High Availability in EtherNet/IP Systems Using Parallel Redundancy Protocol (PRP)

George A. Ditzel III
Ethernet Architect
Schneider Electric

Presented at the ODVA
2014 Industry Conference & 16th Annual Meeting
March 11-13, 2014
Phoenix, Arizona, USA

Abstract:

This paper describes how to provide high availability in EtherNet/IP™ systems using parallel redundancy protocol (PRP) for industrial automation, utility infrastructures, and tunnel applications that demand uninterrupted operation.

Critical system applications are often required to maintain high availability for all transmission, generation, distribution, and communication network components. For critical infrastructures and time sensitive processes, downtime is never allowed.

These systems may incorporate redundancy to cope with points of failure in their infrastructure. The key performance factor of redundancy is the recovery time. Recovery time is the time needed to restore normal operation after a disruption. A key characteristic of recovery time is its determinism, i.e., the certainty that the desired recovery time is met.

Stringent system applications require zero recovery (switchover) time. PRP provides zero recovery time.

Keywords:

High Availability, Availability, System Downtime, Redundancy, Parallel Redundancy Protocol

Introduction

This paper is an introduction to developing high availability for networks in EtherNet/IP systems using parallel redundancy protocol (PRP) for demanding high availability applications in industrial scenarios. This paper will provide:

- A discussion of high availability
- Introduction to the PRP network solution
- Applications of the PRP network solution
- The installation and operation of a PRP network in an EtherNet/IP system
- The fault tolerance features of a PRP network

High Availability

High availability is based on the concept of availability. The availability of a network is the probability (in percent) that the network is in service and available for use at any instant in time.

High availability is represented as a percentage, usually referred to as the *9s*. If the availability metric is specified as *five nines*, it is understood to mean that the network should be functional for 99.999% of the desired duty cycle (24-hours/day).

Availability is expressed using the following measures of reliability.

$$\text{Availability} = \text{MTTF} / (\text{MTTF}+\text{MTTR}) \quad (1)$$

where

MTTF is the mean time to failure**;** a measure of the reliability of a network, otherwise known is its failure rate. The MTTF is the interval in which the network or element can provide service without failure.

MTTR is the mean time to repair; a measure of reliability that represents the time it takes to resume service after a failure has been experienced.

As equation (1) shows, the availability of a network can be increased by designing network elements that are highly reliable (high MTTF), and/or by reducing the time required to repair the network and return it to service (low MTTR).

Since it is impossible to create networks that never fail, the key to high availability is to make recovery time as brief as possible. Availability is increased in networks by introducing redundancy.

Redundancy

High availability can be achieved economically by using techniques that detect points of failure and avoid service interruptions through redundancy in the system. There are two forms of redundancy, dynamic and static.

In dynamic (standby) redundancy the replicated components activate after a failure has been detected. Dynamic redundancy does not actively participate in the control. Switchover logic determines when to insert and activate redundancy. This requires detection and/or recovery.

In static (parallel) redundancy the replicated components are active concurrently. Static redundancy usually participates in the control. No special processing is needed on errors. The system chooses the working unit it trusts. This provides bumpless (0 ms) switchover, with continuously exercised redundancy and increased point-of-failure detection with fail-safe behavior. Static redundancy is provided at the cost of duplication

The PRP Solution

PRP is a solution that provides 100% network availability for a single point of failure using static redundancy. The PRP solution is an Open Systems Interconnection (OSI) model layer 2 protocol defined in IEC 62439-3-Ed 2.0-2012-07 standard, clause 4. The principle behind PRP networks is that they are dual redundant independent (LAN A/LAN B) networks where redundant copies of Ethernet frames travel.

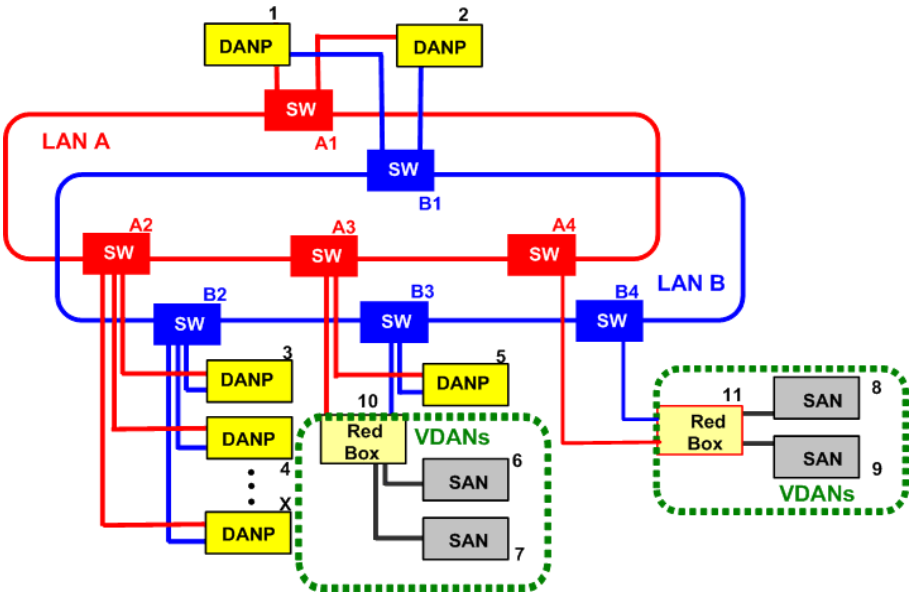

Figure 1: Example of a PRP Redundant Network

The PRP network consists of nodes of the following types:

- Double attached node implementing PRP (DANP)
- Single attached node (SAN)
- Redundancy box (Red-Box)
- Virtual doubly attached node (VDAN): a SAN visible through a Red-Box.

The nodes will be discussed in detail later in this document.

The PRP aware node (e.g. DANP, Red-Box) manipulates each Ethernet frame by appending the redundancy control trailer (RCT) to the frame before transmitting a copy on each local area network (LAN), by removing the RCT from a received frame, and selecting one frame for processing.

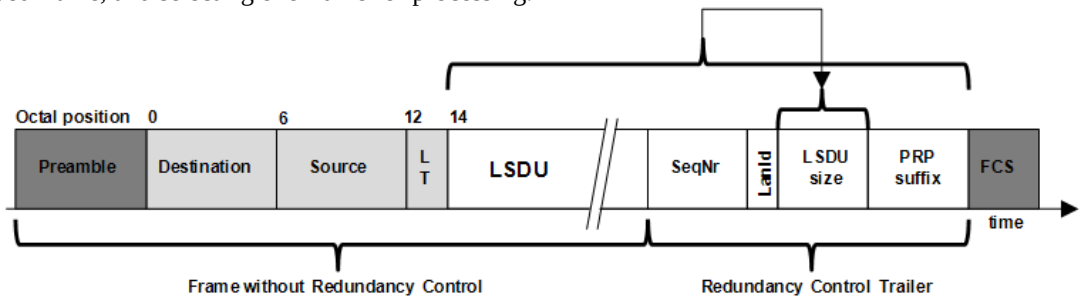

Figure 2: Ethernet Frame with Redundancy Control Trailer

Applications

The PRP solution can be applied to a variety of mission-critical systems requiring redundancy.

In a plant network, high availability can be applied to a mission-critical plant process by providing redundant control networks, and to field sub-systems by providing redundant I/O networks.

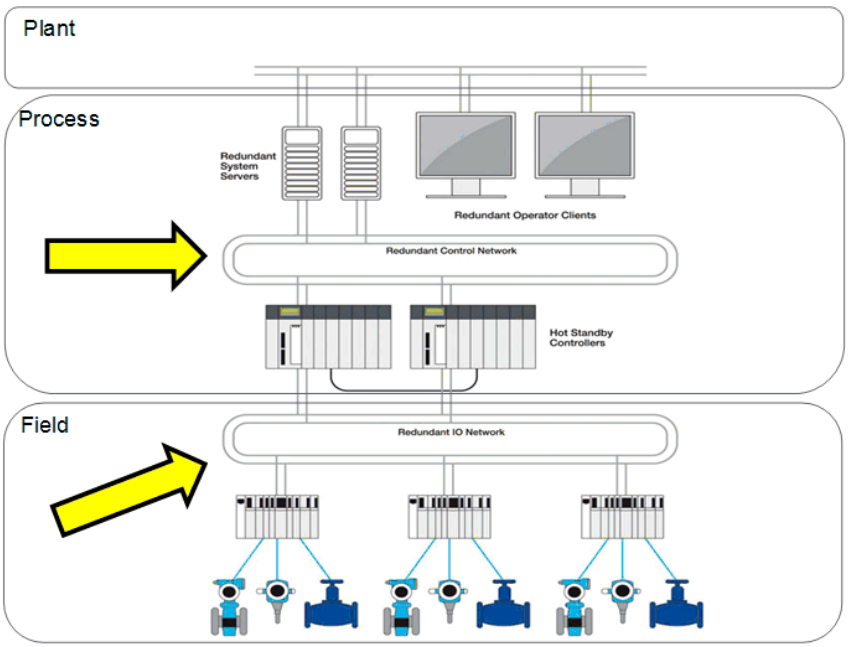

Figure 3: Redundant Plant Network Architectures

Tunnel architectures: High availability can be applied to mission-critical HVAC and fire suppression sub-systems providing independent network in inbound and outbound tunnels.

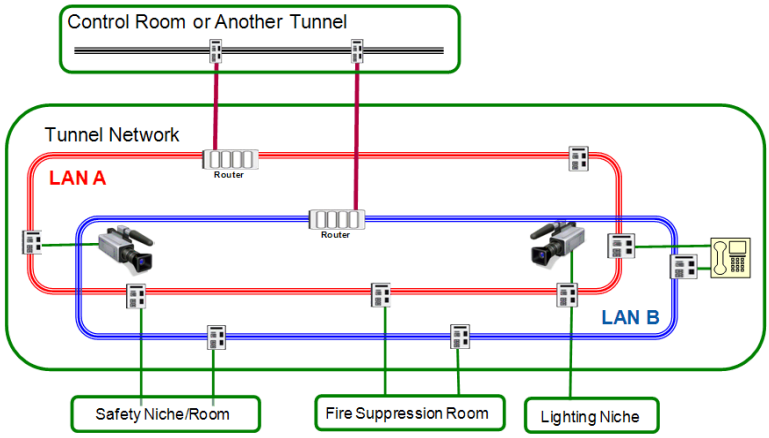

Figure 4: Redundant Tunnel Network Architectures

Marine network architectures: High availability can provide continuous control of mission-critical systems by providing independent port and starboard networks on shipboard.

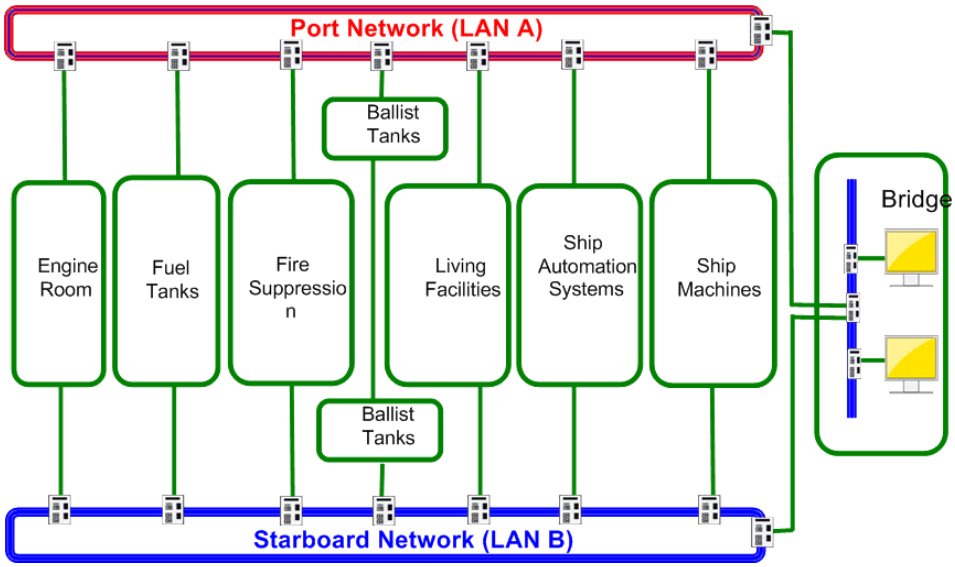

Figure 5: Redundant Shipboard Networks

The American Bureau of Shipping requires network redundancy. If a wire breaks, triggering one network/server to lose communication, a redundant network becomes the alternate communication path for uninterrupted operation.

Installation

When constructing a PRP redundant network, start with the installation of the LAN A/B networks, as in the example PRP system below. The LAN A/B networks are redundant and independent Ethernet LANs. The LANs are not interconnected. The individual LANs can be of any topology, but a ring topology is recommended for deterministic recovery and network symmetry.

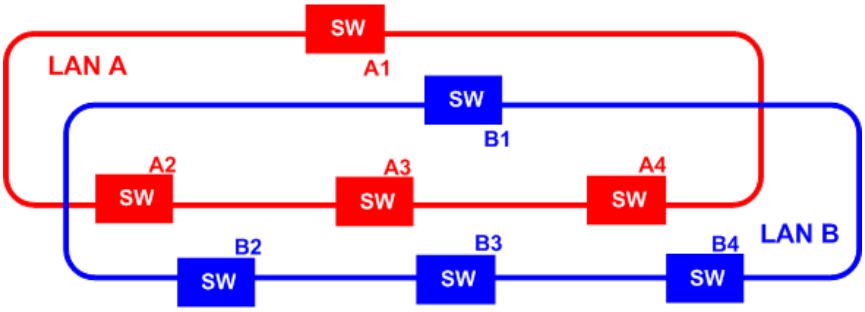

Figure 6: Dual LAN A/B Network

The Ethernet switches (SW) used in the network can be any standard Ethernet switch that supports forwarding an extended frame of 1528 bytes or greater. Switches that can forward only 1522 byte frames are not acceptable.

Each DANP (with PRP implemented) is installed into the PRP system, with each independent port attached to a separate LAN.

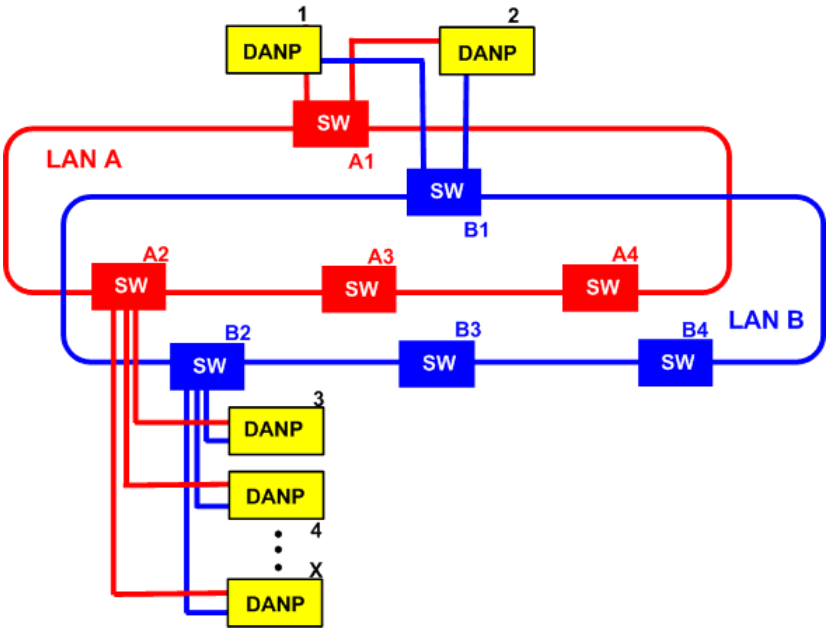

Figure 7: Installation of DANPs

A DANP is an end device that implements PRP for generating and processing the dual Ethernet frame.
IEC standard 62439-3, clause 4, indicates that SANs can be connected to either LAN A or LAN B. A SAN is a single-port end device that does not contain any PRP processing. It is attached to only one of the LANs, as SAN-6 attaches to only LAN B through switch-B3.

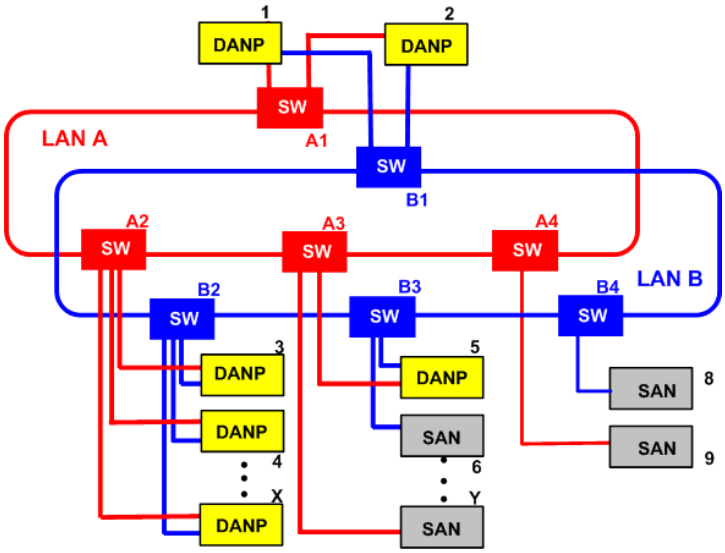

Figure 8: Installation of Single Attached Nodes SANs

In an EtherNet/IP system, directly attached SANs can cause issues with the address conflict detection (ACD) feature. One solution is to install all SANs behind a PRP Red-Box as shown in the figure below.

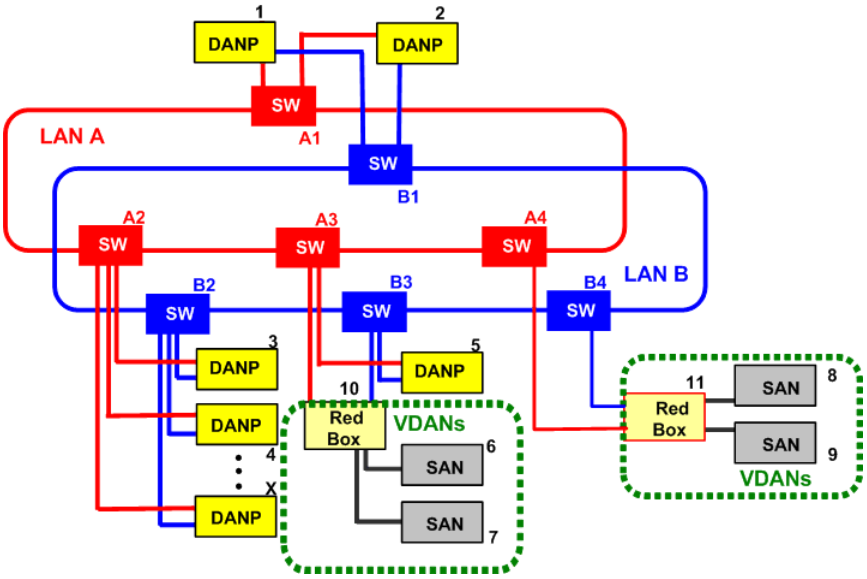

Figure 9: Installation of VDANs

The Redundancy Box (Red-Box) is a PRP proxy for non-PRP devices. Installing SANs behind a Red-Box creates Virtual Double Attached Nodes (VDANs). The use of VDANs remedies the ACD problem. There is more detail in Appendix A.

Initialization

The initialization of a PRP high availability network starts with the generation of PRP supervision frames. PRP supervision frames are used to manage redundancy and check for the presence of other DANPs and Red-Boxes. The following two figures illustrate the distribution of a supervision frame from one DANP.

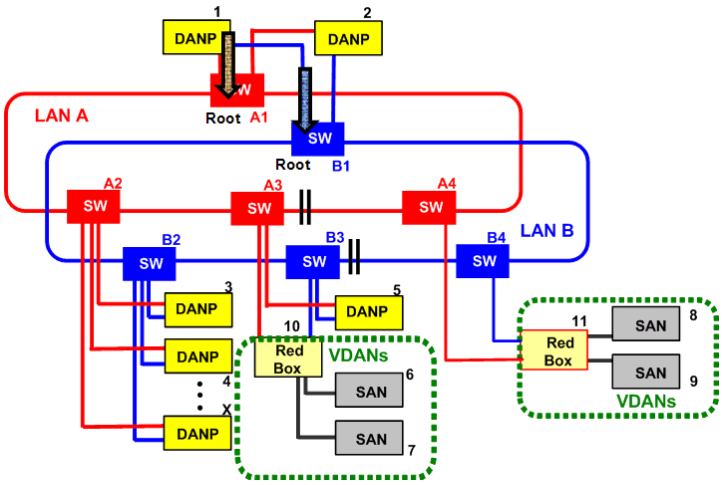

Figure 10: PRP Supervision Frame Generation

The PRP supervision frame is distributed (flooded) throughout the network and is used to identify all PRP compliant devices.

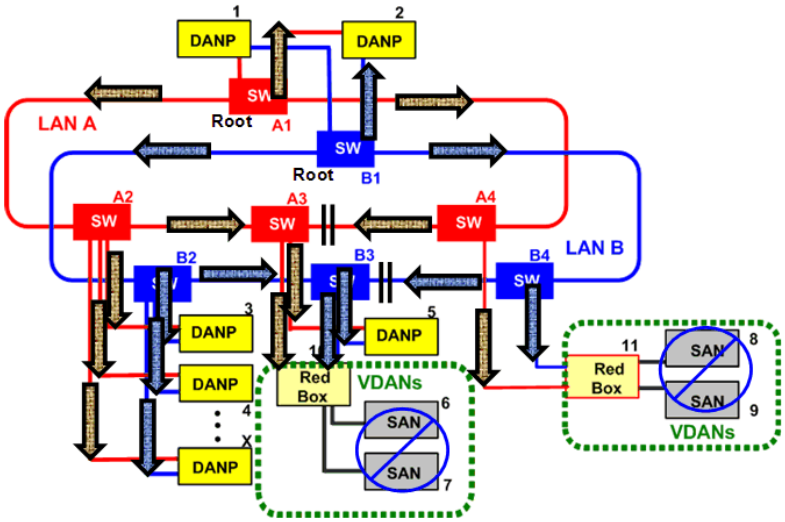

Figure 11: PRP Supervision Frame Flooding

A Red-Box should be configured to stop the transfer of the supervision frames to the SAN devices, so there is no supervision frame flooding to the SANs.

Operation

This section will describe various data frame exchanges that take place within a PRP network. One such exchange is that of a DANP transmitting a frame of data to another DANP. The originating DANP (DANP 1) generates the PRP data frame on both networks (LAN A and LAN B). The target DANP (DANP 4) receives both frames, accepting the first PRP data frame received and dropping the second.

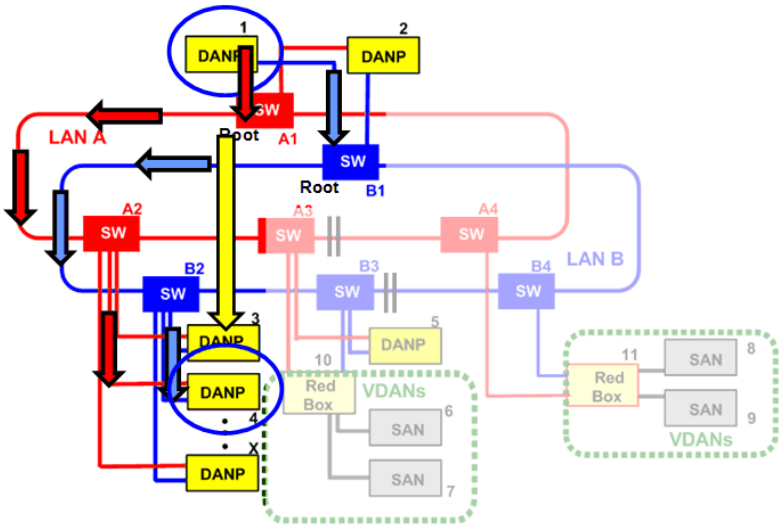

Figure 12: Originating DANP Transmission

A PRP data frame is an Ethernet frame with the PRP RCT appended to it. The target DANP (DANP 4) may then generate a response to the requesting DANP (DANP 1) in the same fashion.

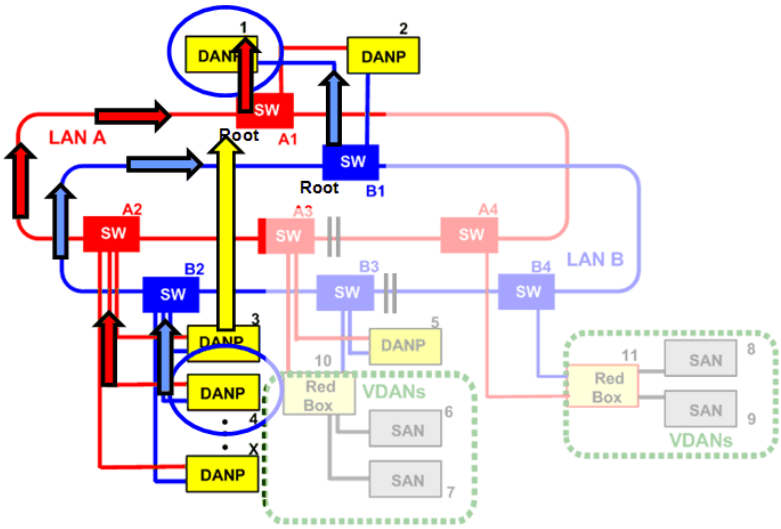

Figure 13: Target DANP Transmission

Another illustration of a PRP data frame transmission is that of a DANP transmitting a PRP data frame to a SAN or VDAN. The originating DANP (DANP 1) generates the data frame on both networks (LAN A/B). The Red-Box (RB 10) captures the frames from both networks and processes both frames.

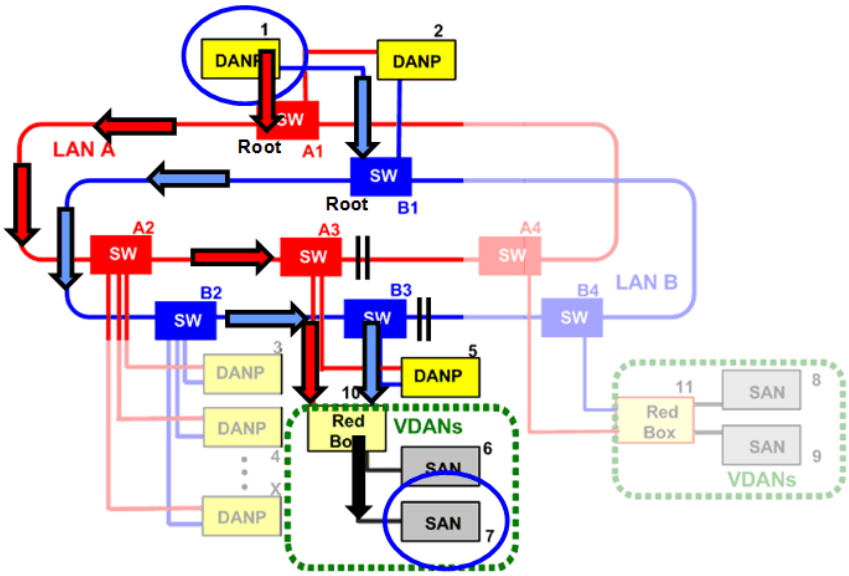

Figure 14: DANP to SAN Transmission

The processing involves selecting one frame, stripping off the PRP trailer, then sending the sanitized frame to the target SAN (SAN 7). The SAN (SAN 7) may transmit a frame to the DANP (DANP 1). The Red-Box (RB 10) appends the RCT to the frame and transmits one copy of the frame to each of the LAN networks.

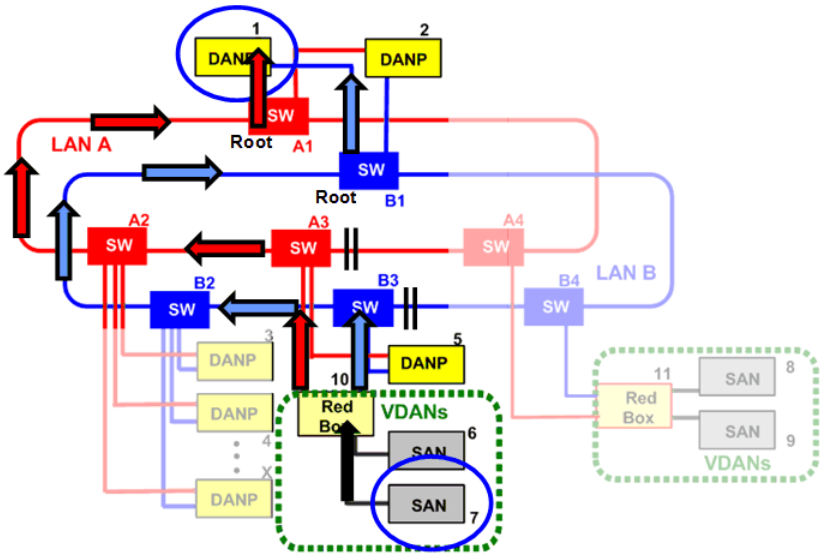

Figure 15: SAN to DANP Transmission

Alternatively, when a SAN (SAN 7) sends a frame for the first time, the Red-Box (RB 10) generates a supervision frame indicating the Red-Box is a proxy for the SAN (SAN 7).

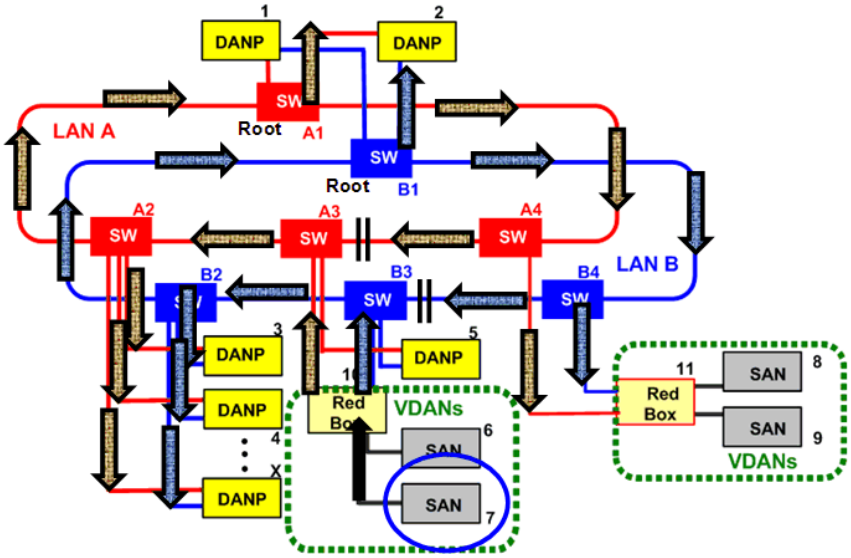

Figure 16: Alternative SAN Transmission – Supervision Frame

The Red-Box (RB 10) also appends the RCT to the data frame and transmits a copy of the data frame on each network.

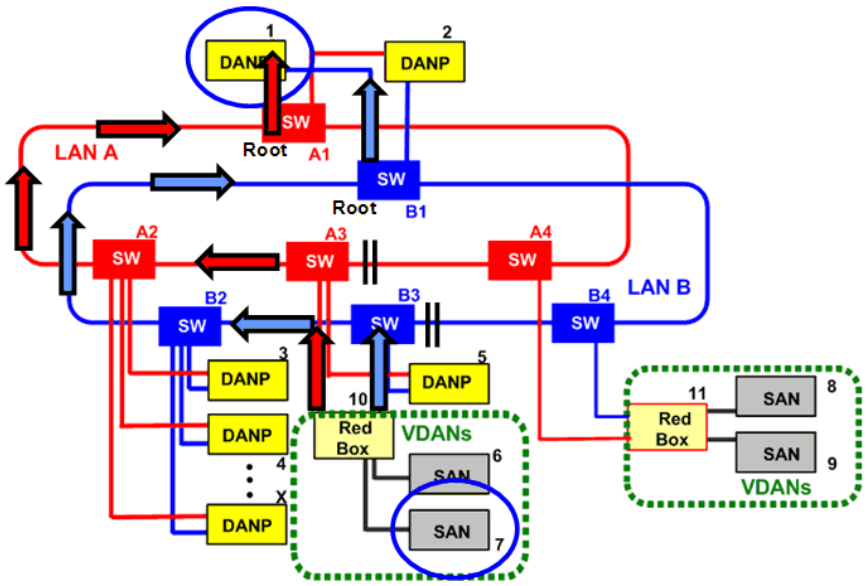

Figure 17: Alternative SAN Transmission – Data Frame

Fault Recovery

The real benefit of PRP is seamless recovery. The points of failure illustrated in this section are: a broken cable, an inoperable network device, an incorrectly designed redundant LAN, and an inoperable Red-Box .

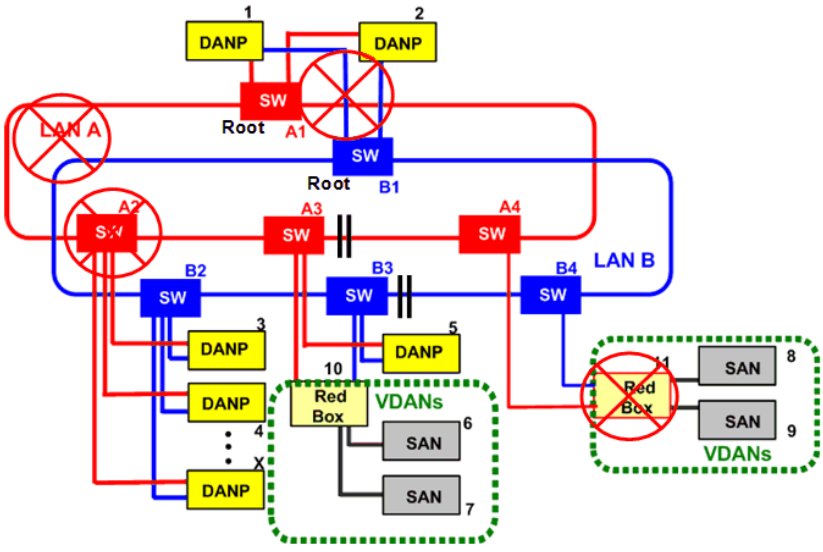

Figure 18: Various Network Faults

The broken cable in this example is the cable connecting DANP1 to Ethernet switch B1 of LAN B. DANP1 transmits a frame to SAN 7. The frame travels only on LAN A. The Red-Box (RD 10) processes the frame and sends the resultant frame to SAN 7.

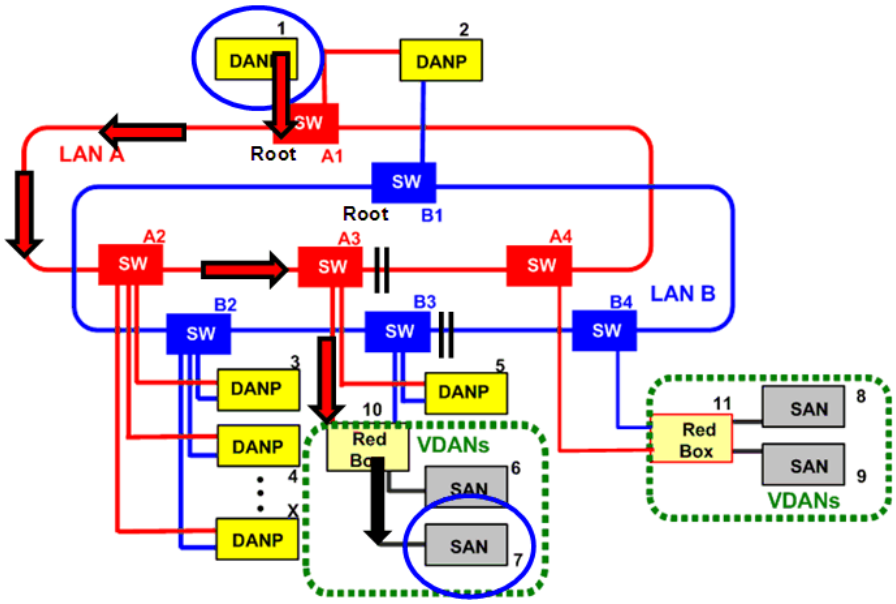

Figure 19: Cable Fault – DANP Transmitting

After a period of time, the SAN 7 may send a frame to DANP 1. This frame is processed by Red-Box 10 and received by DANP 1 on the LAN A connection. The DANP may have been deleted from the filter databases of the Ethernet switches on LAN B. If this has occurred, the frame generated by the Red-Box on LAN B is broadcast on LAN B because the destination is no longer known.

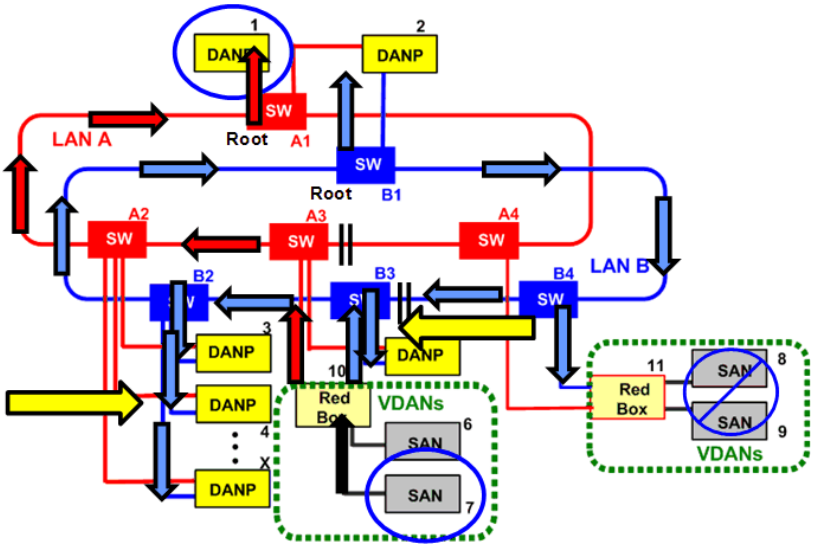

Figure 20: Cable Fault – SAN Transmitting

The use of a PRP implementation option known as the nodes table identifies when communication is lost to a node on a particular LAN

In the inoperable network device, the Ethernet switch A2 is illustrated to have completely failure. The SAN (SAN 7) transmits a frame; the frame is processed by Red-Box 10 which transmits one copy of the frame on LAN A and one copy on LAN B.

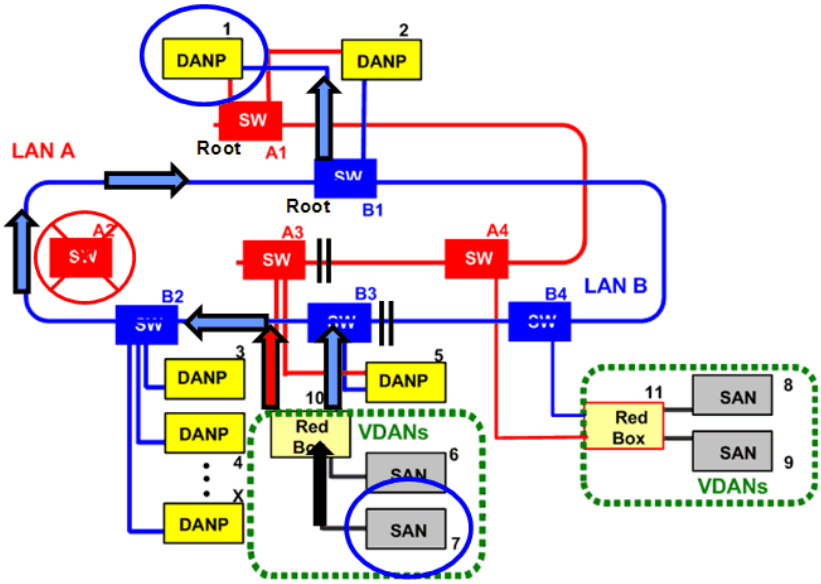

Figure 21: Network Device Fault – Before Network Healing

The frame may be sent before LAN A has had time to reconfigure the network. The frame is then stopped on LAN A at switch A3 as there is no place for it to go. However, the frame is received by DANP 1 on the LAN B connection, as LAN B has not been interrupted.

The frame may later be transmitted and received on both LANs once LAN A has time to re-establish communications on the network. Each copy of the frame traverses the LAN A and LAN B networks.

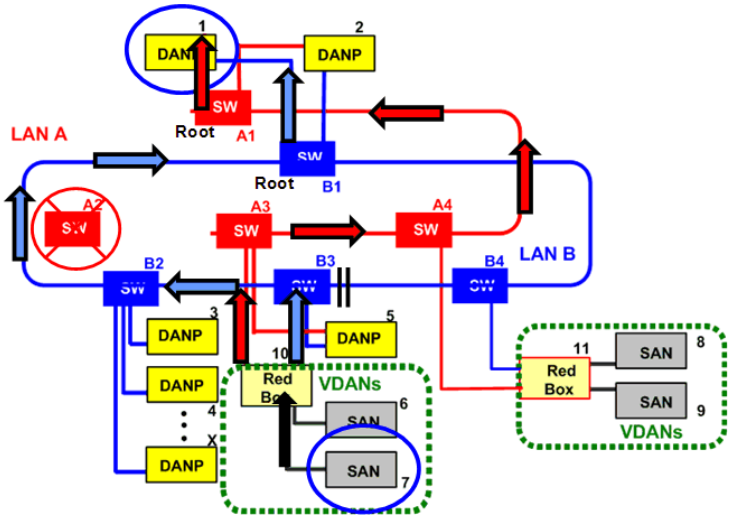

Figure 22: Network Device Fault – After Network Healing

The following illustration shows a redundant LAN where LAN A completely fails. The frame is stopped on LAN A at switch A3 because there is no place for it to go.

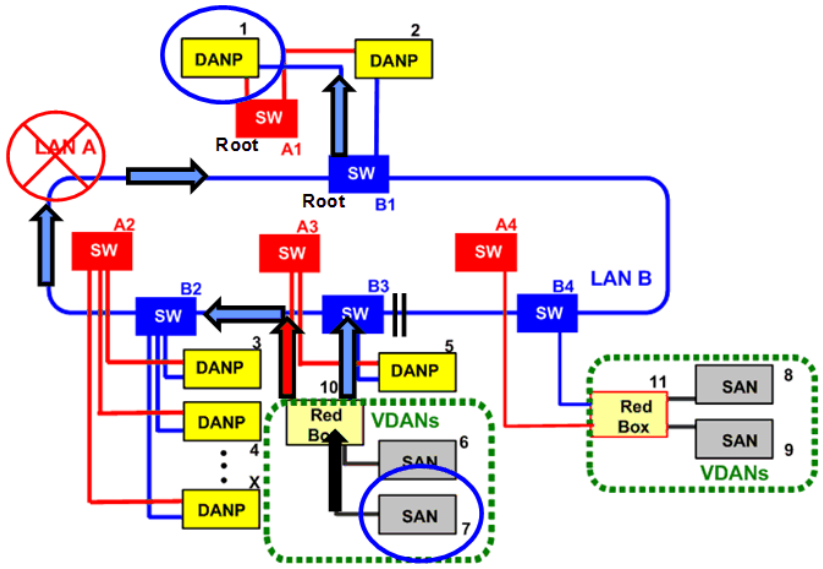

Figure 23: SAN Transmits on LAN B Only

However, the frame is received by DANP 1 on the LAN B connection because LAN B has not been interrupted.

The Red-Box is a single-point failure in the network connecting single attached node (SAN) end devices to the network through Red-Boxes, always creating a single-point-failure zone.

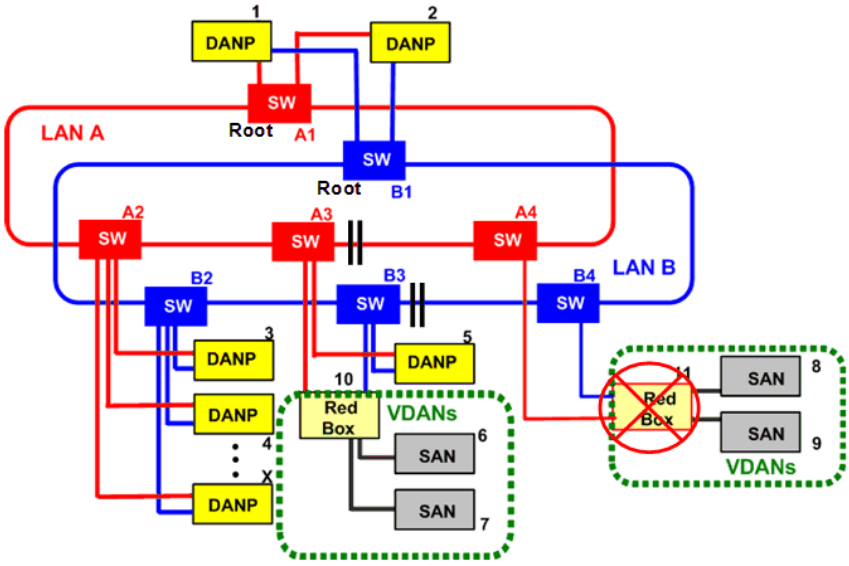

Figure 24: Red-Box as Single Point Failure

But if a double attached node implementing other protocols (DANO) supports a ring protocol, then the single-point failure can be removed using dual coordinated Red-Boxes that support the selected ring protocol.

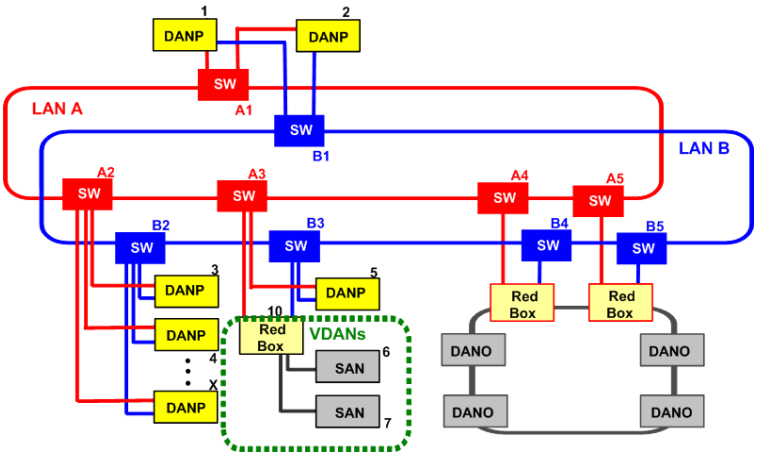

Figure 25: Red-Box Single-Point Failure Solution

Measures have to be taken to make sure that the redundant Red-Boxes do not activate their perspective interlinks the same time, but coordinate interlink activity during operation as well as when there is a failure. This is outside the scope of the PRP specification.

Appendix A

Directly attached SANs can cause some issues with the ACD feature of an EtherNet/IP system. A SAN (SAN Y), with IP address X, broadcasts an ARP probe on one network (LAN A) but not the other network (LAN B). A SAN (SAN 8) with the same IP address (X) on the other network (LAN B) does not see the ARP probe. The ACD algorithm does not operate correctly, leaving the two SANs with the same address.

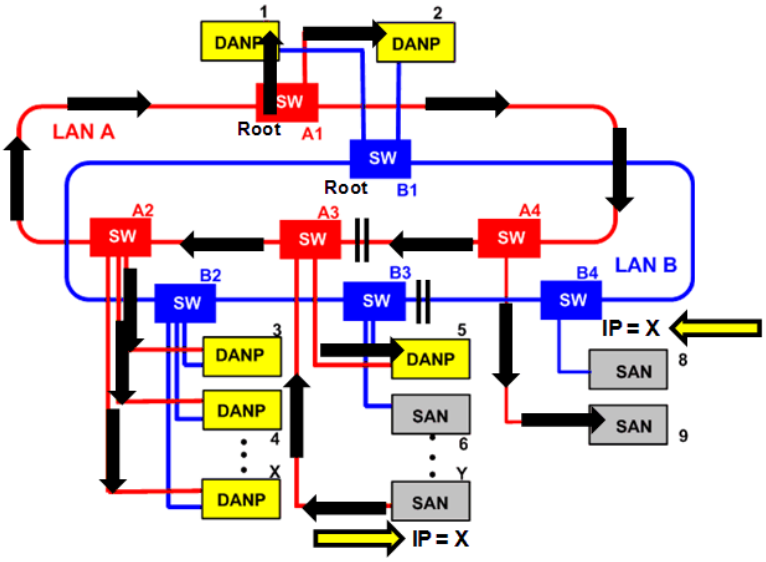

Figure 26: Directly Attached SANs

The solution to this problem is to install all SANs behind a PRP Red-Box creating virtual double attached nodes (VDANs). With VDANS, the SAN (SAN 7) ARP probe broadcasts on both networks and is seen by the other SAN (SAN 8).

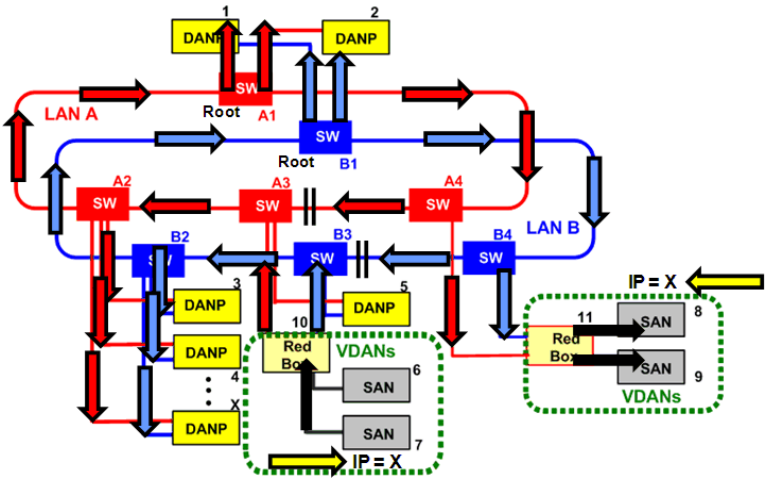

Figure 27: Virtual DANs

The ACD algorithm then operates correctly in resolving the conflict. The use of the nodes table can identify if any SANs are connected directly to the LAN A or LAN B network.

References:

IEC 62439-1 Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods, Ed 1.0 2010-02

IEC 62439-3 Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)