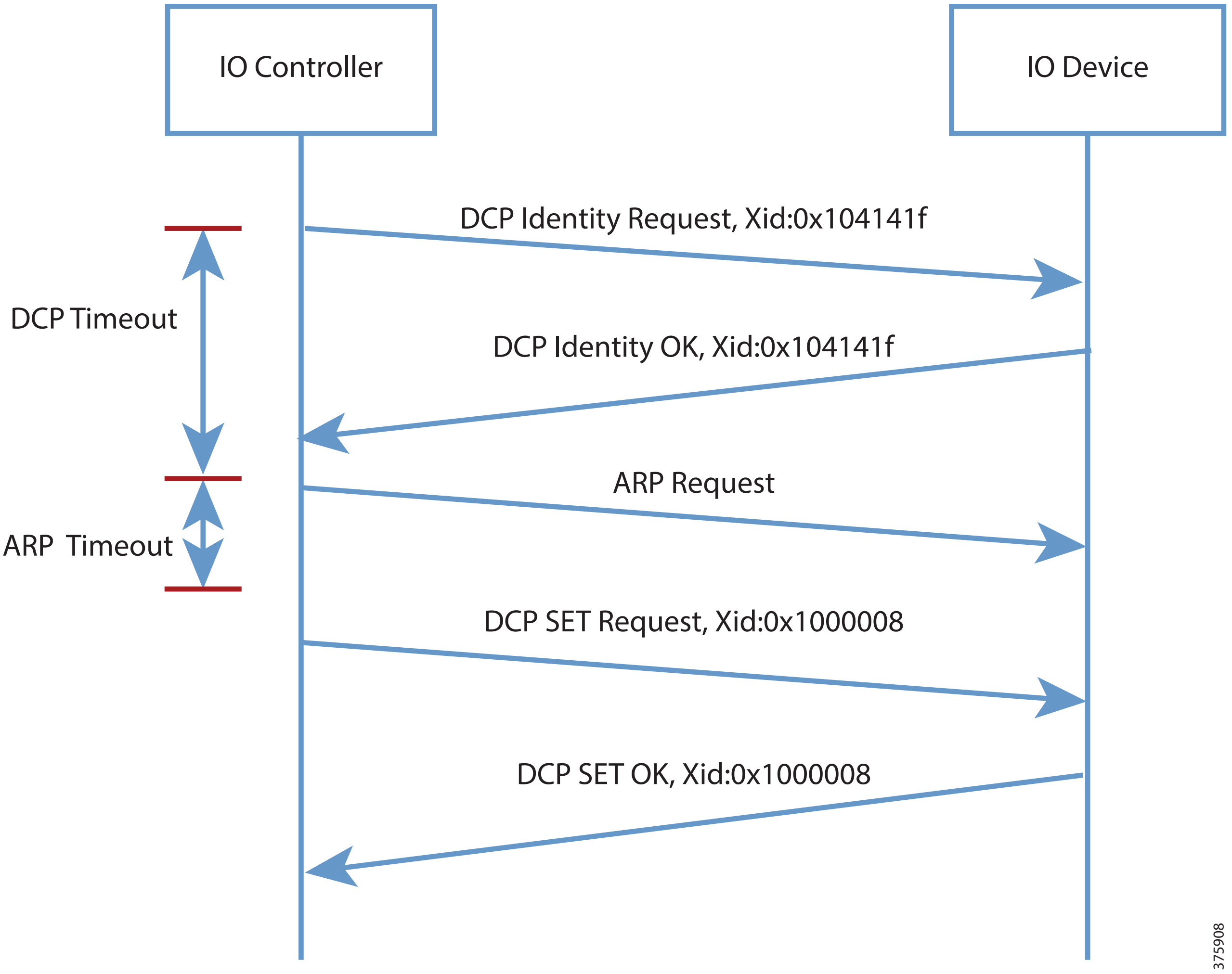
| Cell | VLAN | Subnet |
|---|---|---|
| Cell -1 | 101 | 10.20.25.0/24 |
| Cell -1 | 102 | 10.20.26.0/24 |
| Cell -2 | 201 | 10.20.8.0/24 |
| Cell-2 | 202 | 10.20.29.0/24 |

The devices in the ring are configured with a device name and IP address from the TIA Portal. From the TIA Portal work station, an engineer builds the project, sets up different devices in a ring, and then pushes the configuration to each of them. The necessary and important parameters are device-name and IP address. This information is pushed to the device using a protocol named PN-DCP, which works as follows:

- The controller sends a multi-cast frame to every device configured in the project and it requests the identity of every device by sending “Ident Req” in the PN-DCP protocol.
- Every device responds by sending “Ident Ok” and providing the name and IP address of the device.
- Then the controller sends an ARP Req to the device to learn the mac-address of the device and it uses this information for future communication.

Figure 17 depicts this behavior.

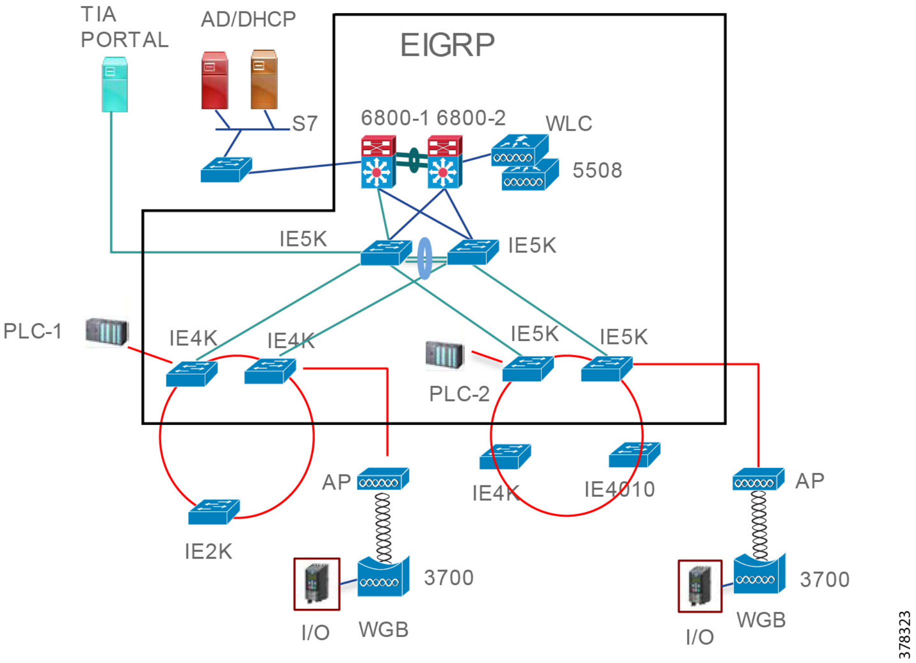
**Figure 17 PN-DCP Protocol Flow**


IO Controller
IO Device
DCP Identity Request, Xid:0x104141f
DCP Timeout
DCP Identity OK, Xid:0x104141f
ARP Request
ARP Timeout
DCP SET Request, Xid:0x1000008
DCP SET OK, Xid:0x1000008
375908

## Routing Design

We have enabled routing in the cell zone to provide alternate connectivity during link or router failures. As shown in Figure 18, EIGRP is extended to the gateway routers in each cell zone. Normally, PLC-to-PLC and PLC -IO communication happens at the cell level, so enabling static routing would have been enough for normal operation. However, as we enable new services (for future designs) such as data analytics, traffic monitoring, and security services we need to have connectivity from the cell zone to other zones, which creates an administrative burden for a network operator to manage routing table as new services are added or modified. The cell zone may also have a requirement to provide access for BYOD devices which need to be managed by IT using different security servers, such as ISE or MDM. Hence considering all the new requirements that can arise in a cell zone, it is beneficial for the network operator to design their network with routing enabled.

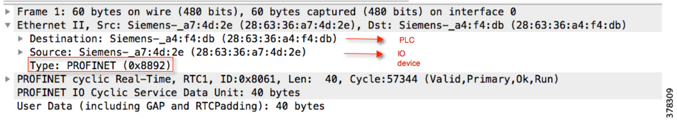
**Figure 18 EIGRP Routing Domain**



## Wireless Architecture Design

This section discusses wireless design to support the PROFINET solution. As explained in PROFINET Traffic Flow, page 7, the key components of the wireless design are the access point, WGB, and the WLC, which must support transportation of PROFINET. With the introduction of PROFINET transportation support in 8.4, PROFINET real time communication is possible in a wireless network. We have used version 8.4 on the autonomous AP that is acting as the WGB so that the WGB treats the real time traffic appropriately. Figure 19 shows a frame coming from a IO device to a WGB.

**Figure 19 Frame from an IO Device to a WGB**



```
▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▾ Ethernet II, Src: Siemens-_a7:4d:2e (28:63:36:a7:4d:2e), Dst: Siemens-_a4:f4:db (28:63:36:a4:f4:db)
  ▸ Destination: Siemens-_a4:f4:db (28:63:36:a4:f4:db)
  ▸ Source: Siemens-_a7:4d:2e (28:63:36:a7:4d:2e)
    Type: PROFINET (0x8892)
▸ PROFINET cyclic Real-Time, RTC1, ID:0x8061, Len:  40, Cycle:57344 (Valid,Primary,Ok,Run)
  PROFINET IO Cyclic Service Data Unit: 40 bytes
  User Data (including GAP and RTCPadding): 40 bytes
```

The essential point is that the WGB must be able to transport the ether type of 0x8892 over the wireless medium to the access point, then the access point must be able to transport the same ether type to the Cisco IE switch.

The other essential requirement for supporting PROFINET is the choice of the wireless architecture, centralized or FlexConnect. For a centralized wireless solution, all the traffic is tunneled from the access point to the controller and is switched from there. This means that when we want to transport PROFINET traffic, we have to tunnel the traffic to the controller and it is possible that the switch that is connected to the WLC may not be a Cisco IE switch. In this scenario, the non-Cisco IE switch may not be able to treat the real time traffic correctly. Hence we have not adopted a centralized WLC architecture. In this design, we have considered FlexConnect as the switching mode for the wireless design and the AP is connected to a Cisco IE switch.

## FlexConnect Design

FlexConnect is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect APs can switch client data traffic and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect AP can also perform local authentication.

In the Cell/Area Zone, the use of FlexConnect configurations on the wireless APs will provide the shortest path connectivity between the WGB/AP-attached equipment and the wired equipment within the Cell/Area Zone. As explained before, the idea is to switch locally in the cell and also ensure that the traffic leaving the AP enters a Cisco IE switch.

### FlexConnect Groups

We have enabled FlexConnect groups in both the cells in our network design. FlexConnect groups simplify the configuration in deploying multiple access points and also assist in faster roaming, especially when CCKM is used as an authentication mechanism between the WGB and the access point. More details on how to configure FlexConnect groups are provided in the implementation section. To obtain more information about FlexConnect groups, refer to: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010001111.html.

### Joining the Controller

Flex connect APs join the controller initially to learn about their configuration. In the FlexConnect architecture, the management of the access point still happens from the centralized controller. Many important settings outside of the assignment of IP address are made at the controller, such as SSID, authentication mechanism for clients, channel plan, etc. The advantage of using a FlexConnect architecture is that the management of the access point happens through the WLC, but the switching of the traffic occurs locally. So, joining the controller is a major step in the design.

There are two choices for an access point to obtain the IP address of the WLC:

- Statically configure the IP address of the controller.
- Get the IP address of the controller through DHCP OPTION-43.

For example, in cell -1 we have defined VLAN 102 for management and an access point in the cell-1 uses this VLAN to contact the DHCP server (10.13.48.26) and obtain the IP address of the WLC. The following configuration shows this option:

```
IE4K-26#show running-config interface vlan 102
Building configuration...

Current configuration : 94 bytes
!
interface Vlan102
 ip address 10.20.26.1 255.255.255.0
 ip helper-address 10.13.48.26
end
IE4K-26#
```

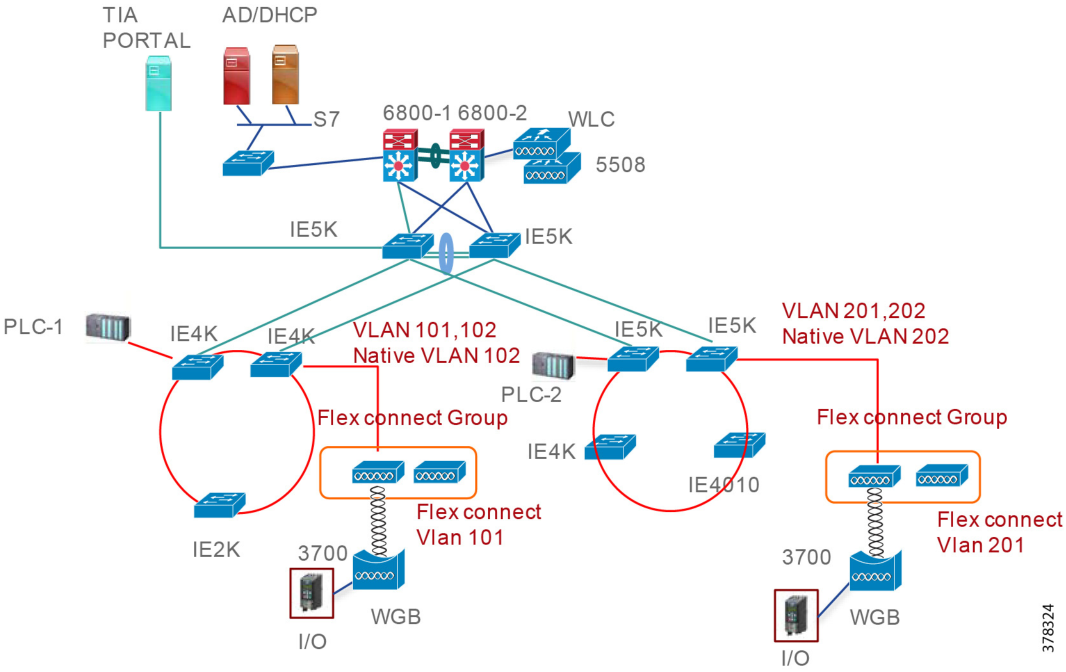
The previous step ensures that the access point knows where to go; however, we have another consideration that needs to be taken by the designer here. If the DHCP server is not configured with Option 43, then IP helper address would forward eight different UDP services listed at UDP services to the IP helper address.

However, WLC port 5246 is not in the above list and the WLC is not in the Layer 2 domain of the access point. As a result, the switch would drop the Layer 2 broadcast coming from the access point. To mitigate this problem, we can enable the following command so the switch, instead of dropping the packet, would forward the request to the controller.

```
IE4K-26#show running-config | include ip forward
ip forward-protocol nd
ip forward-protocol udp 5246
IE4K-26#
```

Figure 20 shows the FlexConnect design.

**Figure 20 FlexConnect Groups**



## Authentication Mechanisms

Authentication is an important security feature because it prevents an unauthorized access point from joining the wireless network. There are three authentication mechanisms that we considered in this design:

- OpenAuth–This is the simplest connection option between the WGB and the access point. An engineering team should use OpenAuth for a trial or a POC activity, but not for production.
- WPA2/AES PSK–WPA 2 creates fresh session keys on every association. The encryption keys that are used for each client on the network are unique and specific to that client. Ultimately, every packet that is sent over the air is encrypted with a unique key. Security is enhanced with the use of a new and unique encryption key generated out of the initial pre-shared key and there is no key reuse.
- WPA2/AES EAP + CCKM–This is a preferred method to use for a roaming scenario. The advantage of this approach is that when a client initially authenticates to the WLC, the session key derived is cached at the WLC, and when the client moves to a different AP, then the previously cached session key is used to obtain the new session key. Using the cached key at the WLC drastically cuts down the number of steps needed for a full authentication exchange. For a detailed explanation of the exchange process, refer to this Fast Roaming document: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html#anc8

## Work Group Bridge

A work group bridge (WGB) provides a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB associates to the root AP through the wireless interface. In this way, wired clients get access to the wireless network. It is also possible to implement WGB functionality with the use of a normal AP by configuring APs as WGBs. In WGB mode, the unit associates to another AP as a client. The unit provides a network connection for the devices that are connected to its Ethernet port.

One of the critical assumptions that we made in this design guide is that the end devices that need to roam do not intrinsically have wireless capability. To mitigate this, we use WGB to connect these end devices to the wireless medium. So in all of the use cases, you would see that we use end devices connected using the WGB.

## Roaming Scenarios

The advantage a wireless architecture brings is the ability for end devices to move from their locations. In industrial environments, for certain use cases, it is a requirement that devices be able to move from one place to another. The essential part of the design is to ensure that when movement occurs, the applications do not time out. The applications can tolerate a delay up to certain extent and the end device should be able to establish the connection within the tolerated threshold. Roaming consists of different scenarios such as movement within an access point, movement to a different access point, and movement across cell zones. We classify roaming within a cell as intra-cell and roaming across the cells as inter-cell.

After research with customers, we came up with the end-to-end goals shown in Table 7 that we should aim for when customers transport PROFINET over a wireless medium.

**Table 7 Critical Parameters**

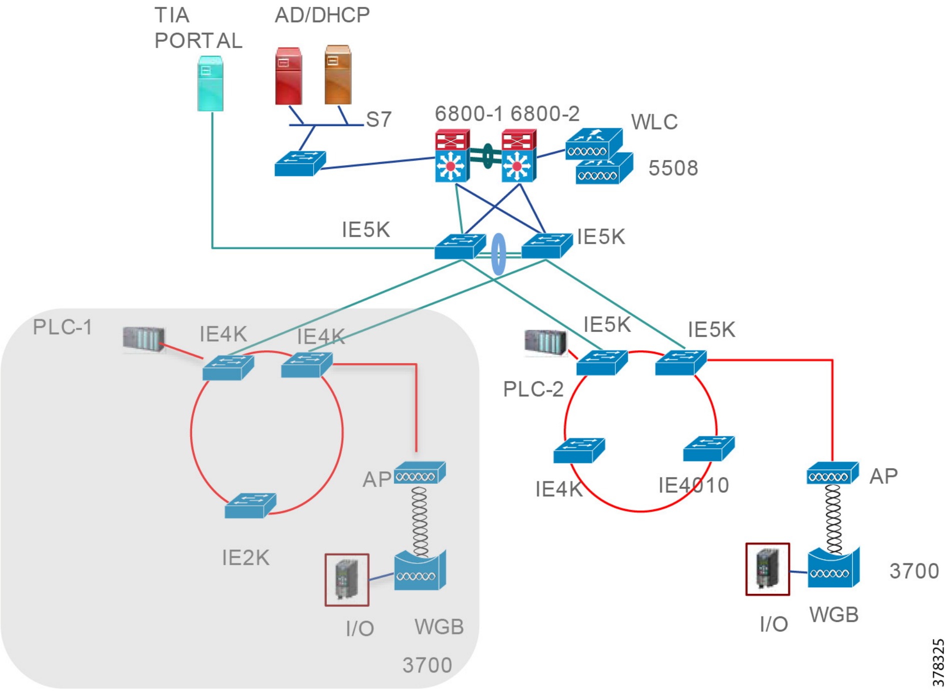
| Parameter | Target | Acceptable | Notes |
|---|---|---|---|
| PROFINET/PROFISAFE over wireless roaming | <10ms | <100ms | Outage time in roaming case. |
| PROFINET transport in wireless medium for stationary and roaming use cases. | Pass | Pass | Successful exchange of Real Time frames. |

The goal of the design is that for each of the roaming scenarios, the infrastructure must meet the critical parameters. We should note that wireless design considerations are unique and different than wired infrastructure considerations. We encourage you to consult the Wireless Design Guide (http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf) to understand the best practices for deploying a successful wireless solution. There are many important considerations for RF coverage, site survey, and frequency plan selection that are discussed at length in the Wireless Design Guide by a Cisco solution engineering team. The next sections describe in more detail the use cases we considered in this design guide. In the implementation section, we provide details about how we validated these scenarios.

### Stationary Use Case

In the stationary use case, the end device (IO device in this CVD) is connected to the controller using a WGB, but is fixed at this location. A large amount of real time traffic messages are exchanged continuously between the PLC and IO device. The important aspect is the transportation of the RT messages and the delay. Figure 21 illustrates the stationary use case.

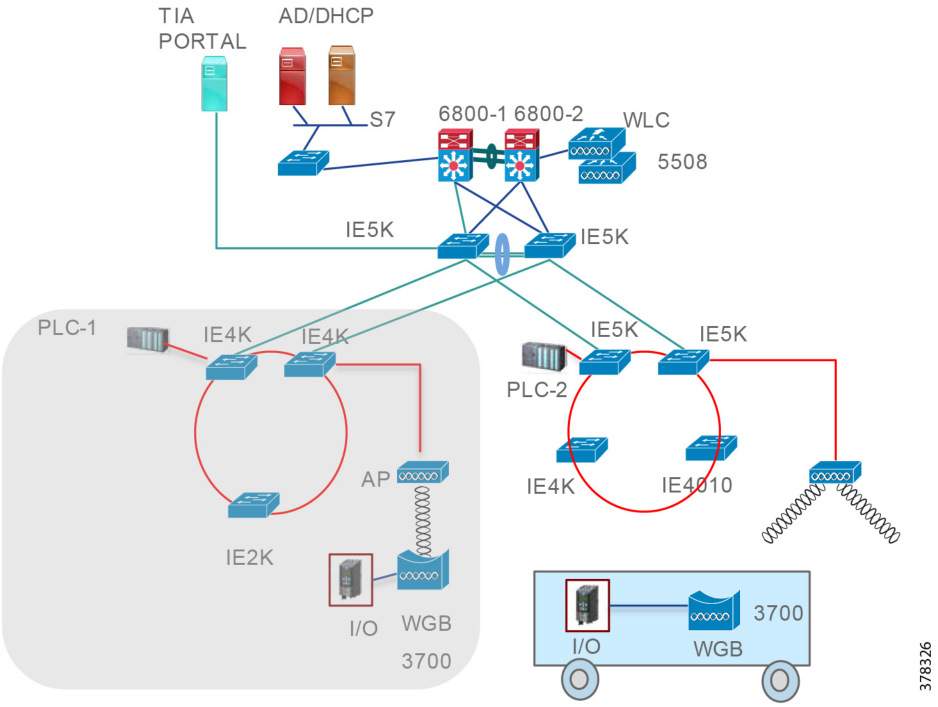
**Figure 21 Stationary Use Case**



## Roaming within an Access Point

In this use case an IO device attached to a WGB roams within the coverage area of the access point. The critical parameters are the transport of the RT messages and also the end-to-end delay. If the IO device moves within the coverage of the access point and the network engineer designed the wireless network following the considerations defined in the Wireless Design Guide (see reference above), then the critical parameters would be met. We provide more details in the implementation section.

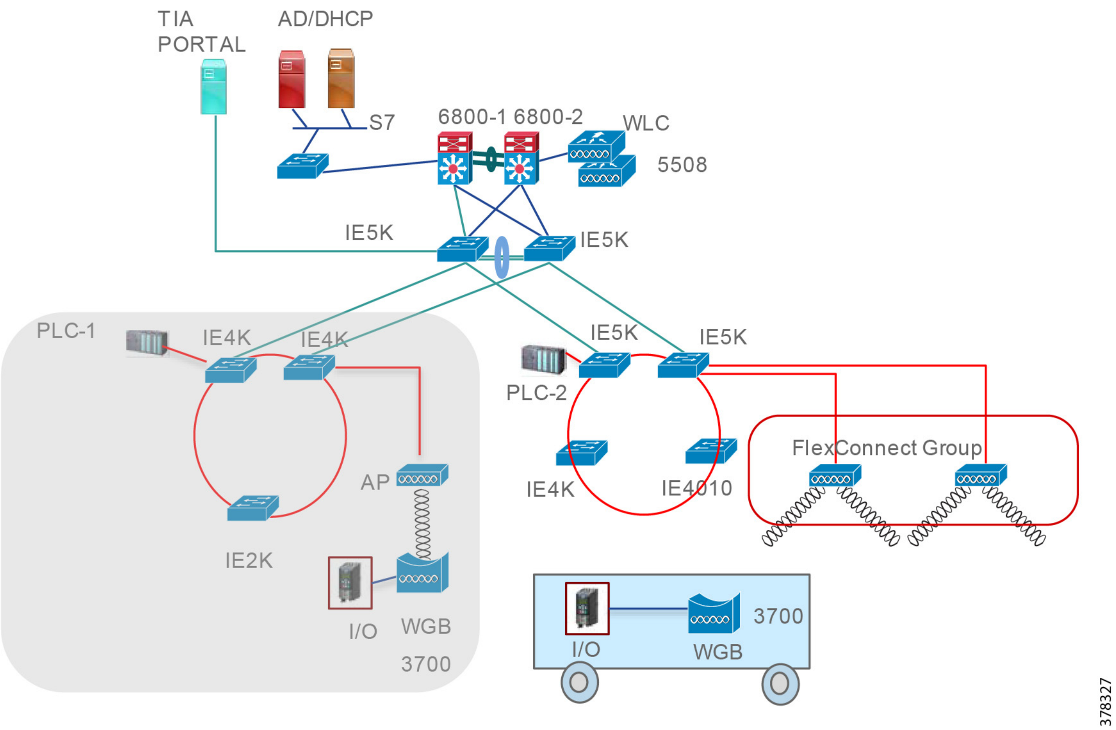
**Figure 22 Roaming within an Access Point**



## Roaming within a Cell

In this use case an end device attached to WGB roams within a cell zone, however it is a challenging use case because we want to bound the delay within the critical parameter. As you can see in Figure 23, the end device needs to disassociate and then associate with the next access point. The switch over happens due to the loss of the signal experienced by the WGB as the device roams. Once the signal strength falls below a certain value, then the WGB associates it to the next access point. We have created an application profile that times out when the delay exceeds 100 msec. and we used this application to measure if our infrastructure can keep the delay bounded to 100 msec. We provide more information about this test case in the implementation section.

**Figure 23 Roaming within a Cell**



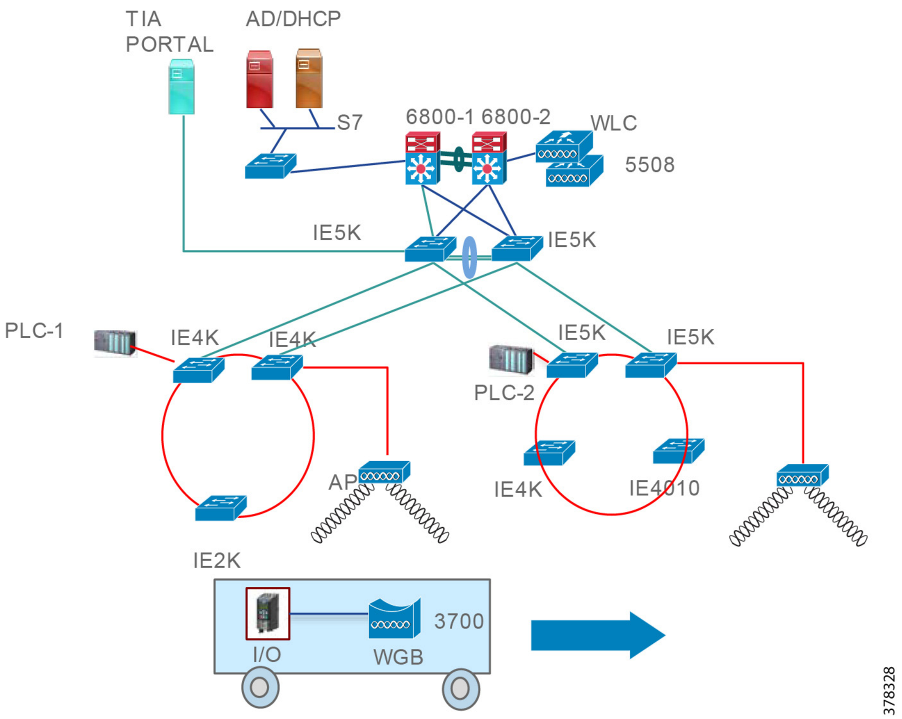
## Roaming Inter-cell

In this use case an industrial device can roam an entire factory floor. To enable this use case, we need to use the centralized architecture where the data traffic is tunneled to the WLC. If we have centralized WLAN and if a WGB connects to the same SSID as it roams the plant, then it could communicate with the controller. However, for a PROFINET implementation this design guide is not practical due to the following reasons:

- WLC may not be attached to a Cisco IE switch because of its location in the factory. Hence non-Cisco IE switches may not be able to handle the real time traffic correctly as Cisco IE switches treat them.
- In the PROFINET world, the RT communication between the PLC and IO happens in Layer 2. Hence, this communication may not happen when the traffic is transported over Layer 3.

Due to the reasons mentioned above, we do not recommend the inter-cell roaming use case depicted in Figure 24 for PROFINET implementations.

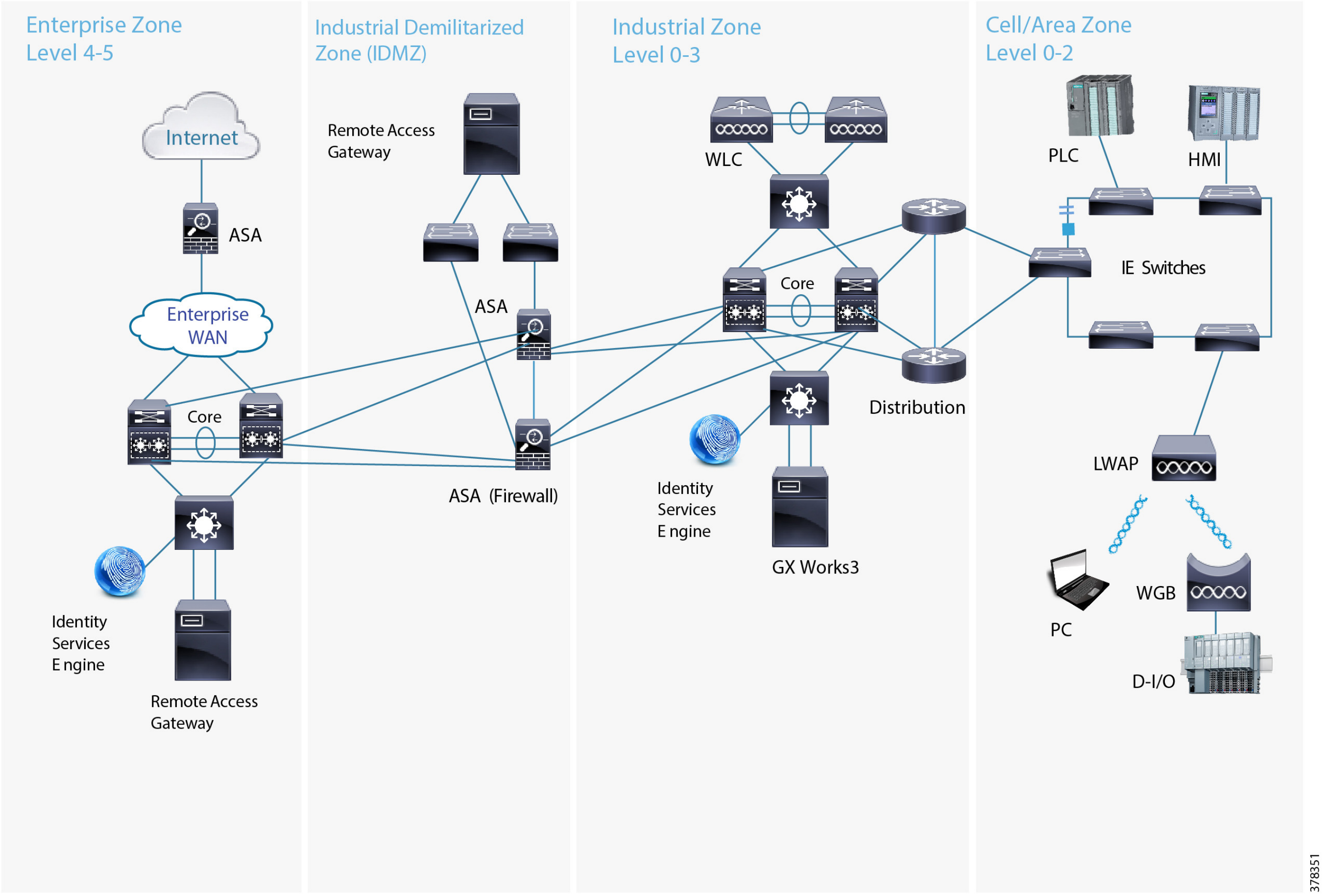
**Figure 24 Inter-cell Roaming**



# System Design Considerations—Manufacturing Zone

This section briefly discusses design considerations for the manufacturing zone. From a PROFINET perspective, most of the traffic is within cell zones. However, the management servers typically reside in the manufacturing zone, such as TIA Portal, SNMP server, Policy server, Syslog server, etc. Figure 25 shows where the manufacturing zone fits in the overall architecture:

**Figure 25 Complete Network Architecture**



- The core has a Cisco Catalyst 6800 VSS architecture, which can provide high resilience and high performance for the core services in the network.
- The entire network from the gateway routers in the cell zone and above are part of a single EIGRP routing domain, which provides connectivity across the layers.
- We are validating different designs in the cell/area zone and also different services that are built on top of these designs in a single architecture. By doing so, we can provide customers the benefit of a validated design on a standard architecture.
- Cisco Catalyst 3850 stack switches provide connectivity to all the services modules in the manufacturing zone.
- Cisco ASA firewalls control the traffic flow coming in and out of the network.

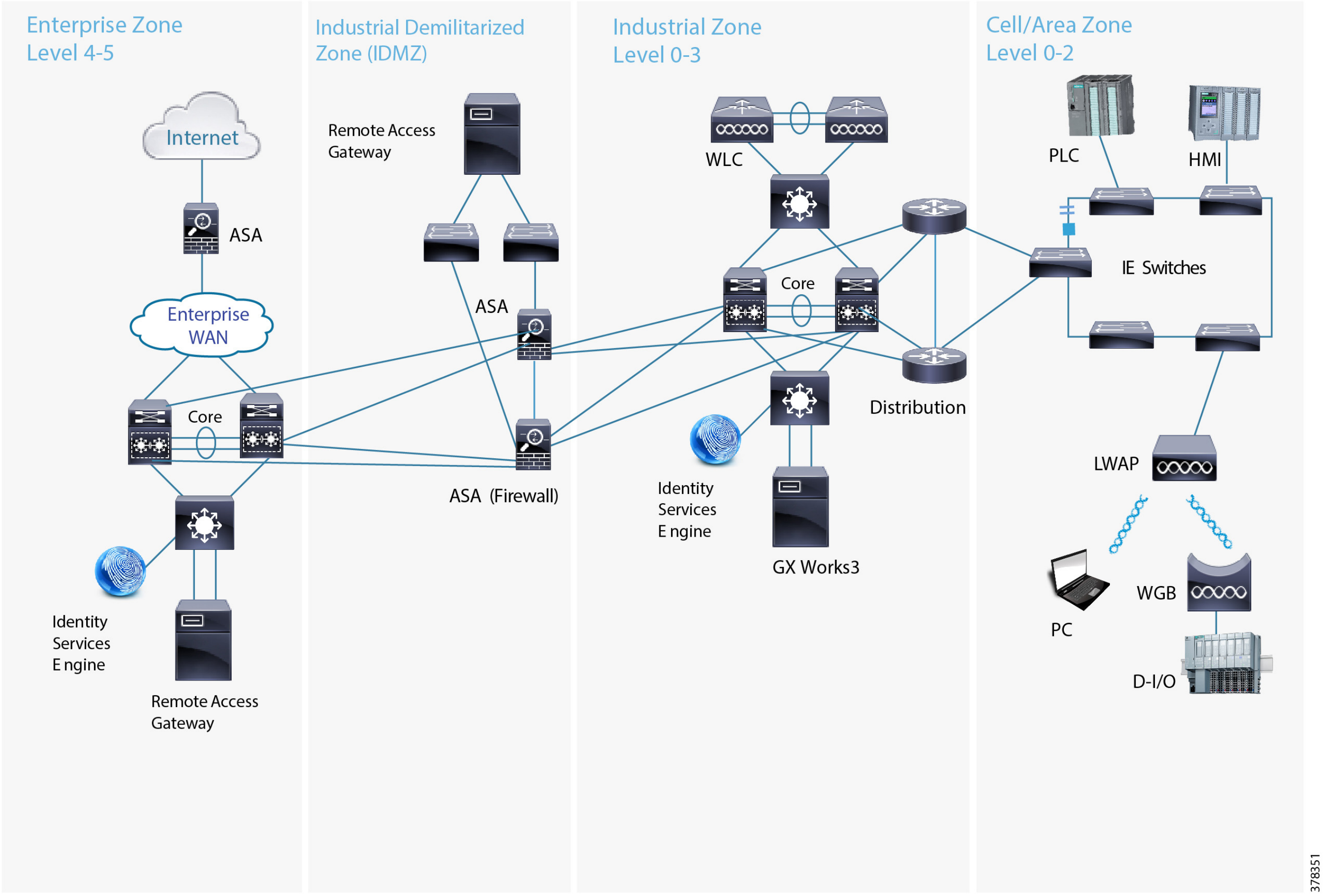
The implementation details for the manufacturing and other zones is beyond the scope of this document, but we encourage you to visit the repository of designs at Design Zone for Manufacturing–Converged Plantwide Ethernet (https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html).

# System Test Bed

At a high level, the Cisco Connected Factory—PROFINET network looks similar to a traditional enterprise campus network that uses a layered design to provide low latency, high resilience, high throughput, and secure connectivity to wired and wireless clients. However, some aspects of the Connected Factory network diverge from the typical enterprise-only campus network due to the physical requirements of an industrial setting, as well as the specific characteristics and protocols used by the connected devices. The network is divided into several layers:

- Access—The access layer provides Layer 2 (OSI model) connectivity to end devices, such as computers, industrial controllers, sensors, etc. This physical connectivity can be wired (with copper- or fiber-based Ethernet) or wireless (IEEE 802.11 WiFi). The network infrastructure physically comprises Cisco IE switches (Cisco IE2000, Cisco IE3000, Cisco IE4000, and Cisco IE5000) and WAPs.
- Distribution—The distribution layer aggregates all of the access layer switches and acts as the Layer 3 (OSI model) boundary, providing a highly-redundant, high throughput connection to the rest of the network. The network infrastructure at this layer typically includes more powerful switches, including the Cisco IE 5000 and Cisco Catalyst series switches (Catalyst 3800, Catalyst 4500, and Catalyst 6800).
- Core—The core layer is the backbone of the network. This layer is often combined with the distribution layer functions in smaller networks and provides routing, load balancing, and interconnections to other networks, as well as the IDMZ. The network infrastructure at this layer is made up of Cisco's enterprise switching portfolio including the Catalyst 4500 and Catalyst 6800 series.

**Figure 26 Connected Factory Architecture**



# Implementation Considerations–Cell Area Zone

The Cisco Connected Factory–PROFINET Cell Area Zone integrates various devices such as PLCs, Remote IO devices, drives, Human Machine Interface (HMI), and networking components such as Cisco Industrial Ethernet series switches used on a factory floor.

This section lists the steps required to implement and integrate various devices used in Cisco Connected Factory–PROFINET Cell Area Zone to configure different topologies as defined in PROFINET.

## Managing the Switches

Cisco provides multiple methods and tools to manage Cisco Industrial Ethernet Switches and Catalyst series switches, including Cisco IOS command line interface (CLI), Express setup, IE Switch macro, etc. This solution is based on using the CLI to manage switches.

For more details on different methods to manage switches, refer to Chapter 6, Implementation Steps in the *Cisco Connected Factory - PROFINET Design and Implementation Guide*: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/manufacturing/profinet-implementation-guide.pdf

## Configuring the Media Redundancy Protocol

The prerequisites to configure the Media Redundancy Protocol are:

- Activate the MRP License.
- Configure Cisco Industrial Ethernet Switches.
- Configure Media Redundancy Protocol on TIA Portal.

## Activating the MRP License

### MRM and MRC Licenses

MRM and MRC licenses are disabled by default. You must activate the MRP license before you configure the MRP feature on the switch. You can activate the license by using the CLI. To activate the license on your switch, enter one of the following commands at the Privileged EXEC mode:

- MRC# **license right-to-use activate mrp-client**
- MRM# **license right-to-use activate mrp-manager**

**Note:** The MRM license enables the Media Redundancy Automanager (MRA) administrative role on the Cisco IE4000 and Cisco IE5000. The same license enables MRM for the Cisco IE2000 and the Cisco IE4010 only.

After entering the above command you will see terms for the license. Answer **yes** to accept.

**Note:** MRP Manager and Client manager licenses are Right-to-Use trust model licenses. You need to purchase the licenses through Cisco Commerce (https://cisco-apps.cisco.com/cisco/psn/commerce).

To view details on the activated license, enter the following command at the Privileged EXEC mode:

```
Switch# show license
……
Index 3 Feature: mrp-manager
    Period left: Life time
    License Type: PermanentRightToUse
    License State: Active, In Use
    License Priority: High
    License Count: 1/1/0  (Active/In-use/Violation)

Index 4 Feature: mrp-client
    Period left: Life time
        License Type: PermanentRightToUse
    License State: Active, In Use
    License Priority: High
    License Count: 1/1/0  (Active/In-use/Violation)
```

## Configuring Cisco Industrial Ethernet Switches

PROFINET MRP is enabled by default on Cisco Industrial Ethernet series switches when MRM or MRC licenses are enabled.

**Note:** Do not use the CLI to configure or modify the switch configuration when PROFINET and the TIA Portal are in use. This includes setting the MRC or MRM role. MRP CLI mode and PROFINET MRP modes are mutually exclusive.

1. Download and Install the IOS software from https://software.cisco.com/download/navigator.html. We recommend that you always use the latest released IOS Release, 15.2.5E2a(ED) in this solution.
2. Enable PROFINET MRP.

   ```
   profinet mrp
   ```

3. PROFINET by default uses VLAN 1 on Cisco Switches. You can choose any available VLAN ID. We have chosen VLAN 101.

   ```
   profinet vlan 101
   ```

4. (Optional) Configure the PROFINET Device Identifier using the PROFINET id command.

   ```
   profinet id mrm
   ```

   You can also configure PROFINET ID on the TIA Portal.

5. Configure interfaces which are in the MRP ring, such as access ports. Refer to the following sample configuration:

   ```
   interface GigabitEthernet1/7
    description MRP port2 to IE2K-17
    switchport trunk allowed vlan 101,102
    switchport mode trunk
     media-type sfp
   ```

6. Configure interfaces connected to PROFINET devices, such as PLC or Remote Input or Output devices, and the PC on which the TIA Portal is installed. Refer to the following sample configuration:

   ```
   interface GigabitEthernet1/10
    description Connect to PLC-2
    switchport access vlan 101
    switchport mode access
    end
   ```

7. Disable one MRP port before configuration. It is recommended to disconnect the ring before configuring MRP to avoid any unnecessary flooding should there be any issues.

   ```
   interface GigabitEthernet1/5
    switchport trunk allowed vlan 101,102
    switchport mode trunk
    shutdown
     media-type sfp
   ```

## Configuring Media Redundancy Protocol on the TIA Portal

Totally Integrated Automation (TIA) Portal is a PROFINET-aware factory floor automation tool that helps to integrate, manage, and monitor various Profinet aware devices like Cisco Industrial Ethernet 2000 series and Cisco Industrial Ethernet 4000 series switches, PLCs, Remote Digital Input and Output devices, Human Machine Interface (HMI) displays, drives, etc. used in Cell Area Zone as defined in Connected Factory—PROFINET. The Connected Factory—PROFINET implementation used TIA Portal as one of the factory floor automation tools.

This section provides an overview of key screens within the TIA Portal. The MRP ring in PROFINET mode can only be configured using TIA Portal. The prerequisites to configure the Media Redundancy Protocol on the TIA Portal are:

- Install the PROFINET GSD File.
- Discover PROFINET devices.
- Create PROFINET MRP network configuration diagram.
- Define PROFINET MRP domain, MRP Roles, and MRP Interfaces.
- Go online.

### Installing the PROFINET GSD File

PROFINET devices including network components like Cisco Industrial Ethernet series switches are integrated in PROFINET aware factory floor automation tools using a General Station Description (GSD) file that contains the properties and information required to exchange data between the device and the supervisor.

1. Get the GSD file by unzipping your image.

   The PROFINET MRP GSD file (Cisco_IE2000_GSD.zip, Cisco_IE4000_GSD.zip, Cisco_IE4010_GSD.zip, or Cisco_IE5000_GSD.zip) is bundled within the Cisco IOS release.

   We recommend that you always use the latest released GSD file. GSD files for Cisco IOS Release 15.2(5)E2 are:

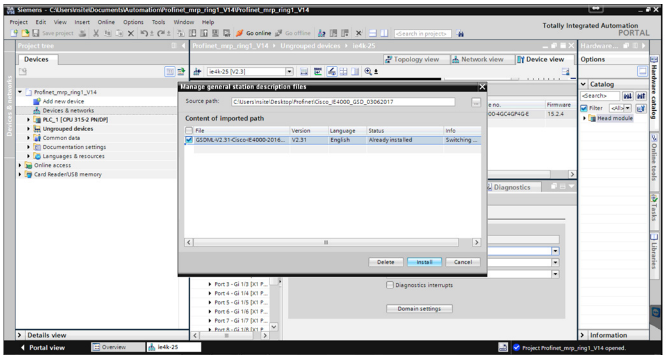
**Note:** In 15.2(5)E2, the SFPs and the combo ports are added as the pluggable module in the GSD for the Cisco IE2000 and Cisco IE5000 platforms. For configuration in the TIA Portal, refer to: http://prrq.cloudapps.cisco.com/prrq/viewReview.do?bugId=DRRaa77395

**Table 8 GSD Files**

| Platform | GSD File |
|---|---|
| Cisco IE 2000 | GSDML-V2.31-Cisco-IE2000-20170228.xml |
| Cisco IE 3000 | GSDML-V2.31-Cisco-IE3000-20160125.xml |
| Cisco IE 4000 | GSDML-V2.31-Cisco-IE4000-20160601.xml |
| Cisco IE 4010 | GSDML-V2.31-Cisco-IE4010-20170330.xml |
| Cisco IE 5000 | GSDML-V2.31-Cisco-IE5000-20170228.xml |

2. Upload the GSD XML file to the GSD directory by selecting **Options** -> **Manage general station description files (GSD)** on the TIA Portal.

**Figure 27 Upload GSD XML File**


Project Edit View Insert Online Options Tools Window Help
Go online
Go offline
Totally Integrated Automation PORTAL
Profinet_mrp_ring1_V14 ▸ Ungrouped devices ▸ ie4k-25
Topology view
Network view
Device view
ie4k-25 [V2.3]
Delete
Install
Cancel
378285

Manage general station description files

Source path: C:\Users\nsite\Desktop\Profinet\Cisco_IE4000_GSD_03062017

Content of imported path

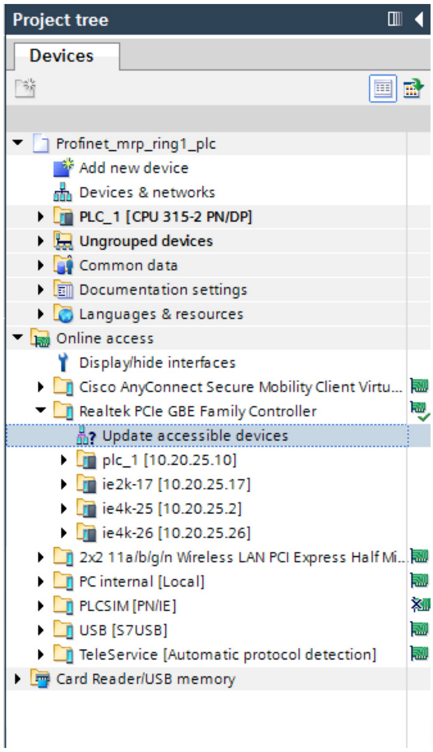
| | File | Version | Language | Status | Info |
|---|---|---|---|---|---|
| ☑ | GSDML-V2.31-Cisco-IE4000-2016... | V2.31 | English | Already installed | Switching ... |

**Note:** If you have a GSD XML file installed that is older than the version bundled with the Cisco IOS software, we recommend that you remove the older file to prevent any possible incompatibilities and confusion.

### Discovering PROFINET Devices

1. At **Online access** under **Devices Panel**, select the interface you use to connect the switch and click **Update accessible devices**.

### Figure 28 Update Accessible Devices

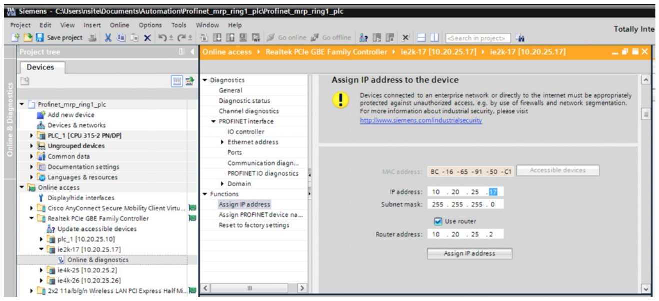


**Note:** You can also discover by using **Accessible Devices** on the tool panel.

2. Assign the IP address for each device.

   **Online & diagnostics** -> **Function** -> **Assign IP Address**

### Figure 29 Assign IP Address



Assign IP address to the device

Devices connected to an enterprise network or directly to the internet must be appropriately protected against unauthorized access, e.g. by use of firewalls and network segmentation. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity

MAC address: BC -16 -65 -91 -50 -C1

IP address: 10 . 20 . 25 . 17

Subnet mask: 255 . 255 . 255 . 0

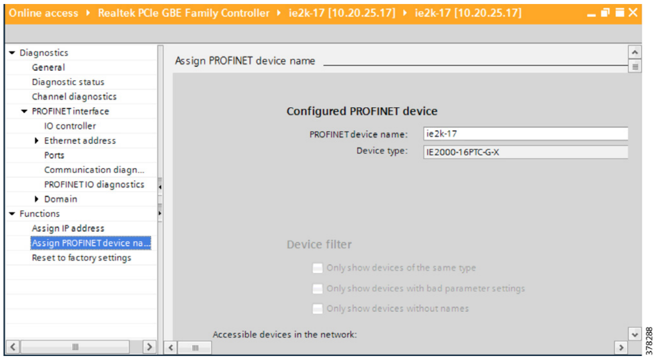
☑ Use router

Router address: 10 . 20 . 25 . 2

3. (Optional) Change the PROFINET ID.

   **Function** -> **Assign Profinet Device Name**

### Figure 30 Assign Profinet Device Name



Assign PROFINET device name

Configured PROFINET device

PROFINET device name: ie2k-17

Device type: IE2000-16PTC-G-X

Device filter

□ Only show devices of the same type

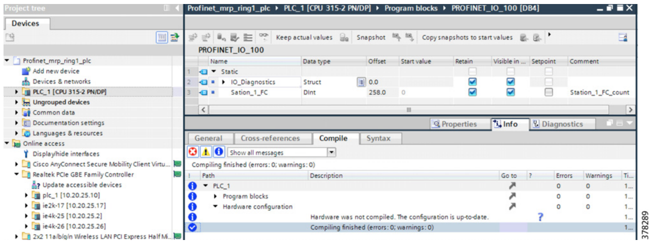
□ Only show devices with bad parameter settings

□ Only show devices without names

Accessible devices in the network:

4. Save Project.
5. Compile by selecting PLC Project.

### Figure 31 Compile PLC Project



PROFINET_IO_100

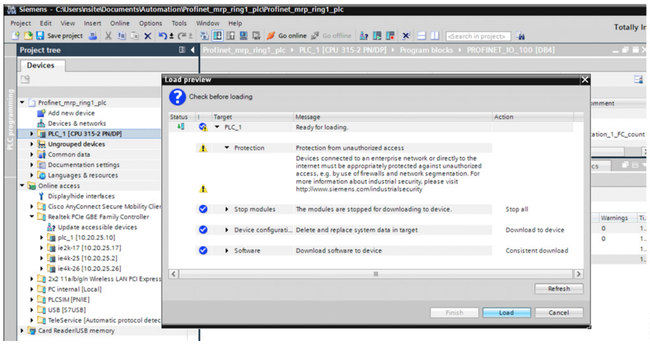
| | Name | Data type | Offset | Start value | Retain | Visible in ... | Setpoint | Comment |
|---|---|---|---|---|---|---|---|---|
| 1 | Static | | | | □ | □ | □ | |
| 2 | IO_Diagnostics | Struct | 0.0 | | ☑ | ☑ | □ | |
| 3 | Sation_1_FC | DInt | 258.0 | 0 | ☑ | ☑ | □ | Station_1_FC_count |

Compiling finished (errors: 0; warnings: 0)

| ! | Path | Description | Go to | ? | Errors | Warnings | Ti... |
|---|---|---|---|---|---|---|---|
| ⓘ | PLC_1 | | ↗ | | 0 | 0 | 1... |
| ⓘ | Program blocks | | ↗ | | 0 | 0 | 1... |
| ⓘ | Hardware configuration | | ↗ | | 0 | 0 | 1... |
| ⓘ | | Hardware was not compiled. The configuration is up-to-date. | | ? | | | 1... |
| ✓ | | Compiling finished (errors: 0; warnings: 0) | | | | | 1... |

6. Download the configuration to the devices.

### Figure 32 Download Configuration

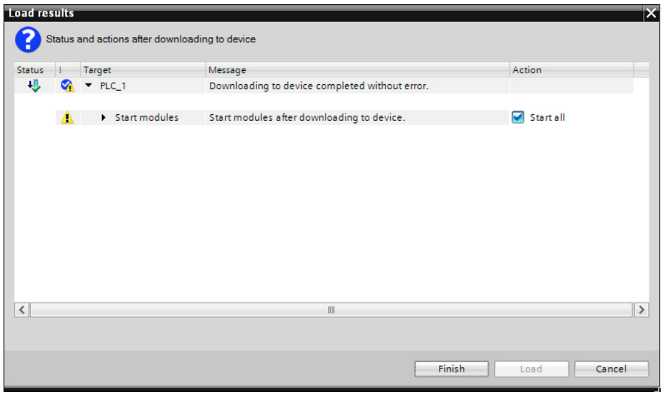


Check before loading

| Status | ! | Target | Message | Action |
|---|---|---|---|---|
| | | PLC_1 | Ready for loading. | |
| | ⚠ | Protection | Protection from unauthorized access | |
| | ⚠ | | Devices connected to an enterprise network or directly to the internet must be appropriately protected against unauthorized access, e.g. by use of firewalls and network segmentation. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity | |
| | ✓ | Stop modules | The modules are stopped for downloading to device. | Stop all |
| | ✓ | Device configurati... | Delete and replace system data in target | Download to device |
| | ✓ | Software | Download software to device | Consistent download |

7. Load, select **Start all**, then click **Finish**.

### Figure 33 Load and Start All



**Load results**

Status and actions after downloading to device

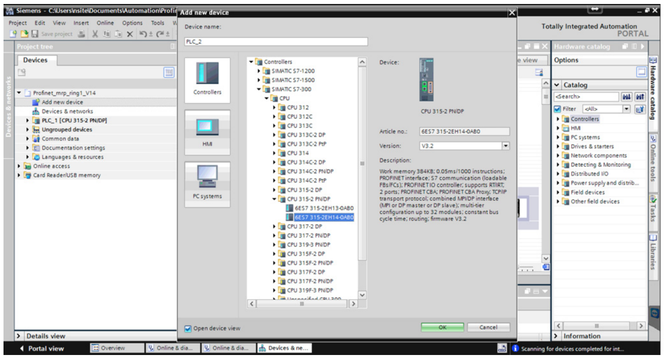
| Status | ! | Target | Message | Action |
|---|---|---|---|---|
|  |  | ▾ PLC_1 | Downloading to device completed without error. |  |
|  | ⚠ | ▸ Start modules | Start modules after downloading to device. | ☑ Start all |

Finish | Load | Cancel

## Creating PROFINET MRP Network Configuration Diagram Devices

1. Choose the PROFINET devices by clicking **Add new devices** under your project. This solution implements PLC 315-2 PN/DP.

### Figure 34 Add New Devices

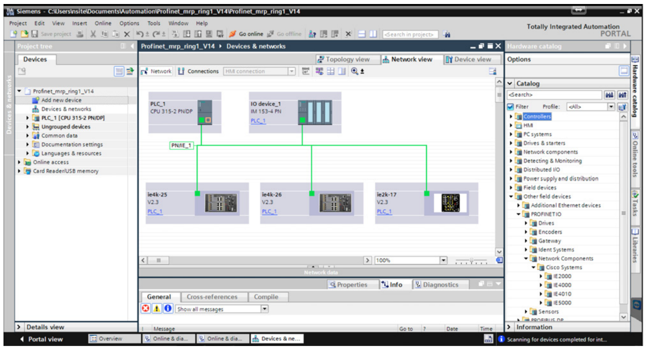


2. Choose other devices under **Catalog** at the **Hardware Catalog** panel.

**Note:** The Cisco IE switches are under **Catalog** -> **Other filed devices** -> **Profinet IO** -> **Network Components** -> **Cisco Systems**.

3. Assign the interfaces of all the devices networked with **PN/IE_1** subnet.

### Figure 35 Assign the Interfaces



4. Save and Compile your project.

5. Download the configuration into your topology. It will automatically change your PC IP subnetted with the switches.

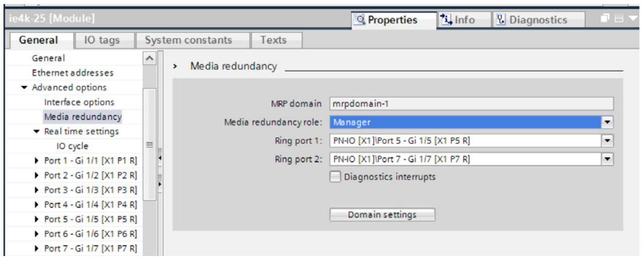
## Defining PROFINET MRP Domain, MRP Roles, and MRP Interfaces

1. **Devices & Network** -> Click the device on the **Device View**.

2. **Property** -> **Advanced Options** -> **Media Redundancy**

3. Assign the domain name, role, and two MRP ports.

### Figure 36 Assign Domain Name, Role, and MRP Ports



ie4k-25 [Module]

Media redundancy

MRP domain: mrpdomain-1

Media redundancy role: Manager

Ring port 1: PN-IO [X1]\Port 5 - Gi 1/5 [X1 P5 R]

Ring port 2: PN-IO [X1]\Port 7 - Gi 1/7 [X1 P7 R]

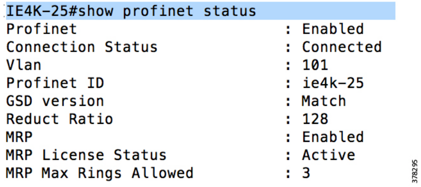
☐ Diagnostics interrupts

4. Compile and download your project.

5. (Optional) In the switch CLI, you can also refer to the MRP status.

```
IE4K-25#show profinet status
```

### Figure 37 MRP Status

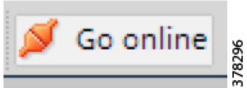


```
IE4K-25#show profinet status
Profinet                            : Enabled
Connection Status                   : Connected
Vlan                                : 101
Profinet ID                         : ie4k-25
GSD version                         : Match
Reduct Ratio                        : 128
MRP                                 : Enabled
MRP License Status                  : Active
MRP Max Rings Allowed               : 3
```

## Going Online

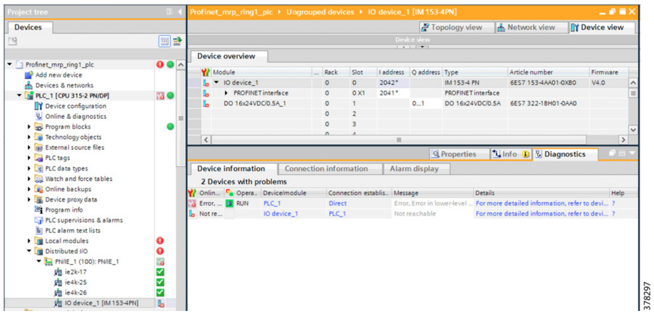
1. Click **Go online** by selecting PLC project.

### Figure 38 Go Online



- If success, all green lights will be shown.
- If fail, there will be red error. Debug it by referring to the information provided in **Diagnostics**.

### Figure 39 Device Information



Profinet_mrp_ring1_plc
- Add new device
- Devices & networks
- PLC_1 [CPU 315-2 PN/DP]
  - Device configuration
  - Online & diagnostics
  - Program blocks
  - Technology objects
  - External source files
  - PLC tags
  - PLC data types
  - Watch and force tables
  - Online backups
  - Device proxy data
  - Program info
  - PLC supervisions & alarms
  - PLC alarm text lists
  - Local modules
  - Distributed I/O
    - PN/IE_1 (100): PN/IE_1
      - ie2k-17 ✓
      - ie4k-25 ✓
      - ie4k-26 ✓
      - IO device_1 [IM 153-4PN]

Device overview

| Module | ... | Rack | Slot | I address | Q address | Type | Article number | Firmware |
|---|---|---|---|---|---|---|---|---|
| IO device_1 | | 0 | 0 | 2042* | | IM 153-4 PN | 6ES7 153-4AA01-0XB0 | V4.0 |
| PROFINET interface | | 0 | 0 X1 | 2041* | | PROFINET interface | | |
| DO 16x24VDC/0.5A_1 | | 0 | 1 | | 0...1 | DO 16x24VDC/0.5A | 6ES7 322-1BH01-0AA0 | |
| | | 0 | 2 | | | | | |
| | | 0 | 3 | | | | | |
| | | 0 | 4 | | | | | |

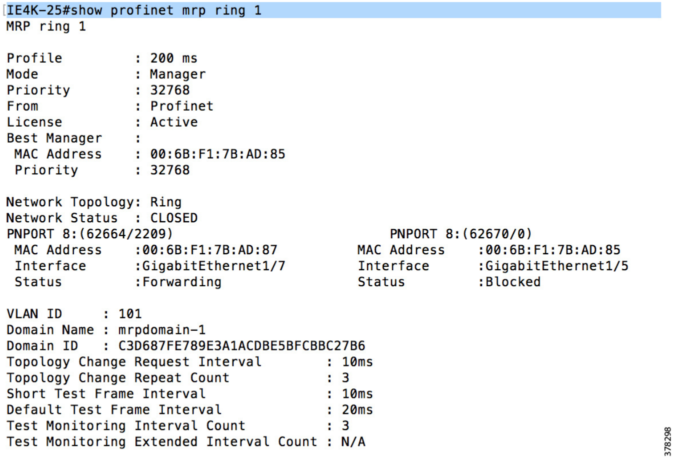
Device information

2 Devices with problems

| Onlin... | Opera... | Device/module | Connection establis... | Message | Details | Help |
|---|---|---|---|---|---|---|
| Error, ... | RUN | PLC_1 | Direct | Error, Error in lower-level ... | For more detailed information, refer to devi... | ? |
| Not re... | | IO device_1 | PLC_1 | Not reachable | For more detailed information, refer to devi... | ? |

2. (Optional) In the switch CLI, you can also refer to the MRP status.

### Figure 40 MRP Status



```
IE4K-25#show profinet mrp ring 1
MRP ring 1

Profile          : 200 ms
Mode             : Manager
Priority         : 32768
From             : Profinet
License          : Active
Best Manager     :
 MAC Address     : 00:6B:F1:7B:AD:85
 Priority        : 32768

Network Topology: Ring
Network Status  : CLOSED
PNPORT 8:(62664/2209)                                 PNPORT 8:(62670/0)
 MAC Address     :00:6B:F1:7B:AD:87          MAC Address     :00:6B:F1:7B:AD:85
 Interface       :GigabitEthernet1/7         Interface       :GigabitEthernet1/5
 Status          :Forwarding                 Status          :Blocked

VLAN ID     : 101
Domain Name : mrpdomain-1
Domain ID   : C3D687FE789E3A1ACDBE5BFCBBC27B6
Topology Change Request Interval        : 10ms
Topology Change Repeat Count            : 3
Short Test Frame Interval               : 10ms
Default Test Frame Interval             : 20ms
Test Monitoring Interval Count          : 3
Test Monitoring Extended Interval Count : N/A
```

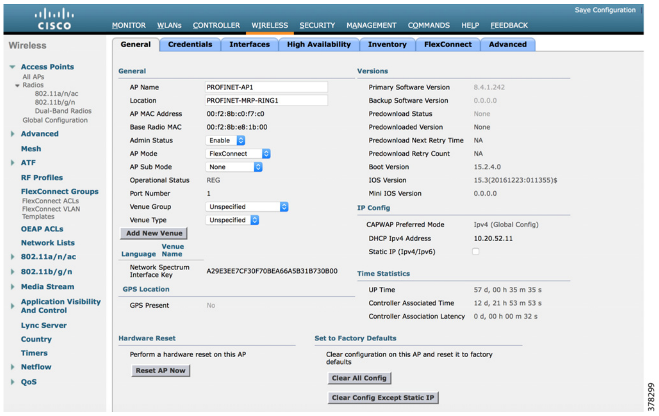
**Note:** The configuration can only be changed in Offline mode.

# Configuring Wireless Cisco Connected Factory—PROFINET

## Configuring Initial Access Point

1. This solution configured an IP address on the AP management interface by using a DHCP server in the infrastructure to automatically configure an IP address.
2. Use the **Wireless LAN Controller** > **Wireless** > **AP** page to configure basic parameters: AP name, AP mode, subnet mask, and default gateway.

### Figure 41 Configure Basic Parameters



General

| | |
|---|---|
| AP Name | PROFINET-AP1 |
| Location | PROFINET-MRP-RING1 |
| AP MAC Address | 00:f2:8b:c0:f7:c0 |
| Base Radio MAC | 00:f2:8b:e8:1b:00 |
| Admin Status | Enable |
| AP Mode | FlexConnect |
| AP Sub Mode | None |
| Operational Status | REG |
| Port Number | 1 |
| Venue Group | Unspecified |
| Venue Type | Unspecified |

| Language | Venue Name |
|---|---|

| | |
|---|---|
| Network Spectrum Interface Key | A29E3EE7CF30F70BEA66A5B31B730B00 |

GPS Location

| | |
|---|---|
| GPS Present | No |

Versions

| | |
|---|---|
| Primary Software Version | 8.4.1.242 |
| Backup Software Version | 0.0.0.0 |
| Predownload Status | None |
| Predownloaded Version | None |
| Predownload Next Retry Time | NA |
| Predownload Retry Count | NA |
| Boot Version | 15.2.4.0 |
| IOS Version | 15.3(20161223:011355)$ |
| Mini IOS Version | 0.0.0.0 |

IP Config

| | |
|---|---|
| CAPWAP Preferred Mode | Ipv4 (Global Config) |
| DHCP Ipv4 Address | 10.20.52.11 |
| Static IP (Ipv4/Ipv6) | ☐ |

Time Statistics

| | |
|---|---|
| UP Time | 57 d, 00 h 35 m 35 s |
| Controller Associated Time | 12 d, 21 h 53 m 53 s |
| Controller Association Latency | 0 d, 00 h 00 m 32 s |

Hardware Reset

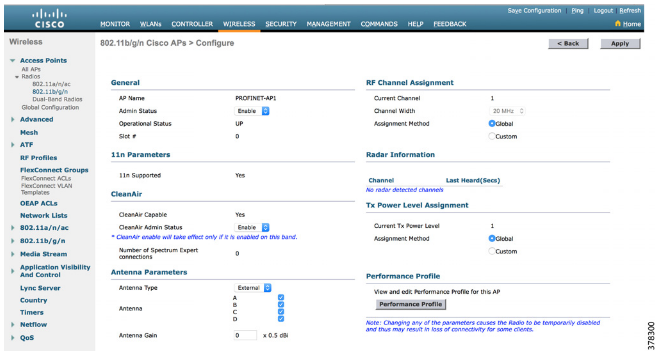
Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

3. Configure basic parameters for the 5 GHz or 2.4 GHz radio in the **Radio Configuration** section.

### Figure 42 Configure Basic Parameters for Radio



802.11b/g/n Cisco APs > Configure

**General**

| | |
|---|---|
| AP Name | PROFINET-AP1 |
| Admin Status | Enable |
| Operational Status | UP |
| Slot # | 0 |

**11n Parameters**

| | |
|---|---|
| 11n Supported | Yes |

**CleanAir**

| | |
|---|---|
| CleanAir Capable | Yes |
| CleanAir Admin Status | Enable |

* CleanAir enable will take effect only if it is enabled on this band.

| | |
|---|---|
| Number of Spectrum Expert connections | 0 |

**Antenna Parameters**

| | |
|---|---|
| Antenna Type | External |
| Antenna | A ☑<br>B ☑<br>C ☑<br>D ☑ |
| Antenna Gain | 0 x 0.5 dBi |

**RF Channel Assignment**

| | |
|---|---|
| Current Channel | 1 |
| Channel Width | 20 MHz |
| Assignment Method | ● Global<br>○ Custom |

**Radar Information**

| Channel | Last Heard(Secs) |
|---|---|

No radar detected channels

**Tx Power Level Assignment**

| | |
|---|---|
| Current Tx Power Level | 1 |
| Assignment Method | ● Global<br>○ Custom |

**Performance Profile**

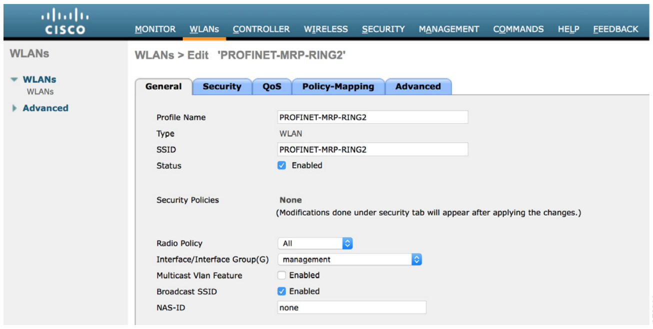
View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

## Configuring SSID and WGB

1. Add and Configure a WLAN SSID in WLANs configuration page.

### Figure 43 Add and Configure WLAN SSID



WLANs > Edit 'PROFINET-MRP-RING2'

| | |
|---|---|
| Profile Name | PROFINET-MRP-RING2 |
| Type | WLAN |
| SSID | PROFINET-MRP-RING2 |
| Status | ☑ Enabled |
| Security Policies | None<br>(Modifications done under security tab will appear after applying the changes.) |
| Radio Policy | All |
| Interface/Interface Group(G) | management |
| Multicast Vlan Feature | □ Enabled |
| Broadcast SSID | ☑ Enabled |
| NAS-ID | none |

2. Configure SSID on WGB CLI.

```
dot11 ssid PROFINET-MRP-RING2
   authentication open
   no ids mfp client
```

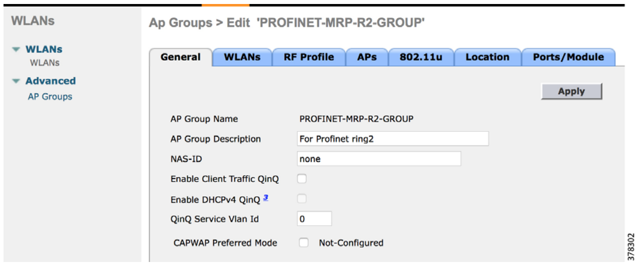
3. Configure the SSID for the 5 GHz radio interface and associate with the corresponding VLAN on the Security - SSID Manager page. If an SSID has been configured previously without a VLAN attached, the old SSID has to be deleted and recreated.

```
interface Dot11Radio1
 no ip address
 ssid PROFINET-MRP-RING2
 station-role workgroup-bridge
 infrastructure-client
 bridge-group 1
 bridge-group 1 spanning-disabled
```

4. Create an AP Group on WLC.

   a. **WLAN** -> **Advance** -> **AP Group**

### Figure 44 Create Access Point Group on WLC

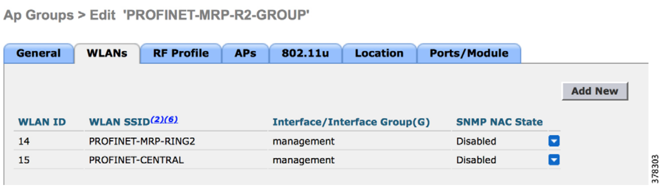


Ap Groups > Edit 'PROFINET-MRP-R2-GROUP'

| | |
|---|---|
| AP Group Name | PROFINET-MRP-R2-GROUP |
| AP Group Description | For Profinet ring2 |
| NAS-ID | none |
| Enable Client Traffic QinQ | □ |
| Enable DHCPv4 QinQ [3] | □ |
| QinQ Service Vlan Id | 0 |
| CAPWAP Preferred Mode | □ Not-Configured |

   b. Add WLAN SSIDs.

### Figure 45 Add WLAN SSIDs

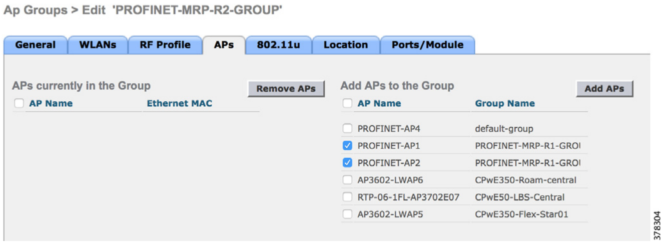


Ap Groups > Edit 'PROFINET-MRP-R2-GROUP'

| WLAN ID | WLAN SSID(2)(6) | Interface/Interface Group(G) | SNMP NAC State |
|---|---|---|---|
| 14 | PROFINET-MRP-RING2 | management | Disabled |
| 15 | PROFINET-CENTRAL | management | Disabled |

   c. Add APs.

### Figure 46 Add Access Points



Ap Groups > Edit 'PROFINET-MRP-R2-GROUP'

APs currently in the Group

| □ AP Name | Ethernet MAC |
|---|---|

Add APs to the Group

| AP Name | Group Name |
|---|---|
| □ PROFINET-AP4 | default-group |
| ☑ PROFINET-AP1 | PROFINET-MRP-R1-GROI |
| ☑ PROFINET-AP2 | PROFINET-MRP-R1-GROI |
| □ AP3602-LWAP6 | CPwE350-Roam-central |
| □ RTP-06-1FL-AP3702E07 | CPwE50-LBS-Central |
| □ AP3602-LWAP5 | CPwE350-Flex-Star01 |

   d. Click **Apply** and **Save configuration**.

## Setting the Update Time in the TIA Portal

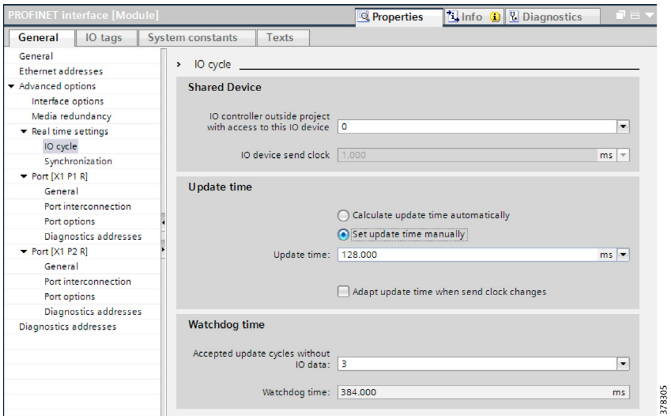
When you set up the wireless configurations, add the wireless devices and follow the same steps to configure the MRP PROFINET ring. The critical item is to set the proper update time for wireless devices.

1. **Real Time** -> **IO Cycle** -> **Propriety**

2. Under **Update Time**, select **Set update time manually**.

   The **Calculate update time automatically** option is good for wired devices, but it is too short for wireless. The short update time will cause the MRP ring to fail when it tries to converge from a link failure.

### Figure 47 Set Update Time



IO cycle

Shared Device

IO controller outside project with access to this IO device: 0

IO device send clock: 1.000 ms

Update time

○ Calculate update time automatically

● Set update time manually

Update time: 128.000 ms

□ Adapt update time when send clock changes

Watchdog time

Accepted update cycles without IO data: 3

Watchdog time: 384.000 ms

## Setting up Security

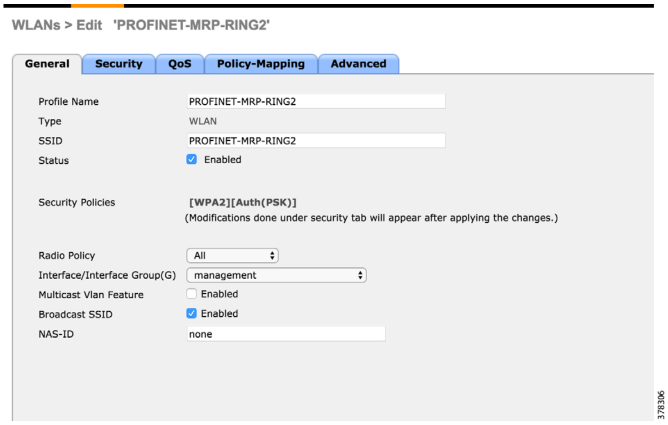
Based on the security design recommendations in System Design, page 9, the following WLAN security methods are discussed here:

- WPA2 with AES PSK
- WPA2 with AES EAP + Cisco Centralized Key Management (CCKM)

## Configuring WPA2/AES PSK

1. Select **Security Policy** in WLAN SSID configuration.

### Figure 48 Security Policy



WLANs > Edit 'PROFINET-MRP-RING2'

| | |
|---|---|
| Profile Name | PROFINET-MRP-RING2 |
| Type | WLAN |
| SSID | PROFINET-MRP-RING2 |
| Status | ☑ Enabled |
| Security Policies | [WPA2][Auth(PSK)]<br>(Modifications done under security tab will appear after applying the changes.) |
| Radio Policy | All |
| Interface/Interface Group(G) | management |
| Multicast Vlan Feature | □ Enabled |
| Broadcast SSID | ☑ Enabled |
| NAS-ID | none |

2. Enable WPAv2 option and WPA PSK in the ASCII format in WGB CLI.

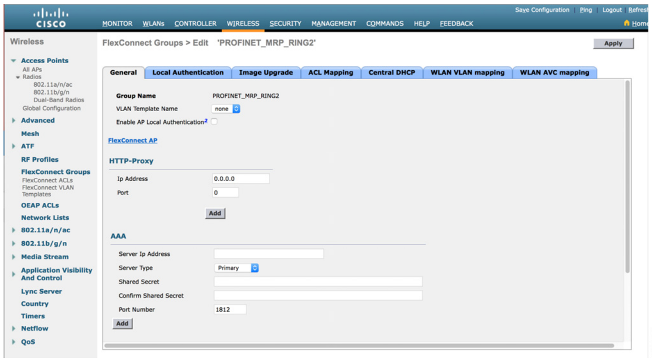
```
configure terminal
    dot11 ssid <SSID>
     authentication open
     authentication key-management wpa version 2
     wpa-psk ascii <PASSWORD>
```

```
no ids mfp client
```

## Configuring WPA2/AES EAP + CCKM

1. Create FlexConnect group.

### Figure 49 Create FlexConnect Group



FlexConnect Groups > Edit 'PROFINET_MRP_RING2'

| | |
|---|---|
| Group Name | PROFINET_MRP_RING2 |
| VLAN Template Name | none |
| Enable AP Local Authentication[2] | □ |

HTTP-Proxy

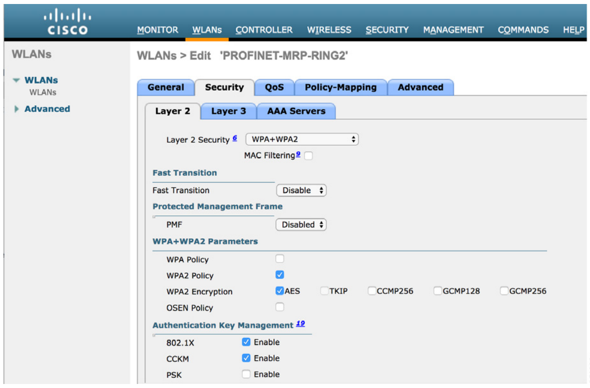
| | |
|---|---|
| Ip Address | 0.0.0.0 |
| Port | 0 |

AAA

| | |
|---|---|
| Server Ip Address | |
| Server Type | Primary |
| Shared Secret | |
| Confirm Shared Secret | |
| Port Number | 1812 |

2. Select **Security Policy** in WLAN SSID configuration.

### Figure 50 Select Security Policy



WLANs > Edit 'PROFINET-MRP-RING2'

Layer 2 Security[6]: WPA+WPA2

MAC Filtering[9] □

Fast Transition

Fast Transition: Disable

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

| | | | | | |
|---|---|---|---|---|---|
| WPA Policy | □ | | | | |
| WPA2 Policy | ☑ | | | | |
| WPA2 Encryption | ☑AES | □TKIP | □CCMP256 | □GCMP128 | □GCMP256 |
| OSEN Policy | □ | | | | |

Authentication Key Management[19]

| | |
|---|---|
| 802.1X | ☑ Enable |
| CCKM | ☑ Enable |
| PSK | □ Enable |

3. Configure SSID for WGBs.

```
dot11 ssid PROFINET-MRP-RING2
 authentication open eap eap
 authentication network-eap eap
 authentication key-management cckm
 dot1x credentials wgb
 dot1x eap profile CPwE350-EAP-FAST
 no ids mfp client
```

4. Configure authentication method and key management.

```
eap profile CPwE350-EAP-FAST
 method fast
```

5. Configure dot1x security profile and credentials.

```
dot1x credentials wgb
 username profinet
```

# Implementation Considerations—Manufacturing Zone

Figure 10 shows a plant-wide security infrastructure for PROFINET/Cisco integration, providing advanced network resiliency and convergence for the communication between the Cell Area Zone and the Manufacturing Zone. Industrial plant security mechanisms are described below.

## Holistic Defense-in-depth Security

Cisco recommends a defense-in-depth approach to securing any network, including industrial networks. Defense-in-depth refers to not only utilizing traditional security mechanisms like firewalls, but also broadly monitoring the entire network to look for indicators of compromise. Cisco's extensive security product portfolio can not only attempt to block attacks at the network perimeter, but also look deep into the network to identify and eliminate attacks as they happen. When designing a secure network, one approach is to consider a model that addresses attacks on a continuum of before, during, and after. In each area of the continuum there are important measures to take to ensure that most attacks are prevented before they are started and any that do make it through the perimeter are quickly and properly identified and eliminated, all while recording critical details that can be used for analysis to prevent future incidents. While many details of this defense-in-depth strategy are beyond the scope of this document, Cisco.com contains a wealth of resources to describe the architecture, products, and features and how they work together.

## Cisco Identity Services Engine

Cisco's Identity Services Engine (ISE) plays a key role in securing the converged plant and enterprise network. Cisco ISE is a powerful software application that gathers detailed information about the devices and users that are trying to access the network, whether it be through a wired, wireless, or Virtual Private Network (VPN) connection. With this information, Cisco ISE can apply custom policies to allow or deny access to any network resources based on any criteria. For example, Cisco ISE can communicate with Microsoft Active Directory (AD) to authenticate users that are trying to connect to specific switches in the network. Based on their AD group membership, dynamic access control lists can be programmed on the switch to restrict access to only the necessary network resources. Additional sample use cases are covered later in this document to further describe the versatility and flexibility that the Cisco ISE can provide.

## Industrial Demilitarized Zone (IDMZ)

The industrial demilitarized zone acts as a kind of intermediate buffer zone between the enterprise and industrial (plant floor) networks. The industrial demilitarized zone includes several mechanisms to strictly limit the types of data flowing between the enterprise and industrial networks. Various proxy and gateway services reside in the industrial demilitarized zone that are used to broker IACS traffic between the networks such that it cannot flow directly between the networks. The industrial demilitarized zone also segments access to IACS network resources into sub-zones so that they can be accesses when required by IT or operations personnel or potentially trusted partners. The industrial demilitarized zone also contains Remote Desktop gateway services for secured access to industrial network resources from outside the industrial network.

# References

- Cisco Connected Factory—PROFINET Design and Implementation Guide
  http://www.cisco.com/c/dam/en_us/solutions/industries/docs/manufacturing/profinet-implementation-guide.pdf

- Media Redundancy Protocol Configuration Guide for IE 2000, IE 4000, IE 4010, and IE 5000 Switches
  http://www.cisco.com/c/en/us/td/docs/switches/connectedgrid/cg-switch-sw-master/software/configuration/guide/mrp/b_mrp_ie.html#id_47406

# About Cisco Validated Design

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by engineers to ensure faster, more reliable, and fully predictable deployment.

The CVD process is comprehensive and focuses on solving business problems for customers and documenting these solutions. The process consists of the following steps:

- Requirements are gathered from a broad base of customers to devise a set of use cases that will fulfill these business needs.
- Network architectures are designed or extended to provide the functionality necessary to enable these use cases, and any missing functionality is relayed back to the appropriate product development team(s).
- Detailed test plans are developed based on the architecture designs to validate the proposed solution, with an emphasis on feature and platform interaction across the system. These tests generally consist of functionality, resiliency, scale, and performance characterization.
- All parties contribute to the development of the CVD guide, which covers both design recommendations and implementation of the solution based on the testing outcomes.

Within the CVD program, Cisco also provides Cisco Reference Designs (CRDs) that follow the CVD process but focus on reference designs developed around specific set of priority use cases. The scope of CRD testing typically focuses on solution functional verification with limited scale.

For more information about the CVD program, please see Cisco Validated Designs:
https://www.cisco.com/c/en/us/solutions/enterprise/validated-design-program/index.html