# High Availability - Guidelines for Use of DLR in EtherNet/IP Networks

Jordon Woods
Director, Deterministic Ethernet Technology Group
Analog Devices, Inc.

February 22, 2017

# Abstract

With the addition of the Device Level Ring (DLR) protocol to the EtherNet/IP specification, there was concern that end users might not fully understand the ramifications of the protocol on network infrastructure, especially with respect to other resiliency protocols. While all of the information contained herein is contained also in the specification, it is hoped this overview will clarify these implications.

This whitepaper is intended to provide an overview of DLR and to provide guidelines for implementing a DLR network comprised of DLR and non-Non-DLR devices. It is intended for those manufacturing or IT professionals responsible for specification, implementation or deployment of networks utilizing EtherNet/IP technologies.

Making this paper available to the masses of ODVA CIP users, will ease the pains of integrating this technology at the end user site.

# Why a DLR Whitepaper?

- In 2009, ODVA added the DLR Protocol to CIP Toolbox.
- Device Level Ring (DLR) protocol provides a means for detecting, managing and recovering from faults in a ring-based network.
- Implementation of DLR imposes certain requirements upon the supporting network infrastructure.
- The Infrastructure SIG has been tasked with developing a set of guidelines for implementing a DLR network comprised of DLR and Non-DLR devices.
  - It is intended for those manufacturing or IT professionals responsible for specification, implementation or deployment of networks utilizing EtherNet/IP technologies.
  - Available to all users (i.e. in the public area of the ODVA Website)
  - published as PUB00316R0 (https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00316R0_Guidelines_for_Using_Device_Level_Ring_(DLR)_with_EtherNetIP.pdf).

# DLR Whitepaper TOC

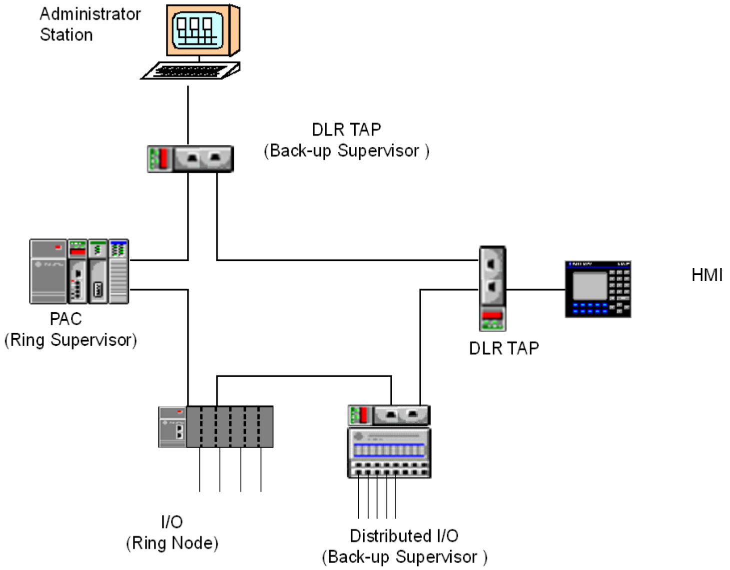
## Contents

# DLR Overview

- **Ring Supervisor**
  - At least one device must be configured to act as the Ring Supervisor
  - Sends beacon and announce messages
  - Prevents messages from circulating
  - Reconfigures on ring break and restoration
  - Multiple supervisors supported (algorithm to determine who is active supervisor)
  - It is strongly recommended that at least one additional device be capable of acting as a back-up ring-supervisor
- **Ring Node, Beacon-based**
  - Required to process beacon frames within a specified beacon interval (100-400 uS)
  - Participates in fault detection (Check Neighbor Process, Fault Detection Process)
  - Upon fault detection, reconfigures & relearns the network topology (Ring Recovery Process)
- **Ring Node, Announce-based**
  - Required to process announce frames (1 second interval)
  - Participates in fault detection (Check Neighbor Process, Fault Detection Process)
  - Upon fault detection, reconfigures & relearns the network topology (Ring Recovery Process)

# DLR Operation

- A DLR network consists of an active Ring Supervisor and any number of Ring Nodes
- Sends beacon and announce frames on both ports
- Ring Supervisor must be capable of blocking traffic on one port to avoid loops
- Faults are detected when beacon traffic is interrupted and/or link/node failure is detected by adjacent nodes.



# Devices which do not support the DLR protocol

- **Non-DLR Device**
  - Any device not supporting the DLR protocol but which complies with all of the guidelines outlined in the whitepaper.

- **Non-compliant Device**
  - A Non-DLR device that fails to comply with one or more of the guidelines outlined in the whitepaper.

**<u>Note: The use of Non-DLR devices is strongly discouraged throughout the whitepaper. Non-compliant devices are considered unsupported.</u>**

# Devices which do not support the DLR protocol

**Required Features**

- Disable unicast MAC learning on those ports connected to the DLR ring

- IEEE 802.3 operation:
  - Auto-negotiation, with 10/100Mbps, full/half duplex
  - Forced setting of speed/duplex
  - Auto MDIX (medium dependent interface crossover), in both auto-negotiate and forced speed/duplex modes. Note: This is a PHY and transformer issue, not an embeddedswitch issue.

- QoS:
  - 2 queues
  - High priority queue for DLR frames, with strict priority scheduling for the high priority queue
  - Prioritization via 802.1Q/D. Usage shall be consistent with the EtherNet/IP QoS scheme shown in Table 3. For non-IP frames the priority in the 802.1Q header should be used.

**Recommended Features**

- QoS:
  - 4 queues
  - Prioritization via DSCP Usage shall be consistent with the EtherNet/IP QoS scheme. For IP frames the switch should use the DSCP value.

# Devices which do not support the DLR protocol

- **Configuration Requirements**
  - Quality of Service (QoS) based upon either the Differentiated Services Code Point (DSCP) or the 3-bit priority field in the VLAN ID

| Traffic Type | CIP Priority | DSCP | 802.1D Priority[1] | CIP Traffic Usage (recommended) |
|---|---|---|---|---|
| PTP Event (IEEE 1588) | n/a | 59 ('111011') | 7 | n/a |
| PTP General (IEEE 1588) | n/a | 47 ('101111') | 5 | n/a |
| CIP class 0 / 1 | Urgent (3) | 55 ('110111') | 6 | CIP Motion |
| | Scheduled (2) | 47 ('101111') | 5 | Safety I/O<br>I/O |
| | High (1) | 43 ('101011') | 4 | I/O |
| | Low (0) | 39 ('100111') | 3 | No recommendation at present |
| CIP UCMM<br>CIP class 3<br>All other EtherNet/IP encapsulation messages | All | 35 ('100011') | 3 | CIP messaging |

[1] Sending 802.1Q tagged frames is disabled by default

# Devices which do not support the DLR protocol

- **Configuration Requirements**
  - Ports connected directly to the ring must be configured to preserve IEEE 802.1Q tag priority of ring protocol frames.
  - Disable IP multicast filtering on the two ports of the switch connected to ring. This step will assure uninterrupted delivery of EtherNet/IP multicast connection data after a ring reconfiguration.
  - Statically configure the three multicast addresses used by ring protocol to be forwarded only on two ports of switch connected to ring. This step must be done to prevent multicast ring protocol frames from being forwarded on other ports of switch

| Message Type | MAC Address |
| --- | --- |
| Beacon | 01:21:6C:00:00:01 |
| Neighbor_Check_Request/Response/Sign_on | 01:21:6C:00:00:02 |
| Announce/Locate_Fault messages | 01:21:6C:00:00:03 |

# DLR and 1588

- The DLR protocol does not require support for IEEE-1588.
- High performance applications can benefit from both the time synchronization of IEEE-1588 and the fast fault detection and ring recovery of DLR .
- It is recommended that all nodes participating in such a high-performance ring support IEEE-1588 and the CIP time sync object.
  - Note: the device itself need not be time-aware (i.e. it need not process IEEE-1588 messages locally), it should include support for end-to-end (E2E) transparent clock..

# DLR and QuickConnect

- QuickConnect is an ODVA technology intended to address specific applications in Automotive Manufacturing.
- Applications such as robots, tool changers and framers are required to quickly exchange tooling fixtures which contain a section or segment of an industrial network.
- This requires the network and nodes to be capable of quickly connecting and disconnecting, both mechanically, and logically.
- Consequently, when in QuickConnect mode, a port configured for forced speed and duplex mode, QuickConnect devices do not use Auto-MDIX (detection of the required cable connection type).
- Because Auto-MDIX is disabled for QuickConnect applications, extra care must be taken to ensure cabling connections are correct.

# General Considerations

- **DLR is generally intended for a simple, single-ring topology requiring fast recovery from network failures**
  - Does not support the concept of multiple or overlapping rings
- **While a DLR ring can contain an arbitrary number of nodes, recommended ring size is less than 50 nodes**
  - As the number of nodes grows, the time required for DLR frames to traverse the ring increases, leading to increased fault detection and recovery time
  - in a larger ring the probability of a fault increases, including double faults in which a segment may be lost from the rest of the network
  - Ultimately the number of nodes a user selects for a given ring depends upon the performance requirements the user has set for that ring

# Example Ring Configuration Parameters and Performance

| Number of Ring Nodes | Beacon Interval (usecs) | Round Trip Time[1] (usecs) | Beacon Timeout (usecs) | Physical Layer Faults Recovery Delay 1 (usecs) | Non-physical Layer Faults Recovery Delay for Beacon Frame Based Nodes (usecs) | Non-physical Layer Faults Recovery Delay for Announce Frame Based Nodes (usecs) | Ring Restore Delay for Beacon frame Based Nodes (usecs) | Ring Restore Delay for Announce frame Based Nodes (usecs) |
|---|---|---|---|---|---|---|---|---|
| **25** | 400 | 905 | 1380 | 980 | 1858 | 2335 | 1808 | **2260** |
| **50 (nominal network size)** | 400 | 1810 | 1960 | 1885 | 2890 | 3820 | 3165 | **4070** |
| **100** | 400 | 3620 | 3120 | 3695 | 4955 | 6790 | 5880 | **7690** |
| **150** | 400 | 5430 | 4280 | 5505 | 7020 | 9760 | 8595 | **11310** |
| **200** | 400 | 7240 | 5440 | 7315 | 9085 | 12730 | 11310 | **14930** |
| **250** | 400 | 9050 | 6600 | 9125 | 11150 | 15700 | 14025 | **18550** |

**1. Same for Beacon and Announce frames based nodes.**

# DLR Attributes, status indicators and diagnostics

- **DLR object attributes can provide helpful information when a fault occurs**
  - Most attributes are available only at the Ring Supervisor
  - Many of the attributes depend upon a beacon frame traversing the network to gather the attribute’s data (e.g. participant’s list)

- **While attribute 1, Network Topology, refers to both linear and ring topologies, this does not imply that DLR supports a line topology**
  - Attribute 1 is a status bit indicating:
    - Supervisor has blocked traffic in one direction on the ring and the ring is in its RING_NORMAL_STATE (linear topology) or,
    - the ring is either in startup or a faulted state (ring topology)

# DLR Attributes

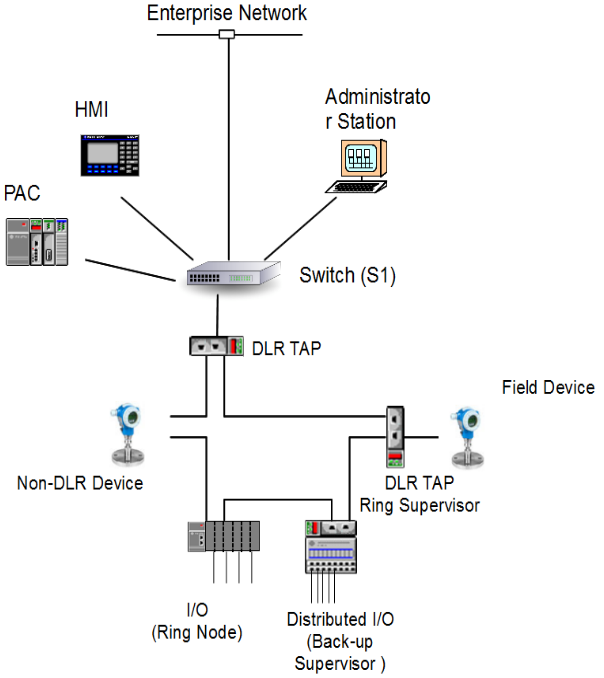
| Attribute ID | Attribute Name | Description | Available from Ring Supervisor | Available from Ring Node |
|---|---|---|---|---|
| 1 | Network Topology | 0 indicates "Linear"<br><br>1 indicates "Ring" | Yes | Yes |
| 2 | Network Status | 0 indicates "Normal"<br><br>1 indicates "Ring Fault"<br><br>2 indicates "Unexpected Loop Detected"<br><br>3 indicates "Partial Network Fault"<br><br>4 indicates "Rapid Fault/Restore Cycle" | Yes | Yes |
| 5 | Ring Fault Count | Number of ring faults since power up | Yes | No |
| 6 | Last Active node on port 1 | Last active node at the end of chain through port 1 of active ring supervisor during ring fault | Yes | No |
| 7 | Last Active node on port 2 | Last active node at the end of chain through port 2 of active ring supervisor during ring fault | Yes | No |
| 8 | Ring Participants Count | Number of devices in ring protocol participants list | Yes | No |
| 9 | Ring Protocol Participants List | List of devices participating in ring protocol | Yes | No |
| 10 | Active Supervisor Address | IP and/or MAC address of the active ring supervisor | Yes | Yes |
| 11 | Active Supervisor Precedence | Precedence value of the active ring supervisor | Yes | No |

# DLR Attributes

| Attribute ID | Attribute Name | Description | Available from Ring Supervisor | Available from Ring Node |
|---|---|---|---|---|
| 12 | Capability Flags | Describes the DLR capabilities of the device | Yes | Yes |
| 13 | Redundant Gateway Config | Redundant Gateway configuration parameters | Yes | No |
| 14 | Redundant Gateway Status | 0 – indicates the device is functioning as a non-gateway DLR node (gateway not enabled)<br><br>1 – indicates the device is functioning as a backup gateway<br><br>2 - indicates the device is functioning as the active gateway<br><br>3 – indicates gateway fault state due to loss of communication on uplink port<br><br>4 – indicates the device cannot support the currently operating gateway parameters (Advertise Interval and/or Advertise Timeout)<br><br>5 – indicates gateway fault state due to partial network fault | Yes | No |
| 15 | Active Gateway Address | IP and/or MAC address of the active gateway device | Yes | No |
| 16 | Active Gateway Precedence | Precedence value of the active gateway | Yes | No |

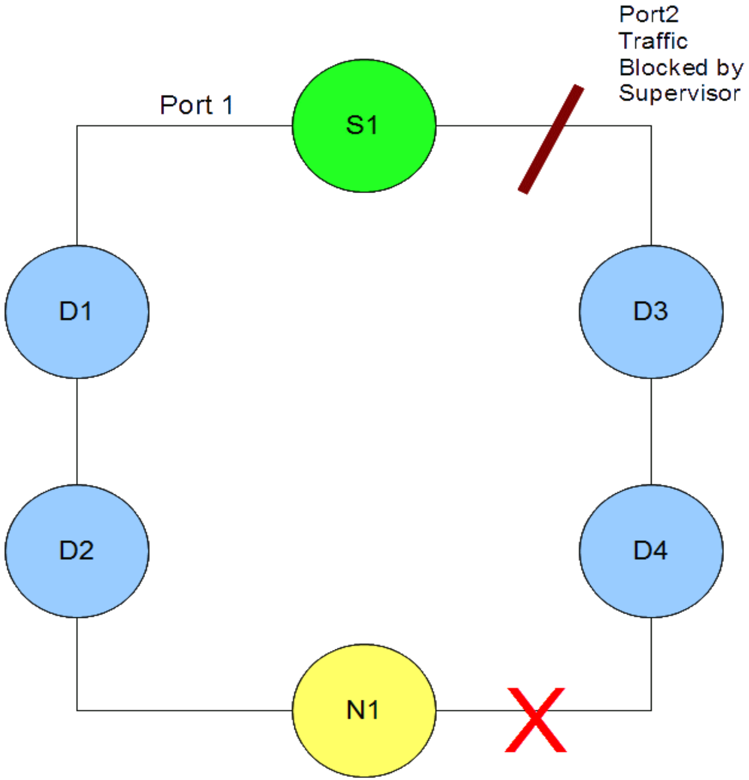
# Inserting Non-DLR Devices in a DLR Ring

- Non-DLR Devices have no adverse impact on worst case fault detection time.
  - Supervisor will still detect a lack of beacon frames and initiate ring recovery
- Including multiple Non-DLR devices in a ring can make isolating and diagnosing a fault problematic if the fault occurs between two non-DLR nodes.



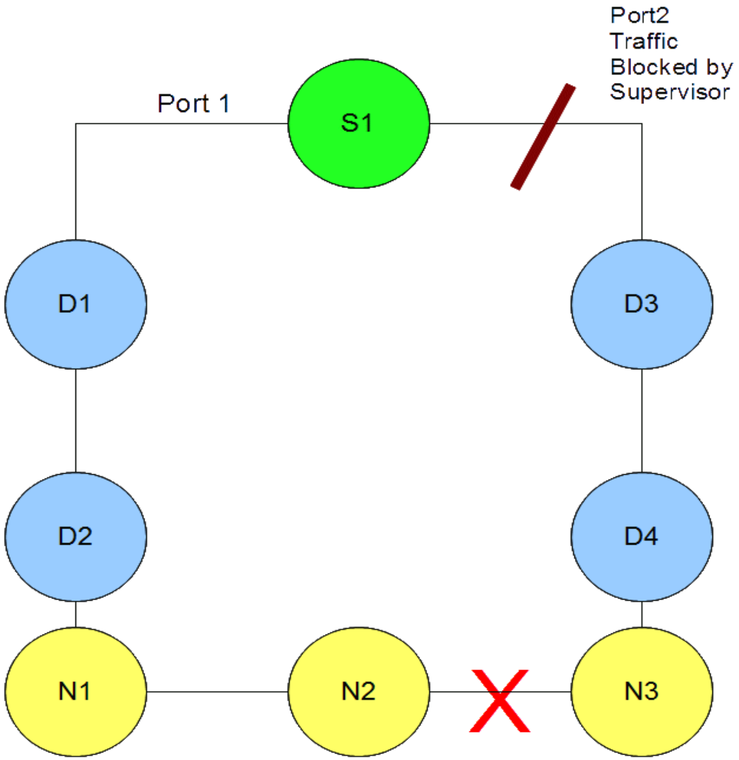
# Inserting Non-DLR Devices in a DLR Ring

- Consider a simple ring consisting of:
  - A supervisor (S1),
  - four DLR nodes (D1 through D4) and
  - a single Non-DLR device (N1).
- Assume that a link failure occurs between N1 and D4
  - Supervisor will still detect a lack of beacon frames and initiate ring recovery
- The fault detection process will:
  - identify D2 as the "Last Active node on port 1" and
  - D4 as the "Last Active node on port 2".
- Querying the link status will show:
  - from D4's perspective, the link with D2 is down, from D2's perspective the link is up
- One can reasonably deduce that the fault lies either with D4's lower port, N1's right port or the cabling between these nodes.



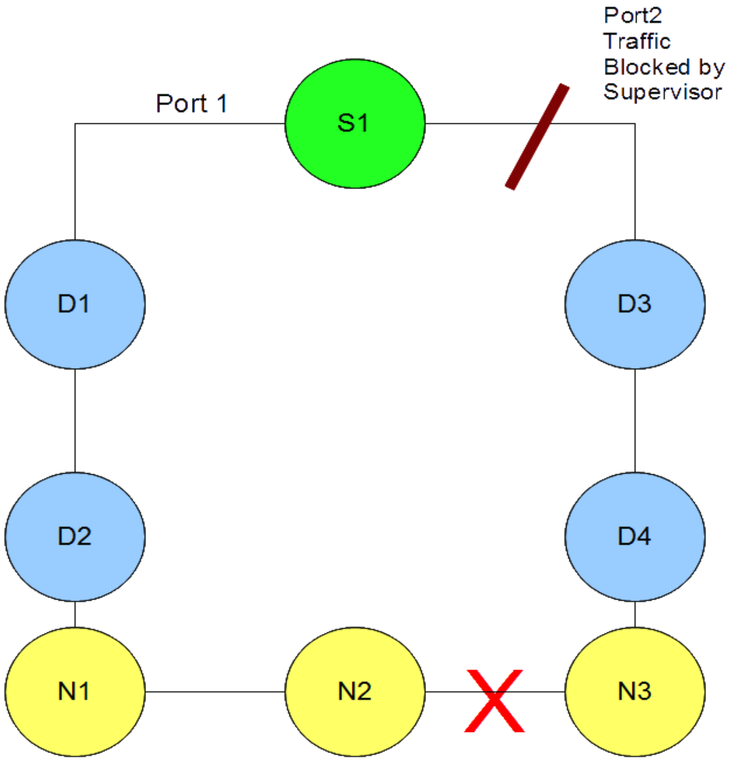
# Inserting Non-DLR Devices in a DLR Ring

- Now consider that Non-DLR devices N2 and N3 have been added to our simple ring
- Assume that a link failure occurs between N2 and N3
  - Supervisor will still detect a lack of beacon frames and initiate ring recovery
- The fault detection process will again:
  - identify D2 as the “Last Active node on port 1” and
  - D4 as the “Last Active node on port 2”.
- Querying the link status will show:
  - from D4’s perspective, the link with D2 is down, from D2’s perspective the link is up
- However, the fault might exist anywhere between D2 and D4.



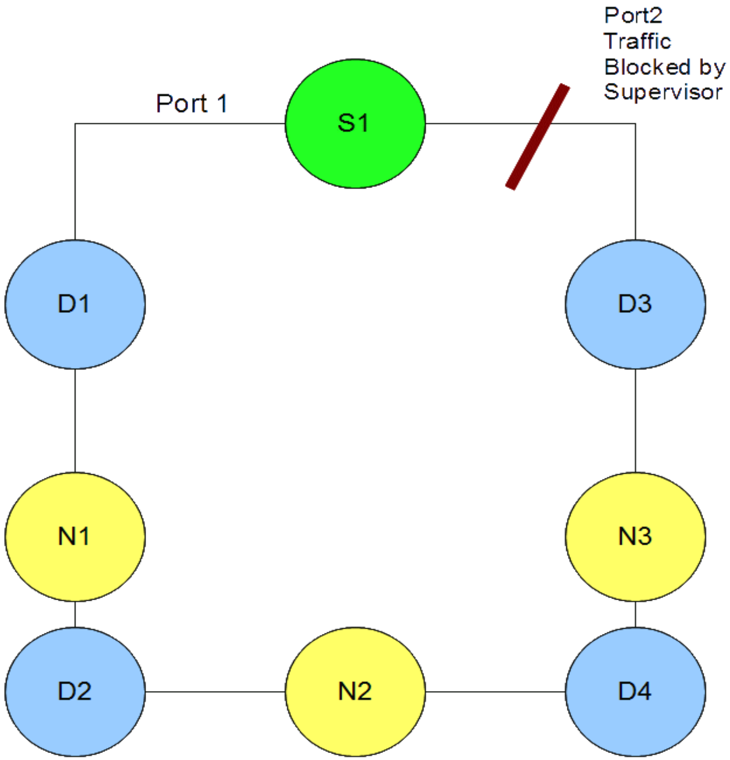
# Inserting Non-DLR Devices in a DLR Ring

- Now consider that Non-DLR devices N2 and N3 have been added to our simple ring
- Assume that a link failure occurs between N2 and N3
  - Supervisor will still detect a lack of beacon frames and initiate ring recovery
- The fault detection process will again:
  - identify D2 as the “Last Active node on port 1” and
  - D4 as the “Last Active node on port 2”.
- Querying the link status will show:
  - from D4’s perspective, the link with D2 is down, from D2’s perspective the link is up
- However, the fault might exist anywhere between D2 and D4.



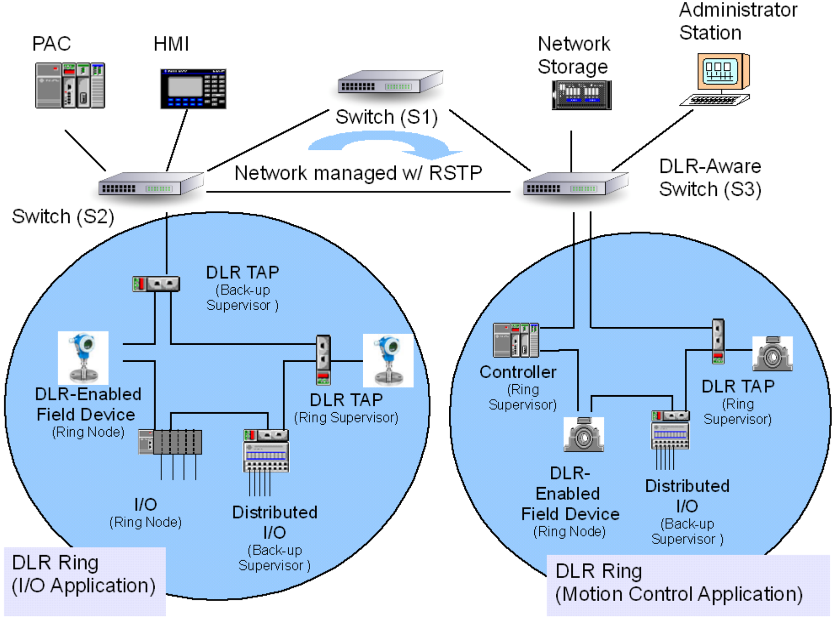
# Inserting Non-DLR Devices in a DLR Ring

- If multiple Non-DLR devices are to be inserted in the ring, it is preferable to insert DLR nodes between these devices for better isolation of faults .



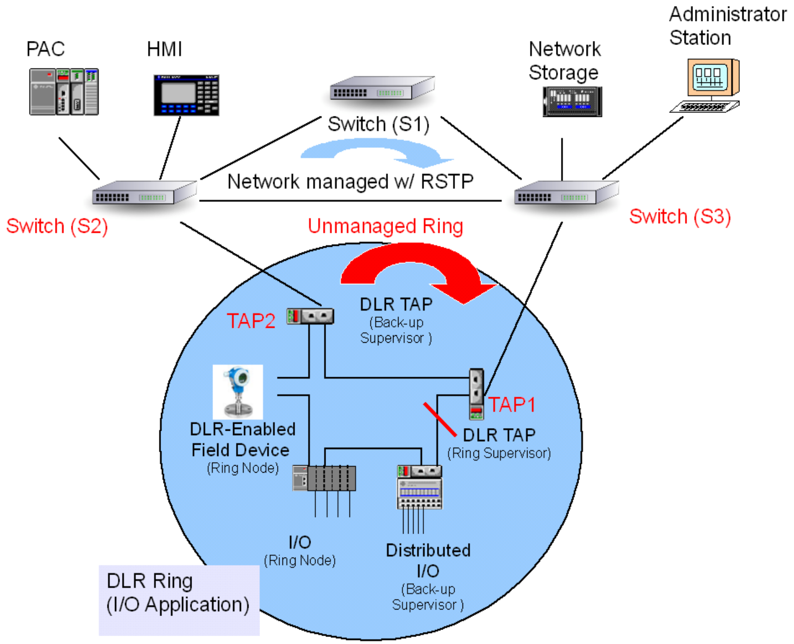
# DLR and Resiliency Protocols

- DLR rings may be connected to networks supporting IEEE Spanning Tree protocols (RSTP, MSTP).
- Care must be taken to ensure that these protocols do not interfere with DLR .
- Spanning tree protocols use special control frames called Bridge Protocol Data Units (BPDUs) to exchange information about network connections and their cost.
- The active Ring Supervisor will not forward multicast messages with the address 01:80:C2:00:00:00 (BPDU frames) from one ring port to the other, regardless of ring state.
- This feature ensures that the spanning tree protocol does not recognize and attempt to manage the DLR ring.



# A non-DLR loop passing through a DLR ring

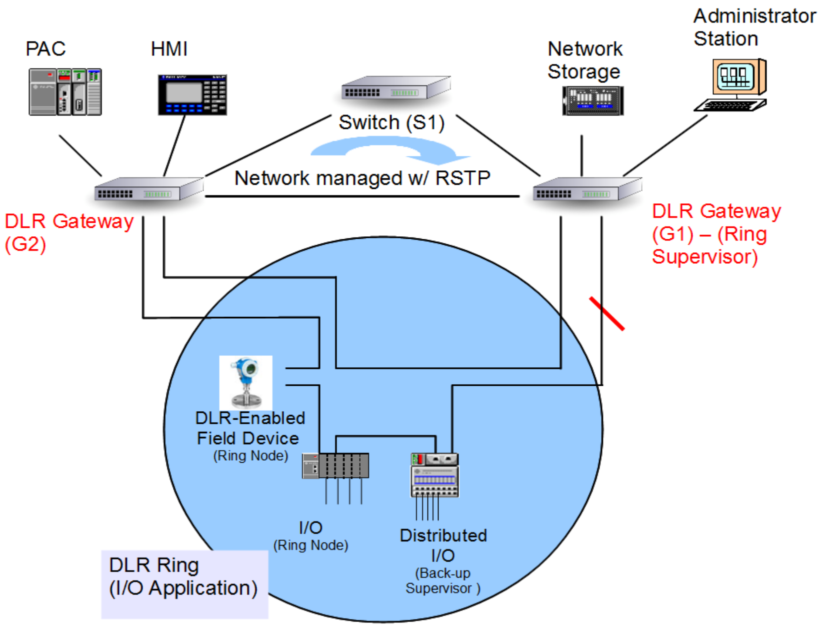
- Avoid multiple connections into a DLR ring:
  - switches S2 and S3 each connect to the DLR ring through a DLR tap
  - the Ring Supervisor will block BPDUs packets sent by each switch
  - the RSTP algorithm will be unable to resolve the network structure potentially resulting in unaddressed nodes, unmanaged rings and network storms
- **DO NOT IMPLEMENT!**



# DLR Redundant Gateways

- DLR supports multiple connections to a DLR network through redundant gateway devices:
  - Two DLR ports to connect to the DLR network
  - One or more uplink ports to connect to the network
  - Implements DLR protocol on its two DLR ports
  - Implements RSTP or MSTP on its uplink ports (other options possible)
  - Only one gateway is active (selection and switch over is automatic)
  - The backup gateway only forwards DLR traffic between its two DLR ports and forwards uplink port traffic only between its uplink ports
  - This prevents the creation of an unmanaged ring

- **It is strongly recommended that multiple connections to the network infrastructure outside of the DLR network be made via these gateway devices**



# Conclusions

- Some of the requirements which DLR imposes upon the network may not be obvious to those unfamiliar with .
- The DLR Whitepaper “Guidelines for Using Device Level Ring (DLR) with EtherNet/IP” is:
  - a resource for end-users and those responsible for specification, implementation or deployment of networks utilizing EtherNet/IP technologies and
  - an educational tool for manufacturers of EtherNet/IP equipment
  - available to all users (i.e. in the public area of the ODVA Website)
  - published as PUB00316R0 (https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00316R0_Guidelines_for_Using_Device_Level_Ring_(DLR)_with_EtherNetIP.pdf).

- ***My thanks to Adrienne Meyer, the TRB and especially the members of the Infrastructure SIG for their support of this effort!***

# References


1. IEEE Std 802.3 ¨C 2005, Part 3: *Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*.
2. IEEE Std 802.1D ¨C 2004, *Media Access Control (MAC) Bridges*.
3. IEEE Std 802.1Q ¨C 2003, *Virtual Bridged Local Area Networks*.
4. IEEE Std 802.1s ¨C 2002, *Virtual Bridged Local Area Networks ¨C Amendment 3: Multiple Spanning Trees*.
5. The CIP Networks Library, Volume 1, *Common Industrial Protocol (CIP)*, Edition 3.5, December 2008.
6. The CIP Networks Library, Volume 2, *EtherNet/IP Adaptation of CIP*, Edition 1.6, December 2008.
7. Moldovansky, A. et. al., *Introduction to Device Level Ring*. Proc. of ODVA 2009, Howey in the Hills, FL.

ODVA 2017
Industry Conference
and 18th Annual Meeting

# THANK YOU