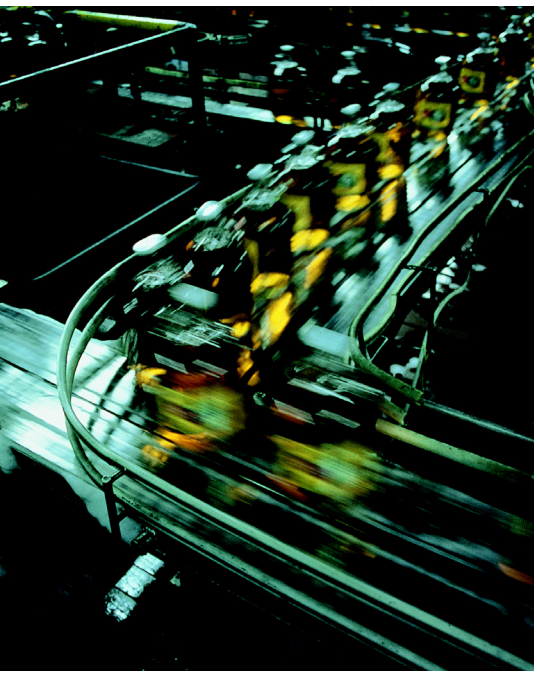


Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture

Design and Implementation Guide

August 2022

Cisco Validated Design

Document Reference Number: ENET-TD021B-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 (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. Rockwell Automation architected, tested, and validated CPwE PRP with assistance by Cisco Systems and Panduit.

Release Notes

This is the summary of the additions or changes in the August 2022 release:

- New IACS and network hardware with PRP support
  - ControlLogix® 5580 Redundancy PAC
  - ControlLogix Ethernet module 1756-EN4TR
  - Stratix® 5800 managed switch
- New or updated LAN topologies and use cases
- Updated Precision Time Protocol (PTP) architecture with multi-VLAN support and boundary clocks (BC) in PRP-independent LAN topologies
- Validated PTP performance and updated recommendations
- Recommendations for HMI, computers, and thin clients in a PRP network

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.
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:
  - https://www.rockwellautomation.com/en-us/capabilities/industrial-networks/design-guides.html
- Cisco site:
  - https://www.cisco.com/c/en/us/solutions/design-zone/industries/manufacturing/cpwe.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

Inclusive Terminology

Rockwell Automation, Cisco and Panduit recognize that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology.

We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

CHAPTER 1

CPwE Parallel Redundancy Protocol Overview

This chapter includes the following major topics:

CPwE PRP Introduction

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 Rockwell Automation with assistance by Cisco Systems and Panduit.

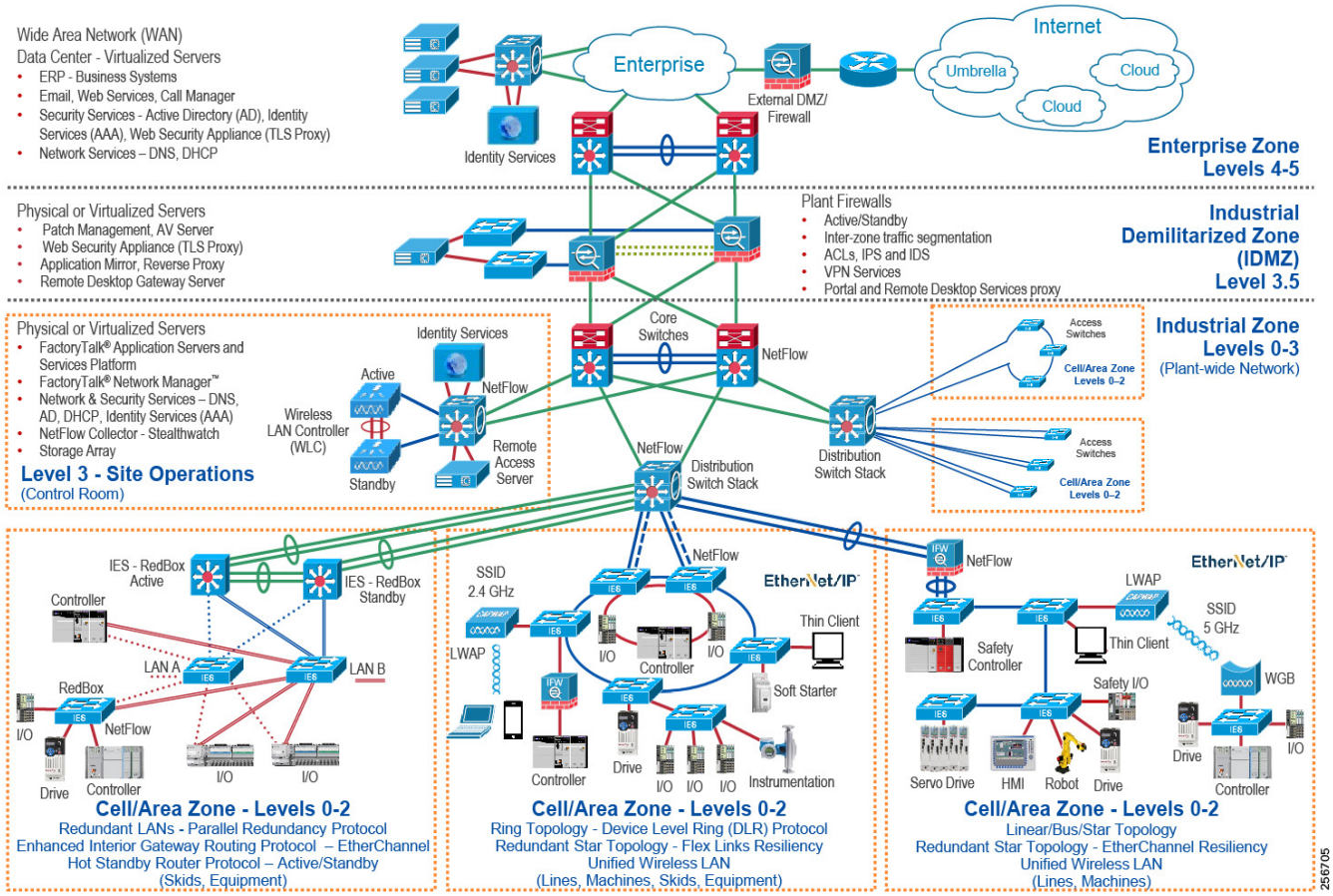
CPwE Overview

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), facilitating both technology coexistence and IACS device interoperability, which helps to enable the choice of best-in-class IACS devices.
- **Zoning (segmentation)**—Smaller connected LANs, functional areas, and security groups (smaller trust zones).
- **Managed infrastructure**—Managed Allen-Bradley® Stratix® industrial Ethernet switches (IES), Cisco Catalyst® distribution/core switches, 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 (for example, 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



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 convergence 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 use 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.

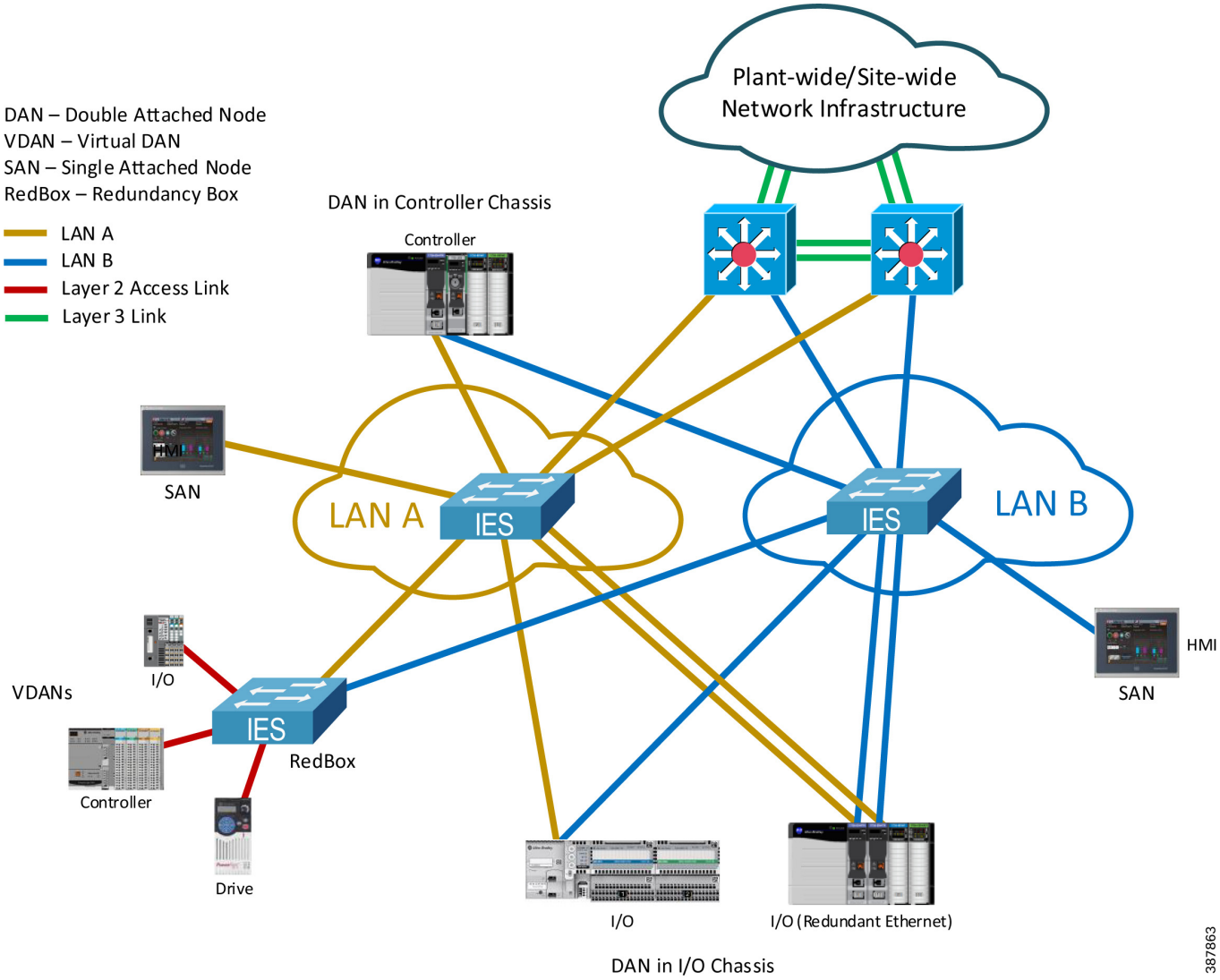
IACS devices that connect to both LAN A and LAN B through a RedBox are referred to as a PRP Virtual DAN (VDAN).

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. There is no convergence time in a PRP network after a fault in one of the LANs.

In contrast, other resiliency technologies are typically single-fault tolerant, are a single LAN, and use 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 that 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 and LAN B switches
  - Allen-Bradley Stratix 5800, 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, using a robust physical layer and resilient LAN 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
- *Physical Infrastructure for the Converged Plantwide Ethernet Architecture Application Guide* helps customers address the physical deployment associated with converged plant-wide or site-wide EtherNet/IP architectures. As a result, users can achieve resilient, scalable EtherNet/IP networks that can support proven and flexible CPwE logical architectures designed to help optimize OEM, plant-wide or site-wide IACS network performance.
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td020_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Phy_Arch/CPwE_PhyArch_AppGuide.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 and RedBox 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 a 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 planning to implement 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
- Configuration of other network services such as multicast management and time synchronization for optimal operation in the PRP network.

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.	Linear, star, redundant star or ring topology using managed switches
Double attached node (DAN)	An IACS device with PRP technology that connects to both LAN A and LAN B.	1756-EN4TR ControlLogix Ether-Net/IP module (firmware 4.001 or later) 1756-EN2TP ControlLogix Ether-Net/IP module 5094-AENTR Flex 5000™ Ether-Net/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.	An HMI terminal, a thin client, an industrial PC
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 and Stratix 5800 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.	Drives, I/O, controllers without PRP support
Infrastructure switches	Switches in LAN A or LAN B that are not configured as a RedBox.	Stratix managed switches

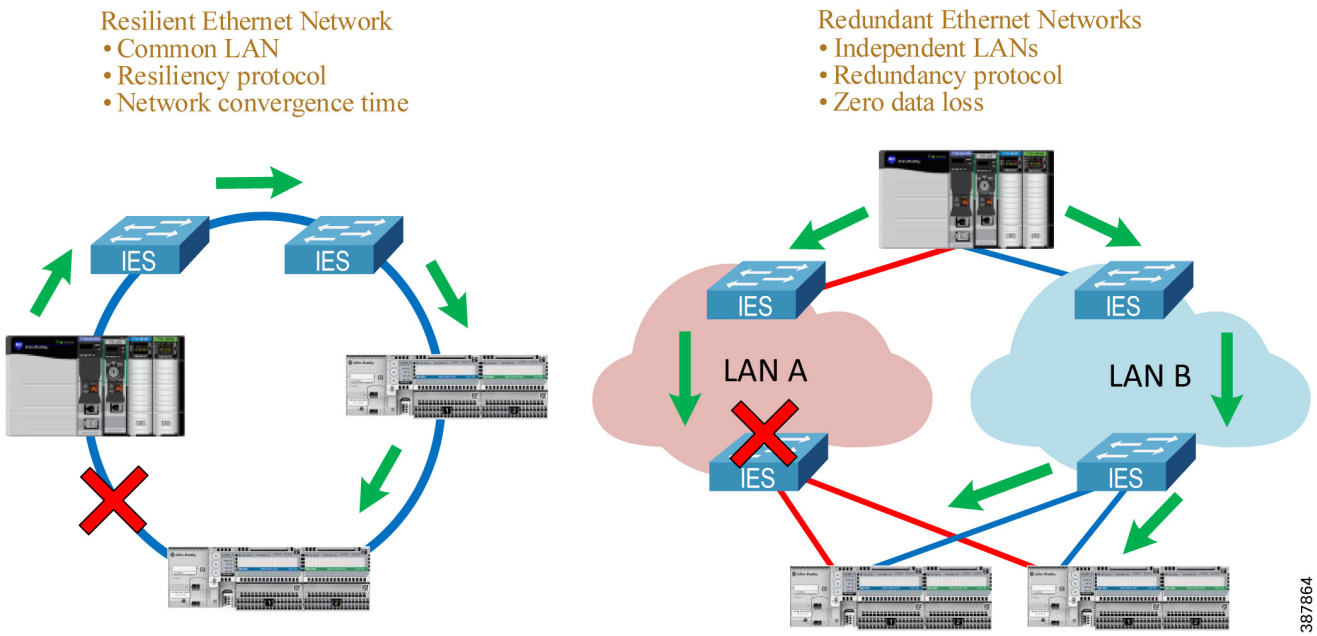
Parallel Redundancy Protocol Operation

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 convergence 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

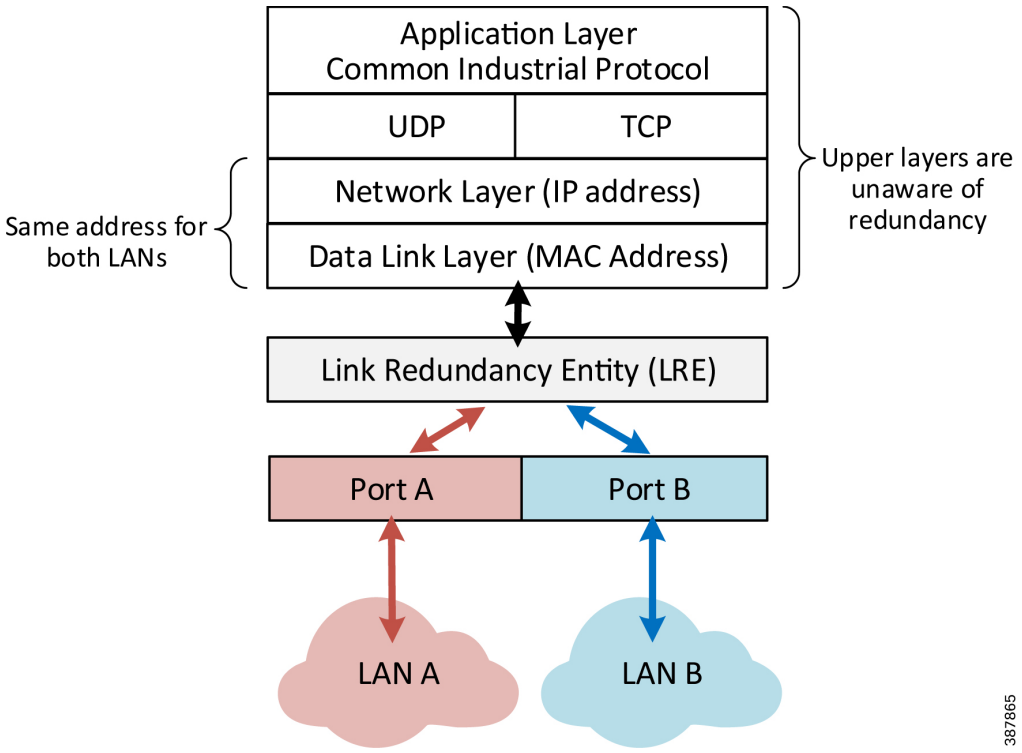


DAN Operation

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.

Note A DAN uses the same MAC address and IP address to communicate on both LANs.

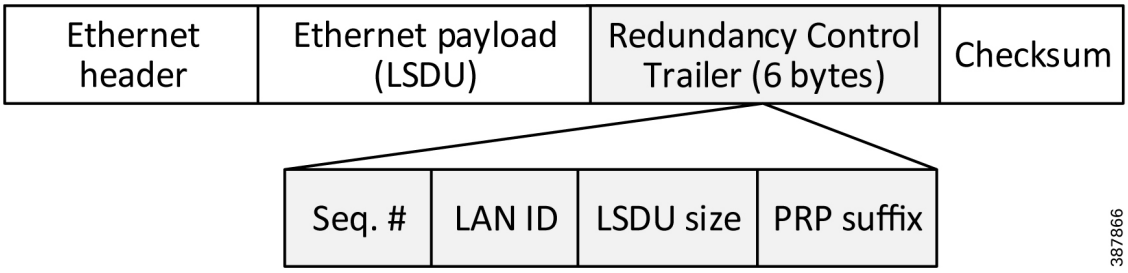
Figure 2-2 PRP DAN Communication Layers



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



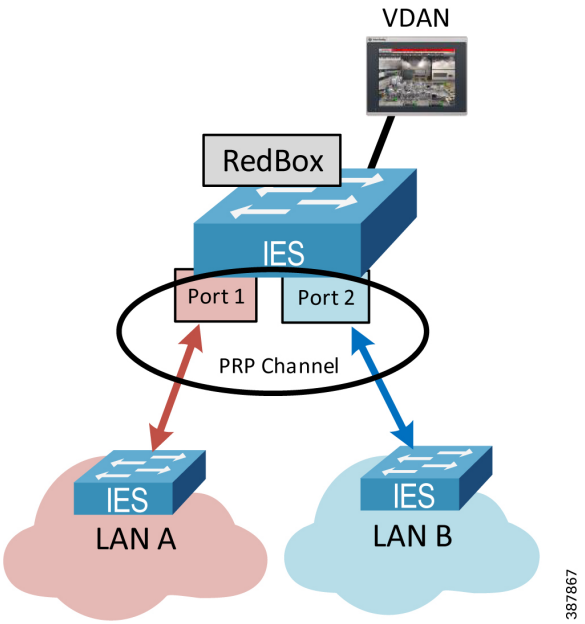
Note The RCT trailer adds six bytes to an Ethernet frame. To accommodate a maximum size Ethernet frame (1500 bytes) with the PRP trailer attached, all LAN A and LAN B network devices should be configured with the maximum transmission unit (MTU) size of at least 1506 bytes. This is not required for a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

RedBox and VDAN 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 and Stratix 5800 IES support up to two PRP channels.
- Only certain pairs of ports can be used in a PRP channel, depending on the platform.
- 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.
- The RedBox IES supports a maximum of 512 SAN and DAN entries in the Node table.
- 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.

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 plant-wide or site-wide time distribution using PTP.

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

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
- *Stratix 5800 Managed Switches User Manual* https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um012_-en-p.pdf

Note A RedBox IES in a PRP system is a single point of failure. IACS availability requirements should be evaluated when connecting critical devices to a RedBox. Best network practices must be implemented, such as using redundant power supplies, installing proper cabling and grounding, and avoiding uncontrolled loops in the LAN A and LAN B topologies.

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.

Note All SANs must have unique IP addresses across the PRP network. Address Conflict Detection (ACD) mechanisms may fail if duplicate addresses are assigned to SANs in different LANs. To avoid that, use RedBoxes and connect devices as VDANs.

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) and other management protocols, EtherNet/IP diagnostic tools, and diagnostic information available in PRP-capable IACS devices and RedBox IES.

PRP nodes (DAN or RedBox) provide real-time PRP statistics and verify if frames from known DANs or VDANs are received via both PRP ports. 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 the 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 redundant power sources and physically isolated cabling conduits for each LAN.
- Help protect the network from uncontrolled Ethernet loops that may cause broadcast or multicast storms. Follow best practices and use recommended topologies for resiliency protocols that may be used in LAN A and LAN B (e.g., Spanning Tree, DLR, REP). Do not disable loop prevention mechanisms on infrastructure IES.
- Use the same or similar topologies for both LANs with comparable 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 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 use 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

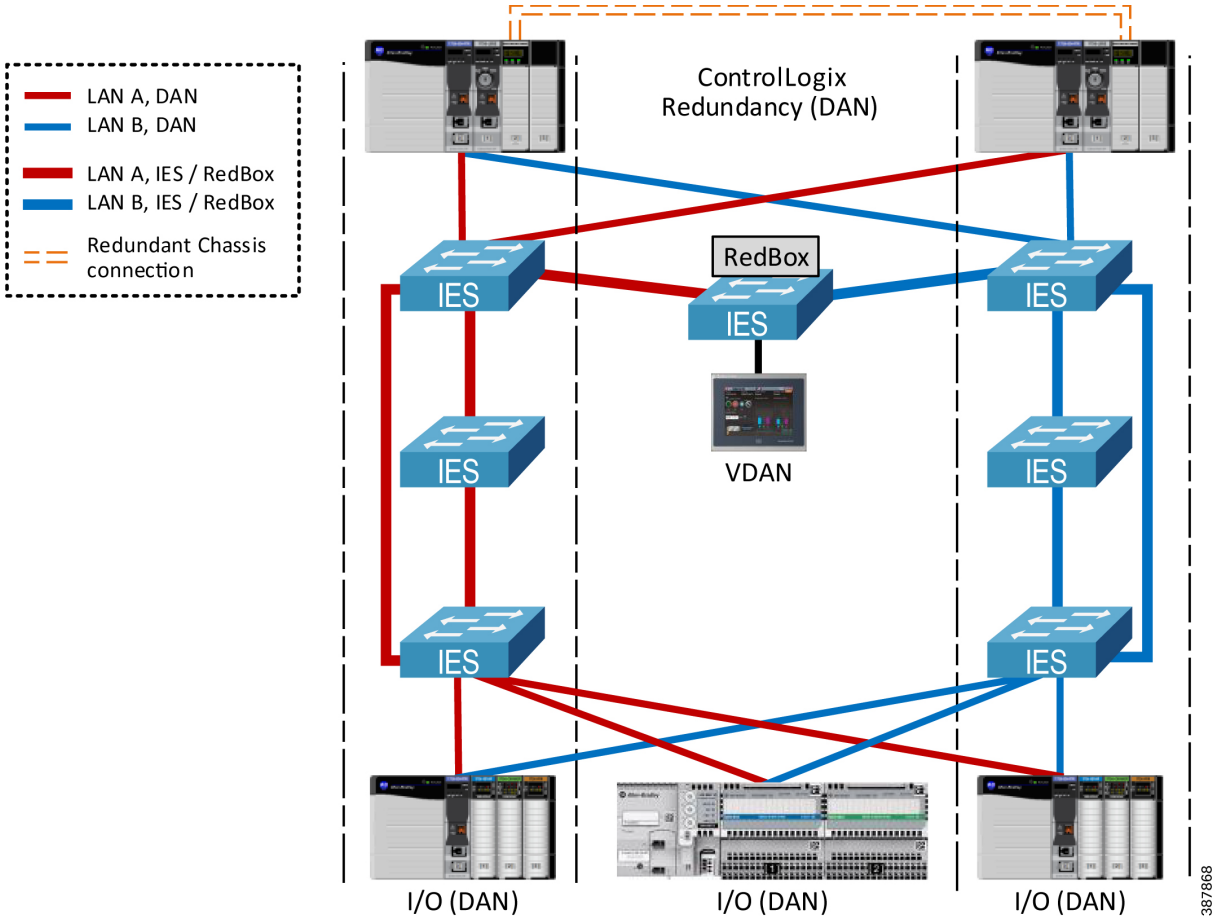


Figure 2-6 shows an example of a PRP topology with dual rings and a single (non-redundant) PAC. A dual-ring topology is common for water/wastewater, mining, oil and gas, and other industries that traditionally have used redundant dual-media topologies over large geographical areas.

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

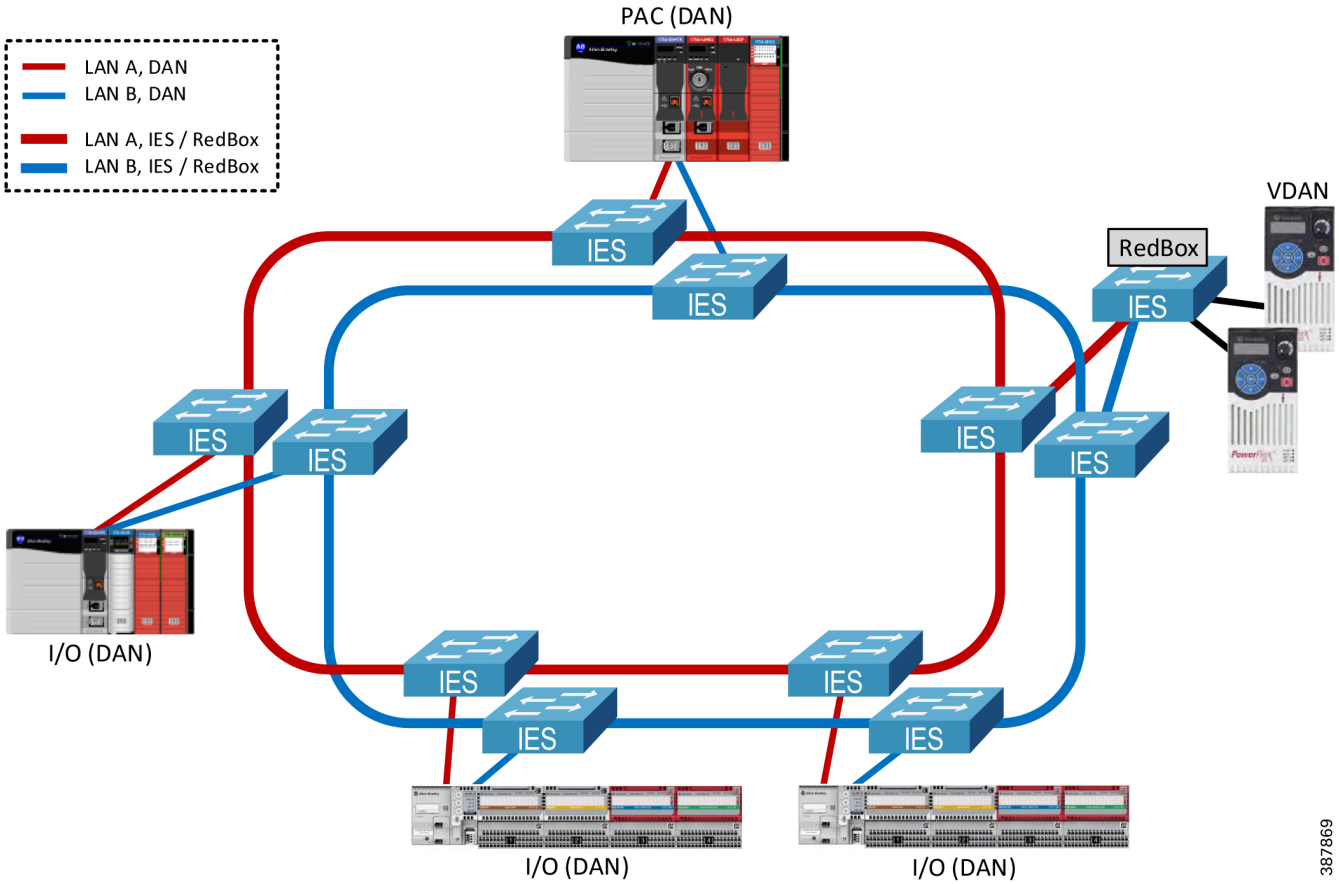


Figure 2-7 shows an example of a PRP topology with dual rings and ControlLogix redundant PACs.

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

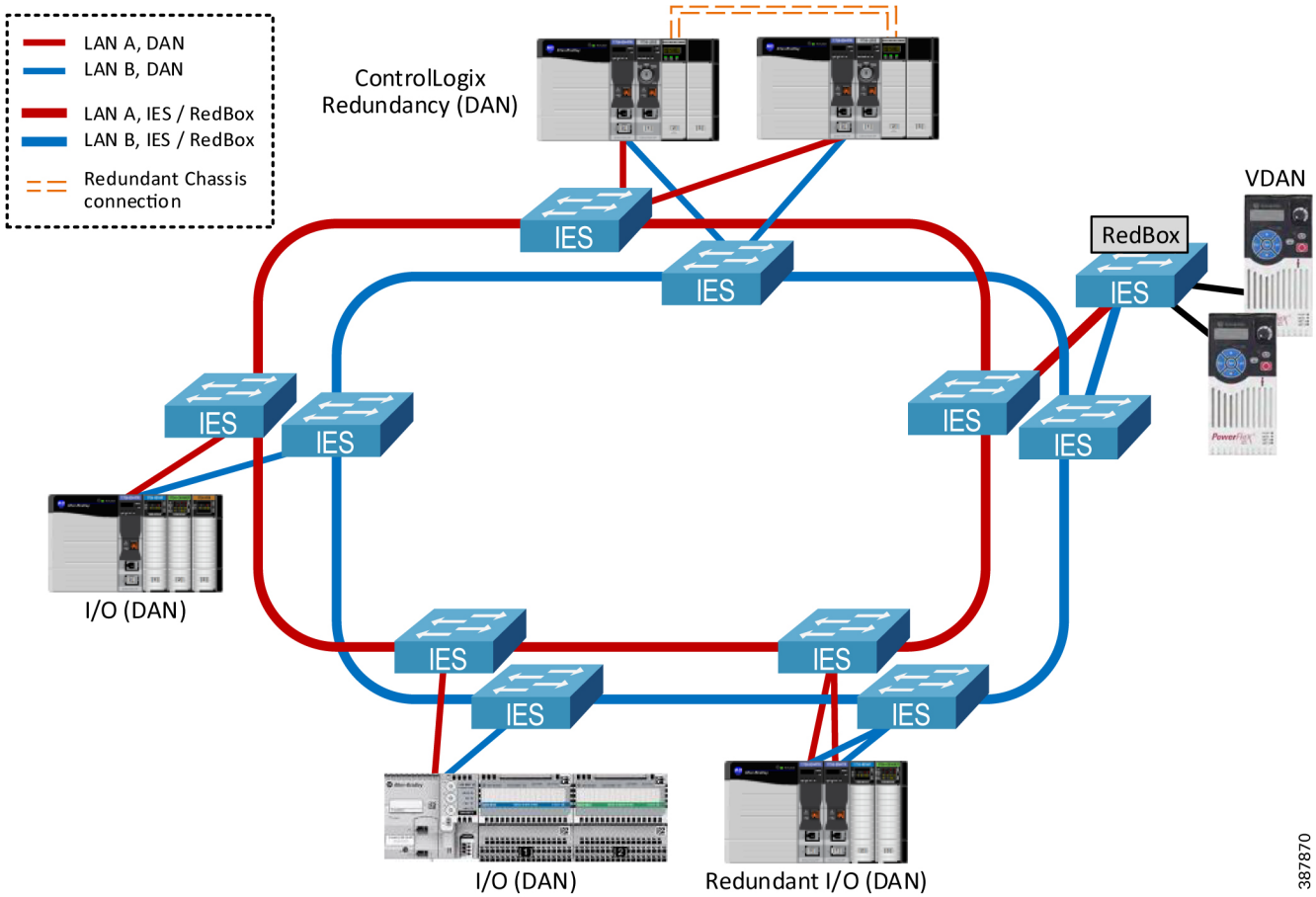
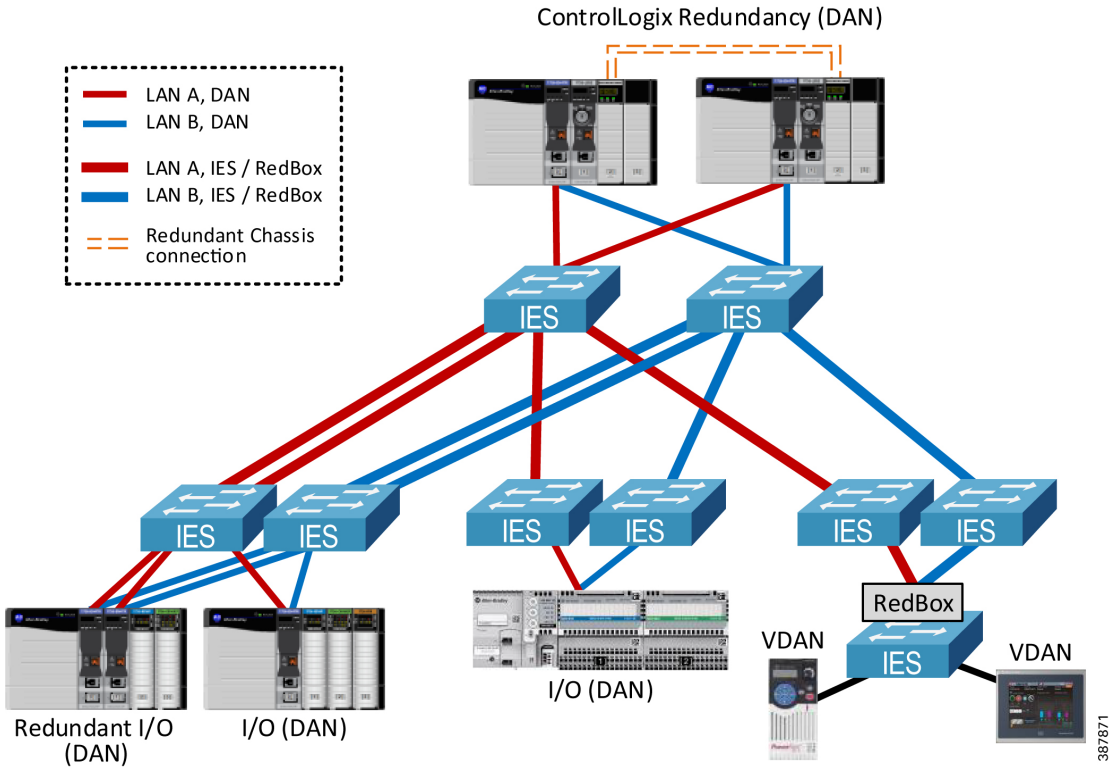


Figure 2-8 shows an example of the star topology in a PRP network.

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 star, redundant star, and dual ring topology for LAN A and LAN B with a mix of redundant and non-redundant PACs.

Connecting HMI and PCs to a PRP Network

PCs, HMI terminals and thin clients with a single Ethernet port can be connected to a PRP network:

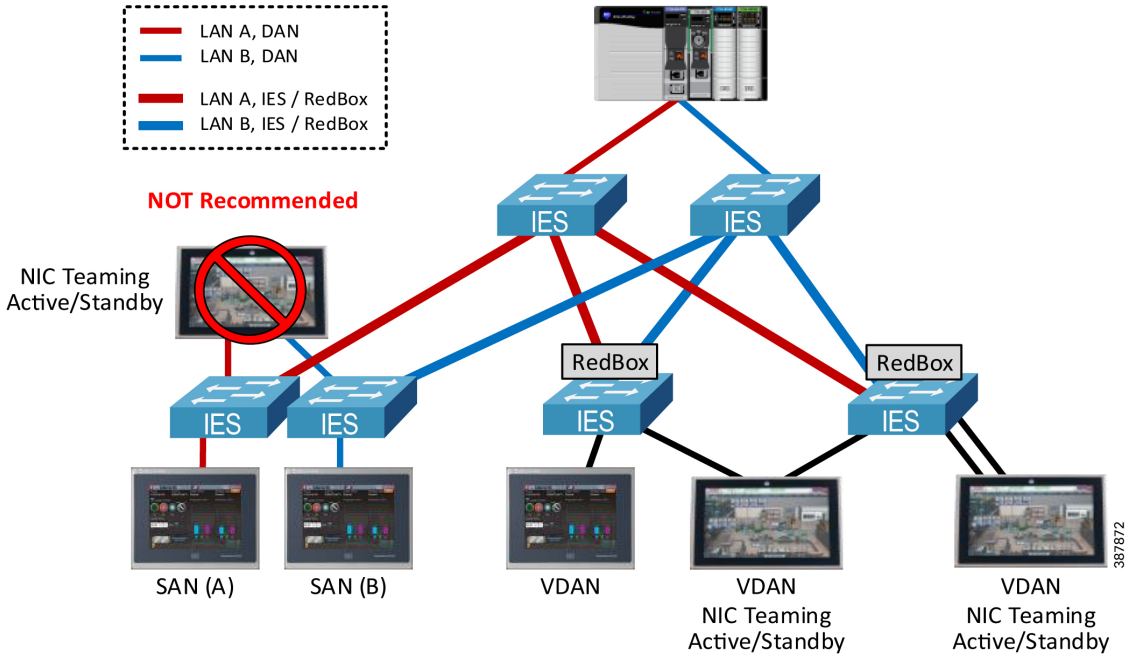
- As a SAN to a LAN A or LAN B (two terminals with identical content can be connected to each LAN for redundancy)
- As a VDAN to a RedBox

PCs with NIC Teaming or thin clients with redundant Ethernet ports in the Active/Standby mode can be connected as a VDAN to one or two RedBoxes using two Ethernet links. See Figure 2-9 below.

- Do NOT connect devices with redundant NICs without native PRP support to LAN A and LAN B switches. Doing so may cause significant delays for HMI traffic during the switchover between the NICs.

Note Validating third-party network adapters with native PRP support is out of scope for CPwE PRP.

Figure 2-9 Connecting PC and HMI Terminals



Using Wireless Media with PRP

PRP over wireless can, in principle, be supported when:

- Both LANs use the same wireless technology with similar latency
- Separate wireless channels are used for LAN A and LAN B links
- Radios and other infrastructure equipment either support PRP as a feature or can forward Ethernet frames with PRP trailer without modification

It is highly recommended to validate PRP operation with the selected wireless equipment and verify compatibility with the vendor before deployment.

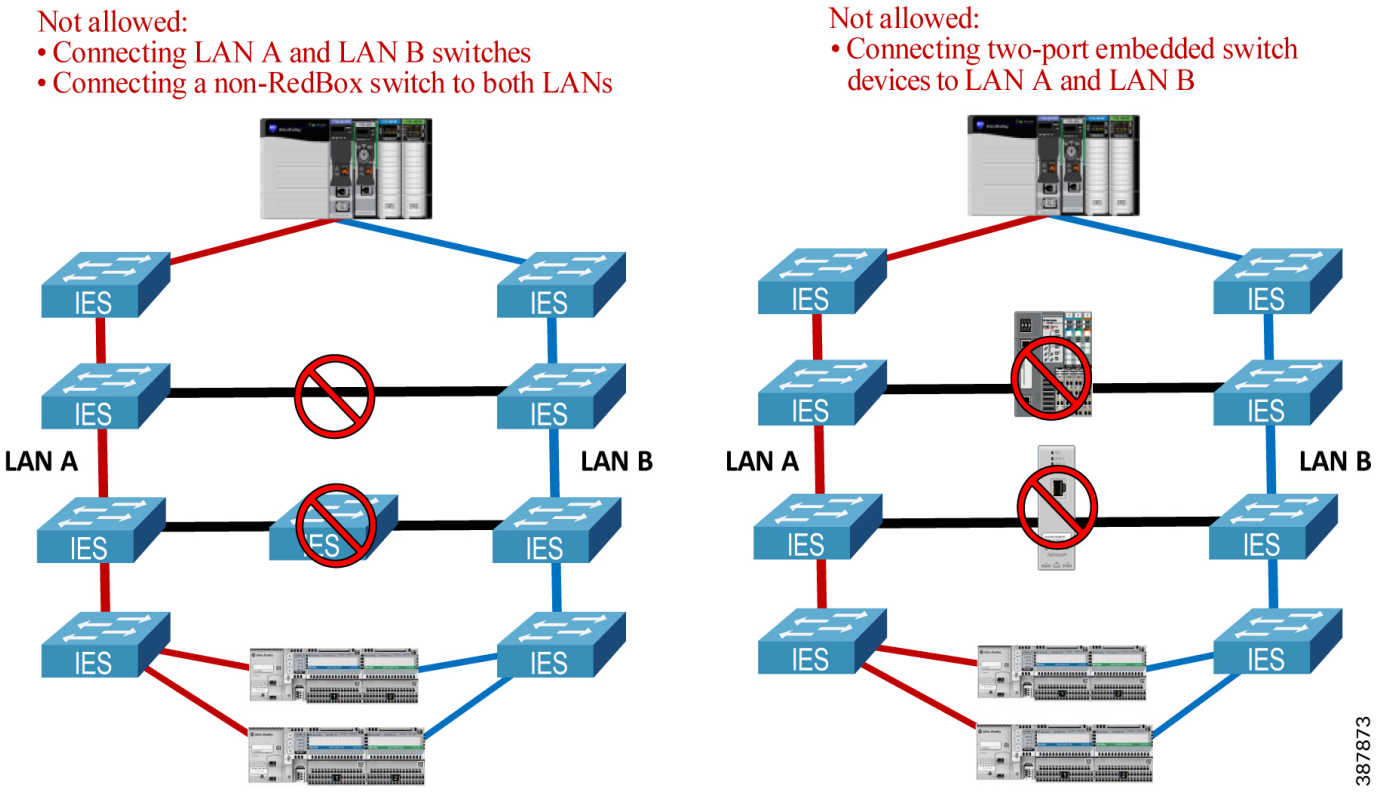
Note PRP over wireless is out of scope for this release of CPwE PRP architecture.

Unsupported Topologies

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

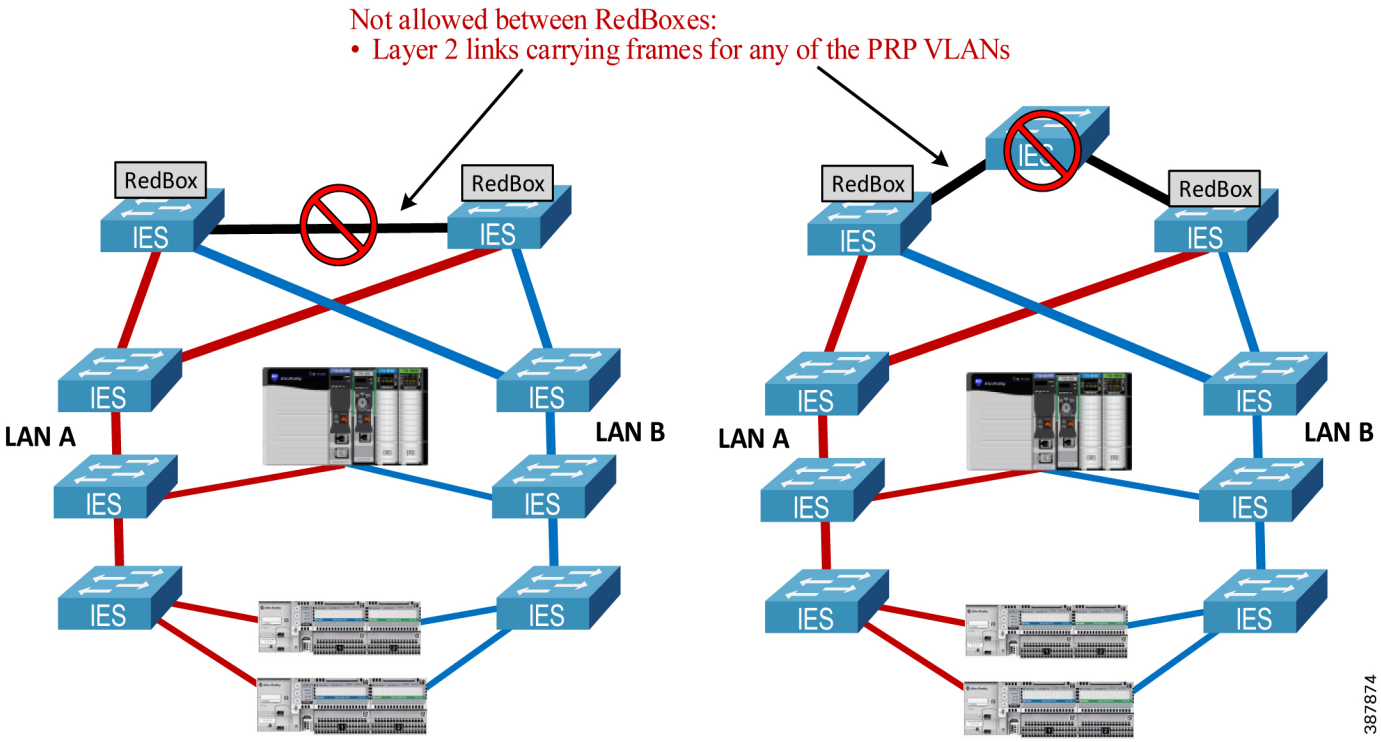
- LAN A and LAN B infrastructure cannot be bridged together using a direct link, a non-RedBox IES, or a 2-port embedded switch device that does not support PRP (e.g., a ControlLogix 1756-EN2TR module or a 1783-ETAP EtherNet/IP DLR tap module). See Figure 2-10 below.

Figure 2-10 Invalid Topology—Bridging LAN A and LAN B



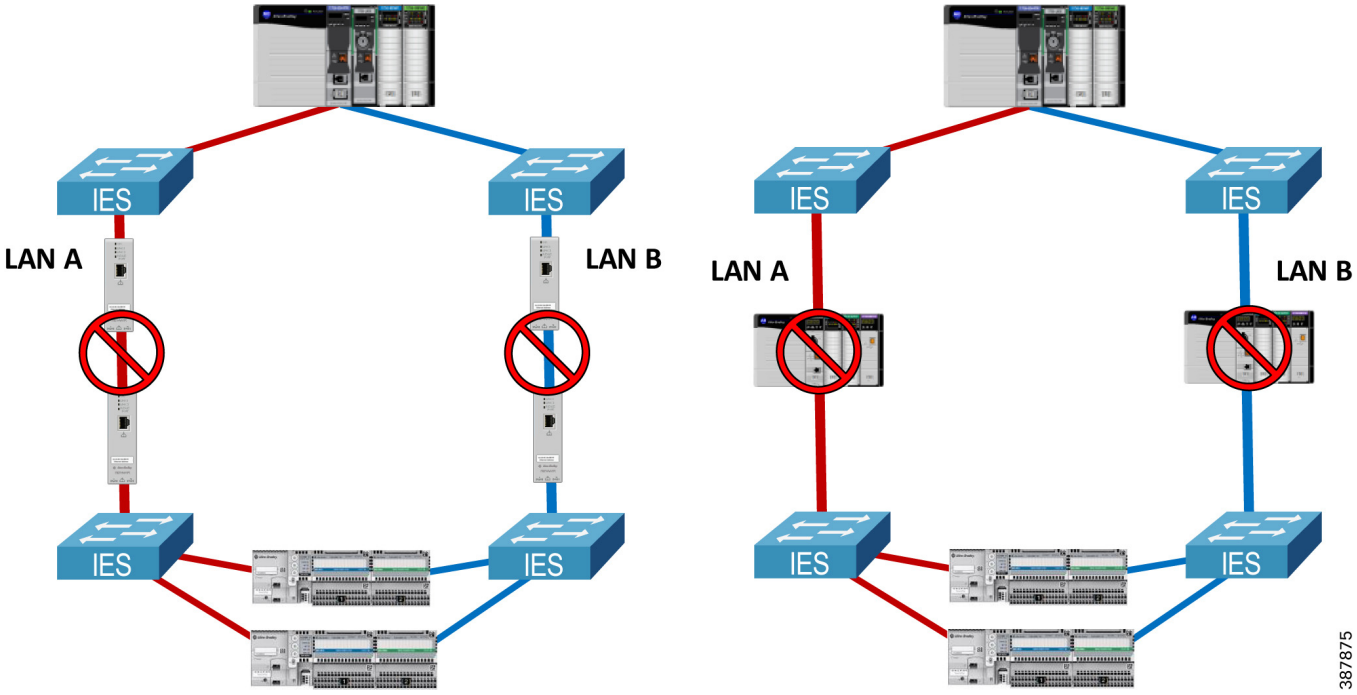
- RedBox IES cannot be connected through non-PRP ports via a Layer 2 path that forwards traffic from any of the PRP VLANs, including IACS data VLANs, management VLAN, or the native VLAN. See Figure 2-11 below.

Figure 2-11 Invalid Topology—Bridging PRP VLAN via RedBox non-PRP Ports



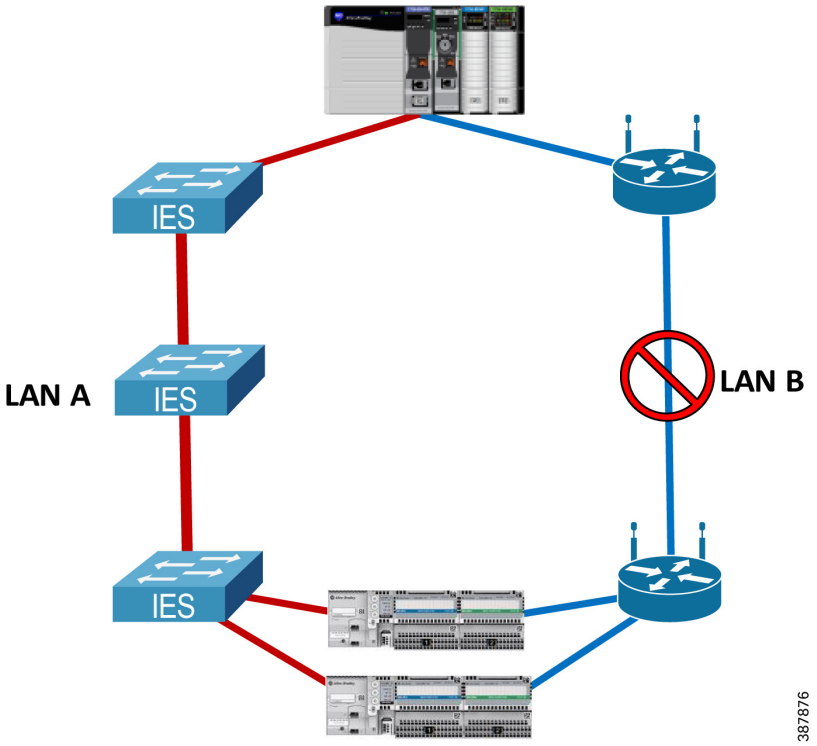
- LAN A and LAN B topologies should not contain 2-port embedded switch devices, including 1783-ETAP modules, in the data path. Embedded switch devices cannot be configured for the larger MTU sizes to accommodate the PRP trailer in the frame. As a result, maximum size Ethernet frames may be dropped. This also applies to any IES without the option to increase the MTU size (Figure 2-12).

Figure 2-12 Unsupported Topology—Traversing 2-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 2-13).

Figure 2-13 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:

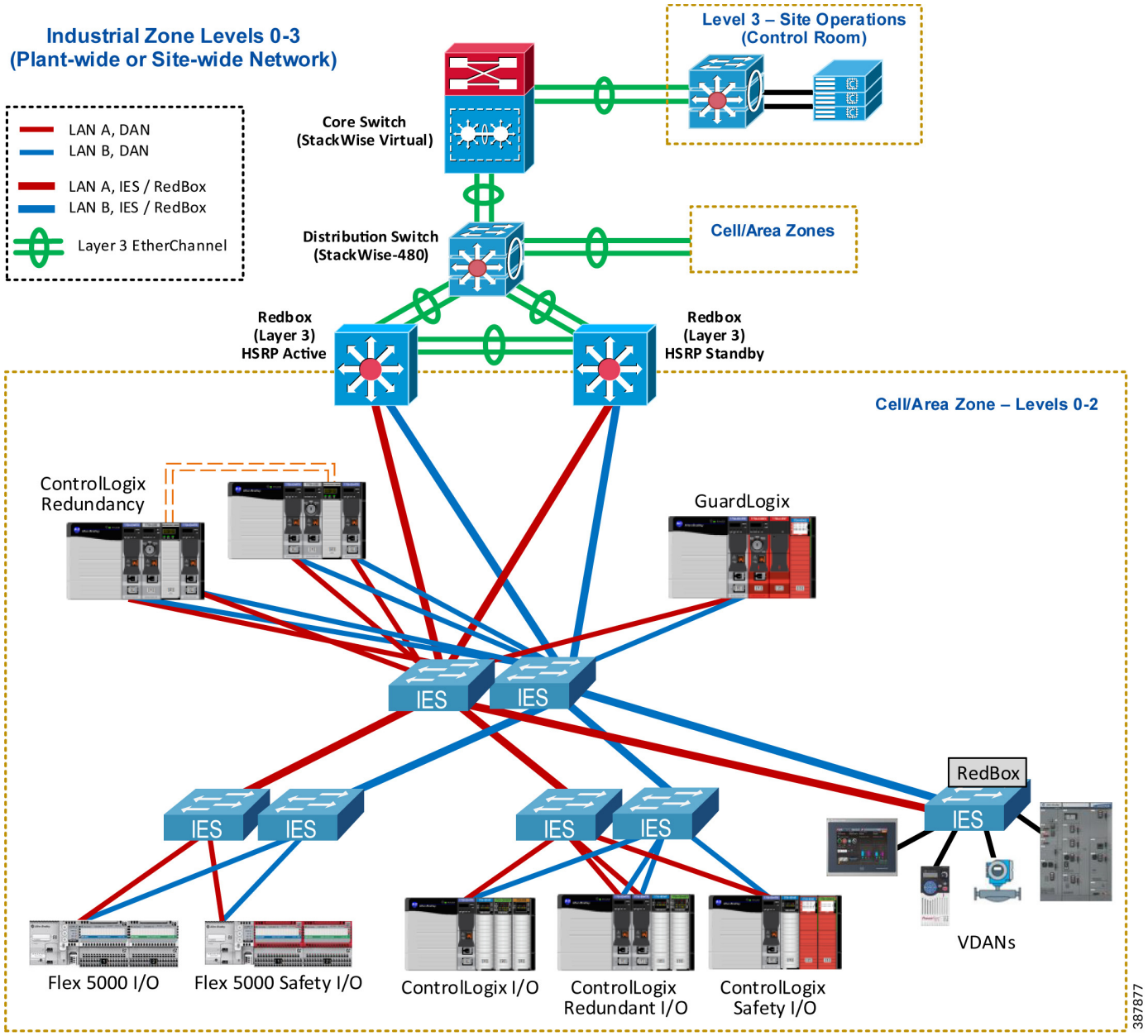
- Remote access for diagnostics and troubleshooting
- Distributed network applications using virtual server environment in the Level 3 Site Operations
- Access to IACS device data and analytics from the Enterprise Zone and / or the cloud as part of the Connected Enterprise® system™.

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 2-14 shows the CPwE PRP architecture that provides redundant connectivity from a resilient distribution layer in the Industrial Zone to a pair of distribution Layer 3 RedBox IES connected to the PRP Cell/ Area Zone with a star LAN topology.

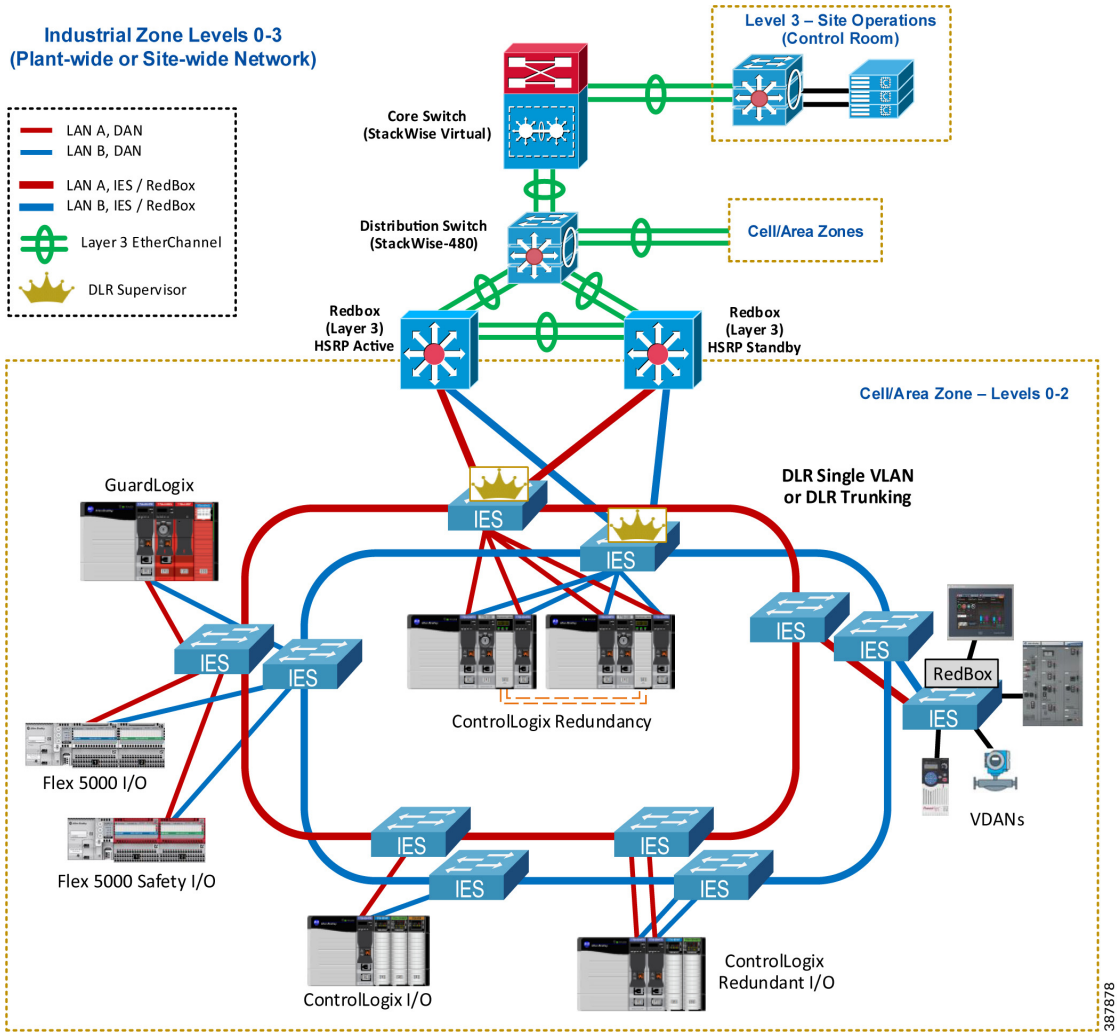
Figure 2-14 Connectivity to the Industrial Zone



- Redundant Layer 3 RedBox IES are configured with Hot Standby Router Protocol (HSRP) as active/standby default gateways for IP subnets in the PRP topology.
  - Layer 3 RedBox IES use PRP channel ports to send HSRP hello packets and monitor redundancy state.
- Redundant links between Layer 3 RedBox IES and uplinks to the distribution stack are configured as Layer 3 EtherChannels (routed ports).
- Dynamic routing protocol is configured between the distribution Layer 3 RedBox IES with HSRP pair and the distribution switch stack.
  - 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 infrastructure and requirements. CPwE PRP has not been validated with OSPF.
  - Static routes between RedBox IES and the distribution / core layer are allowed but not recommended due to anincreased complexity of configuration and maintenance in large environments. CPwE PRP has not been validated with static routing.
- Cisco StackWise-480 technology has been tested with the distribution switches for 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.
- Small-scale deployments can combine core and distribution layers into one redundant switch layer.

Figure 2-15 shows a similar CPwE PRP architecture with redundant connectivity via a pair of Layer 3 RedBox IES where DLR is used in the PRP Cell/Area Zone as a ring LAN topology.

Figure 2-15 Connectivity to the Industrial Zone (DLR LAN Topology)



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:

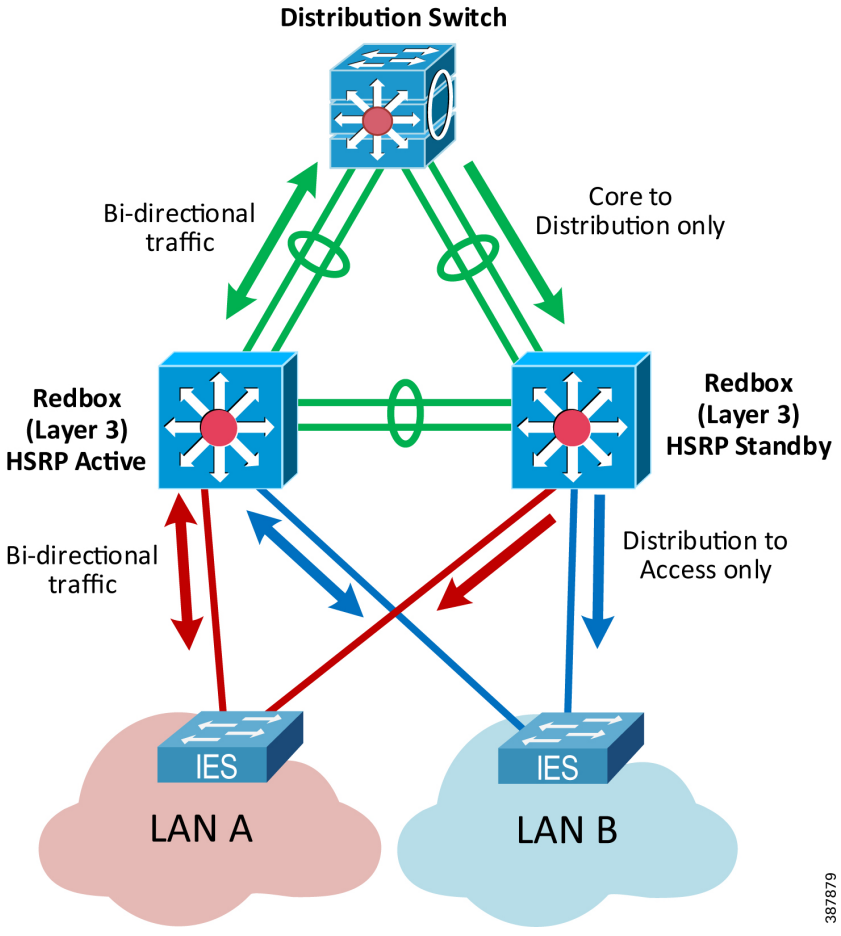
- *OSPF Design Guide*
  http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Note HSRP and EIGRP features require Layer 3 firmware level for Stratix IES and Network Advantage license type for Cisco Catalyst 9300 switches.

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 2-16).

This is due to the equal cost routing in EIGRP or OSPF on the distribution 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 2-16 Routed Traffic with PRP



The recommended and validated EtherChannel, HSRP, and EIGRP configuration for CPwE PRP is provided in Chapter 3, "CPwE Parallel Redundancy Protocol Configuration."

Routed Traffic Convergence

PRP provides zero-loss redundancy and single-fault tolerance for Layer 2 (Ethernet) traffic in the PRP network, including protection against a LAN switch fault or a link fault affecting a DAN, a LAN switch or a PRP channel port on a RedBox.

Layer 3 (routed) traffic traverses a Layer 3 switch (the default gateway) which must be a RedBox IES. CPwE PRP architecture includes two redundant Layer 3 RedBox IES to provide resiliency for the routed traffic.

Note PRP does not provide zero-loss redundancy for routed traffic when a Layer 3 RedBox fails. Routed traffic is interrupted and reconverges during faults impacting the Layer 3 RedBox IES or routed uplinks connected to the RedBoxes.

Depending on the fault type, convergence time for routed IACS data may include:

- HSRP failover time between Layer 3 RedBox IES
- Dynamic routing protocol convergence
- EtherChannel failover
- Layer 2 switched network convergence (e.g., MAC table updates)

Different routing configurations, protocols and distribution switch platforms may provide different results. Table 2-2 summarizes various faults and the observed impact on the routed traffic in the CPwE PRP testing.

Table 2-2 Routed Traffic Convergence [1]

Event Type	Layer 3 traffic to/from PRP Cell/Area Zone		Layer 3 traffic between VLANs in PRP Cell/Area Zone	
	Convergence Time	Typical Time	Convergence Time	Typical Time
Layer 3 EtherChannel link loss or restore	EtherChannel	< 150ms	N/A	N/A
Layer 3 EtherChannel loss (both links)	Routing protocol	1 - 3 seconds	N/A	N/A
Layer 3 RedBox down (HSRP Active)	HSRP and routing protocol	1 - 3 seconds	HSRP	1 - 2 seconds
Layer 3 RedBox down (HSRP Standby)	Routing protocol	1 - 3 seconds	N/A	N/A
Layer 3 RedBox restored (becomes HSRP Standby)	Routing protocol	< 1 second	N/A	N/A
LAN switch fault	PRP	0	PRP	0
Link fault in the PRP LAN	PRP	0	PRP	0
Link fault between Layer 3 RedBox and LAN switch	PRP	0	PRP	0

1. With HSRP hold timers 750 ms, EIGRP routing protocol and LACP Active EtherChannel mode.

Note It is important to evaluate IACS application requirements for the routed traffic and compare with the expected convergence times. For example, timeout period with typical Requested Packet Interval (RPI) values for routed CIP Class 1 data (Produced/Consumed tags) may be lower than the HSRP convergence. As a result, Produced/Consumed connections may be dropped during a Layer 3 RedBox failure.

Connectivity to Device Level Ring

The ODVA, Inc. Device Level Ring (DLR) resilient LAN technology is designed to provide ring topology resiliency for critical IACS applications. DLR supports fast ring convergence (single-fault tolerant) in the event of an IACS device or link failure.

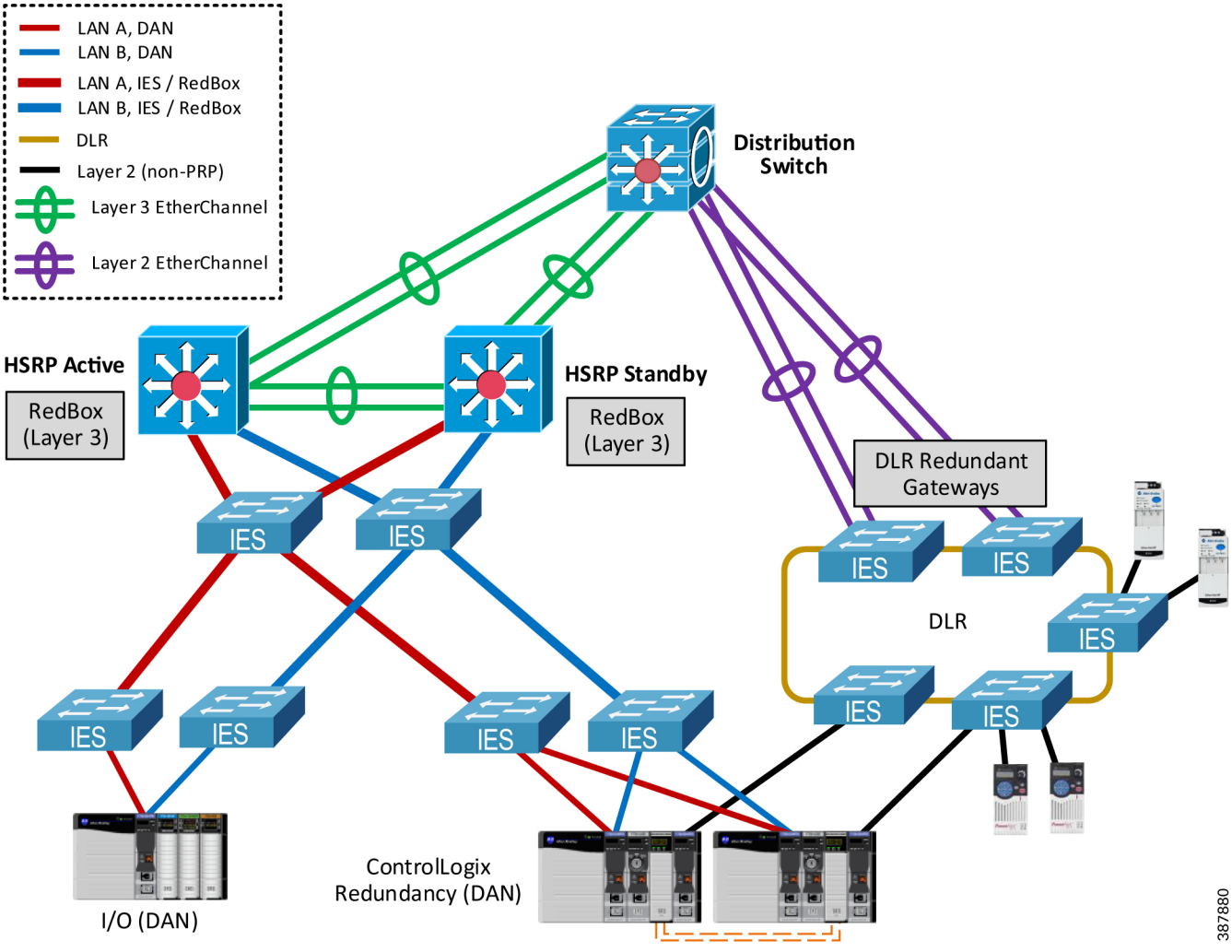
For more information on DLR in CPwE, refer to:

- Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture
  https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td015_-en-p.pdf

This section describes recommendations for connecting an existing DLR topology without PRP to a PRP architecture.

- The recommended resilient architecture is to connect the DLR topology via a separate distribution switch (Figure 2-17) below.
  - A controller chassis can be connected to both PRP and DLR networks using separate Ether-Net/IP modules in the chassis. In this example, a ControlLogix Redundancy chassis is con-nected to the PRP topology and the switch DLR topology.

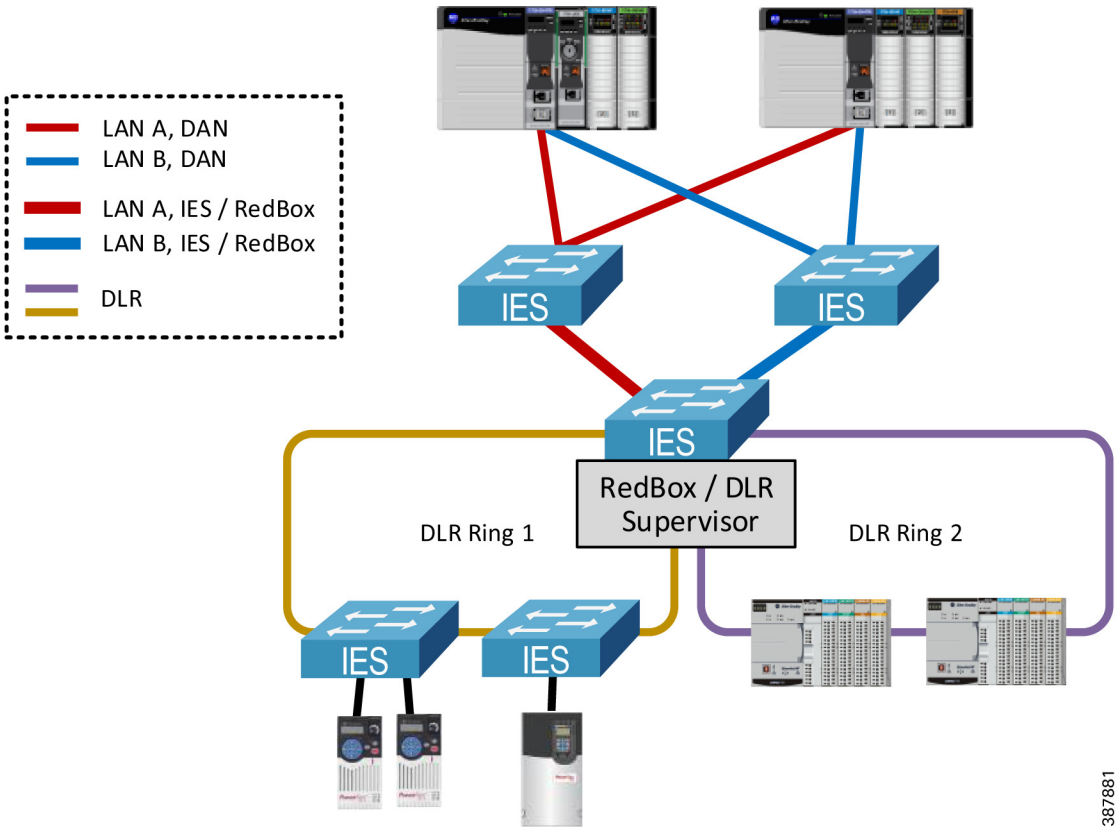
Figure 2-17 Connecting Controller Chassis to both PRP and DLR



- An alternative non-redundant option is to use a RedBox IES as the DLR supervisor for one or multiple rings (Figure 2-18) below. DLR ports cannot be the same as the PRP channel ports.

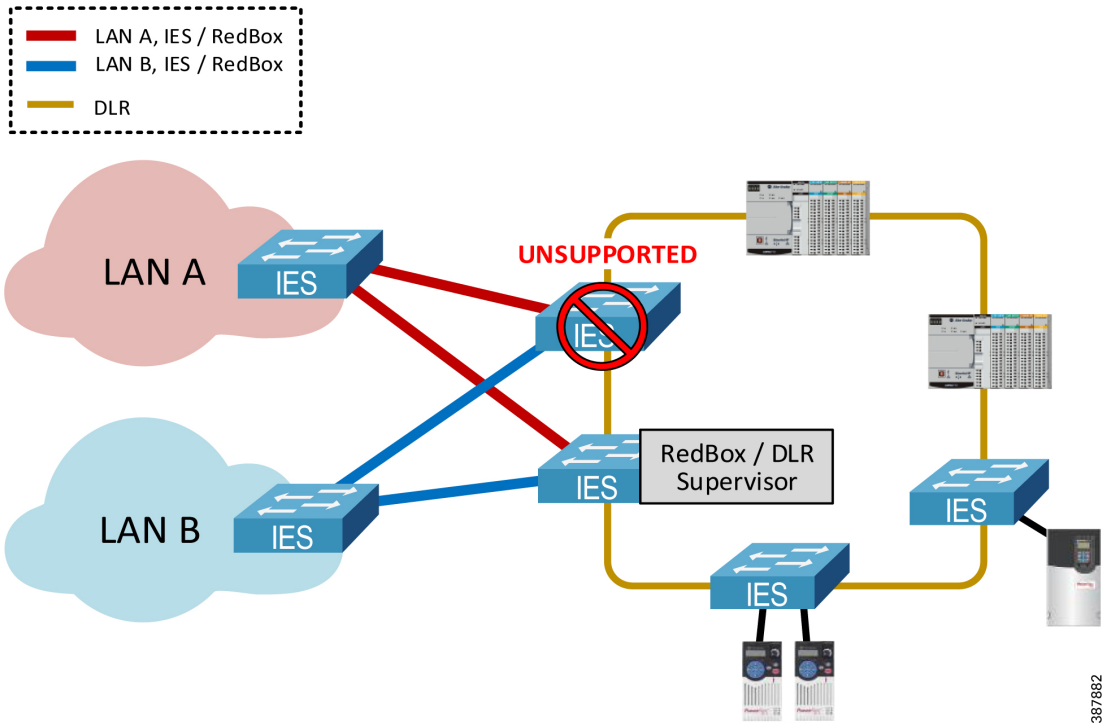
Note In this case the RedBox is a single point of failure for the traffic between the DLR and the PRP topologies. This architecture is not recommended for critical IACS data traversing the RedBox and has not been validated for performance or scalability in this CPwE PRP.

Figure 2-18 PRP to DLR Connectivity via a Single 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 2-19) below.

Figure 2-19 Unsupported Topology—PRP to DLR Redundant Gateways



Note An EtherNet/IP module in the PRP mode cannot be used as part of the DLR or a linear topology. PRP-enabled modules do not implement the embedded switch technology and traffic cannot traverse from port A to port B. Similarly, an Ethernet module in the DLR mode cannot be connected to both LAN A and LAN B.

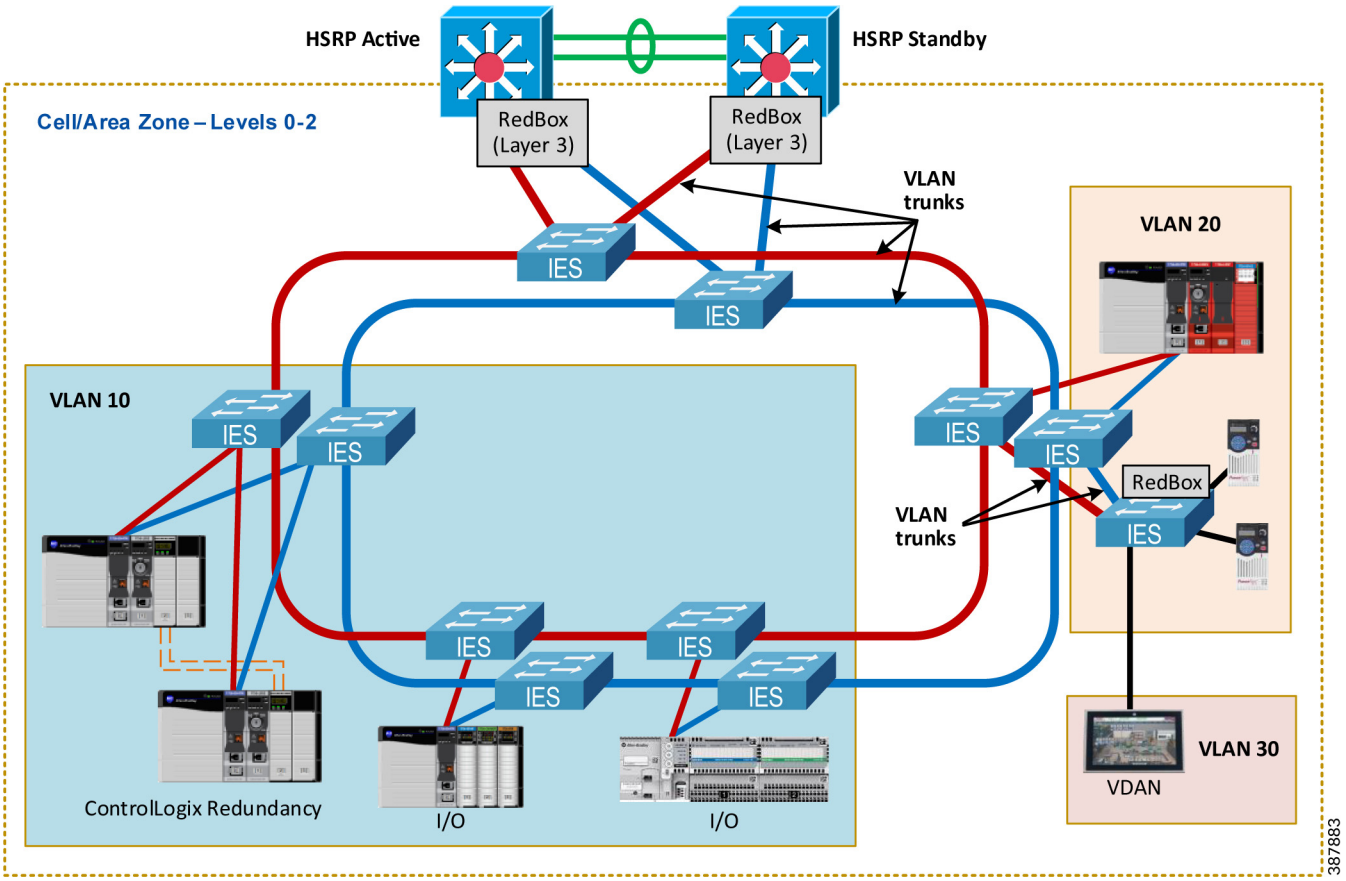
Network Services Recommendations

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

VLAN Segmentation 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 2-20) below.

Figure 2-20 VLAN Segmentation (Zoning) in PRP Network



Follow these recommendations when using VLAN segmentation 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 using a separate management VLAN for the RedBox IES.

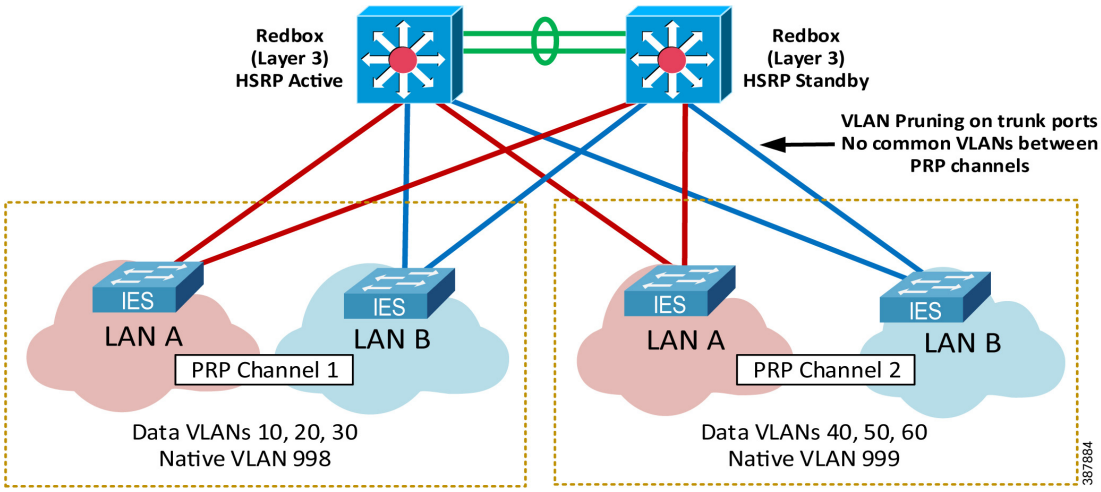
- PRP channels on the redundant Layer 3 RedBox IES in CPwE PRP should be configured as VLAN trunks. The architecture has been validated with inter-VLAN IACS traffic which is routed through the Layer 3 RedBox with HSRP.
  - Traffic between VLANs (Layer 3) is impacted if the active HSRP gateway fails. Convergence time depends on the HSRP parameters.
- Links between IES in each PRP LAN should be configured as VLAN trunks. Per CPwE best practice, the native VLAN should be different from any of the IACS VLANs

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

For network architectures with two PRP channels configured on the same pair of Layer 3 RedBox IES, configure VLANs as follows to avoid network loops (Figure 2-21) below.

- Use separate sets of data, management and native VLANs in Cell/Area Zones connected to each PRP channels
- Configure the allowed VLAN list on the trunk ports in the PRP channel group (VLAN pruning), making sure that VLANs from the other PRP channel are not allowed.

Figure 2-21 Two PRP Channels with VLAN Pruning

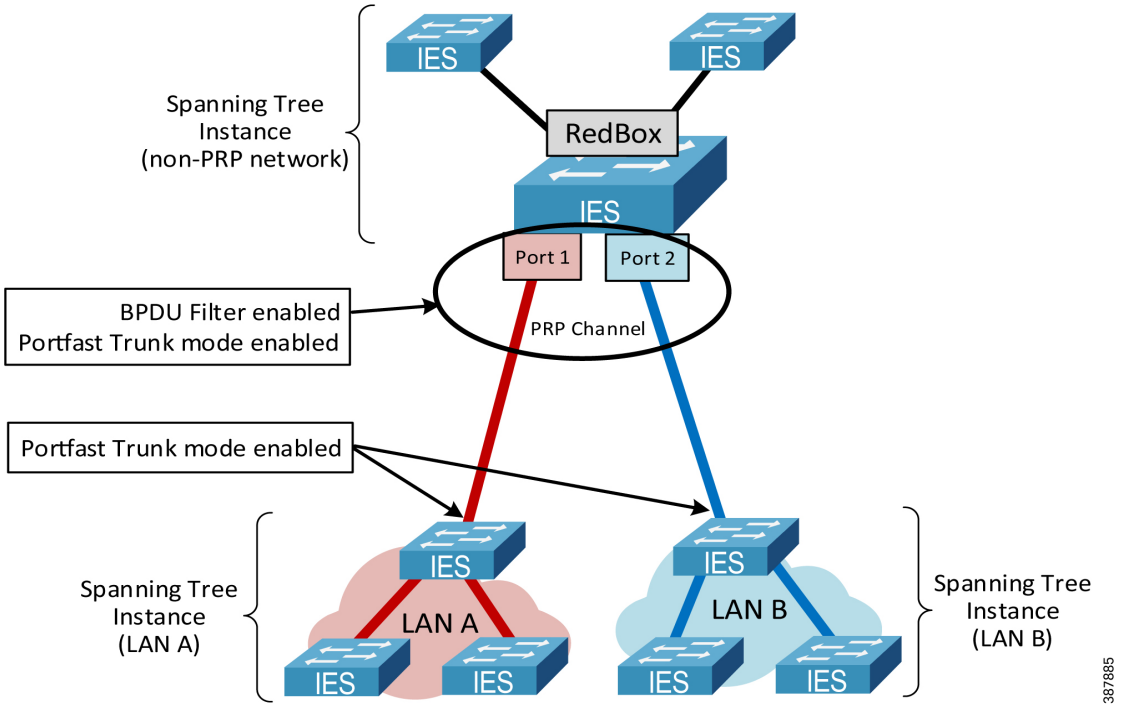


Spanning Tree Protocol

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 2-22) below.

- A RedBox IES serves as a boundary between separate STP instances in LAN A and LAN B. There should be no common STP domain bridging two redundant LAN A and LAN B.
- Bridge Protocol Data Unit (BPDU) frames from STP are filtered on the PRP channel ports. As a result, LAN A and LAN B switches exclude the RedBox IES in the STP operation.
- STP is running on the RedBox IES by default and should be kept enabled for loop prevention on the non-PRP ports.
  - Two RedBox IES cannot be connected to each other via non-PRP ports. Doing so will cause a bridging loop.
- PortFast Trunk mode should be configured for the PRP channel group on all RedBox IES, including redundant Layer 3 RedBox IES, and on the LAN A and LAN B IES ports connected to the RedBox. This is necessary to minimize port recovery time during network faults.
- Best practices for STP should be followed within each LAN, such as explicitly configuring the primary and secondary STP root bridge, using recommended redundant star topologies, and avoiding complex meshed topologies.

Figure 2-22 Spanning Tree Operation in the PRP Network



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

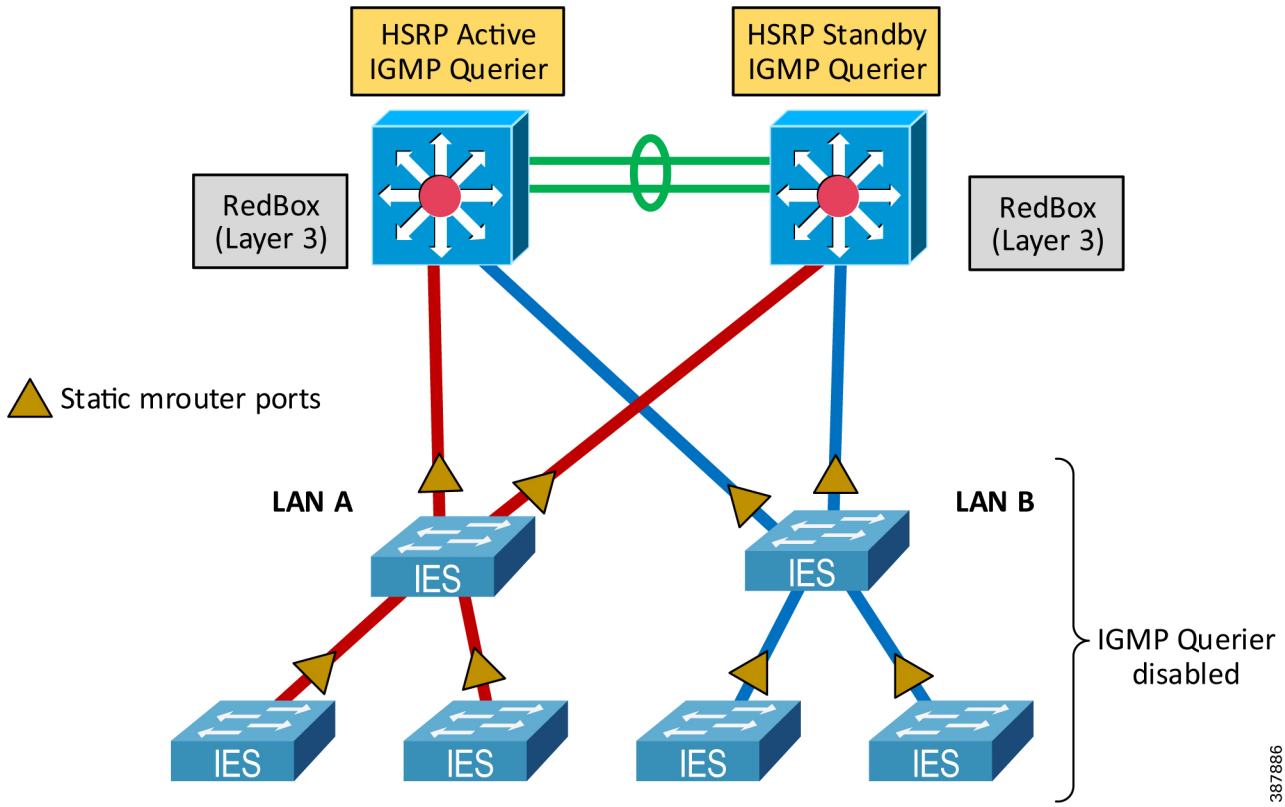
Multicast EtherNet/IP traffic is required for I/O and consumed data in ControlLogix Redundancy and for CIP Sync communication using Precision Time Protocol (PTP). Both types of multicast data could be used in IACS applications where PRP technology is deployed.

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 with HSRP. 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.
  - For networks without routing (not common), a Layer 2 RedBox can be used as a querier
- 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 2-23 below 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 2-23 Multicast Management with PRP



Note After a LAN in a PRP network encounters a fault and is then repaired, there could be a delay until the IGMP querier reinstates the multicast traffic in the recovered LAN (typically within 2 minutes after the LAN is repaired). During that time, the other LAN will continue forwarding multicast traffic, however, PRP redundancy is not provided for multicast data for a short period of time.

Network Address Translation

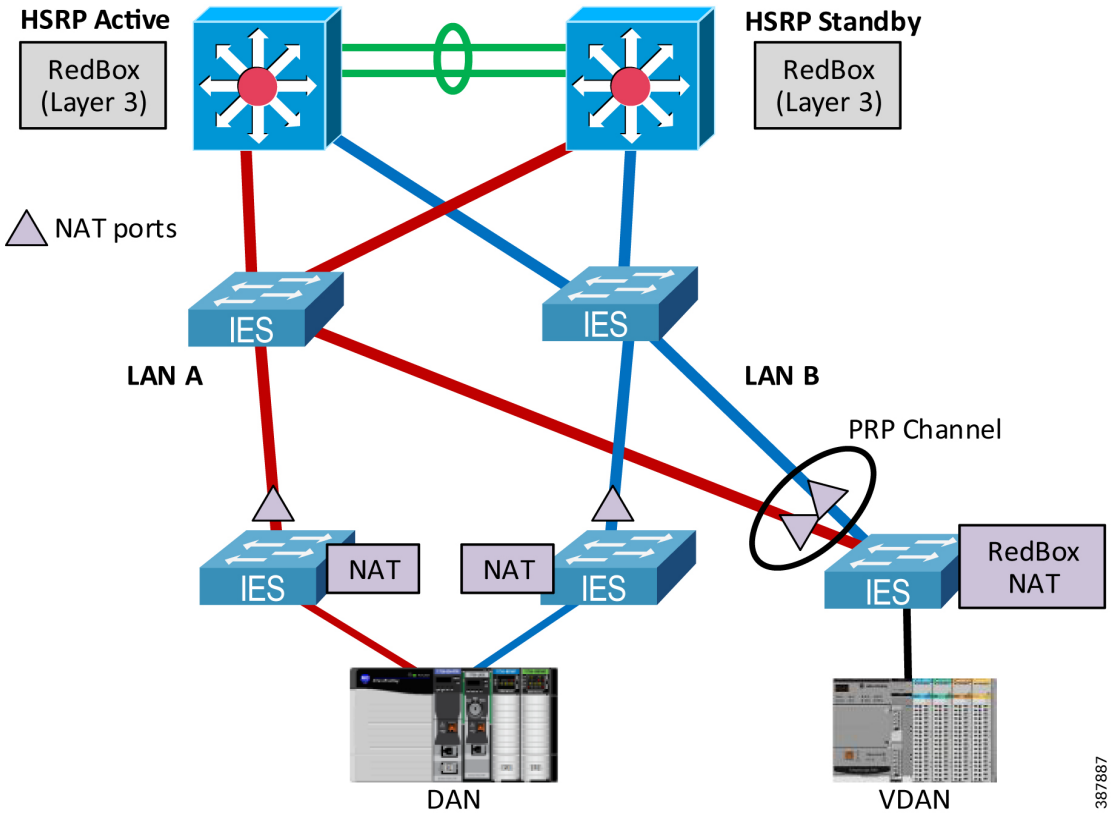
Network Address Translation (NAT) feature in IES provides benefits to OEM machine or process skid builders, such as IP address reuse and commissioning of "cookie cutter" machines without reprogramming, easier maintenance of machine configurations and controller programs, and better traffic control and 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 is transparent to the higher layers of the network stack where IP addresses are used.

There are two possible implementations of NAT in a PRP topology (Figure 2-24) below:

- Configure NAT on the LAN A and LAN B infrastructure IES to provide translation for DANs.
  - NAT configurations must match exactly between switches
- Configure NAT on the RedBox IES to provide translation for VDANs.

Figure 2-24 Network Address Translation with PRP



Since CPwE PRP implements HSRP for router (default gateway) 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
- *Stratix 5800 Managed Switches User Manual*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um012_-en-p.pdf

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) assigns IP address information from a pool of available addresses to newly connected devices (DHCP clients) in the network. In industrial networks that use DHCP, managed IES are typically configured with DHCP persistence to assign IP addresses to IACS devices based on a specific port.

DHCP is supported in the PRP topology, including DHCP Persistence.

- DHCP Persistence can be configured on the Layer 2 RedBox IES to automatically assign IP addresses to VDANs based on the port.
- DHCP Persistence can be enabled on the infrastructure IES to assign IP addresses to DANs based on the port, as long as:
  - DHCP configuration on LAN A and LAN B switches matches exactly including the DHCP pool range and the reserved addresses per port
  - A DAN is connected to the same port number on each LAN IES.
  - Reserved Only setting is enabled for the DHCP scope.
- DHCP configuration on the infrastructure IES without DHCP Persistence is not supported. The risk exists of assigning duplicate IP addresses for DANs.
- Using DHCP for SANs is not recommended. If such configuration is required, DHCP scopes in each LAN should not overlap.
- DHCP Snooping should be enabled for the DHCP scope configured on the infrastructure and RedBox IES

Time Distribution in CPwE PRP

This section provides recommendations for plant-wide or site-wide time distribution in the CPwE PRP architecture.

IACS devices use ODVA, Inc. CIP Sync technology based on the IEEE 1588™ Precision Time Protocol (PTP) to synchronize clocks in the control system. CIP Sync is designed for local and plant-wide or site-wide IACS applications requiring very high accuracies.

Industrial computers, application servers, managed IES and other network devices use Network Time Protocol (NTP) for timestamping Factory Talk® Alarms and Events.

For more information on CIP Sync, refer to:
https://www.odva.org/technology-standards/distinct-cip-services/cip-sync

For general information on designing and configuring time distribution using CIP Sync (PTP) and NTP in the plant-wide or site-wide network, refer to:

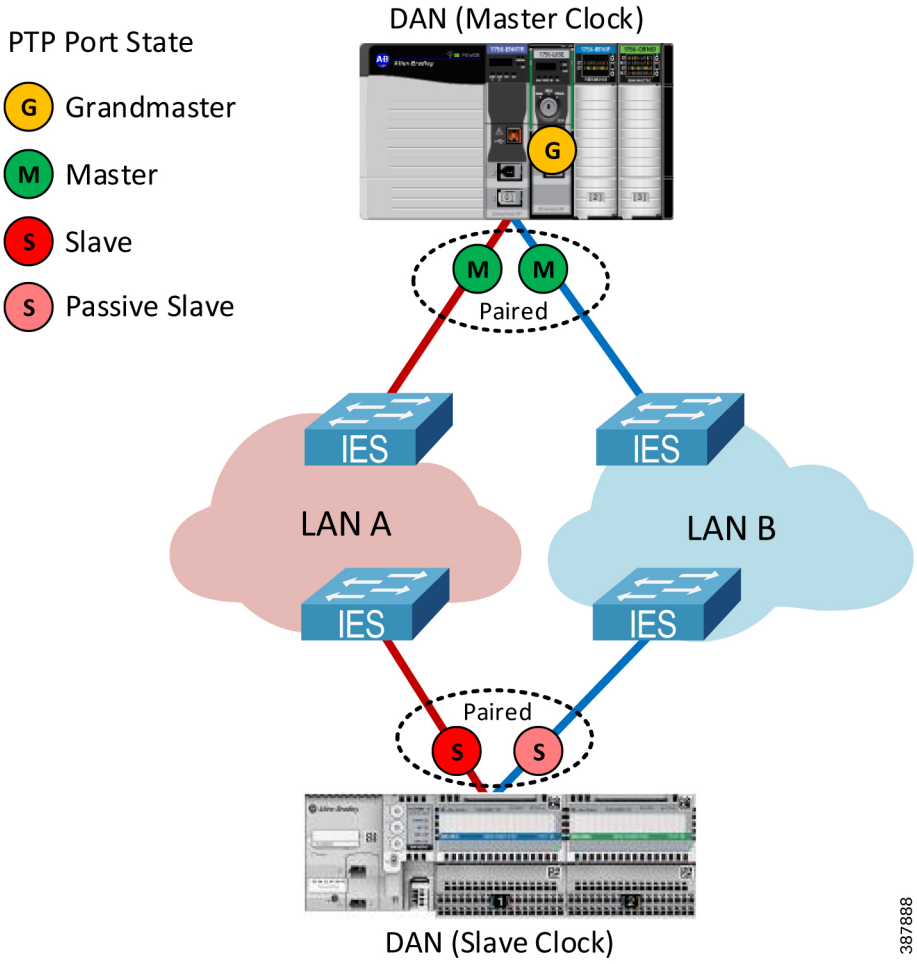
- *Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td016_-en-p.pdf

Precision Time Protocol (CIP Sync) with PRP

PRP networks support CIP Sync by implementing the doubly-attached clock model as specified in IEC 62439-3 standard (Figure 2-25):

- 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 slave port that synchronizes to the master clock, measures path delay, and tunes the clock. This port reports its state as SLAVE.
  - The other port is passive and reports its state as PASSIVE_SLAVE or PASSIVE. The passive slave port also measures path delay and maintains close synchronization to the master clock. In case of a network failure on the active slave port, the passive slave port clock transitions smoothly to the active state.
  - Either LAN A or LAN B port can be chosen as active slave port depending on the Best Master Clock Algorithm (BMCA) of the PTP protocol. As a result, some DANs can be syncing over LAN A and some over LAN B infrastructure.
- PTP traffic in the PRP network is handled differently from non-PTP traffic:
  - Ethernet frames that carry PTP information are not duplicated and exclude the redundancy trailer.
  - PTP packets from DANs, such as Sync, Delay Request and Delay Response, are generated independently for LAN A and LAN B ports.

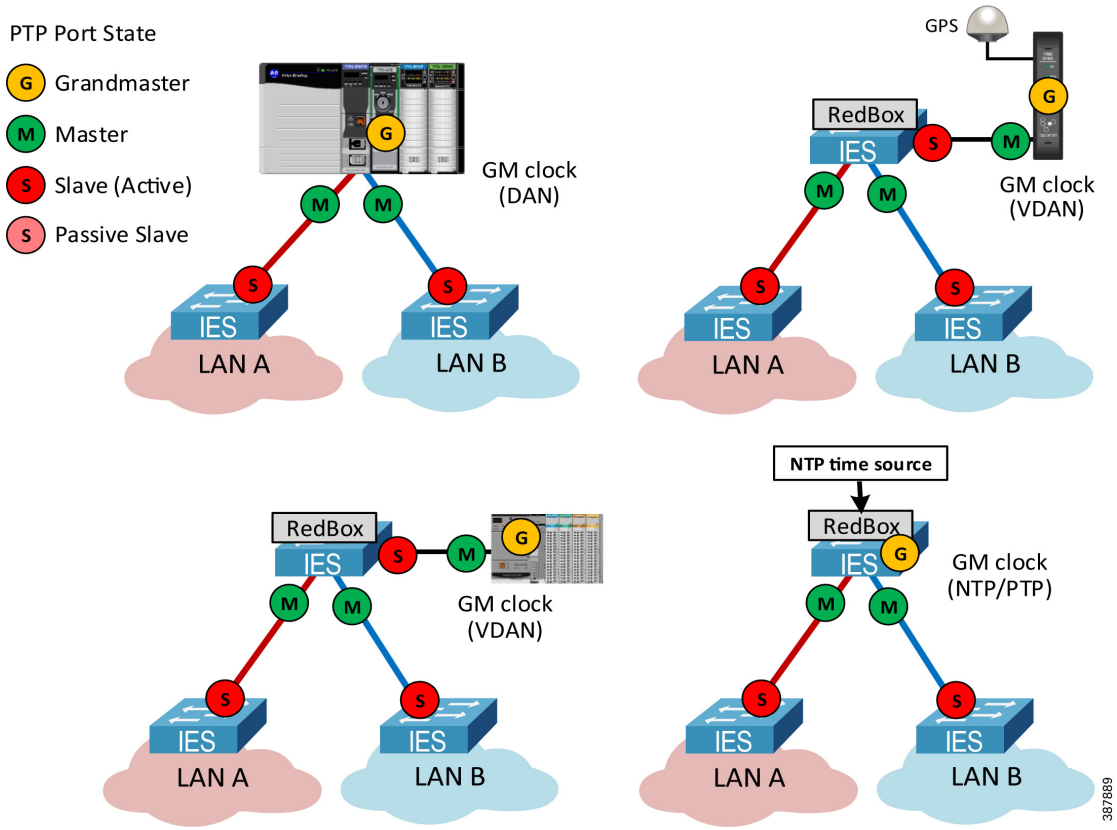
Figure 2-25 PRP Doubly Attached Clock Model



In the PTP architecture, all clocks are synchronized to a Grandmaster clock (GM). The GM must be a DAN or a VDAN and cannot be a SAN attached to LAN A or LAN B. Figure 2-26 shows some of the options for a GM in the PRP topology:

- A PAC in a chassis with an EtherNet/IP PRP module (DAN)
- A PAC (VDAN) connected to a RedBox IES
- A Global Positioning System (GPS) time module (VDAN) connected to a RedBox IES
- A RedBox IES configured as a GM in the NTP/PTP mode

Figure 2-26 Grandmaster Clock in a PRP Topology



For critical applications using time synchronization:

- Use primary and secondary grandmasters for resiliency
- Do **not** connect grandmasters as SANs (one in LAN A, another in LAN B).
- Implement measures to reduce the risk of grandmasters failing such as providing backup power to the grandmasters and network infrastructure
- Reduce the risk of simultaneous failures for the primary and secondary grandmasters by using separate network switches, redundant power supplies, and using multiple reference time sources.

Note Switchover from a primary GM to a backup GM is a system-wide event and may cause disruptions to time synchronization.

PTP Recommendations for IES

Use these guidelines for configuring IES in the CPwE PRP architecture with PTP:

- Configure Layer 2 RedBox IES as boundary clocks (BC).
- Configure Layer 3 RedBox IES as boundary clocks or as NTP/PTP clock (if RedBox IES are used as the active and backup GM).

Note Transparent clock (TC) mode or forward mode are not supported on a RedBox IES.

- Configure infrastructure IES in LAN A and LAN B as boundary clocks if time synchronization is required in multiple VLANs across PRP Cell/Area Zone
  - Use VLAN trunking for Layer 2 links between IES and make sure that the Native VLAN matches on each end of the trunk link.
- Transparent clock mode can be used on infrastructure IES in LAN A and LAN B when only one VLAN is used for time synchronization between IACS devices connected to TC switches.
  - Transparent clock IES do not propagate PTP information between VLANs.
  - PTP VLAN ID should be configured on the boundary clock IES for ports connected to the transparent clock IES.

Note Infrastructure IES without PTP support, or in the PTP forward mode, are allowed but not recommended due to lower time synchronization accuracy in the PRP architecture.

CPwE PRP architecture with GPS Reference Clock

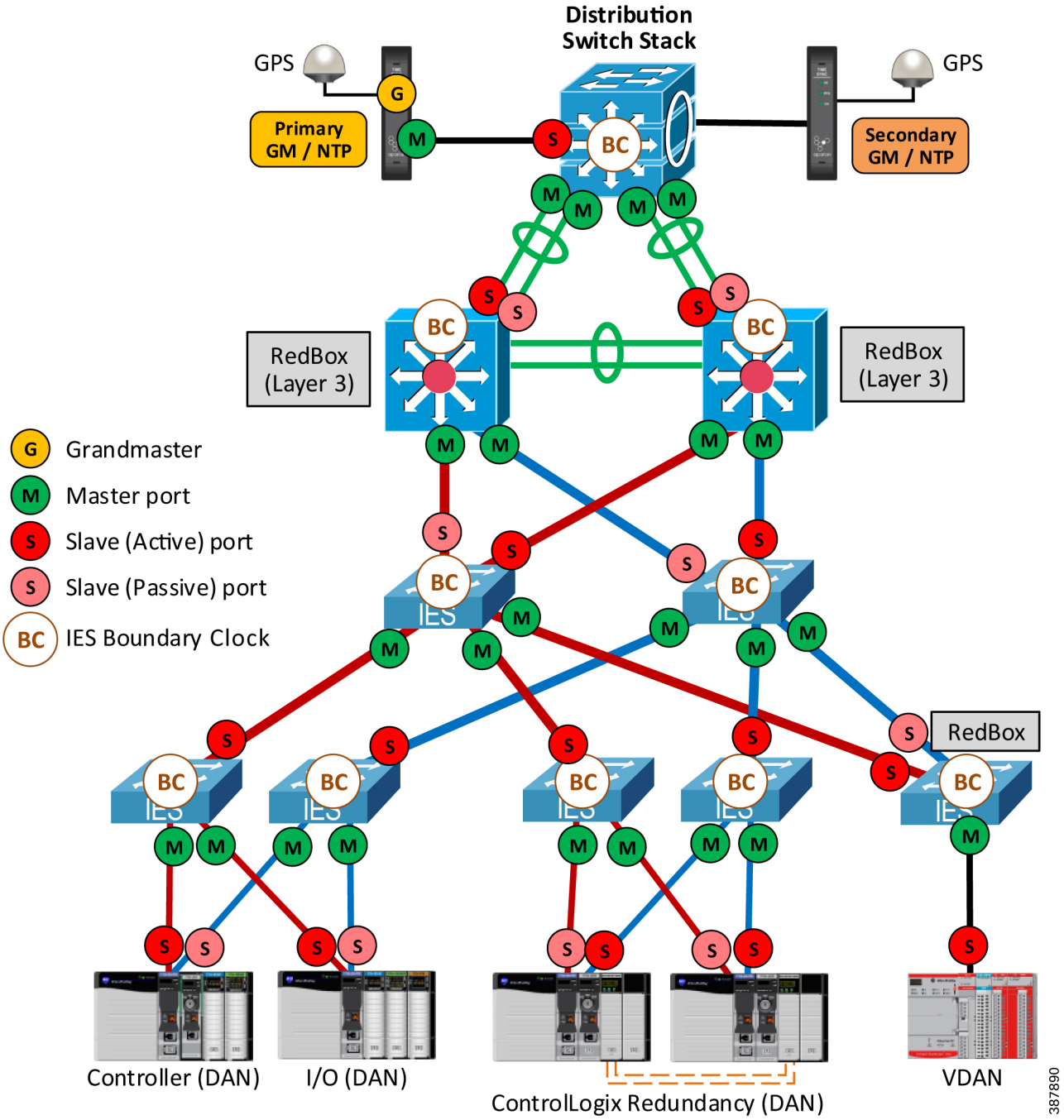
Figure 2-27 shows an example of the recommended and validated CPwE PRP architecture with redundant GPS time modules connected to the distribution switch stack.

- Time modules synchronize to GPS satellites as reference clocks and distribute time information via PTP and NTP to the plant-wide or site-wide network.
- One of the time modules is the primary GM and the primary NTP server. The second module serves as a secondary GM / NTP server in case the first module becomes unreachable.
  - Time modules should be connected to different switches in the distribution stack and should use separate power supplies and preferably separate GPS antennas.
- Cisco Catalyst 9300 switches in the distribution stack and Layer 3 RedBox IES are configured in the BC mode.

  Note PTP BC mode is supported with EtherChannels on the Cisco Catalyst 9300 starting with IOS XE 17.2.1 and on Stratix IES starting with IOS 15.2(7)E3

- Infrastructure IES in LAN A and LAN B are configured in the BC mode to enable time synchronization in multiple VLAN.

Figure 2-27 Example of CPwE PRP architecture with PTP CIP Sync - Redundant GPS Modules



Note Managed IES and other network devices use NTP for timestamping network events in logs. Both NTP and PTP must be configured in IES to correlate all events logged by the network infrastructure devices with IACS events.

Below are considerations and recommendations based on the CPwE PRP testing:

- In steady state with no network faults, time synchronization between IACS devices was maintained within the resolution of the CIP Sync modules used in the testing (< 8 microseconds).
- Switchover from the primary to secondary GM may cause temporary degradation of time accuracy for IACS devices. Time skew as much as 2 milliseconds between IACS devices was observed for a period of several seconds.
- Network events that change master clock for BC switches (LAN or RedBox) or change the active slave port on a DAN can cause similar PTP disturbances. This may include HSRP failover between Layer 3 RedBox IES, LAN A or LAN B switch faults, and various link faults in the network.
- It is recommended to use latest hardware series and firmware revisions for IACS devices and IES.
- 1756-EN4TR ControlLogix Ethernet modules (firmware 4.001 and later) and FLEX 5000 EtherNet/IP adapters are recommended for better CIP Sync performance during network faults.

Examples of PRP Architectures using NTP/PTP mode

If GPS time source is not available, time modules or Layer 3 RedBox IES can be configured as Grandmaster clocks in the NTP/PTP mode. In this case, time modules or RedBoxes use NTP servers in the Industrial or Enterprise Zone as reference clocks and provide PTP synchronization for the IACS devices in one or multiple Cell/Area Zones.

Figure 2-28 below shows an example of a PRP architecture with redundant time modules in NTP/PTP mode (without GPS) connected to the distribution switch stack. In this example, the time modules are the primary and secondary PTP GM and are the NTP servers for infrastructure devices in the Cell/Area Zone.

Figure 2-28 Example of PRP Architecture with Redundant NTP/PTP Module

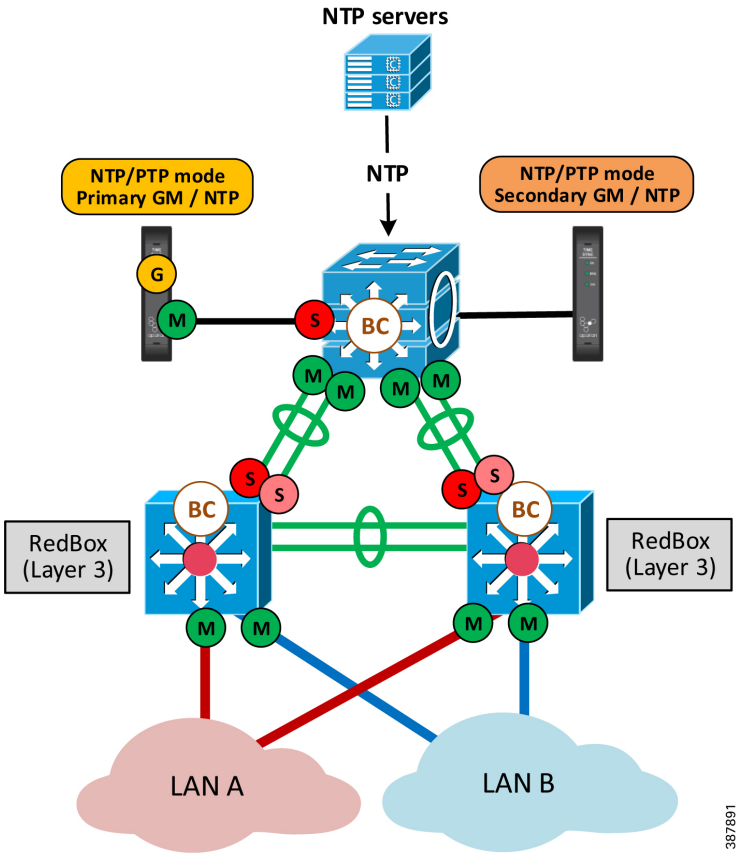
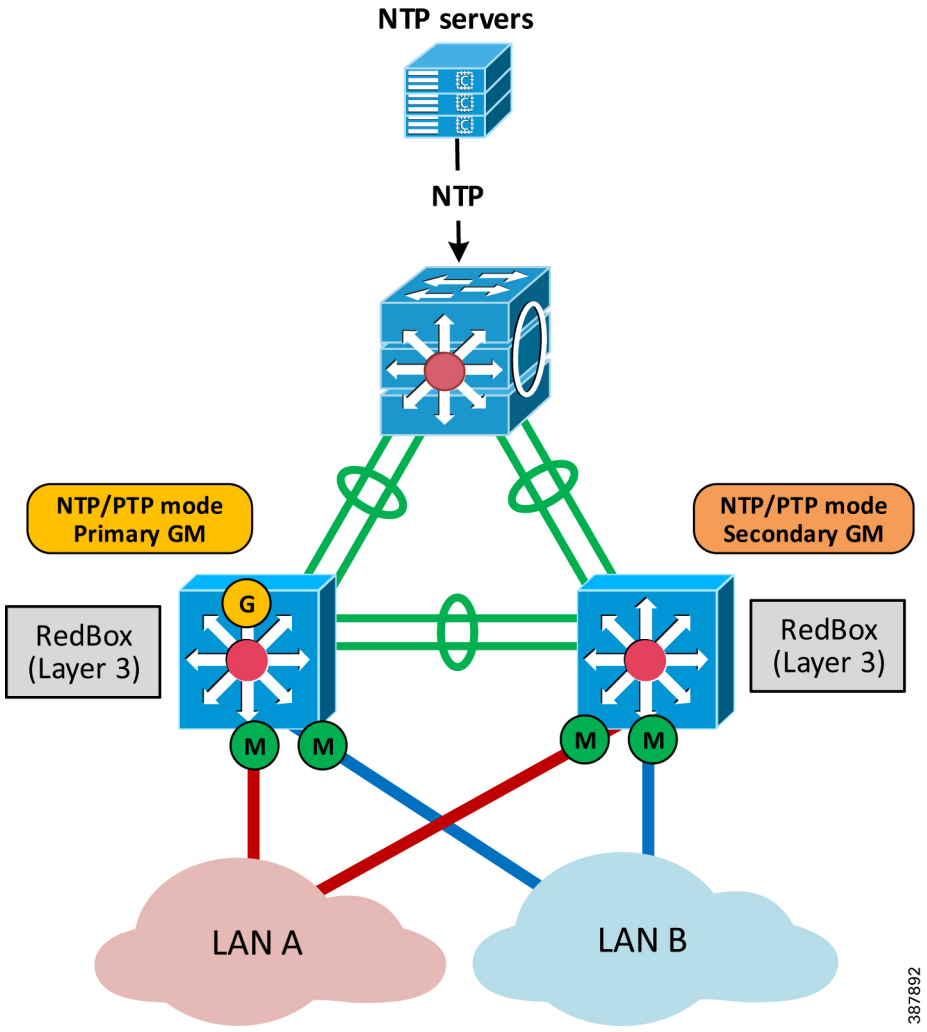


Figure 2-29 shows an example of a PRP architecture with Layer 3 RedBox IES in NTP/PTP mode. In this case, NTP is used for time distribution in the plant-wide or site-wide network, and PTP is used in each Cell/Area Zone with NTP/PTP configuration on IES.

Multiple Cell/Area Zones with PRP use separate pairs of Layer 3 RedBox IEs for NTP to PTP transition. As a result, time synchronization accuracy between IACS devices in different Cell/Area Zones depends on the accuracy that NTP can provide.

Figure 2-29 Example of PRP Architecture with NTP/PTP on RedBox IES



In both NTP/PTP architectures above, using NTP servers as reference clocks instead of GPS limits the accuracy of time synchronization. The system behavior can be impacted by network performance and availability of the NTP time sources. For example, a fault of the active NTP server and switchover to another NTP server may impact PTP time synchronization for IACS devices.

Applying PRP with IACS Applications

PRP technology is independent from 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 the 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 IEEE 1588 Precision Time Protocol (PTP)
- FactoryTalk View Site Edition
- FactoryTalk View Machine Edition
- FactoryTalk Linx
- Studio 5000 Logix Designer®

ControlLogix Redundancy with PRP

A ControlLogix redundancy system provides greater availability by establishing redundancy between a pair of controller chassis with identical components. ControlLogix redundancy is further enhanced by using high availability networks, such as PRP, to provide fault tolerance in the infrastructure.

CPwE PRP architecture has been tested with 5570 and 5580 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 system configuration included the following:

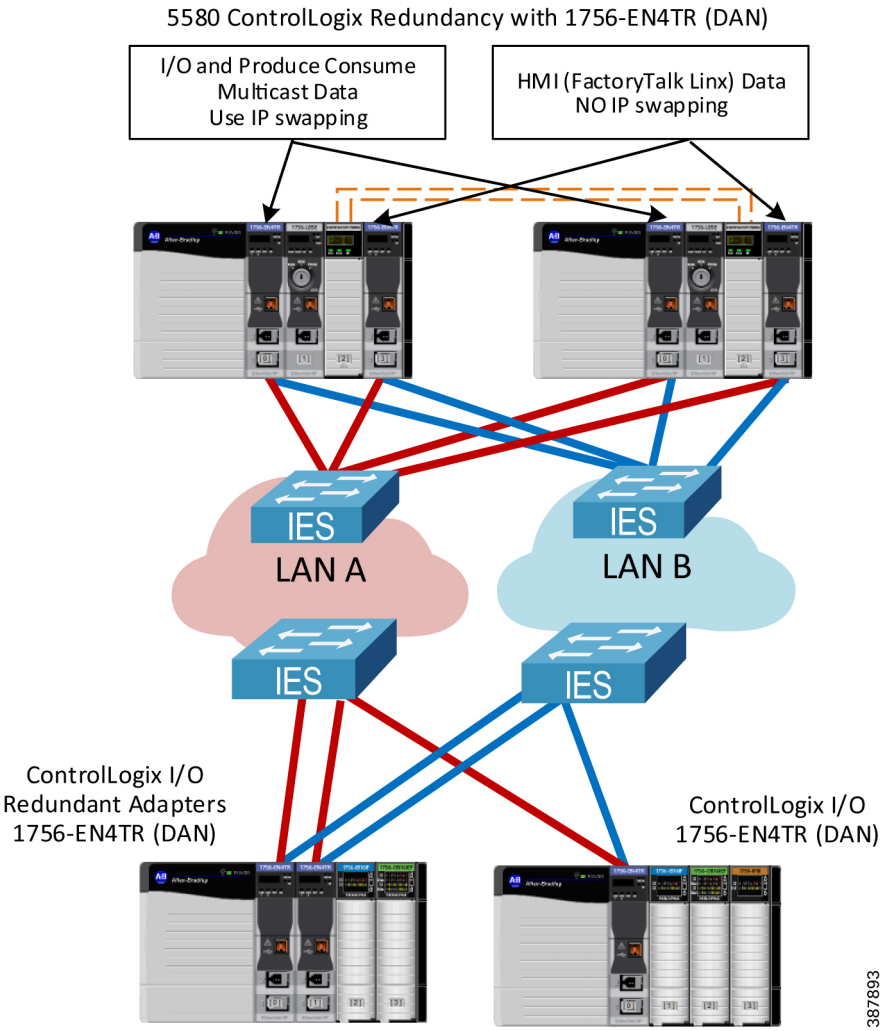
- EtherNet/IP PRP modules for I/O and Produced Consumed data configured for IP address swapping during a chassis switchover
- Dedicated EtherNet/IP PRP modules for HMI data that do not swap IP addresses
- Redundant ControlLogix Controller shortcut type in FactoryTalk Linx that provides paths to the Primary and Secondary controllers through the PRP modules with no IP address swapping.
- ControlLogix Redundancy firmware revision 31.052 or later; FactoryTalk Linx 6.11 or later.
- Infrastructure and RedBox IES configured for IGMP snooping as described earlier

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.

Figure 2-30 shows an example of a 5580 ControlLogix Redundancy system using PRP:

- 1756-EN4TR modules with PRP (firmware 4.001 or later) in the ControlLogix redundant controller chassis (version 34 or later)
- One pair of modules is dedicated for FactoryTalk Linx communication (no IP swapping)
- The second pair of modules is configured with IP swapping to support multicast I/O and Produce Consume traffic
- Single or redundant 1756-EN4TR modules with PRP in the remote I/O chassis

Figure 2-30 Example of 5580 ControlLogix Redundancy with PRP



For more information on using PRP with ControlLogix Redundancy, refer to:

- *High Availability Systems Reference Manual*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/highav-rm002_-en-p.pdf

PlantPAx Distributed Control System with PRP

The PlantPAx® Distributed Control System is an integrated control and information solution that provides Plantwide Optimization for a wide range of industries. This single-platform system is built on open industry standards to help support the seamless integration of system components, and to provide connectivity to high-level business systems.

PRP is the recommended redundancy technology for a PlantPAx system where the highest level of availability is required. A PlantPAx system design uses a CPwE PRP architecture to build a redundant network topology with infrastructure duplication, fault tolerance capability, zero recovery time within the PRP zone, and minimal recovery time for traffic leaving the PRP zone.

For more information on PlantPAx system infrastructures with PRP, refer to:

- *PlantPAx Distributed Control System Configuration and Implementation User Manual* https://literature.rockwellautomation.com/idc/groups/literature/documents/um/proces-um100_-en-p.pdf
- *PlantPAx Distributed Control System Selection Guide* https://literature.rockwellautomation.com/idc/groups/literature/documents/sg/proces-sg001_-en-p.pdf

CHAPTER 3

CPwE Parallel Redundancy Protocol Configuration

IES Configuration

This section describes how to configure Stratix IES in the CPwE PRP architecture using the recommendations provided in Chapter 2, "CPwE Parallel Redundancy Protocol Design Considerations."

Most of the recommended settings can be configured using Stratix Device Manager or WebUI interface. For information on how to do initial setup and configure Stratix IES using the web-based interface, refer to:

- *Stratix Managed Switches User Manual*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf
- *Stratix 5800 Managed Switches User Manual*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um012_-en-p.pdf

Some of the recommended steps require using Command Line Interface (CLI) as per latest Stratix firmware at the time of this publication.

- 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.
- On Stratix 5800 IES, CLI commands can be applied using the WebUI interface on the Administration - command line Interface page.

Note Configuration steps below should be adjusted and applied according to your company's network standards, practices, and specific network topology.

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 web-based Express Setup procedure (recommended), command line Interface (CLI) using serial console connection, or by transferring the configuration file to the Secure Digital (SD) card.
- Make sure that all IES in the PRP network are assigned unique management IP addresses.
- Create necessary VLANs, including the Native VLAN, per network segmentation requirements
- 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 NTP servers on each IES to make sure that network events are logged with accurate timestamps.
- Configure network protocols, security and management settings on the switch as appropriate per your company's policy and standards.
- It is recommended to apply the latest version of IES firmware. Configuration steps in this section assume the IOS version 15.2(8)E or later, and IOS XE version 17.07.01 or later.

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). For example, infrastructure switches may need to be configured first for DLR, Spanning Tree, REP, EtherChannel and so on. Refer to the Stratix switch user manuals, corresponding application guides and CPwE design guides for more information (see Appendix A).

Next steps describe required or recommended settings for infrastructure IES that are specific to the PRP operation.

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

Note After submitting the System MTU change, the Allen-Bradley 5700, 5400 and 5410 switch will restart to apply the change. The Stratix 5800 switches do not require restart.

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

PTP (CIP Sync) Configuration

If time synchronization with PTP (CIP Sync) is required for multiple VLANs in the network, it is recommended to use infrastructure IES that supports PTP in the boundary clock (BC) mode. Configure PTP settings as follows:

Step 3 Configure PTP Boundary Clock mode.

Step 4 Set PTP Priority1 as 255 (lowest priority).

Step 5 Configure on all PTP-enabled ports:

a. Announce Interval as 0 (equals 1 second in base 2 logarithmic scale)

b. Sync Fault Limit as 10,000 (nanoseconds)

Step 6 Configure PTP properties using CLI:

```
ptp time-property persist infinite
ptp transfer feedforward
```

Note If IES in end-to-end transparent clock or forward mode are used in the topology, PTP can only be implemented in a single VLAN. In this case, the PTP-enabled VLAN must be specified on the upstream ports of the closest BC switch.

IGMP Snooping Configuration

Multicast management with IGMP Snooping is recommended if multicast IACS data is present, for example when ControlLogix Redundancy or CIP Sync is used.

Step 7 Disable IGMP Querier on the infrastructure IES. Leave IGMP Snooping enabled for all VLANs.

Step 8 Enable Extended Flood option with the default value of 10 seconds (not applicable to Stratix 5800).

Step 9 Configure static mrouter on all ports in the possible path to the Layer 3 RedBox IES with HSRP (IGMP queriers) for every VLAN that has multicast traffic. This step is necessary to help prevent multicast loss in case of the querier change and recovery, e.g., after the HSRP failover. This is CLI only configuration.

```
ip igmp snooping vlan <VLAN ID> mrouter interface <PORT NAME>
```

Note In a star or linear topology, configure uplink ports to the aggregation or Layer 3 RedBox IES as static mrouter ports. In a ring topology (REP or DLR), configure both ports in the ring as static mrouter ports.

The above recommendations assume that Layer 3 RedBox IES with HSRP are configured with lowest physical IP addresses in each VLAN and take the querier role in the election process.

RedBox IES Configuration—Layer 2 (Access)

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) with a single PRP channel.

PRP Channel Configuration

Step 1 Configure ports that will be in the PRP channel group 1 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
Stratix 5800	1	Gi1/1, Gi1/2 or Gi1/3, Gi1/4

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

Step 3 Add the PRP Channel Group 1 with these settings:

a. Administrative mode: Trunk

b. STP PortFast Edge: Enabled (CLI only on Stratix 5800)

c. Native VLAN and Allowed VLAN list should match exactly the settings on the individual ports

The CLI command to enable PortFast Trunk mode on the PRP channel group is:

```
interface PRP-Channel1
spanning-tree portfast edge trunk
```

Step 4 Configure PRP Supervision Frame Option as VLAN Tagged and select VLAN ID that is used for VDAN devices.

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. The access mode for RedBox IES is out of scope for CPwE PRP.

Step 5 If PRP-enabled ports are using fiber media, Unidirectional Link Detection (UDLD) on the ports must be disabled. UDLD is not supported with PRP and will cause fiber ports to go to error-disable mode.

a. UDLD is automatically disabled on PRP ports starting with IOS 15.2(8)E and IOS XE 17.x

b. For earlier versions, use CLI configuration:

```
interface <PORT NAME>

udld port disable
```

Note After configuring a PRP channel group, do not change settings for individual ports in the PRP channel, such as switchport mode (access or trunk) or VLAN ID. Doing so may cause the port to be suspended.

Note If a PRP group channel is deleted, physical ports in the group will be administratively shutdown to help prevent unintentional loops in the network. After adding the PRP channel back, the ports will be enabled again.

Note Adding a second PRP channel group to a Layer 2 RedBox IES (Stratix 5410 or Stratix 5800) is possible but out of scope for CPwE PRP.

PTP (CIP Sync) Configuration

If time synchronization with PTP (CIP Sync) is required, configure PTP settings as follows:

Step 6 Configure PTP Boundary mode.

Step 7 Configure Priority1 value as **10** (or any value higher than the GM priority but lower than default 128). Configure Priority2 value as **1**

Step 8 Configure on all PTP-enabled ports:

a. Announce Interval as 0

b. Sync Fault Limit as 10,000 (nanoseconds)

Step 9 Configure PTP properties using CLI:

```
ptp time-property persist infinite
ptp transfer feedforward
```

RedBox IES Configuration—Layer 3 (HSRP)

The next steps describe required or recommended settings for the distribution layer RedBox IES (Layer 3 switches with HSRP) in the CPwE PRP architecture.

PRP Channel Configuration

The PRP channel configuration is almost identical to the Layer 2 RedBox steps. The only difference is that a second PRP channel can potentially be used in a large architecture with Stratix 5410 or Stratix 5800 RedBox IES (one pair of HSRP switches connected to two separate PRP Cell/Area Zones).

Step 1 Configure ports that will be in the PRP channel for VLAN trunking using the Switch for Automation Smartport template. The allowed ports are shown in Table 3-2.

Table 3-2 PRP Channel Ports

Switch	PRP Channel Group	Member Ports
Stratix 5400	1	Gi1/1, Gi1/2
Stratix 5410	1	Gi1/17, Gi1/18
Stratix 5410	2	Gi1/19, Gi1/20
Stratix 5800	1	Gi1/1, Gi1/2 or Gi1/3, Gi1/4
Stratix 5800	2	Gi2/1, Gi2/2 (expansion module)

Make sure that ports have exactly the same settings such as port speed, trunk mode, native VLAN, list of allowed VLANs and so on.

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

Step 3 Configure PRP Channel Group 1 or 2 with these settings:

a. Administrative mode: Trunk

b. STP PortFast Edge: Enabled (CLI only on Stratix 5800)

c. IGMP General Query: Enabled

d. Native VLAN and Allowed VLAN list should be the same as settings on the individual ports

The CLI command to enable Portfast Trunk mode on the PRP channel group is:

```
interface PRP-Channel1
spanning-tree portfast edge trunk
```

Step 4 Configure PRP Supervision Frame Option as VLAN Tagged and select one of the VLAN ID configured for IACS.

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.

a. UDLD is automatically disabled on PRP ports starting with IOS 15.2(8)E and IOS XE 17.x

b. For earlier versions, use CLI configuration:

```
interface <PORT NAME>
udld port disable
```

HSRP Configuration

Hot Standby Routing Protocol (HSRP) is enabled and configured on Layer 3 RedBox IES 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.

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 ending with -R, -RDC, and -RAC).

Note Stratix Device Manager configuration for HSRP is available starting with IOS 15.2(8)E2 on Stratix 5410 and Stratix 5400 IES

- HSRP commands are applied to the Switch Virtual Interface (SVI) of the VLANs.
- 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 Layer 3 RedBox IES for HSRP as follows:

a. Standby (virtual IP address): the lowest address in the subnet (typically x.x.x.1)

b. Physical IP address: second lowest in the subnet (typically x.x.x.2)

c. HSRP version 2

d. HSRP hello timer: 200 milliseconds

e. HSRP hold time: 750 milliseconds

f. Delay timers: Minimum 30 seconds, reload 60 seconds

g. Priority: 150 (or any value higher than default 100)

h. Preempt: Disabled

This is a typical CLI configuration on the primary HSRP switch for an SVI (VLAN ID and IP addresses are examples only):

```
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
```

Step 7 Configure each SVI on the secondary Layer 3 RedBox IES for HSRP as follows:

a. Standby (virtual IP address): the lowest address in the subnet (typically x.x.x.1)

b. Physical IP address: third lowest in the subnet (typically x.x.x.3)

c. HSRP version 2

d. HSRP hello timer: 200 milliseconds

e. HSRP hold time: 750 milliseconds

f. Delay timers: Minimum 30 seconds, reload 60 seconds

g. Priority: default 100 (should be lower than the primary HSRP switch)

h. Preempt: Disabled

This is a typical CLI configuration on the secondary HSRP switch for an SVI (VLAN ID and IP addresses are examples only):

```
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
```

Layer 3 EtherChannel Configuration

For additional resiliency, Layer 3 RedBox IES should be connected to the distribution switch layer 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 Layer 3 RedBox IES is configured with two Layer 3 EtherChannels: one for the uplink connection to the distribution switch, and another for a peer connection to the other Layer 3 RedBox IES.

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

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.

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

Step 11 Verify that EtherChannel status is up on both ends of the channel and ports are not suspended after connecting ports.

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.

Other routing protocols such as OSPF can be implemented but are out of scope for CPwE PRP.

Note Dynamic routing protocols like EIGRP or OSPF are only available in the Layer 3 firmware type on Stratix 5400, Stratix 5800 and Stratix 5410 IES (catalog numbers ending with -R, -RDC, or -RAC).

The following steps apply to both Layer 3 RedBox IES:

Step 12 Enable routing on the switch.

Step 13 Configure the EIGRP instance on the switch. In most cases, default settings are sufficient.

Step 14 Add network addresses and wildcard masks for IP subnets that should be routed by EIGRP. The network range should include all IP subnets associated with the PRP VLANs and IP sub-nets configured for all routed ports.

Step 15 As best practice, suppress routing updates (EIGRP Passive mode) on all ports not participating in EIGRP. For example, passive mode should be enabled on the PRP channel ports.

Step 16 It is recommended to redistribute the default route information using EIGRP from the core/distribution layer. Alternatively, a static default route to the distribution switch can be configured.

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

Step 18 Enable Extended Flood option with the default value of 10 seconds (not applicable to Stratix 5800).

PTP (CIP Sync) Configuration - Boundary Clock

This section describes steps for configuring Layer 3 RedBox IES in the recommended architecture for plant-wide or site-wide time synchronization with PTP (see Figure 2-27). In this architecture, the Grandmaster clock is connected in the distribution layer and switches in the PRP Cell/Area Zone are configured as boundary clocks.

Step 19 Configure PTP Boundary mode.

Step 20 Configure Priority1 value as **10** (or any value higher than the GM priority but lower than default 128). Configure Priority2 value as **1**.

Step 21 Configure on all PTP-enabled ports:

a. Announce Interval as **0**

b. Sync Fault Limit as **10,000** (nanoseconds)

Step 22 Configure PTP properties using CLI:

```
ptp time-property persist infinite
ptp transfer feedforward
```

PTP (CIP Sync) Configuration - NTP/PTP mode

The following steps are required **only** if the Layer 3 RedBox IES are primary and backup Grandmaster clocks (**NTP/PTP mode**) for the PTP-enabled VLANs 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 VLANs.

For recommendations on deploying and selecting NTP servers for CPwE, 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

Steps 23-29 below replace steps 19-22 in the previous section if NTP/PTP mode is used for Layer 3 RedBox IES.

Step 23 Configure at least 2 NTP servers on each IES. Three or more NTP servers are recommended to be able to detect and reject bad clock sources. Verify that the switches are successfully synchronized to the NTP source.

Step 24 Configure both Layer 3 RedBox IES (the active and standby HSRP gateway roles) in the NTP-PTP Clock mode.

Step 25 Configure PTP priorities:

a. Configure the first switch with Priority1 value **1** and Priority2 value **1** (primary Grandmaster)

b. Configure the second switch with Priority1 value **1** and Priority2 value **2** (secondary Grandmaster).

Step 26 Verify that PTP is enabled on the PRP channel ports and on the peer link EtherChannel.

Step 27 Disable PTP on the uplinks to the distribution switch (Layer 3 EtherChannel ports).

Step 28 Configure on all PTP-enabled ports:

a) Announce Interval as **0**

b) Sync Fault Limit as **10,000** (nanoseconds)

Step 29 Configure PTP properties using CLI:

```
ptp utc-offset 37
ptp transfer feedforward
```

Distribution Switch Configuration

This section describes settings for the Cisco Catalyst distribution stack that are relevant to the CPwE PRP architecture. Common configuration steps such as basic setup, configuring routed interfaces, routing protocols and EtherChannels on a Catalyst 9000 series switch, are not covered in this guide.

- For more information on configuring Cisco Catalyst 9300 platform, refer to the latest guide: https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/products-installation-and-configuration-guides-list.html

PTP Configuration

This configuration assumes that PTP GMs (primary and secondary) are connected to the distribution stack.

Upgrade the switch stack to IOS XE 17.07.01 or later. Network Advantage license type is needed for PTP support.

Step 1 Configure PTP in the boundary mode using CLI:

```
ptp transport ipv4 udp
```

```
ptp mode boundary delay-req
ptp priority1 10
ptp priority2 1
ptp time-property persist infinite
```

Step 2 Disable PTP on ports where PTP time distribution is not needed, for example on the uplinks to the core layer.

Step 3 Configure on all PTP-enabled ports:

```
interface <PORT NAME>
ptp announce interval 0
ptp sync limit 10000
```

Step 4 Connect primary and secondary GM devices to different switches in the stack. Verify PTP status on the distribution stack and in the rest of the network.

IACS Configuration

PRP-capable IACS devices do not require configuration of any PRP parameters other than enabling PRP mode (if applicable).

- Certain DANs, for example 5094-AEN2TR or 1756-EN4TR, are capable of operating in a DLR or PRP mode. These devices require enabling PRP by using a hardware selector or a rotary switch. Refer to the user manuals for details.
- To enable devices to communicate with each other across a PRP network, DAN, VDAN and SAN IP addresses must be unique. In the CPwE PRP converged architecture with multiple VLAN and routing, unique address requirements apply to any device across the Cell/Area Zone.
- For 5094 series modules, select "Status with PRP" connection type when adding to the controller I/O tree.

PTP Grandmaster Configuration

The recommended CPwE PRP architecture with PTP (CIP Sync) uses redundant time modules in the distribution layer as primary/secondary GM and primary/secondary NTP servers, with GPS as the reference clock.

The following steps apply to Aparian A-TSM modules that have been used in the CPwE PRP testing.

Step 1 Select Time Source as GPS / PTP. Enable PTP and NTP time services.

Step 2 Set CIP Sync Priority1 on both time modules to **1**.

Step 3 Set CIP Sync Priority2 to **1** on the primary module, and **2** on the secondary module.

Step 4 Verify GPS status on the time module and that it displays the correct UTC time.

If GPS signal is not available at the location, select NTP/PTP as the time source, and configure two NTP server IP addresses for redundancy.

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 Diagnostics Overview

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

The main diagnostic information for a PRP topology includes LAN Warning status and traffic statistics for individual DANs and VDANs in the node tables.

The **LAN Warning** flag indicates following conditions for LAN A or LAN B:

- Loss of communication for 3 seconds on one LAN, but not the other. This condition applies to traffic from all nodes (e.g., one of the PRP channel ports is down). The condition is cleared once communication is restored for 3 seconds.
- A DAN or VDAN Node 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 3 seconds. The condition is cleared once packets are received again within 3 seconds.
- Packets from a wrong LAN were received on one of the ports in the last second. The condition is cleared once no wrong packets are received for 1 second.

Typically, a LAN Warning condition comes up after a link fault to a DAN or a RedBox. It can also mean a misconfiguration in the network, for example cables are swapped by mistake between A and B ports, or a 2-port embedded switch device without PRP is connected to both LANs.

In non-resilient linear LAN topologies, a LAN Warning condition may indicate failure of a link or an infrastructure switch in one of the LANs.

Note Resilient LAN topologies, such as DLR or redundant star, may recover quickly after a fault and may not trigger the PRP LAN Warning flag. It is critical to monitor the infrastructure status, in addition to monitoring PRP-specific information, to be able to detect the fault and restore redundancy.

The **Node Table statistics** helps to identify the problem node during the LAN Warning condition. This data shows if packets are being received on each LAN for each known PRP node.

Note The nodes are removed from the table after a certain time if there is no traffic coming on any of the LAN. The PRP LAN Warning flag is not sustained after a complete DAN fault.

RedBox IES

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

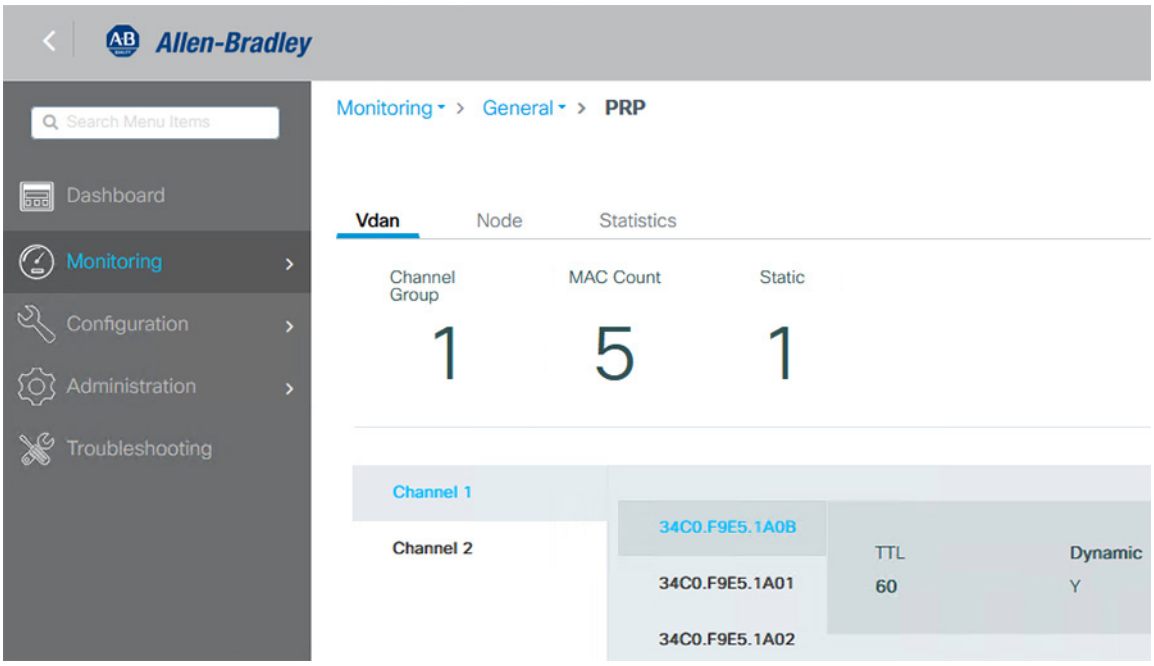
Device Manager or WebUI

Stratix RedBox IES provides information about connected VDANs on the Device Manager (Stratix 5400 and Stratix 5410) or WebUI (Stratix 5800) web-based interface. The following examples are shown using the Stratix 5800 WebUI. The Device Manager information for PRP is similar.

The Monitoring - General - PRP page displays information about VDANs connected to the RedBox, known nodes (SAN, DAN or VDAN) in the PRP VLAN, and PRP channel statistics.

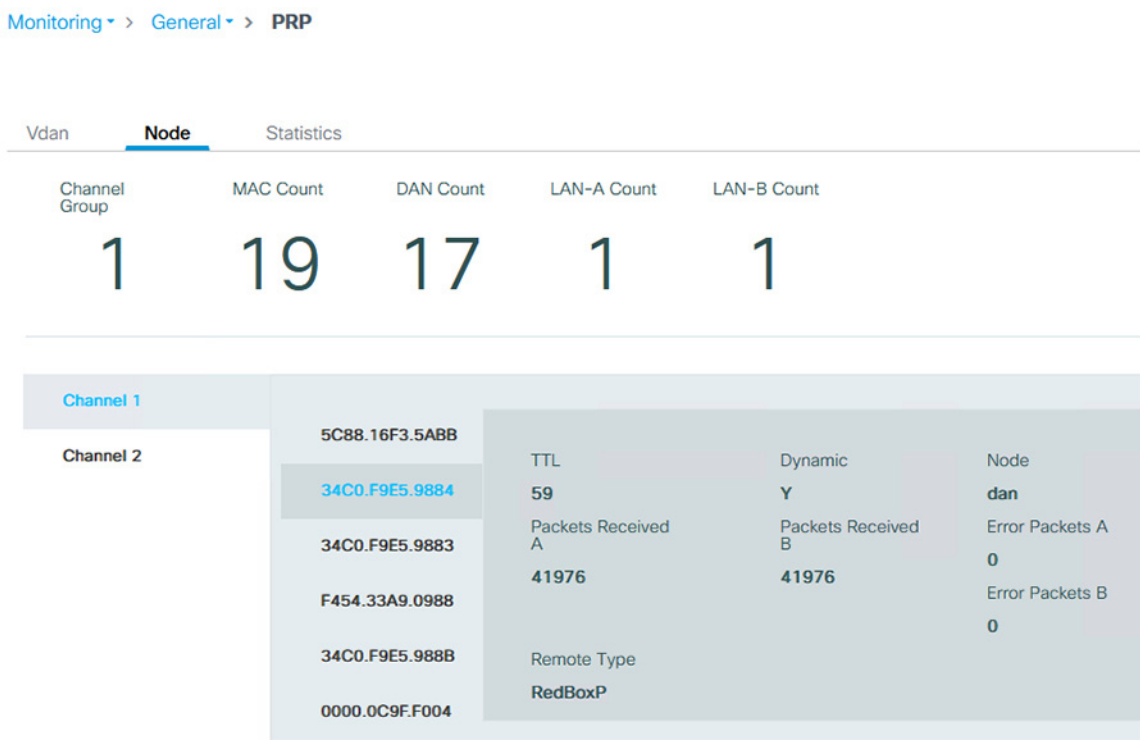
The VDAN MAC addresses are learned automatically from the switch MAC table. The RedBox IES sends PRP supervisory frames for each VDAN via the PRP channel ports.

Figure 4-1 Stratix 5800 VDAN Table



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.

Figure 4-2 Stratix 5800 Node Table



- 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.
- 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.
  - Verify if LAN A and LAN B cables are swapped on any of the modules or RedBoxes
  - Verify if any of the DAN EtherNet/IP modules is incorrectly configured in the DLR mode

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: 1
   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:

  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. The PTP data 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 detail”** command provides warning status and received count per LAN for each PRP node learned by the RedBox, including DANs, SANs, remote VDANs, and other RedBoxes. The table also shows the "last time seen" information for nodes on each LAN which helps to see what devices are impacted by the fault.

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
```

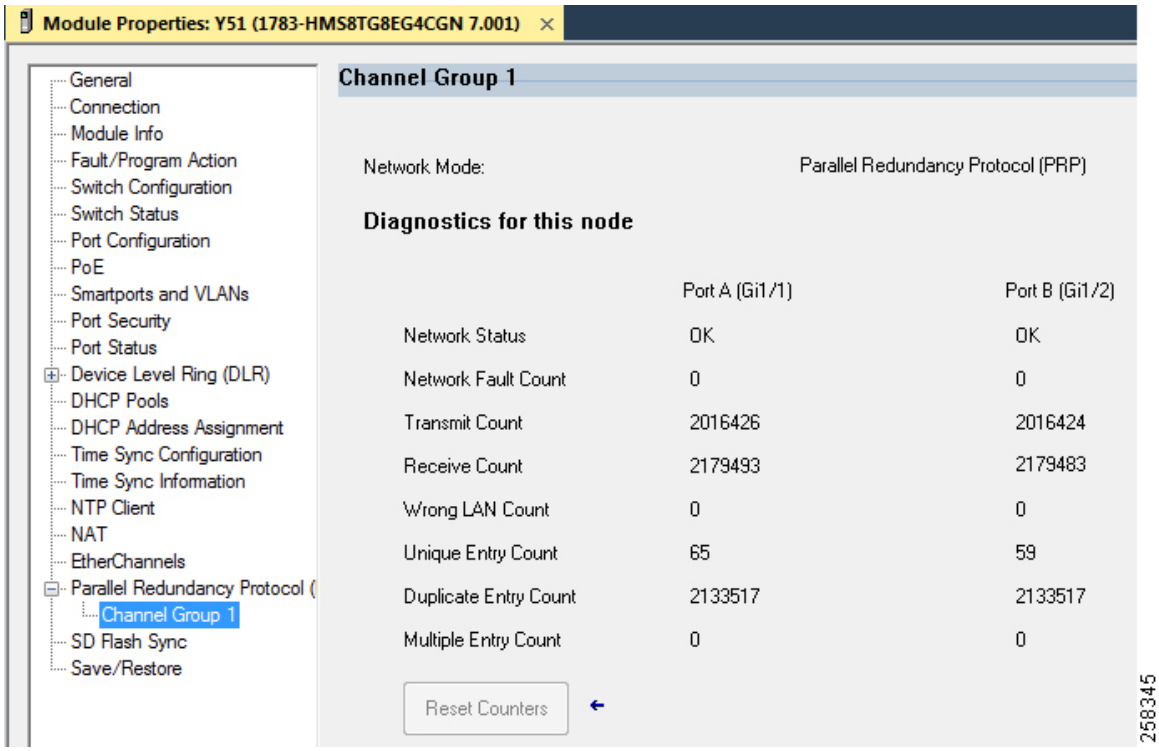
258344

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.

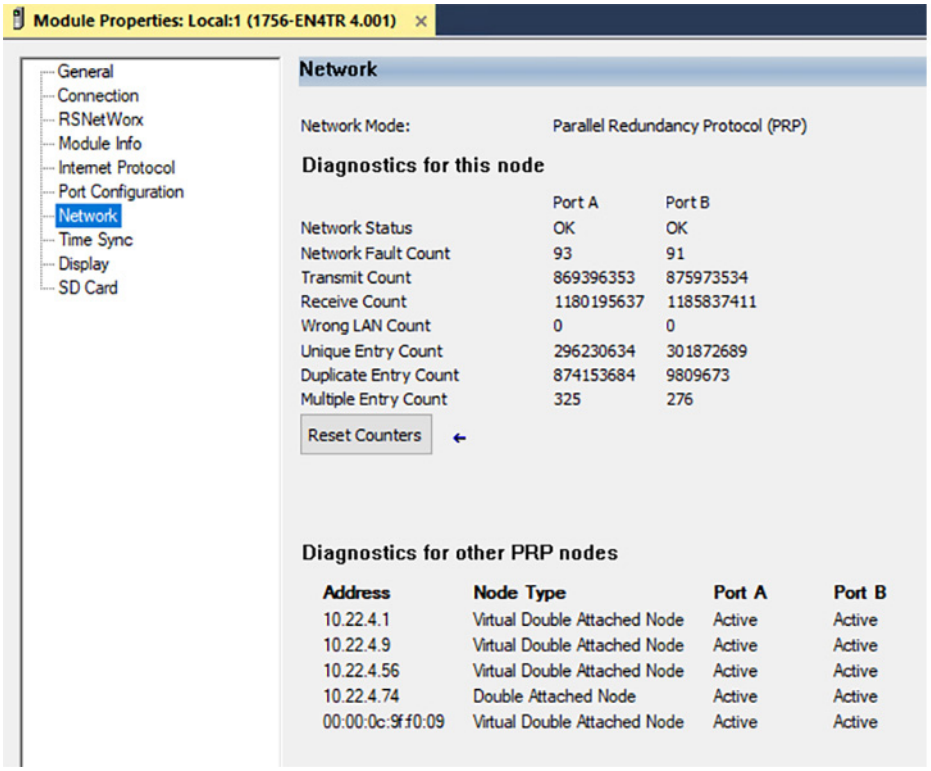
Figure 4-4 Stratix AOP



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.

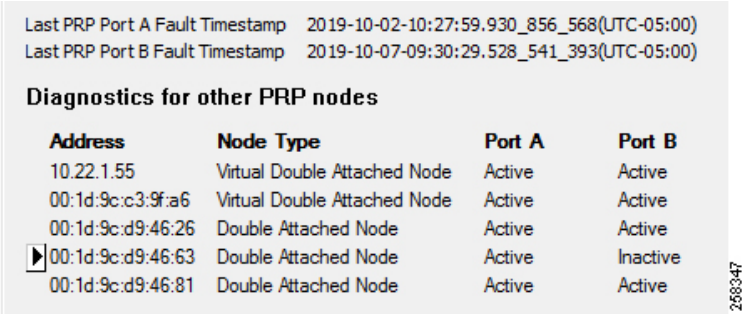
Below is an example of the PRP status page for the 1756-EN4TR module.

Figure 4-5 EtherNet/IP PRP Module AOP



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

Figure 4-6 FLEX 5000 Module AOP

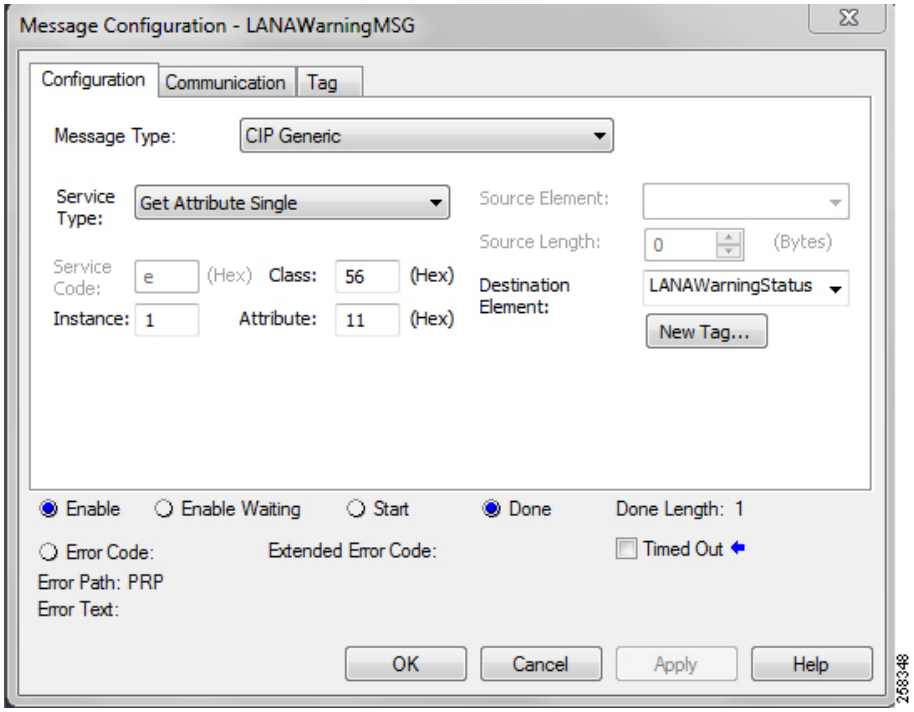


The PRP warning status for a PRP EtherNet/IP module or a RedBox can be obtained by the controller program by sending a CIP message to the device. Parameters for the message instruction are shown below.

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 Configuration



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 revision, web access to the module may need to be enabled first using AOP.

APPENDIX A

References

This appendix includes the following major topics:

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: https://www.rockwellautomation.com/en-us/capabilities/industrial-networks/design-guides.html
- *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 Device Level Ring within a Converged Plantwide Ethernet Architecture:*
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/litera-ture/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
- *Physical Infrastructure for the Converged Plantwide Ethernet Architecture Application Guide:*

  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td020_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Phy_Arch/CPwE_PhyArch_AppGuide.html

- *Deploying Identity Services within a Converged Plantwide Ethernet Architecture*:
  - 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.html
- *Securely Traversing IACS Data Across the IDMZ Using Cisco FirePOWER® Threat Defense:*
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td013_-en-p.pdf
  - Cisco site: http://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*:
  - 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
- *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
- *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 CIP Security within a Converged Plantwide Ethernet Architecture:*
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td022_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/CIP_Secu-rity/DIG/CPwE_CI PSec_CVD.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
- *Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture:*
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
  - Cisco site:
    http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.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/WP/CPwE-5-1-OEM-WP/CPwE-5-1-OEM-WP.html
- *Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture:*
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf
  - Cisco site:
    http://www.cisco.com/c/en/us/td/docs/solutions/Verti-cals/CPwE/NovCVD/CPwE_WLAN_CVD.html

Other References

- *EtherNet/IP Parallel Redundancy Protocol Application Technique*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/at/enet-at006_-en-p.pdf
- *Stratix Managed Switches User Manual*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf
- *Stratix 5800 Managed Switches User Manual*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um012_-en-p.pdf
- *High Availability Systems Reference Manual*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/highav-rm002_-en-p.pdf
- *PlantPAx Distributed Control System Configuration and Implementation User Manual*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/proces-um100_-en-p.pdf
- *PlantPAx Distributed Control System Selection Guide*
  https://literature.rockwellautomation.com/idc/groups/literature/documents/sg/proces-sg001_-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 revisions are listed in Table B-2. Rockwell Automation software versions are listed in Table B-3.

Note Unless noted otherwise, the listed hardware and firmware revisions were tested for the June 2022 release of this CVD.

Table B-1 Network Hardware and Software

Role	Product	Firmware Revision
Core switch	Cisco Catalyst 9500	17.03.02a
Distribution switch	Cisco Catalyst 9300	17.07.01 (Network Advantage license)
Layer 3 RedBox with HSRP	Allen-Bradley Stratix 5400 and Stratix 5410, Layer 3 firmware	15.2(8)E
IES Access switch, Layer 2 RedBox	Allen-Bradley Stratix 5400	15.2(8)E
IES Access switch, Layer 2 RedBox	Allen-Bradley Stratix 5800	17.07.01
IES Access or Aggregation switch, LAN A and LAN B	Allen-Bradley Stratix 5400	15.2(8)E
IES Access switch, LAN A and LAN B	Allen-Bradley Stratix 5700	15.2(8)E
IES Access switch, LAN A and LAN B	Allen-Bradley Stratix 5800	17.07.01
Time Sync Module (GPS, NTP, PTP)	Aparian A-TSM/B	1.020

Table B-2 IACS Hardware and Software

Role	Product	Catalog Number	Firmware Revision
PAC	ControlLogix 5570 (2019 CVD release)	1756-L75	31.011
PAC	ControlLogix 5580	1756-L85E	33.011, 34.011
Redundant PAC	ControlLogix 5570 (2019 CVD release)	1756-L75	31.052
Redundant PAC	ControlLogix 5580	1756-L85E	33.011, 34.011

Table B-2 IACS Hardware and Software (continued)

Role	Product	Catalog Number	Firmware Revision
PAC, VDAN	CompactLogix™ 5380	5069-L340ERM	33.011, 34.011
Safety PAC	GuardLogix® 5570 (2019 CVD release)	1756-L73S 1756-L7SP	31.011
Safety PAC	GuardLogix 5580	1756-L84ES	33.011, 34.011
Ethernet module, DAN (PAC)	ControlLogix EtherNet/IP module, PRP	1756-EN2TP	11.003
Ethernet module, DAN (PAC)	ControlLogix EtherNet/IP module, PRP	1756-EN4TR	4.001
Ethernet module, DAN (I/O)	ControlLogix EtherNet/IP module, PRP	1756-EN2TP	11.003
Redundant Ethernet module, DAN (I/O)	ControlLogix EtherNet/IP module, PRP	1756-EN4TR	4.001
Ethernet module, DAN (I/O)	FLEX 5000 EtherNet/IP Adapter	5094-AEN2TR 5094-AEN2SFPR	5.012
Ethernet module, VDAN (I/O)	POINT I/O™ EtherNet/IP Adapter	1734-AENTR/B	5.018
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 View Site Edition	12.00.00
FactoryTalk Linx	6.20.00

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 Restoration
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 businesses' 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

.

Publication ENET-TD021B-EN-P August 2022