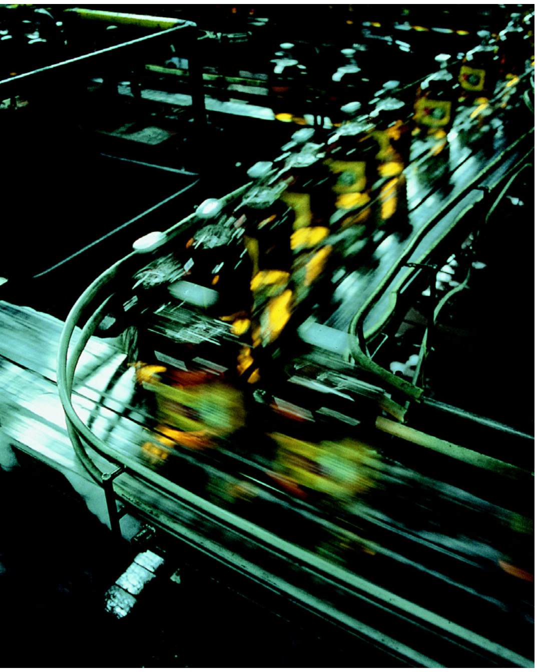


Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture

Design and Implementation Guide

November 2019

Document Reference Number: ENET-TD021A-EN-P

Preface

Converged Plantwide Ethernet (CPwE) is a collection of architected, tested, and validated designs. The testing and validation follow the Cisco® Validated Design (CVD) and Cisco Reference Design (CRD) methodologies. The content of CPwE, which is relevant to both operational technology (OT) and informational technology (IT) disciplines, consists of documented architectures, best practices, guidance, and configuration settings to help industrial operations and OEMs achieve the design and deployment of a scalable, reliable, secure, and future-ready plant-wide or site-wide industrial network infrastructure. CPwE can also help industrial operations and OEMs achieve cost reduction benefits using proven designs that can facilitate quicker deployment while helping to minimize risk in deploying new technology. CPwE is brought to market through an ecosystem consisting of Cisco, Panduit, and Rockwell Automation emergent from the strategic alliance between Cisco Systems and Rockwell Automation.

Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture CVD (CPwE PRP), which is documented in this Design and Implementation Guide (DIG), outlines several use cases for designing and deploying PRP throughout a plant-wide or site-wide Industrial Automation and Control System (IACS) network infrastructure. CPwE PRP highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases within the CPwE framework. CPwE PRP was architected, tested, and validated by Cisco Systems and Rockwell Automation with assistance by Panduit.

Document Organization

This document is composed of the following chapters and appendices.

Chapter/Appendix	Description
CPwE Parallel Redundancy Protocol Overview	Overview of CPwE Parallel Redundancy Protocol.
CPwE Parallel Redundancy Protocol Design Considerations	Describes primary design considerations when choosing how to implement CPwE Parallel Redundancy Protocol in an IACS architecture.
CPwE Parallel Redundancy Protocol Configuration	Describes how to configure CPwE Parallel Redundancy Protocol within the CPwE architecture based on the design considerations and recommendations of the previous chapter.

Chapter/Appendix	Description
CPwE Parallel Redundancy Protocol Monitoring and Troubleshooting	Information on monitoring and troubleshooting CPwE Parallel Redundancy Protocol.
References	Links to documents and websites that are relevant to Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture Design and Implementation Guide.
Test Hardware and Software	Lists the Cisco and Rockwell Automation hardware and software used in testing the CPwE Parallel Redundancy Protocol solution.
Acronyms	List of all acronyms and initialisms used in this document.
About the Cisco Validated Design (CVD) Program	Describes the Cisco Validated Design (CVD) process and the distinction between CVDs and Cisco Reference Designs (CRDs).

For More Information

More information on CPwE Design and Implementation Guides can be found at the following URLs:

- Rockwell Automation site:
  - http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page?
- Cisco site:
  - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Note This release of the CPwE architecture focuses on EtherNet/IP™, which uses the ODVA, Inc. Common Industrial Protocol (CIP™), and is ready for the Industrial Internet of Things (IIoT). For more information on EtherNet/IP and CIP Sync™, see odva.org at the following URL:

- http://www.odva.org/Technology-Standards/EtherNet-IP/Overview

CHAPTER 1

CPwE Parallel Redundancy Protocol Overview

The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network and security technology convergence, including OT-IT persona convergence, by using standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A highly available converged plant-wide or site-wide IACS architecture helps to enable the Industrial Internet of Things (IIoT).

Business practices, corporate standards, policies, industry standards, and tolerance to risk are key factors in determining the degree of resiliency and application availability required within an IACS plant-wide or site-wide architecture, e.g., non-resilient LAN, resilient LAN, or redundant LANs. A highly available network architecture within an IACS application plays a pivotal role in helping to minimize the risk of IACS application shutdowns while helping to maximize overall plant or site uptime.

A holistic resilient plant-wide or site-wide network architecture is composed of multiple technologies (logical and physical) deployed at different levels within the plant or site. When selecting a resiliency technology, various plant or site application factors should be evaluated, including the physical layout of IACS devices (geographic dispersion), recovery time performance, uplink media type, tolerance to data latency and jitter, and future-ready requirements. For more information on resiliency technology, refer to Deploying a Resilient Converged Plantwide Ethernet Architecture (CPwE Resiliency) Design and Implementation Guide (DIG).

Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture (CPwE PRP) outlines several use cases for designing and deploying PRP technology with redundant network infrastructure across plant-wide or site-wide IACS applications. CPwE PRP is an extension to CPwE Resiliency and was architected, tested and validated by Cisco Systems and Rockwell Automation with assistance by Panduit.

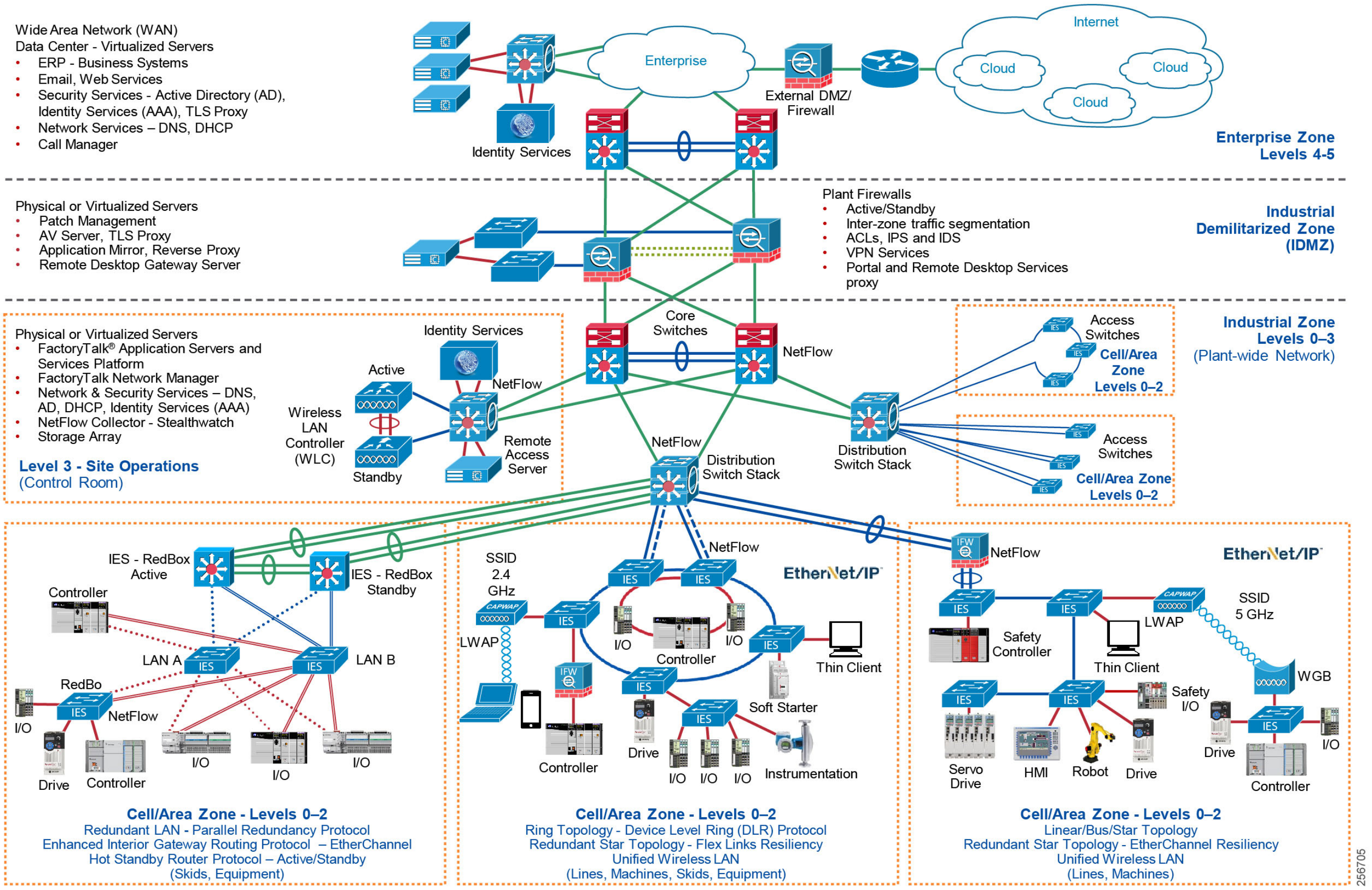
CPwE Overview

CPwE is the underlying architecture that provides standard network and security services for control and information disciplines, devices, and equipment found in modern IACS applications. The CPwE architectures (Figure 1-1) were architected, tested, and validated to provide design and implementation guidance, test results, and documented configuration settings. This can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications. The content and key tenets of CPwE are relevant to both OT and IT disciplines.

CPwE key tenets include:

- **Smart IIoT devices**—Controllers, I/O, drives, instrumentation, actuators, analytics, and a single IIoT network technology (EtherNet/IP)
- **Zoning (segmentation)**—Smaller connected LANs, functional areas, and security groups
- **Managed infrastructure**—Managed Allen-Bradley® Stratix® industrial Ethernet switches (IES), Cisco Catalyst® distribution/core switches, FactoryTalk® Network Manager™ software, and Stratix industrial firewalls
- **Resiliency**—Robust physical layer and resilient or redundant topologies with resiliency protocols
- **Time-critical data**—Data prioritization and time synchronization via CIP Sync™ and IEEE-1588 Precision Time Protocol (PTP)
- **Wireless**—Unified wireless LAN (WLAN) to enable mobility for personnel and equipment
- **Holistic defense-in-depth security**—Multiple layers of diverse technologies for threat detection and prevention, implemented by different persona (e.g., OT and IT) and applied at different levels of the plant-wide or site-wide IACS architecture
- **Convergence-ready**—Seamless plant-wide or site-wide integration by trusted partner applications

Figure 1-1 CPwE Architectures


Wide Area Network (WAN)
Data Center - Virtualized Servers
• ERP - Business Systems
• Email, Web Services
• Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
• Network Services – DNS, DHCP
• Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
• Patch Management
• AV Server, TLS Proxy
• Application Mirror, Reverse Proxy
• Remote Desktop Gateway Server
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services
• Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
• FactoryTalk® Application Servers and Services Platform
• FactoryTalk Network Manager
• Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
• NetFlow Collector - Stealthwatch
• Storage Array
Level 3 - Site Operations
(Control Room)
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
NetFlow
Remote Access Server
Core Switches
NetFlow
NetFlow
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone Levels 0–3
(Plant-wide Network)
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBo
IES
NetFlow
I/O
Drive
Controller
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
SSID 2.4 GHz
LWAP
NetFlow
EtherNet/IP
IES
I/O
Controller
I/O
Thin Client
Soft Starter
Drive
Controller
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
NetFlow
EtherNet/IP
SSID 5 GHz
LWAP
Safety Controller
Thin Client
WGB
Safety I/O
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
256705

CPwE Parallel Redundancy Protocol Use Cases

An IACS is deployed in a wide variety of industries such as automotive, pharmaceuticals, consumer packaged goods, pulp and paper, oil and gas, mining, and energy. IACS applications are composed of multiple control and information disciplines such as continuous process, batch, discrete, and hybrid combinations. One of the challenges facing industrial operations is the industrial hardening of standard Ethernet and IP-converged IACS networking technologies to take advantage of the business benefits associated with IIoT. A high availability network architecture (Figure 1-2) can help to reduce the impact of a network failure on a mission-critical IIoT IACS application.

Parallel Redundancy Protocol (PRP) is a standard defined in IEC 62439-3 and is adopted in the ODVA, Inc. EtherNet/IP specification. PRP technology creates seamless network redundancy by allowing PRP enabled IACS devices to send duplicate Ethernet frames over two independent Local Area Networks (LANs). If a failure occurs in one of the LANs, traffic continues to flow through the other LAN uninterrupted with zero recovery time.

An IACS device enabled with PRP technology has two ports that operate in parallel and attach to two independent LANs (Figure 1-2), e.g., LAN A and LAN B. This type of IACS device is known as a PRP double attached node (DAN). During normal network operation, an IACS DAN simultaneously sends and receives duplicate Ethernet frames across both LAN A and LAN B. The receiving IACS DAN accepts whichever frame arrives first and discards the subsequent copy.

IACS devices that do not support the PRP technology can utilize a PRP redundancy box (RedBox) to connect to the two independent LANs (Figure 1-2). The RedBox functions similarly to the DAN; a PRP enabled IES is an example of a RedBox.

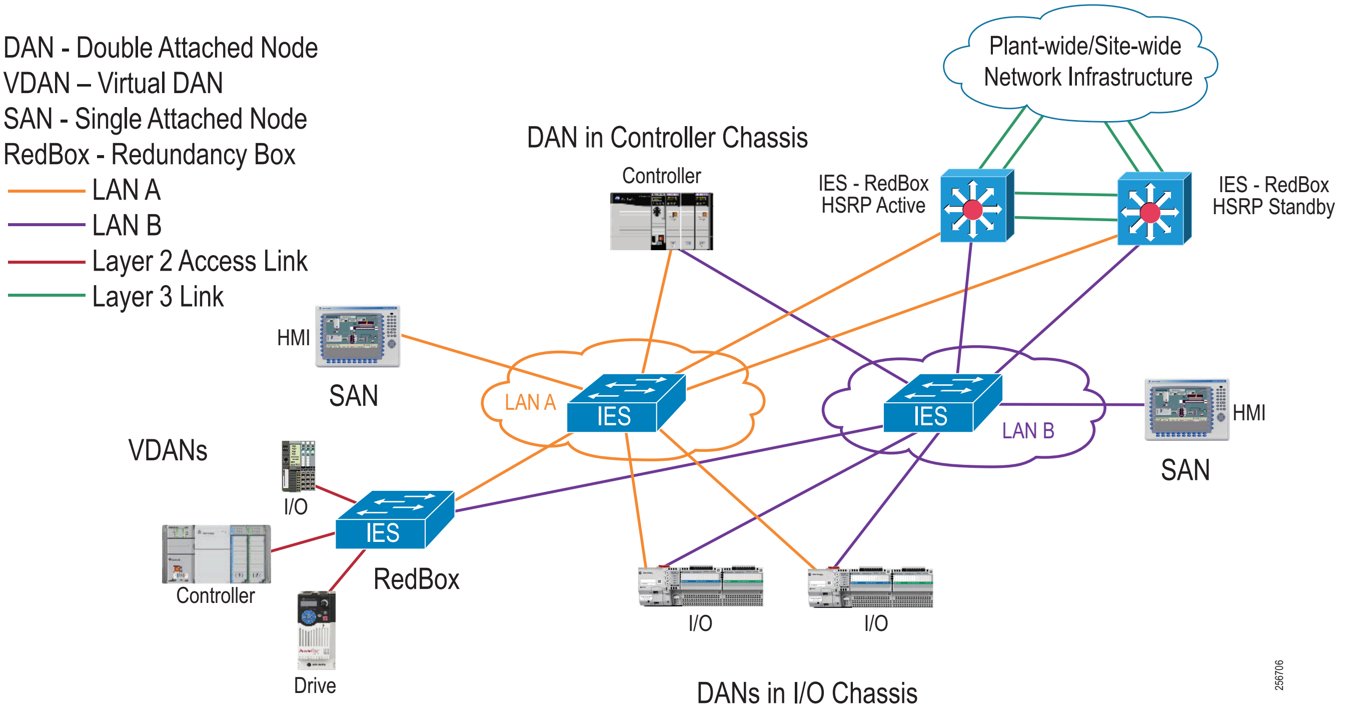
IACS devices that connect to both LAN A and LAN B through a RedBox are referred to as a PRP Virtual DAN (VDAN).

A single attached node (SAN) is an IACS device without PRP support that only resides on either LAN A or LAN B.

PRP supports flexible LAN topologies including linear, star, redundant star, and ring topologies. If both LAN topologies are resilient and single-fault tolerant, PRP architecture can recover from multiple faults in the network.

In contrast, other resiliency technologies are typically single-fault tolerant, are a single LAN, and utilize redundant path topologies (e.g., ring and redundant star). A resiliency protocol is used to forward Ethernet frames along one physical path while blocking the other physical path to avoid Ethernet loops. Network convergence times vary across resiliency technologies. Convergence time disruption is defined as the time it takes to discover a failure (e.g., link or device) along a path, unblock the blocked path, then start forwarding Ethernet frames along that unblocked path. For example, the convergence time for the ODVA, Inc. Device Level Ring (DLR) protocol standard is 3 ms.

Figure 1-2 Representative Plant-wide or Site-wide PRP Deployment



For more information on PRP, see *EtherNet/IP Parallel Redundancy Protocol Application Technique* https://literature.rockwellautomation.com/idc/groups/literature/documents/at/enet-at006_-en-p.pdf

CPwE PRP outlines the concepts, requirements, and technology solutions for reference designs developed around a specific set of priority use cases. These use cases were tested for solution functional validation by Cisco Systems and Rockwell Automation with assistance by Panduit. This helps support a redundant converged plant-wide or site-wide EtherNet/IP IACS architecture.

The CPwE PRP Design and Implementation Guide includes:

- Parallel Redundancy Protocol technology overview
- Design and configuration considerations for plant-wide or site-wide IACS PRP deployments
  - Topology choices
  - PRP devices— e.g., DAN, VDAN, SAN, and RedBox
  - Distribution switch selection
- Selection of Industrial Ethernet Switches (IES)
  - Allen-Bradley Stratix 5700, Stratix 5400, and Stratix 5800 IES as LAN A/B switches
  - Allen-Bradley Stratix 5400 and Stratix 5410 RedBox IES

CPwE Resilient IACS Architectures Overview

Protecting availability for IACS assets requires a defense-in-depth approach where different solutions are needed to address various network resiliency requirements for a plant-wide or site-wide architecture. This section summarizes the existing Cisco, Panduit and Rockwell Automation CPwE Cisco Validated Designs (CVDs) and Cisco Reference Designs (CRDs) that address different aspects of availability for IIoT IACS applications.

- *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing and deploying resilient plant-wide or site-wide architectures for IACS applications, utilizing a robust physical layer and resilient topologies with resiliency protocols.
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- *Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide* outlines several use cases for designing and deploying DLR technology with IACS device-level, switch-level, and mixed device/switch-level single and multiple ring topologies across OEM and plant-wide or site-wide IACS applications.
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td015_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

CHAPTER 2

CPwE Parallel Redundancy Protocol Design Considerations

This chapter describes design considerations and configuration recommendations when implementing Parallel Redundancy Protocol (PRP) in an IACS architecture. This includes guidelines for creating redundant EtherNet/IP network topologies in a Cell/Area Zone using PRP, and connecting PRP topologies to a larger plant-wide or site-wide network using redundant distribution switches.

Parallel Redundancy Protocol Overview

PRP is defined in the international standard IEC 62439-3 and provides high availability in Ethernet networks. PRP implements redundancy by using PRP-enabled nodes (IACS devices) that send duplicate Ethernet frames to two fail-independent network infrastructures, known as LAN A and LAN B.

PRP technology is well suited for variety of critical infrastructure IACS in process and heavy industries that require continuous, high availability operation. Advantages of using PRP over other network resiliency technologies include:

- No IACS data loss during a single fault in LAN A or LAN B
- Protection against extended infrastructure failures in a single LAN (e.g., maintenance work, prolonged power outages, multiple network faults)
- Recovery after multiple faults in certain situations depending on the LAN topologies
- Flexibility of allowing various network topologies, resiliency protocols, and IES platforms for each LAN
- Ease of migration from non-Ethernet redundant media technologies such as ControlNet® Networks (not covered as part of CPwE PRP)

Important factors when selecting PRP technology are support of PRP by IACS devices, possibility of building two independent network topologies without common faults, connectivity to non-PRP parts of the plant-wide or site-wide infrastructure, and proper configuration of other network services such as multicast management and time synchronization.

The following sections provide a brief overview of the PRP operation, components, and topologies. For more details refer to:

- EtherNet/IP Parallel Redundancy Protocol Application Technique
https://literature.rockwellautomation.com/idc/groups/literature/documents/at/enet-at006_-en-p.pdf

Parallel Redundancy Protocol Components

A PRP network includes the components shown in Table 2-1.

Table 2-1 PRP Components

Component	Description	Examples
LAN A and LAN B	Redundant, active Ethernet networks that operate in parallel and are fault independent.	
Double attached node (DAN)	An IACS device with PRP technology that connects to both LAN A and LAN B.	1756-EN2TP ControlLogix® EtherNet/IP module 5094-AENTR Flex 5000™ EtherNet/IP module
Single attached node (SAN)	An IACS device without PRP technology that connects to either LAN A or LAN B. A SAN does not have PRP redundancy and typically is a non-critical device or its function is duplicated in both LANs.	
Redundancy box (RedBox)	An IES with PRP technology that connects non-PRP IACS devices or non-PRP part of the network to both LAN A and LAN B.	Stratix 5400, Stratix 5410 managed switches
Virtual double attached node (VDAN)	An IACS device without PRP technology that connects to both LAN A and LAN B through a RedBox. A VDAN has PRP redundancy and appears to other nodes in the network as a DAN.	
Infrastructure switches	Switches in LAN A or LAN B that are not configured as a RedBox.	Any of the Stratix managed switches

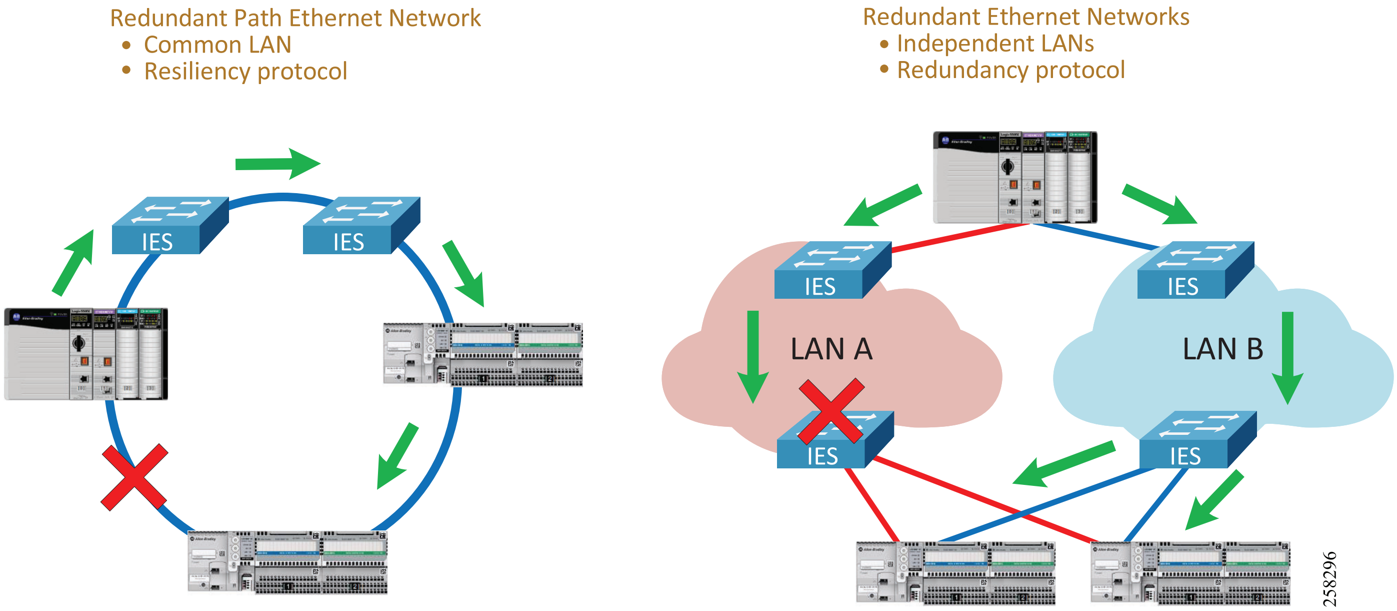
Parallel Redundancy Protocol Operation

An IACS device with PRP technology (a DAN) has two Ethernet ports that operate in parallel and attach to independent LAN A and LAN B. During normal network operation, a DAN simultaneously sends and receives duplicate Ethernet frames through both ports.

The receiving node accepts whichever frame arrives first and discards the subsequent copy. If a failure occurs in one of the LANs, traffic continues to flow through the other LAN uninterrupted with no recovery time.

Unlike other resiliency protocols, such as Spanning Tree Protocol (STP) or DLR, PRP does not require reconfiguration in LAN A or B after the fault (e.g., unblocking the port). PRP provides redundancy by using duplicate network infrastructure rather than redundant paths in the same network.

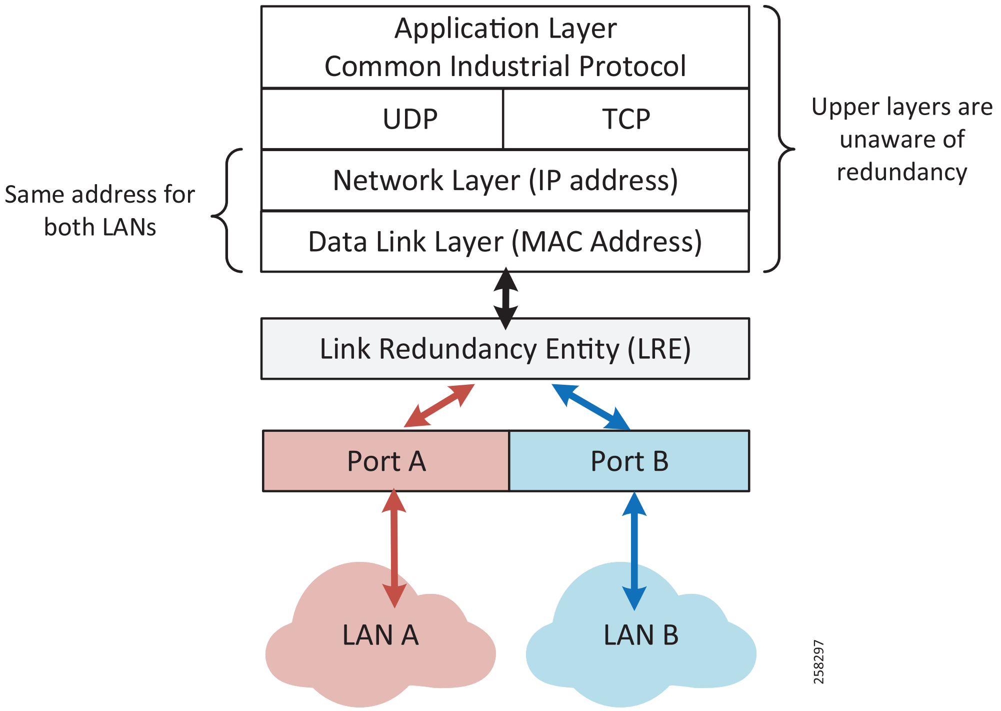
Figure 2-1 Redundant Path versus Redundant Networks



DAN Operation

A DAN has two Ethernet ports that are attached to the upper communication layers of the IACS device through the Link Redundancy Entity (LRE). The LRE handles duplication of packets and management of redundancy (Figure 2-2). The upper layers are unaware of redundancy because the LRE provides to them the same interface as a non-redundant network adapter. The DAN uses the same MAC address and IP address to communicate on both LANs.

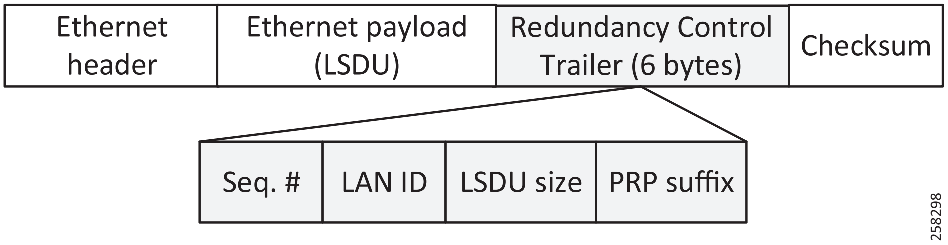
Figure 2-2 PRP DAN Communication Layers


Application Layer
Common Industrial Protocol
UDP
TCP
Network Layer (IP address)
Data Link Layer (MAC Address)
Same address for both LANs
Upper layers are unaware of redundancy
Link Redundancy Entity (LRE)
Port A
Port B
LAN A
LAN B
258297

When a DAN sends a frame to another DAN:

- The LRE creates two copies of the frame and sends them through LAN A and LAN B ports with a Redundancy Check Trailer (RCT) appended to each frame. The 6-byte trailer contains a sequence number, the LAN identifier, frame data size, and the PRP suffix that identifies the trailer type as PRP (Figure 2-3).
- The duplicate frames traverse the two LANs, perhaps under different network conditions and with slightly different delays, and arrive at the destination node.
- The LRE in the destination DAN forwards the first received copy of the frame to the upper layers (without the PRP trailer) and discards the second copy (if it arrives).
- PRP algorithm is designed in a way that it should never reject a legitimate frame, however in rare cases a duplicate frame can be accepted as a new one and passed to the upper layers. This could happen if the duplicate frame arrives with significant time difference. Upper layer protocols (TCP or EtherNet/IP) are able to handle occasional duplicate frames.

Figure 2-3 Ethernet Frame with RCT Appended



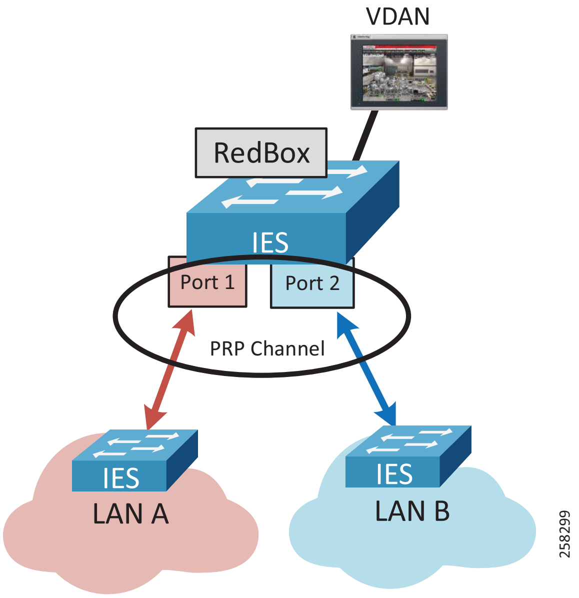
Note The PRP trailer adds six bytes to an Ethernet frame. To accommodate a maximum size 1500 byte Ethernet frame with the PRP trailer attached, all LAN A/B network devices should be configured with the maximum transmission unit (MTU) size of at least 1506 bytes. This is not required for a RedBox IES.

RedBox Operation

The RedBox device acts as LRE for one or several connected VDANs or for a non-PRP bridged network segment. The RedBox keeps track of sequence numbers and handles duplicate received frames for multiple VDANs.

Two Gigabit Ethernet ports on the RedBox IES are configured as one logical interface—a PRP channel group (Figure 2-4). The PRP ports can be in access mode for single VLAN deployments, trunk mode to support multiple VLANs, or routed mode. In the channel group, the lower numbered member port is the primary port and connects to LAN A. The higher numbered port is the secondary port and connects to LAN B.

Figure 2-4 RedBox PRP Channel



- The Stratix 5400 IES supports one PRP channel. The Stratix 5410 IES supports up to two PRP channels.
- A maximum of 512 VDAN entries are supported in the PRP VDAN table. If the VDAN table is full, the switch cannot send supervisory frames for new VDANs.
- Ports in the PRP channel group cannot be configured for other resiliency protocol, e.g., DLR or Resilient Ethernet Protocol (REP).
- Once the PRP ports are added to the group, individual port settings should not be changed unless the port is removed from the group.

For more information about Stratix switch PRP functionality and configuration, refer to:

- Stratix Managed Switches User Manual
https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

In addition to connecting VDANs, a RedBox IES in the PRP network is necessary in following situations:

- Routing is enabled in the network.

- Connectivity to a non-PRP LAN is required, e.g., a DLR segment, a plant-wide or site-wide connectivity.
- Internet Group Management Protocol (IGMP) querier role is required for multicast management.
- Boundary clock role is required for CIP Sync operation.

Recommendations for configuring RedBox IES for these use cases are described in later sections of this Design and Implementation Guide.

SAN Operation

Devices without PRP support (SAN) can be included in the PRP topology as non-redundant devices connected to either LAN A or LAN B:

- A SAN can accept and process Ethernet frames with the RCT attached. The SAN simply ignores the PRP trailer as the Ethernet padding in the frame.
- To avoid duplication of packets for SANs, the DAN or the RedBox IES keeps track of learned MAC addresses in the PRP node table, identifies the device as attached to only one LAN, then sends the frame to that LAN only without the PRP trailer.
- The SAN traffic from one of the LANs can be received and processed by the destination DAN in a normal way.
- All SANs should have unique IP addresses in the PRP network, even if they belong to different LANs.

Network Management and Supervision

Benefits of network redundancy can only be realized if the network status and performance is monitored. This can be achieved with a Network Monitoring Tool (NMT) using Simple Network Management Protocol (SNMP), EtherNet/IP diagnostic tools, and using built-in diagnostic available in PRP-capable IACS devices and RedBox IES.

PRP nodes (DAN or RedBox) verify if frames from known DANs or VDANs are received from both PRP ports and provide real-time PRP statistics and status. For more information, refer to Chapter 4, "CPwE Parallel Redundancy Protocol Monitoring and Troubleshooting."

Each DAN periodically sends a PRP supervision frame that announces its presence on the network and allows other nodes to check health of the PRP network. The RedBox sends supervisory frames on behalf of connected VDANs. The supervisory frames are Layer 2 multicast Ethernet frames sent to a reserved multicast MAC address.

Note An NMT should be connected to the PRP network via a RedBox to access IACS devices and IES in both LANs. While LAN A and LAN B are isolated on the network layer, all managed IES and IACS devices should have different IP addresses within and between each LAN for management purposes.

Parallel Redundancy Protocol Network Design Recommendations

PRP technology is implemented in IACS devices, therefore network infrastructure devices (other than the RedBoxes) do not have to be PRP capable. PRP is not dependent on any particular LAN topology and should provide a single fault tolerance with zero data loss even with non-resilient topologies in each LAN such as star, linear, or a single switch.

When designing a PRP network, follow these recommendations:

- If possible, use resilient topologies (redundant star, ring) in each LAN for additional resiliency protection. In this case, an extended outage or maintenance in one of the LANs still should allow the IACS to recover from a subsequent fault in the other LAN (with convergence time depending on the resilient LAN protocol).
- Design the architecture to avoid or minimize architecture-wide faults that impact both LANs such as power failures or damage of both redundant cabling paths.
- Use similar topologies for both LANs with similar network latency and number of hops in normal network conditions. Avoid using different types of connectivity between LAN A and LAN B, for example a high-speed wired network for LAN A and low bandwidth, high-latency cellular, satellite, or wireless technology for LAN B.
- Do not connect IES (other than RedBoxes) to both LAN A and LAN B. Direct links between LAN A and LAN B IES are not allowed.
- Do not connect any RedBox IES to each other via a Layer 2 path that bridges any of the VLANs that exist in the PRP network. Such a connection creates a bridging loop in the network. Layer 3 routed paths are allowed.
- If routing is required in the PRP network, configure a RedBox IES as the router. Do not enable routing on the LAN A or LAN B IES. For recommendations on the routing redundancy design with PRP and how to connect to the Industrial Zone network, see Connectivity to the Industrial Zone Network.
- Apply the same recommended network and security practices as for a non-PRP network, such as using managed switches with diagnostic, loop prevention, multicast management and security features, minimizing broadcast domains with VLAN segmentation, hardening the network and the IACS applications against security threats, maintaining good change control practices, and IES configuration management.

Parallel Redundancy Protocol Topology Examples

This section provides some examples of PRP architectures and topologies.

Figure 2-5 shows an example of PRP deployment with two parallel fault-isolated physical paths. This could be useful in mining or transportation applications (e.g., parallel tunnels), marine applications (two sides of a ship), and other similar use cases.

In the example below, both LANs utilize a ring topology rather than linear topology for additional resiliency. In most greenfield installations, the cost of having a return cable path is insignificant when installing a cable bundle. The benefits of using a resilient LAN topology are greater than the additional effort of configuring and monitoring of a ring protocol.

The example architecture also implements redundant programmable automation controllers (PAC) with ControlLogix® redundancy for greater availability and protection from controller faults.

Figure 2-5 PRP Topology Example with Parallel Paths

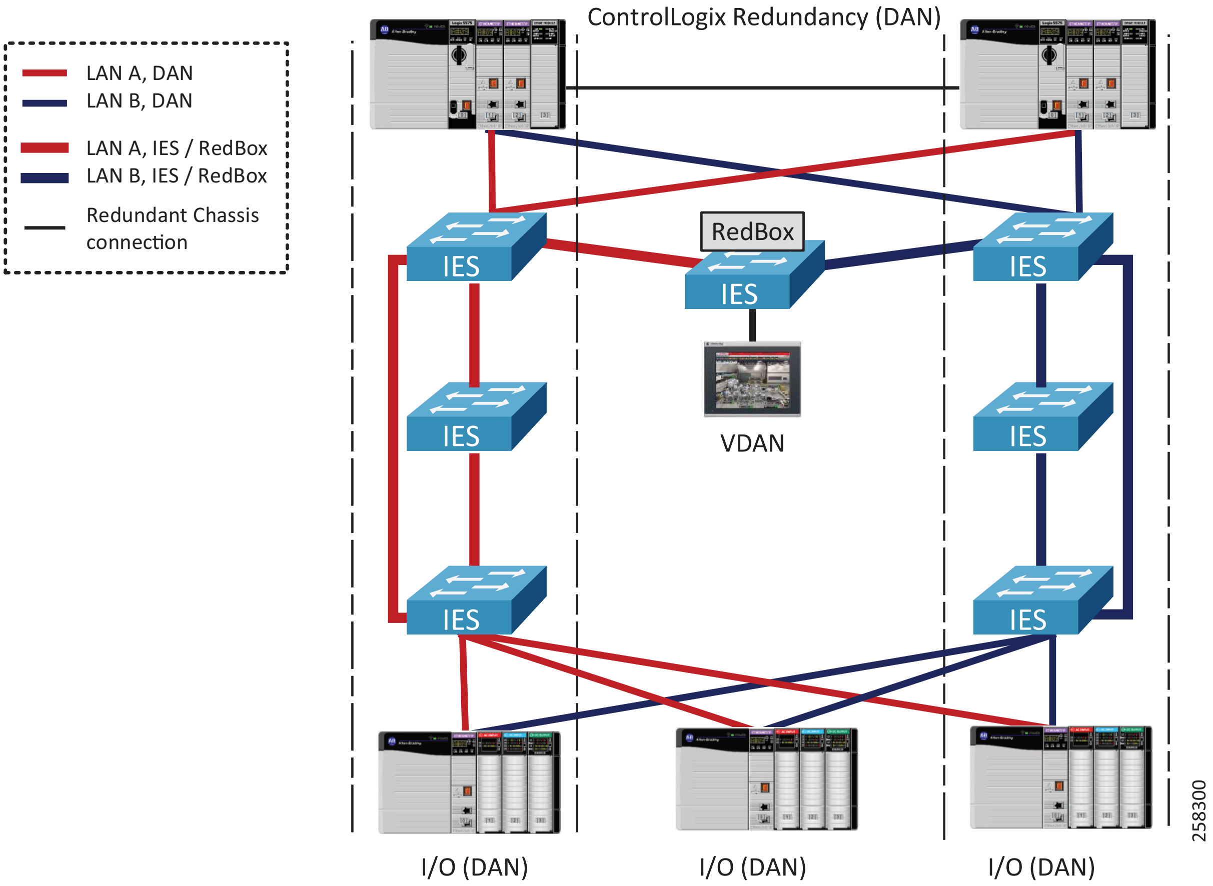


Figure 2-6 shows an example of a PRP topology with dual rings and a single (non-redundant) PAC. This topology is common for water/wastewater, mining, oil and gas, and other industries that traditionally have used redundant dual-media topologies over large geographical areas.

Figure 2-6 PRP Topology Example with Dual Rings—Single PAC

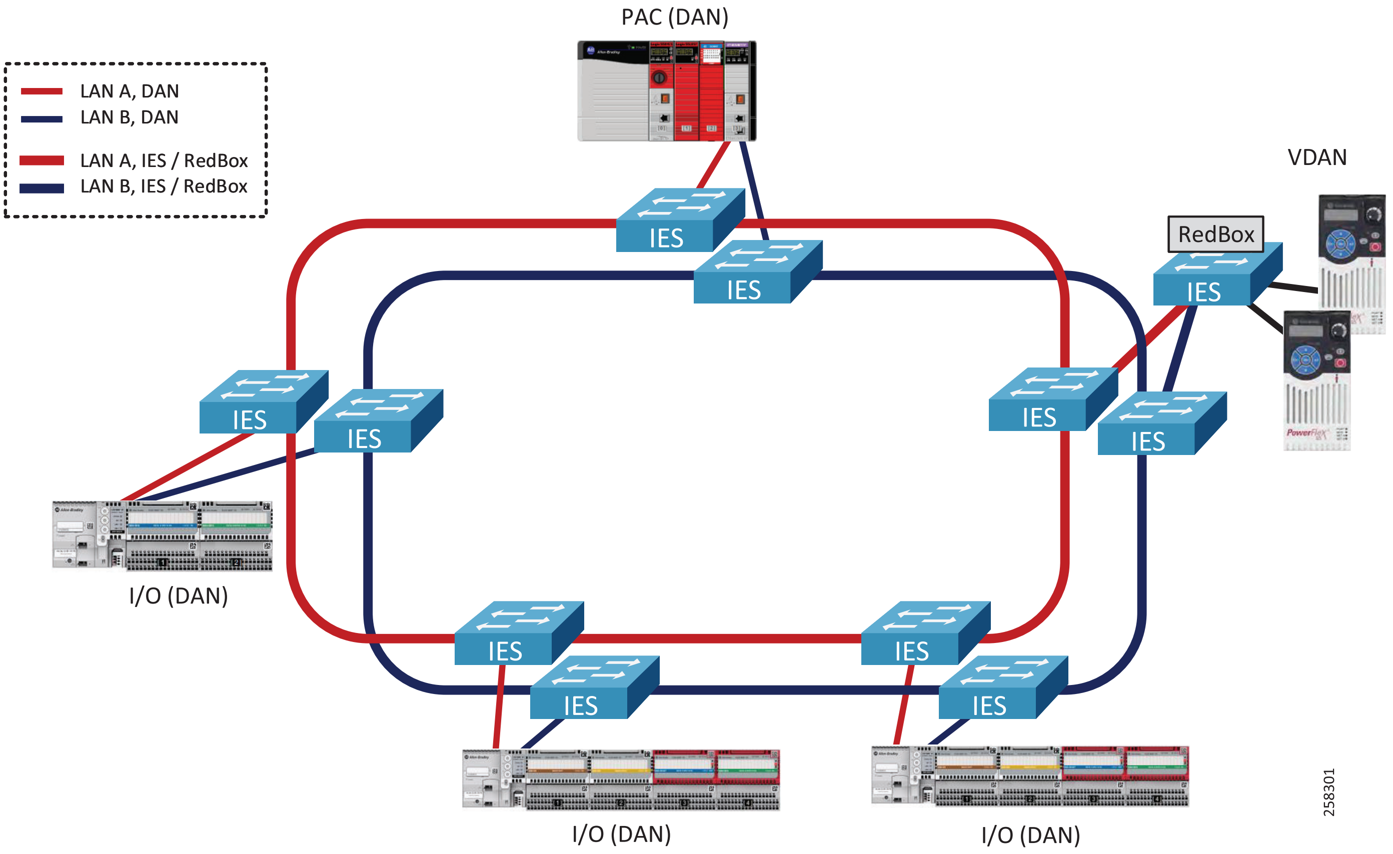


Figure 2-7 shows an example of a PRP topology with dual rings and ControlLogix redundant PACs.

Figure 2-7 PRP Topology Example with Dual Rings—Redundant Controllers

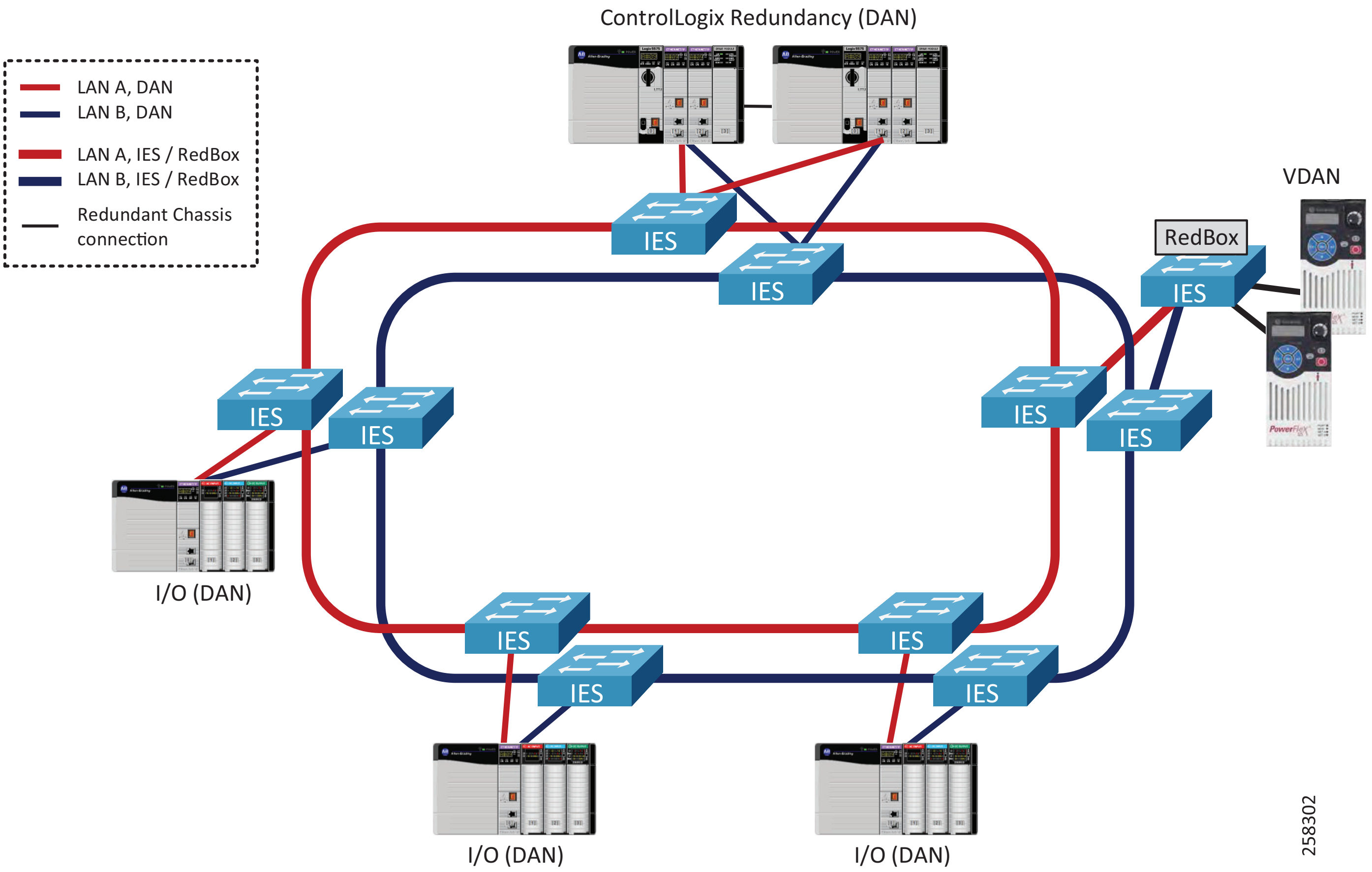
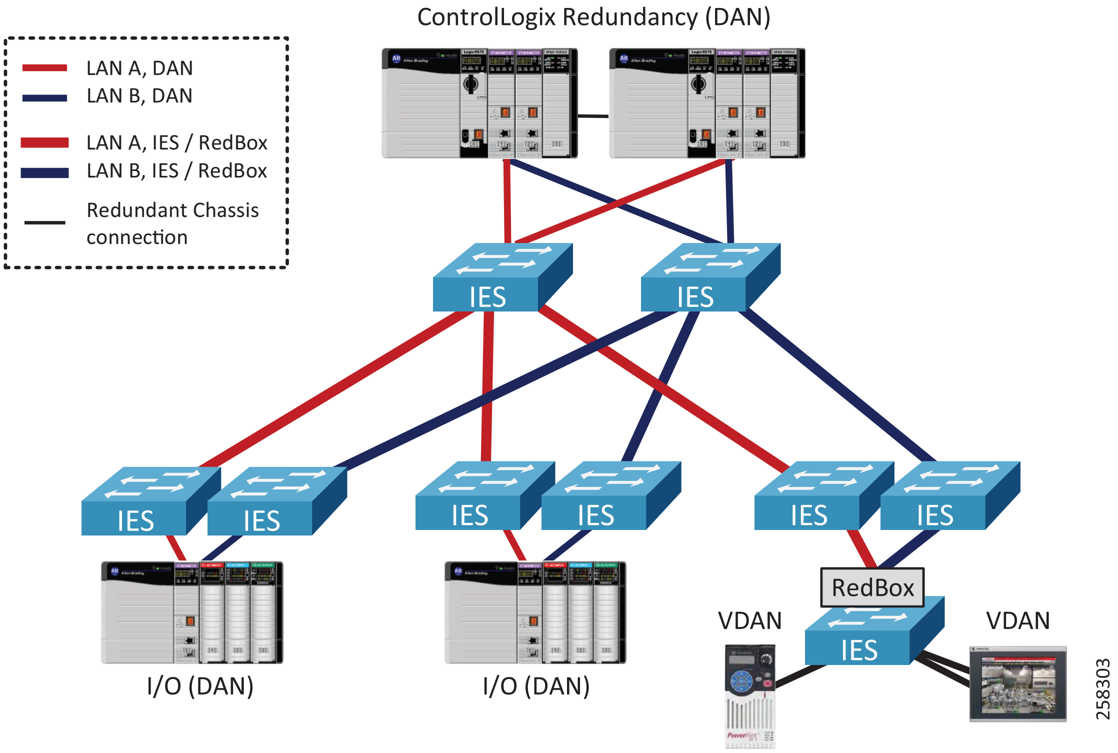


Figure 2-8 shows an example of the star topology in a PRP network.

Note that access IES could also be connected with redundant uplinks to the aggregation IES in the LAN A or B, for example using EtherChannel technology. The cost of additional cabling and available ports should be considered.

Figure 2-8 PRP Star Topology Example



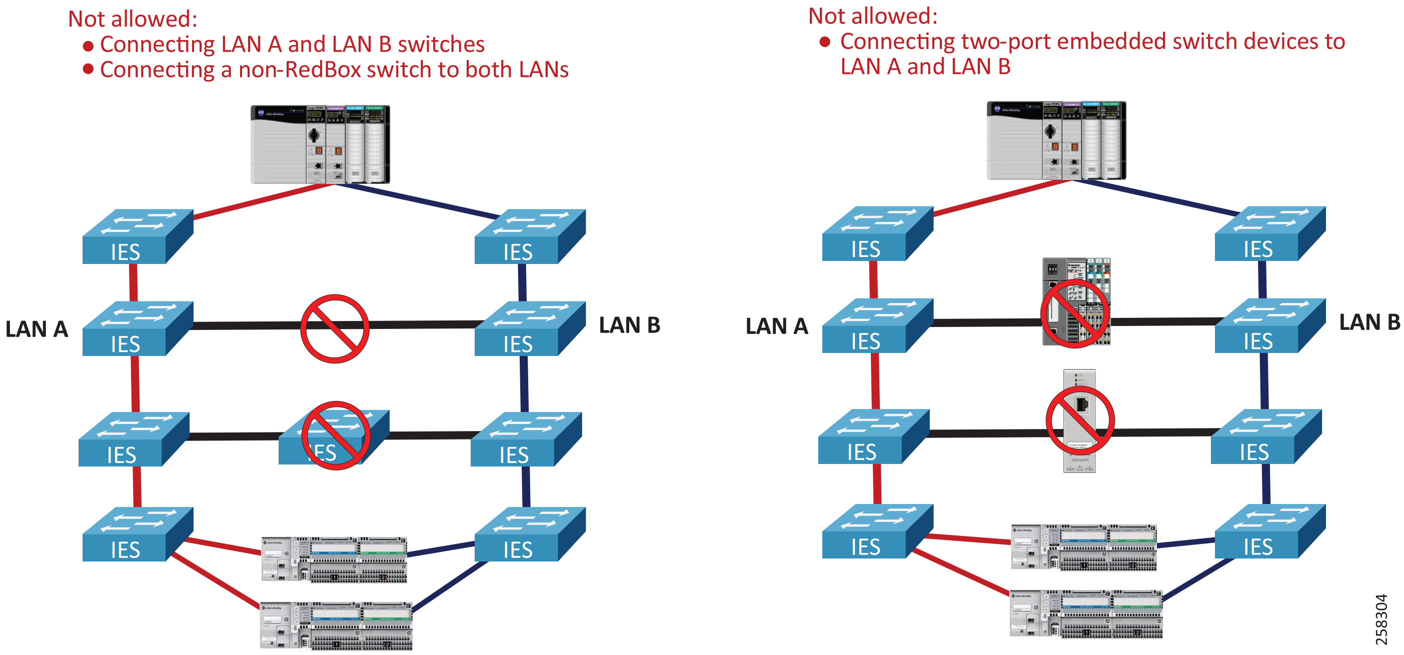
Note The CPwE PRP architecture has been tested and validated using a dual ring topology for LAN A and LAN B with a mix of redundant and non-redundant PACs (Figure 2-6 and Figure 2-7). Other topologies (star, redundant star, linear) are supported if configuration recommendations in this Design and Implementation Guide are followed.

Unsupported Topologies

This section describes a number of invalid PRP topologies or topologies that are not recommended due to performance or availability concerns.

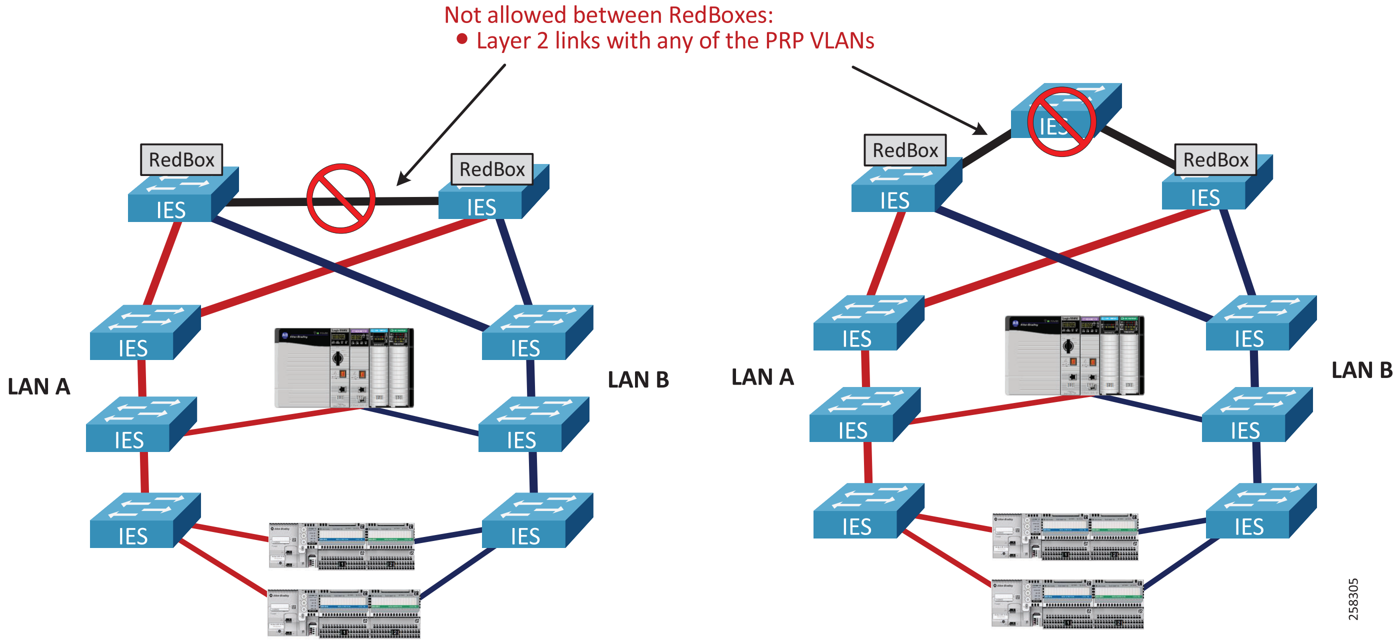
- LAN A and LAN B infrastructure cannot be bridged together using a direct link, a non-RedBox IES, or a two-port embedded switch device that does not support PRP (e.g., a ControlLogix 1756-EN2TR module or a 1783-ETAP EtherNet/IP DLR tap module).

Figure 2-9 Invalid Topology—Bridging LAN A and LAN B


Not allowed:
● Connecting LAN A and LAN B switches
● Connecting a non-RedBox switch to both LANs
Not allowed:
● Connecting two-port embedded switch devices to LAN A and LAN B
LAN A
LAN B
LAN A
LAN B
IES
258304

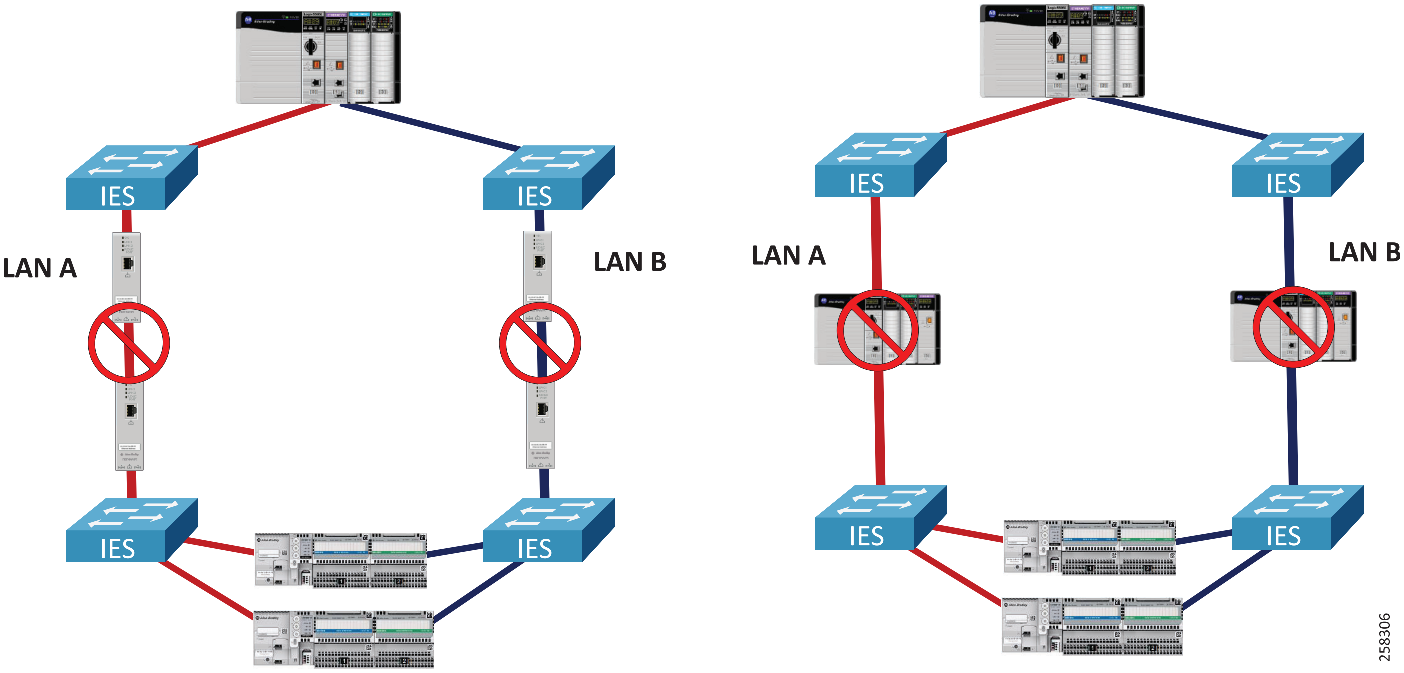
- RedBox IES cannot be connected through a non-PRP ports via a Layer 2 path that forwards traffic from any of the PRP VLANs, including IACS data VLANs, management VLAN, or the native VLAN (Figure 2-10).

Figure 2-10 Invalid Topology—Bridging PRP VLAN via RedBox non-PRP Ports


Not allowed between RedBoxes:
● Layer 2 links with any of the PRP VLANs
RedBox
RedBox
RedBox
RedBox
IES
LAN A
LAN B
LAN A
LAN B
258305

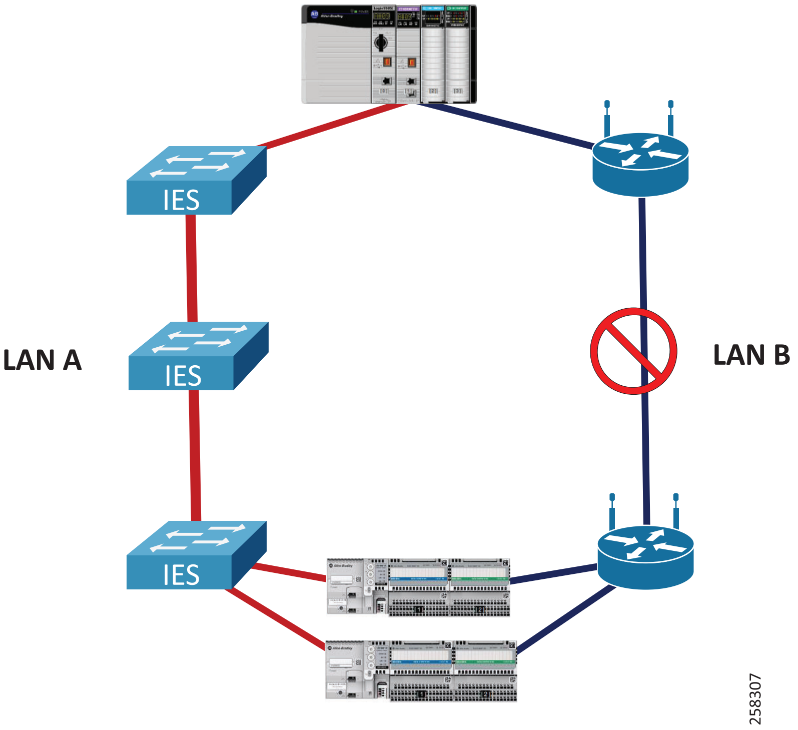
- LAN A/B topologies should not contain two-port embedded switch devices, including 1783-ETAP modules, in the data path. Embedded switch devices cannot be configured for the larger MTU sizes to accommodate the PRP trailer in the frame. As a result, maximum size Ethernet frames may be dropped. This also applies to any IES without the option to increase the MTU size (Figure 2-11).

Figure 2-11 Unsupported Topology—Traversing Two-port Embedded Switch Devices



- It is not recommended to combine high-bandwidth low-latency LAN as the primary LAN and low-bandwidth high-latency WAN or wireless technology as the secondary LAN. One of the possible issues could be increased chance of duplicate frames arriving late and being wrongly accepted as non-duplicate (Figure 2-12).

Figure 2-12 Unsupported Topology—Using High-latency Connection as Secondary



Connectivity to the Industrial Zone Network

The CPwE PRP architecture provides guidelines for connecting a PRP-enabled Cell/Area Zone to the plant-wide or site-wide network in the Industrial Zone.

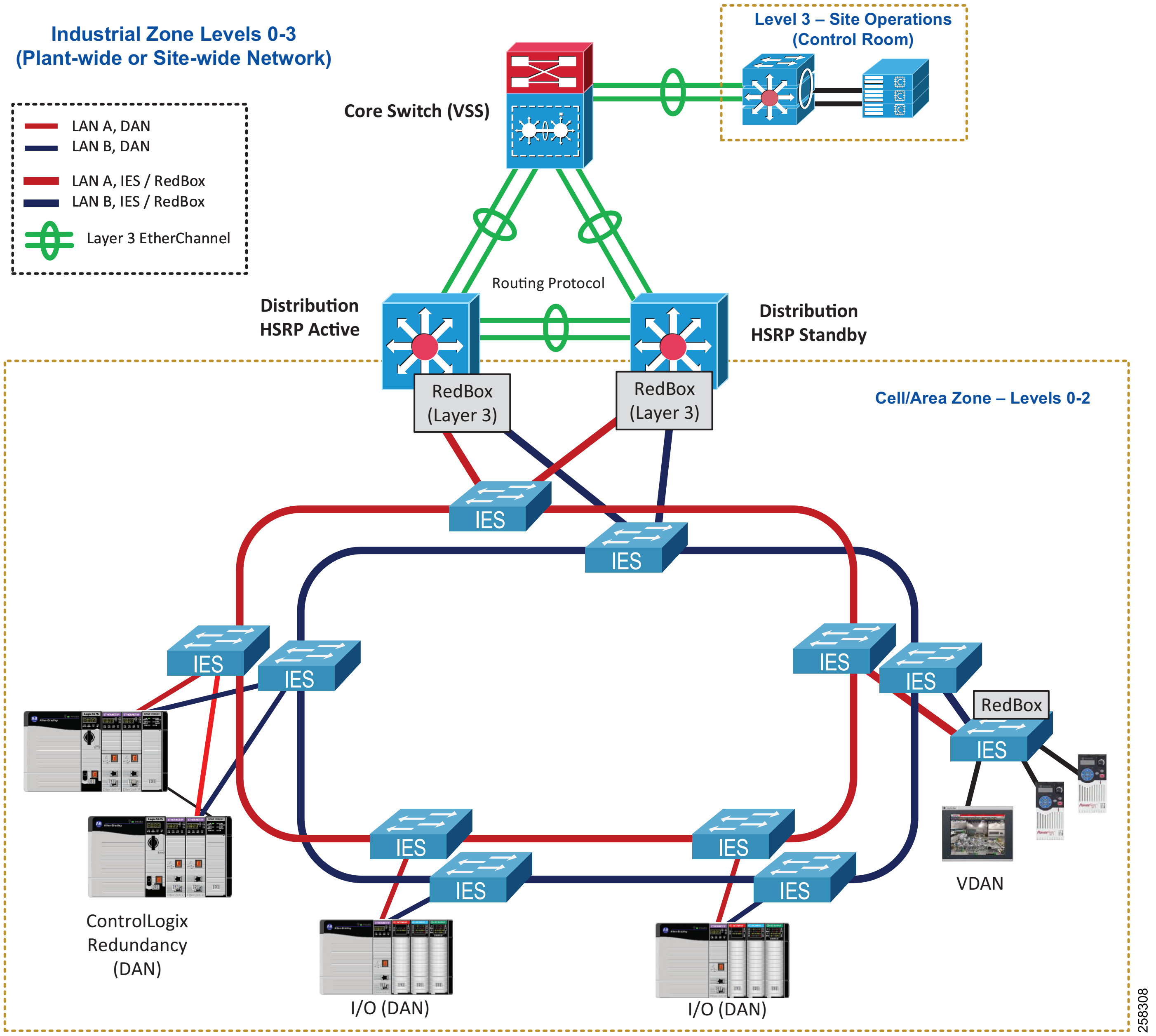
Although IACS applications may exist when a PRP network is deployed as a standalone network (e.g., an isolated I/O network), having plant-wide or site-wide connectivity to the IACS network with PRP technology allows many benefits of the converged network model. This consists of remote access for diagnostics and troubleshooting, distributed network applications using virtual server environment in the Level 3 Site Operations, and access to IACS device data and analytics as part of the Connected Enterprise™ smart manufacturing model.

When connecting a PRP topology with two redundant and isolated LANs to a non-PRP resilient topology, these rules should be followed to avoid bridging loops:

- Only RedBox IES can be used as gateways from a PRP to a non-PRP part of the network.
- Any non-PRP enabled path between RedBox IES should only include Layer 3 (routed) connections.

Figure 2-13 shows the CPwE PRP architecture that provides redundant connectivity from a resilient core layer in the Industrial Zone to a pair of distribution RedBox IES connected to the PRP topology (shown as redundant rings in this example).

Figure 2-13 Connectivity to the Industrial Zone



- Redundant RedBox IES are configured with Hot Standby Router Protocol (HSRP) as active/standby default gateways for IP subnets in the PRP topology.
- Redundant links between RedBoxes and towards the core are configured as Layer 3 EtherChannels (routed ports).
- Dynamic routing protocol is configured between the distribution RedBox HSRP pair and the core switch network.
  - Enhanced Interior Gateway Routing Protocol (EIGRP) has been validated as part of the CPwE PRP.
  - Open Shortest Path First (OSPF) routing protocol can also be used depending on the existing infra-structure and requirements. OSPF has not been validated as part of CPwE PRP.

    - Static routes between RedBox IES and the core are allowed but not recommended due to increased complexity of configuration and maintenance in large environments. CPwE PRP has not been validated with static routing.
- Cisco StackWise Virtual technology or Virtual Switching System (VSS) technology is used for the Cisco Catalyst core switch redundancy.
    - Other resiliency protocols and technologies can be used as outlined in the CPwE Resiliency DIG but have not been tested and validated as part of this CPwE PRP.

EtherChannel, HSRP, and Routing Protocol Considerations

General EtherChannel and HSRP recommendations and configuration guidelines are provided in the CPwE Resiliency Design and Implementation Guide:

- Deploying a Resilient Converged Plantwide Ethernet Architecture
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

For information about EIGRP design and configuration, refer to:

- Enhanced Interior Gateway Routing Protocol
http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html

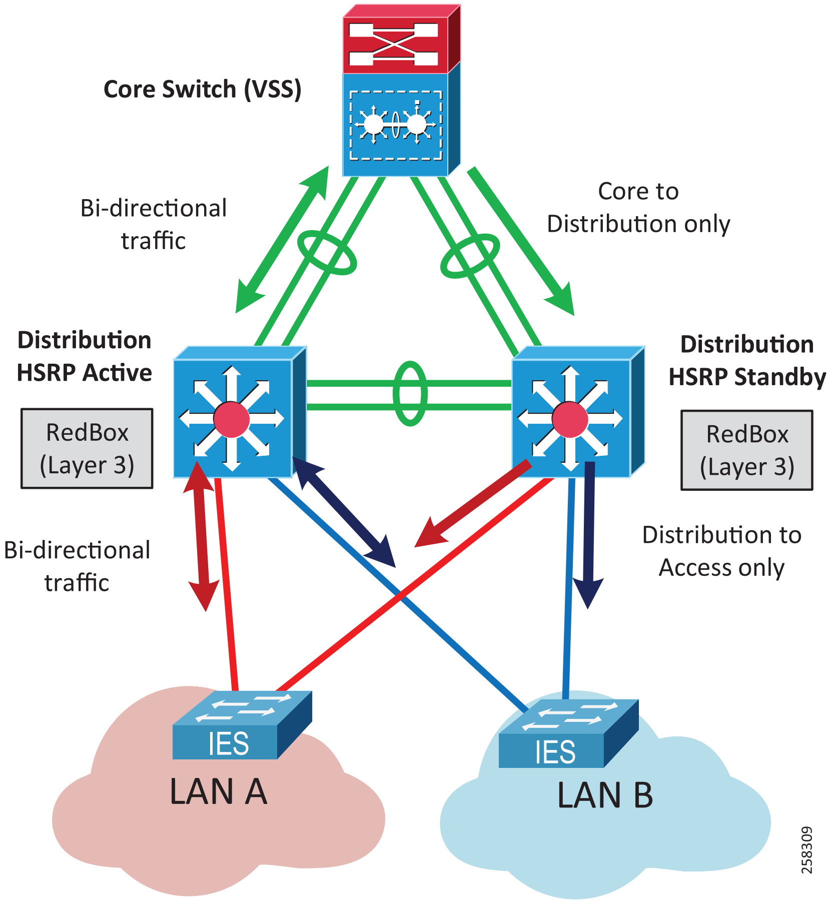
For information about OSPF, refer to:

- OSPF Design Guide
http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

An important consideration for the CPwE PRP routed design is that both Layer 3 RedBox IES carry traffic from the Industrial Zone core network to the Cell/Area Zone, e.g., from an HMI server to an HMI client or a controller (Figure 2-14).

This is due to the equal cost routing on the core switch where downstream traffic is split roughly evenly between the links to the RedBoxes. As a result, a failure of either the active or the standby HSRP RedBox IES may impact the IACS traffic from Level 3 Site Operation. Similarly, restoring a RedBox IES as the standby HSRP gateway may lead to comparatively small convergence times as the traffic is restored on the second path.

Figure 2-14 Routed Traffic Flow



The recommended and validated EtherChannel, HSRP, and EIGRP configuration for CPwE PRP is provided in Chapter 3, "CPwE Parallel Redundancy Protocol Configuration." Maximum observed convergence times for different faults affecting Layer 3 traffic are listed in Table 2-2.

Note Convergence times for routed IACS data include the sum of multiple events including HSRP failover time, dynamic routing protocol convergence, and Layer 2 switched network convergence. Different routing configurations, protocols, and core switch platforms may provide different results.

Table 2-2 Routed Traffic Convergence Times for HSRP[1] and EIGRP

Event Type	Maximum Observed Convergence Time (ms)		
	Core to Cell/Area Zone	Cell/Area Zone to Core	Inter-VLAN to Cell/Area Zone
Gateway down (HSRP Active)	2200	1215	1155
Gateway down (HSRP Standby)	2180	0	0
Gateway restored (HSRP Standby)	320	0	0

[1] With HSRP hold timers 750 ms.

Table 2-3 provides maximum observed converged times for Layer 3 EtherChannel faults. These results are comparable to convergence results for Layer 2 EtherChannel documented in the CPwE Resiliency DIG.

The results for loss of both EtherChannel links are also included. This event can happen, for example, due to misconfiguration of the EtherChannel or physical damage to both links.

Table 2-3 Routed Traffic Convergence Times for Layer 3 EtherChannel[1]

Event Type	Maximum Observed Convergence Time (ms)	
	Core to Cell/Area Zone	Cell/Area Zone to Core
EtherChannel link loss (HSRP Active to Core)	85	90
EtherChannel link restore (HSRP Active to Core)	70	60
EtherChannel link loss (HSRP Standby to Core)	90	0
EtherChannel link restore (HSRP Standby to Core)	135	0
EtherChannel loss, **both** links (HSRP Active to Core)	1735	2400
EtherChannel loss, **both** links (HSRP Standby to Core)	2265	0

[1] With LACP Active mode.

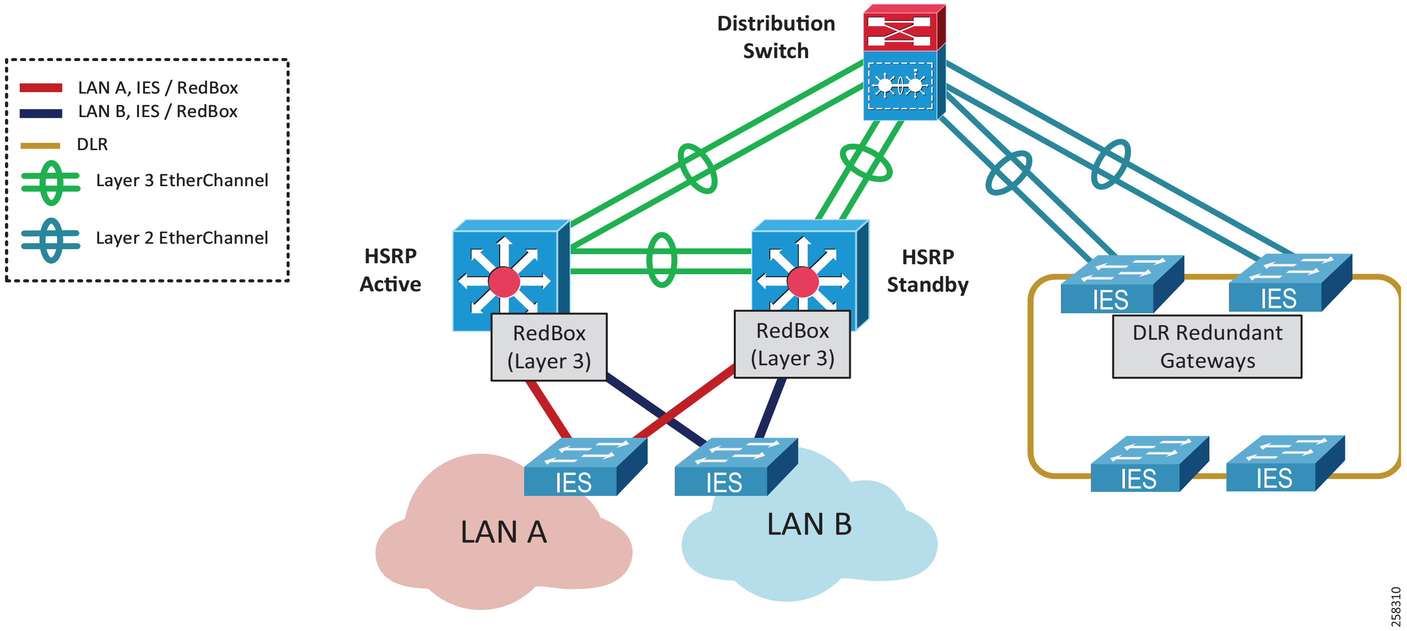
Note It is important to evaluate IACS application requirements for the routed traffic and compare with the expected convergence times. For example, Requested Packet Interval (RPI) values for routed CIP Class 1 data (I/O or Produced Consumed tags) may need to be increased to allow for higher convergence.

Connectivity to Device Level Ring (DLR)

This section describes recommendations for integrating existing or new DLR networks with PRP topologies.

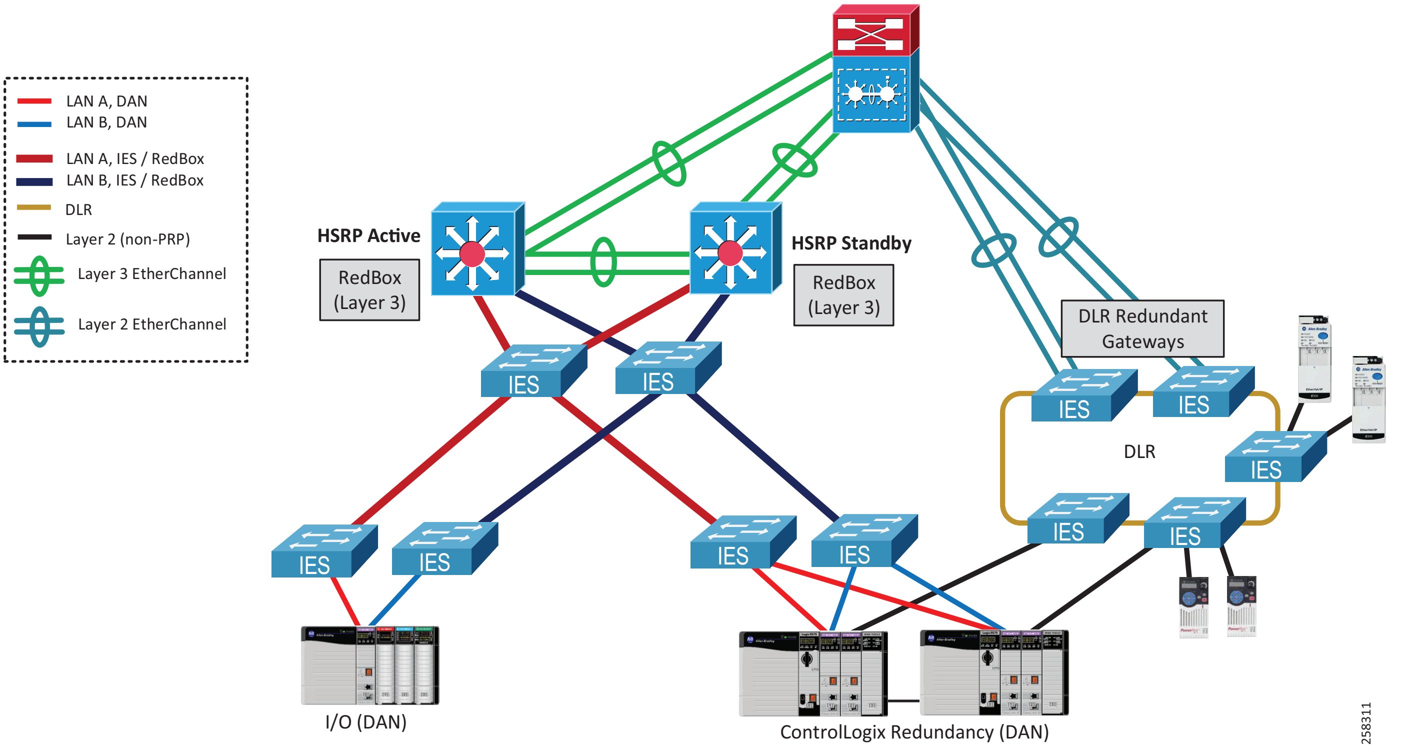
- The recommended resilient architecture is to connect the DLR topology to a separate distribution switch (Figure 2-15).

Figure 2-15 Connecting DLR Topology—Separate Distribution Switch



- Connecting a controller chassis to both PRP and DLR networks using separate EtherNet/IP modules is allowed, as long as other guidelines are followed (Figure 2-16). In this example, a ControlLogix Redundancy chassis is connected to the PRP topology as well as the switch DLR topology.

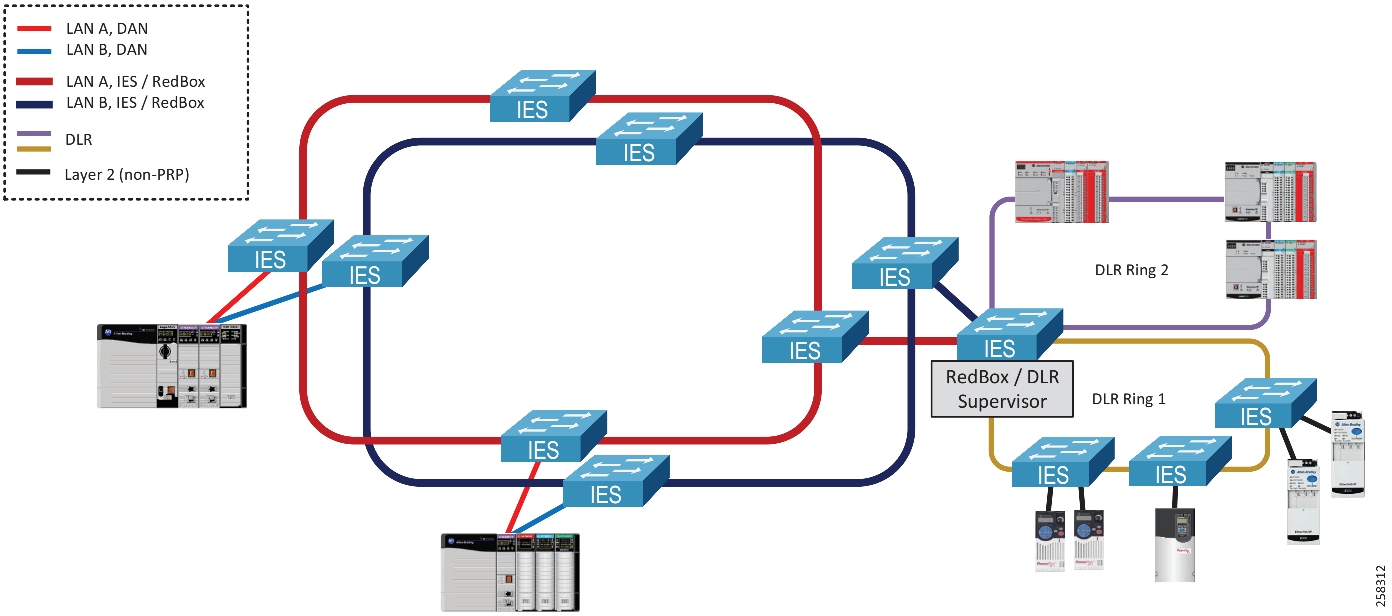
Figure 2-16 Connecting Controller Chassis to both PRP and DLR



- A RedBox IES can be included in the DLR topology as the DLR supervisor for one or multiple rings (Figure 2-17). DLR ports cannot be the same as the PRP channel ports.

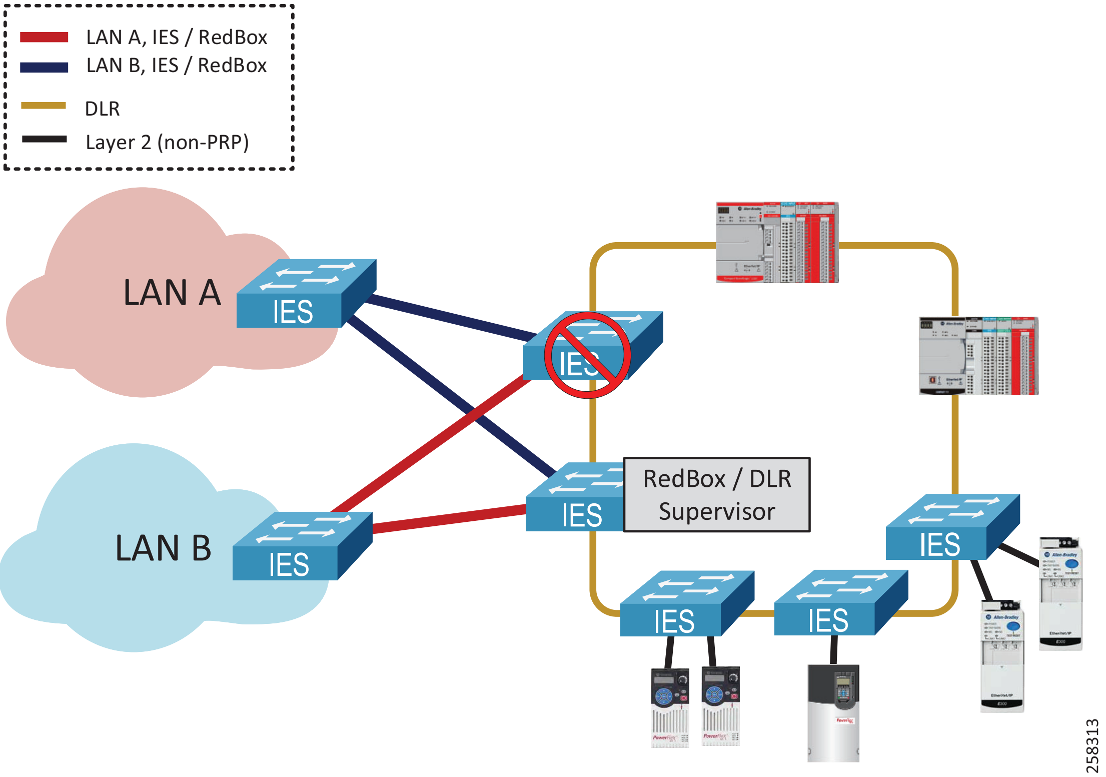
Note In this case the RedBox is a single point of failure for the traffic between the DLR and the PRP topologies. This architecture is not recommended for critical application data traversing the RedBox and has not been validated for performance or scalability in this CPwE PRP.

Figure 2-17 PRP to DLR Connectivity via a RedBox



- Using two RedBox IES as redundant DLR gateways is not supported due to increased convergence time for traffic traversing the gateways during certain faults, which exceeded requirements for IACS applications (Figure 2-18).

Figure 2-18 Unsupported Topology—PRP to DLR Redundant Gateways



Note A PRP-enabled EtherNet/IP module cannot be used as part of the DLR or a linear topology. PRP modules do not implement the embedded switch technology and traffic cannot traverse from port A to port B.

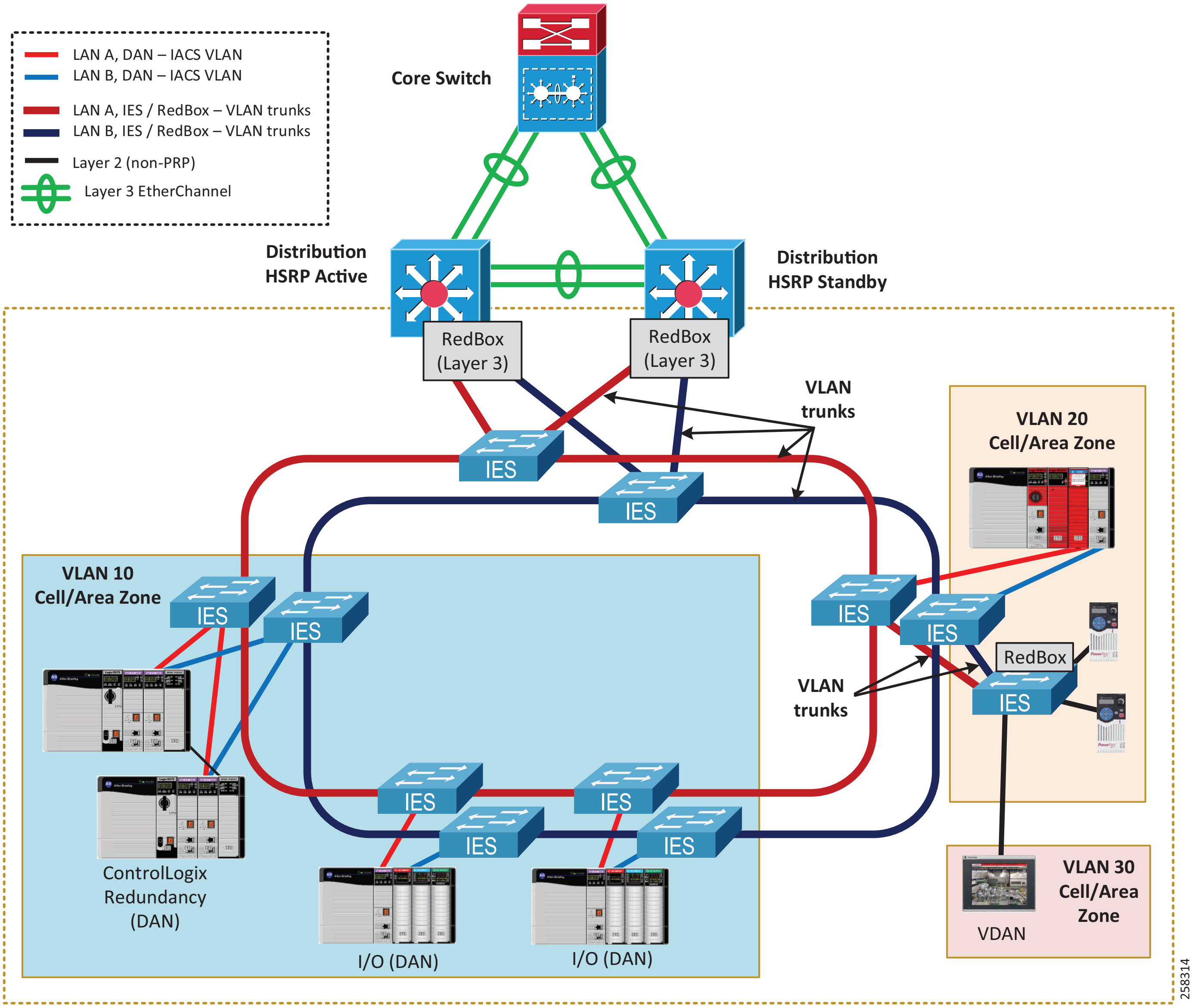
Network Services Recommendations

This section provides recommendations for network services and IES features that could be required in the PRP-enabled IACS network, such as VLAN segmentation (zoning) and trunking, multicast traffic management, time synchronization, and network address translation (NAT).

VLAN Segmentation (Zoning) and Trunking

PRP technology can be deployed in networks with VLAN segmentation. Links between IES can be configured with VLAN trunking to carry traffic from DANs and VDANs that belong to multiple VLANs (Figure 2-19).

Figure 2-19 VLAN Segmentation (Zoning) in PRP Network



Follow these recommendations when using VLAN segmentation (zoning) with PRP:

- Both PRP ports on a DAN should be connected to the same VLAN in LAN A and LAN B.
- The PRP channel ports on a RedBox IES can be configured as VLAN trunk ports (more common) or access mode ports (i.e., single VLAN). Trunk mode allows having VDANs in multiple VLANs or use a separate management VLAN for the RedBox IES.
- PRP channels on the redundant Layer 3 RedBox IES in CPwE PRP are configured as VLAN trunks. The architecture has been validated with inter-VLAN IACS traffic which is routed through the RedBox.
- Links between IES in each PRP LAN are configured as trunks which follows CPwE best practices. The native VLAN should differ from any of the IACS VLANs.

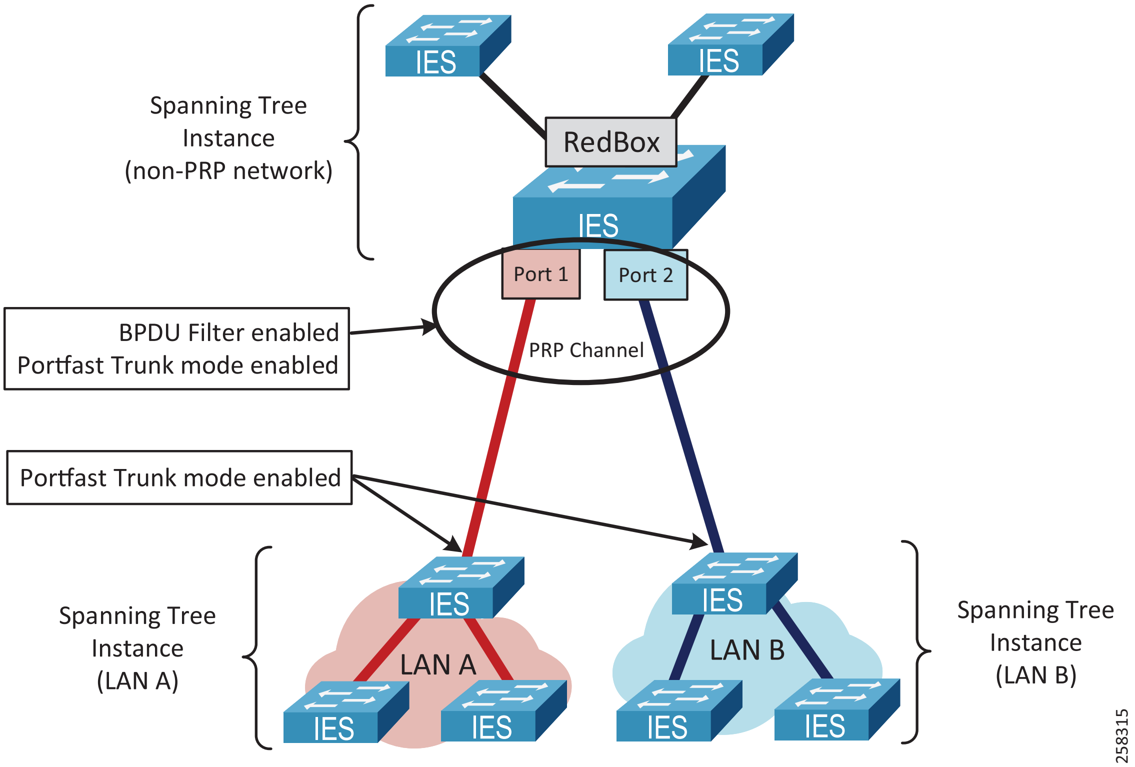
Note PRP supervisory frames are Layer 2 multicast Ethernet frames that cannot be routed between VLANs. DANs can only report diagnostic information about PRP devices in their VLANs.

Spanning Tree Protocol

Design and configuration of the Spanning Tree Protocol (STP) in PRP LAN A and LAN B should follow general recommendations in the CPwE Resiliency Design and Implementation Guide. Special considerations exist for STP operation between a RedBox IES and infrastructure IES (Figure 2-20):

- Bridge Protocol Data Unit (BPDU) frames from STP are filtered on the PRP channel ports. As a result, LAN A/B switches exclude the RedBox IES in the STP operation.
- STP is running on the RedBox IES by default and can operate in the non-PRP infrastructure connected to the RedBox (if it exists) for normal loop prevention and resiliency purposes.
- PortFast Trunk mode should be configured for the PRP channel group on all RedBox IES, including redundant Layer 3 Redboxes, and on the LAN A/B IES ports connected to the RedBox. This is necessary to minimize port recovery time during network faults.

Figure 2-20 Spanning Tree Operation in the PRP Network


IES
IES
Spanning Tree Instance (non-PRP network)
RedBox
IES
Port 1
Port 2
BPDU Filter enabled
Portfast Trunk mode enabled
PRP Channel
Portfast Trunk mode enabled
Spanning Tree Instance (LAN A)
IES
LAN A
IES
IES
IES
LAN B
IES
IES
Spanning Tree Instance (LAN B)
258315

Note Other resiliency protocols such as DLR and REP, if present in the PRP LAN topologies, may have their own considerations for STP interoperability, separate from the PRP considerations. Refer to the corresponding CPwE DLR Design Guide and CPwE Resiliency Design and Implementation Guide for more information.

Multicast Management

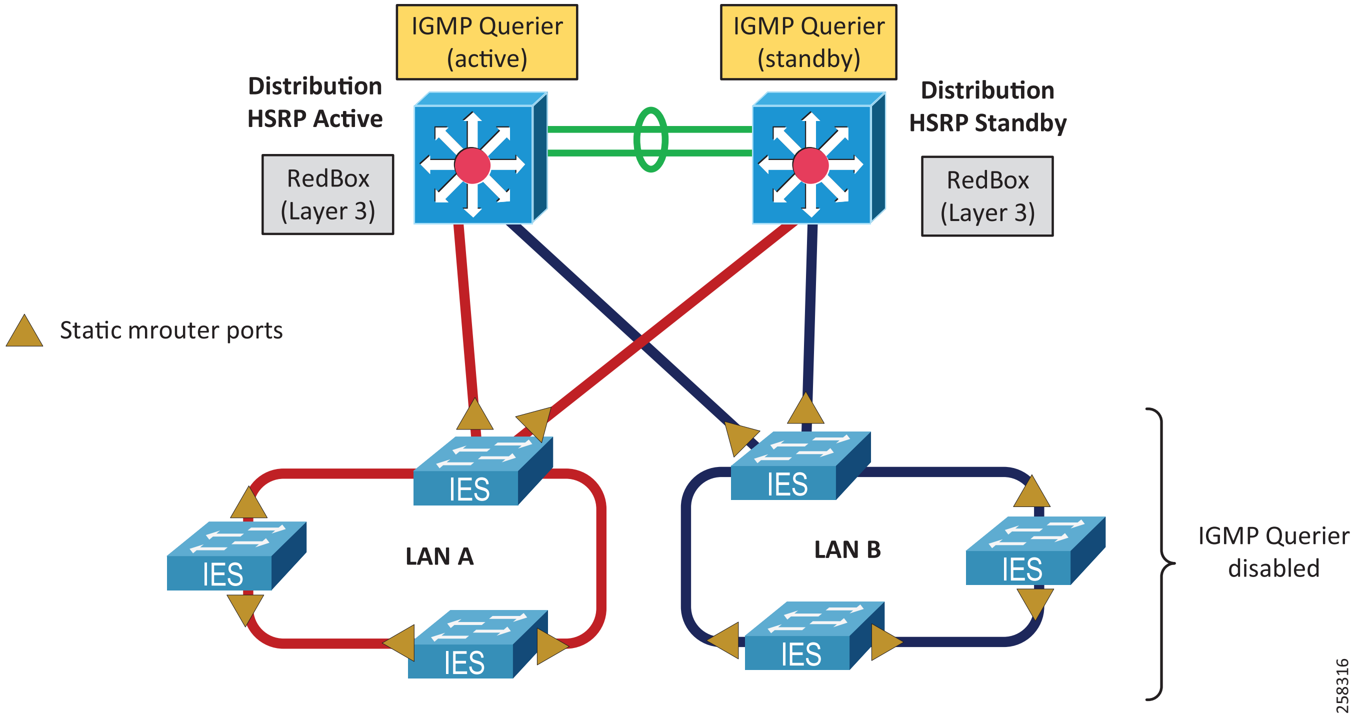
Multicast EtherNet/IP traffic is required for I/O and consumed data in ControlLogix Redundancy and for CIP Sync communication using Precision Time Protocol (PTP). Both types of multicast data could be used in IACS applications where PRP technology is deployed.

It is critical to follow design and configuration guidelines for multicast traffic management in CPwE PRP to make sure that high availability is achieved:

- Enable Internet Group Management Protocol (IGMP) snooping on all IES to reduce the amount of unnecessary multicast traffic to end nodes. IGMP snooping is enabled by default after Express Setup on Stratix managed switches.
- Configure IGMP querier on the redundant Layer 3 RedBox IES (distribution switches in active/standby HSRP configuration). Make sure that at least two IGMP queriers are present. In order to win the querier election, switches should have the lowest IP addresses in the subnet.
- Disable IGMP querier on each IES in LAN A and LAN B.
- Configure uplink ports on the LAN IES as static multicast router (mrouter) ports, specifically the ports that could be in the path to the IGMP querier (distribution RedBox IES). This configuration enables multicast traffic flow in the topology when the IGMP querier changes (for example when the active HSRP gateway reboots).

Figure 2-21 illustrates IGMP snooping configuration in the PRP topology. For details on how to configure these settings, refer to Chapter 3, “CPwE Parallel Redundancy Protocol Configuration.”

Figure 2-21 Multicast Management with PRP



Note After a LAN in a PRP network encounters a fault and is then repaired, there could be a delay in restoring multicast traffic PRP redundancy. The delay lasts until the IGMP querier reinstates the multicast traffic in the recovered LAN (typically within two minutes after the LAN is repaired). During that time, the other LAN will continue forwarding multicast traffic.

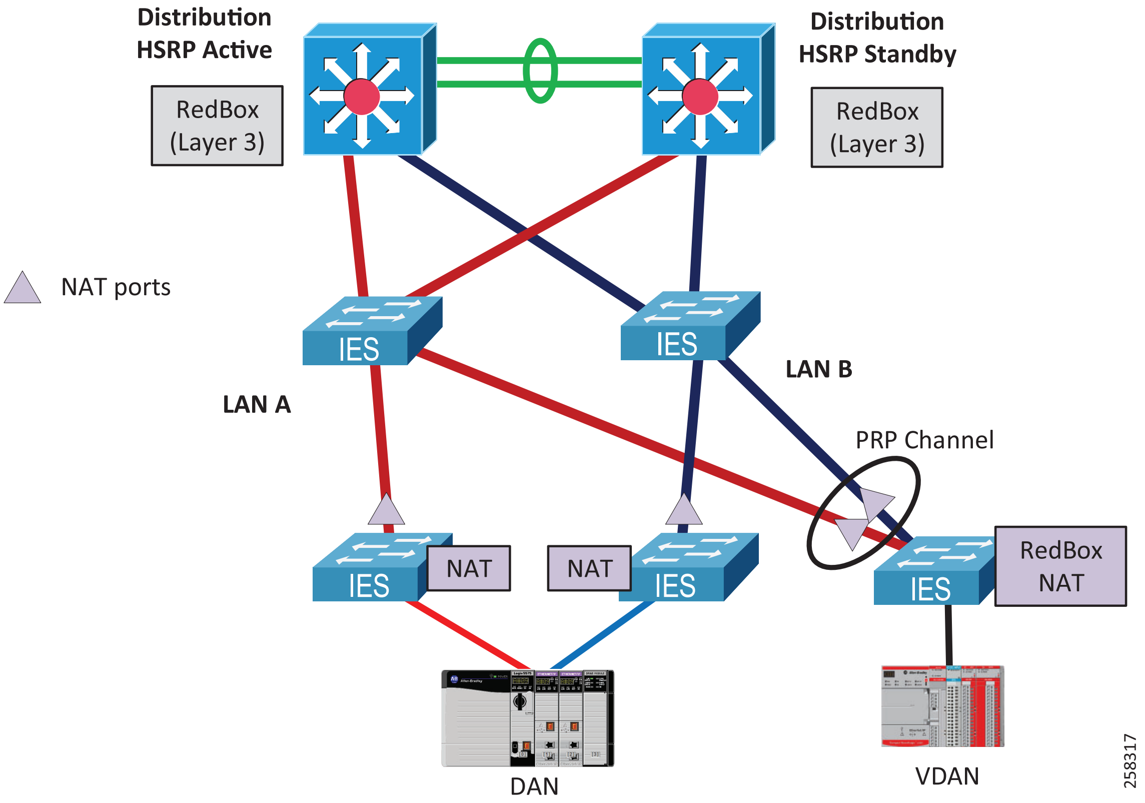
Network Address Translation

Network Address Translation (NAT) feature in IES provides benefits to OEM machine or process skid builders, such as IP address reuse and commissioning of "cookie cutter" machines without reprogramming, easier maintenance of machine configurations and controller programs, and better traffic control and additional security by limiting access only to selected devices on a machine or skid. It may also help plant or site engineers with integrating legacy stand-alone equipment into the plant-wide or site-wide network.

PRP technology is compatible with NAT since PRP operates in Layer 2 and does not rely on IP addresses (Layer 3). There are two possible implementations of NAT in a PRP topology (Figure 2-22):

- Configure NAT on the LAN A/B infrastructure IES to provide translation for DANs.
- Configure NAT on the RedBox IES to provide translation for VDANs.

Figure 2-22 Network Address Translation with PRP



Since CPwE PRP implements HSRP for router redundancy, the following translation rules need to be added to the NAT configuration:

- Gateway translation for the virtual IP address of the HSRP gateways

- Public-to-Private translation for the physical IP addresses of both active and standby HSRP gateways (RedBox IES)

Other general NAT recommendations and limitations may apply, for example topology considerations, multicast restrictions, or application restrictions. For more information on NAT with Stratix IES, refer to:

- Deploying Network Address Translation (NAT) within a CPwE Architecture
  https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
- Stratix Managed Switches User Manual
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

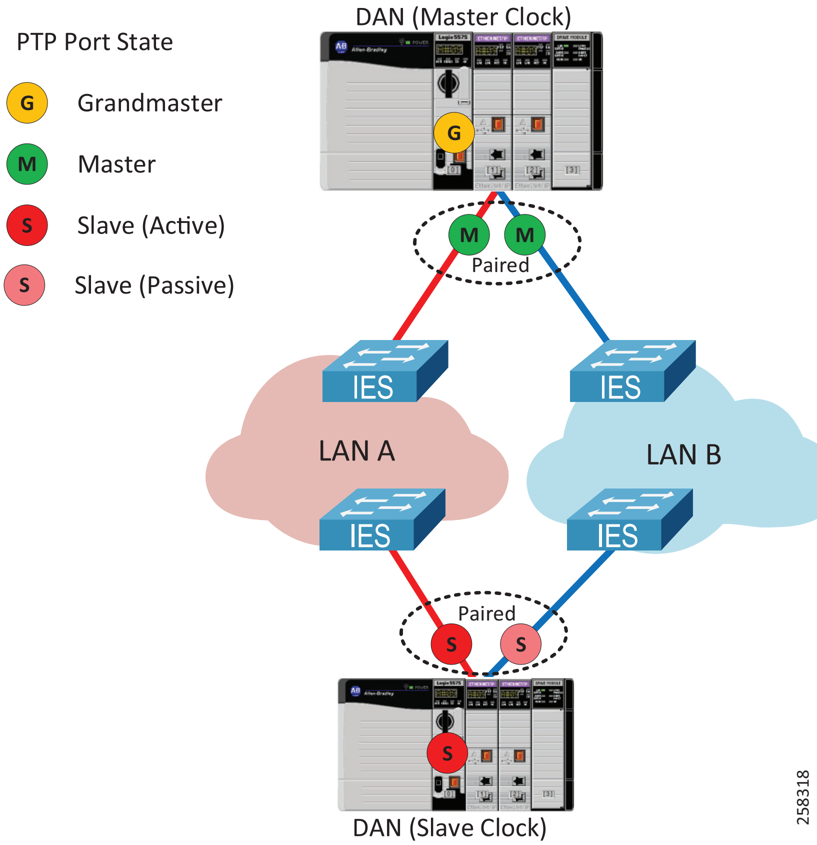
Precision Time Protocol (CIP Sync)

CIP Sync technology uses the IEEE 1588-2008 Precision Time Protocol (PTP) standard for time synchronization. CIP Sync is designed for local and plant-wide or site-wide IACS applications requiring high accuracies beyond those attainable with Network Time Protocol (NTP).

PRP networks support CIP Sync by implementing the doubly-attached clock model as specified in IEC 62439-3 standard (Figure 2-23):

- In a DAN or a RedBox with the master clock role, both ports A and B operate as CIP Sync master ports in their LAN segments.
- In a DAN or a RedBox with a slave clock role, both ports A and B are paired and function as CIP Sync slave ports.
  - One port is the active port that tunes the clock and reports its state as SLAVE.
  - The other port is passive and reports its state as PASSIVE_SLAVE. The passive port also measures path delay and maintains close synchronization to the active port. In case of a network failure on the active port, the passive port clock transitions smoothly to the active state.
- PTP traffic in the PRP network is handled differently from other traffic, specifically the Ethernet frames do not have RCT attached and bypass the duplicate/discard mechanism. PTP packets from DANs, such as Sync, Delay Request, and Delay Response are generated independently by each physical port.

Figure 2-23 PRP Doubly Attached Clock Model



Using PTP and CIP Sync in CPwE PRP requires specific configuration of the infrastructure IES and RedBox IES, as well as properly selecting the Grandmaster clock in the topology:

- Select **one** of the following as the Grandmaster for a PRP network:
  - A DAN (a doubly-attached clock)
  - A PAC or a time module in the PAC chassis that accesses the PRP network via a DAN module or via a RedBox IES
  - A VDAN that connects to a RedBox, e.g., a GPS time source device
  - A RedBox IES in the NTP/PTP Clock.
- For critical applications using time synchronization, consider implementing redundant Grandmasters connected as DANs, VDANs, or RedBoxes. Do not use Redundant Grandmasters connected as SANs (one in LAN A and another in LAN B).
- Configure RedBox IES in Boundary or NTP/PTP Clock mode. These modes are the only PTP modes that are supported on a RedBox IES.
  - A RedBox IES works as a boundary clock between the PRP and non-PRP segment of the network. It does not operate as a boundary clock between LAN A and LAN B.
- Configure infrastructure IES in LANA and LAN B as transparent clocks.
  - Transparent clock IES do not propagate PTP information between VLANs. Only one VLAN in a PRP topology should be enabled for time distribution.

  - Switches that do not support PTP, or in the PTP forward mode, are allowed but not recommended due to lack of delay compensation and lower time synchronization accuracy in the PRP architecture. IACS requirements for time accuracy should be considered.
  - If a switch in LAN A or LAN B is configured as a boundary clock, it may become the Grandmaster after the network fault in the local segment. This results in two Grandmaster clocks for the PRP architecture, which can create undesirable effects for doubly-attached clocks, for example causing time to drift apart.
- Select only one of the IACS VLAN for time distribution. Disable CIP Sync in all devices on all other VLANs,
  - Make sure that DANs in other VLANs have the Time Sync property disabled in the module properties.
  - Configure PTP VLAN explicitly on the PRP channel ports of RedBox IES.

These recommendations are summarized in Table 2-4 and Table 2-5.

Table 2-4 PTP Clock Roles in the PRP Network

Device Type	Possible Clock Roles		
	Grandmaster	Master Clock	Slave Clock
DAN	Yes	Yes	Yes
PAC	Yes (via DAN in the controller chassis or a RedBox)	Yes	Yes
VDAN	Yes (via a RedBox)	Yes	Yes
SAN	No	No	Yes
RedBox IES	Yes (NTP/PTP mode in the Stratix 5400 and Stratix 5410)	Yes	Yes
LAN A/B IES	No	No	No

Table 2-5 PTP Modes for IES in the PRP Network

Device Type	Allowed IES Clock Roles			
	NTP	Boundary	End-to-end Transparent	Forward
RedBox IES	Yes	Yes	No	No
LAN A/B IES	No	No	Yes	Yes

Figure 2-24 shows an example of a CIP Sync architecture with a DAN as the master clock in the PTP-enabled VLAN. The Grandmaster clock in this example is a GPS time source (ControlLogix 1756-TIME module) connected via a DAN module in the chassis. All IACS devices are in the same PTP-enabled VLAN. PTP information is only distributed in one VLAN because of the transparent clock requirement for the infrastructure IES.

Figure 2-24 Example of CIP Sync with PRP Topology—DAN as the Grandmaster

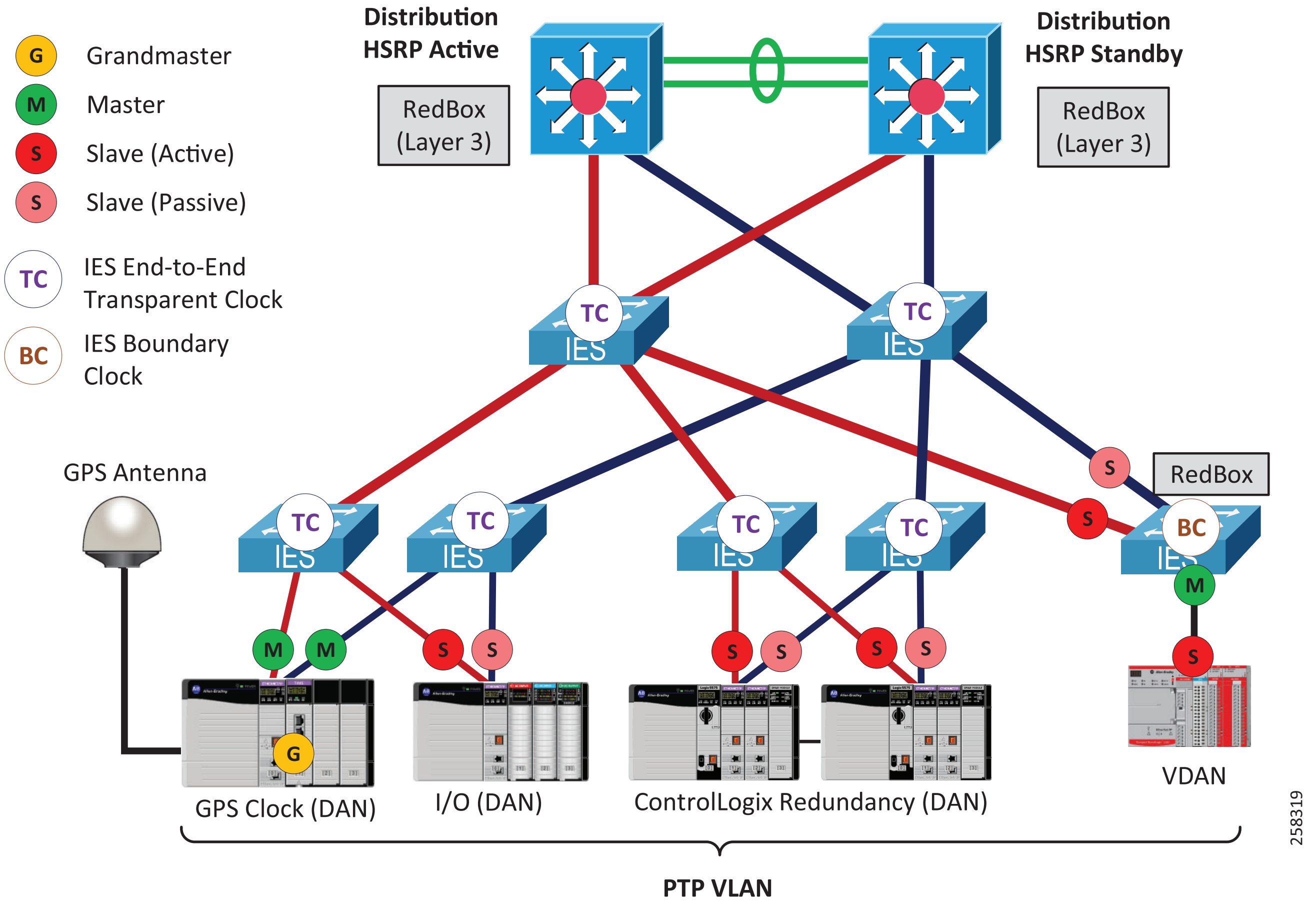
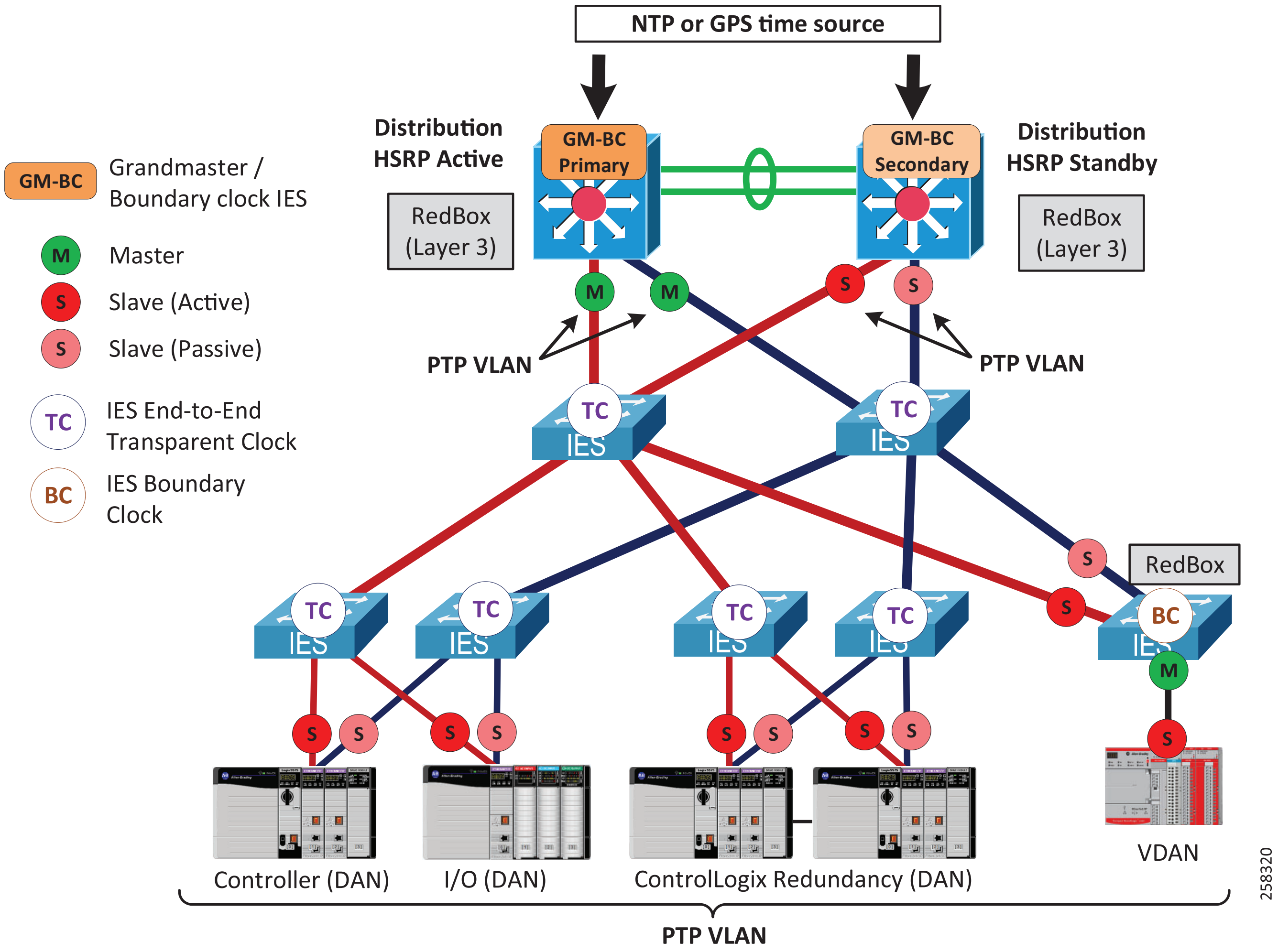


Figure 2-25 shows an example of a CIP Sync architecture where RedBox IES (Layer 3 switches) are the primary and secondary Grandmasters in the CIP Sync architecture (NTP/PTP clock mode). Distribution switches can synchronize to an NTP source, e.g., a GPS receiver in the plant-wide or site-wide network.

In this example, PTP VLAN ID should be configured explicitly on the trunk ports (PRP channel ports) between the RedBox IES and the infrastructure switches. PTP information is only distributed in one VLAN because of the transparent clock requirement for the infrastructure IES.

Figure 2-25 Example of CIP Sync with PRP Topology—RedBox IES as the Grandmaster



For general information on designing and configuring time distribution in the plant-wide or site-wide network, refer to:

- Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td016_-en-p.pdf

For information on how to configure PTP on Stratix managed switches, refer to:

- Stratix Managed Switches User Manual https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

Applying Parallel Redundancy Protocol with IACS Applications

PRP technology does not depend on the network layer or IACS application layer and therefore can be used with different types of IACS applications that require high availability. The following IACS applications and data types have been tested and validated within CPwE PRP:

- CIP Class 1 I/O and Produced Consumed tags (unicast and multicast)
- ControlLogix Redundancy (requires version 31.052 or higher)
- CIP Class 3 messaging

- CIP Safety™
- CIP Sync and PTP
- FactoryTalk® View Site Edition
- FactoryTalk® View Machine Edition
- FactoryTalk® Linx
- RSLinx® Classic
- Studio 5000 Logix Designer®

ControlLogix Redundancy with Parallel Redundancy Protocol

CPwE PRP architecture has been tested with ControlLogix Redundancy including redundant PAC chassis with EtherNet/IP modules (DAN) communicating to DAN or VDAN I/O devices, other PACs, and FactoryTalk applications. ControlLogix Redundancy included the following components:

- EtherNet/IP PRP modules for I/O and Produced Consumed data configured for IP address swapping during a chassis switchover.
- Dedicated EtherNet/IP PRP modules for HMI data that do not swap IP addresses.
- Redundant ControlLogix Controller shortcut type in FactoryTalk Linx that points to the Primary and Secondary controllers through the PRP modules without swapping IP addresses.
- ControlLogix Redundancy firmware revision 31.052 or later, FactoryTalk Linx 6.11 or later
- Infrastructure and RedBox IES configured for IGMP snooping as described in the previous sections.

PRP modules in the primary and secondary chassis can be connected to the same switch in LAN A and the same switch in LAN B or can be connected to different pair of switches in each LAN, depending on the physical layout of the architecture.

Note Routed traffic to and from the ControlLogix Redundancy (e.g., FactoryTalk data or CIP Class 3 messages between VLANs) can be affected by Layer 3 switch faults, HSRP, and routing protocol convergence. These types of faults are not covered by the PRP zero data loss mechanism and should be considered independently in the PRP architecture design calculations.

CHAPTER 3

CPwE Parallel Redundancy Protocol Configuration

IES Configuration

This section describes how to configure Stratix IES in the CPwE PRP architecture using recommendations provided in Chapter 2, “CPwE Parallel Redundancy Protocol Design Considerations.” The included configurations have been validated during testing. The network infrastructure has been configured to support HSRP routing redundancy, VLAN segmentation and VLAN trunking, multicast IACS traffic, and CIP Sync.

Note The configuration examples and screen captures below are provided for Stratix 5700 and Stratix 5400 platforms and should be used only as reference. Configurations should be modified and applied according to the specific network topology, company standards, and practices.

Initial Configuration

Before configuring IES features for the PRP network, switches should be configured according to general recommendations and best practices for IACS networks:

- Apply initial configuration using Express Setup procedure, Plug-n-Play (PnP) method, Command Line Interface (CLI) using serial console connection, or by transferring the configuration file to the SD flash card.
- Make sure that all IES in the PRP network are assigned unique management IP addresses.
- Configure switch ports according to their function using Smartport roles. Smartports optimize switch port configuration according to the type of device connected to the port.
- Configure network protocols, security, and other settings on the switch as appropriate per your company’s policy and standards.

Configuration files can be transferred to a Stratix switch using SD flash cards, Stratix Device Manager, or Studio 5000 Logix Designer® Add-on Profile (AOP).

For more information, refer to:

- Stratix Managed Switches User Manual
https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

Infrastructure IES Configuration

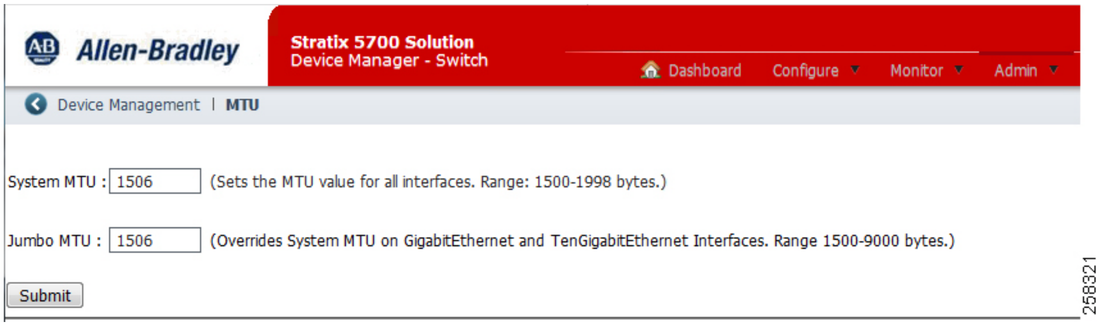
Configuration of infrastructure switches in LAN A and LAN B depends on the chosen topology and resiliency protocol in the LAN (if applicable). Refer to the Stratix switch user manual, corresponding application guides, and CPwE design guides for more information (see Appendix A, "References").

The next steps describe required or recommended settings for infrastructure IES that are specific to the PRP operation. IP addresses, VLAN IDs, and port numbers are examples only.

Step 1 Configure Maximum Transmission Unit (MTU) size to 1506 bytes or greater.

Note After submitting the MTU change, the switch will restart.

Figure 3-1 Configure System MTU Size

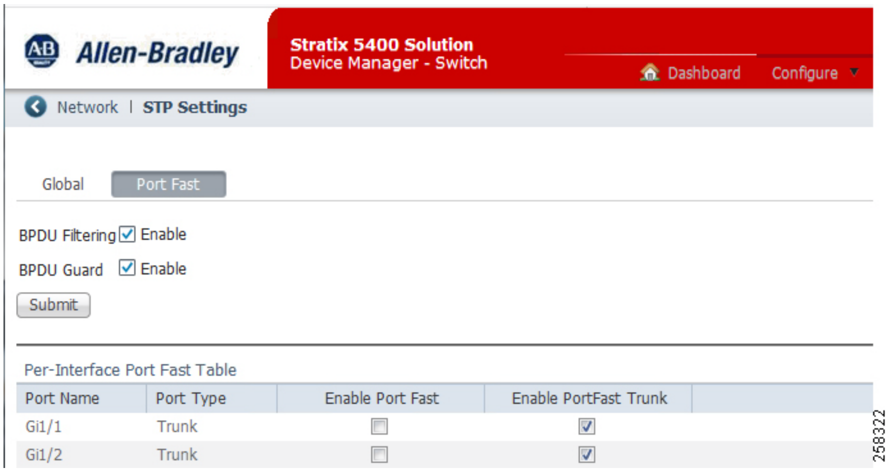


System MTU : 1506 (Sets the MTU value for all interfaces. Range: 1500-1998 bytes.)

Jumbo MTU : 1506 (Overrides System MTU on GigabitEthernet and TenGigabitEthernet Interfaces. Range 1500-9000 bytes.)

Step 2 If the infrastructure switch connects to a RedBox IES using VLAN trunking (Smartport Switch for Automation), configure PortFast Trunk on the port(s) connected to the RedBox.

Figure 3-2 Configure PortFast Trunk



BPDU Filtering ☑ Enable

BPDU Guard ☑ Enable

Per-Interface Port Fast Table

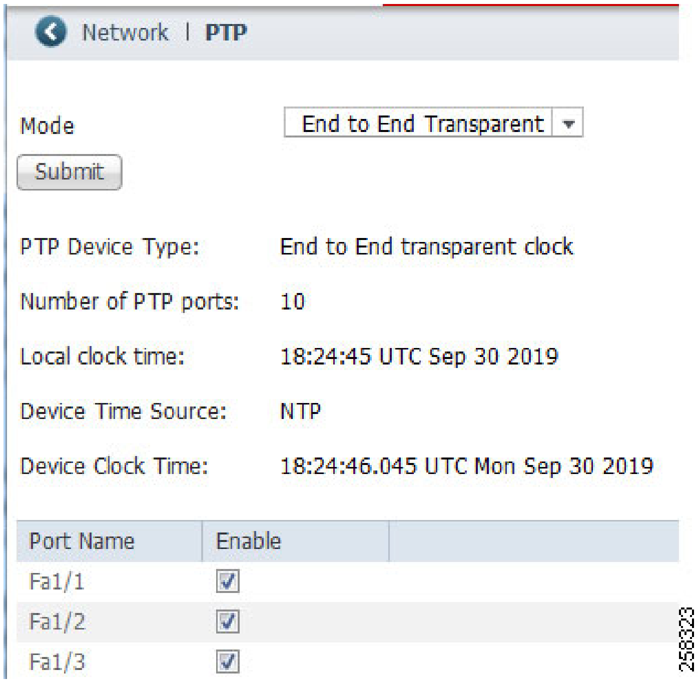
Port Name	Port Type	Enable Port Fast	Enable PortFast Trunk
Gi1/1	Trunk	□	☑
Gi1/2	Trunk	□	☑

PTP (CIP Sync) Configuration

Step 3 If time synchronization is enabled in the network (CIP Sync) and the switch supports PTP, configure PTP End-to-End Transparent mode.

Step 4 Enable PTP on the ports with CIP Sync devices in the PTP VLAN and on the trunk ports to other infrastructure switches. Disable PTP on the ports in other VLANs.

Figure 3-3 PTP Transparent Mode



Mode: End to End Transparent

PTP Device Type:	End to End transparent clock
Number of PTP ports:	10
Local clock time:	18:24:45 UTC Sep 30 2019
Device Time Source:	NTP
Device Clock Time:	18:24:46.045 UTC Mon Sep 30 2019

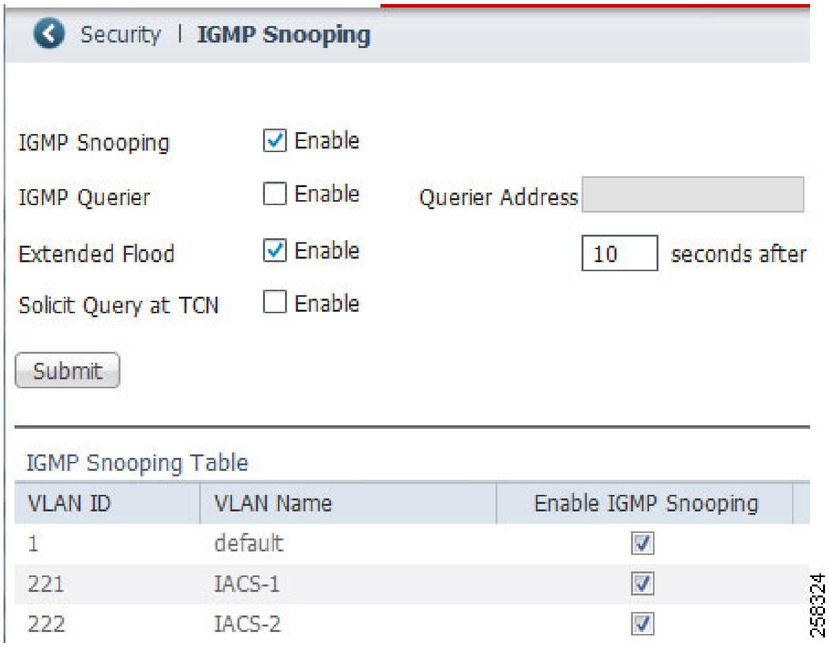
Port Name	Enable
Fa1/1	☑
Fa1/2	☑
Fa1/3	☑

IGMP Snooping Configuration

Step 5 Disable IGMP Querier on the switch. Leave IGMP Snooping enabled for all VLANs.

Step 6 Enable Extended Flood option with the default value of 10 seconds.

Figure 3-4 IGMP Snooping



IGMP Snooping ☑ Enable

IGMP Querier ☐ Enable Querier Address

Extended Flood ☑ Enable 10 seconds after

Solicit Query at TCN ☐ Enable

IGMP Snooping Table

VLAN ID	VLAN Name	Enable IGMP Snooping
1	default	☑
221	IACS-1	☑
222	IACS-2	☑

Step 7 Configure static mrouter on all ports in the possible path to the IGMP queriers for every VLAN that has multicast traffic. This step is necessary to help prevent multicast loss if there is a querier change, e.g., the HSRP failover. This is CLI only configuration.

- In a star or linear topology, configure uplink ports to the aggregation or distribution IES as static mrouter ports.
- In a ring topology, configure both ports in the ring as static mrouter ports.
- The above recommendations assume that RedBox IEs with HSRP are configured with lowest IP addresses in the VLAN and take the querier role in the election process.

```
LAN-IES(config) ip igmp snooping vlan <VLAN ID> mrouter interface <PORT NAME>
```

Note CLI commands are executed in a terminal emulation software via a serial or USB console port or by using remote access methods such as Secure Shell (SSH). For more information on configuring switches using the CLI and its functionality, refer to the Cisco IOS Configuration Fundamentals Configuration Guide for the applicable IOS release version on the IES.

CLI Configuration Example

This is an example of the CLI commands for an infrastructure IES for steps 1-7 above. VLAN IDs and names are just examples. The CLI command syntax is specific to the test hardware and IOS version and may be different for your environment. Note that the other settings may also change depending on the switch platform, topology, resiliency protocol in the LAN, and other factors.

```
!
system mtu 1506
system mtu jumbo 1506
!
```

```
ptp mode e2etransparent
!
vlan 221
 name IACS-1
!
vlan 222
 name IACS-2
!
vlan 333
 name Native
!
interface GigabitEthernet1/1
 description To LAN IES
 switchport trunk native vlan 333
 switchport mode trunk
 <...>
!
interface GigabitEthernet1/2
 description To LAN IES
 switchport trunk native vlan 333
 switchport mode trunk
 <...>
!
interface GigabitEthernet1/3
 description To RedBox IES
 switchport trunk native vlan 333
 switchport mode trunk
 spanning-tree portfast edge trunk
 <...>
!
no ip igmp snooping querier
ip igmp snooping mrouter-ext-flood
ip igmp snooping vlan 221 mrouter interface Gi1/1
ip igmp snooping vlan 221 mrouter interface Gi1/2
ip igmp snooping vlan 222 mrouter interface Gi1/1
ip igmp snooping vlan 222 mrouter interface Gi1/2
```

RedBox IES Configuration—Access Layer

The next steps describe required or recommended settings for RedBox IES that are specific to the PRP operation. These steps apply to the access layer RedBox IES (Layer 2 switches). IP addresses, VLAN IDs, and port numbers are examples only.

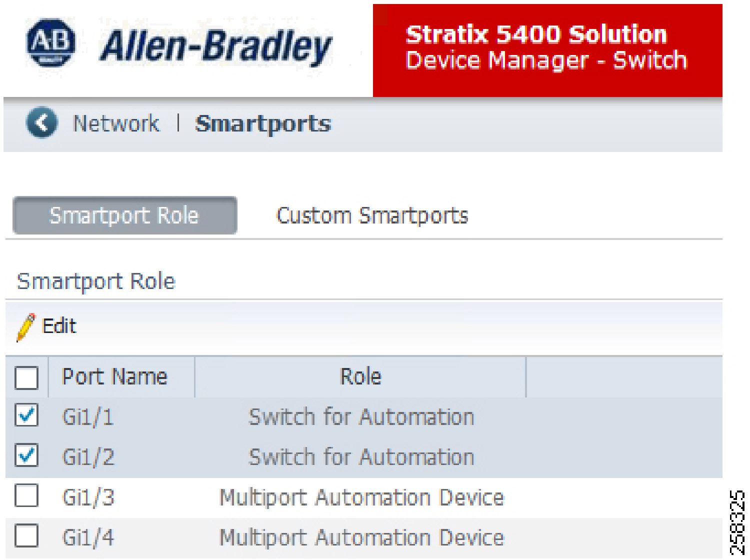
Parallel Redundancy Protocol Channel Configuration

Step 1 Configure ports that will be in the PRP channel for VLAN trunking using the Switch for Automation Smartport template. The applicable ports are shown in Table 3-1.

Table 3-1 PRP Channel Ports

Switch	PRP Channel Group	Member Ports
Stratix 5400	1	Gi1/1, Gi1/2
Stratix 5410	1	Gi1/17, Gi1/18
	2	Gi1/19, Gi1/20

Figure 3-5 Smartports for PRP Channel Ports

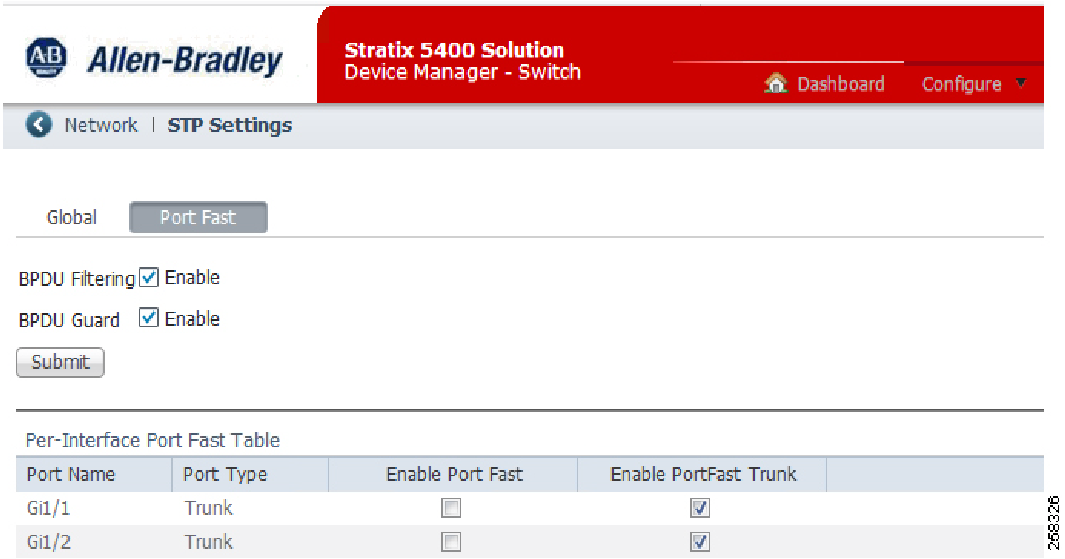


Smartport Role

☐	Port Name	Role
☑	Gi1/1	Switch for Automation
☑	Gi1/2	Switch for Automation
☐	Gi1/3	Multiport Automation Device
☐	Gi1/4	Multiport Automation Device

Step 2 Configure PortFast Trunk mode for ports that will be in the PRP channel.

Figure 3-6 PortFast Trunk



BPDU Filtering ☑ Enable

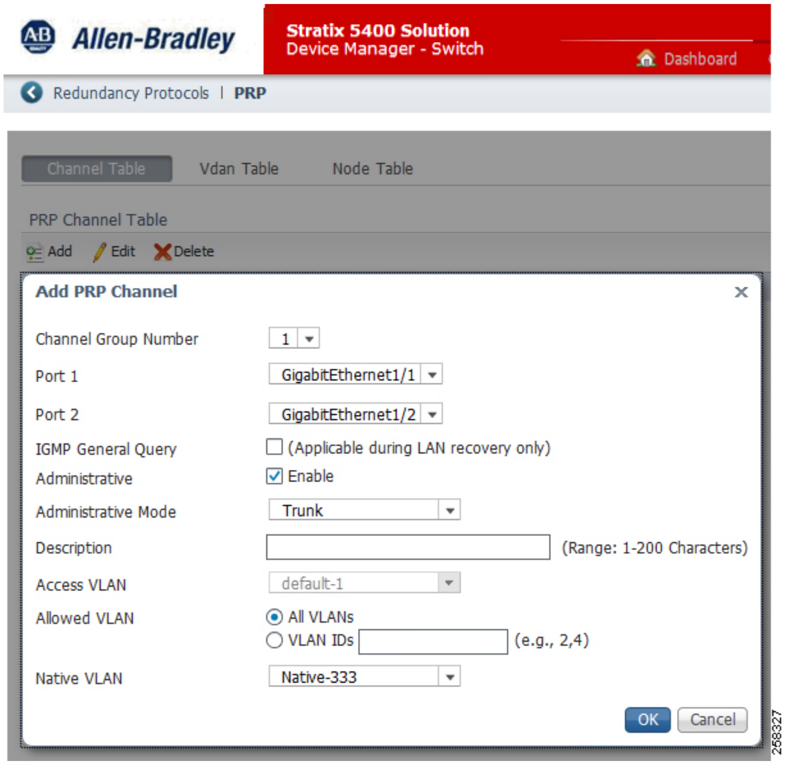
BPDU Guard ☑ Enable

Per-Interface Port Fast Table

Port Name	Port Type	Enable Port Fast	Enable PortFast Trunk
Gi1/1	Trunk	☐	☑
Gi1/2	Trunk	☐	☑

Step 3 Configure PRP Channel Group(s) in the trunk mode.

Figure 3-7 Adding PRP Channel



Add PRP Channel

Channel Group Number: 1

Port 1: GigabitEthernet1/1

Port 2: GigabitEthernet1/2

IGMP General Query: □ (Applicable during LAN recovery only)

Administrative: ☑ Enable

Administrative Mode: Trunk

Description: (Range: 1-200 Characters)

Access VLAN: default-1

Allowed VLAN: ● All VLANs ○ VLAN IDs (e.g., 2,4)

Native VLAN: Native-333

Note A RedBox IEs can also be connected to the infrastructure with PRP ports and the PRP channel in the access mode (single VLAN, smartport Multiport Automation Device). In this case, the management interface of the RedBox and all VDANs are assigned to the same VLAN and IP subnet.

Step 4 Configure PortFast Trunk mode for the PRP channel logical interface. This is CLI only configuration.

```
RedBox-IES(config) interface PRP-Channel1
RedBox-IES(config-if) spanning-tree portfast edge trunk
```

Step 5 If PRP-enabled ports are using fiber media, disable Unidirectional Link Detection (UDLD) on the ports. UDLD is not supported with PRP and will cause fiber ports to go to err-disable mode. This is CLI only configuration.

```
RedBox-IES(config) interface GigabitEthernet1/1
RedBox-IES(config-if) udld port disable

RedBox-IES(config) interface GigabitEthernet1/2
RedBox-IES(config-if) udld port disable
```

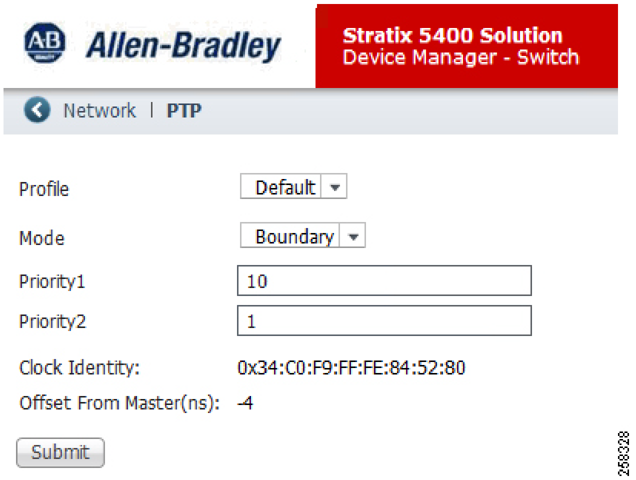
For more information on selection of copper versus fiber media, refer to Appendices C-F of the *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*:

- Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
- Cisco site:
http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/REP/CPwE_REP_DG.html

PTP (CIP Sync) Configuration

Step 6 If time synchronization is enabled in the network (CIP Sync), configure PTP Boundary mode on the access layer RedBox IES. Configure Priority1 value as 10 (lower than default) and Priority2 value as 1.

Figure 3-8 PTP Configuration for Boundary Mode

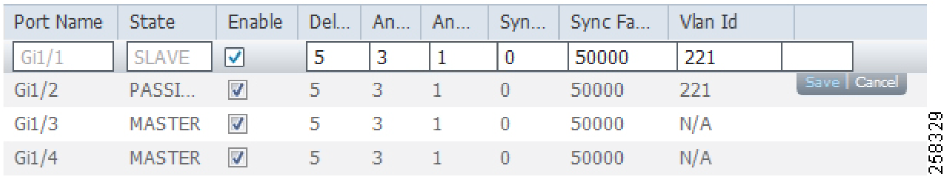


Profile: Default
Mode: Boundary
Priority1: 10
Priority2: 1
Clock Identity: 0x34:C0:F9:FF:FE:84:52:80
Offset From Master(ns): -4

Step 7 Verify that PTP is enabled on the PRP channel ports and on the ports with CIP Sync devices in the PTP VLAN. Disable PTP on the ports in other VLANs or on the ports that do not require CIP Sync operation.

Step 8 Configure PTP VLAN ID on the trunk ports, including the PRP channel ports if the trunk mode is used.

Figure 3-9 PTP Port Configuration



Port Name	State	Enable	Del...	An...	An...	Syn...	Sync Fa...	Vlan Id
Gi1/1	SLAVE	☑	5	3	1	0	50000	221
Gi1/2	PASSI...	☑	5	3	1	0	50000	221
Gi1/3	MASTER	☑	5	3	1	0	50000	N/A
Gi1/4	MASTER	☑	5	3	1	0	50000	N/A

Step 9 Configure the following settings to improve PTP performance and resiliency (CLI only):

```
RedBox-IES(config) ptp transfer feedforward
RedBox-IES(config) ptp time-property persist infinite
```

For more information on these settings and other considerations for plant-wide or site-wide time distribution refer to:

- Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td016_-en-p.pdf

CLI Configuration Example

This is an example of the CLI commands for an access layer RedBox IES for steps 1-9 above. The CLI command syntax is specific to the test hardware and IOS version and may be different for your environment.

```
!
```

```
ptp mode boundary
ptp priority1 10
ptp priority2 1
ptp time-property persist infinite
ptp transfer feedforward
!
vlan 221
 name IACS-1
!
vlan 222
 name IACS-2
!
vlan 333
 name Native
!
interface PRP-channel1
 switchport trunk native vlan 333
 switchport mode trunk
 spanning-tree portfast edge trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/1
 description PRP LAN A
 switchport trunk native vlan 333
 switchport mode trunk
 ptp sync limit 50000
 ptp vlan 221
 prp-channel-group 1
 spanning-tree portfast edge trunk
 <...>
!
interface GigabitEthernet1/2
 description PRP LAN B
 switchport trunk native vlan 333
 switchport mode trunk
 ptp sync limit 50000
 ptp vlan 221
 prp-channel-group 1
 spanning-tree portfast edge trunk
 <...>
!
interface GigabitEthernet1/3
 description To IACS device VLAN 221
 switchport access vlan 221
 switchport trunk native vlan 221
 switchport mode access
 <...>
!
interface GigabitEthernet1/4
 description To IACS device VLAN 222
 switchport access vlan 222
 switchport trunk native vlan 222
 switchport mode access
 <...>
```

RedBox IES Configuration—Distribution Layer

The next steps describe required or recommended settings for the distribution layer RedBox IES (Layer 3 switches with HSRP) in the CPwE PRP architecture. IP addresses, VLAN IDs, and port numbers are examples only.

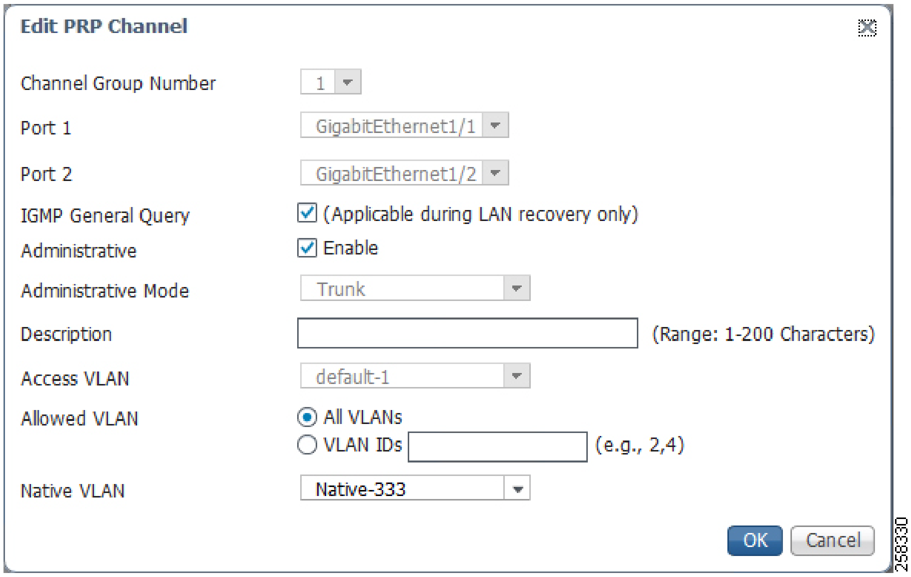
Parallel Redundancy Protocol Channel Configuration

Step 1 Configure ports that will be in the PRP channel for VLAN trunking using the Switch for Automation Smartport template.

Step 2 Configure PortFast Trunk mode for ports that will be in the PRP channel.

Step 3 Configure PRP Channel Group(s) in the trunk mode. Enable IGMP General Query option.

Figure 3-10 PRP Channel for Distribution RedBox



Edit PRP Channel

Channel Group Number: 1

Port 1: GigabitEthernet1/1

Port 2: GigabitEthernet1/2

IGMP General Query: ☑ (Applicable during LAN recovery only)

Administrative: ☑ Enable

Administrative Mode: Trunk

Description: (Range: 1-200 Characters)

Access VLAN: default-1

Allowed VLAN: ● All VLANs
○ VLAN IDs (e.g., 2,4)

Native VLAN: Native-333

Step 4 Configure PortFast Trunk mode for the PRP channel logical interface. This is CLI only configuration.

```
RedBox-IES(config) interface PRP-Channel1
RedBox-IES(config-if) spanning-tree portfast edge trunk
```

Step 5 If PRP-enabled ports are using fiber media, disable Unidirectional Link Detection (UDLD) on the ports. UDLD is not supported with PRP and will cause fiber ports to go to err-disable mode. This is CLI only configuration.

```
RedBox-IES(config) interface GigabitEthernet1/1
RedBox-IES(config-if) udld port disable

RedBox-IES(config) interface GigabitEthernet1/2
RedBox-IES(config-if) udld port disable
```

HSRP Configuration

Hot Standby Routing Protocol (HSRP) is enabled and configured on the Switch Virtual Interface (SVI) of each distribution switch for each VLAN in the PRP-enabled Cell/Area Zone. This section describes how to configure HSRP features to achieve optimum performance and fast convergence for routed traffic.

This is CLI only configuration.

Note HSRP feature is only available in the Layer 3 firmware type on Stratix 5400 switches (catalog numbers ending with -R) and Stratix 5410 switches (catalog numbers -RDC and -RAC).

- HSRP is enabled by configuring an instance, specified by an ID value, and the virtual IP that will be shared between the HSRP peers. The virtual IP will be used as the default gateway address for hosts in the PRP VLAN.
- The primary HSRP peer should be configured with the lower physical IP address so that it will win elections for protocols that do not rely on the virtual IP, such as IGMP. The secondary HSRP peer is typically assigned the next IP address in the subnet.
- The desired active peer should be configured with a higher HSRP priority so that it consistently wins the election.
- HSRP timers (hello and hold timers) should be decreased from default values to provide sub-second protocol convergence.
- HSRP preemption should be disabled. As a result, when the active HSRP RedBox IES reboots, it assumes the standby HSRP role, which minimizes routing convergence.
- The HSRP process should be delayed on startup to help prevent a new HSRP peer from assuming too quickly that it is the only peer in the network and taking on the active role.

Step 6 Configure each SVI on the primary HSRP switch. The following CLI configuration has been used for CPwE PRP testing:

```
interface Vlan221
 ip address 10.22.1.2 255.255.255.0
 standby delay minimum 30 reload 60
 standby version 2
 standby 1 ip 10.22.1.1
 standby 1 timers msec 200 msec 750
 standby 1 priority 150
!
interface Vlan222
 ip address 10.22.2.2 255.255.255.0
 standby delay minimum 30 reload 60
 standby version 2
 standby 2 ip 10.22.2.1
 standby 2 timers msec 200 msec 750
 standby 2 priority 150
```

Step 7 Configure each SVI on the secondary HSRP switch. The following CLI configuration has been used for CPwE PRP testing:

```
interface Vlan221
 ip address 10.22.1.3 255.255.255.0
 standby delay minimum 30 reload 60
 standby version 2
 standby 1 ip 10.22.1.1
 standby 1 timers msec 200 msec 750
!
interface Vlan222
 ip address 10.22.2.3 255.255.255.0
 standby delay minimum 30 reload 60
 standby version 2
 standby 2 ip 10.22.2.1
 standby 2 timers msec 200 msec 750
```

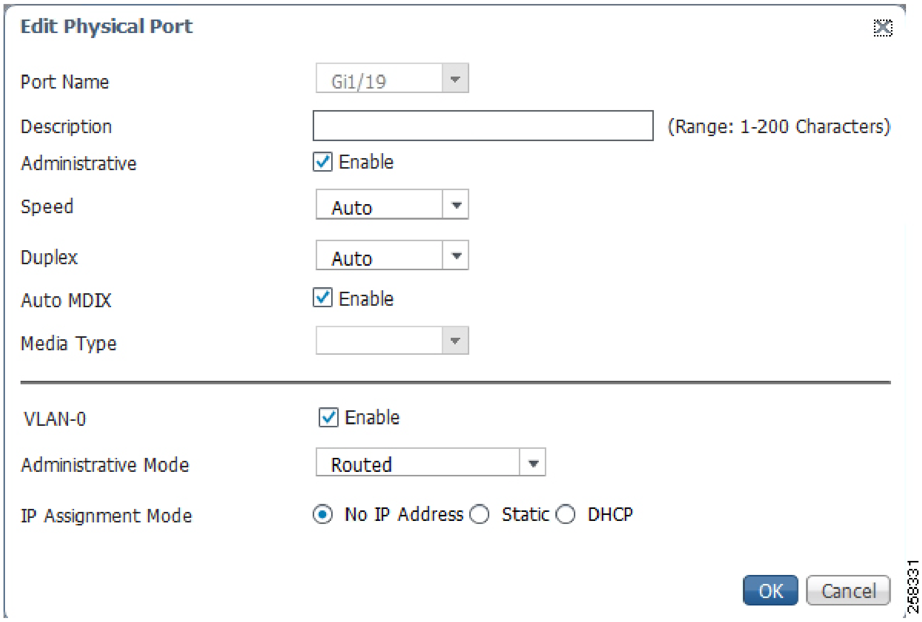
Layer 3 EtherChannel Configuration

For additional resiliency, distribution RedBox IES should be connected to the core switch infrastructure and to each other with Layer 3 (routed) EtherChannel links. Note that Layer 2 connections are not allowed between the RedBoxes except for the PRP channel ports.

Each distribution RedBox IES is configured with two Layer 3 EtherChannels: one for the uplink connection to the core switch, and another for a peer connection to the other distribution IES.

Step 8 Configure ports that will be part of the Layer 3 EtherChannel groups as routed ports (No IP Address).

Figure 3-11 Routed Port Configuration

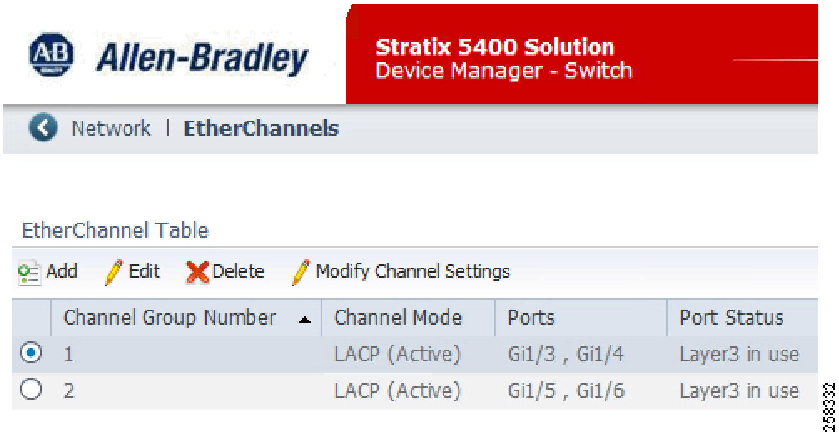


Edit Physical Port

Port Name	Gi1/19
Description	(Range: 1-200 Characters)
Administrative	☑ Enable
Speed	Auto
Duplex	Auto
Auto MDIX	☑ Enable
Media Type	
VLAN-0	☑ Enable
Administrative Mode	Routed
IP Assignment Mode	● No IP Address ○ Static ○ DHCP

Step 9 Configure two EtherChannel groups using previously configured routed ports. LACP Active mode is recommended. The channel mode should be compatible with the mode on the connected switch.

Figure 3-12 EtherChannel Configuration

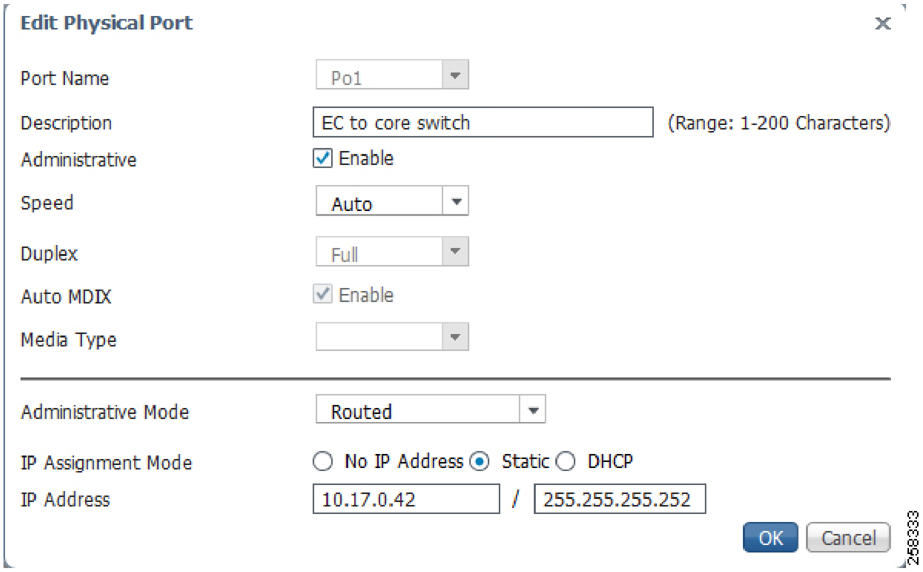


EtherChannel Table

	Channel Group Number	Channel Mode	Ports	Port Status
●	1	LACP (Active)	Gi1/3 , Gi1/4	Layer3 in use
○	2	LACP (Active)	Gi1/5 , Gi1/6	Layer3 in use

Step 10 Configure IP address for each routed EtherChannel port according to the IP scheme in the routed network.

Figure 3-13 Routed EtherChannel Configuration



Edit Physical Port ✕

Port Name: Po1
Description: EC to core switch (Range: 1-200 Characters)
Administrative: ☑ Enable
Speed: Auto
Duplex: Full
Auto MDIX: ☑ Enable
Media Type:

Administrative Mode: Routed
IP Assignment Mode: ○ No IP Address ● Static ○ DHCP
IP Address: 10.17.0.42 / 255.255.255.252

EIGRP Configuration

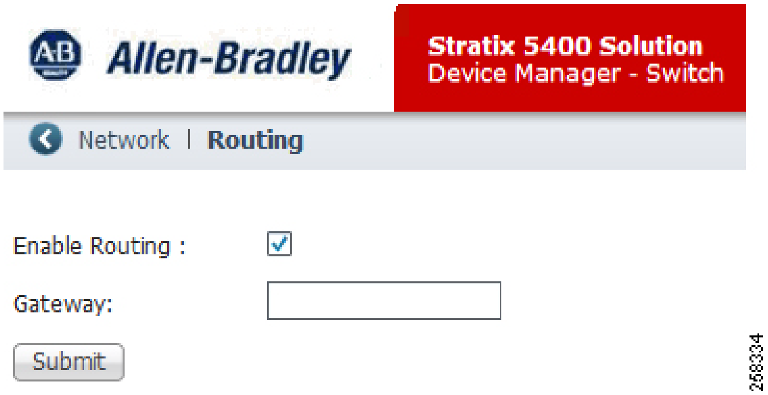
The following steps are provided only as an example of the EIGRP configuration that was used for the CPwE PRP testing. Note that routing protocol configuration can be very specific to the network environment and EIGRP parameters in your environment may be different.

Note Dynamic routing protocols like EIGRP are only available in the Layer 3 firmware type on Stratix 5400 switches (catalog numbers ending with -R) and Stratix 5410 switches (catalog numbers -RDC and -RAC).

The following steps apply to both distribution RedBox IES.

Step 11 Enable routing on the switch.

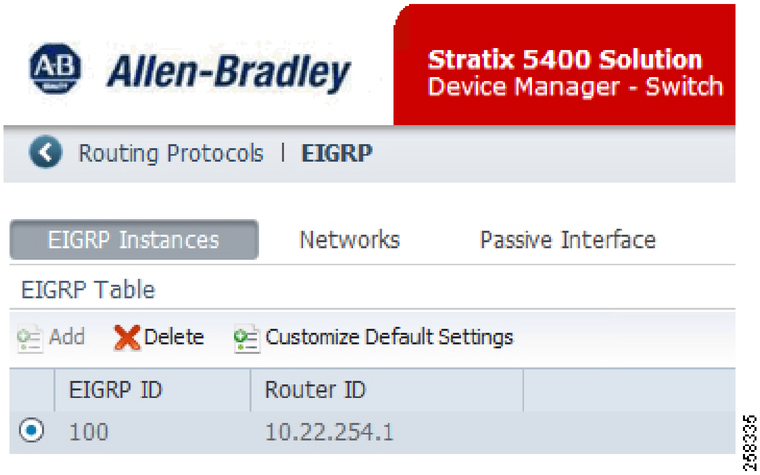
Figure 3-14 Enable Routing



Enable Routing : ☑
Gateway:

Step 12 Configure the EIGRP instance on the switch. In most cases, default settings are sufficient.

Figure 3-15 EIGRP Instance

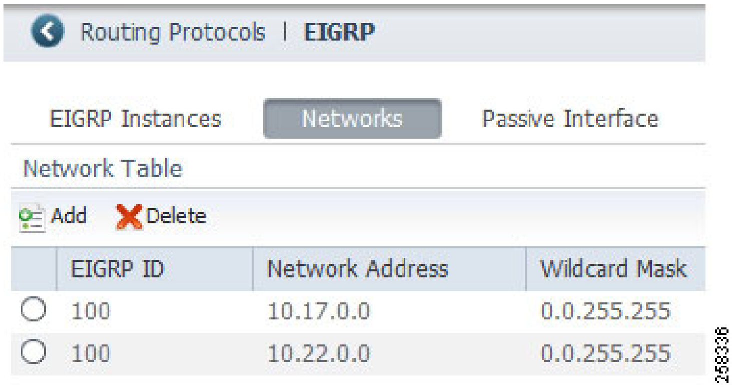


EIGRP Table

	EIGRP ID	Router ID
●	100	10.22.254.1

Step 13 Configure network addresses and wildcard masks for IP subnets that are associated with an EIGRP routing process. The network information should include IP subnets associated with the PRP VLANs.

Figure 3-16 EIGRP Networks

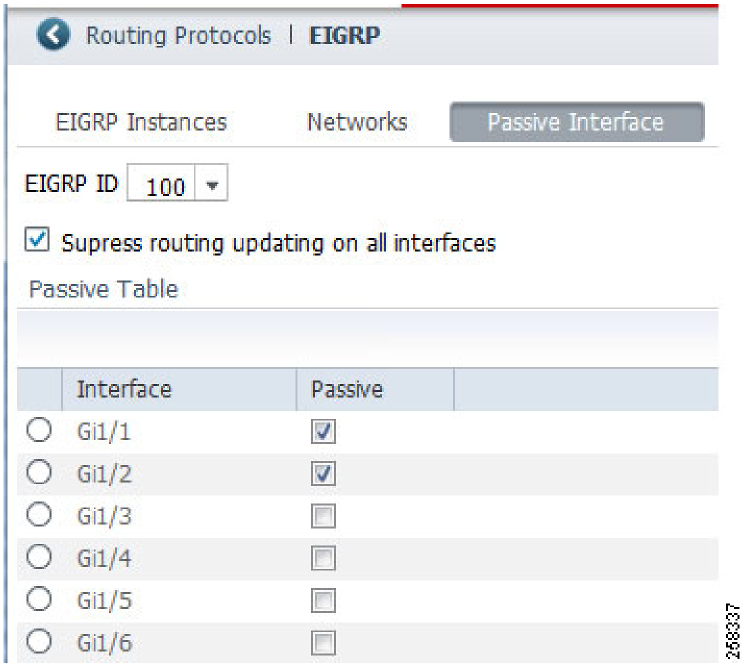


Network Table

	EIGRP ID	Network Address	Wildcard Mask
○	100	10.17.0.0	0.0.255.255
○	100	10.22.0.0	0.0.255.255

Step 14 As best practice, suppress routing updates (Passive mode) on all ports not participating in the EIGRP. In this example, passive mode is enabled on the PRP channel ports (Gi1/1 and Gi1/2).

Figure 3-17 EIGRP Passive Interfaces



EIGRP ID 100 ▾

☑ Supress routing updating on all interfaces

	Interface	Passive
○	Gi1/1	☑
○	Gi1/2	☑
○	Gi1/3	□
○	Gi1/4	□
○	Gi1/5	□
○	Gi1/6	□

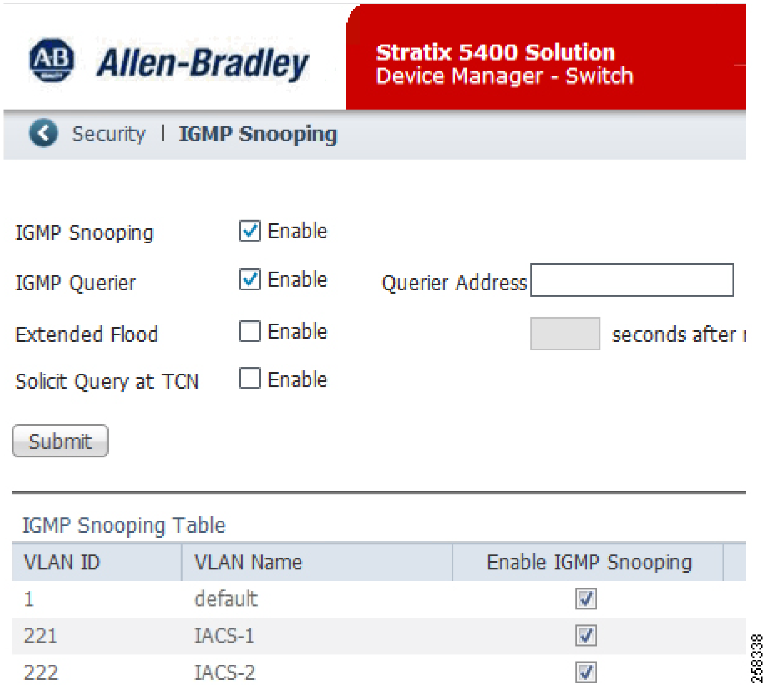
Step 15 If necessary, configure a static default route to the core switch or other static routes as required in your environment. Typically, the default route information is distributed from the core router to the distribution layer dynamically, in which case this step is not required.

IGMP Snooping Configuration

The following configuration steps are recommended for the distribution RedBox IES with the IGMP snooping querier role. In the CPwE PRP architecture, distribution IES (active and standby HSRP gateway) should be assigned the lowest IP addresses in each PRP VLAN to win the querier election.

Step 16 Enable IGMP Snooping for PRP VLANs where multicast traffic management is necessary. Enable IGMP Querier.

Figure 3-18 IGMP Snooping for Distribution RedBox



IGMP Snooping ☑ Enable

IGMP Querier ☑ Enable Querier Address

Extended Flood □ Enable seconds after ι

Solicit Query at TCN □ Enable

IGMP Snooping Table

VLAN ID	VLAN Name	Enable IGMP Snooping
1	default	☑
221	IACS-1	☑
222	IACS-2	☑

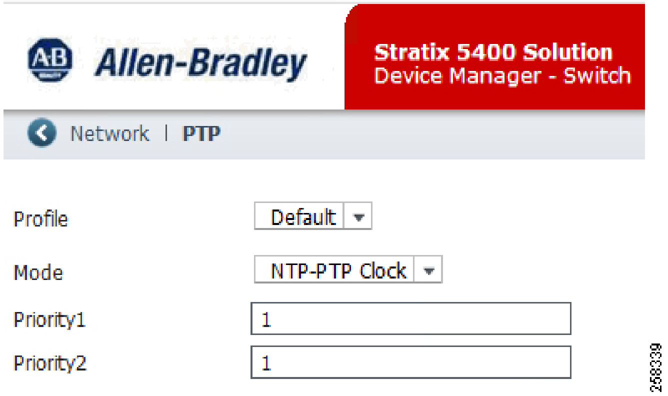
PTP (CIP Sync) Configuration

For information on how to configure RedBox IES in the boundary clock mode, see steps 6-9 in the previous section for the access layer RedBox IES.

The following steps are necessary only if the distribution RedBox IES are primary and backup Grandmaster clocks (NTP/PTP mode) for the PTP-enabled VLAN in the network. In this case, switches use NTP time source in the plant-wide or site-wide network to distribute time in the PTP-enabled VLAN.

Step 17 Configure the distribution IES with the active HSRP gateway role in the NTP-PTP Clock mode with Priority1 value 1 and Priority2 value 1 (primary Grandmaster).

Figure 3-19 NTP-PTP Mode for Primary Grandmaster



Profile Default

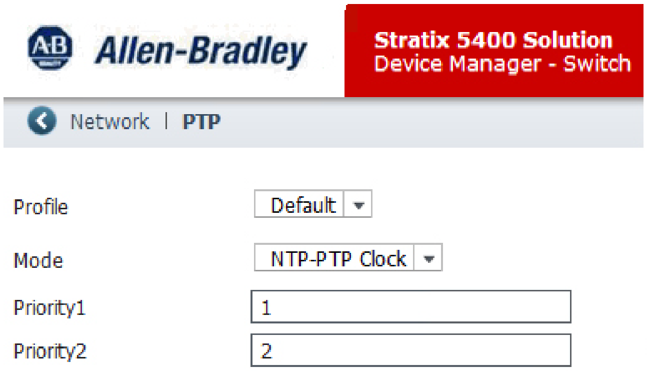
Mode NTP-PTP Clock

Priority1 1

Priority2 1

Step 18 Configure the distribution IES with the standby HSRP gateway role in the NTP-PTP Clock mode with Priority1 value 1 and Priority2 value 2 (secondary Grandmaster).

Figure 3-20 NTP-PTP Mode for Secondary Grandmaster



Profile Default

Mode NTP-PTP Clock

Priority1 1

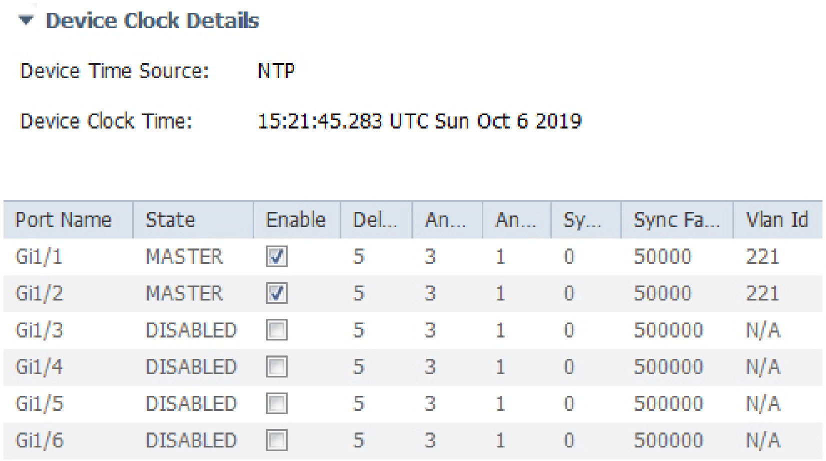
Priority2 2

258340

Step 19 For both distribution IES, verify that PTP is enabled on the PRP channel ports and configure PTP VLAN ID.

Step 20 Disable PTP on the Layer 3 EtherChannel ports.

Figure 3-21 PTP Port Configuration on Distribution IES



Device Time Source: NTP

Device Clock Time: 15:21:45.283 UTC Sun Oct 6 2019

Port Name	State	Enable	Del...	An...	An...	Sy...	Sync Fa...	Vlan Id
Gi1/1	MASTER	☑	5	3	1	0	50000	221
Gi1/2	MASTER	☑	5	3	1	0	50000	221
Gi1/3	DISABLED	□	5	3	1	0	500000	N/A
Gi1/4	DISABLED	□	5	3	1	0	500000	N/A
Gi1/5	DISABLED	□	5	3	1	0	500000	N/A
Gi1/6	DISABLED	□	5	3	1	0	500000	N/A

258341

CLI Configuration Example

This is an example of the CLI commands for the primary distribution RedBox IES for steps 1-20 above.

- Configuration for the secondary distribution IES is similar except for IP addresses and HSRP priority values.
- PTP configuration is given for the NTP-PTP clock mode on the distribution switch. It does not apply when the Grandmaster clock is in the Cell/Area Zone (not on the distribution switches).

The CLI command syntax is specific to the test hardware and IOS version and may be different for your environment.

```
ip routing
!
ip igmp snooping querier
prp channel-group 1 igmpquerier sendGQOnLANRecovery
!
ptp mode gmc-bc
ptp priority1 1
ptp priority2 1
!
vlan 221
 name IACS-1
!
vlan 222
 name IACS-2
!
vlan 333
 name Native
!
interface Port-channel1
 description EC to core switch
 no switchport
 ip address 10.17.0.42 255.255.255.252
!
interface Port-channel2
 description EC to HSRP peer
 no switchport
 ip address 10.22.254.1 255.255.255.252
!
interface PRP-channel1
 switchport trunk native vlan 333
 switchport mode trunk
 spanning-tree portfast edge trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/1
 description PRP LAN A
 switchport trunk native vlan 333
 switchport mode trunk
 udld port disable
 ptp sync limit 50000
 ptp vlan 221
 prp-channel-group 1
 spanning-tree portfast edge trunk
 <...>
!
interface GigabitEthernet1/2
 description PRP LAN B
 switchport trunk native vlan 333
 switchport mode trunk
 udld port disable
 ptp sync limit 50000
 ptp vlan 221
 prp-channel-group 1
 spanning-tree portfast edge trunk
 <...>
!
interface GigabitEthernet1/3
 description Uplink to core 1
 no switchport
 no ip address
 no ptp enable
 channel-group 1 mode active
 <...>
!
interface GigabitEthernet1/4
 description Uplink to core 2
 no switchport
 no ip address
 no ptp enable
 channel-group 1 mode active
 <...>
!
interface GigabitEthernet1/5
 description Peer link 1
 no switchport
 no ip address
 no ptp enable
 channel-group 2 mode active
 <...>
!
interface GigabitEthernet1/6
 description Peer link 2
 no switchport
 no ip address
 no ptp enable
 channel-group 2 mode active
 <...>
!
interface Vlan221
 ip address 10.22.1.2 255.255.255.0
 standby delay minimum 30 reload 60
 standby version 2
 standby 1 ip 10.22.1.1
 standby 1 timers msec 200 msec 750
 standby 1 priority 150
!
interface Vlan222
 ip address 10.22.2.2 255.255.255.0
 standby delay minimum 30 reload 60
 standby version 2
 standby 2 ip 10.22.2.1
 standby 2 timers msec 200 msec 750
 standby 2 priority 150
!
router eigrp 100
 network 10.17.0.0 0.0.255.255
 network 10.22.0.0 0.0.255.255
 passive-interface default
 no passive-interface GigabitEthernet1/3
 no passive-interface GigabitEthernet1/4
 no passive-interface GigabitEthernet1/5
 no passive-interface GigabitEthernet1/6
 no passive-interface Port-channel1
 no passive-interface Port-channel2
```

IACS Configuration

PRP-capable IACS devices do not require configuration of any PRP parameters. Certain DANs may require enabling PRP mode explicitly, for example if the device is capable of switching between PRP and DLR modes of operation. Refer to device user manual for details.

- To enable devices to communicate with each other across a PRP network, DAN, VDAN, and SAN IP addresses must be unique within the same subnet. In the CPwE PRP converged architecture with multiple VLAN and routing, unique address requirements apply to any device across the Cell/Area Zone.
- Static IP address assignment is recommended for DANs and SANs.
- Dynamic Host Configuration Protocol (DHCP) and DHCP Persistence per port on IES for DANs and SANs are outside of scope for this CPwE PRP release.

- DHCP Persistence per port feature is supported for VDANs connected to a Layer 2 RedBox IES.

CHAPTER 4

CPwE Parallel Redundancy Protocol Monitoring and Troubleshooting

This chapter describes management tools and diagnostic information available to monitor and troubleshoot PRP status and operation, including DANs, VDANs, and RedBox IES.

PRP information can be obtained using Stratix IES Device Manager, Cisco CLI commands, Studio 5000 Logix Designer Add-on Profiles (AOP), CIP message diagnostic and IACS device webpages.

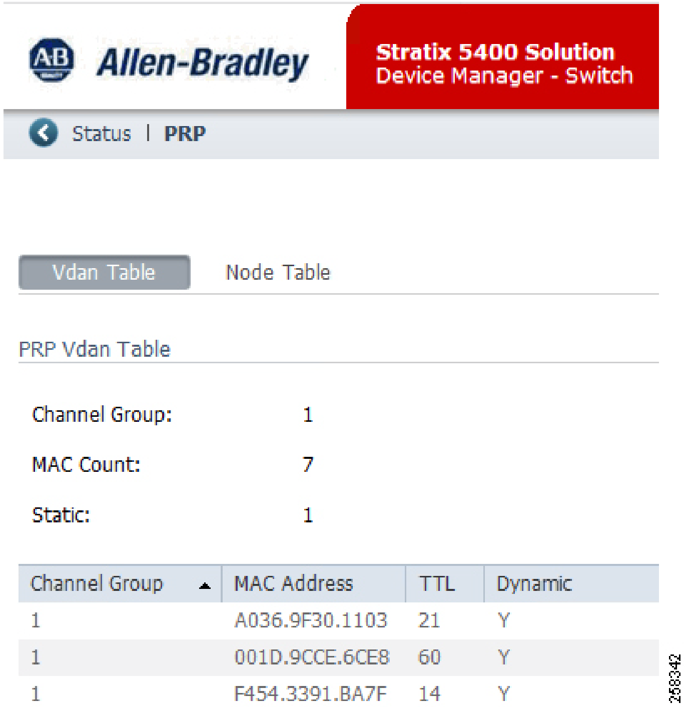
RedBox IES

This section provides PRP information available from a RedBox IES via Device Manager webpage or CLI commands.

Device Manager

Stratix RedBox IES provides information about connected VDANs on the Device Manager **Monitor->Status ->PRP** page. The VDAN MAC addresses are learned automatically from the switch MAC table. The RedBox IES sends PRP supervisory frames for each VDAN via the PRP channel ports.

Figure 4-1 VDAN Table



PRP Vdan Table

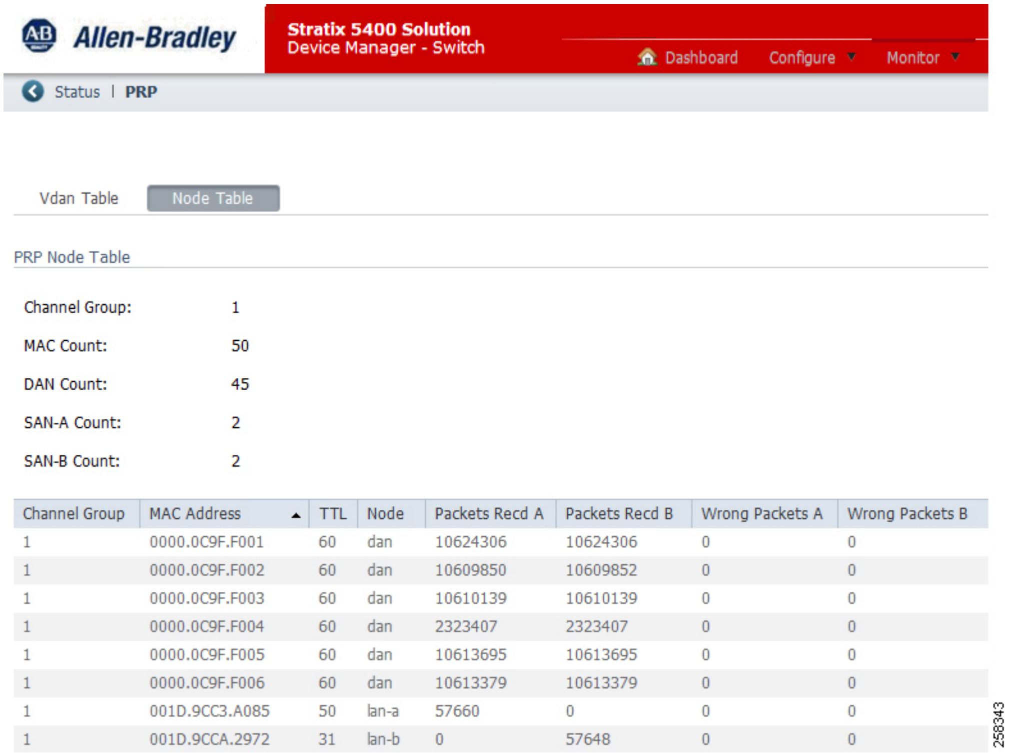
Channel Group:	1
MAC Count:	7
Static:	1

Channel Group	MAC Address	TTL	Dynamic
1	A036.9F30.1103	21	Y
1	001D.9CCE.6CE8	60	Y
1	F454.3391.BA7F	14	Y

RedBox IES learns about DANs and SANs in the network from the supervisory frames received on the PRP channel ports. These frames are propagated within a VLAN as special Layer 2 multicast frames.

The DAN and SAN information can be viewed on the **Monitor->Status->PRP** page.

Figure 4-2 Node Table



PRP Node Table

Channel Group:	1
MAC Count:	50
DAN Count:	45
SAN-A Count:	2
SAN-B Count:	2

Channel Group	MAC Address	TTL	Node	Packets Recd A	Packets Recd B	Wrong Packets A	Wrong Packets B
1	0000.0C9F.F001	60	dan	10624306	10624306	0	0
1	0000.0C9F.F002	60	dan	10609850	10609852	0	0
1	0000.0C9F.F003	60	dan	10610139	10610139	0	0
1	0000.0C9F.F004	60	dan	2323407	2323407	0	0
1	0000.0C9F.F005	60	dan	10613695	10613695	0	0
1	0000.0C9F.F006	60	dan	10613379	10613379	0	0
1	001D.9CC3.A085	50	lan-a	57660	0	0	0
1	001D.9CCA.2972	31	lan-b	0	57648	0	0

- Time To Live (TTL) value shows the number of seconds since the last received frame. Node entries age out and are removed from the tables after 60 seconds.
- The switch supports a maximum of 512 SAN and DAN entries in the Node table. If the Node table is full, the switch treats new nodes as a DAN by default.
- The switch supports a maximum of 512 VDAN entries in the VDAN table. If the VDAN table is full, the switch cannot send supervisory frames for new VDANs.
- In a multi-VLAN network with PRP channel ports in the trunk mode, the RedBox IES receives supervisory frames and displays information about nodes in all VLANs enabled on the trunk
- The number of DAN packets received from LAN A and LAN B should be the same or very close in a normally functioning network. The increasing difference may be due to dropping packets in one of the LANs and may require further troubleshooting.
- There should be no Wrong Packets entries. If any exist and are increasing, this indicates incorrect cabling of a DAN or a RedBox.

Note DANs, SANs, and VDANs can be manually added to and deleted from the corresponding tables on the **Configure->PRP** page. Normally dynamic learning should be sufficient. Static configuration may be needed only if PRP devices do not support supervisory frames.

Command Line Interface

CLI diagnostics commands for PRP provide more detailed information for troubleshooting.

- **show prp statistics egress** command shows detailed packet counts and byte counts for transmitted frames over the PRP channel.

```
PRP-IES-RB1#show prp statistics egressPacketStatistics

 PRP channel-group 1 EGRESS STATS:
   duplicate packet: 2308893385
   supervision frame sent: 7883182
   packet sent on lan a: 2308893377
   packet sent on lan b: 2308890642
   byte sent on lan a: 389844980047
   byte sent on lan b: 389924896911
   egress packet receive from switch: 2309098088
   overrun pkt: 0
   overrun pkt drop: 0
```

- **show prp statistics ingress** command shows detailed packet counts and byte counts for different types of frames received on the PRP channel.

```
PRP-IES-RB1#show prp statistics ingressPacketStatistics

 PRP channel-group 1 INGRESS STATS:
   ingress pkt lan a: 2503748276
   ingress pkt lan b: 2503792103
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 2449954701
   ingress danp pkt dscrd: 2449759968
   ingress supfrm rcv a: 53914548
   ingress supfrm rcv b: 53914032
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
   ingress oversize pkt a: 0
   ingress oversize pkt b: 0
   ingress byte lan a: 530416337651
   ingress byte lan b: 530510451733
   ingress wrong lan id a: 0
   ingress wrong lan id b: 0
   ingress warning lan a: 0
   ingress warning lan b: 0
   ingress warning count lan a: 1
   ingress warning count lan b: 0
   ingress unique count a: 105123619610672
   ingress unique count b: 377957242996
   ingress duplicate count a: 2449759973
   ingress duplicate count b: 2449759973
   ingress multiple count a: 0
   ingress multiple count b: 0
```

- Ingress Warning status indicates following conditions for LAN A or LAN B:
  - Loss of communication for three seconds on one LAN, but not the other. This condition applies to traffic from all nodes. The condition is cleared once communication is restored for three seconds.
  - Node status is active on one LAN but not the other. This means that no packets were received from one of the PRP nodes in the switch table (DANs or VDANs) on one of the LANs for three seconds. The condition is cleared once packets are received again within three seconds.
  - Packets from a wrong LAN were received on one of the ports in the past second. The condition is cleared once no wrong packets are received for one second.
  - Warning counts and wrong LAN counts show total number of faults since the last reset of counters.

```
PRP-IES-RB1#show prp statistics ingressPacketStatistics
<…>
ingress wrong lan id a: 12
ingress wrong lan id b: 2
ingress warning lan a: 0
ingress warning lan b: 0
ingress warning count lan a: 8
ingress warning count lan b: 3
<…>
```

- **show prp statistics ptp** command displays PTP traffic counters for the PRP channel (which is sent and received independently on each port, bypassing PRP duplication mechanism).

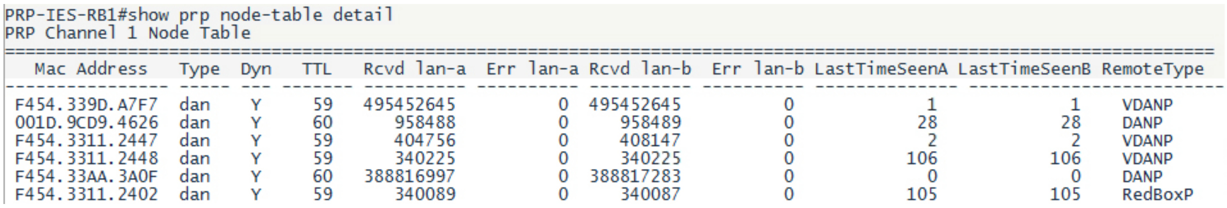
```
PRP-IES-RB1#show prp statistics ptpPacketStatistics
 PRP channel-group 1 PTP STATS:
   ingress lan a: 13665146
   ingress drop lan a: 0
   ingress lan b: 14556100
   ingress drop_lan b: 0
   egress lan a: 107395
   egress lan b: 996227
```

- **clear prp statistics** command resets all PRP counters and could be useful when troubleshooting an ongoing problem with PRP communication.

```
PRP-IES-RB1#clear prp statistics
```

- **show prp node-table statistics** command provide warning status and received count per LAN for each PRP node learned by the RedBox, including DANs, SANs, remote VDANs, and other RedBoxes.

Figure 4-3 Node Table Statistics



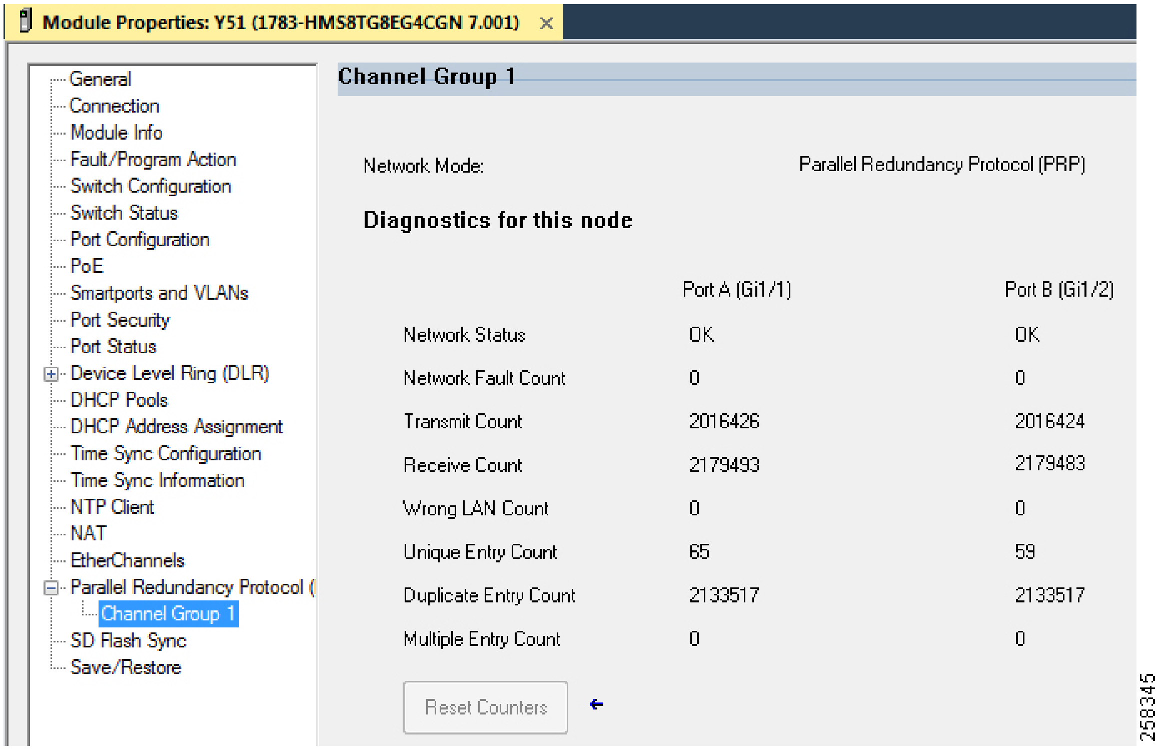
```
PRP-IES-RB1#show prp node-table detail
PRP Channel 1 Node Table
==========================================================================================================================
  Mac Address    Type  Dyn   TTL    Rcvd lan-a  Err lan-a Rcvd lan-b  Err lan-b LastTimeSeenA LastTimeSeenB RemoteType
---------------- ----- --- ------- ---------- ---------- ---------- ---------- ------------- -------------------------
 F454.339D.A7F7  dan    Y     59   495452645          0  495452645          0             1             1    VDANP
 001D.9CD9.4626  dan    Y     60      958488          0     958489          0            28            28    DANP
 F454.3311.2447  dan    Y     59      404756          0     408147          0             2             2    VDANP
 F454.3311.2448  dan    Y     59      340225          0     340225          0           106           106    VDANP
 F454.33AA.3A0F  dan    Y     60   388816997          0  388817283          0             0             0    DANP
 F454.3311.2402  dan    Y     59      340089          0     340087          0           105           105    RedBoxP
```

Studio 5000 Logix Designer

Studio 5000 Logix Designer Add-on Profile provides PRP diagnostics, counters, and node information for PRP-enabled devices in the controller I/O tree.

The AOP for a Stratix RedBox IES displays PRP warning status and total counters for the PRP channel. This information is available in the AOP for Stratix IOS version 15.2(6)E2a or later.

Figure 4-4 Stratix AOP



Channel Group 1

Network Mode: Parallel Redundancy Protocol (PRP)

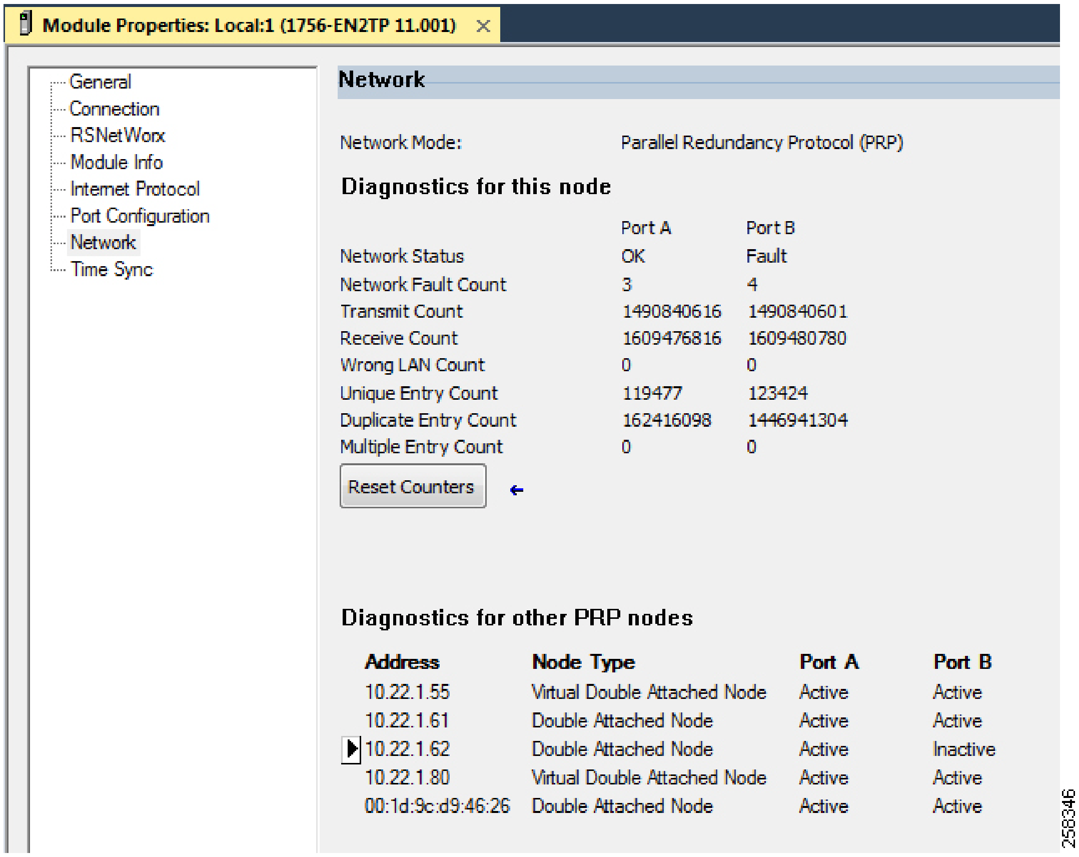
Diagnostics for this node

	Port A (Gi1/1)	Port B (Gi1/2)
Network Status	OK	OK
Network Fault Count	0	0
Transmit Count	2016426	2016424
Receive Count	2179493	2179483
Wrong LAN Count	0	0
Unique Entry Count	65	59
Duplicate Entry Count	2133517	2133517
Multiple Entry Count	0	0

The AOP for a PRP EtherNet/IP module displays the PRP network status, total counters, and the node table with node status. IP addresses are displayed for PRP nodes in the I/O tree, otherwise only MAC addresses are shown.

Below is an example of the PRP status page for the 1756-EN2TP module.

Figure 4-5 EN2TP Module AOP



Network

Network Mode: Parallel Redundancy Protocol (PRP)

Diagnostics for this node

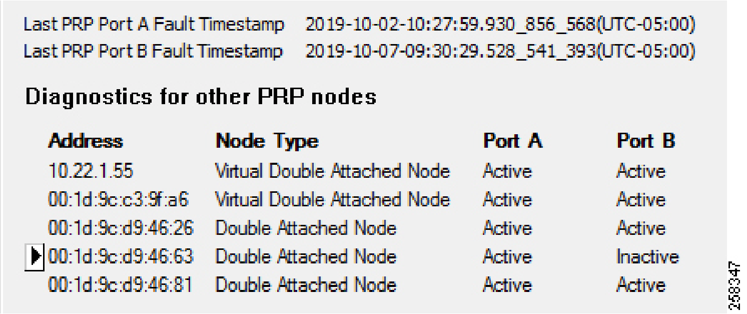
	Port A	Port B
Network Status	OK	Fault
Network Fault Count	3	4
Transmit Count	1490840616	1490840601
Receive Count	1609476816	1609480780
Wrong LAN Count	0	0
Unique Entry Count	119477	123424
Duplicate Entry Count	162416098	1446941304
Multiple Entry Count	0	0

Diagnostics for other PRP nodes

Address	Node Type	Port A	Port B
10.22.1.55	Virtual Double Attached Node	Active	Active
10.22.1.61	Double Attached Node	Active	Active
10.22.1.62	Double Attached Node	Active	Inactive
10.22.1.80	Virtual Double Attached Node	Active	Active
00:1d:9c:d9:46:26	Double Attached Node	Active	Active

The AOP for the FLEX 5000^{TM} EtherNet/IP adapter also includes a last PRP fault time stamp data (connection type “Status with PRP”).

Figure 4-6 Flex 5000 Module AOP



Last PRP Port A Fault Timestamp 2019-10-02-10:27:59.930_856_568(UTC-05:00)
Last PRP Port B Fault Timestamp 2019-10-07-09:30:29.528_541_393(UTC-05:00)

Diagnostics for other PRP nodes

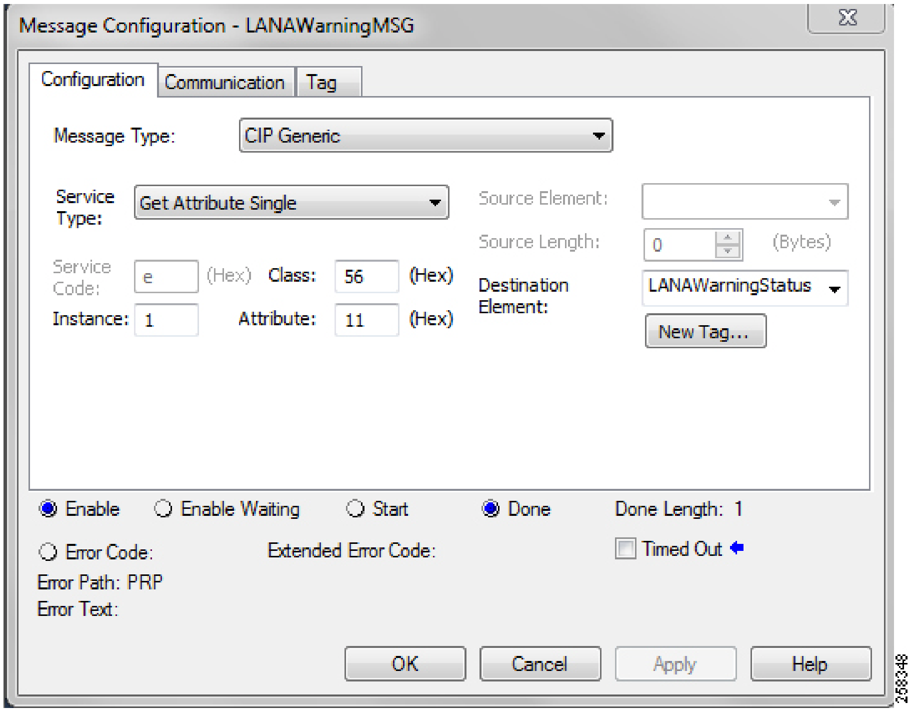
Address	Node Type	Port A	Port B
10.22.1.55	Virtual Double Attached Node	Active	Active
00:1d:9c:c3:9f:a6	Virtual Double Attached Node	Active	Active
00:1d:9c:d9:46:26	Double Attached Node	Active	Active
00:1d:9c:d9:46:63	Double Attached Node	Active	Inactive
00:1d:9c:d9:46:81	Double Attached Node	Active	Active

The PRP warning status for a PRP EtherNet/IP module or a RedBox can be obtained by the controller program by sending a CIP message to the device. Parameters for the message instruction are shown in Table 4-1.

Table 4-1 CIP Message Parameters for PRP Status

Field	Parameter
Message Type	CIP Generic
Service Type	Get Attribute Single
Class	56 (Hex)
Instance	1
Attribute	11 (Hex) for LAN A
12 (Hex) for LAN B	
Data Type	DINT

Figure 4-7 CIP Message


Message Configuration - LANAWarningMSG

Message Type: CIP Generic

Service Type: Get Attribute Single

Service Code: e (Hex)

Class: 56 (Hex)

Instance: 1

Attribute: 11 (Hex)

Source Element:

Source Length: 0 (Bytes)

Destination Element: LANAWarningStatus

● Enable ○ Enable Waiting ○ Start ● Done Done Length: 1

○ Error Code: Extended Error Code: □ Timed Out

Error Path: PRP

Error Text:

Note PRP-enabled EtherNet/IP modules also provide PRP diagnostics via webpages, similar to data available in the AOP. Depending on the platform and the firmware version, web access to the module may need to be enabled explicitly.

APPENDIX A

References

This appendix includes the following major topics:

- Converged Plantwide Ethernet (CPwE), page A-1
- Other References, page A-3

Converged Plantwide Ethernet (CPwE)

- Design Zone for Manufacturing-Converged Plantwide Ethernet: http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Industrial Network Architectures-Converged Plantwide Ethernet: http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page
- *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide*:
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html
- *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*:
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/REP/CPwE_REP_DG.html
- *Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide*:
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.ht ml
- *Cloud Connectivity to a Converged Plantwide Ethernet Architecture*:

- Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td017_-en-p.pdf
- Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Cloud/DIG/CPwE_Cloud_Connect_CVD.html

- *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide*:
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html
- *Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide*:
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html
- *Deploying Network Security within a Converged Plantwide Ethernet Architecture*
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG.html
- *Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture*
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td015_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/DLR/DIG/CPwE-5-1-DLR-DIG.html
- *Deploying Industrial Data Center within a Converged Plantwide Ethernet Architecture*
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td014_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/IDC/DIG/CPwE-5-1-IDC-DIG.html
- *OEM Networking within a Converged Plantwide Ethernet Architecture*
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td018_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/OEM/DIG/CPwE-5-1-OEM-CRD.html
- *Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture*

- Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td016_-en-p.pdf
- Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/STD/DIG/CPwE-5-1-STD-DIG.html

Other References

- *Stratix Managed Switches User Manual*
  - http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf
- *EtherNet/IP Parallel Redundancy Protocol Application Technique*
  - https://literature.rockwellautomation.com/idc/groups/literature/documents/at/enet-at006_-en-p.pdf

APPENDIX B

Test Hardware and Software

The network hardware devices used in CPwE PRP testing are listed in Table B-1. Rockwell Automation hardware and firmware versions are listed in Table B-2. Rockwell Automation software versions are listed in Table B-3.

.

Table B-1 Network Hardware and Firmware

Role	Product	Firmware Version
Core switch	Cisco Catalyst 4500X	3.7.2E
Distribution switch, Layer 3 RedBox	Allen-Bradley Stratix 5400, Layer 3 firmware	15.2(7)E
IES access switch, Layer 2 RedBox	Allen-Bradley Stratix 5400	15.2(7)E
IES access switch, LAN A/B	Allen-Bradley Stratix 5400	15.2(7)E
IES access switch, LAN A/B	Allen-Bradley Stratix 5700	15.2(7)E
IES access switch, LAN A/B	Allen-Bradley Stratix 5800	16.12.01

.

Table B-2 IACS Hardware and Firmware

Role	Product	Catalog Number	Firmware Version
PAC	ControlLogix 5570	1756-L75	31.011
Redundant PAC	ControlLogix 5570	1756-L75	31.052
PAC, VDAN	ControlLogix 5580	1756-L85E	31.011
Safety PAC	GuardLogix® 5570	1756-L73S 1756-L7SP	31.011
Ethernet module, DAN (PAC)	ControlLogix EtherNet/IP module, PRP	1756-EN2TP	11.001
Ethernet module, DAN (I/O)	ControlLogix EtherNet/IP module, PRP	1756-EN2TP	11.001
Ethernet module, DAN (I/O)	Flex 5000 EtherNet/IP Adapter	5094-AEN2TR/A	4.011
Ethernet module, VDAN (I/O)	POINT I/O™ EtherNet/IP Adapter	1734-AENTR/B	5.016
Ethernet module, VDAN (I/O)	Compact 5000™ I/O EtherNet/IP Adapter	5069-AEN2TR	3.011

.

Table B-3 Rockwell Automation Software

Product	Version
FactoryTalk Service Platform	6.11.00 (CPR 9 SR 11)
FactoryTalk View Site Edition	11.00.00 (CPR 9 SR 11)
FactoryTalk Linx	6.11.00 (CPR 9 SR 11)
FactoryTalk Live Data Test Client	6.110.00

APPENDIX C

Acronyms

Table C-1 lists the acronyms and initialisms commonly used in CPwE documentation.

Table C-1 Acronyms and Initialisms

Term	Description
1:1	One-to-One
AAA	Authentication, Authorization, and Accounting
AD	Microsoft® Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
ACL	Access Control List
AH	Authentication Header
AIA	Authority Information Access
AMP	Advanced Malware Protection
ASDM	Cisco Adaptive Security Device Manager
ASIC	Application Specific Integrated Circuit
ASR	Cisco Aggregation Services Router
BYOD	Bring Your Own Device
CA	Certificate Authority
CDP	CRL Distribution Points
CIP	ODVA, Inc. Common Industrial Protocol
CLI	Command Line Interface
CoA	Change of Authorization
CoS	Class of Service
CPwE	Converged Plantwide Ethernet
CRD	Cisco Reference Design
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSSM	Cisco Smart Software Manager
CTL	Certificate Trust List
CUR	Coarse Update Rate
CVD	Cisco Validated Design

Table C-1 Acronyms and Initialisms (continued)

Term	Description
DACL	Downloadable Access Control List
DAN	Double Attached Node
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DIG	Design and Implementation Guide
DLR	Device Level Ring
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name System
DPI	Deep Packet Inspection
DSRM	Directory Services Restoration Mode
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Enterprise Manufacturing Intelligence
EoIP	Ethernet over IP
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Protocol
ESR	Embedded Services Router
FIB	Forwarding Information Base
FIFO	First-In First-Out
FPGA	Field-Programmable Gate Array
FQDN	Fully Qualified Domain Name
FVRF	Front-door Virtual Route Forwarding
GNSS	Global Navigation Satellite Systems
GRE	Generic Routing Encapsulation
HMAC	Hash Message Authentication Code
HMI	Human-Machine Interface
HSRP	Hot Standby Router Protocol
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zones
IES	Industrial Ethernet Switch (Allen-Bradley Stratix, Cisco IE)
IGMP	Internet Group Management Protocol
IIoT	Industrial Internet of Things
IKE	Internet Key Exchange
I/O	Input/Output
IoT	Internet of Things
IP	Internet Protocol
IPDT	IP Device Tracking
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ISE	Cisco Identity Services Engine
ISR	Integrated Service Router
IT	Information Technology

Table C-1 Acronyms and Initialisms (continued)

Term	Description
LBS	Location Based Services
LWAP	Lightweight Access Point
MAB	MAC Authentication Bypass
MAC	Media Access Control
MDM	Mobile Device Management
ME	FactoryTalk View Machine Edition
mGRE	Multipoint Generic Routing Encapsulation
MLS	Multilayer Switching QoS
MMC	Microsoft Management Console
MnT	Monitoring Node
MPLS	Multiprotocol Label Switching
MQC	Modular QoS CLI
MSE	Mobile Service Engine
MSS	Maximum Segment Size
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDES	Network Device Enrollment Service
NHRP	Next Hop Routing Protocol
NOC	Network Operation Center
NPS	Microsoft Network Policy Server
NSP	Native Supplicant Profile
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OEE	Overall Equipment Effectiveness
OEM	Original Equipment Manufacturer
OT	Operational Technology
OTA	Over-the-Air
OU	Organizational Unit
PAC	Programmable Automation Controller
PAN	Policy Administration Node
PAT	Port Address Translation
PCS	Process Control System
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
pps	Packet per second
PRP	Parallel Redundancy Protocol
PSK	Pre-Shared Key
PSN	Policy Service Node
PTP	Precision Time Protocol
QoS	Quality of Service
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service

Table C-1 Acronyms and Initialisms (continued)

Term	Description
RAS	Remote Access Server
RD	Route Descriptor
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
RedBox	PRP redundancy box
REP	Resilient Ethernet Protocol
RPI	Request Packet Interval
RTT	Round Trip Time
SA	Security Association
SaaS	Software-as-a-Service
SAN	Single Attached Node
SCEP	Simple Certificate Enrollment Protocol
SE	FactoryTalk View Site Edition
SHA	Secure Hash Standard
SIG	Secure Internet Gateway
SPW	Software Provisioning Wizard
SSID	Service Set Identifier
STP	Spanning Tree Protocol
SYN	Synchronization
TAI	International Atomic Time
TCN	Topology Change Notification
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VDAN	Virtual Double Attached Node
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
VSS	Virtual Switching System
WAN	Wide Area Network
wIPS	wireless Intrusion Prevention Service
WLAN	Wireless LAN
WLC	Cisco Wireless LAN Controller
WSA	Cisco Web Security Appliance
ZFW	Zone-Based Policy Firewall

APPENDIX D

About the Cisco Validated Design (CVD) Program

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation with assistance by Panduit, which follows the Cisco Validated Design (CVD) program.

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 help achieve 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 sets 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 the Cisco Validated Designs at the following URL:

https://www.cisco.com/c/en/us/solutions/enterprise/validated-design-program/index.html

Panduit Corp. is a world-class provider of engineered, flexible, end-to-end electrical and network connectivity infrastructure solutions that provides businesses with the ability to keep pace with a connected world. Our robust partner ecosystem, global staff, and unmatched service and support make Panduit a valuable and trusted partner.

www.panduit.com

US and Canada:
Panduit Corp.
World Headquarters
18900 Panduit Drive
Tinley Park, IL 60487
iai@panduit.com
Tel. 708.532.1800

Asia Pacific:
One Temasek Avenue #09-01
Millenia Tower
039192 Singapore
Tel. 65 6305 7555

Europe/Middle East/Africa:
Panduit Corp.
West World
Westgate London W5 1XP Q
United Kingdom
Tel. +44 (0) 20 8601 7219

Latin America:
Panduit Corp.
Periférico Pte Manuel Gómez
Morin #7225 - A
Guadalajara Jalisco 45010
MEXICO
Tel. (33) 3777 6000

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at www.cisco.com. For ongoing news, please go to http://newsroom.cisco.com. Cisco equipment in Europe is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

www.cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.

Rockwell Automation is a leading provider of power, control and information solutions that enable customers to be more productive and the world more sustainable. In support of smart manufacturing concepts, Rockwell Automation helps customers maximize value and prepare for their future by building a Connected Enterprise.

www.rockwellautomation.com

Americas:
Rockwell Automation
1201 South Second Street
Milwaukee, WI 53204-2496 USA
Tel: (1) 414.382.2000
Fax: (1) 414.382.4444

Asia Pacific:
Rockwell Automation
Level 14, Core F, Cyberport 3
100 Cyberport Road, Hong Kong
Tel: (852) 2887 4788
Fax: (852) 2508 1846

Europe/Middle East/Africa:
Rockwell Automation
NV, Pegasus Park, De Kleetlaan 12a
1831 Diegem, Belgium
Tel: (32) 2 663 0600
Fax: (32) 2 663 0640

Publication ENET-TD021A-EN-P November 2019