



Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture

Design and Implementation Guide

January 2022



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 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 a CPwE ecosystem consisting of Cisco, Panduit, and Rockwell Automation emergent from the strategic alliance between Cisco Systems and Rockwell Automation.

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

Release Notes

This section summarizes the extensions to CPwE DLR in this January 2022 release:

- Updated DLR Participant List considerations within Chapter 2, DLR VLAN Trunking Restrictions
- Added note for proper VLAN configuration within Chapter 2, DLR VLAN Trunking Restrictions

This section summarizes the extensions to CPwE DLR in this November 2020 release:

- Test Hardware and Software for DLR Reference Architectures
- DLR VLAN Trunking feature and restrictions
- DLR application use case for single Industrial Ethernet Switch (IES) ring with Redundant Gateway and DLR VLAN Trunking
- Configuration of DLR VLAN Trunking via Device Manager and Command Line Interface

This section summarizes the extensions to CPwE DLR in this April 2020 release:

- Test Hardware and Software for DLR Reference Architectures
- DLR System Components Overview
- DLR application use case for single Industrial Ethernet Switch (IES) ring with Redundant Gateway
- DLR application use cases including single mixed IACS device/Industrial Ethernet Switch (IES) ring and multiple mixed IACS device/IES rings with Redundant Gateway
- DLR Monitoring and Troubleshooting with FactoryTalk[®] Network Manager[™] software

This section summarizes the extensions that were added to the CPwE DLR April 2019 release:

- Quality of Service (QoS) requirements
- Multiple ring specifications
- Dynamic Host Configuration Protocol (DHCP) for ring nodes
- Internet Group Management Protocol (IGMP) enhancement features
- DLR application use cases including single mixed IACS device/industrial Ethernet switch (IES) ring and multiple mixed IACS device/IES rings

Document Organization

This document is composed of the following chapters and appendices.

Chapter/Appendix	Description
CPwE Device Level Ring Overview	Overview of CPwE DLR.
CPwE Device Level Ring Design Considerations	Describes primary design considerations when choosing whether to implement the DLR protocol in an IACS architecture.
CPwE Device Level Ring Configuration	Describes how to configure the DLR protocol within the CPwE architecture based on the design considerations and recommendations of the previous chapter.
CPwE Device Level Ring Monitoring and Troubleshooting	Describes various DLR monitoring and troubleshooting options.
DLR Port Choices for Stratix Switches	Lists port choices for various Allen-Bradley [®] Stratix [®] industrial Ethernet switches (IES).
References	Links to documents and websites that are relevant to the Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture.
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/network-architectures.html>

- Cisco site:
 - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

**Note**

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

- <https://www.odva.org/technology-standards/key-technologies/ethernet-ip/>

CPwE Device Level Ring Overview

The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network and security technology convergence, including OT-IT persona convergence, by using standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A reliable and secure converged plant-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 resilient 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 made up 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)*.

The ODVA, Inc. Device Level Ring (DLR) resilient LAN technology is optimized to provide ring topology resiliency for time critical IACS applications. DLR supports fast ring convergence (single-fault tolerant) in the event of an IACS device or link failure. DLR also supports flexible topologies for OEM (equipment, skid, machine) and plant-wide or site-wide IACS deployments such as IACS device-level (embedded switch), switch-level (Layer 2, IES only), and hybrid topologies. DLR is standard Ethernet (OT-IT convergence) with standard network services such as quality of service (QoS) and IEEE 1588 PTP (Precision Time Protocol).

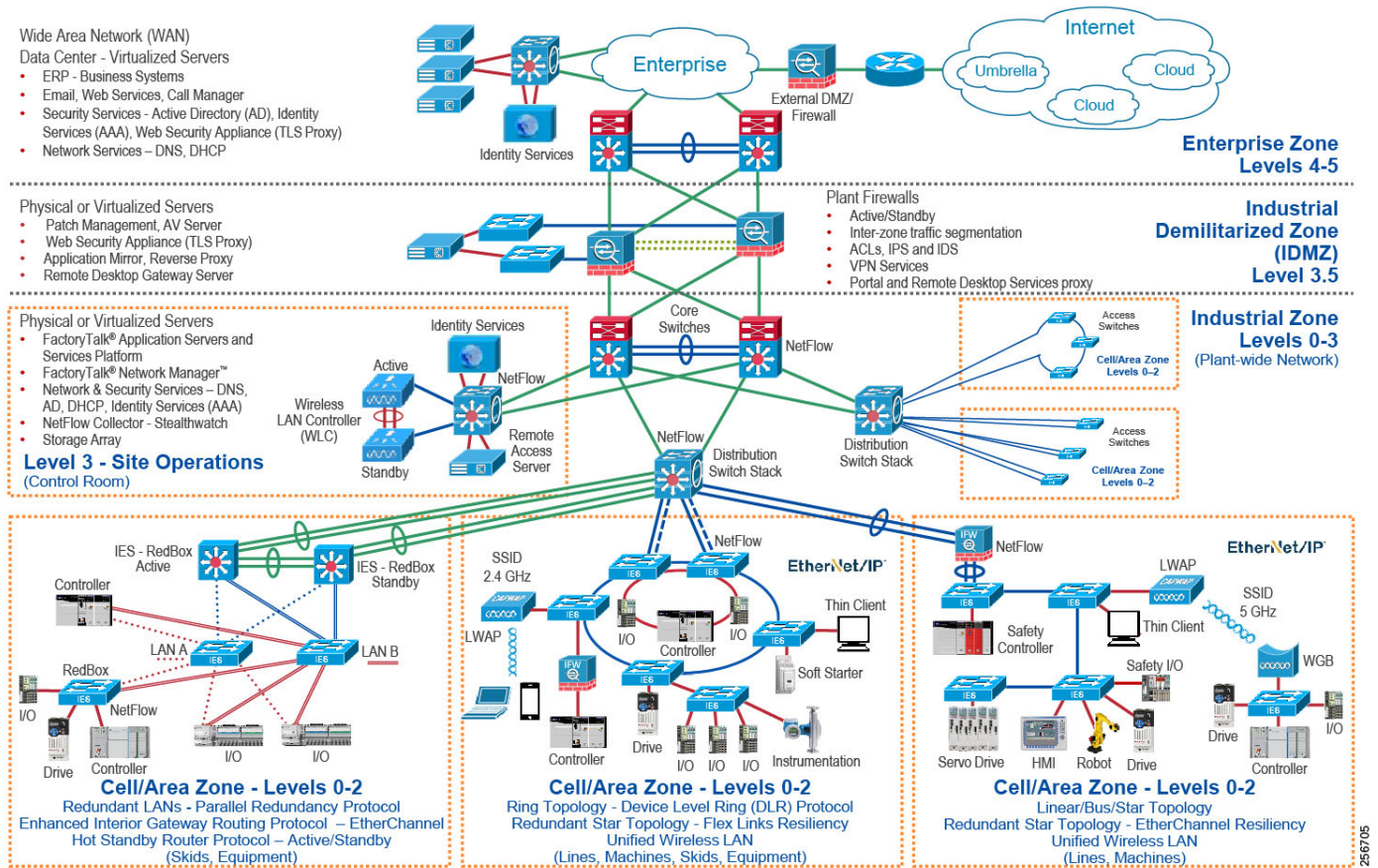
Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design and Implementation Guide outlines several use cases for designing and deploying DLR technology with IACS device-level, switch-level, and mixed device/switch-level ring topologies across OEM and plant-wide or site-wide IACS applications. CPwE DLR is an extension to CPwE Resiliency and was architected, tested, and validated by Cisco Systems and Rockwell Automation with assistance by Panduit.

CPwE Overview

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

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

Figure 1-1 CPwE Architectures



CPwE Device Level Ring Solution 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 made up 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 resilient network architecture (Figure 1-2) can help to increase the overall equipment effectiveness (OEE) of the IACS by helping to reduce the impact of a failure and speed recovery from an outage, which lowers Mean-Time-to-Repair (MTTR).

CPwE DLR 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 resilient converged plant-wide or site-wide EtherNet/IP IACS architecture.

This CPwE DLR Design and Implementation Guide includes:

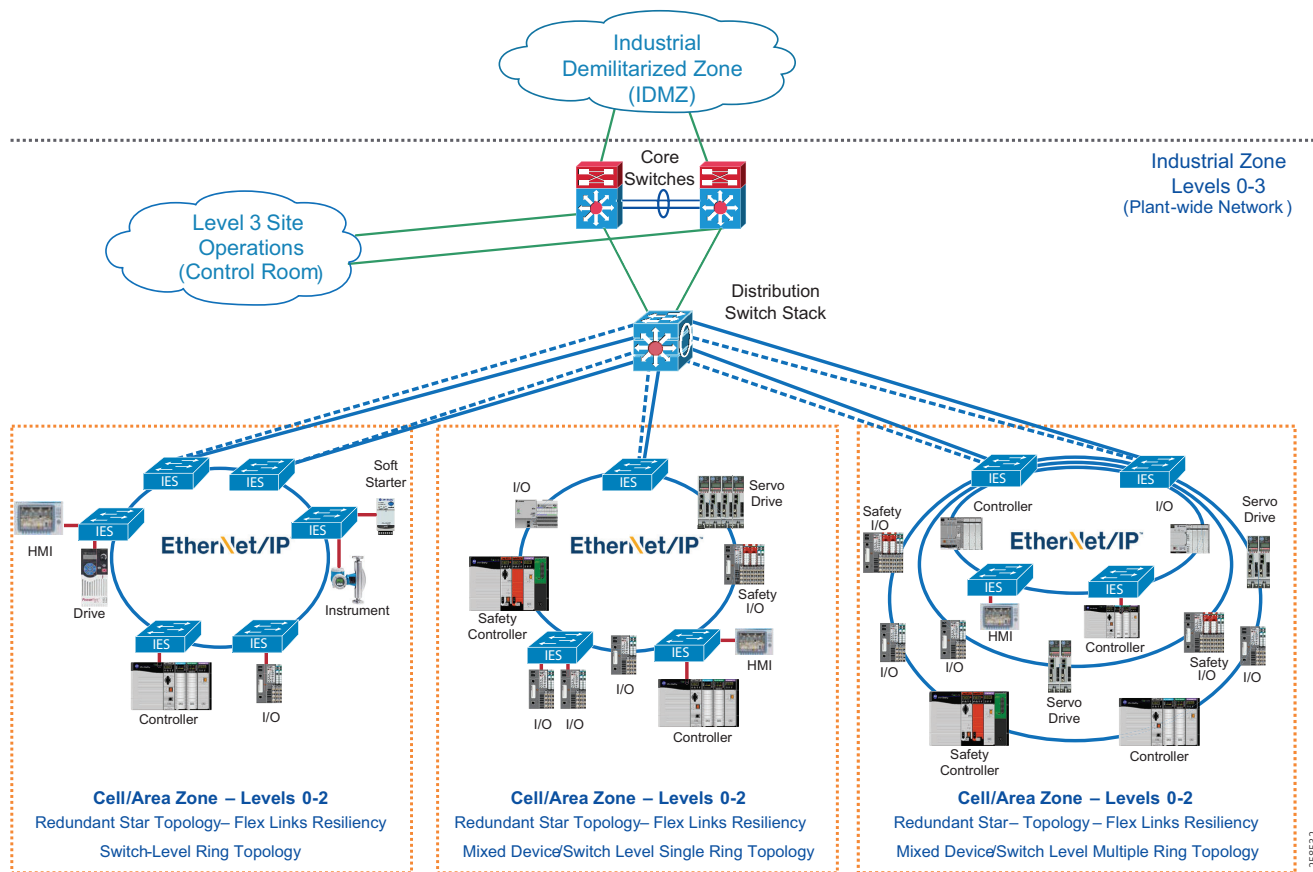
- Device Level Ring technology overview
- Design and configuration considerations for plant-wide or site-wide IACS device-level, switch-level, and mixed device/switch-level DLR deployments

- Selection of Industrial Ethernet Switches (IES)
 - Allen-Bradley Stratix 5700 and Stratix 5400 managed IES

Table 1-1 DLR Application Use Cases

Switch-Level DLR Reference Architectures	Reference Architecture Figure
Switch-Level DLR with Single Gateway	Figure 2-13
Switch-Level VLAN-Segmented DLR with Single Gateway	Figure 2-14
Switch-Level DLR with Redundant Gateway	Figure 2-15
Switch-Level DLR with Redundant Gateway and DLR VLAN Trunking	Figure 2-18
Mixed Device/Switch-Level DLR Reference Architectures	
Single Mixed Device/Switch-Level DLR (100 Mbps)	Figure 2-22
Single Mixed Device/Switch-Level DLR (1 Gbps)	Figure 2-23
Single Mixed Device/Switch-Level DLR (100 Mbps) with Redundant Gateway	Figure 2-24
Multiple Mixed Device/Switch-Level DLR (100 Mbps)	Figure 2-25
Multiple Mixed Device/Switch-Level DLR at Mixed Ring Speeds	Figure 2-26
Multiple Mixed Device/Switch-Level DLR with Redundant Gateway at Mixed Ring Speeds (Single VLAN)	Figure 2-27
Multiple Mixed Device/Switch-Level DLR with Redundant Gateway at Mixed Ring Speeds (Multiple VLANs)	Figure 2-28

Figure 1-2 Representative Plant-wide or Site-wide Switch-Level and Mixed Device/Switch-Level DLR Deployments



CPwE Resilient IACS Architectures Overview

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

- *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing and deploying resilient plant-wide or site-wide architectures for IACS applications, utilizing a robust physical layer and resilient topologies with resiliency protocols.
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- *Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing and deploying Parallel Redundancy Protocol (PRP) technology with redundant network infrastructure across plant-wide or site-wide IACS applications.

- Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td021_-en-p.pdf
- Cisco site:
https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

CPwE Device Level Ring Design Considerations

This chapter describes primary design considerations when implementing the DLR protocol in an IACS architecture.

Test Hardware and Software

The network hardware devices used in the CPwE DLR reference architectures are listed in [Table 2-1](#). Rockwell Automation® hardware and firmware versions are listed in [Table 2-2](#). Rockwell Automation software versions are listed in [Table 2-3](#).

Table 2-1 Network Hardware and Firmware

Role	Product	Firmware Version	
		April 2020 Release	November 2020 Release
Distribution Switch	Cisco Catalyst 3850	16.3.7	16.9.5 ¹
Distribution Switch	Cisco Catalyst 9300	16.12.1	17.3.1 ¹
Distribution Switch	Cisco Catalyst 4500-X	3.8.7E	3.11.2E ¹
Distribution Switch	Cisco Catalyst 9500	16.12.1	17.3.1 ¹
IES Access Switch	Allen-Bradley Stratix 5400	15.2(7)E	15.2(7)E2
IES Access Switch	Allen-Bradley Stratix 5700	15.2(7)E	15.2(7)E2

1. Cisco, Panduit, and Rockwell Automation recommend using the most recent CCO versions of Long-Term maintenance code for their deployments and to check the release notes for fixes and updates that are included in each release, especially regarding key features and functions upon which they may be relying.

Table 2-2 IACS Hardware and Firmware

Role	Product	Catalog Number	Firmware Version
Programmable Automation Controller (PAC)	ControlLogix [®] 5580 Controller	1756-L85E	32.014
	CompactLogix [™] 5380 Controller	5069-L340ERM	32.014
Redundant PAC	ControlLogix 5570 Controller	1756-L75	31.052
Safety PAC	GuardLogix [®] 5570 Controller	1756-L73S 1756-L7SP	32.011
Ethernet Module	ControlLogix EtherNet/IP Module	1756-EN2TR	11.004
Ethernet Module	POINT I/O [™] EtherNet/IP Adapter	1734-AENTR	5.018
Ethernet Module	Compact 5000 [™] I/O EtherNet/IP Adapter	5069-AEN2TR	3.011
Ethernet Module	Flex 5000 [™] EtherNet/IP Adapter	5094-AEN2TRXT	4.011
Redundancy Module	ControlLogix Redundancy Module	1756-RM2	20.010

Table 2-3 Rockwell Automation Software

Product	Version
Studio 5000 Logix Designer [®] Software	32.00.00
FactoryTalk Network Manager Software	1.08
FactoryTalk [®] View Site Edition Software	11.00.00
FactoryTalk Linx Software	6.11.00

**Note**

Test hardware and software versions listed in Table 2-1, Table 2-2, and Table 2-3 reflect versions utilized in select reference architectures at the time of publication. For more information on product-related downloads including firmware, release notes, associated software, drivers, tools, and utilities refer to the Product Compatibility and Download Center (PCDC):

<https://compatibility.rockwellautomation.com/Pages/home.aspx>

Network Topologies

Choosing the appropriate IACS EtherNet/IP network topology is a critical decision that relies heavily on the system or IACS application. There are three primary network topologies within the CPwE framework:

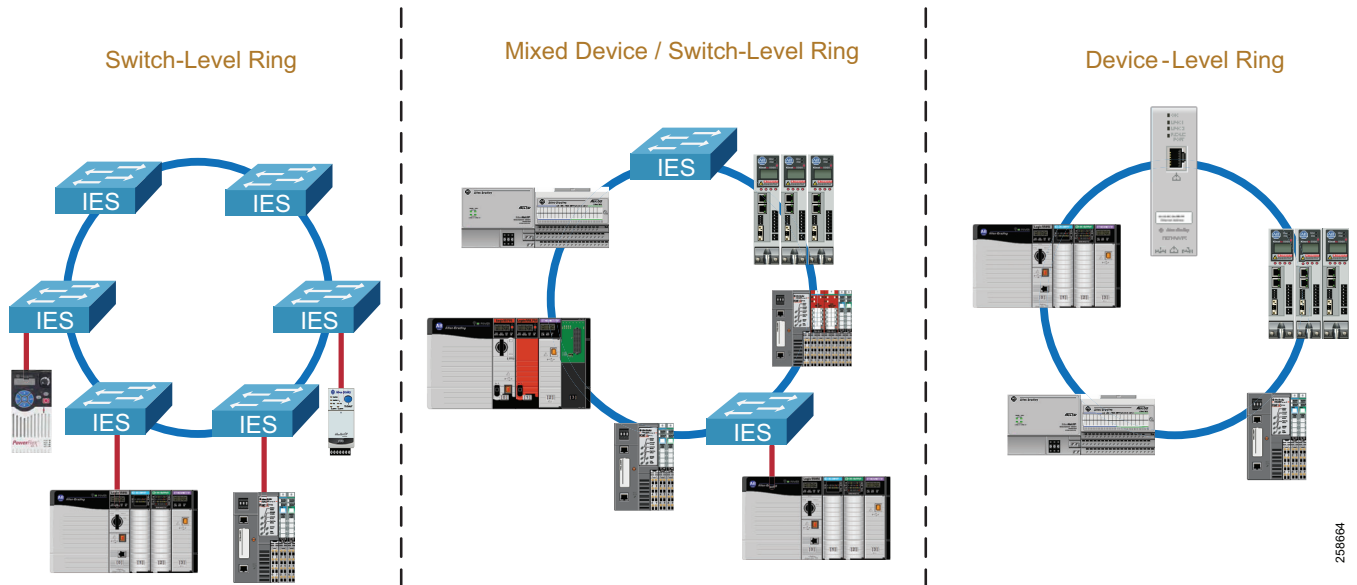
- Linear/star
- Redundant star
- Ring—switch-level and device-level

The DLR protocol is deployed in the ring topology and is intended for an IACS application that requires high speed convergence and single fault recovery for continuous operation. For more information on implementing a CPwE Reference Architecture or deploying DLR as part of a holistic resilient network, refer to:

- *Converged Plantwide Ethernet Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
- *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

The DLR protocol can be implemented in switch-level (IES only), mixed device/switch-level (combination of IES and IACS devices), and device-level (IACS devices only) ring topologies (Figure 2-1).

Figure 2-1 Switch-Level Ring (Left), Mixed Device/Switch-Level Ring (Middle), and Device-Level Ring (Right)



Embedded Switch Technology

The Embedded Ethernet Switch is an IEEE 802.1D compliant Layer 2 switch that is based on embedded switch technology and allows for IACS devices to be connected in a DLR device-level ring topology. Prior to embedded switch technology, the traditional EtherNet/IP network topologies were switch-centric using Layer 2 access industrial Ethernet switches (IES) to connect to IACS devices in a star topology and enabling communications between them. With embedded switch technology, IES ports can be conserved by connecting multiple IACS devices to a single port. Embedding switches directly into EtherNet/IP devices provides the following features:

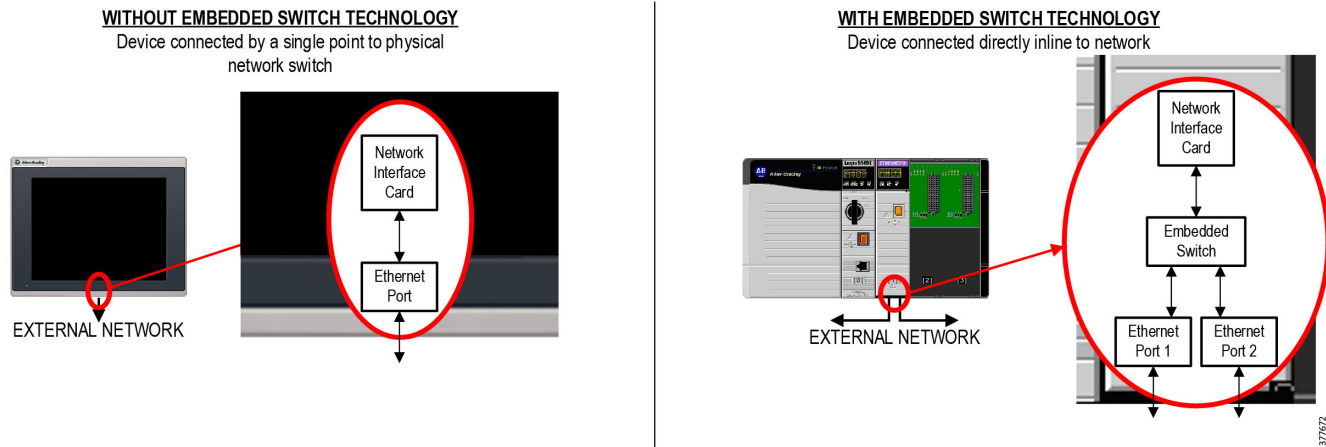
- Each IACS device supports the prioritization of network traffic to ensure timely delivery of critical data; that is, QoS and IGMP protocols are supported.
- Each product is designed and conformance tested per the ODVA, Inc. specification for EtherNet/IP.
- Each IACS device supports an IEEE 1588 transparent clock for Integrated Motion on EtherNet/IP and CIP Sync applications.

Each IACS device has a single network interface card (NIC) that is directly connected to a port on the embedded switch. The remaining two ports on the embedded switch are connected to ports 1 and 2 on the module which connect the module to the ring topology. Figure 2-2 provides a graphical representation of the Embedded Switch Technology.

**Note**

Some Rockwell Automation IACS devices provide the ability to operate as either embedded network switches or in dual NIC mode for separate IP address assignment to each port. When an IACS device is in dual NIC mode, the DLR functionality cannot be used.

Figure 2-2 Embedded Switch Technology Overview



Quality of Service

Quality of Service (QoS) is required for IACS devices that implement the DLR protocol. QoS refers to the capability of a network to provide higher priority to selected network traffic during times of congestion. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. It is also important to make sure that providing priority for one or more flows does not make other flows fail.

- Class of Service (CoS) is the classification of traffic at Layer 2 in the frame header. By manipulating the class of service bits, traffic is marked so that QoS can use this identification as a means to manipulate the traffic according to the policy.
- Differentiated Services Code Point (DSCP) is a field in an IP packet at Layer 3 that enables different levels of service to be assigned to network traffic. This is achieved by marking each packet on the network with a DSCP code and appropriating to it the corresponding level of service.
- The embedded switch technology implements four prioritized transmit queues per port, as follows:
 - Frames received with DSCP 59 are queued in highest priority transmit queue 1.
 - Frames received with DSCP 55 are queued in second highest priority transmit queue 2.
 - Frames received with DSCP 47 and 43 are queued in third highest priority transmit queue 3
 - Frames received with other DSCP values are queued in lowest priority transmit queue 4.

In addition, ring protocol frames are queued in highest priority queue 1. When a port is ready to transmit the next frame, the highest priority frame is chosen from the current set of queued frames for transmission based on strict priority ordering. Within a given priority queue, frames are transmitted in first-in first-out (FIFO) order. (See [Table 2-4](#).)

Table 2-4 Embedded Switch Technology Four Prioritized Transmit Queues

Priority Level (queue)	Class of Service (CoS)	Differentiated Services Code Point (DSCP)	Notes
Highest priority (queue 1)	7	59	DLR/Beacon protocol for ring configurations, PTP Event (IEEE 1588)
High priority (queue 2)		55	CIP Motion
Low priority (queue 3)		43, 47	Input/Output (I/O), CIP Safety I/O, PTP Management (IEEE 1588)
Lowest priority (queue 4)	1, 2, 3, 4, 5, 6	0-42, 44-46, 48-54, 56-58, 60-63	CIP messaging, HMI, tools

- Stratix IES with the DLR feature handles DLR control traffic both in the field-programmable gate array (FPGA) and the IOS through the application specific integrated circuit (ASIC). The FPGA has two queues, one for DLR control and the other for all other traffic. ASIC queues prioritize CPU traffic according to the CoS set in the VLAN header and the FPGA/CPU sets this to the highest priority for both ingress and egress traffic.
 - IACS traffic should take priority over other applications in the Cell/Area Zone. Non-industrial traffic should have little or no effect on the IASC application. See IACS traffic items in [Table 2-5](#).
 - The Stratix 5700 full firmware IES further extends QoS for IACS traffic in software using multilayer switching QoS (MLS) and the Stratix 5400 IES implements modular QoS CLI (MQC) to prioritize CIP traffic items.
 - Express setup is an out-of-box configuration process on Stratix IES that will implement a QoS framework on the network. By executing the Express setup, a macro runs and configures the IES with recommended QoS settings for classification, marking, queuing, and policing of CIP, PTP, and other traffic. It is also recommended to apply the appropriate Smartport roles for the IES ports. Smartports provide ease of configuration and management by using recommended preconfigurations specific for an IACS environment.

Table 2-5 CIP Traffic Items

CIP Traffic Type	Class of Service (CoS)	DSCP	Port number	CIP Traffic Usage
CIP Class 0/1	6	55	UDP 2222	CIP Motion
	4	47	UDP 2222	CIP Safety I/O
	4	43	UDP 2222	CIP Standard I/O
PTP Event (IEEE 1588)	7	59	UDP 319	CIP Sync
PTP General (IEEE 1588)	4	47	UDP 320	CIP Sync

Table 2-5 CIP Traffic Items

CIP Class 3	0	27	TCP 44818	CIP messaging, HMI, tools
Unclassified	0	0	Any	N/A

DLR Protocol Overview

Any DLR-compliant IACS device can be configured as a DLR ring node. Ring nodes can be categorized into three roles:

- Supervisor(s)
- Ring Participant(s)
- Gateway(s)

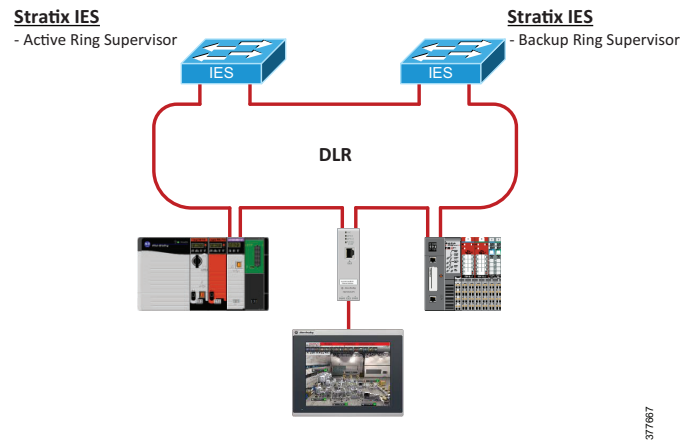
For all DLR deployments, there exist two primary DLR participant roles: the supervisor and the participant. The gateway is not required to be configured for DLR operation. Ring supervisors are considered either active or backup (if multiple supervisors are configured); this role is determined by the configurable supervisor precedence value. Any IACS device not operating as an active or backup supervisor, but participating in the DLR ring, is considered a ring node. Ring nodes are either Beacon- or Announce-Based (determined by the rate that the node is capable of processing DLR frames).

Supervisor

In all DLR deployments, at least one DLR ring supervisor must be defined. Deploying two DLR ring supervisors adds an additional layer of resiliency to the DLR ring network (as seen in [Figure 2-3](#)). During normal network operation, an active ring supervisor uses DLR protocol frames to monitor the health of the network. Backup supervisors and ring nodes monitor beacon or announce frames to track ring transitions between Normal (all links are working) and Faulted (the ring is broken in at least one place) states. If the backup supervisor does not receive the supervisor heartbeat for a period of time, it assumes that the supervisor failed and takes over the active supervisor role. The ring supervisor is responsible for the following DLR activities:

- Network Loop Prevention
- Determining Active or Backup Status
- Ring Integrity Verification
- Ring Fault Recovery via Ring Topology Reconfiguration
- Ring Diagnostics Aggregator
- Active Ring DHCP Server (configuration required)

Figure 2-3 DLR Ring with a Typical Active/Backup Supervisor Configuration

**Note**

Only select IACS devices are capable of acting as a DLR supervisor. Refer to the specific IACS device user manual for features and capabilities.

Network Loop Prevention

To prevent and manage network loops, the DLR ring supervisor blocks traffic on its highest numerical port per ring, except for a few special DLR frames. By blocking a single DLR port, the supervisor maintains a linear network topology. In the event of a single network fault, the supervisor will unblock its port to restore connectivity to the network segment between the port and the fault.

Active and Backup Status Determination

If multiple ring supervisors are deployed, each must be configured with a precedence value between 0-255 (default is 0). The active supervisor is the IACS device with the highest precedence value. If two supervisors are configured with the same precedence value, the IACS device with the numerically higher MAC address will become the active supervisor. Upon determination of the active supervisor role, the backup supervisor will then change its beacon interval, beacon timeout, and VLAN ID values to match those of the active supervisor.

Ring Integrity Verification

The active ring supervisor must be capable of transmitting an individual DLR Beacon Frame, at default, every 400 μ s and a DLR Announce frame every second. These frames are transmitted out of both DLR ring ports and in the event of a ring fault will not be received by the opposite port. This informs the ring supervisor that a fault has occurred. The location of the fault is determined by the last node that processed each beacon. The fault location is between these two respective nodes.

Ring Fault Recovery

Ring topology changes occur due to the addition or loss of a ring participant or ring media and are detected by loss of a beacon or announce frame on one or both port(s) of the supervisor and ring nodes, signaling all ring participants to flush and relearn their MAC tables. In addition to flushing its MAC address table, the ring supervisor will also unblock both DLR ports and send both Beacon and Announce frames informing all ring participants that the ring is now in the fault state.

This process allows for very fast recovery in the case of a ring fault and creates a consistent order of succession in the event that an active ring supervisor fails.

Ring Diagnostics Aggregator

As the supervisor's beacons traverse the ring in opposite directions, multiple attributes within the DLR frame collect real-time ring topology information. The DLR supervisor processes the beacons as it receives them and extracts the attributes associated with ring diagnostics to allow for diagnostic interfacing and ring state updates, if necessary.

DLR Ring Participants and Topologies

Beacon-Based

Beacon-based ring nodes are required to process beacon frames within a beacon interval time. The default beacon interval is 400 μ s and the minimum is 100 μ s. This interval allows for ring recovery times less than, or equal to, 3 ms for a 50 node ring. Any IACS device configured as a beacon-based node must, at minimum, be able to process beacons at the default interval of 400 μ s.

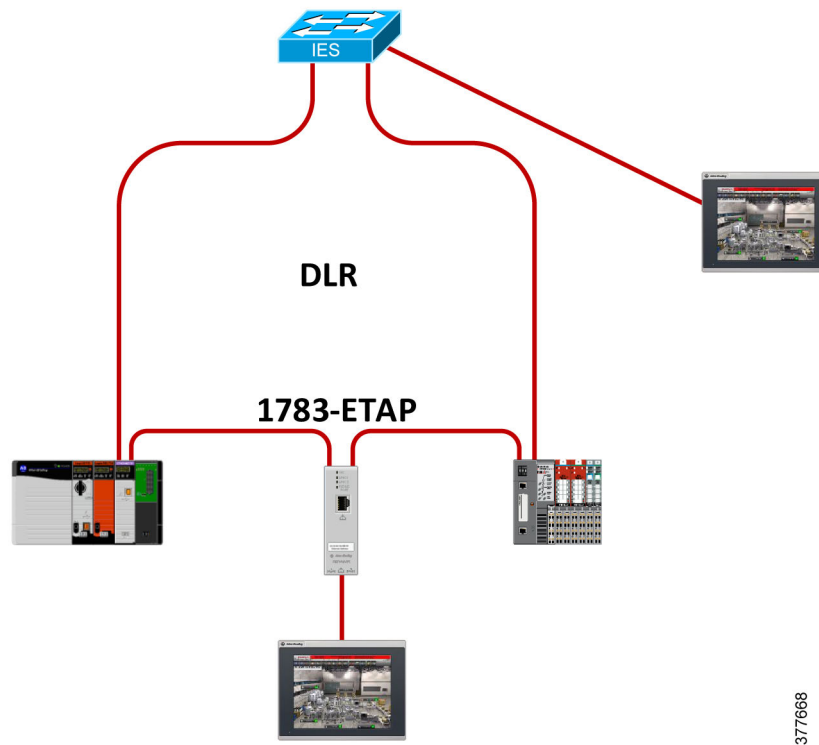
Announce-Based

Ring participants that are not capable of processing DLR beacon frames should be configured as DLR Announce-Based Nodes. These nodes will forward—but not explicitly process—beacon frames and instead process announce frames. Announce frames are generated by the supervisor at a default interval of one second or whenever a ring topology change is detected. Due to the larger frame interval inherent with announce frames, ring recovery times will be less than or equal to 4 ms for a 50-node ring as compared to 3 ms in a ring of beacon-based nodes.

Non-DLR Compliant Devices

Non-DLR Complaint Devices are IACS devices that do not have the required feature set to be deployed directly in a DLR ring. As these IACS devices were not designed for use in a DLR network, their functionality has not been fully tested and verified. It is strongly recommended to connect such devices to a DLR network via an Ethernet tap, such as a 1783-ETAP or a DLR-capable IES, for instance a Stratix 5700 or Stratix 5400. An example can be seen in [Figure 2-4](#).

Figure 2-4 Connecting a Non-DLR Compliant IACS Device to a DLR Topology



Single Ring

Single DLR rings can be either switch-level, mixed device/switch-level, or device-level. The single ring configuration deploys a dedicated, DLR-capable IES as the ring network egress point for the ring network. The choice of utilizing Redundant Gateways to create multiple ring egress points, or using a single IES to act as an egress point without being configured as a Redundant Gateway, is based on customer and IACS application resiliency requirements.

Multiple Rings

Currently, the Stratix 5400 is the only IES capable of supporting as many as three device-level rings simultaneously on the same IES. For this CVD, the multiple ring topologies using the Stratix 5400 IES were configured with the following specifications:

- Multiple rings cannot share the same ring ports. The Stratix 5400 has six dedicated DLR ring ports for up to three DLR Rings. Each ring can be logically isolated using VLANs. These ports are SKU dependent. The complete list of DLR compatible ports for the Stratix 5700 and Stratix 5400 can be found in [Appendix A, “DLR Port Choices for Stratix Switches.”](#)
- Using a single Stratix 5400 IES as the ring egress point and a single gateway, all three rings and their DLR ports were assigned to a single VLAN.
- Using dual Stratix 5400 IES with Redundant Gateway as the ring egress point, all three rings and their DLR ports were assigned to either a single VLAN or a VLAN per ring.

IES that can support multiple pairs of DLR ports must conform to the following rules:

- Each pair of DLR ports will operate independently from each other.
- Each pair of DLR ports will have separate DLR Objects, therefore logically each will have its own operational code with unique parameters and MAC address tables.

For example, when Ring 1 is in a Normal State and Ring 2 goes into a Fault State, only Ring 2 unicast MAC address table will be flushed.

DLR VLAN Trunking

The DLR VLAN Trunking feature allows a DLR network to carry traffic through a trunk link. A trunk link is a connection between switches that carries traffic from multiple VLANs, unlike an access link that can only carry a single VLAN. DLR VLAN Trunking allows switches and star connected devices in multiple VLANs to communicate through a DLR network. Traffic that passes from one switch to the next can either remain on the same VLAN or pass to a different VLAN via routing. The DLR VLAN Trunking feature was introduced for both single supervisor and Redundant Gateway applications in the following firmware versions:

- Single Supervisor firmware version 15.2(7)E
- Redundant Gateway firmware version 15.2(7)E2

DLR VLAN Trunking Restrictions

These restrictions should be strictly followed to achieve the best performance when using DLR VLAN Trunking.

- A routing capable IES or Distribution switch is required to route traffic to different VLANs in one of the following:
 - A Layer 2 switch is configured for connected routing in the ring or to the plant-wide or to the site-wide network. Connected routing enables configured devices on any VLAN to communicate through the same connected switch via the default gateway.
 - A Layer 3 routing capable device is configured to route traffic within the ring or to the plant-wide or site-wide network.
- The Stratix 5400 IES switch is the recommended series switch when using DLR VLAN Trunking. Performance issues have been identified with the Stratix 5700 IES switch with DLR VLAN Trunking enabled. Control plane functionality was impacted from high CPU utilization and slow response times for remotely managing the switch via Device Manager and the command line interface was observed during testing.
- The ring must consist of DLR capable IES switches as ring nodes.
- All Stratix switches on the ring must be configured as a DLR-enabled trunk port. Intermixing access and trunk ports on ring nodes will result in a ring fault.
- By default, a trunk link is configured to carry all VLANs that are configured on the IES switch. It is required to manually prune the DLR-enabled trunk ports to allow only the VLANs that reside on the ring in which the VLANs are needed.
- VLANs must be dedicated to a single DLR and cannot span multiple rings. The native VLAN must have a dedicated unique VLAN ID per ring. Secondary DLR that are configured off the main DLR trunk ring must utilize a single VLAN from the allowed list of VLANs for that specific DLR trunk.

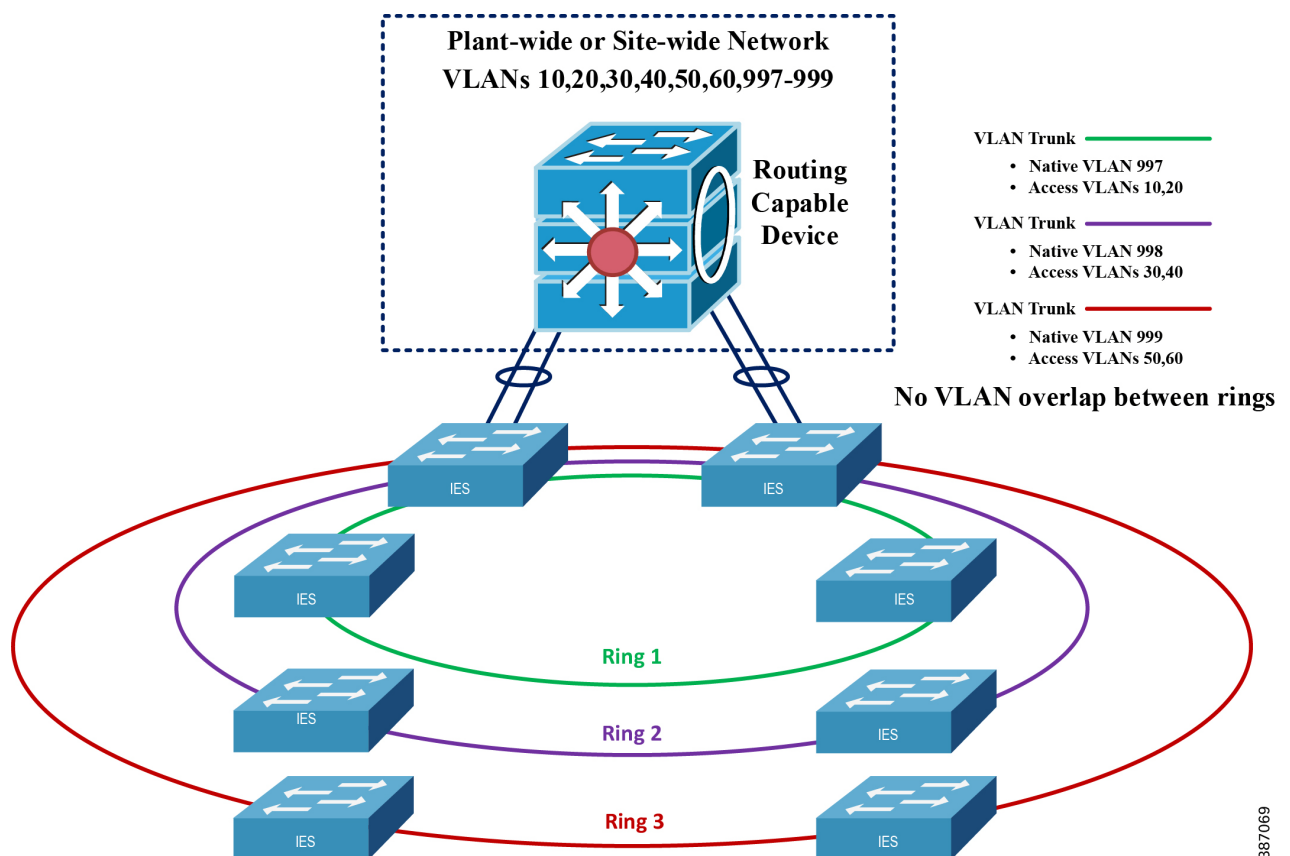
- If Native VLAN does not have an IP address associated with it, the DLR Participant List will show node IP addresses as 0.0.0.0 in the Stratix Device Manager. In order for the DLR Participant List to populate accurately, configure the Switched Virtual Interface (SVI) for the configured native VLAN ID.

**Note**

For proper VLAN configuration, reference the Allen-Bradley Stratix Managed Switches User Manual, 1783-UM007:
http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

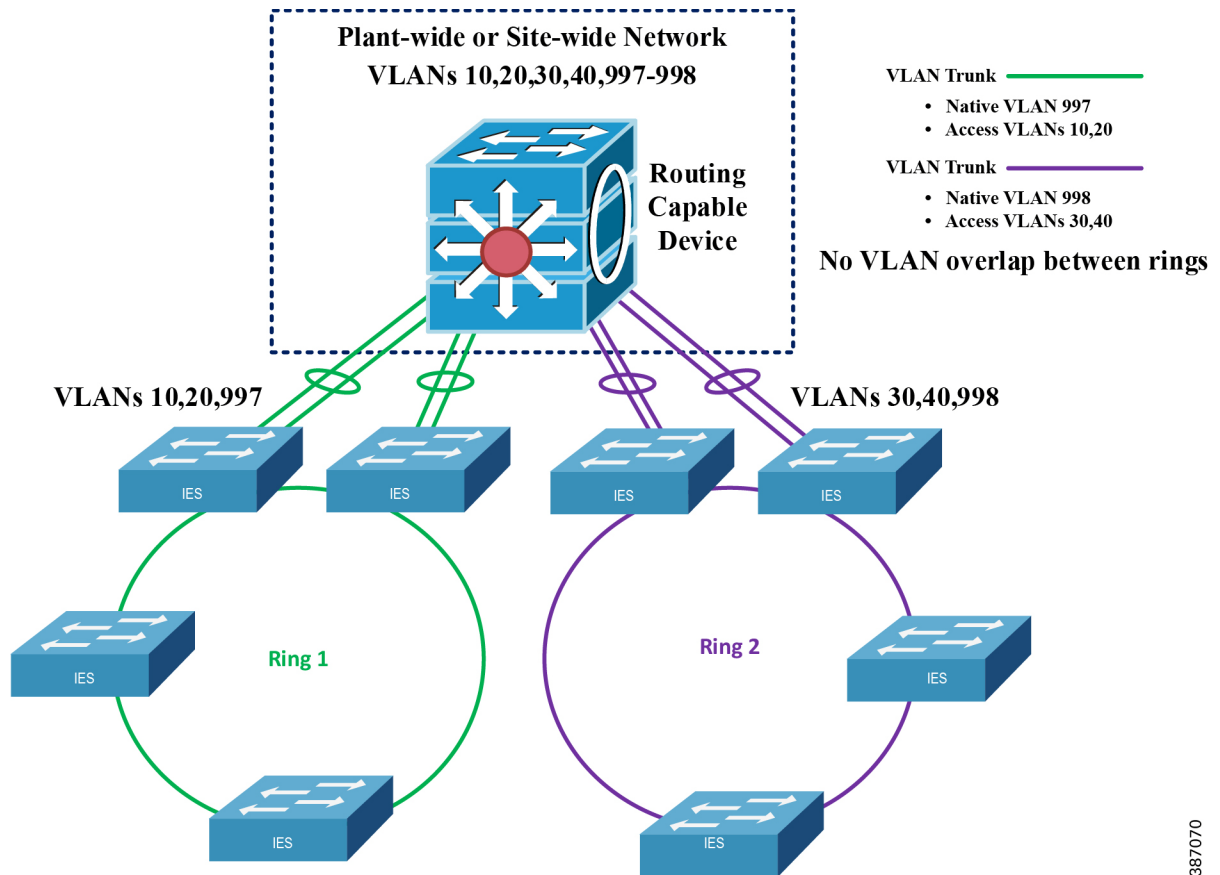
- Figure 2-5 illustrates the proper implementation of isolating VLANs for remote ports on a routing capable device from the plant-wide or site-wide network to the DLR network for the allowed VLANs to multiple ring DLR.
 1. Ring 1, all DLR-enabled trunk ports are configured to allow VLANs 10,20 and 997
 2. Ring 2, all DLR-enabled trunk ports are configured to allow VLANs 30,40 and 998
 3. Ring 3, all DLR-enabled trunk ports are configured to allow VLANs 50,60 and 999

Figure 2-5 DLR VLAN Trunking Restriction—Multiple Ring DLR



- Figure 2-6 illustrates the proper implementation of isolating VLANs for remote ports on a routing capable device from outside the DLR network for the allowed VLANs to separate DLR rings.
 1. Ring 1, all DLR-enabled trunk ports are configured to allow VLANs 10,20 and 997
 2. Ring 2, all DLR-enabled trunk ports are configured to allow VLANs 30,40 and 998

Figure 2-6 DLR VLAN Trunking Restriction—Multiple Single Ring DLR Example



387070

DLR Redundant Gateway

DLR Redundant Gateways provide multiple communication paths between a DLR ring and the surrounding network infrastructure. Typically, there are two gateway IES per DLR network. DLR Redundant Gateway provides the DLR nodes an additional layer of network resiliency by having Redundant Gateway IES and connections to the external IACS network. If single gateway IES to the external network is desired, it is not necessary to configure Redundant Gateway ports.

Redundant Gateway IES require, at minimum, two physical ports to connect to the DLR network and one or more uplink ports for connection to the surrounding IACS network infrastructure. It is for this reason that DLR gateways must be the DLR-compatible Stratix 5700 and/or Stratix 5400 IES. The ports designated as uplinks to surrounding network(s) must implement redundant star network resiliency protocols such as EtherChannel or Flex Links or ring network resiliency protocols such as Rapid Spanning Tree (RSTP), Multiple Spanning Tree (MSTP), or REP.

The DLR Redundant Gateway feature provides mechanisms for automatically or manually selecting an active gateway as well as for automatic switchover to a backup gateway in the event of a connection failure. Gateway switchover times range from 14 ms to 6.1 seconds, depending on the uplink network resiliency protocol. DLR Redundancy Gateway performance applies to traffic sourced from inside the DLR destined to the outside network:

- Uplink connection failure detected by the active gateway at the physical layer: up to 14 - 150ms

- Active Gateway failure: up to 19-150 ms

System performance, which applies to most applications, describes traffic sourced from the outside network destined to the DLR:

- Higher layer uplink fault detection: up to 6.1 seconds

**Note**

Refer to the corresponding tables in this chapter for guidance on convergence times when implementing DLR Redundant Gateway with specific distribution and uplink resiliency in a variety of architectures.

An active gateway is defined during configuration by setting a precedence value for all gateways. This value ranges from 0-255, with 255 being the highest precedence. Controlling gateway precedence values allows for control of gateway switchovers in the event of an uplink failure on the active gateway. In the event of this uplink failure, the active gateway role is shifted to the next highest precedence in the DLR ring.

**Note**

The Redundant Gateway feature requires all IACS devices on the ring to be compatible with Redundant Gateway. If all DLR network IACS devices are not compatible with Redundant Gateway, connections to IACS devices wired to or through a DLR network can be lost upon a gateway changeover. Refer to the specific IACS device user manual for features and capabilities.

DLR Redundant Gateway Restrictions

These rules should be strictly followed to achieve the best performance when using DLR Redundant Gateway.

- IACS devices required to communicate to the DLR or uplink ports should not be directly connected to either the active or backup Redundant Gateway IES. Non-essential IACS devices may be connected linearly to the Redundant Gateway if they can tolerate long periods of network isolation. If a Redundant Gateway switchover were to occur, IACS devices connected linearly to non-DLR ports will lose connectivity during the duration of the fault. The active and backup Redundant Gateway IES should only have the following connections otherwise:
 - DLR ports
 - Uplink ports
- Multicast convergence times have shown to be higher than Unicast convergence times, therefore this type of traffic should be limited from traversing the gateway uplinks. This type of traffic may include the following:
 - Multicast I/O (examples are ControlLogix Redundancy I/O and IEEE 1588 CIP Sync traffic)
 - Multicast Produced/Consumed Tags
- Application requirements should be rigorously reviewed prior to designing a network using DLR Redundant Gateway.
 - It is recommended that critical traffic remains local to the ring in which the source and destination device reside and only non-critical and HMI traffic traverse the DLR Redundant Gateways. Information on maximum convergence times that support Redundant Gateway are available later in this chapter in the appropriate reference architecture.

Redundant Gateway Traffic Flow

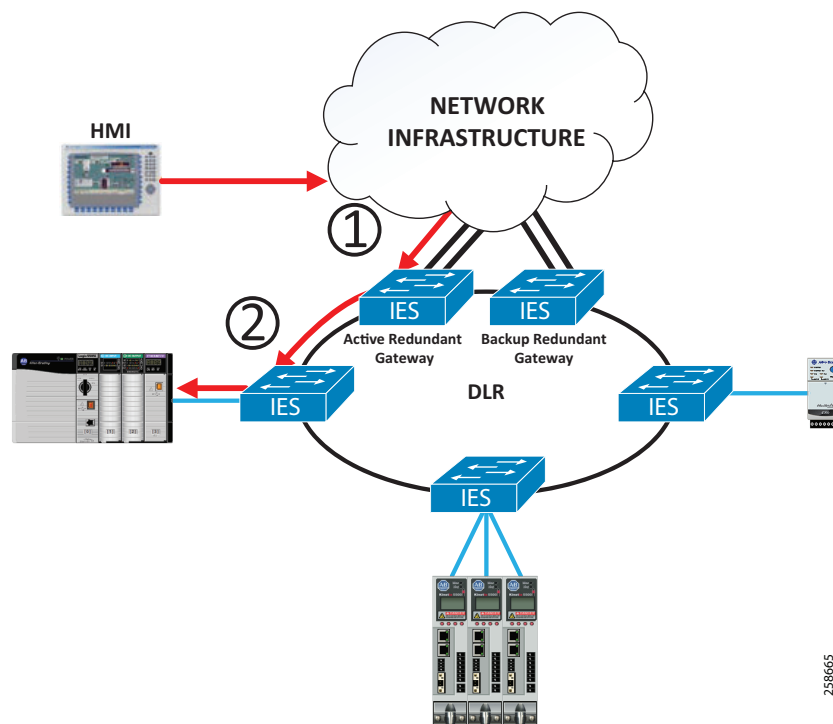
When properly configured, the primary gateway is the only device that will forward DLR traffic between its DLR ring port, uplink, and IACS end device ports. Backup gateways do not directly link DLR ring ports with the uplink and IACS end device ports and must therefore forward all traffic from directly connected end devices to the surrounding network infrastructure and back to the DLR ring via the primary gateway uplink(s). In the event of an uplink failure, end devices on a backup gateway will lose their connection to ring traffic. It is for this reason that IACS end devices should not be connected to a DLR gateway. Input/Output (I/O) and DLR traffic flows on each Redundant Gateway can be seen in [Figure 2-7](#) and [Figure 2-8](#).

Active Gateway Flow Diagram

A properly configured active gateway can freely forward all traffic on the same subnet between its uplink, DLR ring, and IACS end device ports. As a reminder, it is not recommended to connect IACS end devices directly to DLR Redundant Gateway IES.

1. Network traffic from outside of the DLR ring destined for the DLR ring from the IACS end device is received by the active gateway.
2. The active gateway forwards the IACS traffic to its DLR ring ports and out to the ring.

Figure 2-7 IACS Traffic Flow through an Active Redundant Gateway

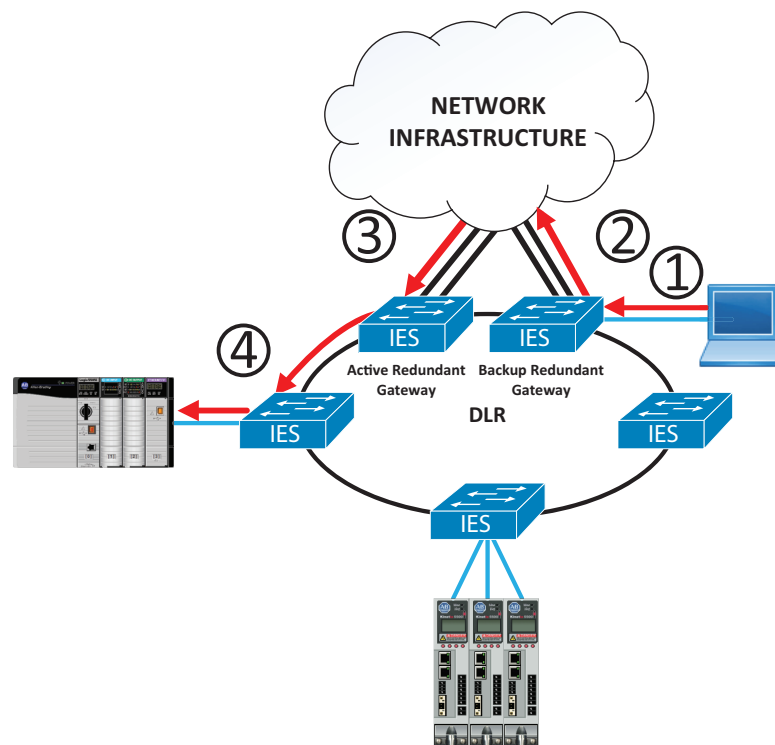


Backup Gateway Flow Diagram

The traffic flow for any IACS end device(s) directly connected to a backup Redundant Gateway is shown in [Figure 2-8](#). This flow path only applies to IACS end devices connected to backup gateway switch ports. All other ring switches not designated as backup gateways have a direct link between IACS end devices and DLR ring traffic. As a reminder, it is not recommended to connect IACS devices directly to DLR Redundant Gateway IES.

1. Network traffic destined for the DLR ring from the IACS end device is received by the backup gateway.
2. The IES forwards IACS traffic destined to the ring through its uplink port(s) to the gateway-linked network infrastructure.
3. IACS traffic is then forwarded, via the active gateway uplinks, to the active gateway IES.
4. The active gateway forwards the IACS traffic to its DLR ring ports and out to the ring.

Figure 2-8 IACS Traffic Flow through a Backup Redundant Gateway



258666

Protocol Compatibility

This section provides an overview of network resiliency protocols that can be implemented on IES acting as DLR ring participants. In terms of deploying a switch-level ring into a larger network architecture, there must be a distinction between DLR-enabled ring ports and IES ports operating outside of the DLR protocol. Stratix 5700 and Stratix 5400 IES can utilize ports designated for DLR participation, as well as uplink ports for inclusion in larger, external architectures. DLR ring ports are not compatible with the following IES capabilities:

- EtherChannels

- Network Address Translation (NAT)
- Resilient Ethernet Protocol (REP)
- MSTP/PVST/RPVST
- Flex Links
- 802.1x Security
- Smartport roles, except for Multiport Automation Device or None

**Note**

The listed capabilities may coexist on the same DLR capable IES, but only on non-DLR ports. DLR ports must be segregated from these resiliency protocols.

Dynamic Host Configuration Protocol (DHCP)

Traditionally, static IP addressing is the desired approach to allocate IP addresses for both IACS devices (for example, drives and I/O) and network infrastructure devices (for example, IES). Static IP addressing requires a user to manually configure an IP address on an IACS device as it is provisioned onto the IACS network. This makes the process of provisioning or replacing an IACS device time consuming and results in high administrative overhead. Dynamic Host Configuration Protocol (DHCP) is used to provide quick, automatic, dynamic, and centralized management for the distribution of IP addresses within an IACS network. This capability helps to reduce the amount of time required to provision or replace IACS devices, such as drives and I/O. However, with dynamic addressing, an IACS device can have a different IP address every time it connects to the network. In IACS applications, like Studio 5000 Logix Designer, static IP addressing is referenced directly by the IACS applications for communication and control purposes. Therefore, the IP addressing assigned must be consistent and defined for proper IACS application operation. The Stratix IES supports two features that allow administrators in an IACS network to dynamically assign specific IP addresses to specific IACS devices. The features are:

- DHCP Persistence (Per Port)
- DHCP for Ring Devices

DHCP Persistence

The Stratix 5400, Stratix 5700, and ArmorStratix™ 5700 IES support a feature called DHCP Persistence (also referred to as DHCP per port). This feature enables users to reserve and pre-assign an IP address to a specific switch port on the IES. An IES that has been configured to act as a DHCP server enables an IACS device connected to that specific IES port to always receive a consistent IP address regardless of its MAC address. This capability helps to reduce the amount of time required to provision or replace IACS devices, such as drives and I/O.

**Warning**

During the IACS device replacement using the DHCP Persistence feature process, it is critical to ensure that the replacement IACS device is connected to the correct IES port with DHCP configuration. The programmable automation controller (PAC) will connect to any IACS device, i.e., drive or I/O with the same IP address and the same catalog number in the I/O tree, regardless of their function.

Stratix IES in a switch-level or mixed device/switch-level ring topology with a ring role of Beacon-Node can be configured with DHCP Persistence to provide star connected IACS devices with IP addresses.

DHCP Persistence guidelines:

- When creating the DHCP pool, enable the Reserved-Only option to restrict IP addresses in the pool to pre-configured DLR IES ports.
- If using a VLAN ID [#] other than the default VLAN ID 1, enable DHCP snooping on the VLAN ID [#].

DHCP for Ring Devices (DLR DHCP)

Stratix 5400, Stratix 5700, and ArmorStratix 5700 IES that support DLR also support a feature called DHCP for ring devices (also referred to as DLR DHCP). The DLR DHCP feature is another way for users to reserve and pre-assign an IP address, but based on the position of nodes in a ring instead of per-port basis. This allows the Stratix IES to act as a DHCP server to assign designated IP addresses to properly configured ring participants. This feature is useful in the event of a ring participant failure or loss of ring participant power. A replacement IACS device can be installed in the same node position and the same IP address will automatically be assigned to it. Stratix IES in a mixed IACS device/IES ring topology, with ring roles of active or backup DLR supervisor, can be configured with DLR DHCP. This will provide ring participants with IP addresses.

There are several considerations when configuring DLR DHCP:

- The Stratix IES must be configured as the active ring supervisor and enabled as the primary DHCP server on the ring.
- The Stratix IES serving as the active DLR supervisor and primary ring DHCP server needs to be configured with the DHCP pool, the DLR supervisor role, and the DHCP Server Reference Address table. The DHCP Server Reference Address table contains the configured node/index position and specific designated IP address assignment.
 - If a ring topology is expanded, the DHCP Server Reference Address table must be updated to include the added node. Without properly updating configuration of the DHCP Server Reference Address Table when adding a new IACS device, the new IACS device along with all nodes behind it will be assigned an incorrect IP address. The DHCP Server Reference Address Table assigns IP addresses based on node number in the DLR ring and does not automatically detect and adjust for topology changes.
- If another Stratix IES in the ring is configured as a backup supervisor, it can also be enabled to act as a backup ring DHCP server. Do not configure a DHCP pool or the DHCP Server Reference Address table on the Stratix backup ring DHCP server. The backup server will obtain the configured DHCP pool and DHCP Server Reference Address table from the primary ring DHCP server through a synchronization process.
- If the active ring supervisor/primary DHCP server fails, the next-in-precedence backup ring supervisor/DHCP server will become the active. It will manage IP address assignment and renewal until one of the following happens:
 - The original primary ring DHCP server is restored.
 - A new primary ring DHCP server with a higher precedence is manually configured.



Note

If the nodes were initially given an IP address from the Stratix IES primary ring DHCP server, followed by a primary DHCP server failover, the nodes will hold the IP address until the node is power cycled.

- Both the primary ring DHCP server and the backup ring DHCP server must have CIP enabled.
 - The CIP VLAN allows the primary ring DHCP server to synchronize its DHCP Server Reference Address table and DHCP pool configuration with the backup ring DHCP server.

While the DLR protocol is compatible with DHCP, there are a number considerations:

- Though the Stratix IES directly on the ring can be a DHCP server, it cannot be a DHCP client. All Stratix IES directly on the ring must be configured with a static IP address.
- As of IOS Release 15.2(6)E2 or higher, both the DHCP Persistence and DLR DHCP features can co-exist (be configured) on the same IES at the same time with some limitations. Prior to this release, in older firmware, both features could not be configured on the same IES—only DHCP Persistence or DLR DHCP could be configured on the IES. See Knowledgebase Answer ID 1081858 (https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1081858) for more details on limitations.

**Note**

The coexistence of both DHCP features was not tested for CPwE DLR. For more information on earlier IOS Releases regarding DHCP support, visit the Rockwell Automation Product Compatibility & Download Center to view the Release Notes for each IOS Release.

Stratix IES in a mixed device/switch-level ring topology with ring roles of Active or Backup DLR Supervisor with Ring DHCP server enabled can be configured with DHCP capabilities. This will provide ring participants with IP addresses.

DLR DHCP guidelines:

- When creating the DHCP pool on the primary ring DHCP server, enable the Reserved-Only option to restrict IP addresses in the pool to pre-configured DLR IES ports.
- If a backup ring DHCP server is configured, enable the Ring DHCP Server feature but do not configure a DHCP pool or DHCP Server Reference Address table.
- Both the primary ring DHCP server and the backup ring DHCP server must have the DHCP snooping enabled globally.
 - If using a VLAN ID [#] other than the default VLAN ID 1, enable DHCP snooping on the VLAN ID [#].
- DLR DHCP snooping must be enabled on the primary ring DHCP server and backup ring server to use the DLR DHCP feature. (DLR DHCP snooping is enabled by default.)
 - When enabled, DLR DHCP snooping restricts DHCP address assignments from going beyond an active ring DHCP server DLR ports and the devices within the ring. DHCP requests from another server cannot enter the ring and DHCP requests from the active ring DHCP server cannot leave the ring.
- Both DLR ports of the primary ring DHCP server and the backup ring DHCP server must have the `ip dhcp snooping trust interface` command. (This trust command is automatically added to the DLR interfaces of those Stratix with the role of Active or Backup DLR supervisors and Ring DHCP Server feature enabled.)
 - Any Stratix IES with the DLR capability directly on the ring operating as a beacon node must have the DLR ports configured with the following interface command via CLI. This will allow DHCP server messages to flow around the ring to all nodes:

```
switch(config-if)# ip dhcp snooping trust
```

DHCP Snooping

DHCP snooping is a Layer 2 IES feature used to allow coexistence of multiple DHCP servers in the same VLAN. It is also used to mitigate security risks of an unauthorized rogue DHCP server offering IP addresses to DHCP clients. DHCP snooping should be enabled globally and on a per-VLAN basis. Once enabled, all IES ports will be in an untrusted state and therefore will drop all DHCP server messages. This will prevent

the DHCP client from obtaining an IP address until a trusted DHCP server is identified and properly configured. Trusted DHCP servers are identified by configuring an IES port's DHCP snooping trust state. Once an IES port has been configured to a trusted state, DHCP server messages can flow through the port to complete the DHCP server/client communication exchange for the DHCP client to obtain an IP address from the trusted DHCP server.

As DHCP messages flow to and from the server and client on the trusted port, the DHCP snooping feature will “listen” to the messages to build and maintain a DHCP snooping binding database called the DHCP snooping binding table. The DHCP snooping binding table contains data such as the client MAC address, DHCP assigned IP address, VLAN ID, switch port, and lease time. DHCP snooping is enabled by default on Stratix IES.

Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) is the protocol used by IACS devices to indicate that they are interested in receiving traffic for a multicast group. If multicast traffic is not managed by the IES, then by design, an IES will forward multicast frames out all ports within the same VLAN. Essentially the IES will treat multicast as a broadcast. In the Layer 2 IES network, there are two key components used in the network infrastructure to manage multicast traffic:

- IGMP snooping querier
- IGMP snooping

IGMP Snooping Querier

The IGMP snooping querier function is to use IGMP messages to keep track of group membership on each VLAN or network. It will send out periodic IGMP queries that trigger IGMP report messages from hosts that want to receive IP multicast traffic.

Typically, it is best practice to have the IGMP snooping querier located on the distribution switch for the network. The IES are configured to all act as IGMP snooping queriers, therefore the switch with the lowest IP address will take over the responsibility of IGMP snooping querier.

**Note**

The IGMP snooping and querier features are enabled by default when the Express setup is executed during the initial setup of the Stratix IES.

IGMP Snooping

IGMP snooping is compatible with DLR and is implemented in Layer 2 IES and the 1783-ETAP network tap. This implementation constrains multicast traffic port flooding by restricting it to switch ports associated with IP multicast IACS devices. This protocol can be very useful in high-speed, time-dependent applications as it reduces the amount of network bandwidth consumed by I/O multicast messaging.

The IGMP snooping feature includes two optional extensions: the Extended Flood and the Solicit Query at Topology Change Notification (TCN).

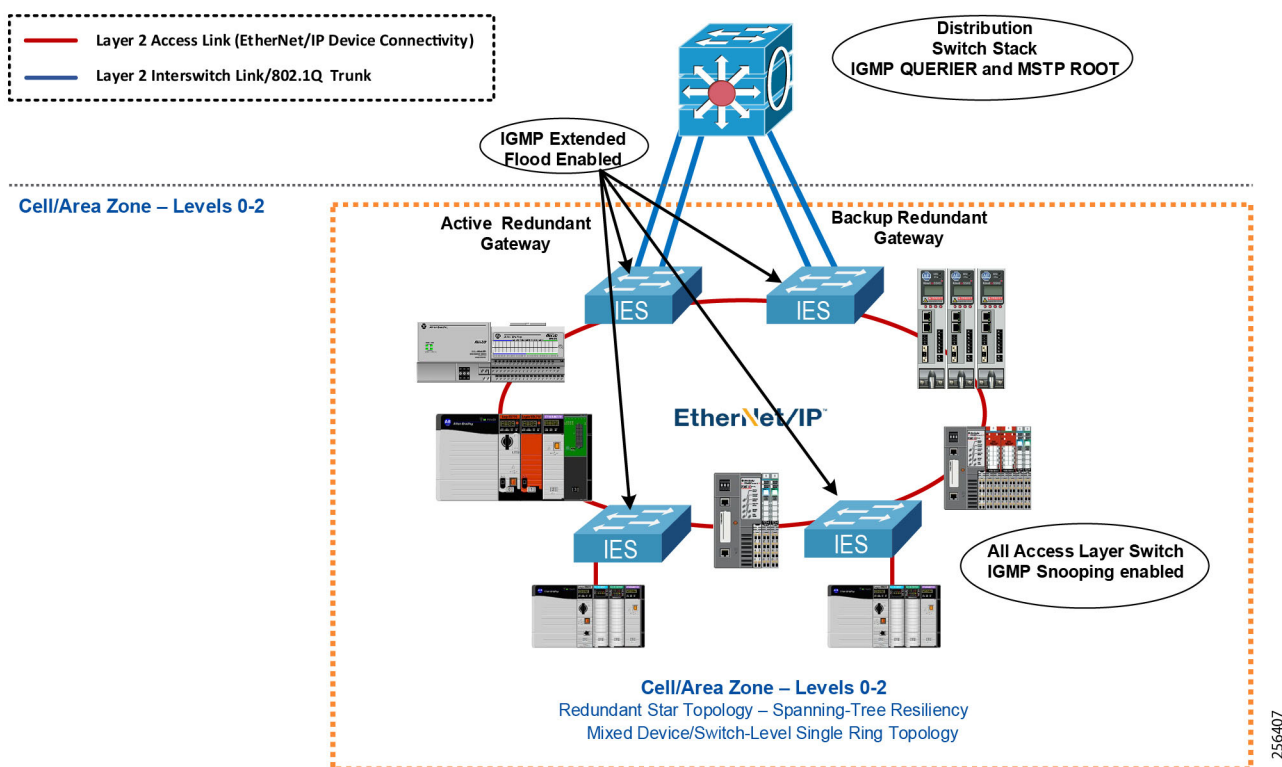
- The Extended Flood extension (Figure 2-9) can be enabled to help prevent the loss of multicast traffic when the IGMP snooping querier is disconnected and then reconnected. When there is a loss of the IGMP snooping querier, the IES will continue flooding multicast traffic after a multicast router is detected for the default of 10 seconds to ensure all IACS devices receive the multicast traffic. The number of seconds to flood can be adjusted for mature IACS applications on the network. It is recommended to enable the Extended Flood extension globally on the Layer 2 IES when:

- IACS applications use multicast traffic.
- The network resiliency Multiple Spanning Tree Protocol (MSTP) is used as the uplink with DLR.
- The network resiliency MSTP is used as the uplink with DLR Redundant Gateway.

**Note**

Enable the Extended Flood extension on all IES directly in the ring (Figure 2-9) when MSTP is used as the uplink protocol. For details on how to configure IGMP snooping extension Extend Floor, refer to Chapter 3, “CPwE Device Level Ring Configuration.”

Figure 2-9 IGMP Extended Flood with DLR Redundant Gateway Architecture

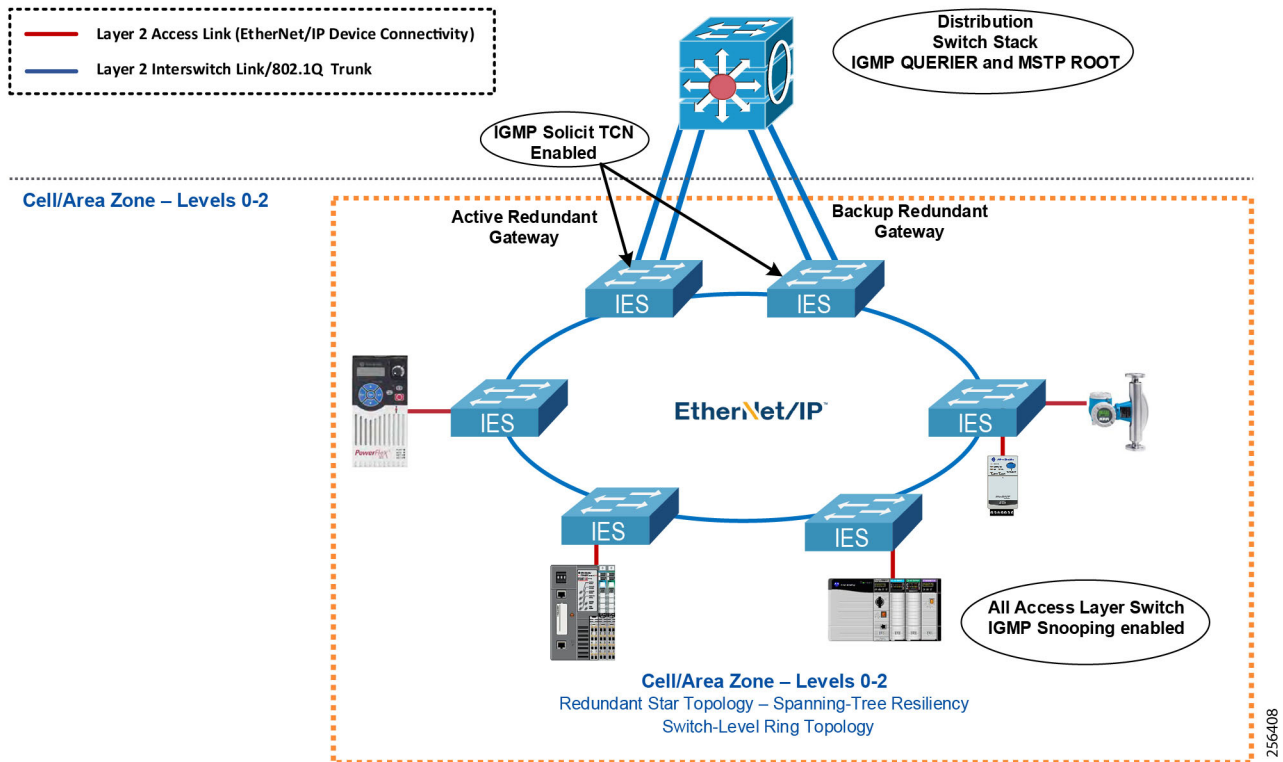


- The Solicit Query at TCN extension can be enabled to direct a Layer 2 in a spanning-tree domain that is not the root bridge, which will issue a query solicitation message when there is a topology change. This is necessary for redundant configurations. When the upstream IGMP snooping querier receives the query solicitation message, it immediately issues an IGMP general query to stop the multicast flooding. It is recommended to enable the Solicit Query at TCN extension enabled globally on the Layer 2 IES when:
 - IACS applications use multicast traffic.
 - The network resiliency MSTP is used as the uplink with DLR Redundant Gateway.

**Note**

If using the Device Manager for configuration, the Solicit Query at TCN extension will be enabled automatically when Redundant Gateway is enabled. Enable this extension only on the active and backup DLR Redundant Gateway IES directly in the ring when MSTP is used as the uplink protocol. See [Figure 2-10](#).

Figure 2-10 IGMP Solicit Query at TCN with DLR Redundant Gateway Architecture

**Note**

For details on how to configure IGMP snooping with Querier, refer to [Chapter 3, “CPwE Device Level Ring Configuration.”](#)

Network Resiliency Protocols

As stated previously, the DLR protocol can coexist with Layer 2 Network Protocols in gateway IES, but these protocols cannot be implemented on DLR ports. Gateway uplink ports can participate in resiliency protocols such as RSTP, MSTP, Per-VLAN Spanning Tree (PVST), Per-VLAN Spanning Tree Plus (PVST+), REP, Flex Links, and EtherChannel. This participation makes installation of a DLR Ring topology into existing network architectures seamless, giving the user the ability to deploy DLR ring architectures into existing network infrastructure with minimal change to existing network protocols.

**Note**

MSTP and REP protocols can be implemented as uplink protocols in larger ring topologies, but cannot co-exist with DLR within the same ring. DLR ports must be segregated from these resiliency protocols.

Distribution and Uplink Resiliency

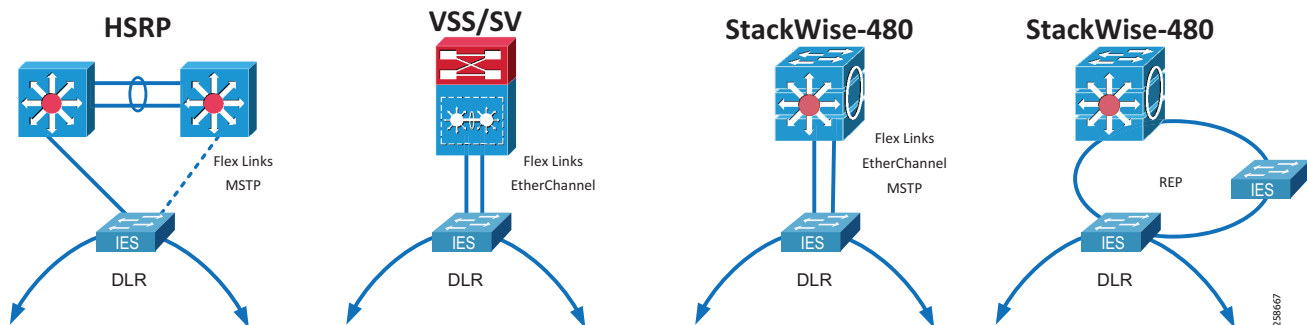
As part of the CPwE DLR Reference Architecture testing, the following uplink technologies were deployed and tested with both the switch-level and mixed IACS device/IES topologies with the DLR protocol; these are graphically represented in [Figure 2-11](#).

Hot Standby Redundancy Protocol (HSRP) is a default gateway redundancy solution developed by Cisco. It allows a highly available network to recover from the failure of the device acting as the default gateway.

Virtual Switching System (VSS) and Stackwise Virtual (SV) are technologies that combines a pair of switches into a single network element. When you create the VSS or SV, one switch becomes the active chassis and the other becomes the standby. VSS is supported on higher end switches like the Cisco Catalyst 4500-X while SV is supported on the Cisco 9500 switches.

Stackwise-480 technology allows you to create a group (switch stack) of Cisco Catalyst 3850 and Cisco Catalyst 9300 switches into a single network element. One switch in the stack is the active switch and controls the switch management for the entire stack.

Figure 2-11 Reference Architectures—Distribution and Uplinking Resiliency Protocol Permutations

**Note**

If MSTP is enabled on the distribution switches connected to the IES running Flex Links, a switch disruption could cause MSTP to converge. This results in traffic loss for up to 30 seconds and transitions the port through the listening and learning states before forwarding traffic. To prevent this loss and allow the port to immediately forward traffic after a convergence event, enable the following command on the downlinks facing the IES: `spanning-tree portfast edge trunk`.

```
Distribution(config)# interface Gi1/0/11
```

```
Distribution(config-if)# spanning-tree portfast edge trunk
```

**Note**

When using the Cisco Catalyst 4500-X as the distribution platform with VSS, during an up convergence of a failover after the SSO, much of the processing power of the VSS Active supervisor engine is consumed in bringing up a large number of ports simultaneously in the VSS Standby switch. As a result, some links might be brought up before the supervisor engine has configured forwarding for the links, causing traffic to those links to be lost until the configuration is complete. As a workaround for the best performance using Multi-Chassis EtherChannel (MEC) downlink connections to the access layer IES, it is recommended the access layer IES uplink ports are configured to use either PAGP or LACP EtherChannel negotiation protocols. Also apply the port-channel load-defer command to the access layer IES port channel interface(s).

```
IES(config)# interface Port-channel15
IES(config-if)# port-channel load-defer
```

Network Capacity

A key aspect of deploying any network architecture is to model and understand network bandwidth capacity in the proposed network. The DLR segments are shared bandwidth with the local DLR node communications and the non-DLR hosts communications that need to leave the access layer. This makes this metric a key factor in DLR network planning. It is also important to understand the application requirements such as type of traffic, RPIs, data sizes, as well as reliability and latency requirements. Integrated Architecture[®] Builder is a Rockwell Automation product that provides a means to plan and configure Logix-based automation systems. This robust tool also allows for system modeling and projected network bandwidth utilization analysis.

More information on this product can be found on the Rockwell Automation Integrated Architecture Builder web page:

<http://www.rockwellautomation.com/global/support/integrated-architecture-builder.page>

All CPwE DLR testing of the DLR architecture included 128 I/O connections at varying RPIs as well as traffic generation at approximately 32,000 packets per second (pps) sized at 70 bytes. Table 2-6 shows IACS traffic types and CIP standards used in the testing of the DLR architecture. These numbers are for reference only and do not represent any limits of the DLR protocol and architectures.

Table 2-6 Use of IACS Application with DLR Architecture

IACS Traffic Type	CIP Standard	RPI / CUR	Type of Traffic
Motion Control	CIP Motion	1-2 ms ¹	UDP unicast
Time Synchronization	CIP Sync	N/A	UDP multicast
Safety Control	CIP Safety	10 ms (default)	UDP unicast (default)
I/O Control	CIP Class 1	20 ms (default)	UDP unicast (default)
Peer-to-Peer Control	CIP Class 1	20 ms (default)	UDP multicast ²
Peer-to-Peer Messaging	CIP Class 3	Timeout 30 sec (default)	TCP unicast (default)
Information and Diagnostics (HMI)	CIP Class 3	1 sec (default)	TCP unicast

1. The course update rate (CUR) recommended for the switch-level ring is 1 ms while for the mixed IACS device/IES ring is 2 ms. The actual impact may vary depending on CIP motion system, type of controller, and axis configuration.
2. For Peer-to-Peer Control Produce/Consume applications the default is unicast and is still the recommended option. Multicast was used for testing only.

System Components Overview

Allen-Bradley Stratix 5400 Series IES

This platform has been selected for the CPwE DLR Solution for the following reasons:

- Bandwidth and capacity to grow with your networking requirements.
- Cisco IOS software features for smooth IT integration and policy consistency.
- Robust resiliency enabled by 4x Gigabit Ethernet uplink ports for Device Level Ring (DLR) for ring topology, EtherChannel and Flex Links for redundant star topology, and redundant power input.
- True zero-touch replacement for middle-of-the-night or middle-of-nowhere situations.
- Simplified software upgrade path with universal images.
- Industrial environmental compliance and certifications.
- Industrial protocol support: e.g., EtherNet/IP and PROFINET.

Distribution Switch Platforms

Cisco Catalyst 3850 Switch

The Cisco Catalyst 3850 Series multigigabit and 10-Gbps network switches provide both wired and wireless to support the scalability of a large network. These switches support stacking and are ideal for distribution in the CPwE network architecture. They offer different models for aggregation; details can be found at: <https://www.cisco.com/c/en/us/products/switches/catalyst-3850-series-switches/index.html#~stickynav=1>

**Note**

Cisco announced the end-of-sale and end-of-life dates for the Cisco Catalyst 3850 switches. The last day to order the affected product(s) was October 30, 2020. The direct replacement for the Cisco Catalyst 3850 switch is the Cisco Catalyst 9300 switch. Details can be found at: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/eos-eol-notice-c51-743072.html>

Cisco Catalyst 9300 Switch

The Cisco Catalyst 9300 Series is the next generation multigigabit and 10-Gbps network switch that provides both wired and wireless to support the scalability of a large network. Built for security, IoT, and the cloud, these network switches form the foundation for Cisco's Software-Defined Access, Cisco's leading enterprise architecture. These switches support Stackwise Virtual and are ideal for distribution in the CPwE network architecture. They offer different models for aggregation; details can be found at: <https://www.cisco.com/c/en/us/products/switches/catalyst-9300-series-switches/index.html#~stickynav=1>

Cisco Catalyst 4500-X Switch

The Cisco Catalyst 4500-X Series is a fixed aggregation switch that delivers best-in-class scalability, simplified network virtualization, and integrated network services for space-constrained environments in campus networks. These switches support virtual switching system (VSS) and are ideal for distribution in the CPwE network architecture. They offer different models for aggregation; details can be found at:

<https://www.cisco.com/c/en/us/products/switches/catalyst-4500-x-series-switches/index.html#~stickynav=1>

**Note**

Cisco announced the end-of-sale and end-of-life dates for the Cisco Catalyst 4500-X switches. The last day to order the affected product(s) was October 30, 2020. The direct replacement for the Cisco Catalyst 4500-X switch is the Cisco Catalyst 9500 switch. Details can be found at:

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-x-series-switches/eos-eol-notice-c51-743098.html>

Cisco Catalyst 9500 Switch

The Cisco Catalyst 9500 Series is the next generation 100/40-Gbps switch purpose built for the enterprise campus. Designed for security, the Internet of Things (IoT), and the cloud, Cisco Catalyst 9500 fixed-core switches are high-density building blocks for a next-generation, intent-based network. These switches support virtual stackwise and are ideal for distribution in the CPwE network architecture. They offer different models for aggregation; details can be found at:

<https://www.cisco.com/c/en/us/products/switches/catalyst-9500-series-switches/index.html#~stickynav=1>

Rockwell Automation FactoryTalk Network Manager

A purpose-built platform for managing IACS networks, Rockwell Automation FactoryTalk Network Manager (FTNM) software is designed to provide insight into the design, performance, and health of an IACS network. Use FactoryTalk Network Manager to view your network topology and manage switch-level alarms as they happen. Monitor the health of network devices and reduce downtime to improve overall IACS equipment efficiency. FactoryTalk Network Manager:

- Discovers both network and IACS devices including IACS devices across a ControlLogix backplane.
- Generates an overall topology and a device-centric view of plant-wide or site-wide assets for increased network visibility.
- Captures managed switch level alarms and events in real-time for more precise troubleshooting.
- Provides DLR-specific alarms, diagnostics, and DLR topology overlay.
- Provides historical data and logging for analysis and resolution.
- Provides configuration backup and firmware revision management of Stratix IES for simplified deployment and maintenance.

More details about FactoryTalk Network Manager can be found at:

https://literature.rockwellautomation.com/idc/groups/literature/documents/pp/ftalk-pp024_-en-p.pdf

ControlLogix Redundancy

The ControlLogix Redundancy System is a system that provides greater availability because it uses a redundant chassis pair. The redundant chassis pair maintains process operation when events, such as a fault on a controller occur that stop process operation on non-redundant systems.

The redundant chassis pair includes two synchronized ControlLogix chassis with identically specific components in each. For example, one redundancy module and at least one ControlNet[®] or EtherNet/IP communication module are required.

Controllers are typically used in redundancy systems, but are not required if the application only requires communication redundancy. The application operates from a primary chassis, but can switch over to the secondary chassis and components if necessary.

ControlLogix Redundancy with Device Level Ring

CPwE DLR reference architectures has been tested with ControlLogix Redundancy including redundant PAC chassis with EtherNet/IP communicating to I/O devices, other PAC's and FactoryTalk applications. ControlLogix Redundancy included the following components and considerations.

- EtherNet/IP communications for I/O and Produced Consumed data configured for IP address swapping during a chassis switchover.
- ControlLogix Redundancy should be positioned within the DLR and traffic should remain local to ring and not traverse the DLR Redundant Gateways.
- In multiple ring architectures ControlLogix Redundancy traffic should remain local to the ring on which the chassis and associated I/O reside.
- In the event of a DLR failure, proper placement should be considered for ControlLogix Redundancy chassis pairs in the network architecture. Reference Architectures illustrate chassis placement on either side of the ring to lessen the impact from DLR devices that could fail on the ring.
- ControlLogix Redundancy firmware revision 31.052 or later, FactoryTalk Linx 6.11 or later.



Note

ControlLogix redundancy systems were positioned in reference architectures for network testing purposes only and no faults or chassis switchovers occurred during testing. More details regarding ControlLogix redundancy high availability Ethernet system testing and architectures can be found at:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/463904

(Knowledgebase article requires Rockwell Automation account for viewing)

Switch-Level DLR Reference Architectures

A switch-level ring consists of only DLR capable IES with IACS devices connected to the DLR IES via star or linear and can be configured in the same or different VLANs. Currently, the Stratix 5700 and Stratix 5400 are the only managed IES that implement the DLR protocol and Redundant Gateways. DLR ring speeds can be set to either 100 Mbps/full duplex or 1 Gbps/full duplex but may not be intermixed between ring participants within a single ring. It is recommended that there not be more than 24 IES within the DLR ring for all switch-level DLR ring deployments. This limit is based on the number of hosts per network that is recommended per CPwE best practices using a /24 subnet allowing for 253 total hosts. In addition, CPwE recommends creating smaller rings to lower the probability of single and dual fault scenarios. The DLR protocol is only single-fault tolerant. As such, a larger number of ring participants will result in a higher probability of experiencing multiple ring faults. This results in the loss of a network segment.

DLR requires one ring participant to be configured as a DLR supervisor to manage the ring. After a single fault in the ring, essentially it becomes a linear topology and a ring supervisor is no longer needed for loop prevention. In rare cases of a software fault not detected on the physical layer, a backup DLR supervisor will be able to manage the loop. In this case it is recommend that no more than two supervisors are configured in a single ring.

The following application communication and configuration apply to all Switch-Level DLR use cases:

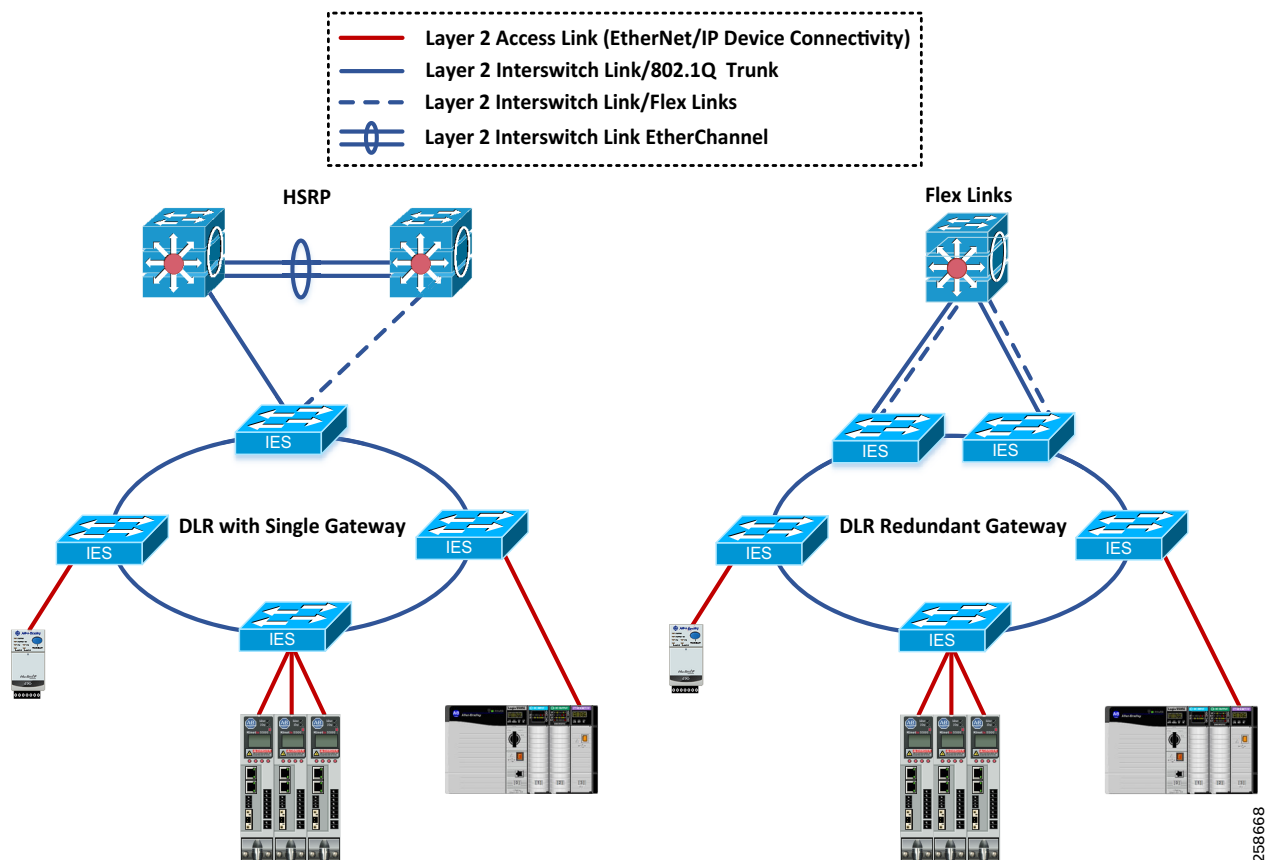
- All devices participating in the reference architecture were connected to the DLR via star topology to one of the Stratix IES on the ring. All Stratix IES ring participants were configured with PTP End-to-End Transparent mode.
- CIP Standard and CIP Safety Produced/Consumed (P/C) (Class 1), and HMI (Class 3) traffic were local on the DLR as well as outside of the local DLR. CIP Safety I/O RPIs used the default 10 ms and default of unicast. CIP Standard I/O RPIs used the default 20 ms and default of unicast. Both CIP Standard and CIP Safety P/C RPIs used the default 20 ms and configured as multicast. For both I/O and P/C applications, unicast is the default and is still the recommended option. Multicast was used for testing purposes only.

Recommended Topologies

A switch-level DLR consists solely of DLR-capable, access layer IES acting as ring participants. As with device-level DLR, switch-level DLR speeds can be set to either 100 Mbps or 1 Gbps, but may not be intermixed from IES to IES. The Stratix 5700 and Stratix 5400, are the only managed IES that implement the DLR protocol.

Figure 2-12 illustrates two converged single and Redundant Gateway switch-level DLR architectures recommended for usage with the DLR protocol in the CPwE for switch-level DLR deployments with uplinks to distribution switches.

Figure 2-12 Switch-Level DLR Ring Connected Directly to Layer 3 Distribution Switches



**Note**

DLR-Capable Stratix Industrial Ethernet Switches have specific ports for which DLR can be implemented. The complete list of DLR compatible ports for the Stratix 5700 and Stratix 5400 can be found in [Appendix A, “DLR Port Choices for Stratix Switches.”](#)

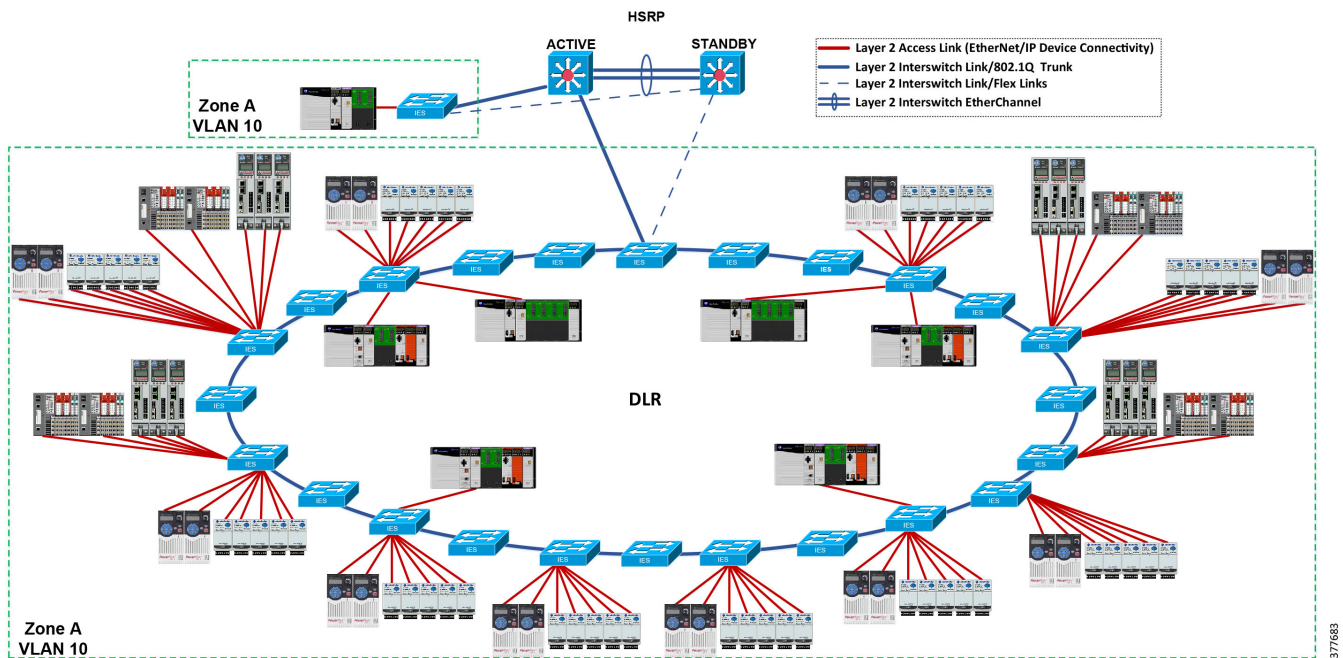
**Note**

Hot Standby Router Protocol (HSRP) is shown as the distribution resiliency protocol in all of the following architecture figures. However, reference architecture testing and verification was also completed with VSS (Catalyst 4500-X) and Stackwise-480 (Catalyst 3850) technologies configured. Further, EtherChannel and Flex Links were also configured as IES-distribution link resiliency protocols and are not shown.

Reference Architecture 1—Single Switch-Level DLR with Single Gateway

Figure 2-13 represents reference architecture testing for a single 24 IES switch-level ring with various distribution and uplinking resiliency protocols. A single switch-level ring media can be either copper, fiber (single-mode or multi-mode), or a combination of both. Hence media types between the segments can be intermixed. The single switch-level ring speed can be either 100 Mbps or 1 Gbps but cannot be both. Therefore, the entire single ring must run at the same speed and cannot be intermixed. In this reference architecture a single VLAN is used throughout all IACS and IES devices in the ring.

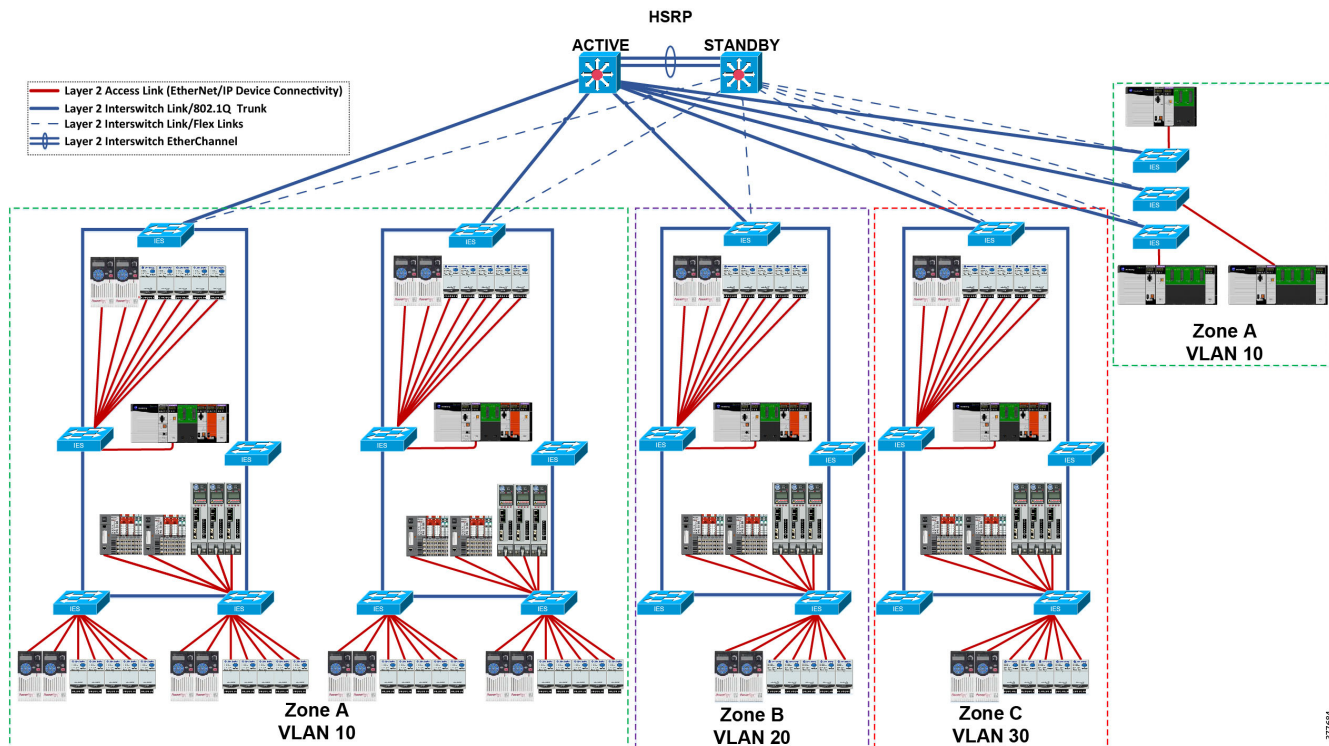
Figure 2-13 DLR Reference Architectures—Switch-Level Ring (24 Switches)



Reference Architecture 2—Switch-Level VLAN Segmented DLR with Single Gateway

Figure 2-14 represents reference architecture testing for multiple switch-level DLR rings with various distribution and uplinking resiliency protocols. A single switch-level ring media can be either copper, fiber (single-mode or multi-mode), or a combination of both. This means that media types between the segments can be intermixed. A single switch-level ring speed can be either 100 Mbps or 1 Gbps, but cannot be both. Therefore, the entire single ring must run at the same speed and cannot be intermixed. In this reference architecture each ring can exist in a unique VLAN or the same VLAN.

Figure 2-14 DLR Reference Architectures—Multi-VLAN Segmentation



Expected Convergence Times with Single Gateway

Reference architecture testing for a single switch-level DLR, utilizing Single Gateway, produced convergence times of 3 ms or less for a localized traffic disruption. This is consistent with the ODVA, Inc. standard for DLR.

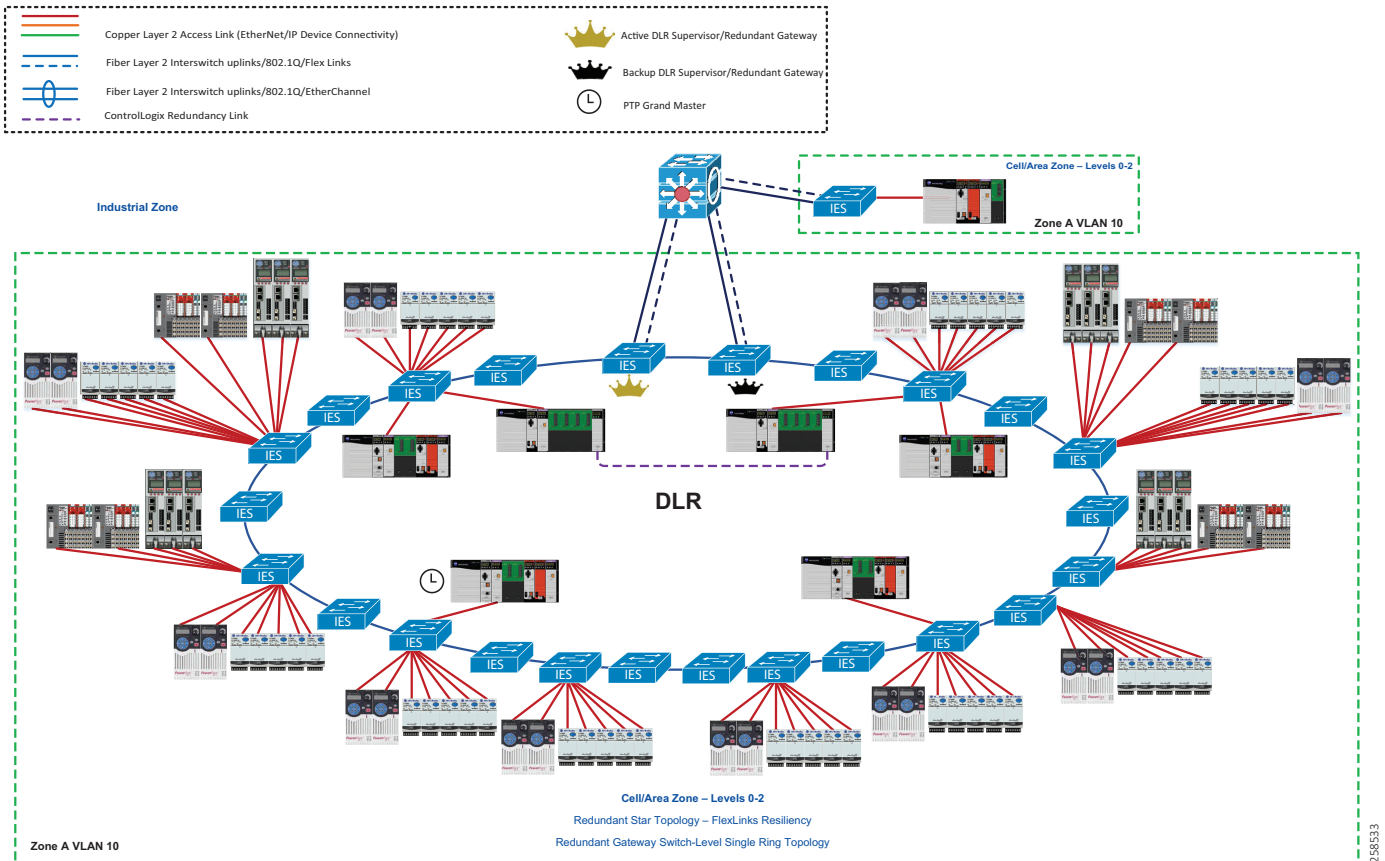
Reference architecture testing of the switch-level DLR with a variety of distribution platforms resulted in convergence times that are consistent with what is published in the *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide* (http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf).

Refer to the corresponding tables in that document for guidance on convergence times when implementing switch-level DLR.

Reference Architecture 3—Single Switch-Level DLR with Redundant Gateway

Figure 2-15 represents reference architecture testing for a single 24 IES switch-level ring with Redundant Gateway with various distribution and uplinking resiliency protocols. A single switch-level ring media can be either copper, fiber (single-mode or multi-mode), or a combination of both. Hence media types between the segments can be intermixed. The single switch-level ring speed can be either 100 Mbps or 1 I Gbps but cannot be both. Therefore, the entire single ring must run at the same speed and cannot be intermixed. In this reference architecture a single VLAN is used throughout all IACS and IES devices in the ring.

Figure 2-15 DLR Reference Architectures-Switch-Level DLR with Redundant Gateway (24 Switches)



Expected Convergence Times with Redundant Gateway

Convergence times for single switch-level DLR with Redundant Gateway reference architecture for traffic disruption localized to the DLR ring were 3 ms or less. This is consistent with the ODVA, Inc. standard for DLR. This DLR convergence time had no impact on local CIP Standard and CIP Safety control and messaging applications; standard and safety controllers reported no I/O or produce/consume connection loss within the local DLR. Additionally, high-speed motion application with a coarse update rate (CUR) of 2 ms showed no impact. Therefore, no motion faults occurred during traffic disruption localized to the DLR ring. The recommendation is to use CUR no lower than 2 ms for single switch-level DLR with Redundant Gateway. It was observed and recommended not to apply standard and safety applications or high-speed motion beyond the local DLR as it pertains to the single ring architecture.

- Active Gateway Failure describes a test action that was performed to simulate the failure of the active Redundant Gateway IES resulting in the backup Redundant Gateway IES becoming the new operational active Redundant Gateway.
- Active Gateway Recovery describes a test action was performed to simulate the recovery of the previously failed active Redundant Gateway IES while the backup Redundant Gateway reassumes its original role as backup Redundant Gateway resulting in normal operational state.
- Traffic direction referenced in the tables as DLR Cell/Area Zone to Outside the DLR is illustrated in [Figure 2-16](#). Traffic direction reference in the tables as Outside the DLR to DLR Cell/Area Zone is illustrated in [Figure 2-17](#). The results in [Table 2-7](#) (Unicast) and [Table 2-8](#) (Multicast) illustrate Redundant Gateway switchover maximum convergence times for Layer 2 uplinks connected to Redundant Gateway switches to the distribution switch with multiple uplinking technologies and distribution platforms for traffic sourced from DLR Cell/Area Zone destined for the Outside network.

Network Infrastructure

Traffic sourced from Outside DLR

Zone A VLAN 10

Active Redundant Gateway

Backup Redundant Gateway

EtherNet/IP

Sourced from Inside DLR

Cell/Area Zone – Levels 0-2

Redundant Star Topology – Spanning-Tree Resiliency Switch-Level Ring Topology

Zone A VLAN 10

Figure 2-17 Traffic from Outside the DLR to DLR Cell/Area Zone

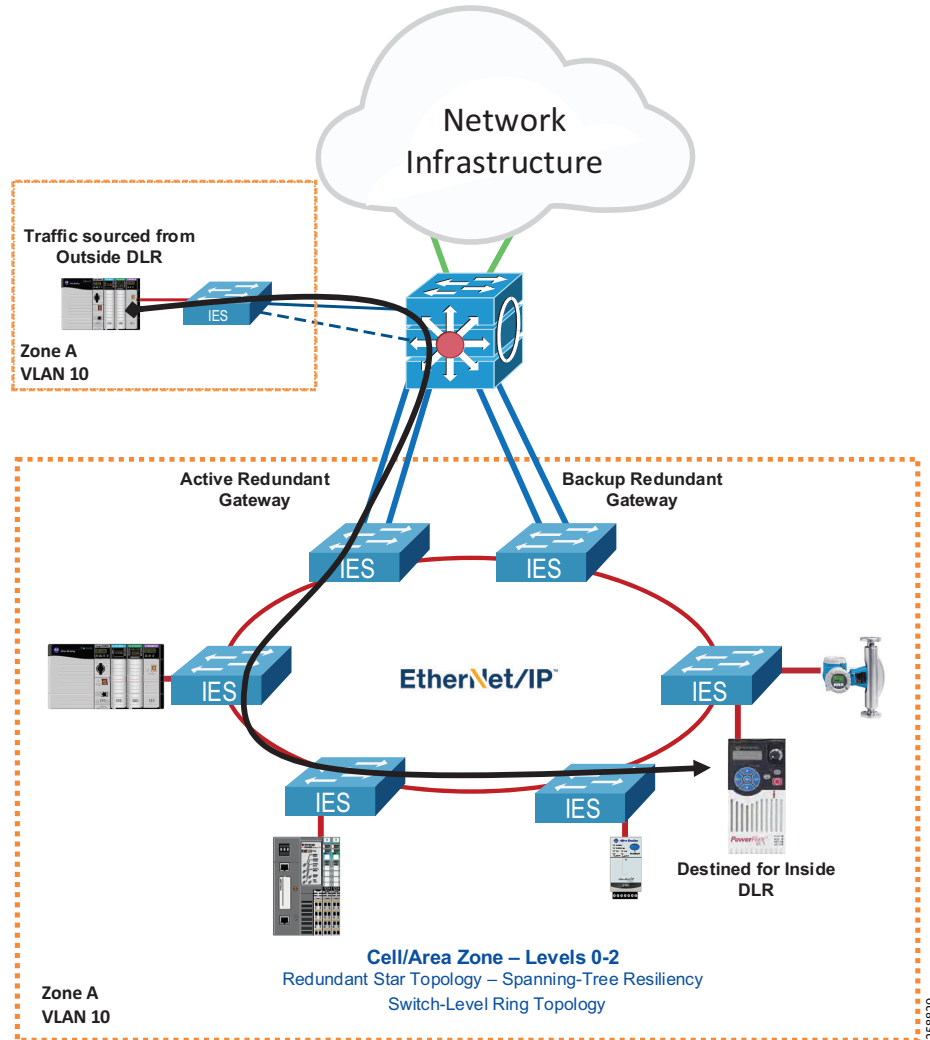


Table 2-7 Max Convergence Unicast—Switch-Level DLR with Redundant Gateway

Description Type	Traffic Type	Unicast—Maximum Convergence Time (ms)			
		Flex Links	EtherChannel	MSTP	REP
Active Gateway Failure (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	10	11	10	30
Active Gateway Recovery (Traffic from Cell/Area Zone to Outside the DLR)	L2	42	95	83	280
Active Gateway Failure (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	82	48	137	87

Table 2-7 Max Convergence Unicast—Switch-Level DLR with Redundant Gateway (continued)

Active Gateway Recovery (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	124	64	83	62
Active Gateway Failure (Traffic Local to Ring)	L2	2	2	2	2
Active Gateway Recovery (Traffic Local to Ring)	L2	33	40	2	11
Redundant Star/Ring Topology Resiliency Protocol (Link and Switch) ¹	L2/L3	N/A	N/A	N/A	N/A

1. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:
Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

Table 2-8 Max Convergence Multicast—Switch-Level DLR with Redundant Gateway

Description Type	Traffic Type	Multicast—Maximum Convergence Time (ms)			
		Flex Links	EtherChannel	MSTP	REP
Active Gateway Failure (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	10	10	10	30
Active Gateway Recovery (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	6	8	6	6
Active Gateway Failure (Traffic from Outside the DLR Cell/Area Zone)	L2	10	183	80	85
Active Gateway Recovery (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	5	6	6	6
Active Gateway Failure (Traffic Local to Ring)	L2	2	2	3	2
Active Gateway Recovery (Traffic Local to Ring)	L2	5	8	4	6
Redundant Star/Ring Topology Resiliency Protocol (Link and Switch) ¹	L2/L3	N/A	N/A	N/A	N/A

1. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:
Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

**Note**

Recovery of a failed Redundant Gateway to restore the original active gateway as primary should be initiated during a maintenance window to minimize production downtime.

**Note**

It is recommended to use an uninterruptable power supply (UPS), such as Rockwell Automation Bulletin 1609 UPS, for backup of Redundant Gateway switches to prevent unnecessary Redundant Gateway switchovers and network downtime from power bumps and outages.

For the best performance for IACS applications when communicating to and from outside the DLR, it is recommended to implement the unicast connection type and to use Flex Links or EtherChannel Layer 2 resiliency protocols for the uplinks in redundant star topology.

Multicast traffic should be kept local to the DLR ring and limited from traversing the uplinks. This type of traffic may include the following:

- Multicast I/O (examples are ControlLogix Redundancy I/O and IEEE 1588 CIP Sync traffic)
- Multicast Produced/Consumed Tags

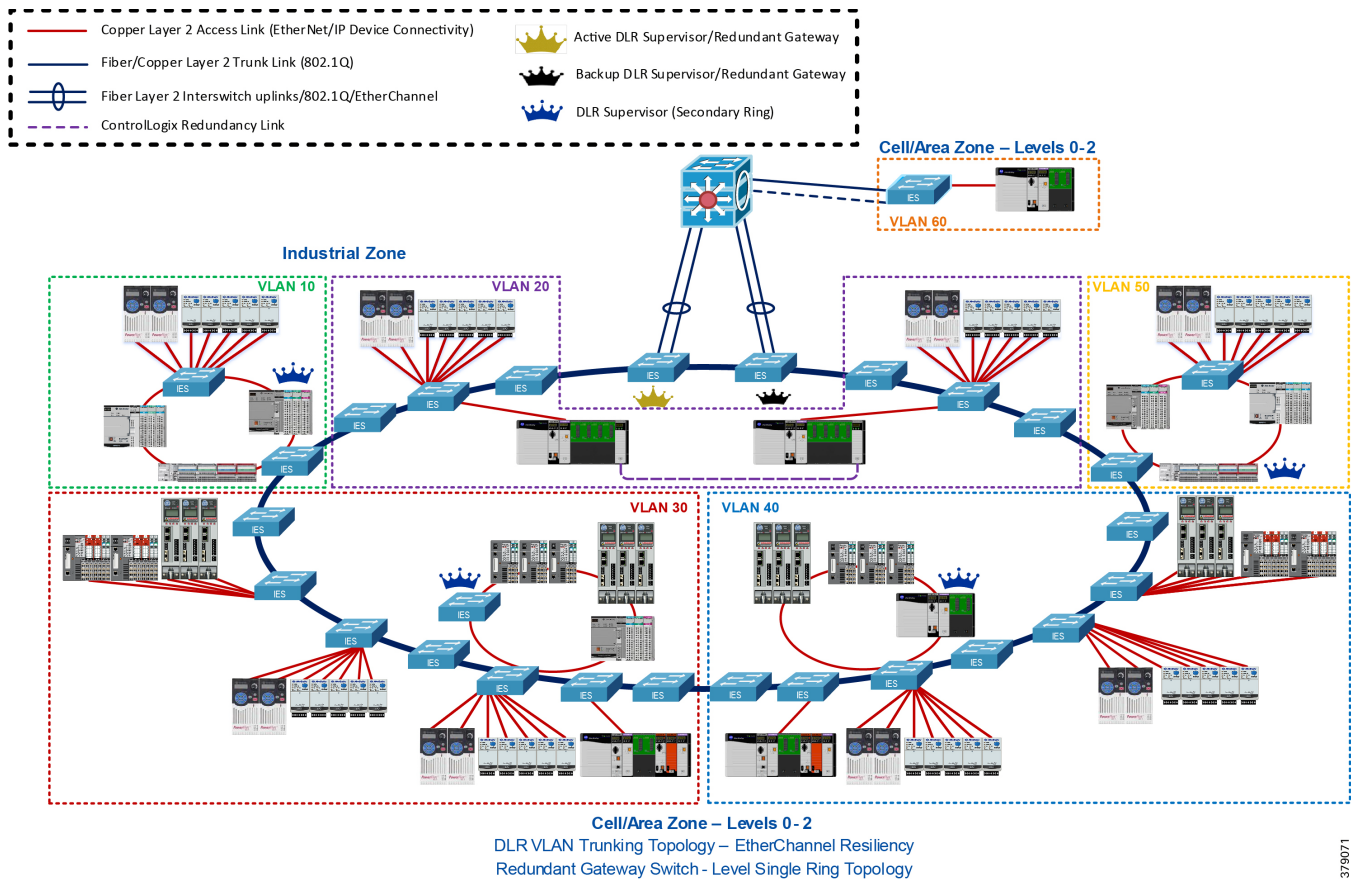
Reference architecture testing of the single DLR switch-level ring utilizing a Redundant Gateway with a variety of distribution platforms produced results that were consistent with the convergence times published in the *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:

Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

Reference Architecture 4—Single Switch-Level DLR with Redundant Gateway and DLR VLAN Trunking

Figure 2-18 represents reference architecture testing for a single 24 IES switch-level ring with Redundant Gateway and DLR VLAN Trunking with various distribution and uplinking resiliency protocols. A single switch-level ring media can be either copper, fiber (single-mode or multi-mode), or a combination of both. Hence media types between the segments can be intermixed. The single switch-level ring speed can be either 100 Mbps or 1 Gbps but cannot be both. Therefore, the entire single ring must run at the same speed and cannot be intermixed. In this reference architecture multiple VLANs are used throughout all IES devices in the ring.

Figure 2-18 Reference Architecture 4—Single Switch-Level DLR with Redundant Gateway and DLR VLAN Trunking

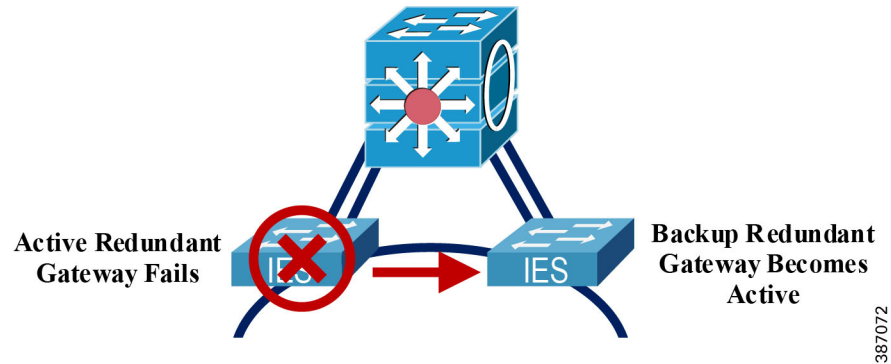


Expected Convergence Times with Redundant Gateway and DLR VLAN Trunking

Convergence times for single switch-level DLR with Redundant Gateway and DLR VLAN Trunking reference architecture for traffic disruption localized to the DLR ring were 3 ms or less. This is consistent with the ODVA, Inc. standard for DLR. This DLR convergence time had no impact on local CIP Standard and CIP Safety control and messaging applications; standard and safety controllers reported no I/O or produce/consume connection loss within the local DLR when safety devices resided on the same VLAN as the safety controller. Additionally, high-speed motion application with a coarse update rate (CUR) of 2 ms showed no impact. Therefore, no motion faults occurred during traffic disruption localized to the DLR ring when high-speed motion resided on the same VLAN as the motion controller. The recommendation is to use CUR no lower than 2 ms for single switch-level DLR with Redundant Gateway and DLR VLAN Trunking. It was observed and recommended not to apply standard and safety applications or high-speed motion beyond the local DLR or routed to different VLANs as it pertains to the single switch ring architecture with the DLR Trunking feature.

Figure 2-19 illustrates the test action of the Active Gateway Failure for data collection purposes to capture expected packet loss in milliseconds for Redundant Gateway convergence times.

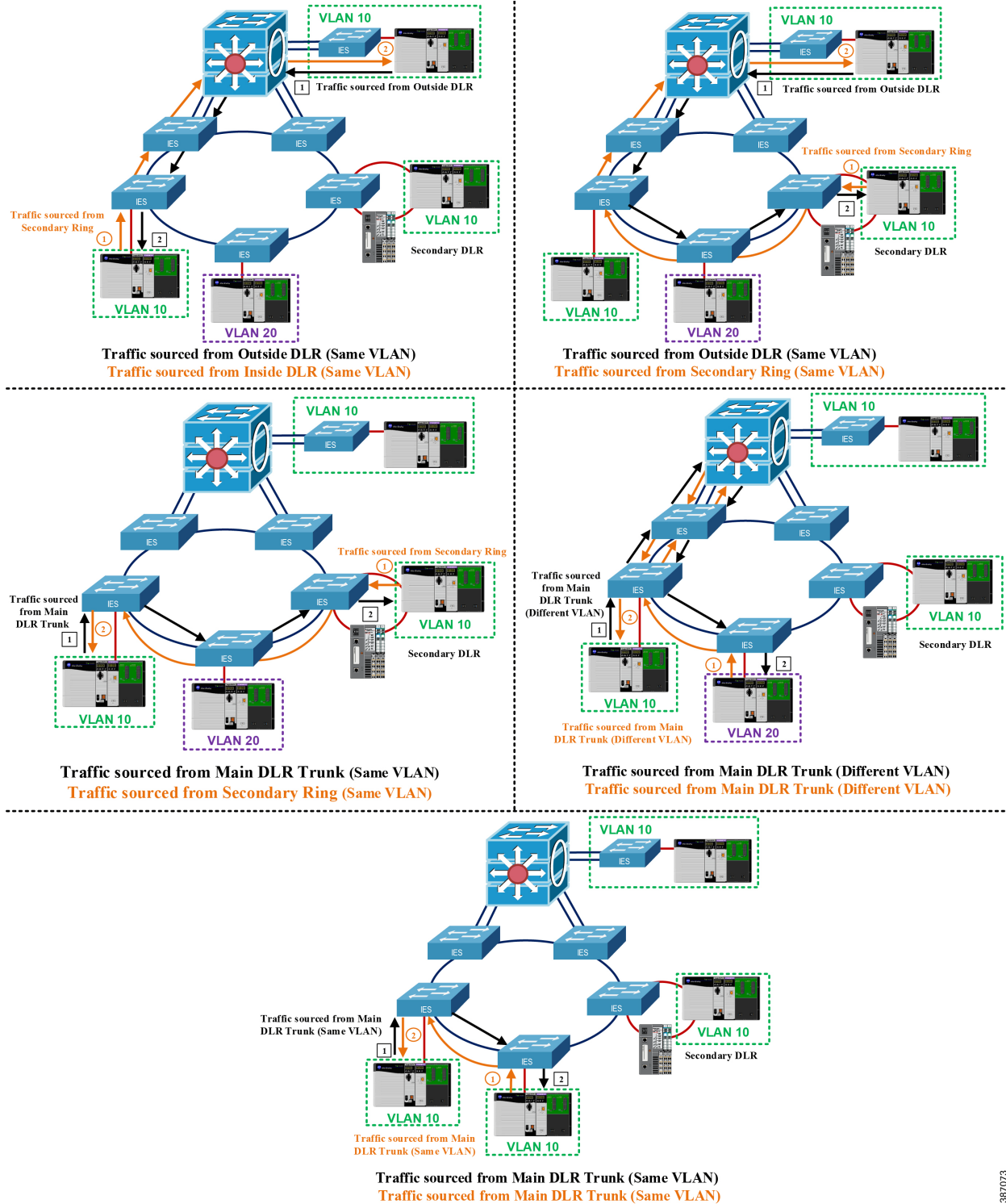
Figure 2-19 DLR Active Redundant Gateway Failover and Recovery



The following data tables represent the test action for Active Gateway Failure from different source and destination points within the reference architecture.

- Active Gateway Failure describes a test action that was performed to simulate the failure of the active Redundant Gateway IES resulting in the backup Redundant Gateway IES becoming the new operational active Redundant Gateway.
- Traffic direction referenced in the tables are illustrated in [Figure 2-20](#). The results in [Table 2-9](#) (Unicast) and [Table 2-10](#) (Multicast) illustrate Redundant Gateway switchover maximum convergence times for Layer 2 uplinks connected to Redundant Gateway switches to the distribution switch with multiple uplinking technologies and distribution platforms for traffic sourced from DLR Cell/Area Zone destined for outside the network.

Figure 2-20 DLR VLAN Trunking Traffic Flow Overview



387073

Table 2-9 Max Convergence Unicast—Single Switch-Level DLR with Redundant Gateway and DLR VLAN Trunking

Disruption Type	Traffic Type	Unicast - Maximum Convergence Time (ms)			
		Flex Links	EtherChannel	MSTP	REP
Active Gateway Failure (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	10	11	11	10
Active Gateway Failure (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	159	216	160	86
Active Gateway Failure (Traffic from Outside the DLR to Cell/Area Zone Secondary DLR)	L2	83	150	160	86
Active Gateway Failure (Traffic from Cell/Area Zone Secondary DLR to Outside the DLR)	L2	11	10	11	11
Active Gateway Failure (Traffic local from the Main DLR Trunk Ring to Cell/Area Zone Secondary DLR)	L2	0	0	0	0
Active Gateway Failure (Traffic local on the Main DLR Trunk Ring - Same VLAN)	L2	0	0	0	0
Active Gateway Failure (Traffic local on the Main DLR Trunk Ring - Different VLANs)	L3	159	149	160	84
Redundant Star/Ring Topology Resiliency Protocol (Link and Switch)	L2/L3	N/A ¹	N/A ¹	N/A ¹	N/A ¹

1. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide* (http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf).

Table 2-10 Max Convergence Multicast—Single Switch-Level DLR with Redundant Gateway and DLR VLAN Trunking

Disruption Type	Traffic Type	Multicast - Maximum Convergence Time (ms)			
		Flex Links	EtherChannel	MSTP	REP
Active Gateway Failure (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	79	796	10	0
Active Gateway Failure (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	164	291	11	9
Active Gateway Failure (Traffic from Outside the DLR to Cell/Area Zone Secondary DLR)	L2	0	0	0	0

Table 2-10 Max Convergence Multicast—Single Switch-Level DLR with Redundant Gateway and DLR VLAN Trunking (continued)

Active Gateway Failure (Traffic from Cell/Area Zone Secondary DLR to Outside the DLR)	L2	0	0	0	0
Active Gateway Failure (Traffic local from the Main DLR Trunk Ring to Cell/Area Zone Secondary DLR)	L2	0	0	0	0
Active Gateway Failure (Traffic local on the Main DLR Trunk Ring - Same VLAN)	L2	0	0	0	0
Active Gateway Failure (Traffic local on the Main DLR Trunk Ring - Different VLANs)	L3	N/A ¹	N/A ¹	N/A ¹	N/A ¹
Redundant Star/Ring Topology Resiliency Protocol (Link and Switch)	L2/L3	N/A ²	N/A ²	N/A ²	N/A ²

1. Multicast routing was not in scope for this test criteria.
2. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide* (http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf).

To get the best performance of IACS applications when communicating to and from outside the DLR, it is recommended to implement a unicast connection type and to use EtherChannel for Layer 2 resiliency protocols for the uplinks in redundant star topology.

Multicast traffic should be kept local to the DLR ring and limited from traversing the uplinks. This type of traffic may include the following:

- Multicast I/O (examples are ControlLogix redundancy I/O and IEEE 1588 CIP Sync traffic)
- Multicast Produced/Consumed Tags



Note

Testing the recovery of a failed Redundant Gateway has shown unusually high packet loss for unicast and multicast traffic resulting in a loss of all CIP connections in the DLR. The following events were recorded upon recovery of the active Redundant Gateway and/or backup Redundant Gateway:

- Local CIP Standard and CIP Safety control and messaging applications; standard and safety controllers reported faults for I/O and/or produce/consume for connection loss.
- High speed motion reported an axis error and all motion halted requiring a manual reset to restart.
- ControlLogix redundancy become disqualified from high multicast packet loss detected on the main ring.
- Multicast flooding.



Warning

Multicast flooding can occur from a network topology when unknown multicast traffic is flooded out a switch port. Multicast flooding can adversely impact network performance and IACS applications. In severe cases, excessive network flooding may result in IACS devices faulting.

**Warning**

Recovery of a failed Redundant Gateway switch should be initiated during a maintenance window to minimize production downtime.

**Warning**

Firmware upgrades of the Redundant Gateway switches should be initiated during a maintenance window to minimize production downtime. Firmware upgrades require a switch reload for the new firmware version to become active. Manual interventions may be required for IACS devices that were affected from the firmware upgrade reload process.

**Note**

It is recommended to use an uninterruptable power supply, such as Rockwell Automation Bulletin 1609, for backup of Redundant Gateway switches to prevent unnecessary Redundant Gateway switchovers and network downtime from power bumps and outages.

Reference architecture testing of single switch-level DLR with Redundant Gateway and DLR VLAN Trunking with a variety of distribution platforms results were consistent with the convergence times published in the Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:

- *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

Mixed Device/Switch-Level DLR Reference Architectures

A mixed IACS device/switch-level ring consists of a combination of DLR-capable devices and DLR-capable IES acting as ring participants. While single or multiple rings can be configured in a mixed device/switch-level architecture, there are a number considerations such as configuration and protocol compatibility. See [Unsupported Topologies](#) for more details. Currently, the Stratix 5700 and Stratix 5400, are the only managed IES that implement the DLR protocol and Redundant Gateways. The Stratix 5400 is the only IES capable of supporting as many as three device-level rings simultaneously on the same IES.

DLR ring speeds can be set to either 100 Mbps/full duplex or 1 Gbps/full duplex but may not be intermixed between ring participants within a single ring. DLR-capable devices as ring participants must be capable of communicating at the chosen ring speed and full duplex. Selected Stratix 5700 IES support up to two 1 Gigabit Ethernet ports. Although selected Stratix 5400 IES support anywhere from four 1 Gigabit Ethernet port IES configuration to an all Gigabit Ethernet port configuration. The Ethernet Taps (1783-ETAP) only support 100 Mbps Fast Ethernet ports and do not support Redundant Gateways.

It is recommended to keep ring node count to 50 or lower within a single DLR ring for mixed device/switch-level DLR ring deployments. The worst-case fault recovery time in a 50-node DLR network is 3 ms. This limit is based on DLR performance metrics, default beacon interval value of 400 μ s and timeout value of 1960 μ s. The default performance metrics are optimized for a maximum of 50 nodes, single copper ring at 100 Mbps and full-duplex. It is recommended the copper cable length between any two nodes in the entire ring is not more than 100 meters. Exceeding the 50 node threshold is possible, but there should be an expectation of a decrease in performance related to ring fault detection and recovery time and a requirement to change beacon timeout values to longer intervals. This is due to the increase in time required for DLR frames to traverse the entire ring. Also, note that the DLR protocol is only single-fault tolerant. As such, a larger amount of ring participants will result in a higher probability of experiencing multiple ring faults, resulting in the loss of a network segment.

DLR requires one ring participant to be configured as a DLR supervisor to manage the ring. After a single fault in the ring, essentially it becomes a linear topology and a ring supervisor is no longer needed for loop prevention. In rare cases of a software fault not detected on the physical layer, a backup DLR supervisor will be able to manage the loop. In this case it is recommended that no more than two supervisors are configured in a single ring.

The following application communication and configuration apply to all Single Mixed Device/Switch-Level DLR use cases.

- The high-speed CIP Motion traffic between the ControlLogix CIP Motion controller and CIP Motion drives with the Coarse Update Rate (CUR) of 2 ms were local on the DLR. The motion controller was outside of the DLR connected via star topology to one of the Stratix IES on the ring while all drives were ring participants. All Stratix IES ring participants were configured with PTP End-to-End Transparent mode.
- CIP Standard and CIP Safety Produced/Consumed (P/C) (Class 1), and HMI (Class 3) traffic were local on the DLR as well as outside of the local DLR. CIP Safety I/O RPIs used the default 10 ms and default of unicast. CIP Standard I/O RPIs used the default 20 ms and default of unicast. Both CIP Safety and CIP Standard P/C RPIs used the default 20 ms and configured as multicast. For both I/O and P/C applications, unicast is the default and is still the recommended option. Multicast was used for testing purposes only.



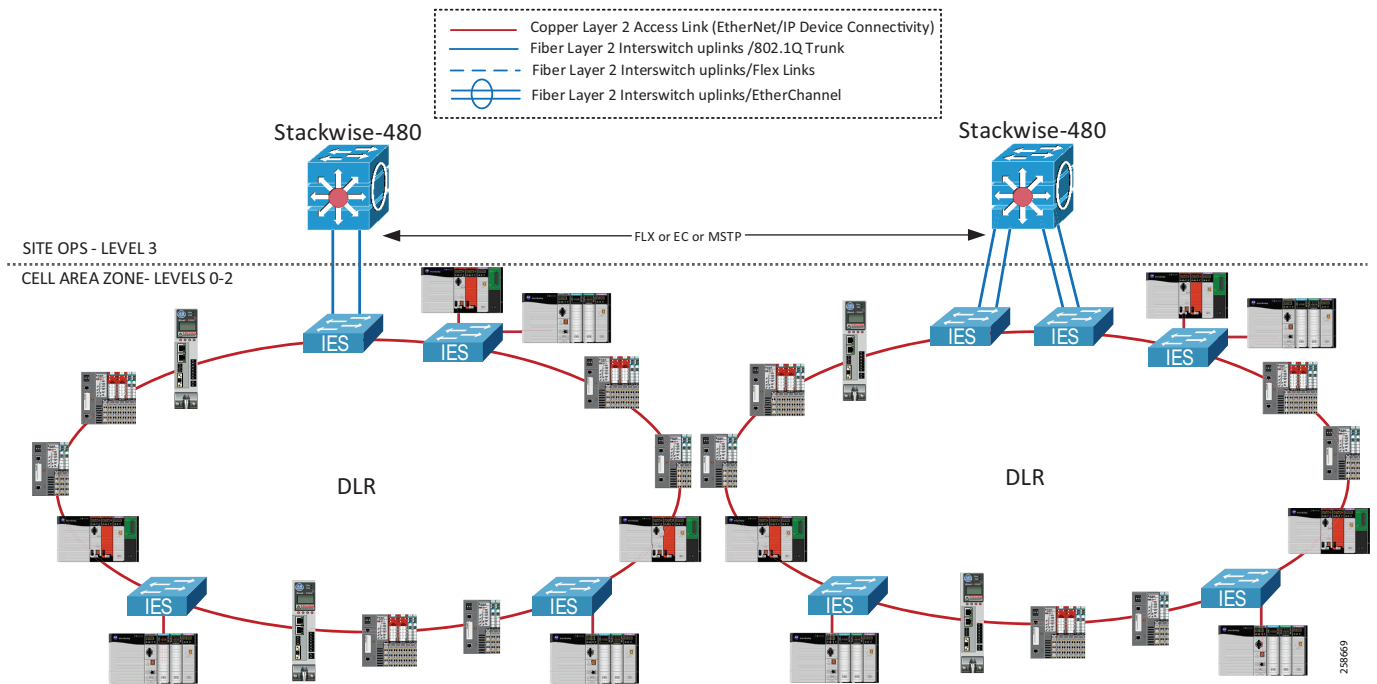
Note

For all reference architectures, intra-VLAN connectivity was tested and validated. Intra-VLAN connectivity includes single VLAN communication localized in a DLR and remote traffic traversing the distribution switch.

Recommended Topologies

The recommended usage of the DLR protocol in a mixed device/switch-level DLR deployment within CPwE is limited to Cell/Area Zones with the uplinks to distribution. [Figure 2-21](#) represents one example of a simplified recommended topology when using converged mixed device/switch-level DLR architectures with single gateway and Redundant Gateways.

Figure 2-21 Mixed Device/Switch-Level DLR Ring Connected Directly to Layer 3 Distribution Switches

**Note**

DLR-Capable Stratix Industrial Ethernet Switches have specific ports for which DLR can be implemented. The complete list of DLR compatible ports for the Stratix 5700 and Stratix 5400 can be found in [Appendix A, “DLR Port Choices for Stratix Switches.”](#)

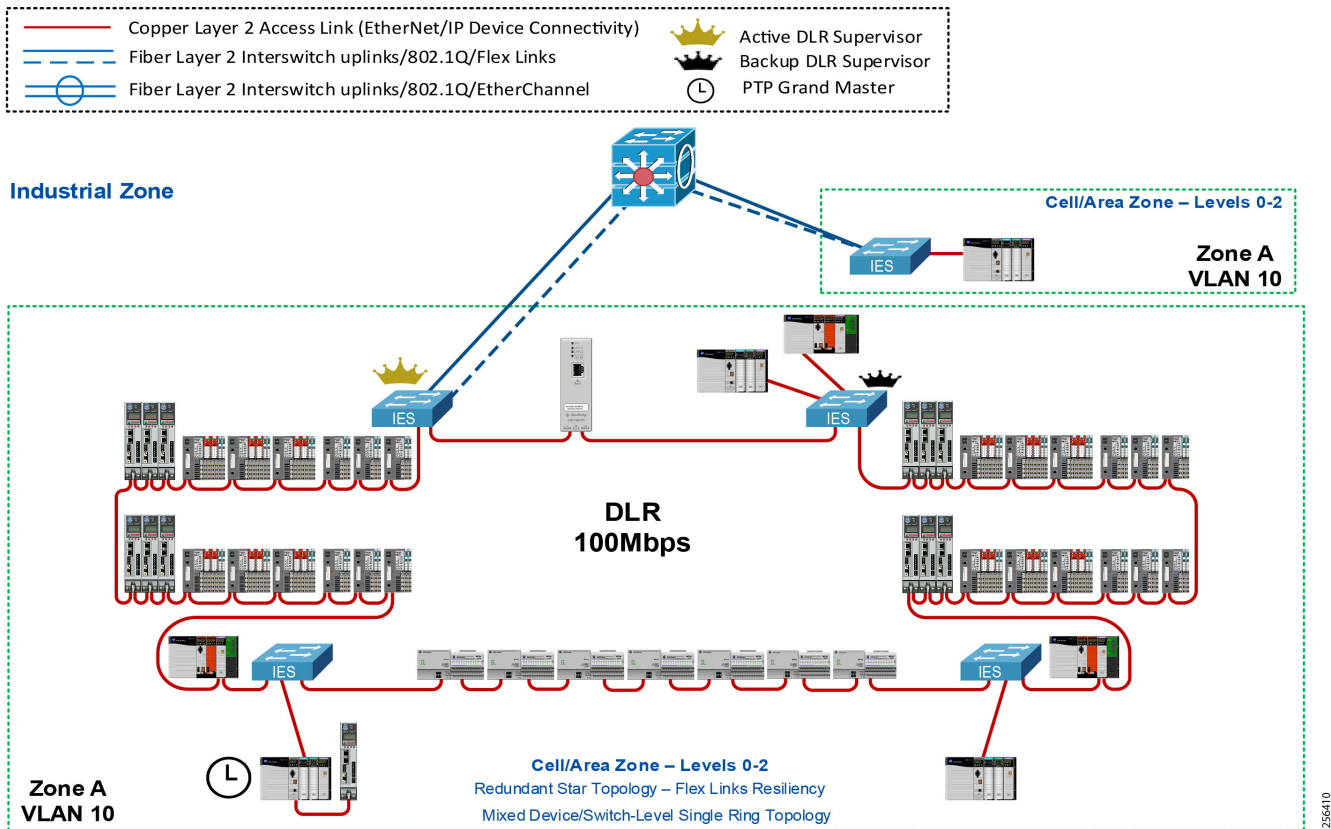
**Note**

Stackwise-480 (Cisco Catalyst 3850 or 9300) is shown as the distribution resiliency protocol in all of the following architecture figures. However, reference architecture testing and verification was also completed with VSS (Cisco Catalyst 4500-X) and SV (Cisco Catalyst 9500) technologies. Further, EtherChannel and Flex Links were also configured as IES-distribution link resiliency protocols and are not shown.

Reference Architecture 1—Single Ring Mixed Device/Switch-Level DLR Ring at 100 Mbps

[Figure 2-22](#) represents reference architecture testing for a single mixed device/switch-level ring at 100 Mbps with various distribution and uplink resiliency protocols. In this reference architecture a single VLAN is used throughout all IACS and IES devices in the ring.

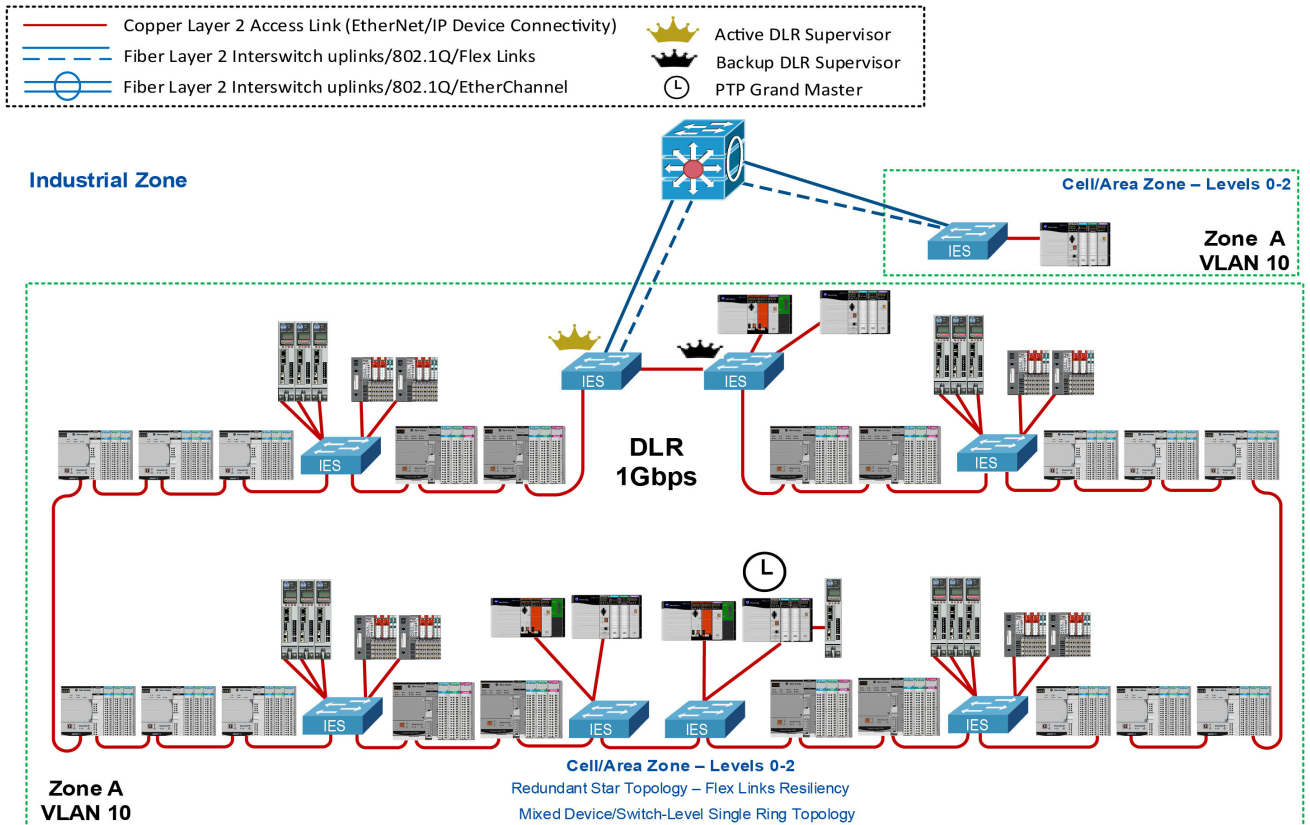
Figure 2-22 DLR Reference Architectures—Single Mixed Device/Switch-Level Ring at 100 Mbps (50 Ring Nodes)



Reference Architecture 2—Single Ring Mixed Device/Switch-Level DLR Ring (1Gbps)

Figure 2-23 represents reference architecture testing for a single mixed device/switch-level ring at 1 Gbps with various distribution and uplink resiliency protocols. In this reference architecture a single VLAN is used throughout all IACS and IES devices in the ring.

Figure 2-23 DLR Reference Architectures-Single Mixed Device/Switch-Level Ring (1 Gbps)



Expected Convergence Times for Single Gateway

Convergence times for both single mixed IACS device/switch-level ring reference architectures for traffic disruption localized to the DLR ring were 3 ms or less. This is consistent with the ODVA, Inc. standard for DLR. This DLR convergence time had no impact on local CIP Standard and CIP Safety control and messaging applications; Standard and Safety controllers reported no I/O or produce/consume connection loss within the local DLR. Additionally, high-speed motion application with a coarse update rate (CUR) of 2 ms showed no impact. Therefore no motion faults occurred during traffic disruption localized to the DLR ring. The recommendation is to use CUR no lower than 2 ms for mixed device/switch-level rings. It was observed and recommended not to apply standard and safety applications or high-speed motion beyond the local DLR as it pertains to the single ring architecture.

For the best performance for IACS applications when communicating to and from outside the DLR, it is recommended to implement unicast connection type and to use Flex Links or EtherChannel Layer 2 resiliency protocols for the uplinks in redundant star topology.

Reference architecture testing of the mixed device/switch-level DLR, with a variety of distribution platforms implemented with MSTP or REP, showed higher convergence times. This is regardless of uplink topology. These must be applied strictly following the rules to achieve the best performance:

- Multicast convergence times have shown to be higher than expected when traversing the uplinks with a single gateway. Therefore, multicast traffic should be kept local to the DLR ring and limited from traversing the uplinks. This type of traffic may include the following:
 - Multicast I/O (examples are ControlLogix Redundancy I/O and IEEE 1588 CIP Sync traffic)

– Multicast Produced/Consumed Tags

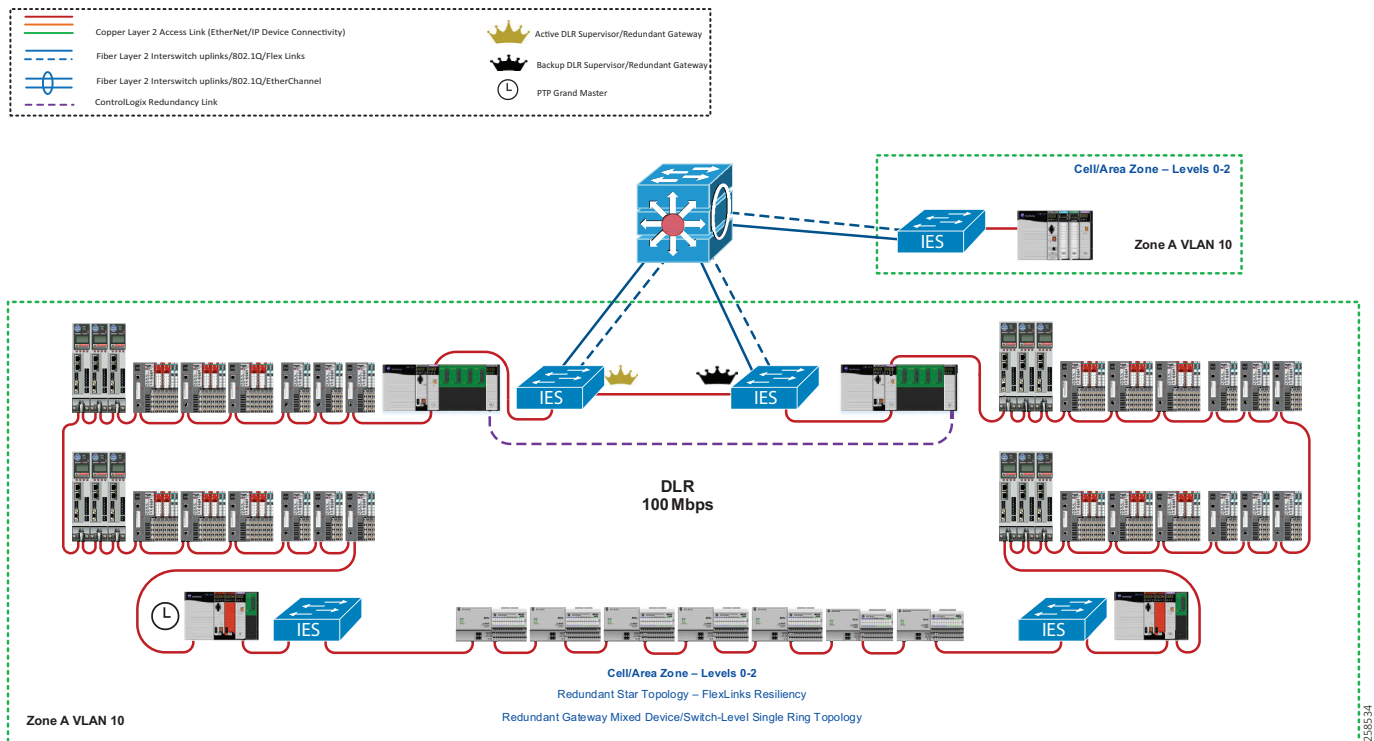
Reference architecture testing of the mixed device/switch-level DLR with a variety of distribution platforms results were consistent with the convergence times published in the *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:

- *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

Reference Architecture 3—Single Ring Mixed Device/Switch-Level DLR (100 Mbps) with Redundant Gateway

Figure 2-24 represents reference architecture testing for a single mixed device/switch-level DLR at 100 Mbps with Redundant Gateway with various distribution and uplink resiliency protocols. In this reference architecture a single VLAN is used throughout all IACS and IES devices in the ring. A DLR network with Redundant Gateway requires two dedicated IES to be configured as gateways in the DLR for the feature to work. These IES will be configured as either the active or backup gateway. Only one gateway can be active at any given time and the backup uses the configuration of the active gateway in the event of a failure. The backup gateway forwards DLR traffic between only the DLR ports and forwards uplink port traffic only between the uplink ports and non-DLR ports, this prevents an unmanaged ring. DLR requires one ring participant to be configured as an active DLR supervisor to manage the ring.

Figure 2-24 DLR Reference Architectures-Single Mixed Device/Switch-Level DLR (100 Mbps) with Redundant Gateway



Expected Convergence Times with Redundant Gateway

Reference architecture testing for a single mixed device/switch-level DLR ring, at 100 Mbps, utilizing Redundant Gateway, produced convergence times of 3 ms or less for a localized traffic disruption. This is consistent with the ODVA, Inc. standard for DLR. This DLR convergence time had no impact on local CIP Standard and CIP Safety control and messaging applications; Standard and Safety controllers reported no I/O or produce/consume connection loss within the local DLR. Additionally, high-speed motion application with a coarse update rate (CUR) of 2 ms showed no impact. Therefore no motion faults occurred during traffic disruption localized to the DLR ring. The recommendation is to use CUR no lower than 2 ms for single mixed device/switch-level DLR at 100 Mbps with Redundant Gateway. It is recommended not to apply standard and safety applications or high-speed motion beyond the local DLR as it pertains to the single ring architecture.

The following data tables use the same test actions for Active Gateway Failure and Active Gateway Recovery but from different source and destination points within the reference architecture.

- Active Gateway Failure describes a test action that was performed to simulate the failure of the active Redundant Gateway IES resulting in the backup Redundant Gateway IES becoming the new operational active Redundant Gateway.
- Active Gateway Recovery describes a test action was performed to simulate the recovery of the previously failed active Redundant Gateway IES while the backup Redundant Gateway reassumes its original role as backup Redundant Gateway resulting in normal operational state.
- Traffic direction referenced in the tables as DLR Cell/Area Zone to Outside the DLR is illustrated in [Figure 2-16](#). Traffic direction reference in the tables as Outside the DLR to DLR Cell/Area Zone is illustrated in [Figure 2-17](#). The results in [Table 2-11](#) (Unicast) and [Table 2-12](#) (Multicast) illustrate Redundant Gateway switchover maximum convergence times for Layer 2 uplinks connected to Redundant Gateway switches to the distribution switch with multiple uplinking technologies and distribution platforms for traffic sourced from DLR Cell/Area Zone destined for the Outside network.

Table 2-11 Max Convergence Unicast—Single Mixed Device/Switch-Level DLR (100 Mbps) with Redundant Gateway

Description Type	Traffic Type	Unicast—Maximum Convergence Time (ms)			
		Flex Links	EtherChannel	MSTP	REP
Active Gateway Failure (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	10	11	10	30
Active Gateway Recovery (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	42	95	83	280
Active Gateway Failure (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	82	48	137	87
Active Gateway Recovery (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	124	64	83	62
Active Gateway Failure (Traffic Local to Ring)	L2	2	2	2	2
Active Gateway Recovery (Traffic Local to Ring)	L2	33	40	2	11

Table 2-11 Max Convergence Unicast—Single Mixed Device/Switch-Level DLR (100 Mbps) with Redundant Gateway (continued)

Redundant Star/Ring Topology Resiliency Protocol (Link and Switch) ¹	L2/L3	N/A	N/A	N/A	N/A
---	-------	-----	-----	-----	-----

1. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:
Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

Table 2-12 Max Convergence Multicast—Single Mixed Device/Switch-Level DLR (100 Mbps) with Redundant Gateway

Description Type	Traffic Type	Multicast—Maximum Convergence Time (ms)			
		Flex Links	EtherChannel	MSTP	REP
Active Gateway Failure (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	10	10	10	30
Active Gateway Recovery (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	6	8	6	6
Active Gateway Failure (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	10	183	80	85
Active Gateway Recovery (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	5	6	6	6
Active Gateway Failure (Traffic Local to Ring)	L2	2	2	3	2
Active Gateway Recovery (Traffic Local to Ring)	L2	5	8	4	6
Redundant Star/Ring Topology Resiliency Protocol (Link and Switch) ¹	L2/L3	N/A	N/A	N/A	N/A

1. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:
Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

**Note**

Recovery of a failed Redundant Gateway to restore the original active gateway as primary should be initiated during a maintenance window to minimize production downtime.

**Note**

It is recommended to use an uninterruptable power supply, such as Rockwell Automation Bulletin 1609 uninterruptable power supplies, for backup of Redundant Gateway switches to prevent unnecessary Redundant Gateway switchovers and network downtime from power bumps and outages.

For the best performance for IACS applications when communicating to and from outside the DLR, it is recommended to implement unicast connection type and to use Flex Links or EtherChannel Layer 2 resiliency protocols for the uplinks in redundant star topology.

Multicast traffic should be kept local to the DLR ring and limited from traversing the uplinks. This type of traffic may include the following:

- Multicast I/O (examples are ControlLogix Redundancy I/O and IEEE 1588 CIP Sync traffic)
- Multicast Produced/Consumed Tags

Reference architecture testing of the single mixed device/switch-level DLR ring, at 100 Mbps, utilizing Redundant Gateway, with a variety of distribution switch platforms, produced results that were consistent with the convergence times published in the *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:

- *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

Reference Architecture 4—Multiple Rings Mixed Device/Switch-Level DLR (100 Mbps)

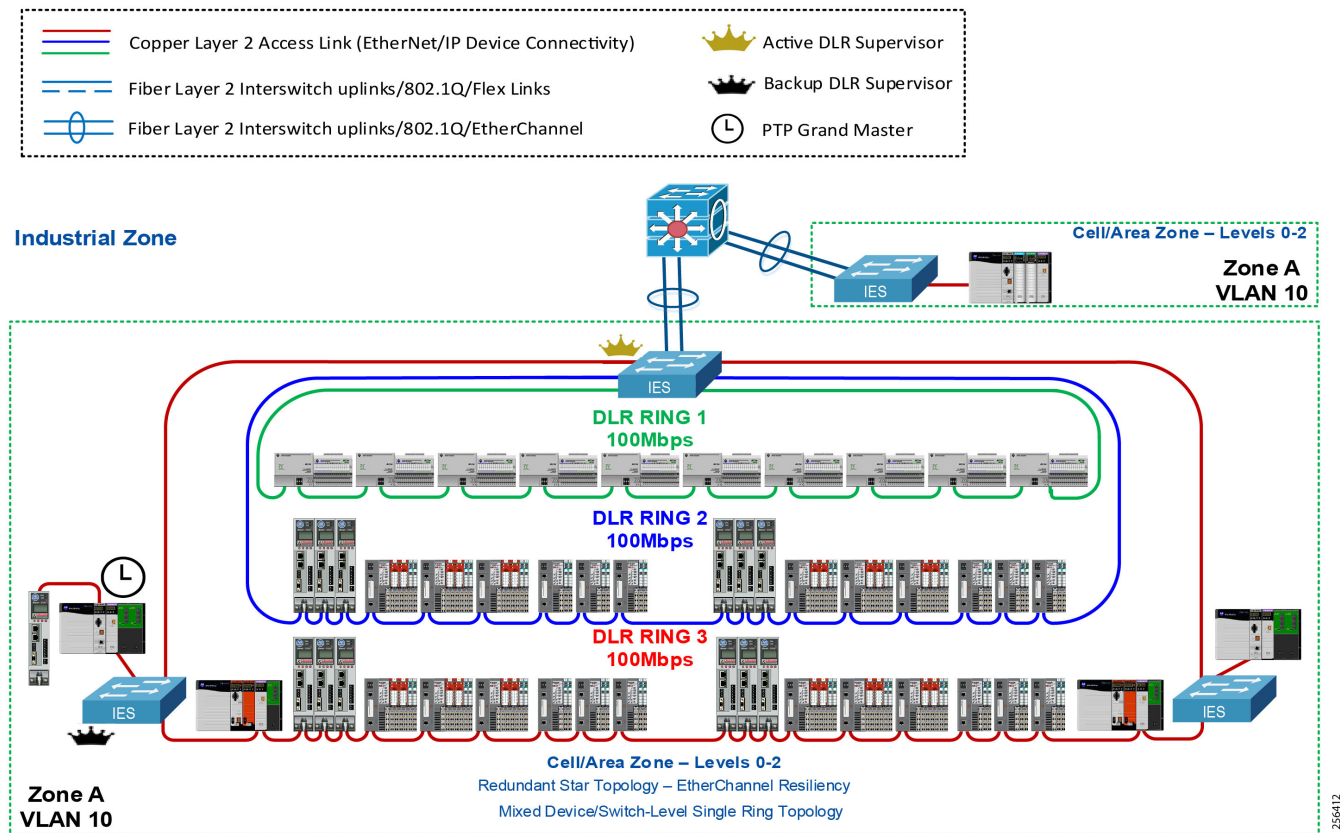
Figure 2-25 represents reference architecture testing for multiple mixed device/switch-level rings. In this reference architecture, all rings are at 100 Mbps with various distribution and uplink resiliency protocols. A single VLAN is used throughout all IACS and IES devices in the ring.

Currently, the Stratix 5400 is the only IES capable of supporting as many as three device-level rings simultaneously on the same IES. DLR requires one ring participant to be configured as an active DLR supervisor to manage the ring. After a single fault in the ring, essentially it becomes a linear topology and a ring supervisor is no longer needed for loop prevention. In rare cases of a software fault not detected on the physical layer, a backup DLR supervisor will be able to manage the loop. In this case it is recommended that no more than two supervisors are configured in a single ring. Typically, in a use case shown in Figure 2-25 where ring 1 and 2 ring participant nodes do not have the DLR supervisory capabilities, a 1783-ETAP can be placed in ring 1 and 2 as a backup DLR supervisor. The ETAP can also be used as a communication port directly on to those rings if needed for configuration or troubleshooting.

The high-speed CIP Motion traffic between the ControlLogix CIP Motion controller and CIP Motion drives with the Coarse Update Rate (CUR) of 2 ms were local on the DLR. The motion controller was outside of Ring 3 connected via star topology to one of the Stratix IES on ring 3, while all drives were distributed on Ring 2 and 3 as ring participants. All Stratix IES ring participants were configured with PTP End-to-End Transparent mode.

CIP Standard and CIP Safety Produced/Consumed (P/C Class 1), and HMI (Class 3) traffic were local on the DLR as well as outside of the local DLR. CIP Safety I/O RPIs used the default 10 ms and default unicast. CIP Standard I/O RPIs used the default 20 ms and default unicast. Both CIP Standard and CIP Safety P/C RPIs used the default 20 ms and configured as multicast. For both I/O and P/C applications, unicast is the default and is still the recommended option. Multicast was used for testing purposes only.

Figure 2-25 DLR Reference Architectures—Multiple Mixed Device/Switch-Level Ring at 100 Mbps



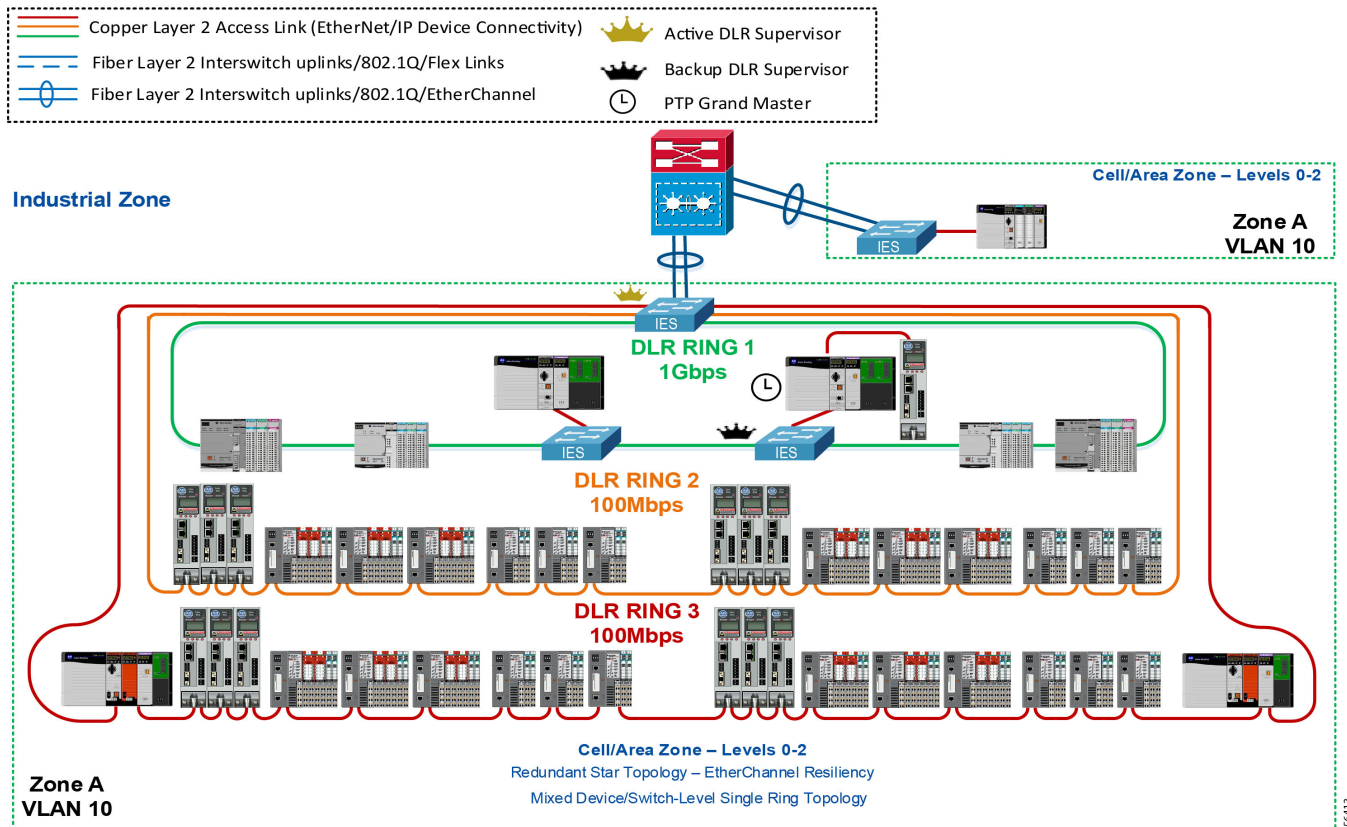
Reference Architecture 5—Multiple Rings Mixed Device/Switch-Level DLR at Mixed Ring Speeds

Figure 2-26 represents reference architecture testing for multiple mixed IACS device/switch-level rings. It shows two rings at 100 Mbps and one ring at 1 Gbps with various distribution and uplink resiliency protocols. In this reference architecture a single VLAN is used throughout all IACS and IES devices in the ring. Currently, the Stratix 5400 is the only IES capable of supporting as many as three device-level rings simultaneously on the same IES. DLR requires one ring participant to be configured as an active DLR supervisor to manage the ring. After a single fault in the ring, essentially it becomes a linear topology and a ring supervisor is no longer needed for loop prevention. In rare cases of a software fault not detected on the physical layer, a backup DLR supervisor will be able to manage the loop. In this case it is recommended that no more than two supervisors are configured in a single ring. Typically, in a use case shown in Figure 2-26 where ring 2 and 3 ring participant nodes do not have the DLR supervisory capabilities, a 1783-ETAP can be placed in ring 2 and 3 as a backup DLR supervisor. The ETAP can also be used as a communication port directly on to those rings if needed for configuration or troubleshooting.

The high-speed CIP Motion traffic between the ControlLogix CIP Motion controller and CIP Motion drives with the Coarse Update Rate (CUR) of 2 ms were local on the DLR. The motion controller was outside of Ring 1 connected via star topology to one of the Stratix IES on Ring 1, while all drives were distributed on Ring 2 and 3 as ring participants. All Stratix IES ring participants were configured with PTP End-to-End Transparent mode.

CIP Standard and CIP Safety Produced/Consumed (P/C) (Class 1), and HMI (Class 3) traffic were local on the DLR as well as outside of the local DLR. CIP Safety I/O RPIs used the default 10 ms and default unicast. CIP Standard I/O RPIs used the default 20 ms and default unicast. Both CIP Standard and CIP Safety P/C RPIs used the default 20 ms and configured as multicast. For both I/O and P/C applications, unicast is the default and is still the recommended option. Multicast was used for testing purposes only.

Figure 2-26 DLR Reference Architectures—Multiple Mixed Device/Switch-Level Ring at Mixed Ring Speeds



Expected Convergence Times with Single Gateway

Convergence times for both multiple mixed device/switch-level ring reference architectures for traffic disruption localized to the DLR ring were 3 ms or less. This is consistent with the ODVA, Inc. standard for DLR. This DLR convergence time had no impact on local CIP Standard and CIP Safety control and messaging applications; Standard and Safety controllers reported no I/O or produce/consume connection loss within the local DLR. Additionally, high-speed motion application with a coarse update rate (CUR) of 2 ms showed no impact, meaning no motion faults occurred during traffic disruption localized to the DLR ring. The recommendation is to use CUR no lower than 2 ms for mixed device/switch-level rings. It was observed and recommended not to apply standard and safety applications or high-speed motion beyond the local DLR as it pertains to the single ring architecture. DLR is the only resiliency protocol that can provide the 3 ms converge time required for these applications.

For the best performance for IACS applications when communicating to and from outside the DLR, it is recommended to implement unicast and to use Flex Links or EtherChannel Layer 2 resiliency protocols for the uplinks in redundant star topology.

Reference architecture testing of the mixed device/switch-level DLR with a variety of distribution platforms implemented with MSTP or REP showed higher convergence times. This is regardless of uplink topology. These must be applied strictly following the rules to achieve the best performance:

- Multicast convergence times have shown to be higher than expected when traversing the uplinks, therefore multicast traffic should be kept local to the DLR ring and limited from traversing the uplinks. This type of traffic may include the following:
 - Multicast I/O (examples are ControlLogix Redundancy I/O and IEEE 1588 CIP Sync traffic)
 - Multicast Produced/Consumed Tags

Reference architecture testing of the mixed device/switch-level DLR with a variety of distribution platforms results were consistent with the convergence times published in the *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:

- *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

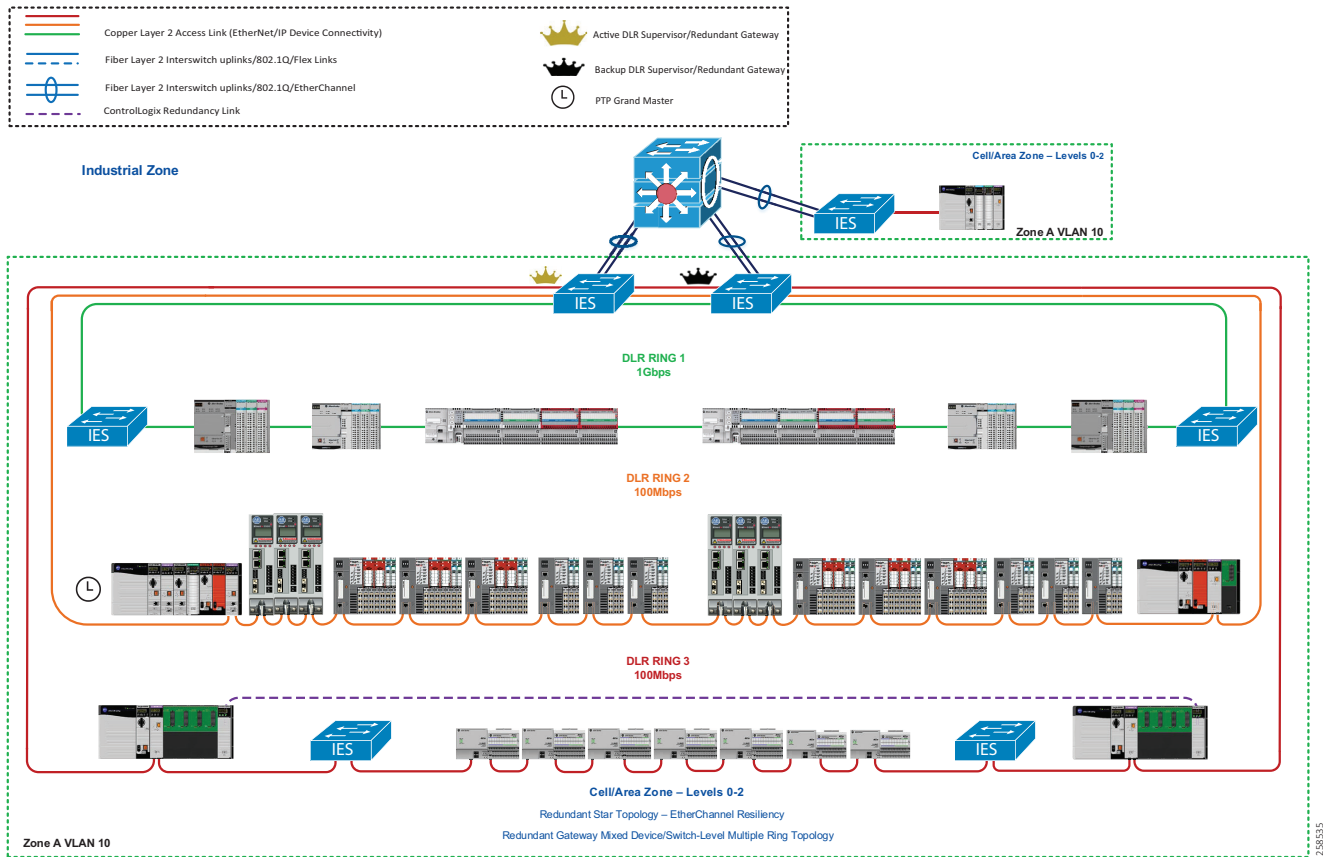
Reference Architecture 6—Multiple Mixed Device/Switch-Level DLRs with Redundant Gateway at Mixed Ring Speeds (Single VLAN)

Figure 2-27 represents reference architecture testing for multiple mixed device/switch-level DLR with Redundant Gateway at mixed ring speeds (Single VLAN). It shows two rings at 100 Mbps and one ring at 1 Gbps with various distribution and uplink resiliency protocols. In this reference architecture a single VLAN is used throughout all IACS and IES devices in the ring. A DLR network with Redundant Gateway requires two dedicated IES to be configured as gateways in the DLR for the feature to work. These IES will be configured as either the active or backup gateway. Only one gateway can be active at any given time and the backup uses the configuration of the active gateway in the event of a failure. The backup gateway forwards DLR traffic between DLR ports and forwards uplink port traffic only between the uplink ports, this prevents an unmanaged ring. DLR requires one ring participant to be configured as an active DLR supervisor to manage the ring.

The high-speed CIP Motion traffic between the ControlLogix CIP Motion controller and CIP Motion drives with the Coarse Update Rate (CUR) of 2 ms were local on the DLR. The motion controller was positioned directly on ring 2 while all drives were distributed on ring 2 as ring participants. All Stratix IES ring participants were configured with PTP End-to-End Transparent mode.

CIP Standard and CIP Safety Produced/Consumed (P/C) (Class 1), and HMI (Class 3) traffic were local on the DLR. CIP Safety I/O RPIs used the default 10 ms and default of unicast. CIP Standard I/O RPIs used the default 20 ms and default of unicast. Both CIP Standard and CIP Safety P/C RPIs used the default 20 ms and configured as multicast. For both I/O and P/C applications, unicast is the default and is still the recommended option. Multicast was used for testing purposes only.

Figure 2-27 DLR Reference Architectures- Multiple Mixed Device/Switch-Level DLR with Redundant Gateway at Mixed Ring Speeds (Single VLAN)



Expected Convergence Times with Redundant Gateway

Reference architecture testing for multiple mixed device/switch-level DLR rings, with mixed ring speeds (Single VLAN), utilizing Redundant Gateway, produced convergence times of 3 ms or less for a localized traffic disruption. This is consistent with the ODVA, Inc. standard for DLR. This DLR convergence time had no impact on local CIP Standard and CIP Safety control and messaging applications; Standard and Safety controllers reported no I/O or produce/consume connection loss within the local DLR. Additionally, high-speed motion application with a coarse update rate (CUR) of 2 ms showed no impact. Therefore no motion faults occurred during traffic disruption localized to the DLR ring. The recommendation is to use CUR no lower than 2 ms for multiple mixed device/switch-level DLR with Redundant Gateway at mixed ring speeds (Single VLAN). It was observed and recommended not to apply standard and safety applications or high-speed motion beyond the local DLR as it pertains to the single ring architecture.

The following data tables use the same test actions for Active Gateway Failure and Active Gateway Recovery but from different source and destination points within the reference architecture.

- Active Gateway Failure describes a test action that was performed to simulate the failure of the active Redundant Gateway IES resulting in the backup Redundant Gateway IES becoming the new operational active Redundant Gateway.
- Active Gateway Recovery describes a test action was performed to simulate the recovery of the previously failed active Redundant Gateway IES while the backup Redundant Gateway reassumes its original role as backup Redundant Gateway resulting in normal operational state.

- Traffic direction referenced in the tables as DLR Cell/Area Zone to Outside the DLR is illustrated in [Figure 2-16](#). Traffic direction reference in the tables as Outside the DLR to DLR Cell/Area Zone is illustrated in [Figure 2-17](#). The results in [Table 2-13](#) (Unicast) and [Table 2-14](#) (Multicast) illustrate Redundant Gateway switchover maximum convergence times for Layer 2 uplinks connected to Redundant Gateway switches to the distribution switch with multiple uplinking technologies and distribution platforms for traffic sourced from DLR Cell/Area Zone destined for the Outside network.

Table 2-13 Max Convergence Unicast—Multiple Mixed Device/Switch-Level DLR with Redundant Gateway at Mixed Ring Speeds (Single VLAN)

Description Type	Traffic Type	Unicast—Maximum Convergence Time (ms)			
		Flex Links	EtherChannel	MSTP	REP
Active Gateway Failure (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	11	11	116	11
Active Gateway Recovery (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	427	128	593	133
Active Gateway Failure (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	299	2010	1792	96
Active Gateway Recovery (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	2028	2010	2028	646
Active Gateway Failure (Traffic from Ring to Ring)	L2	300	671	632	96
Active Gateway Recovery (Traffic from Ring to Ring)	L2	641	671	632	647
Active Gateway Failure (Traffic Local to Ring)	L2	2	569	565	2
Active Gateway Recovery (Traffic Local to Ring)	L2	536	569	565	531
Redundant Star/Ring Topology Resiliency Protocol (Link and Switch) ¹	L2/L3	N/A	N/A	N/A	N/A

1. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to: *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

Table 2-14 Max Convergence Multicast—Multiple Mixed Device/Switch-Level DLR with Redundant Gateway at Mixed Ring Speeds (Single VLAN)

Description Type	Traffic Type	Multicast—Maximum Convergence Time (ms)			
		Flex Links	EtherChannel	MSTP	REP
Active Gateway Failure (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	11	11	593	10
Active Gateway Recovery (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	611	1315	593	546
Active Gateway Failure (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	77	3462	711	11
Active Gateway Recovery (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	4616	3856	711	7
Active Gateway Failure (Traffic from Ring to Ring)	L2	11	606	598	11
Active Gateway Recovery (Traffic from Ring to Ring)	L2	1310	1310	598	603
Active Gateway Failure (Traffic Local to Ring)	L2	2	841	598	2
Active Gateway Recovery (Traffic Local to Ring)	L2	551	966	598	551
Redundant Star/Ring Topology Resiliency Protocol (Link and Switch) ¹	L2/L3	N/A	N/A	N/A	N/A

1. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:

Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide

http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf



Note

Recovery of a failed Redundant Gateway to restore the original active gateway as primary should be initiated during a maintenance window to minimize production downtime.



Note

It is recommended to use an uninterruptable power supply, such as Rockwell Automation Bulletin 1609, for backup of Redundant Gateway switches to prevent unnecessary Redundant Gateway switchovers and network downtime from power bumps and outages.

For the best performance for IACS applications when communicating to and from outside the DLR, it is recommended to implement unicast connection type and to use Flex Links for Layer 2 resiliency protocol for the uplinks in redundant star topology.

Multicast traffic should be kept local to the DLR ring and limited from traversing the uplinks. This type of traffic may include the following:

- Multicast I/O (examples are ControlLogix Redundancy I/O and IEEE 1588 CIP Sync traffic)
- Multicast Produced/Consumed Tags

Reference architecture testing of the multiple mixed device/switch-level DLR with Redundant Gateway at mixed ring speeds (One VLAN) with a variety of distribution platforms results were consistent with the convergence times published in the *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:

- *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

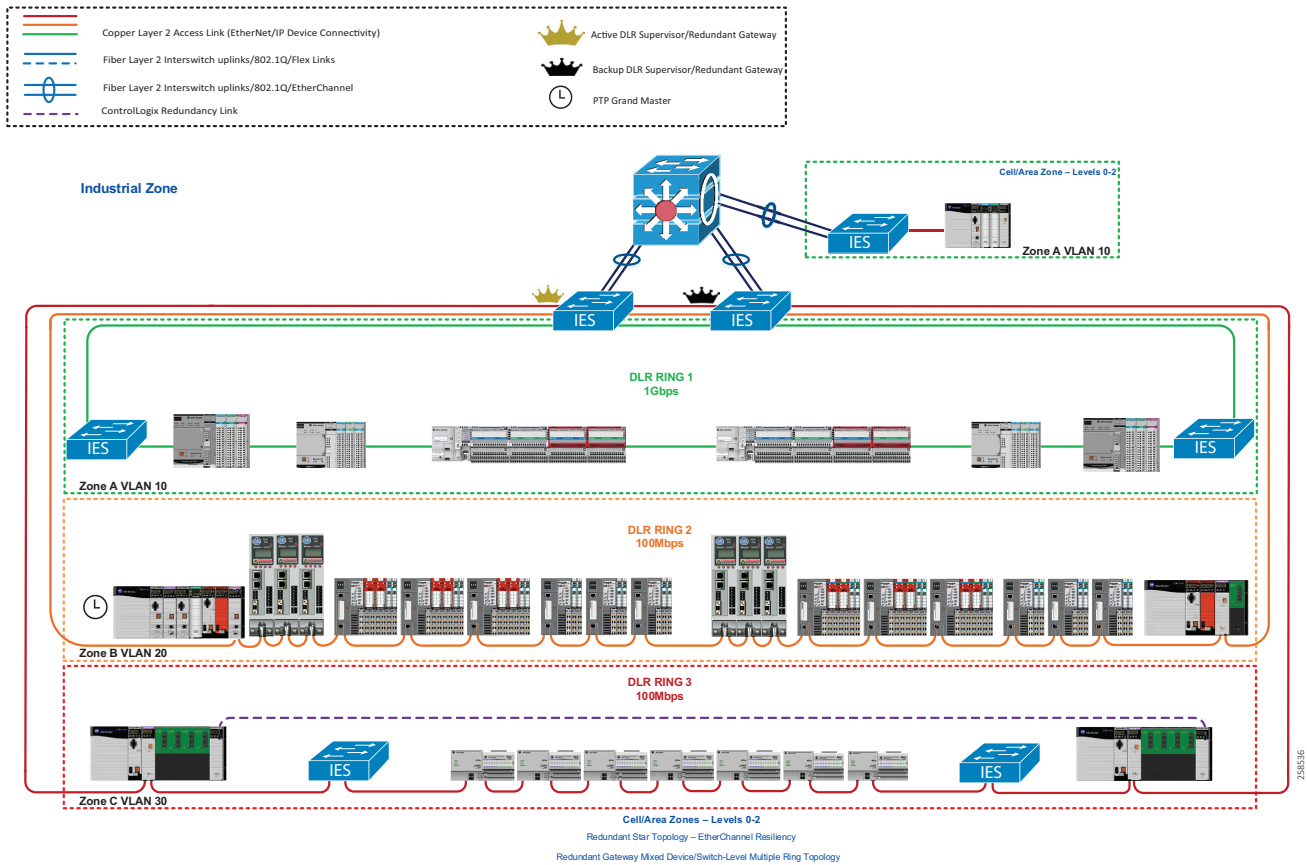
Reference Architecture 7—Multiple Mixed Device/Switch-Level DLR with Redundant Gateway at Mixed Ring Speeds (Multiple VLANs)

Figure 2-28 represents reference architecture testing for multiple mixed device/switch-level DLR with Redundant Gateway at mixed ring speeds (Multiple VLANs). It shows two rings at 100 Mbps and one ring at 1 Gbps with various distribution and uplink resiliency protocols. In this reference architecture a single VLAN is used throughout all IACS and IES devices in the ring. A DLR network with Redundant Gateway requires two dedicated IES to be configured as gateways in the DLR for the feature to work. These IES will be configured as either the active or backup gateway. Only one gateway can be active at any given time and the backup uses the configuration of the active gateway in the event of a failure. The backup gateway forwards DLR traffic between DLR ports and forwards uplink port traffic only between the uplink ports, this prevents an unmanaged ring. DLR requires one ring participant to be configured as an active DLR supervisor to manage the ring.

The high-speed CIP Motion traffic between the ControlLogix CIP Motion controller and CIP Motion drives with the Coarse Update Rate (CUR) of 2 ms were local on the DLR. The motion controller was positioned directly on Ring 2 while all drives were distributed on Ring 2 as ring participants. All Stratix IES ring participants were configured with PTP End-to-End Transparent mode.

CIP Standard and CIP Safety Produced/Consumed (P/C) (Class 1), and HMI (Class 3) traffic were local on the DLR. CIP Safety I/O RPIs used the default 10 ms and default unicast. CIP Standard I/O RPIs used the default 20 ms and default unicast. Both CIP Standard and CIP Safety P/C RPIs used the default 20 ms and configured as multicast. For both I/O and P/C applications, unicast is the default and is still the recommended option. Multicast traffic was localized to ring 3 and was not captured traversing the Redundant Gateways.

Figure 2-28 DLR Reference Architectures- Multiple Mixed Device/Switch-Level DLR with Redundant Gateway at Mixed Ring Speeds (Multiple VLANs)



Expected Convergence Times with Redundant Gateway

Reference architecture testing for multiple mixed device/switch-level DLR rings, with mixed ring speeds (Multiple VLANs), utilizing Redundant Gateway, produced convergence times of 3 ms or less for a localized traffic disruption. This is consistent with the ODVA, Inc. standard for DLR. This DLR convergence time had no impact on local CIP Standard and CIP Safety control and messaging applications; Standard and Safety controllers reported no I/O or produce/consume connection loss within the local DLR. Additionally, high-speed motion application with a coarse update rate (CUR) of 2 ms showed no impact. Therefore, no motion faults occurred during traffic disruption localized to the DLR ring. The recommendation is to use CUR no lower than 2 ms for multiple mixed device/switch-level DLR with Redundant Gateway at mixed ring speeds (Multiple VLANs). It was observed and recommended not to apply standard and safety applications or high-speed motion beyond the local DLR as it pertains to the single ring architecture.

The following data tables use the same test actions for Active Gateway Failure and Active Gateway Recovery but from different source and destination points within the reference architecture.

- Active Gateway Failure describes a test action that was performed to simulate the failure of the active Redundant Gateway IES resulting in the backup Redundant Gateway IES becoming the new operational active Redundant Gateway.
- Active Gateway Recovery describes a test action was performed to simulate the recovery of the previously failed active Redundant Gateway IES while the backup Redundant Gateway reassumes its original role as backup Redundant Gateway resulting in normal operational state.

- Traffic direction referenced in the tables as DLR Cell/Area Zone to Outside the DLR is illustrated in [Figure 2-16](#). Traffic direction reference in the tables as Outside the DLR to DLR Cell/Area Zone is illustrated in [Figure 2-17](#). The results in [Table 2-15](#) (Unicast) illustrate Redundant Gateway switchover maximum convergence times for Layer 2 uplinks connected to Redundant Gateway switches to the distribution switch with multiple uplinking technologies and distribution platforms for traffic sourced from DLR Cell/Area Zone destined for the Outside network.

Table 2-15 Max Convergence Unicast—Multiple Mixed Device/Switch-Level DLR with Redundant Gateway at Mixed Ring Speeds (Multiple VLANs)

Description Type	Traffic Type	Unicast—Maximum Convergence Time (ms)			
		Flex Links	EtherChannel	MSTP	REP
Active Gateway Failure (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	11	11	11	11
Active Gateway Recovery (Traffic from DLR Cell/Area Zone to Outside the DLR)	L2	27	23	23	23
Active Gateway Failure (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	307	115	127	120
Active Gateway Recovery (Traffic from Outside the DLR to DLR Cell/Area Zone)	L2	103	83	74	54
Active Gateway Failure (Traffic from Ring to Ring)	L2	306	116	127	95
Active Gateway Recovery (Traffic from Ring to Ring)	L2	104	103	85	64
Active Gateway Failure (Traffic Local to Ring)	L2	2	2	2	2
Active Gateway Recovery (Traffic Local to Ring)	L2	2	2	2	2
Redundant Star/Ring Topology Resiliency Protocol (Link and Switch) ¹	L2/L3	N/A	N/A	N/A	N/A

1. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to: *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf



Note

Recovery of a failed Redundant Gateway to restore the original active gateway as primary should be initiated during a maintenance window to minimize production downtime.

**Note**

It is recommended to use an uninterruptable power supply, such as Rockwell Automation Bulletin 1609, for backup of Redundant Gateway switches to prevent unnecessary Redundant Gateway switchovers and network downtime from power bumps and outages.

To get the best performance of IACS applications when communicating to and from outside the DLR, it is recommended to implement a unicast connection type and to use EtherChannel for Layer 2 resiliency protocols for the uplinks in redundant star topology.

Multicast traffic should be kept local to the DLR ring and limited from traversing the uplinks. This type of traffic may include the following:

- Multicast I/O (examples are ControlLogix Redundancy I/O and IEEE 1588 CIP Sync traffic)
- Multicast Produced/Consumed Tags

Reference architecture testing of the multiple mixed device/switch-level DLR with Redundant Gateway at mixed ring speeds (Multiple VLANs) with a variety of distribution platforms results were consistent with the convergence times published in the *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*. For guidance on uplink resiliency protocol convergence when implementing a mixed IACS device/switch-level DLR, refer to:

- *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

Summary of DLR Redundant Gateway Recommendations

The tables below show the summary of use cases performed with different distribution platform with resiliency recommendation (Table 2-16 shows the legend for the tables). Refer to the previous section for detailed information on the topology.

Table 2-16 Legend for Resiliency Recommendation Tables

✓	Validated and Recommended
✓	Validated
✗	Not Recommended
O	Not Tested

Table 2-17 Switch-Level DLR

Distribution switch	L2 Protocol	Flex Links	EtherChannel	MSTP	REP
Catalyst 3850	StackWise-480	✓	✓	✓	✓
Catalyst 9300	StackWise-480	✓	✓	✓	✓
Catalyst 4500-X	VSS	✓	✓	O	O
Catalyst 9500	SV	✓	✓	O	O
IE 5000/Stratix 5410	HSRP	O	O	O	O

Table 2-18 Switch-Level DLR with DLR VLAN Trunking

Distribution switch	L2 Protocol	Flex Links	EtherChannel	MSTP	REP
Catalyst 3850	StackWise-480	✓	✓	✓	✓
Catalyst 9300	StackWise-480	✓	✓	✓	✓
Catalyst 4500-X	VSS	✓	✓	0	0
Catalyst 9500	SV	✓	✓	0	0
IE 5000/Stratix 5410	HSRP	0	0	0	0

Table 2-19 Single Mixed Device/Switch-Level DLR

Distribution switch	L2 Protocol	Flex Links	EtherChannel	MSTP	REP
Catalyst 3850	StackWise-480	✓	✓	✓	✓
Catalyst 9300	StackWise-480	✓	✓	✓	✓
Catalyst 4500-X	VSS	✓	✓	0	0
Catalyst 9500	SV	✓	✓	0	0
IE 5000/Stratix 5410	HSRP	0	0	0	0

Table 2-20 Multiple Mixed Device/Switch-Level DLR (Single VLAN)

Distribution switch	L2 Protocol	Flex Links	EtherChannel	MSTP	REP
Catalyst 3850	StackWise-480	✓	✓	✗	✓
Catalyst 9300	StackWise-480	✓	✓	✗	✓
Catalyst 4500-X	VSS	✓	✓	0	0
Catalyst 9500	SV	✓	✓	0	0
IE 5000/Stratix 5410	HSRP	0	0	0	0

Table 2-21 Multiple Mixed Device/Switch-Level DLR (Multiple VLANs)

Distribution switch	L2 Protocol	Flex Links	EtherChannel	MSTP	REP
Catalyst 3850	StackWise-480	✓	✓	✓	✓
Catalyst 9300	StackWise-480	✓	✓	✓	✓
Catalyst 4500-X	VSS	✓	✓	0	0

Table 2-21 Multiple Mixed Device/Switch-Level DLR (Multiple VLANs) (continued)

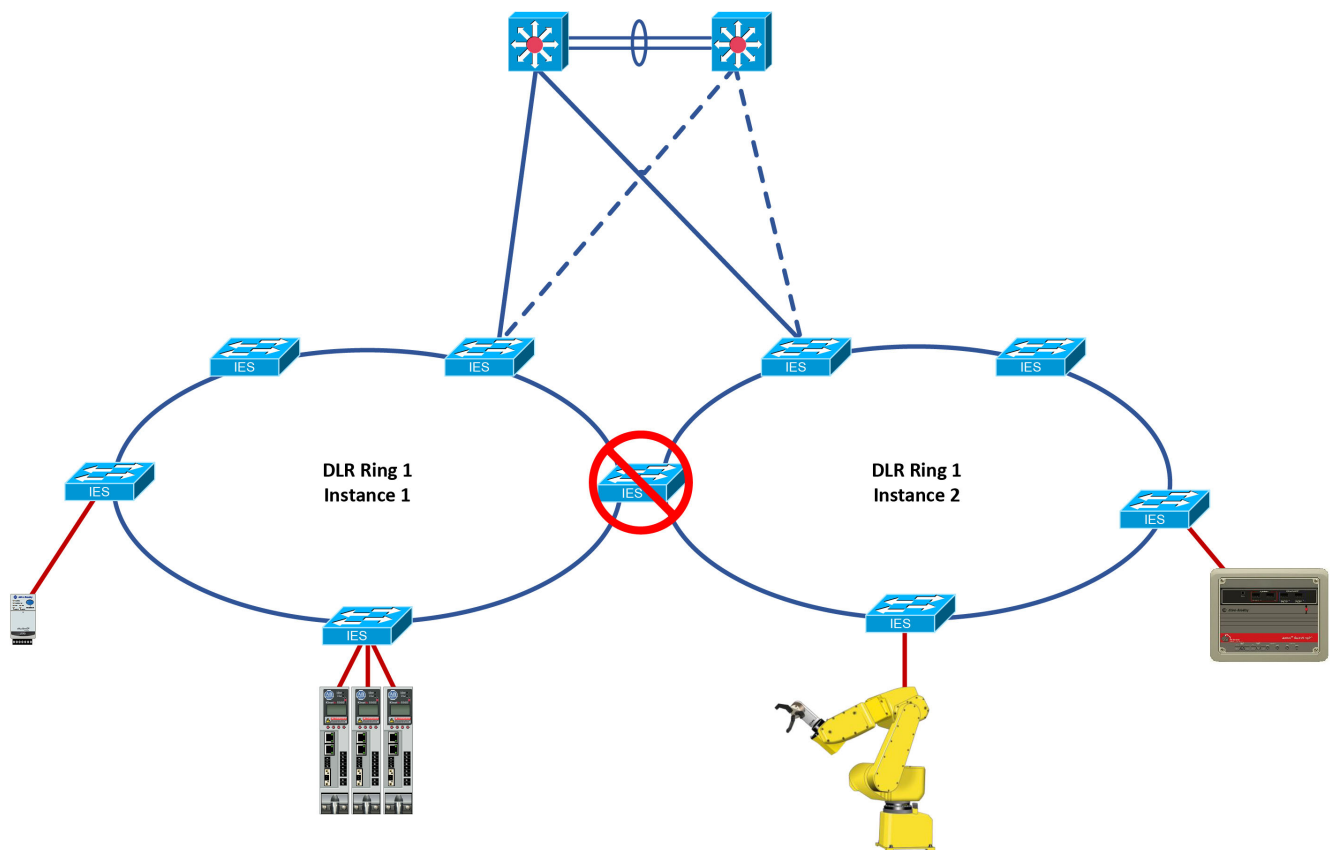
Catalyst 9500	SV	✓	✓	0	0
IE 5000/Stratix 5410	HSRP	0	0	0	0

Unsupported Topologies

DLR Rings Sharing a Node

The DLR protocol does not support sharing of a DLR node between two separate ring protocol implementations as shown in Figure 2-29.

Figure 2-29 Unsupported Topologies—DLR Rings Sharing a Node

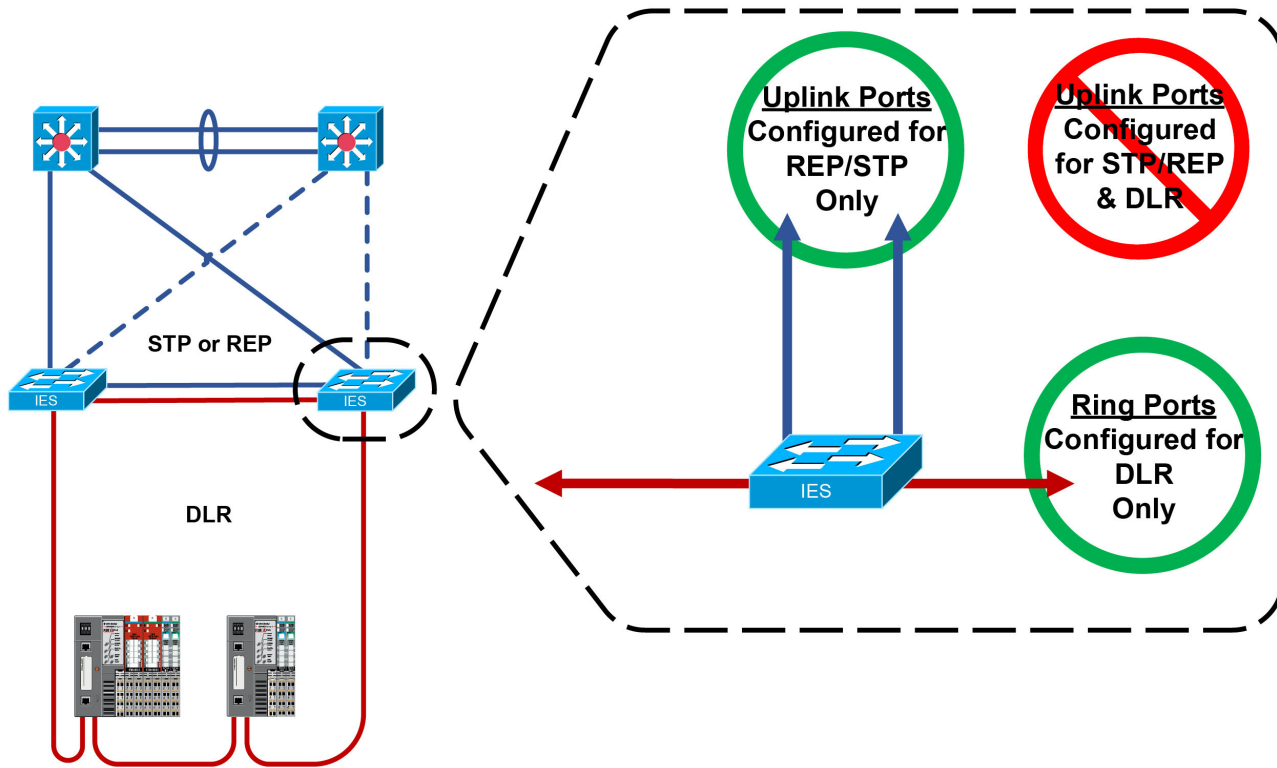


377685

Intermixing DLR with Resiliency Protocols

The DLR protocol cannot be implemented on the same port as other resiliency protocols. DLR ring ports and uplink ports must be segregated. This unsupported topology is represented in [Figure 2-30](#).

Figure 2-30 Unsupported Topologies—Implementing DLR and Resiliency Protocol on the Same Port

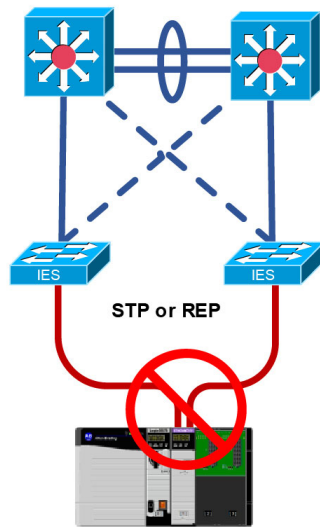


377686

Connecting Both Ports of an Embedded Switch Device to a Non-DLR Ring

Embedded IACS devices cannot have each port connected to an IES in a ring topology that does not implement the DLR protocol as shown in [Figure 2-31](#).

Figure 2-31 Unsupported Topologies—Implementing Embedded Switch Technology in MSTP/REP

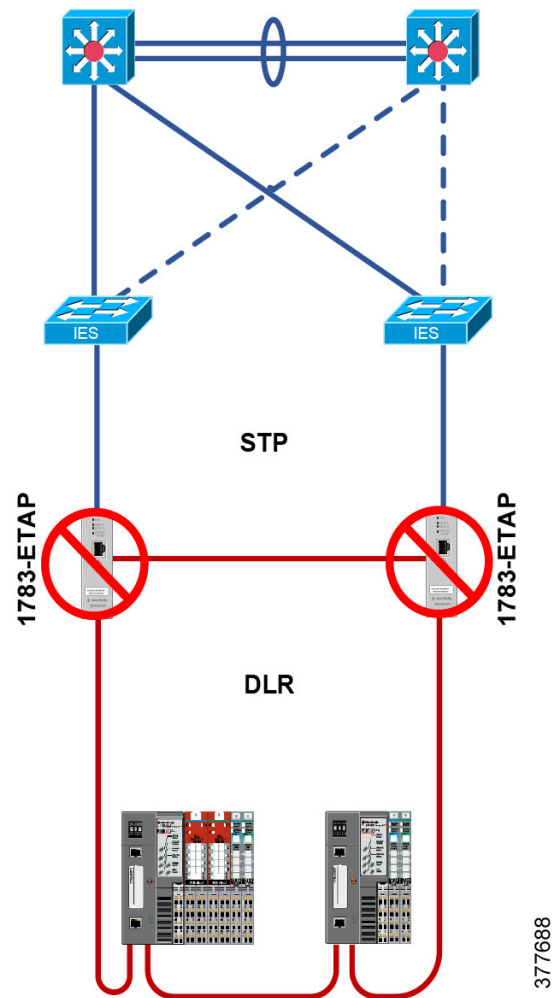


377687

Connecting Multiple ETAP Devices from a DLR Topology to Multiple IES

The 1783-ETAP is an embedded IACS device and as such, is not supported by IES topology Spanning Tree Protocols. Additionally, 1783-ETAPs cannot be configured as Redundant Gateways in a DLR ring. [Figure 2-32](#) represents an unsupported usage of 1783-ETAPs with Spanning Tree Protocol.

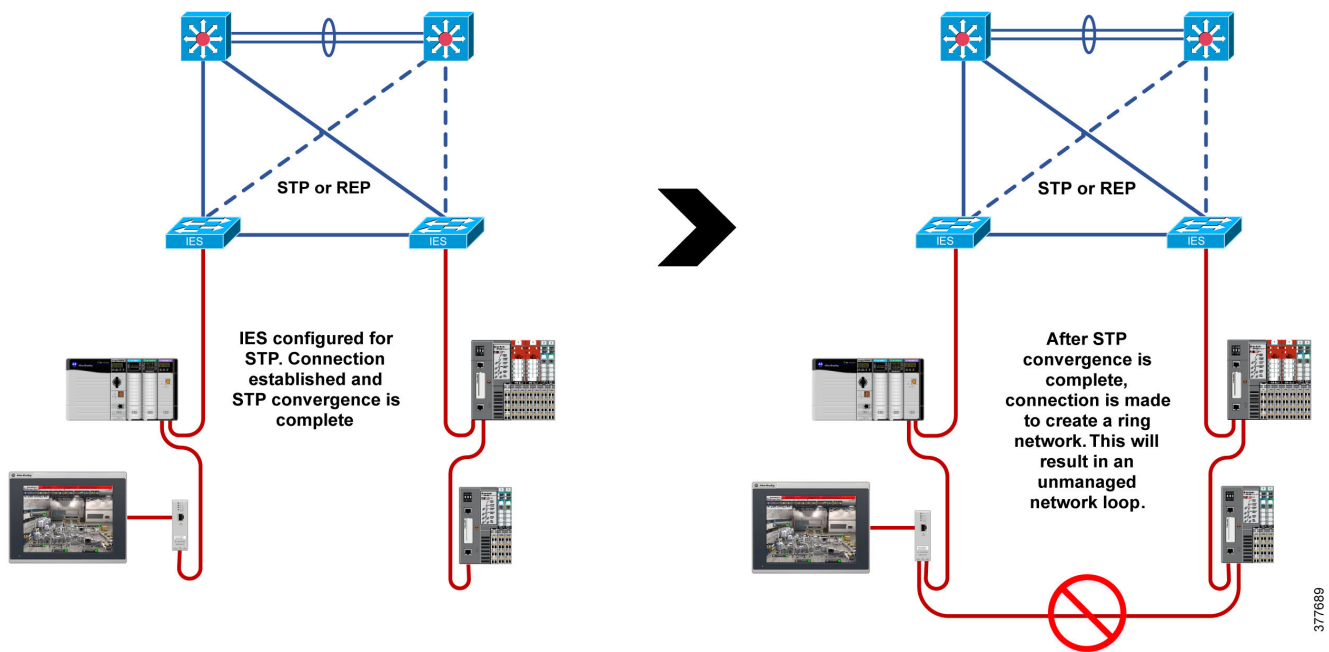
Figure 2-32 Unsupported Topologies—Connecting Multiple ETAPs from a DLR Topology to MSTP/REP



Connecting Linear Topologies into a Ring Topology without the DLR Protocol

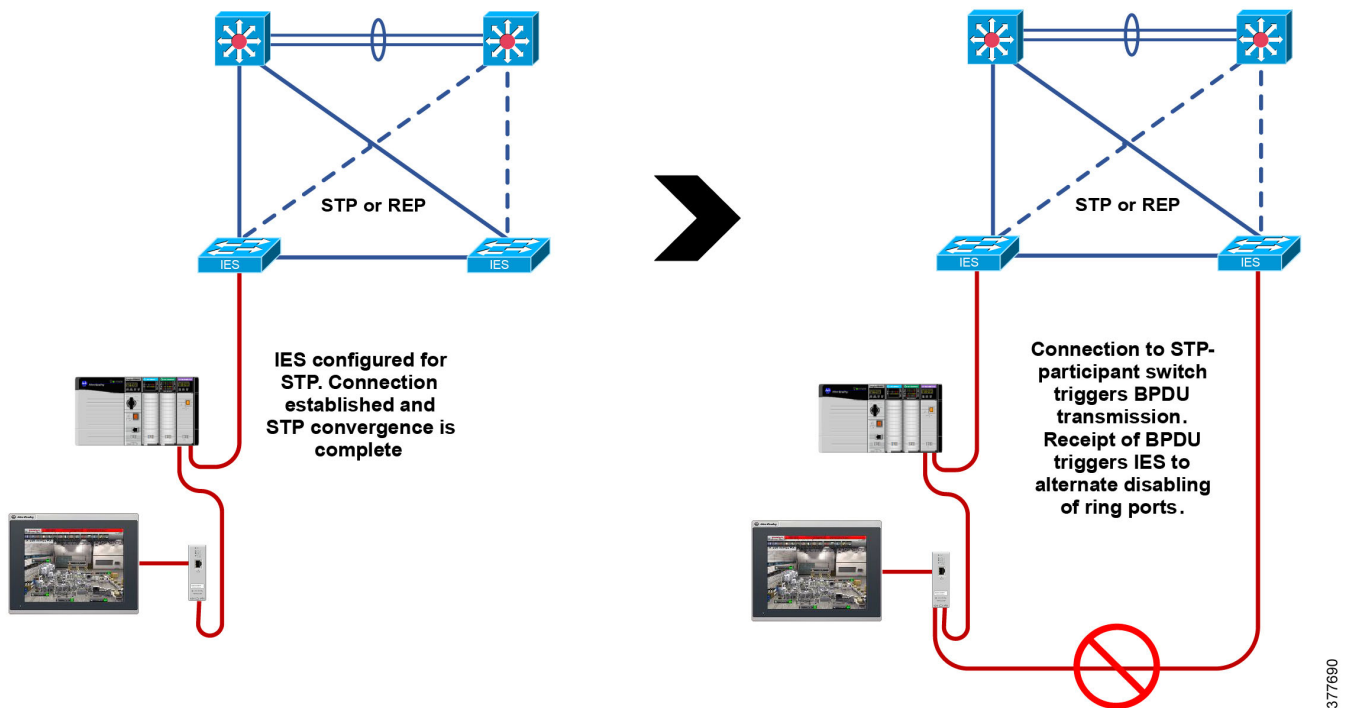
Two separately configured linear topology networks, created using the IES Multiport Automation Device Smartport role, cannot be connected directly into a ring topology without reconfiguring devices for DLR prior. Without the DLR protocol, connecting the MSTP IES after they are established in the MSTP topology will generate a broadcast storm and cause network failure. A representation of this unsupported topology is shown in Figure 2-33.

Figure 2-33 Unsupported Topologies—Connecting Two Linear Topologies Together without Configuring DLR



A linear topology connected to an IES participating in an MSTP implementation will function normally. If the linear topology is then connected to a second IES participating in the same MSTP implementation, the protocol will trigger the IES to transmit Bridge Protocol Data Units (BPDUs). BPDUs are messages sent between switches in a Multiple Spanning Tree Domain that contain MSTP network information. The switch receiving the BPDU will disable its port to prevent network looping. After some time, the disabled port will be enabled and transmit a BPDU, which is then received by the second switch in the newly introduced ring. This switch will follow the same pattern as the first, resulting in an alternating pattern of ports being disabled on either side of the linear topology. The DLR protocol must be configured prior to making this connection as seen in Figure 2-34.

Figure 2-34 Unsupported Topologies—Creating a Loop Topology without Configuring DLR



Note

Additional unsupported topologies may be found in the EtherNet/IP Device Level Ring Application Technique (ENET-AT007):

https://literature.rockwellautomation.com/idc/groups/literature/documents/at/enet-at007_-en-p.pdf

CPwE Device Level Ring Configuration

This chapter describes how to configure the DLR protocol within the CPwE architecture based on the design considerations and recommendations of [Chapter 2, “CPwE Device Level Ring Design Considerations.”](#) The included configurations have been verified during reference architecture testing.


Note

For proper IES installation and basic configuration, reference the Allen-Bradley Stratix Managed Switches User Manual, 1783-UM007 (http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf).

Overview

Deployment of a DLR is a relatively straightforward process that involves configuration of three primary components:

- Supervisor(s)
- Gateway(s)
- Ring Participant(s)

The order of component configuration is paramount, as a ring configured with no supervisor constitutes an unmanaged network loop and can result in unicast, multicast, or broadcast storms causing disruptions to network communications. See [Figure 3-1](#) for the steps.

- Step 1 Enable one of the ring participants to be the DLR supervisor and configuring the Stratix IES DLR settings. Typically, enabling DLR supervisory capabilities on a ring participant requires a checkbox to be checked either in RSLinx Classic or Studio 5000 Logix Designer. The ring supervisor maintains loop-free topologies by enabling limited port blocking on one of its two DLR ring ports, only opening the port when a ring topology change is detected. For the Stratix IES, configure the DLR settings which includes selecting the Mode and DLR ports.
- Step 2 (Optional) For the Stratix IES, if multiple connections to external network infrastructure are required, then enable the Redundant Gateway feature and configure the Redundant Gateways ports.

As with the ring supervisor maintaining a logical loop-free ring topology, multiple gateway connections to an external architecture can introduce network loops. This is mitigated by properly configuring DLR Redundant Gateways.

**Note**

If Redundant Gateways are to be implemented, be sure to configure DLR settings prior to connecting ring ports or gateway uplinks. This includes configuration for the Mode and DLR ports on the Stratix IES.

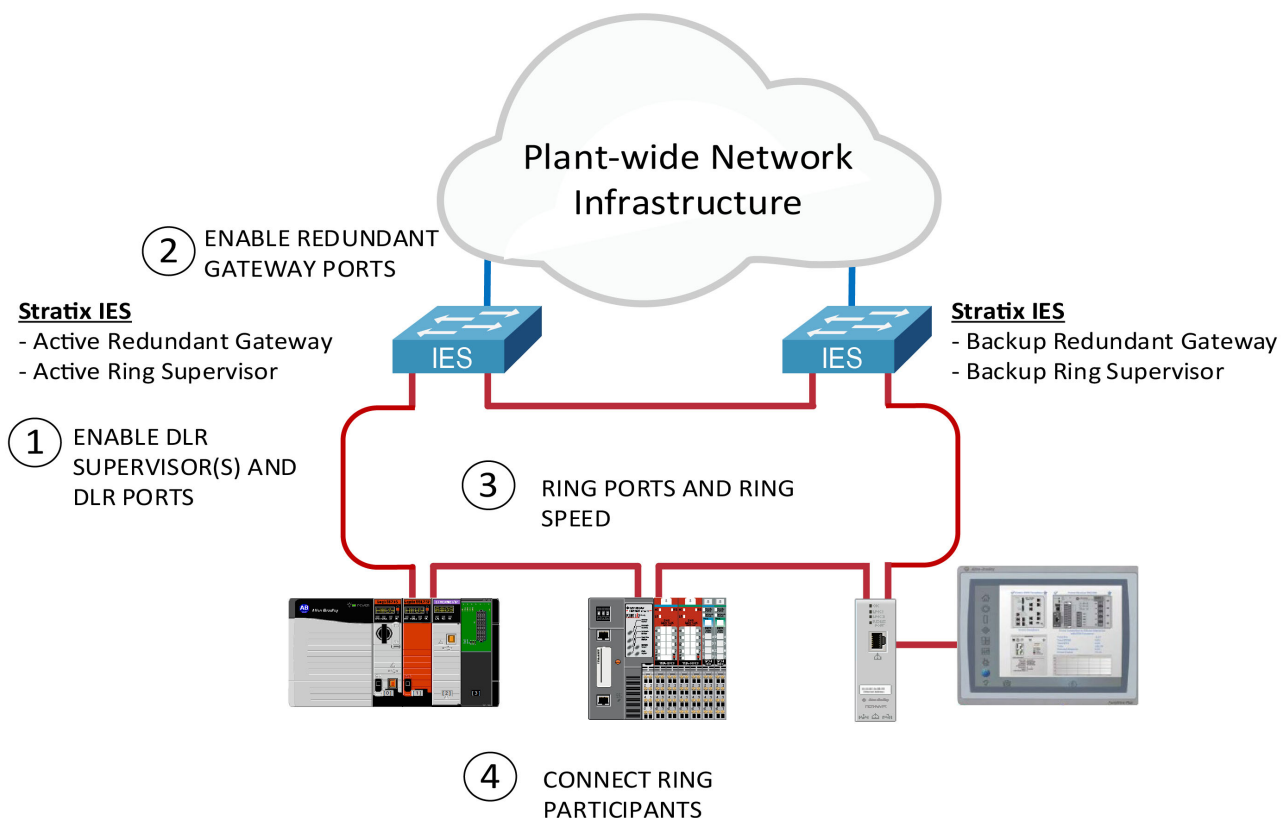
- Step 3 It is recommended to leave all ring participant DLR ports to auto negotiate. In a scenario where one of the ring participants must be configured to a hardcoded speed and duplex, then it is recommended to hardcode the speed and duplex for all ring participants.

**Note**

Prior to IOS 15.2(6)E2a, in the instance of direct Stratix-to-Stratix: If using the Gigabit ports on the Stratix IES as DLR ports on copper interconnection media with the desired ring speed of 100 Mbps, then port speeds must be hardcoded to 100 Mbps and IES interconnections must use Ethernet crossover cables.

- Step 4 Connect ring participants and close the ring.

Figure 3-1 DLR Order of Configuration



377692

Configuration Methods

There exist three primary methods to configure a DLR ring using Stratix Industrial Ethernet Switches:

- Device Manager (Web Browser)
- Studio 5000 Logix Designer Application
- IES Command Line Interface (CLI)



Note

The following configuration methodologies assumes that the Express Setup procedure, or similar, was already used to properly configure basic IES settings, IP address, Smartport Roles, and VLANs (as applicable). For more information, reference the Stratix Managed Switches User Manual, 1783-UM007 (http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf).

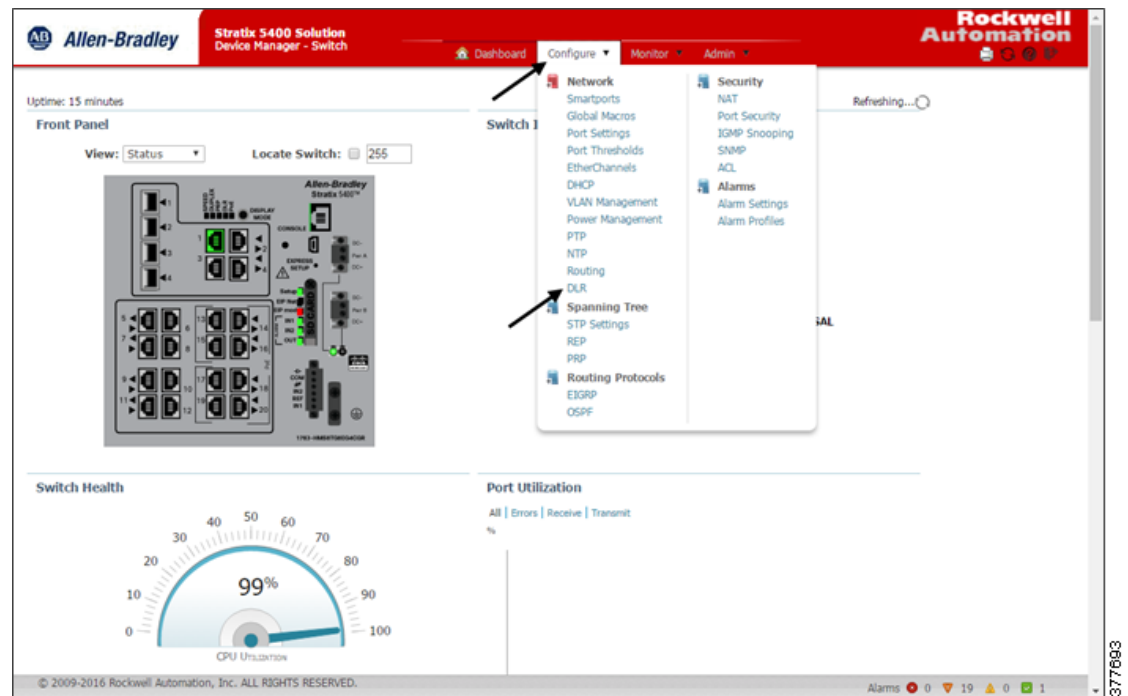
Device Manager

To configure a DLR network, start with a linear network by temporarily leaving the Ethernet segment between two nodes disconnected from each other.

Complete the Express setup to give the Stratix 5700 or Stratix 5400 IES an IP address and username/password to access the Device Manager web browser interface. In the Device Manager of the Stratix 5700 or Stratix 5400 IES, configure a common VLAN, and set the Multiport Automation Device Smartport roles for the DLR ring ports. IACS device ports that are not participating in the DLR ring may use Automation Device or Multiport Automation device Smartports, depending on security policies and procedures.

Once complete, configure DLR using the following methods.

Figure 3-2 Device Manager—DLR Configuration Mode Selection



Click the **Configure** button found in the header menu at the top of the page and choose **DLR** from the drop-down options:

- To configure the IES as a ring node or a ring supervisor, complete the fields on the Config DLR tab, as described in [Table 3-1](#).
- To configure the IES for Redundant Gateway, complete the fields on the Config tab, as described in [Table 3-2](#).
- To configure DHCP for ring devices, complete the fields on the Config DHCP tab, as described in [Table 3-5](#).

Configuring a DLR Ring Supervisor or Participant



Note

The first step in implementing a DLR is to configure a DLR supervisor, which must be done prior to physically connecting any ring media.

Figure 3-3 Device Manager—DLR Configuration

The screenshot shows the 'Stratix 5700 Device Manager - Switch' web interface. The top navigation bar includes the Allen-Bradley logo, a red header with the device name, and links for 'Dashboard' and 'Configuration'. Below this, a breadcrumb trail shows 'Network' and 'DLR'. Two tabs are visible: 'Config DLR' (selected) and 'Config DHCP'. The 'Config DLR' tab contains the following settings:

- Mode:** A dropdown menu set to 'Supervisor'.
- Port1:** A dropdown menu set to 'FastEthernet1/15'.
- Port2:** A dropdown menu set to 'FastEthernet1/16'.
- Supervisor Settings:** A section with several fields:
 - Role(Precedence):** A dropdown menu set to 'Primary'.
 - Beacon Interval:** A text input field set to '400' with the unit 'uSec'.
 - Beacon Timeout:** A text input field set to '1960' with the unit 'uSec'.
 - DLR Vlan Id:** A text input field set to '0'.
 - Reset To Default Values:** A button.
- Enable Redundant Gateway:** A checkbox that is currently unchecked.
- Submit:** A button at the bottom right.

378712

Applicable fields and their associated entries are shown in [Table 3-1](#).

Table 3-1 Device Manager—DLR Configuration Fields Applicable to Figure 3-3


Field	Description
DLR Ring ID	(Stratix 5400 IES only). Choose the ring number to configure: <ul style="list-style-type: none"> • Ring 1 • Ring 2 • Ring 3
Mode	Choose one of these modes: <ul style="list-style-type: none"> • Disabled—The DLR feature is disabled on the IES. • Node—The IES is a ring node. • Supervisor—The IES is a ring supervisor. Default: Disabled
Port 1	Choose a ring port. See Appendix B, “References” for Stratix DLR-compatible ports. <div>  Note By default, if the IES is the ring supervisor, then port 1 is node 1 on the ring and port 2 is blocked. </div>
Port 2	Choose a ring port.
Supervisor Settings	
Role (Precedence)	Choose a role to assign to the ring supervisor that corresponds to a predefined precedence value. The IES transmits the precedence value in beacon frames and uses it to determine the active ring supervisor when multiple supervisors are configured. A higher value means higher precedence. When two DLR supervisors have the same precedence, the IACS device with the numerically highest MAC address becomes the active supervisor. Valid values: <ul style="list-style-type: none"> • None—0 • Primary—255 • Backup 1—100 • Backup 2—90 • Backup 3—80 • Custom—Type a value from 0...255
Beacon Interval	Type an interval for the supervisor to transmit beacon frames. Valid values: <ul style="list-style-type: none"> • 200...100,000 μs Default: 400 μ s

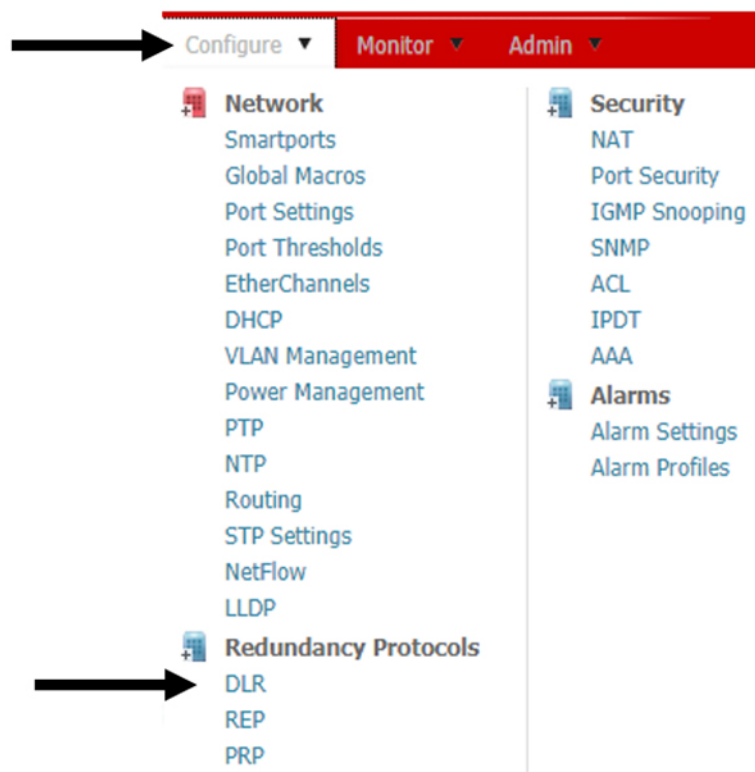
Table 3-1 Device Manager—DLR Configuration Fields Applicable to Figure 3-3 (continued)

Field	Description
Beacon Timeout	Type the amount of time ring nodes wait before timing out in the absence of received beacon messages. Valid values: <ul style="list-style-type: none"> 200...500,000 μs Default: 1960 μ s
DLR VLAN ID	Type the VLAN ID for sending DLR protocol management frames. Valid values: <ul style="list-style-type: none"> 0...4095 Default: 0 (no VLAN ID is used)

Configuring a DLR Redundant Gateway

Click the **Configure** button found in the header at the top of the page and choose DLR from the drop-down options.

Figure 3-4 Device Manager—DLR Configuration Mode Selection



To configure the IES as a DLR Redundant Gateway, click the **Enable Redundant Gateway** button and complete the required and recommended field as described in Table 3-2.

Figure 3-5 Device Manager—DLR Redundant Gateway Configuration—Primary

☒ Enable Redundant Gateway

Redundant Gateway Settings

Role(Precedence): Primary 255

Advertise Interval: 2000 uSec

Advertise Timeout: 5000 uSec

Learning Update: ☒

Uplink Ports:

- ☐ GigabitEthernet1/1
- ☐ GigabitEthernet1/2
- ☒ GigabitEthernet1/3
- ☒ GigabitEthernet1/4
- ☐ GigabitEthernet1/5
- ☐ GigabitEthernet1/6
- ☐ GigabitEthernet1/7
- ☐ GigabitEthernet1/8
- ☐ GigabitEthernet1/9
- ☐ GigabitEthernet1/10
- ☐ GigabitEthernet1/11

Reset To Default Values

Submit

Figure 3-6 Device Manager—DLR Redundant Gateway Configuration—Backup

☒ Enable Redundant Gateway

Redundant Gateway Settings

Role(Precedence): Backup 1 100

Advertise Interval: 2000 uSec

Advertise Timeout: 5000 uSec

Learning Update: ☒

Uplink Ports:

- ☐ GigabitEthernet1/1
- ☐ GigabitEthernet1/2
- ☒ GigabitEthernet1/3
- ☒ GigabitEthernet1/4
- ☐ GigabitEthernet1/5
- ☐ GigabitEthernet1/6
- ☐ GigabitEthernet1/7
- ☐ GigabitEthernet1/8
- ☐ GigabitEthernet1/9
- ☐ GigabitEthernet1/10
- ☐ GigabitEthernet1/11

Reset To Default Values

Submit

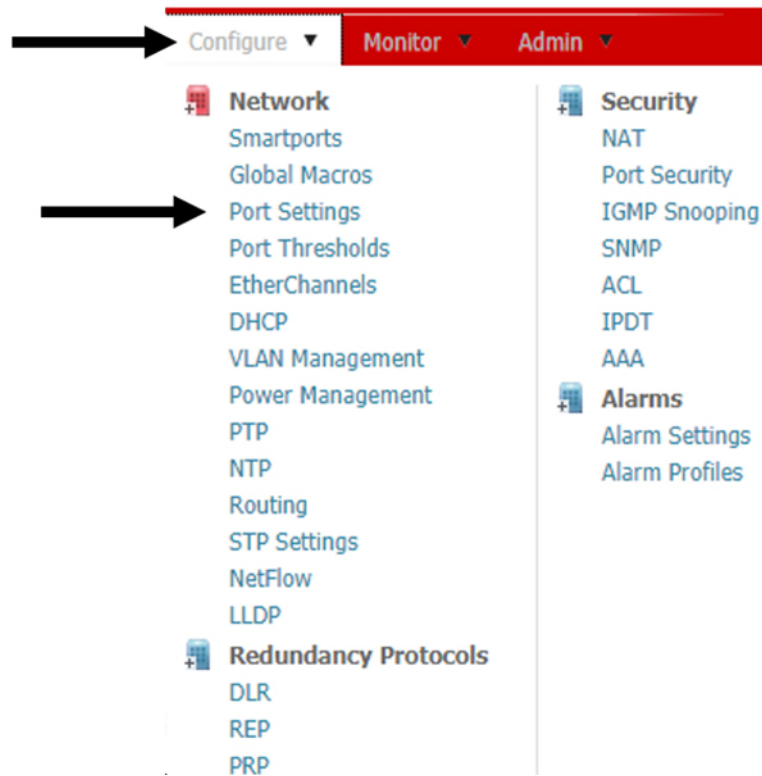
Table 3-2 Device Manager—DLR Redundant Gateway Configuration Fields Applicable to Figure 3-5 and Figure 3-9

Field	Description
Redundant Gateway Settings	
Enable Redundant Gateway	Check the checkbox to enable the configuration of Redundant Gateways. The configuration fields are available only after you enable the feature. Default: Disabled
Role (Precedence)	Choose a role to assign to the Redundant Gateway that corresponds to a predefined precedence value. The IES transmits the precedence value as advertise messages and the value is used to select the active Redundant Gateway when multiple Redundant Gateways are configured. A higher value means higher precedence. When two DLR Redundant Gateways have the same precedence, the IES with the numerically highest MAC address will become the Redundant Gateway. Valid values: <ul style="list-style-type: none"> None—0 Primary—255 Backup 1—100 Backup 2—90 Backup 3—80 Custom—Type a value from 0...255
Advertise Interval	Type the time interval for the gateway to transmit advertise messages. Valid values: <ul style="list-style-type: none"> 200...100,000 μs Default: 2000 μ s
Advertise Timeout	Type the duration of time for nodes to wait before timing out in the absence of received advertise messages. Valid values: <ul style="list-style-type: none"> 200...500,000 μs Default: 5000 μ s
Learning Update	Check the checkbox to enable learning update messages. Default: Enabled
Uplink Ports	Check the checkbox for each uplink port on which you want to enable Redundant Gateway.

Configuring DLR VLAN Trunking

Click the **Configure** button found in the header menu at the top of the page and choose **Port Settings** from the drop-down options.

Figure 3-7 Device Manager—Port Settings Configuration Mode Selection



To configure the IES port as a trunk link for DLR VLAN Trunking, select the appropriate DLR-capable port and click the **Edit** button and complete the required and recommended field as described in [Table 3-3](#).

Figure 3-8 Device Manager—Port Settings Configuration

Stratix 5400 Solution Device Manager - Switch										
Dashboard Configure Monitor Admin										
Network Port Settings										
Physical Port Table										
Edit										
	Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode	Native VLAN
<input type="radio"/>	Gi1/1	DLR VLAN Trunking	●	Auto-1000Mb/s	Auto-Full	AUTO-SELECT 10/100...	Trunk		Trunk	999
<input type="radio"/>	Gi1/2	DLR VLAN Trunking	●	Auto-1000Mb/s	Auto-Full	AUTO-SELECT 10/100...	Trunk		Trunk	999
<input type="radio"/>	Gi1/3		●	Auto	Auto	AUTO-SELECT Not Pr...	Down	1	Access	
<input type="radio"/>	Gi1/4		●	Auto	Auto	AUTO-SELECT Not Pr...	Down	1	Access	

Figure 3-9 Device Manager—Physical Port Configuration—Trunk

Edit Physical Port [X]

Port Name: Gi1/1

Description: DLR VLAN Trunking (Range: 1-200 Characters)

Administrative: ☒ Enable

Speed: Auto

Duplex: Auto

Auto MDIX: ☒ Enable

Media Type: Auto

VLAN-0: ☒ Enable

Administrative Mode: Trunk

Access VLAN: default-1

Allowed VLAN:

- ☐ All VLANs
- ☒ VLAN IDs

 10,20,30,40,50,60,999 (e.g., 2,4,10-20)

Native VLAN: NATIVE-999

[OK] [Cancel]

Refer to [Appendix A, “DLR Port Choices for Stratix Switches”](#) for DLR port choices.

Table 3-3 Device Manager—Port Settings Fields Applicable to Figure 3-12

Field	Description
Port Name	The number of the switch port, including port type, such as Fa for Fast Ethernet and Gi for Gigabit Ethernet, and the specific port number: <ul style="list-style-type: none"> Gi/1 is the Gigabit port 1 of the switch. Fa1/1 is Fast Ethernet port 1 on the switch.
Description	The description of the switch port. We recommend that you provide a port description to help identify the port during monitoring and troubleshooting. The description can be the location of the connected device or the name of the person who uses the connected device.
Port Status	(Appears only on the Edit Physical Port page; not editable). Indicates whether a device is connected to the port: <ul style="list-style-type: none"> Green = Connected Gray = Not connected

Table 3-3 Device Manager—Port Settings Fields Applicable to Figure 3-12 (continued)

Field	Description
Speed	<p>The operating speed of the switch port. If the connected device can negotiate the link speed with the switch port, choose Auto (autonegotiation).</p> <p>We recommend that you use Auto speed so that the speed of the switch port automatically matches the speed of the connected device. If the connected device requires a specific speed, change the speed of the switch port.</p> <p>Default: Auto</p>
Duplex	<p>The duplex mode of the switch port:</p> <ul style="list-style-type: none"> Auto-(Autonegotiation). The connected device can negotiate the duplex mode with the switch. In the Physical Port table, the negotiated setting is Auto-Full or Auto-Half. If the port is not connected or has not completed negotiation, the status is Auto. Half- (Half-duplex mode). The connected device must alternate sending or receiving data. Full- (Full-duplex mode). Both devices can send data simultaneously. <p>On Gigabit Ethernet ports, you cannot set the port to Half-duplex mode if the port speed is set to Auto.</p> <p>We recommend that you use Auto mode so that the mode on the switch port automatically matches the mode of the connected device. If the connected device requires a specific duplex mode, change the mode of the switch port.</p> <p>Default: Auto</p>
Auto MDX	<p>(Appears only on the Edit Physical Port page). When enabled, this feature detects the port cable (straight-through or crossover) and configures the port pinouts, speed, and duplex mode to communicate correctly with the connected device. This setting is not available on SFP module ports.</p> <p>Default: Enabled</p>
Media Type	<p>(Applies to dual-purpose uplink ports). The active port type (either the RJ45 port or the SFP module port) of a dual-purpose uplink port.</p> <p>By default, the switch detects whether the RJ45 port or SFP module port of a dual-purpose port is connected and uses the port accordingly. Only one port can be active at a time. If both ports are connected, the SFP module port has priority. You cannot change the priority setting.</p> <p>Choose from the following media types:</p> <ul style="list-style-type: none"> SFP-Only the SFP module port of a dual-port is active. You can set the speed and duplex settings. Auto-MDIX is not available. For Gigabit Ethernet SFP ports, you can set the speed and duplex to Auto or 1000 Mb/s. This configures the port not to negotiate a device that does not support autonegotiation. RJ45-Only the RJ45 port of a dual-port is active. You can enter the settings for port speed and duplex or choose Auto MDIX. Auto-(Autonegotiation). The switch detects whether the RJ45 port or the SFP module port is connected and uses the port accordingly. Only one port can be active at a time. If both ports are connected to the network, the SFP module port has priority. The speed and duplex are set to Auto. <p>Default: Auto</p>

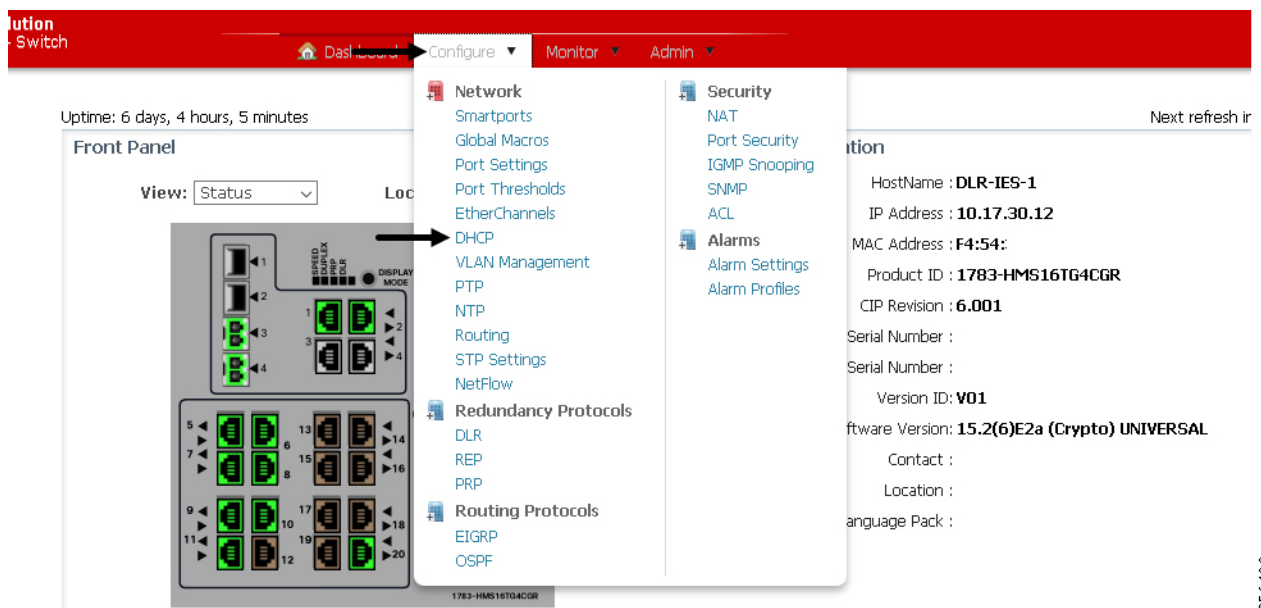
Table 3-3 Device Manager—Port Settings Fields Applicable to Figure 3-12 (continued)

Field	Description
Operational Mode	(Appears only in the Physical Port table; not editable). The operational state of the port. Displays the administrative mode or Down if disabled.
VLAN-0	(Appears only on the Edit Physical Port page). Enables the system to handle 802.1Q Ethernet frames with VLAN ID 0, which are called priority tagged frames. The purpose of priority tagged frames is to give priority to the frames with no significance to the VLAN ID. For example, PROFINET messaging requires priority tagged frames to pass CIP messages through the switch. For more information about VLAN 0 priority tagging Default: Enabled

Configuring a DHCP Pool

Click the **Configure** button found in the header menu at the top of the page and choose **DHCP** from the drop-down options.

Figure 3-10 Device Manager-DHCP



To configure the IES as a DHCP server, click the **Add** button and complete the required and recommended field as described in Table 3-4.

Figure 3-11 Device Manager-DHCP Pool Configuration

The screenshot displays the 'DHCP Persistence' configuration window in the Device Manager. The window is titled 'Global Settings' and 'DHCP Persistence'. On the left, there are checkboxes for 'Enable DHCP:' and 'DHCP Snooping:', both of which are checked. Below these is a 'Submit' button. The main area of the window contains a 'DHCP Pool Table' with columns for 'Pool Name' and 'Network'. The table is currently empty. To the right of the table is a configuration form for a DHCP pool. The form includes the following fields and values:

- DHCP Pool Name ***: CPwE_DLR
- DHCP Pool Network ***: 192.168.1.0
- Subnet Mask ***: 255.255.255.0
- Starting IP ***: 192.168.1.50
- Ending IP ***: 192.168.1.80
- Default Router**: 192.168.1.1
- Domain Name**: cpwe-rockwell.com
- DNS Server**: (empty)
- CIP Instance**: 2
- Reserved Only**: ☒
- DHCP Snooping**: ☒
- Never Expires**: ☒
- User Defined**: ☐ (with sub-fields for Days, HH, MM, and SS)

At the bottom right of the form are 'OK' and 'Cancel' buttons. The background of the Device Manager interface shows a red header with 'ution Switch' and navigation tabs for 'Dashboard', 'Configure', 'Monitor', and 'Admin'.

Table 3-4 Device Manager—DLR Configuration Fields Applicable to Figure 3-11

Field	Description
DHCP Pool Name	<p>The name of the DHCP IP address pool that is configured on the IES. The name can have up to 31 alphanumeric characters. A DHCP IP address pool is a range (or pool) of available IP addresses that the IES can assign to connected IACS devices. The name cannot contain a ? or a tab.</p> <p>This field is required.</p>
DHCP Pool Network	<p>The sub-network IP address of the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers separated by periods. Each number can be from 0...255.</p> <p>This field is required.</p>
Subnet Mask	<p>The network address that identifies the subnetwork (subnet) of the DHCP IP address pool. Subnets segment the IACS devices in a network into smaller groups. The default is 255.255.255.0 (/24).</p> <p>This field is required.</p>
Starting IP	<p>The starting IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers separated by periods. Each number can be from 0...255.</p> <p>Be sure that none of the IP addresses that you assign are being used by another IACS device in your network.</p> <p>This field is required.</p>

Table 3-4 Device Manager—DLR Configuration Fields Applicable to Figure 3-11 (continued)

Field	Description
Ending IP	<p>The ending IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers separated by periods. Each number can be from 0...255.</p> <p>Make sure that none of the IP address you assign are being used by other devices in your network.</p> <p>This field is required.</p>
Default Router	<p>The default router IP address for the DHCP client that uses this server. The format is a 32-bit numeric address that is written as four numbers separated by periods. Each number can be from 0... 255.</p> <p>This field is optional; use to set the default gateway field on DHCP clients.</p>
Domain Name	<p>The domain name for the DHCP client. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab.</p> <p>This field is optional.</p>
Reserved-Only	<p>Use the reserved-only DHCP pool configuration to restrict assignments from the DHCP pool to preconfigured reservations.</p> <p>This field is optional but recommended.</p>
DHCP Snooping	<p>Enables DHCP snooping on a VLAN associated to the sub-network IP address of the IP address pool identified in the DHCP Pool Network field.</p> <p>This field is optional but recommended.</p>
DNS Server	<p>The IP addresses of the domain name system (DNS) IP servers available to a DHCP client. The format is a 32-bit numeric address that is written as four numbers separated by periods. Each number can be from 0...255.</p> <p>This field is optional.</p>
CIP Instance	<p>A number from 1...15 to identify the address pool.</p> <p>This field is read-only.</p>
[Lease Length]	<p>The duration of the lease for an IP address that is assigned to a DHCP client. Click one of the following:</p> <ul style="list-style-type: none"> • Never Expires • User Defined <p>If User Defined is enabled, enter the duration of the lease in the numbers of days, hours, and minutes. This lease length is used for all assignments.</p>

Configuring a DLR Ring DHCP Server

Figure 3-12 Device Manager—DHCP Server Configuration

Config DLR Config DHCP

☒ Ring DHCP Server Enable Role : Primary

☒ Ring DHCP Snooping Status : Ring Fault

Number of Devices : 5 Backup Interval : 60

	Index	IP Address	Host Name	Pool
1 <input type="radio"/>	2	192.168.1.50	1756-EN2T	CPwE_DLR
2 <input type="radio"/>	3	192.168.1.60	E300	CPwE_DLR
3 <input type="radio"/>	4	192.168.1.70	PF525_1	CPwE_DLR
4 <input type="radio"/>	5	192.168.1.71	PF525_2	CPwE_DLR

Applicable fields and their associated entries are shown in [Table 3-5](#).

Table 3-5 Device Manager—DHCP Server Configuration Fields Applicable to [Figure 3-12](#)

Field	Description
Ring DHCP Server Enable	Check the checkbox to enable the ring DHCP server on the DLR supervisor device.
Role	Choose a role to assign to the ring DHCP server. Valid values: <ul style="list-style-type: none"> • None—The server is inactive. • Primary—The DLR supervisor functions as the active ring DHCP server. • Backup—The DLR supervisor functions as the backup ring DHCP server.
Ring DHCP Snooping	Check the checkbox to restrict the broadcast of DHCP requests from going beyond the ring. Only devices in the ring receive address assignments from the DHCP server. DHCP snooping is enabled by default. If you are not using DLR DHCP, you must disable Ring DHCP Snooping to use DHCP server functionality outside of the ring. This includes DHCP Port Persistence on individual IES ring participants.
Status	Displays the status of the ring. Valid values: <ul style="list-style-type: none"> • Normal • Ring Fault • Unexpected Loop Detected • Partial Network Fault • Rapid Fault/Restore Cycle

Table 3-5 Device Manager—DHCP Server Configuration Fields Applicable to Figure 3-12 (continued)

Field	Description
Number of Devices	Type the number of IACS devices in the ring, including IES.
Backup Interval	Type the interval in seconds at which the backup ring DHCP server reads the reference table of the active ring DHCP server. Valid values: <ul style="list-style-type: none"> 1...65535 seconds Default: 60

Manually Assigning IP Addresses to Ring Devices

To manually assign IP addresses to ring devices via Ring DHCP, click the **Add Entry** button on the DLR DHCP configuration page. This will prompt you to enter host information as seen in Figure 3-13.

Figure 3-13 Device Manager—Manual IP Address Assignment via Ring DHCP

Applicable fields and their associated entries are shown in Table 3-6.

Table 3-6 Device Manager—DLR Node Address Manual Assignment via DHCP

Field	Description
Index	Type a value that indicates the location of the ring node in relation to the active DHCP server. Valid values: <ul style="list-style-type: none"> 2 ...255
IP Address	Type the IP address for the entry.
Host Name	Type a host name to associate with the IP address for the entry.
DHCP Pool	Choose the name of the IP address pool to use for ring devices. DHCP persistence and DHCP for ring devices can coexist, but cannot share the same pool.

Specifying a Range of IP Addresses to Assign to Ring Devices

To specify a range of IP addresses to assign to ring devices via Ring DHCP, click the **Add Range** button on the DLR DHCP configuration page. This will prompt you to enter host range information as seen in [Figure 3-14](#).

Figure 3-14 Device Manager—Assigning IP Addresses to DLR Ring Participants from a Pre-Defined Pool

Applicable fields and their associated entries are shown in [Table 3-7](#).

Table 3-7 Device Manager—Assigning DLR Node Addresses from an Address Range

Field	Description
Starting Index	Type a value that indicates the starting location of the ring devices in the range. Valid values: <ul style="list-style-type: none"> 2 ...255
Starting IP Address	Type the starting IP address for the range of entries.
Number of Entries	Type the number of entries in the range.
DHCP Pool	Choose the name of the IP address pool to use for ring devices. This pool must be previously configured. DHCP persistence and DHCP for ring devices can coexist, but cannot share the same pool.

Configure IGMP Snooping Extension Extended Flood

From the Configure menu, choose IGMP Snooping.

Figure 3-15 Device Manager—Configure IGMP Snooping with Querier

Security | IGMP Snooping

IGMP Snooping ☒ Enable
 IGMP Querier ☒ Enable Querier Address:
 Extended Flood ☒ Enable 10 seconds after multicast router detected (Range 1-300, Default value is 10 seconds)
 Solicit Query at TCN ☒ Enable

VLAN ID	VLAN Name	Enable IGMP Snooping
1	default	<input checked="" type="checkbox"/>
30	VLAN0030	<input checked="" type="checkbox"/>
999	NATIVE	<input checked="" type="checkbox"/>

Total: 3

Table 3-8 Device Manager—IGMP Snooping Fields

Field	Description
IGMP Snooping	Check Enable to activate IGMP snooping for all VLAN IDs.
IGMP Querier	Check Enable to activate IGMP querier for all VLAN IDs. To specify an IP address for the querier, enter the address in the Querier Address Field. If an address is not specified, then the switch uses the IP address of the first SVI available for the process.
Extended Flood	Check Enable to help prevent the loss of multicast traffic when the IGMP snooping querier is disconnected and then reconnected. Enter the number of seconds after a multicast router is detected to continue flooding multicast traffic. After a period, multicast flooding is stopped. Valid values: 1...300 seconds Default: 10 seconds
Solicit Query at TCN	Check Enable to activate a multicast querier to send IGMP queries during a spanning-tree Topology Change Notification (TCN) event. Solicit Query at TCN is effective even if the querier is not the spanning-tree root. Clear the Enable checkbox to limit IGMP queriers to when the multicast querier is the spanning-tree root.
IGMP Snooping Table	
VLAN ID	The VLAN ID and name on which to enable or disable IGMP snooping.
VLAN Name	
Enable IGMP Snooping	Check Enable IGMP Snooping to enable IGMP snooping on all ports that are assigned to the corresponding VLAN. Clear Enable IGMP Snooping to disable IGMP snooping on all ports that are assigned to the corresponding VLAN.

IES Command Line Interface

Only IES ring participants can be fully configured using CLI, as IACS devices do not have this feature. To configure DLR on IES using the CLI, you must have access to Privileged EXEC mode. As with all configuration methods, the planned ring active supervisor **must** be configured before any DLR network connections are made.

**Note**

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 DLR IES. You can use the **show version** command in the CLI to display the implemented IOS version.

Command Line Interface—Ring Active Supervisor Configuration

To configure the Active supervisor for a planned DLR deployment, see the commands below or refer to [Example 3-1](#).

- Step 1 At the switch CLI, enable privileged EXEC mode using the **enable** command:

```
Switch> enable
```

Enter your password if prompted.

- Step 2 Enter global configuration mode using the **configure terminal** command:

```
Switch# configure terminal
```

- Step 3 Access the DLR Ring 1 configuration settings:

```
Switch(config)# dlr ring 1
```

- Step 4 Assign the supervisory role with all default settings to the IES:

```
Switch(config-dlr)# mode supervisor
```

- Step 5 Set the highest precedence value for **only** the intended active supervisor:

```
Switch(config-dlr-supervisor)# precedence 255
```

Refer to [Chapter 2, “CPwE Device Level Ring Design Considerations”](#) for recommended precedence values for backup supervisors.

Example 3-1 Command Line Interface—Configuring DLR Ring Supervisor Settings

```
Switch#configure terminal
Switch(config)#dlr ring 1
Switch(config-dlr)#mode supervisor
Switch(config-dlr-supervisor)#precedence 255
```

Command Line Interface—DLR Port Configuration

To configure the DLR ports, see the commands below or refer to [Example 3-2](#).

- Step 1 Enter global configuration mode using the configure terminal command:

```
Switch# configure terminal
```

- Step 2 Navigate to the desired interface to be the DLR interfaces:

```
Switch(config)# interface range fastEthernet 1/15-16
```

Refer to [Appendix A, “DLR Port Choices for Stratix Switches”](#) for DLR port choices.

- Step 3 Assign the DLR role to the switchport:

```
Switch(config-if)# dlr ring 1
```

Example 3-2 Command Line Interface—Configuring DLR Ring Supervisor Settings

```
Switch#configure terminal  
Switch(config)#interface range fastethernet 1/15-16  
Switch(config-if)#dlr ring 1
```

Command Line Interface—DLR VLAN Trunking

To configure the DLR VLAN Trunking ports, see the commands below or refer to [Example 3-3](#).

- Step 1 Enter global configuration mode using the configure terminal command:

```
Switch# configure terminal
```

- Step 2 Navigate to the desired interface to be the DLR interfaces:

```
Switch(config)# interface range fastEthernet 1/15-16
```

Refer to [Appendix A, “DLR Port Choices for Stratix Switches”](#) for DLR port choices.

- Step 3 Assign the port role to trunk:

```
Switch(config-if)# switchport mode trunk
```

- Step 4 Assign the native VLAN to the trunk:

```
Switch(config-if)# switchport trunk native vlan 999
```

- Step 5 Assign the VLANs allowed to the trunk:

```
Switch(config-if)# switchport trunk allowed vlan 10,20,30,40,50,999
```

Example 3-3 Command Line Interface—Configuring DLR VLAN Trunking

```
Switch#configure terminal  
Switch(config)#interface range fastethernet 1/15-16  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#switchport trunk native vlan 999  
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,999
```

Command Line Interface—DLR Redundant Gateway Configuration



Note

The following procedures assume you are already in the switch's Privileged Exec mode as described in [Command Line Interface—Ring Active Supervisor Configuration](#).

To configure the DLR Redundant Gateway, see the commands below or refer to [Example 3-4](#).

-
- Step 1 Enter global configuration mode using the **configure terminal** command:

```
Switch# configure terminal
```

- Step 2 Access the DLR Ring 1 configuration settings:

```
Switch(config)# dlr ring 1
```

- Step 3 Assign the gateway role with all default settings to the IES:

```
Switch(config-dlr)# gateway enable
```

- Step 4 Set the highest precedence value for **only** the intended active gateway:

```
Switch(config-dlr-gateway)# gateway-precedence 255
```

It is a good practice to assign the same precedence value for the DLR supervisor and Redundant Gateway.

Example 3-4 Command Line Interface—Redundant Gateway Configuration

```
Switch(config)#dlr ring 1  
Switch(config-dlr)#gateway enable  
Switch(config-dlr-gateway)#gateway-precedence 255
```

Command Line Interface—Redundant Gateway Uplink Port Configuration

To configure the Redundant Gateway uplink port see the commands below or refer to [Example 3-5](#):

-
- Step 1 Enter global configuration mode using the **configure terminal** command:

```
Switch# configure terminal
```

- Step 2 Navigate to the desired interface to be the uplink interface:

```
Switch(config)# interface gigabitethernet (1/1-2)
```

The interface could be Gigabitethernet or Fastethernet 1/1 through 1/20.

- Step 3 Assign the uplink role to the switchport:

```
Switch(config-if)# dlr ring 1 uplink
```

Example 3-5 Command Line Interface—Redundant Gateway Uplink Port Configuration

```
Switch#configure terminal  
Switch(config)#interface range gigabitethernet 1/1-2  
Switch(config-dlr)#dlr ring 1 uplink  
Switch(config-dlr-supervisor)#precedence 255
```



Note

For EtherChannel as the uplinking technology, the DLR uplink command must be assigned on the port-channel interface rather than the individual ports as seen in [Example 3-6](#). The DLR uplink command must be configured on individual ports or the port-channel, not both.

Example 3-6 Command Line Interface—Redundant Gateway Uplink EtherChannel Configuration

```
Switch#configure terminal
Switch(config)#interface port-channel 1
Switch(config-if)#dlr ring 1 uplink
```

Command Line Interface—Configure DHCP Pool

To configure the DHCP pool, see the commands below or refer to [Example 3-7](#).

- Step 1 Enter global configuration mode using the configure terminal command:

```
Switch# configure terminal
```

- Step 2 Enable DHCP snooping globally and, if applicable, on the VLAN:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan [ID]
```

- Step 3 Specify the IP address that the DHCP Server should not assign to clients:

```
Switch(config)# ip dhcp excluded-address [low ip address] [high ip address]
```

Unless explicitly excluded, the DHCP Server assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients.

- Step 4 Create the DHCP pool only on the primary ring DHCP server and assign it a name:

```
Switch(config)# ip dhcp pool [name]
```

- Step 5 Specify the subnet network number and mask of the DHCP address pool:

```
Switch(dhcp-config)# network [network number] [subnet mask]
```

- Step 6 Use the reserved-only DHCP pool configuration to restrict assignments from the DHCP pool to preconfigured reservations:

```
Switch(dhcp-config)# reserved-only
```

Optional: Set the default-router, domain-name, and lease:

```
Switch(dhcp-config)# default-router [ip address of default gateway device]
Switch(dhcp-config)# domain-name [name]
Switch(dhcp-config)# lease infinite
```

Example 3-7 Command Line Interface—Configure DHCP Pool

```
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 30
Switch(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.49
Switch(config)#ip dhcp pool CPwE_DLR
Switch(config-dhcp)#network 192.168.1.0 255.255.255.0
Switch(config-dhcp)#reserved-only
Switch(config-dhcp)#default-router 192.168.1.1
Switch(config-dhcp)#domain-name cpwe-rockwell-cisco.com
Switch(config-dhcp)#lease infinite
```

Command Line Interface—Configuring DLR Ring DHCP Server

To configure the DLR Ring DHCP Server, see the commands below or refer to [Example 3-8](#) for primary ring DHCP server, [Example 3-9](#) for backup ring DHCP server, and [Example 3-10](#) for interface configuration.

- Step 1 Enter global configuration mode using the configure terminal command:

```
Switch# configure terminal
```

- Step 2 Navigate to the desired dlr ring #:

```
Switch(config)# dlr ring 1
```

- Step 3 Enter the ring-dhcp configuration mode:

```
Switch(config-dlr)# ring-dhcp
```

- Step 4 Enable the ring dhcp snooping:

```
Switch(config-dlr-dhcp)# snooping enable
```

- Step 5 Enable the ring dhcp server:

```
Switch(config-dlr-dhcp)# dhcp-server enable
```

- Step 6 Specify intended role of the ring DHCP server as primary or backup:

```
Switch(config-dlr-dhcp)# intended-role [primary|backup]
```

Only for the backup ring DHCP server, there is an additional configuration command to point to the primary ring DHCP server's CIP IP address for synchronization purposes:

```
Switch(config-dlr-dhcp)# intended-role backup  
Switch(config-dlr-dhcp)# active-cip-addr [ip address]
```

- Step 7 Specify the total number of devices directly in the ring:

```
Switch(config-dlr-dhcp)# number-of-devices [1-255]
```

- Step 8 Only for the primary ring DHCP server, enter each ring node position with specific IP address assignment and specify the DHCP pool to be used:

```
Switch(config-dlr-dhcp)# entry 2 add [ip address] [DHCP pool name] [description]  
Switch(config-dlr-dhcp)# entry 3 add [ip address] [DHCP pool name] [description]  
Switch(config-dlr-dhcp)# entry 4 add [ip address] [DHCP pool name] [description]  
Switch(config-dlr-dhcp)# entry 5 add [ip address] [DHCP pool name] [description]
```

If node in position 6 has a static IP address already assigned to it, do not enter an entry for the sixth position and continue to the next node position in the ring.

```
Switch(config-dlr-dhcp)# entry 7 add [ip address] [DHCP pool name] [description]
```

Example 3-8 Command Line Interface—Configuring a DLR Primary Ring DHCP Server

```
Switch#configure terminal  
Switch(config)#dlr ring 1  
Switch(config-dlr)#ring-dhcp  
Switch(config-dlr-dhcp)#snooping enable  
Switch(config-dlr-dhcp)#dhcp-server enable  
Switch(config-dlr-dhcp)#intended-role primary  
Switch(config-dlr-dhcp)#number-of-devices 6  
Switch(config-dlr-dhcp)#entry 2 add 192.1681.50 CPwE DLR 1756-EN2TR  
Switch(config-dlr-dhcp)#entry 3 add 192.1681.60 CPwE DLR E300
```

```
Switch(config-dlr-dhcp)#entry 4 add 192.1681.70 CPwE DLR PF525_1
Switch(config-dlr-dhcp)#entry 5 add 192.1681.71 CPwE DLR PF525_2
Switch(config-dlr-dhcp)#entry 6 add 192.1681.80 CPwE DLR Safety_IO
```

Example 3-9 Command Line Interface—Configuring a DLR Backup Ring DHCP Server

```
Switch#configure terminal
Switch(config)#dlr ring 1
Switch(config-dlr)#ring-dhcp
Switch(config-dlr-dhcp)#snooping enable
Switch(config-dlr-dhcp)#dhcp-server enable
Switch(config-dlr-dhcp)#intended-role backup
Switch(config-dlr-dhcp)#active-cip-addr 192.168.1.2
Switch(config-dlr-dhcp)#number-of-devices 6
```

Example 3-10 Command Line Interface—Configuring a DLR Ring DHCP Server Interfaces

```
Switch#configure terminal
Switch(config)#interface range fastethernet 1/15-16
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#load-interval 30
Switch(config-if-range)#srr-queue bandwidth share 1 19 40 40
Switch(config-if-range)#priority-queue out
Switch(config-if-range)#no cdp enable
Switch(config-if-range)#dlr ring 1
Switch(config-if-range)#mls qos trust dscp
Switch(config-if-range)#alarm profile ab-alarm
Switch(config-if-range)#service-policy input CIP-PTP-Traffic
Switch(config-if-range)#ip dhcp snooping trust
```

Command Line Interface—Configuring IGMP Snooping Extensions

To configure IGMP Snooping with Querier see the commands below or refer to [Example 3-11](#).

- Step 1 Enter global configuration mode using the configure terminal command:

```
Switch# configure terminal
```

- Step 2 Enable IGMP Snooping:

```
Switch(config)# ip igmp snooping
```

- Step 3 Enable IGMP Snooping with Querier:

```
Switch(config)# ip igmp snooping querier
```

- Step 4 Enable Extended Flood:

```
Switch(config)# ip igmp snooping mrouter-ext-flood
```

- Step 5 Enable Solicit Query at TCN:

```
Switch(config)# ip igmp snooping tcn query solicit
```

Example 3-11 Command Line Interface—Configuring IGMP Snooping with Querier

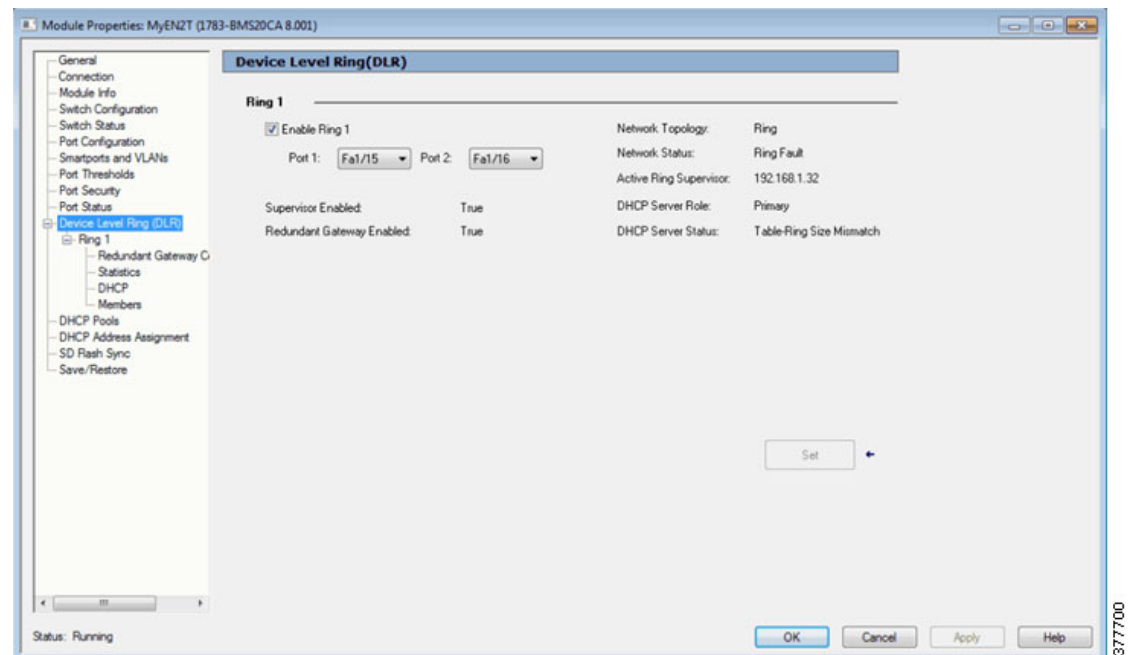
```
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)#ip igmp snooping querier
Switch(config)#ip igmp snooping mrouter-ext-flood
Switch(config)#ip igmp snooping tcn query solicit
```

Studio 5000 Logix Designer Application

For configuration guidelines when using the Studio 5000 Logix Designer Application, see the section “Configure DLR via the Studio 5000 Logix Designer Application” in the Stratix Managed Switches User Manual (http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf).

Enabling DLR on Specified Ring Ports and Viewing DLR Network Status

Figure 3-16 Studio 5000 Logix Designer—Enabling DLR on Specified Ring Ports and Viewing DLR Network Status



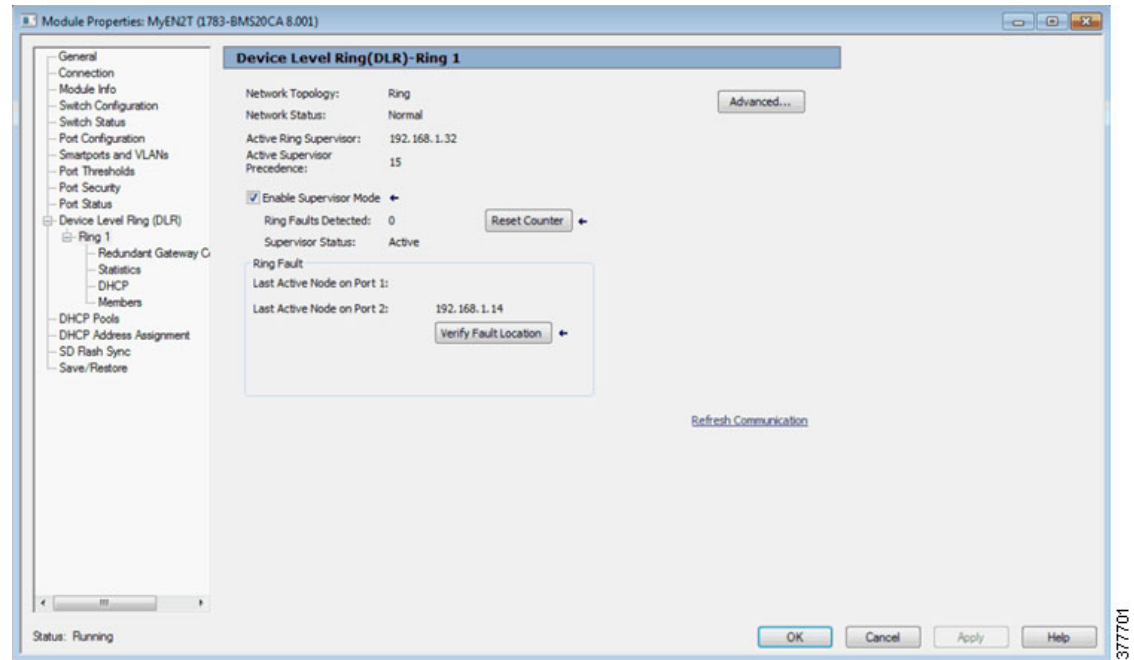
Applicable fields and their associated entries are shown in Table 3-9.

Table 3-9 Studio 5000 Logix Designer—DLR Ring Port Configuration and Network Status Applicable to Figure 3-16

Field	Description
Enable Ring 1/Enable Ring 2/Enable Ring 3 (5400 only) Enable Ring 1 (5700 only)	Check to enable DLR on the ports that are specified in the associated Port 1 and Port 2 fields for the ring.
Port 1	Choose a ring port. This field is unavailable if the Enable Ring 1 checkbox is cleared. The default value is None.
Port 2	Choose a ring port. Port 1 and Port 2 cannot be the same port. This field is unavailable if the Enable Ring 1 checkbox is cleared. The default value is None.
Supervisor Enabled	Displays whether the IES is a ring supervisor. Valid values: <ul style="list-style-type: none"> • True—The IES is a ring supervisor. • False—The IES is a ring node.
Redundant Gateway Enabled	Displays whether Redundant Gateways are enabled for the ring.
Network Topology	Displays whether the IES is operating in a DLR or linear network. Valid values: <ul style="list-style-type: none"> • Ring • Linear
Network Status	Displays the status of the network. Valid values: <ul style="list-style-type: none"> • Normal • Ring Fault • Unexpected Loop Detected • Partial Network Fault • Rapid Fault/Restore Cycle
Active Ring Supervisor	Displays the IP address of the active ring supervisor.
DCHP Server Role	Displays the role of the ring DHCP server. Valid values: <ul style="list-style-type: none"> • Disabled • Primary • Secondary • Backup
DHCP Server Status	Displays the status of the DHCP server. Valid values: <ul style="list-style-type: none"> • Normal operation • Table-ring size mismatch • Table-ring order mismatch • IP address conflict

Configuring a Ring Network

Figure 3-17 Studio 5000 Logix Designer—Configuring a Ring Network



Applicable fields and their associated entries are shown in Table 3-10.

Table 3-10 Studio 5000 Logix Designer—Configuring a Ring Network Applicable to Figure 3-17

Field	Description
Network Topology	Displays whether the IES is operating in a DLR or linear network. Valid values: <ul style="list-style-type: none"> • Ring • Linear
Network Status	Displays the status of the network. Valid values: <ul style="list-style-type: none"> • Normal • Ring Fault • Unexpected Loop Detected • Partial Network Fault • Rapid Fault/Restore Cycle
Active Ring Supervisor	Displays the IP address of the active ring supervisor.
Active Supervisor Precedence	Displays the precedence that is assigned to the ring supervisor. You assign the precedence value on the Advanced Network Configuration dialog box.
Enable Supervisor Mode	Check to make the IES a ring supervisor. The configuration takes effect immediately.

Table 3-10 Studio 5000 Logix Designer—Configuring a Ring Network Applicable to Figure 3-17 (continued)

Field	Description
Ring Faults Detected	Displays the number of faults that are currently detected in the ring. When a DLR network is powered-up, the supervisor can detect ring faults as a result of powering up before other IACS and IES devices on the network. You can use an MSG instruction to clear the faults.
Supervisor Status	Displays whether the IES is operating as the active ring supervisor or backup ring supervisor. Valid values: <ul style="list-style-type: none"> Active Backup
Last Active Node on Port 1	Displays the IP address of the last active node on DLR port 1.
Last Active Node on Port 2	Displays the IP address of the last active node on DLR port 2.

Advanced DLR Network Configuration

Figure 3-18 Studio 5000 Logix Designer—Configuring Advanced DLR Network Parameters

Advanced Network Configuration

Network Topology: Ring

Active Ring Supervisor: 192.168.1.2

Active Supervisor Precedence: 255

Supervisor Mode: Enabled

Supervisor Precedence: 255

Supervisor Status: Active

Ring Parameters

Beacon Interval: 400 μs

Beacon Timeout: 1960 μs

Ring Protocol VLAN ID: 0

Set

Close Help

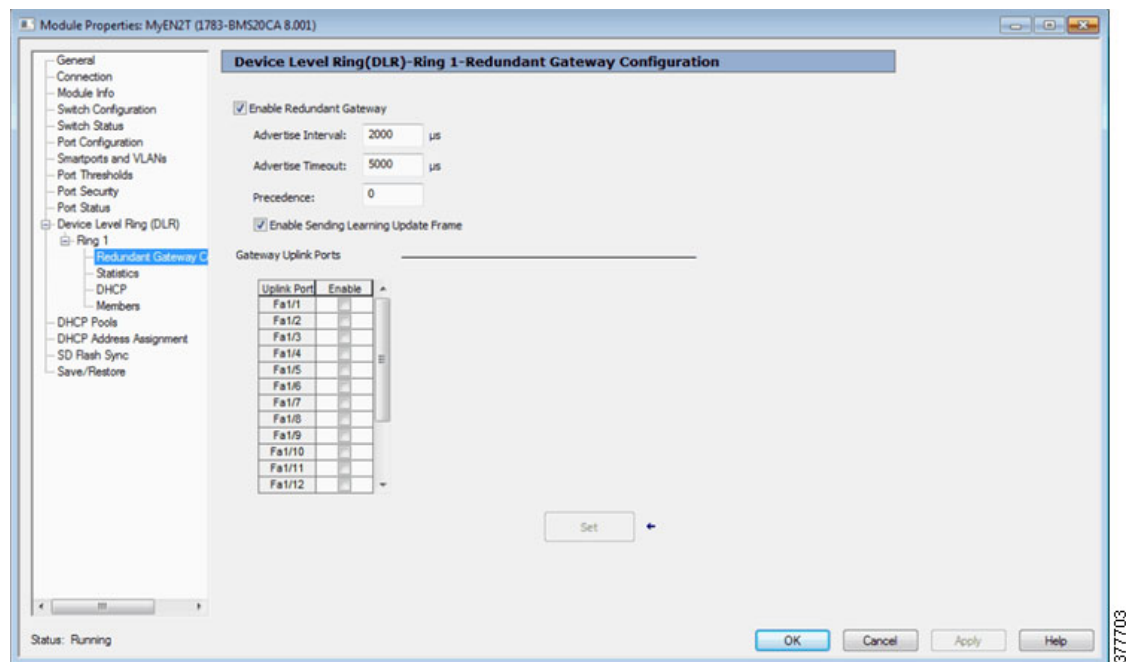
Applicable fields and their associated entries are shown in Table 3-11.

Table 3-11 Studio 5000 Logix Designer—Advanced DLR Network Configuration Applicable to Figure 3-18

Field	Description
Network Topology	Displays whether the IES is operating in a DLR or linear network. Valid values: <ul style="list-style-type: none"> • Ring • Linear
Active Ring Supervisor	Displays the IP address of the active ring supervisor.
Active Supervisor Precedence	Displays the precedence that is currently assigned to the active ring supervisor.
Supervisor Mode	Displays the status of Supervisor mode. You can enable Supervisor mode on the Ring 1, Ring 2, or Ring 2 view. Valid values: <ul style="list-style-type: none"> • Enabled • Disabled (default)
Supervisor Precedence	Type a precedence value to assign to the ring supervisor. When multiple supervisors are configured, the precedence value determines the active ring supervisor. Only one supervisor can be active at one time. The precedence is transmitted in beacon frames. When two supervisors have the same precedence, the supervisor with the numerically highest MAC address becomes the active supervisor. Valid values: <ul style="list-style-type: none"> • 0...255 The default precedence is 0.
Beacon Interval	Type an interval for the supervisor to transmit beacon frames. Valid values: <ul style="list-style-type: none"> • 200...100,000 μs The default interval is 400 μ s.
Beacon Timeout	Type the amount of time ring nodes wait before timing out in the absence of received beacon messages. Valid values: <ul style="list-style-type: none"> • 400...500,000 μs The default timeout is 1960 μ s.
Ring Protocol VLAN ID	Reserved for future use.

Redundant Gateway Configuration

Figure 3-19 Studio 5000 Logix Designer—Configuring a DLR Redundant Gateway



Applicable fields and their associated entries are shown in Table 3-12.

Table 3-12 Studio 5000 Logix Designer—Configuring the Redundant Gateway Feature Applicable to Figure 3-19

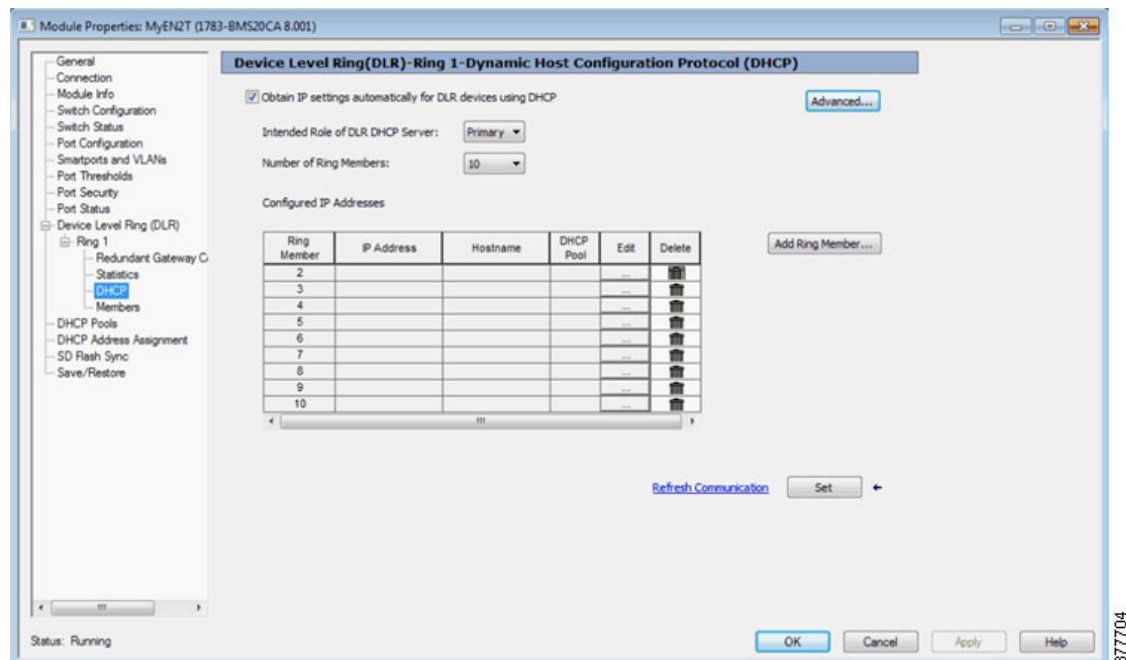
Field	Description
Enable Redundant Gateway	Check the checkbox to enable the configuration of Redundant Gateways. The configuration fields are available only after you enable the feature. Default: Disabled
Advertise Interval	Type the time interval for the gateway to transmit advertise messages. Valid values: <ul style="list-style-type: none"> 200...100,000 μs Default: 2000 μs
Advertise Timeout	Type the duration of time for nodes to wait before timing out in the absence of received advertise messages. Valid values: <ul style="list-style-type: none"> 200...500,000 μs Default: 5000 μs

Table 3-12 Studio 5000 Logix Designer—Configuring the Redundant Gateway Feature Applicable to Figure 3-19

Field	Description
Precedence	<p>Choose a role to assign to the Redundant Gateway that corresponds to a predefined precedence value. The IES transmits the precedence value in advertise messages and is used to select the Redundant Gateway when multiple Redundant Gateways are configured. A higher value means higher precedence. When two DLR Redundant Gateways have the same precedence, the IES with the numerically highest MAC address will become the active Redundant Gateway.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • None—0 • Primary—255 • Backup 1—100 • Backup 2—90 • Backup 3—80 • Custom—Type a value from 0...255
Enable Sending Learning Update Frame	<p>Check the checkbox to enable learning update messages.</p> <p>Default: Enabled</p>
Gateway Uplink Ports	<p>Check the Enable checkbox for each uplink port on which to enable Redundant Gateway.</p>

Configuring Ring DHCP

Figure 3-20 Studio 5000 Logix Designer—Configuring DLR DHCP



Applicable fields and their associated entries are shown in Table 3-13.

Table 3-13 Studio 5000 Logix Designer—DLR Ring DHCP Configuration Applicable to Figure 3-20

Field	Description
Obtain IP settings automatically for DLR devices using DHCP	Check the checkbox to enable the ring DHCP server on the DLR supervisor device.
Intended Role of DHCP Server	Choose the role to assign to the DHCP server: <ul style="list-style-type: none"> • Primary—The DLR supervisor functions as the active ring DHCP server. • Backup—The DLR supervisor functions as the backup ring DHCP server.
Number of Ring Members	Choose the number of IACS devices in the ring, including IES.
Ring Member	Displays the order of devices in the ring when the IES is the ring supervisor. The IES is always ring member 1.
IP Address	Displays the IP address of the ring member. The IP address is reserved for the selected port and is not available for normal DHCP assignment. The IP address must be an address from the pool specified in DHCP IP address pool.
Hostname	Displays the name for the host associated with the ring member.
DHCP Pool	Displays the name of the DHCP IP address pool configured on the IES.

For more information on configuring a DLR DHCP Server and adding devices to the DHCP participant list, refer to the Allen-Bradley Stratix Managed Switches User Manual, 1783-UM007 (http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf).

CPwE Device Level Ring Monitoring and Troubleshooting

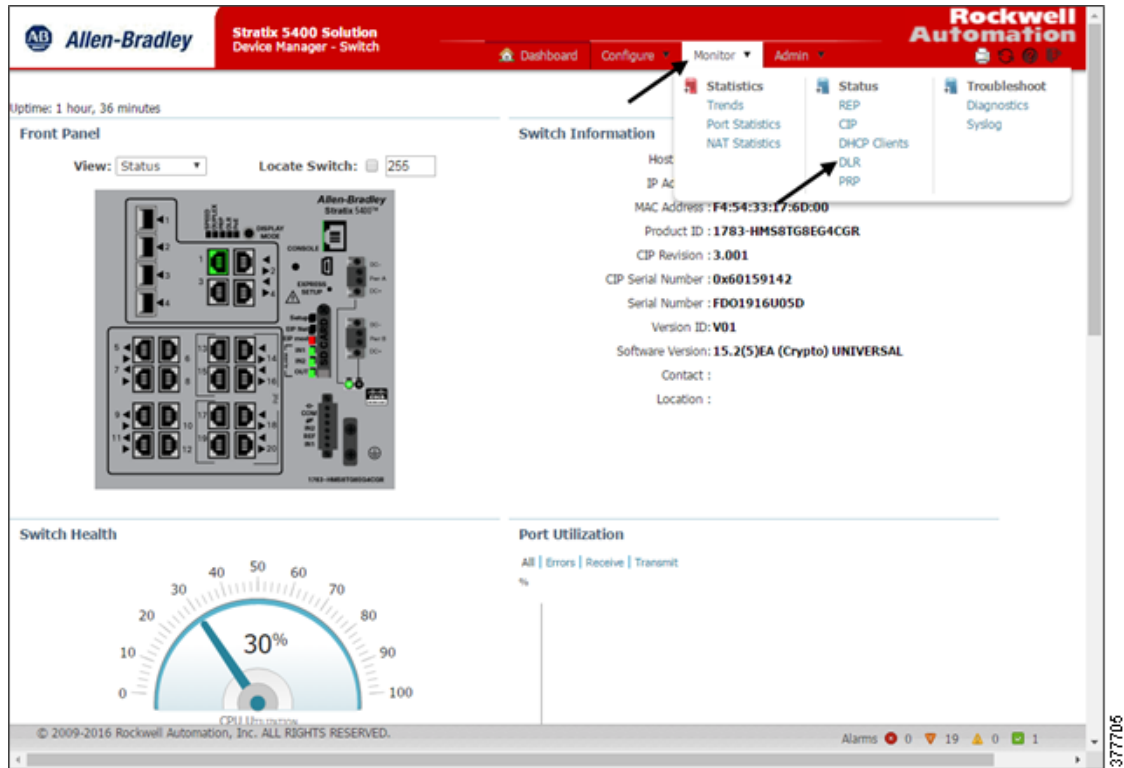
Overview

The CIP DLR object can be utilized to gather diagnostics about the ring. Network diagnostic information can be retrieved from ring supervisor-capable devices using:

- Device web pages (Device Manager)
- Studio 5000 Logix Designer programming software status pages
- Command Line Interface (CLI)
- Rockwell Automation DLR Faceplates
- FactoryTalk Network Manager (FTNM)

Device Manager

Figure 4-1 Device Manager—DLR Monitor Selection



From the Monitor menu, choose DLR (Figure 4-1).

- The Overview tab, shown in Figure 4-2, shows the status and parameters that are configured for the IES, Redundant Gateway, ring DHCP server, and the active ring supervisor.

You can also clear these faults:

- Partial gateway faults that can occur when traffic is lost in only one direction. The active ring supervisor detects a partial fault by monitoring the loss of beacon frames on a port.
- Rapid faults that can occur after five intentional disconnections and reconnections within 30 seconds of a node from the network. When the active ring supervisor detects either type of fault, it blocks traffic on the port, which results in network segmentation. To resolve this condition, you must manually clear the faults.
- The Faults tab shows the number, time, and location of faults in a ring as shown in Figure 4-3.
- The Members tab lists the MAC and IP addresses of each node in a ring as shown in Figure 4-4.

Figure 4-2 Device Manager—DLR Status Monitor Screen

Stratix 5400 Solution Device Manager - Switch

Dashboard Configure Monitor Admin

Ring1 Ring2 Ring3

Overview Faults Members

Switch DLR Status

Topology	Ring
Status	Normal
Mode	Active Supervisor
Redundant GW	Active Gateway
MAC Address	F4:54:33:16:BC:85
IP Address	10.208.105.10
Port 1	GigabitEthernet1/5, vlan 533, UP
Port 2	GigabitEthernet1/6, vlan 533, UP

Active Ring Supervisor

Supervisor MAC	F4:54:33:16:BC:85
Supervisor IP	10.208.105.10
Beacon Interval	400
Beacon Timeout	1960
Supervisor Precedence	200
VLAN ID	0

DHCP Server Status

Current Role	Backup
Status	Not in Active or Standby state.

Redundant Gateway

Status	Active Gateway
Advertise Interval	2000
Advertise Timeout	5000
GW Precedence	200
Learning Enabled	yes
Uplink Port(s)	GigabitEthernet1/1 GigabitEthernet1/2

Clear Partial Gateway Fault Clear Rapid Faults

Figure 4-3 Device Manager—DLR Fault Status Screen

Stratix 5400 Solution Device Manager - Switch

Dashboard Configure Monitor Admin

Ring1 Ring2 Ring3

Overview Faults Members

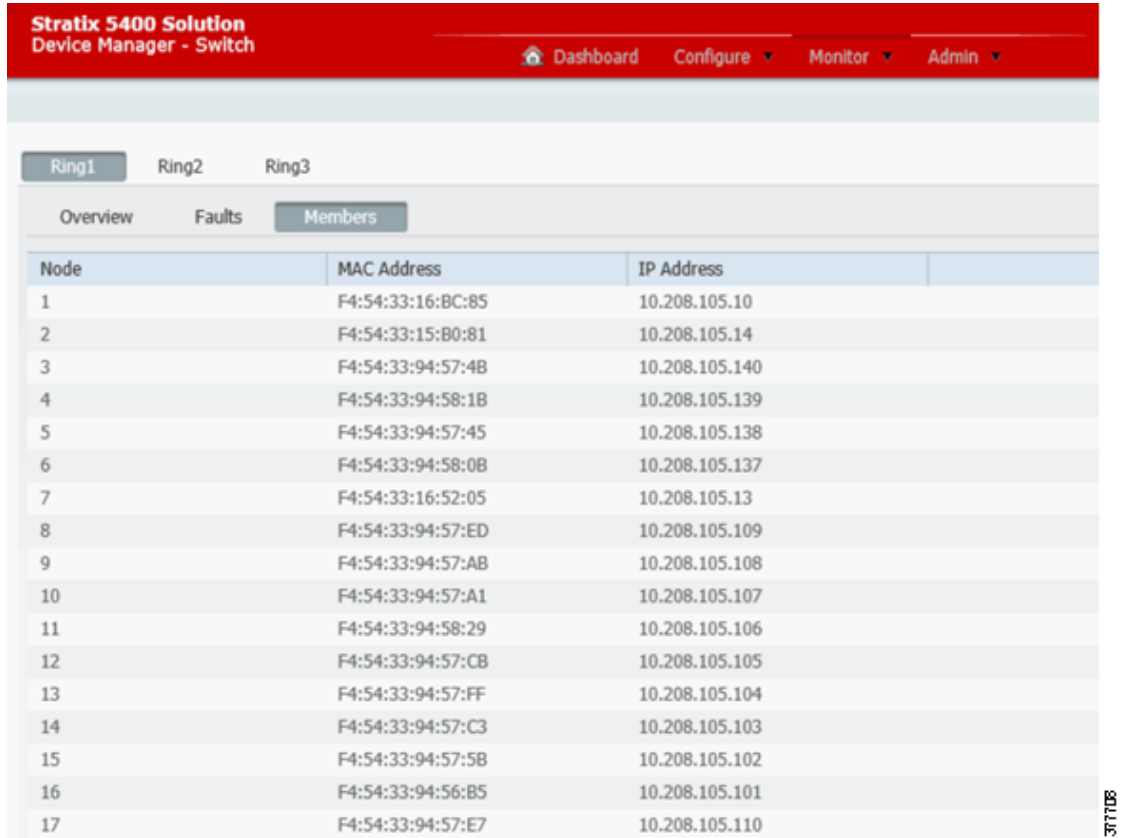
Ring Faults since power up 93

Time of Last Fault 15:05:08 EDT Wed Aug 3 2016

Clear Ring Faults

Ring Fault Location	MAC Address	IP Address
Last Active Node on Port 1	F4:54:33:5D:50:81	10.208.105.16
Last Active Node on Port 2	F4:54:33:16:BC:85	10.208.105.10

Figure 4-4 Device Manager—DLR Members Status Screen



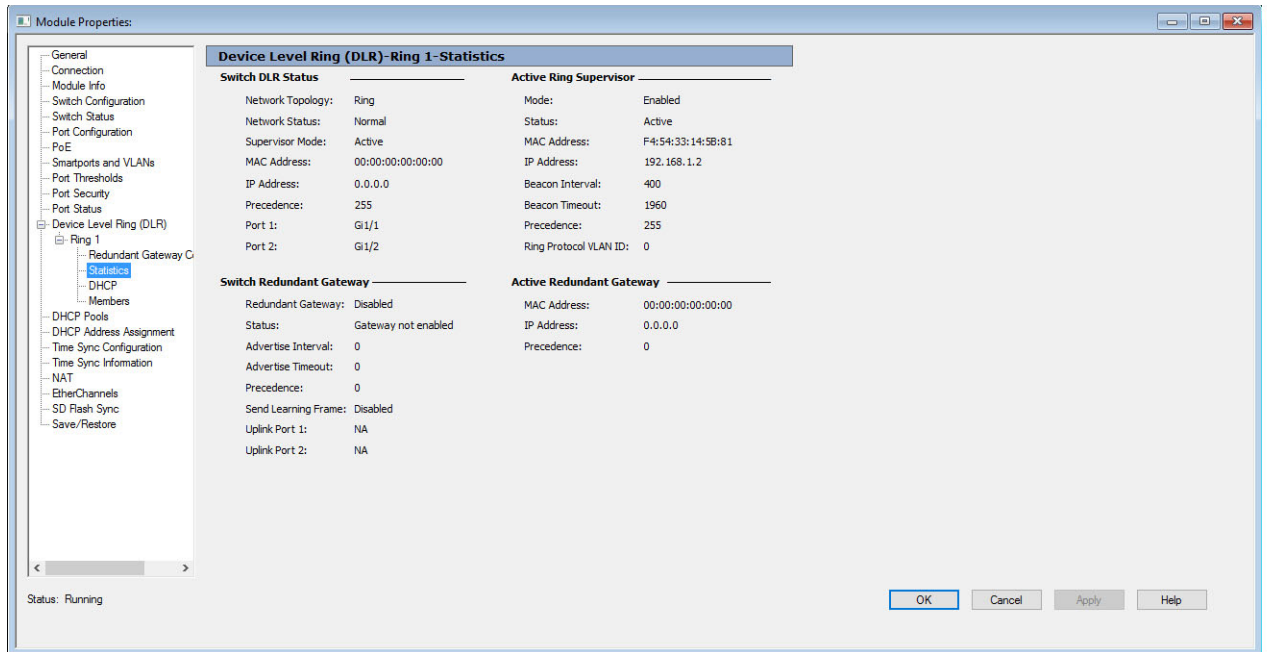
Node	MAC Address	IP Address
1	F4:54:33:16:BC:85	10.208.105.10
2	F4:54:33:15:B0:81	10.208.105.14
3	F4:54:33:94:57:4B	10.208.105.140
4	F4:54:33:94:58:1B	10.208.105.139
5	F4:54:33:94:57:45	10.208.105.138
6	F4:54:33:94:58:0B	10.208.105.137
7	F4:54:33:16:52:05	10.208.105.13
8	F4:54:33:94:57:ED	10.208.105.109
9	F4:54:33:94:57:AB	10.208.105.108
10	F4:54:33:94:57:A1	10.208.105.107
11	F4:54:33:94:58:29	10.208.105.106
12	F4:54:33:94:57:CB	10.208.105.105
13	F4:54:33:94:57:FF	10.208.105.104
14	F4:54:33:94:57:C3	10.208.105.103
15	F4:54:33:94:57:5B	10.208.105.102
16	F4:54:33:94:56:B5	10.208.105.101
17	F4:54:33:94:57:E7	10.208.105.110

Studio 5000 Logix Designer

From the navigation pane, expand Device Level Ring (DLR), expand Ring 1, Ring 2, or Ring 3, and then click one of the following:

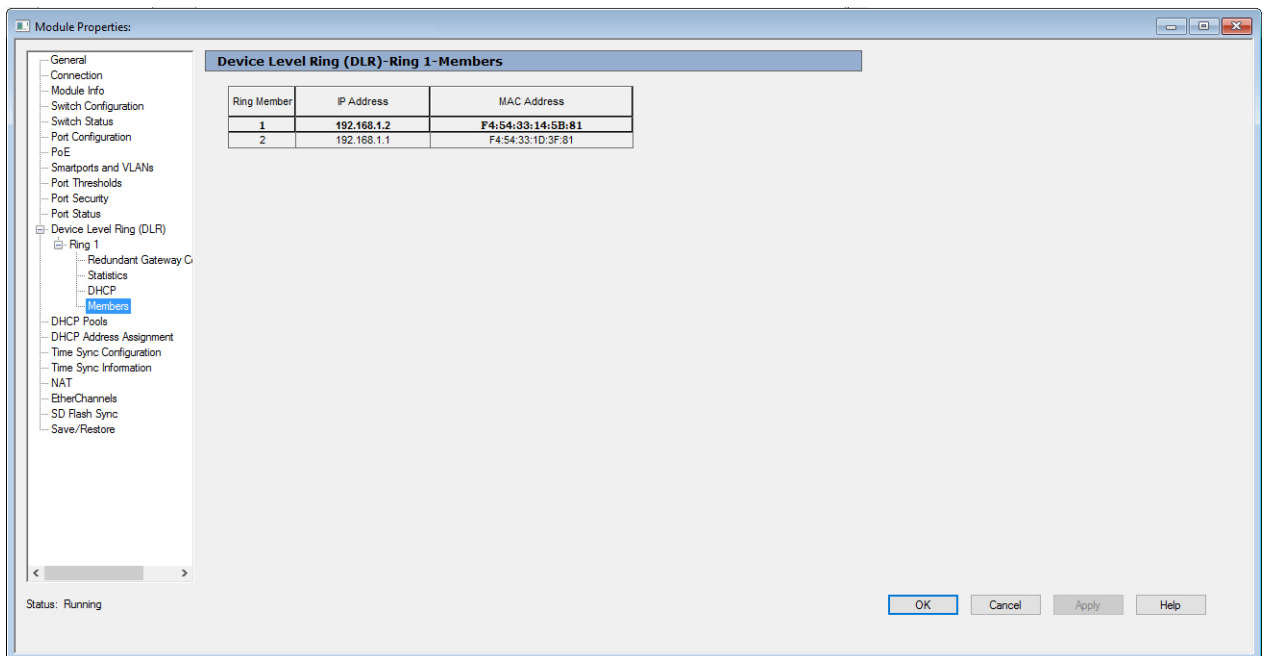
- To view the status and parameters that are configured for the IES, the Redundant Gateway, and the active ring supervisor, click **Statistics** as shown in [Figure 4-5](#).
- To view the MAC and IP addresses of each node in the ring, click **Members** as shown in [Figure 4-6](#).

Figure 4-5 Studio 5000 Logix Designer—Monitor DLR Ring Statistics



377709

Figure 4-6 Studio 5000 Logix Designer—Monitor DLR Ring Members



377710

Command Line Interface

Cisco and Rockwell Automation recommend that the following command be executed using the CLI on a DLR ring supervisor, either active or backup. DLR Supervisors are ring diagnostics aggregators and provide much fuller context around ring status. You can execute the command on any ring participant Stratix IES, though only limited ring status information will be displayed. An example of the output of the command is shown in [Figure 4-7](#) and detailed explanations of the diagnostics are shown in [Table 4-1](#).

To display specified DLR ring status information:

```
Switch# show DLR <ring ID>
```

For example:

```
Switch# show DLR Ring 1
```

Displays DLR ring status information for Ring 1.

The Stratix 5700, as a supervisor, is only capable of supporting a single DLR ring. For a Stratix 5700, the command will always be Ring 1.

Figure 4-7 Command Line Interface—Show DLR Ring 1 Output

```

Switch#sh dlr ring 1
DLR ring 1

mode: Active Supervisor
Network Topology: Ring      Network Status: Normal
IOS state: NORMAL_ACTIVE   Hardware State: NORMAL_ACTIVE
Mac-Addr: F4:54:33:11:71:01 IP-Addr: 10.17.30.19
Port1: GigabitEthernet1/1, vlan 30, UP    Port2: GigabitEthernet1/2, vlan 30, UP
LastBcnRcvPort: Port 1: Yes    Port 2: Yes|

Active Supervisor Parameters:
Beacon Interval (usec): 400      Beacon Timeout (usec): 1960
DLR VLAN ID: 0                  Precedence: 255
Mac-Addr: F4:54:33:11:71:01     IP-Addr: 10.17.30.19

Locally Configured Supervisor Parameters:
Beacon Interval (usec): 400      Beacon Timeout (usec): 1960
DLR VLAN ID: 0                  Precedence: 255
Port1: GigabitEthernet1/1       Port2: GigabitEthernet1/2

Supervisor DHCP Parameters:
DHCP Snooping: Enable
DHCP Server: Disable
ROLE: Backup -- (Inactive)
Number of Devices: 0
DHCP Entry Count: 0
DHCP Backup Interval: 60
DHCP Active cip address: 0.0.0.0

Ring Protocol Participants Count: 3
No      Mac-Addr      IP-Addr
1       F4:54:33:11:71:01  10.17.30.19
2       F4:54:33:11:5C:01  10.17.30.20
3       F4:54:33:17:6D:01  10.17.30.18

```

377711

Table 4-1 Show DLR Ring Output

Field	Description
General DLR Node Information (any ring participant)	<p>This field displays general DLR ring information for the DLR ring participant or supervisor to which the user is currently connected and on which the user is running the CLI.</p> <ul style="list-style-type: none"> • Network Topology: • IOS State: • Mac-Addr: MAC address of connected node • Port 1: Information and status for switchport assigned as DLR Port 1 • Port 2: Information and status for switchport assigned as DLR Port 2 • Network Status: • Hardware State: • IP-Addr: IP address of connected node • LastBcnRcvPort: Displays whether a valid supervisor beacon frame was received on ports 1 and 2
Active Supervisor Parameters (any ring participant)	<p>This field displays the configured parameters of the current active ring supervisor, regardless of whether or not the user is connected directly to the supervisor itself.</p> <ul style="list-style-type: none"> • Beacon Interval (usec): DLR Ring beacon interval (in microseconds) • Beacon Timeout (usec): DLR Ring beacon timeout (in microseconds) • DLR VLAN ID: The VLAN ID assigned to the ring • Precedence: The precedence value for the active ring supervisor • Mac-Addr: The MAC Address of the active ring supervisor • IP-Addr: The IP address of the active ring supervisor
Locally Configured Supervisor Parameters (ring supervisor only)	<p>This field is only available if the user is running CLI on a ring supervisor, whether active or backup. Ring parameters can be locally configured for all backup supervisors, but the ring itself is configured via the parameters of the active supervisor only.</p> <ul style="list-style-type: none"> • Beacon Interval (μsec): DLR Ring beacon interval (in microseconds) • Beacon Timeout (μsec): DLR Ring beacon timeout (in microseconds) • DLR VLAN ID: The VLAN ID assigned to the ring • Precedence: The precedence value for the connected ring supervisor • Port1: Information and status for the active supervisor switchport assigned as DLR Port 1 • Port2: Information and status for the active supervisor switchport assigned as DLR Port 2

Table 4-1 Show DLR Ring Output (continued)

Field	Description												
Supervisor DHCP Parameters (ring supervisor only)	<p>This field displays the configured parameters for the ring supervisor/DHCP server.</p> <ul style="list-style-type: none"> DHCP Snooping: Status of Ring DHCP Snooping DHCP Server: Status of Ring DHCP Server ROLE: Role of DHCP Server to which the user is connected Number of Devices: Number of devices to which the server has leased IP addresses DHCP Entry Count: Number of IP Addresses assigned to the server's DHCP table DHCP Backup Interval: 												
Fault Statistics	<p>This field displays fault statistics for the ring.</p> <ul style="list-style-type: none"> Ring Faults since power up: Number of ring faults recorded since the active supervisor was last powered up Ring Fault Location: The MAC and IP addresses of the last active nodes on each of the supervisor's ring ports. This information is very useful when determining the location of a ring fault. <p>The following example shows ring fault information for a fault that occurred between two IES with IP addresses 192.168.1.2 and 192.168.1.3:</p> <table> <tr> <td>Ring Fault Location</td><td>Mac-Addr</td></tr> <tr> <td>IP-Addr</td><td></td></tr> <tr> <td>Last Active Node on Port 1</td><td>00:14:00:00:00:00</td></tr> <tr> <td>192.168.1.2</td><td></td></tr> <tr> <td>Last Active Node on Port 1</td><td>00:15:00:00:00:00</td></tr> <tr> <td>192.168.1.3</td><td></td></tr> </table>	Ring Fault Location	Mac-Addr	IP-Addr		Last Active Node on Port 1	00:14:00:00:00:00	192.168.1.2		Last Active Node on Port 1	00:15:00:00:00:00	192.168.1.3	
Ring Fault Location	Mac-Addr												
IP-Addr													
Last Active Node on Port 1	00:14:00:00:00:00												
192.168.1.2													
Last Active Node on Port 1	00:15:00:00:00:00												
192.168.1.3													
Redundant Gateway Information (ring gateways only)	<p>This field displays the status and information related to the Redundant Gateway to which the user is currently connected.</p> <ul style="list-style-type: none"> Redundant Gateway Status: Current status of the connected gateway Hardware State: Mac-Addr: The MAC Address of the connected gateway IP_addr: The IP address of the connected gateway Uplink Port(s): The port(s) assigned as the currently connected gateway's uplink to the external network architecture 												
Active Gateway Parameters	<p>This field displays the status and information related to the active Redundant Gateway, regardless of whether the user is directly connected to it.</p> <ul style="list-style-type: none"> Advertise Interval (usec): The advertise interval of the active gateway. This is configurable on the active gateway itself and designates the interval, in microseconds, between gateway status advertise frames. Advertise Timeout (usec): The amount of time, in microseconds, the active gateway will wait while not receiving gateway advertise beacons before updating the Redundant Gateway status. Precedence: The configured precedence value for the active gateway Learning Update Enable: Mac-Addr: The MAC address of the active gateway IP-Addr: The IP address of the active gateway 												

Table 4-1 Show DLR Ring Output (continued)

Field	Description
Fault Statistics (ring gateways only)	<p>This field displays general statistics about faults in the Redundant Gateway network.</p> <ul style="list-style-type: none"> Gateway Faults since power up: The number of Redundant Gateway faults, either on the gateway or the link to the external network, since the IES was last powered up Time of last fault: The time (UTC) and date of the last Redundant Gateway fault
Locally Configured Gateway Parameters (ring gateways only)	<p>This field displays the configured parameters of the gateway to which the user is connected, which may not necessarily be the active gateway. Regardless of the locally configured gateway parameters, the Redundant Gateway parameters are set by the active gateway only. Upon a gateway switchover, the parameters will be set to the new active gateway.</p> <ul style="list-style-type: none"> Advertise Interval (μsec): The advertise interval of the connected gateway. This is configurable on the gateway itself and designates the interval, in microseconds, between gateway status advertise frames. Advertise Timeout (μsec): The amount of time, in microseconds, the connected gateway will wait while not receiving gateway advertise beacons before updating the Redundant Gateway status. Precedence: The configured precedence value for the connected gateway

Rockwell Automation DLR Faceplates



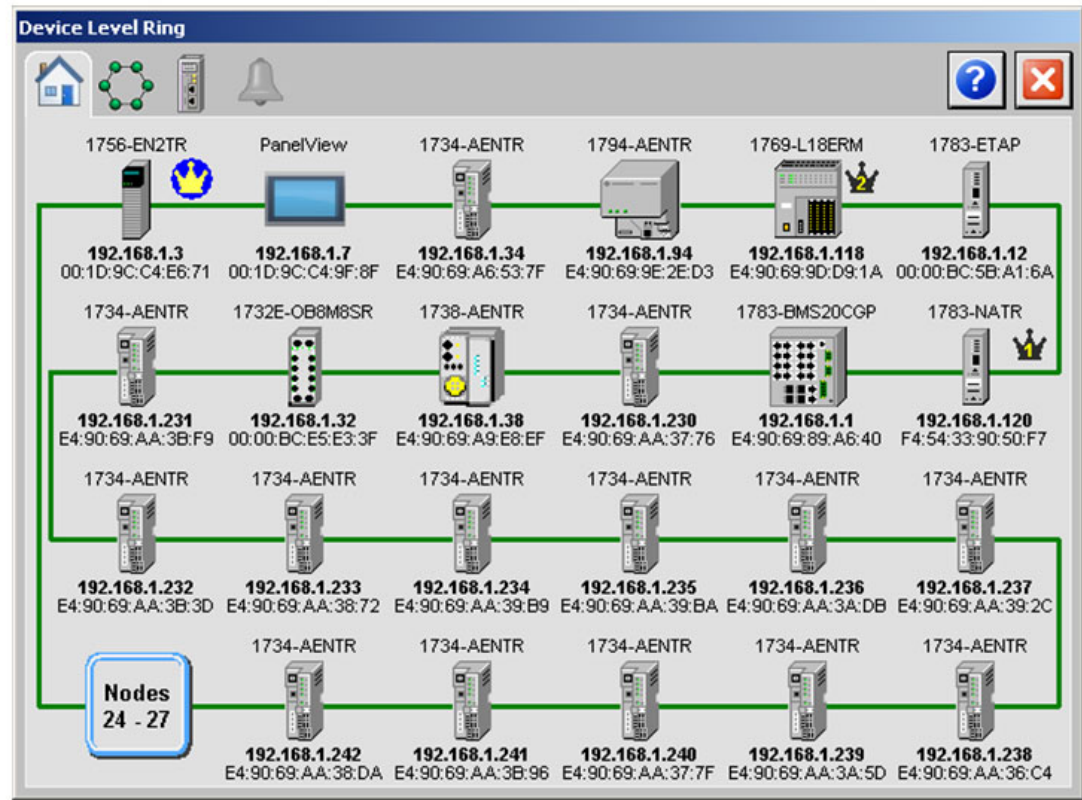
Note

This section only introduces the Rockwell Automation DLR Faceplates. For further information regarding configuring and interpreting the DLR Faceplate AOI and associated FactoryTalk View graphics, refer to the Device Level Ring Diagnostic Faceplate Implementation and Configuration Instructions manual, available with the DLR Faceplate download package found in the Rockwell Automation Sample Code Library.

EtherNet/IP Device Level Ring Networks Diagnostics Faceplate

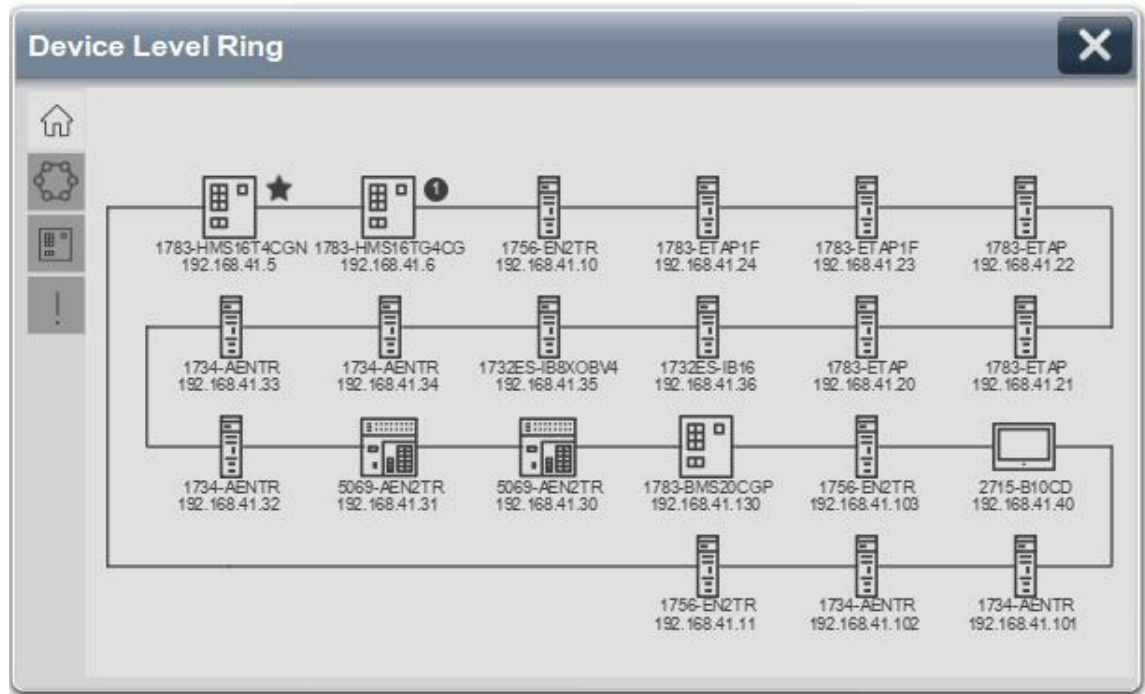
The Rockwell Automation DLR Faceplate provides a visualization of a configured DLR Ring including the status of all participants, active supervisor status, and overall ring health. [Figure 4-8](#) and [Figure 4-9](#) illustrate diagnostics and troubleshooting capabilities that can be made available on the plant floor on an HMI because it is implemented within Studio 5000 Logix Designer as an Add-On Instruction.

Figure 4-8 Rockwell Automation DLR Faceplate—Home Screen



377714

Figure 4-9 Rockwell Automation DLR Faceplate—Studio 5000 View Designer



Selecting the ring tab will display the following details:

- Detailed information about the DLR network
- Current Ring Supervisor Information
- DLR Supervisor Capabilities
- Detailed mode information for each network node
- Device Information
- Device DLR Capabilities
- Device Supervisor Capabilities

Selecting the alarm tab will show the ring and fault count for the DLR Ring. Network faults are indicated by a Network Alert notification, with the fault location shown as a red line segment on the ring image.

FactoryTalk Network Manager



Note

This section only introduces the FactoryTalk Network Manager. For further information regarding the installation and configuring of FactoryTalk Network Manager refer to FactoryTalk Network Manager Quick Start Guide publication:

https://literature.rockwellautomation.com/idc/groups/literature/documents/qs/fnm-qs001_-en-c.pdf

Topology View

FactoryTalk Network Manager is a server application and can be accessed by any client machine that can connect to the host system via a web browser. FactoryTalk Network Manager allows for network discovery of IACS and network devices and provides a visual representation of the network through discovering a network topology. This helps assist with monitoring and troubleshooting networks. Manually created network diagrams are often not up to date, inaccurate or not available. FactoryTalk Network Manager allows you to see the actual connectivity information with inventory and diagnostic data overlaid on top of the network topology. Figure 4-10 and Figure 4-11 illustrate the capabilities of the network topology view by showing two different Reference Architecture topologies.

Figure 4-10 FactoryTalk Network Manager—DLR Reference Architecture Switch-Level DLR Ring

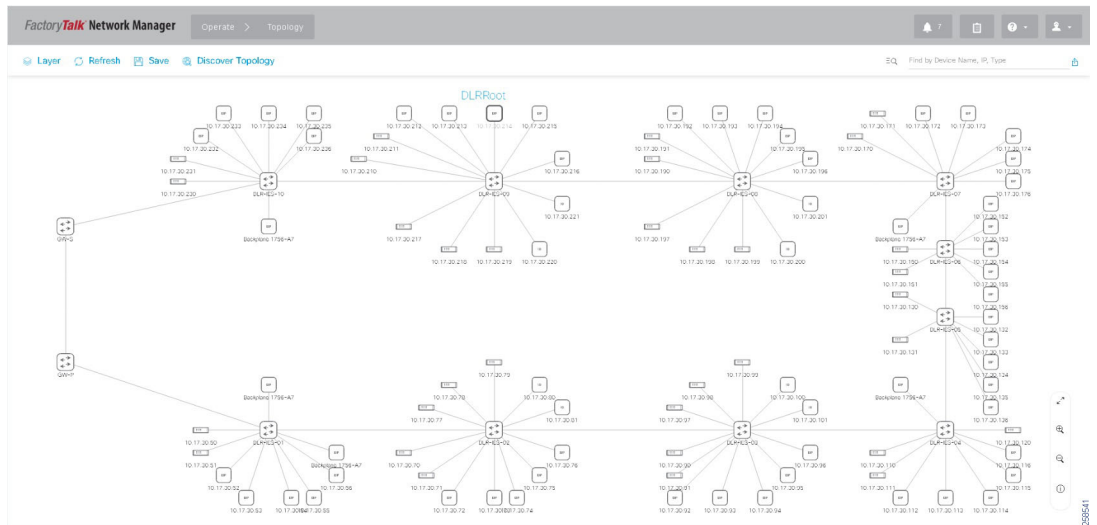
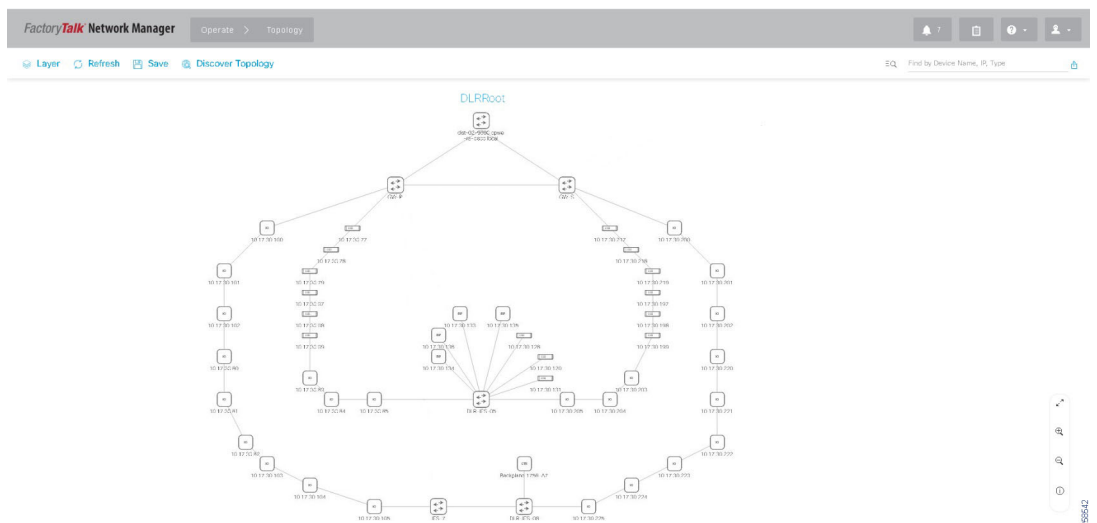


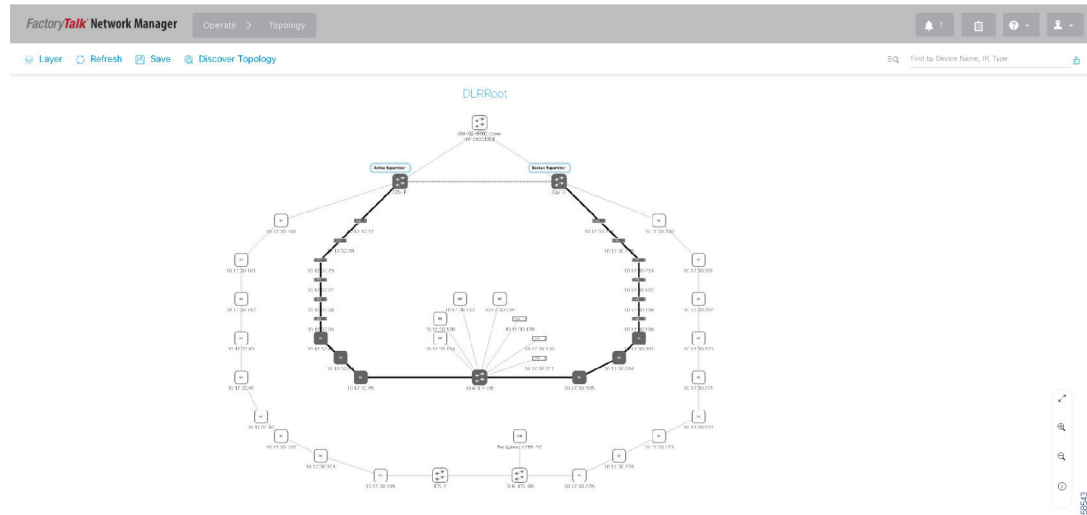
Figure 4-11 FactoryTalk Network Manager—DLR Reference Architecture Multiple Mixed Devices/Switch Level DLR Ring



Topology Overlays

FactoryTalk Network Manager can provide different overlay views for the topology to make monitoring and troubleshooting easier. The DLR overlay view illustrates the DLR information, including the number of discovered rings, active and backup DLR supervisor and DLR gateway devices in each ring. [Figure 4-12](#) illustrates the DLR Overlay by highlighting the selected ring to display the active and backup DLR supervisor and network nodes that make up the ring participants.

Figure 4-12 FactoryTalk Network Manager—DLR Overlay



DLR Monitoring and Troubleshooting with FactoryTalk Network Manager

FactoryTalk Network Manager provides a single network management view for the DLR network and can help to correlate alarms and events from multiple devices. This reduces time and effort spent troubleshooting the problem and prevent production outages. [Figure 4-13](#) illustrates how the network topology view depicts that a network fault has occurred on a DLR ring and provides a visual representation of what devices have alarms. In this instance the DLR supervisor has a critical alarm stating there is a ring fault as noted by selecting the DLR supervisor device from the network topology view. The DLR supervisor device properties will appear on the right side of the topology view and will provide the DLR information for troubleshooting.

Figure 4-13 FactoryTalk Network Manager—DLR Topology Ring Fault

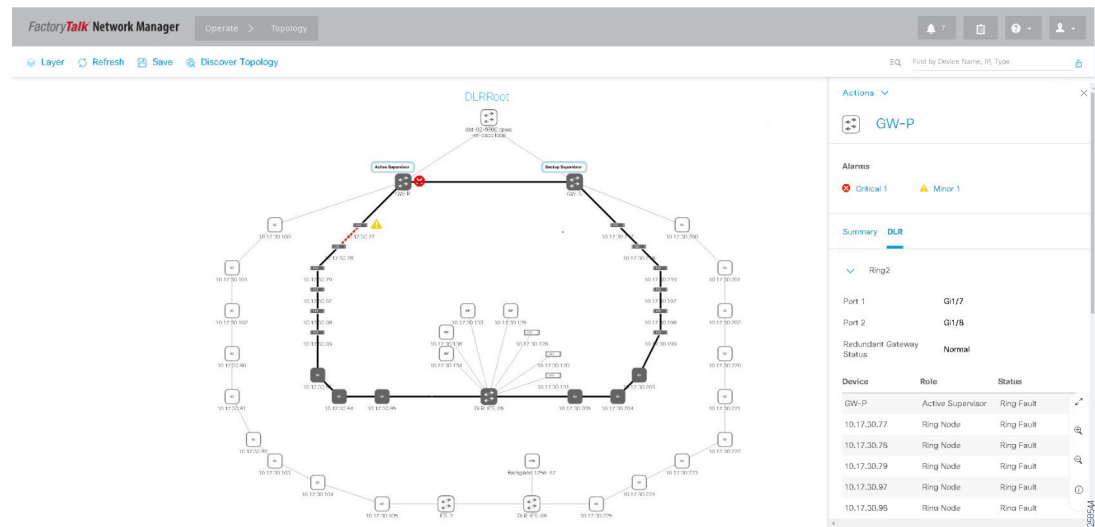


Figure 4-14 illustrates the DLR supervisor device overview as another way to assist in monitoring and troubleshooting the device health. FactoryTalk Network Manager collects important DLR statistics and diagnostic data from the DLR supervisor managed switch in a user friendly format. This assists in detecting and resolving issues faster.

Figure 4-14 FactoryTalk Network Manager—DLR Device Alarm

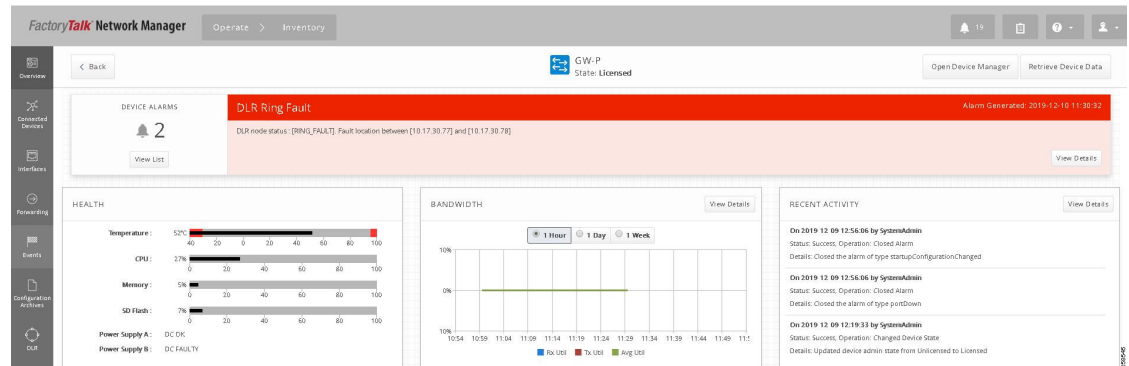


Figure 4-15 illustrates the Alarms Details page that provides a critical alarm has occurred on the DLR supervisor and states that a ring fault has occurred between ring participants 10.17.30.77 and 10.177.30.78. FactoryTalk Network Manager real-time alarming and event notifications can reduce time and effort troubleshooting the problem and may help to prevent production outages.

Figure 4-15 FactoryTalk Network Manager—Alarms

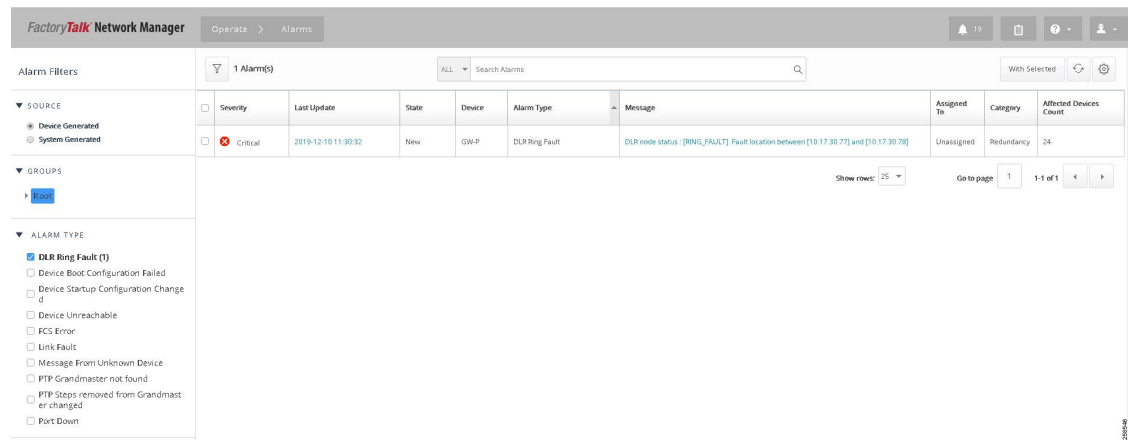
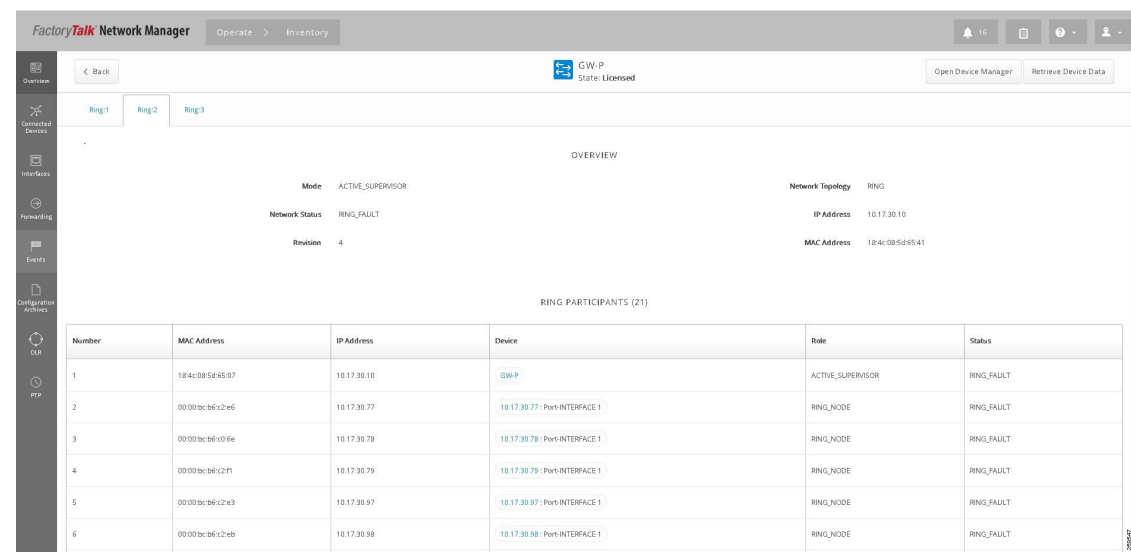


Figure 4-16 illustrates the DLR tab which provides an overview of the DLR supervisor capabilities which include a list of the DLR Participants with following information:

- Node Number
- MAC Address
- IP Address
- Device
- Role
- Status

Figure 4-16 FactoryTalk Network Manager—Device DLR Overview



DLR Port Choices for Stratix Switches

From the Allen-Bradley Managed Switches User Manual, 1783-UM007
(http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf).

Table A-1 DLR Ports for Stratix 5400 IES

IES	Ring 1		Ring 2		Ring 3	
	Port 1	Port 2	Port 1	Port 2	Port 1	Port 2
1783-HMS4C4CGN	1, 5	2, 6	3, 7	4, 8	7	8
1783-HMS8T4CGN	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS8S4CGN	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS4T4E4CGN	1, 9	2, 10	3, 11	4, 12	7	8
1783-HMS16T4CGN	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS4S8E4CGN	1, 5, 9	2, 6, 10	3, 7, 11	4, 8, 12	1, 7, 13	2, 8, 14
1783-HMS8TG4CGN	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS8TG4CGR						
1783-HMS8SG4CGN	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS8SG4CGR						
1783-HMS4EG8CGN	1, 5, 9	2, 6, 10	3, 7, 11	4, 8, 12	1, 7, 13	2, 8, 14
1783-HMS4EG8CGR						
1783-HMS16TG4CGN	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS16TG4CGR						
1783-HMS8TG8EG4CGN	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS8TG8EG4CGR						
1783-HMS4SG8EG4CGN	1, 5, 9	2, 6, 10	3, 7, 11	4, 8, 12	1, 7, 13	2, 8, 14
1783-HMS4SG8EG4CGR						

Table A-2 DLR Ports for Stratix 5700 IES

IES	Stratix 5700 DLR-Capable Ports					
1783-BMS10CGP	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2		
1783-BMS10CGN	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2		
1783-BMS12T4E2CGL	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2		
1783-BMS12T4E2CGP	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2		
1783-BMS12T4E2CGNK	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2		
1783-BMS20CL	Fa 1/15	Fa 1/16	Fa 1/17	Fa 1/18	Fa 1/19	Fa 1/20
1783-BMS20CA	Fa 1/15	Fa 1/16	Fa 1/17	Fa 1/18	Fa 1/19	Fa 1/20
1783-BMS20CGL	Fa 1/15	Fa 1/16	Fa 1/17	Fa 1/18	Gi 1/1	Gi 1/2
1783-BMS20CGP	Fa 1/15	Fa 1/16	Fa 1/17	Fa 1/18	Gi 1/1	Gi 1/2
1783-BMS20CGN	Fa 1/15	Fa 1/16	Fa 1/17	Fa 1/18	Gi 1/1	Gi 1/2
1783-BMS20CGPK	Fa 1/15	Fa 1/16	Fa 1/17	Fa 1/18	Gi 1/1	Gi 1/2
1783-ZMS4T4E2TGP	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2		
1783-ZMS8T8E2TGP	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2		
1783-ZMS4T4E2TGN	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2		
1783-ZMS8E82TGN	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2		

References

This appendix includes the following major topics:

- [Converged Plantwide Ethernet \(CPwE\)](#), page B-1
- [Other References](#), page B-3

Converged Plantwide Ethernet (CPwE)

- Design Zone for Manufacturing—Converged Plantwide Ethernet
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Industrial Network Architectures—Converged Plantwide Ethernet
<http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page>
- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/CPwE/CPwE-CVD-Sept-2011.pdf>
- Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html

- Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/4-0/Resiliency/DIG/CPwE_resil_CVD.html
- Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
 - Cisco site:
http://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 Industrial Demilitarized Zone Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html
- Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html>
- OEM Networking within a Converged Plantwide Ethernet Architecture Design Guide:
 - Rockwell Automation site:
http://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 Industrial Data Center within a Converged Plantwide Ethernet Architecture Design Guide:
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td014_-en-p.pdf
 - Cisco site:
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.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 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 Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture:
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td021_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/PRP/DIG/CPwE-5-1-PRP-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

Other References

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

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
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
FTNM	FactoryTalk Network Manager
FPGA	Field-Programmable Gate Array
FQDN	Fully Qualified Domain Name
FVRF	Front-door Virtual Route Forwarding
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)
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
LBS	Location Based Services

Table C-1 Acronyms and Initialisms (continued)

Term	Description
LWAP	Lightweight Access Point
MAB	MAC Authentication Bypass
MAC	Media Access Control
MDM	Mobile Device Management
ME	FactoryTalk View Machine Edition
mGRE	Multipoint Generic Routing Encapsulation
MLS	Multilayer Switching QoS
MMC	Microsoft Management Console
MnT	Monitoring Node
MPLS	Multiprotocol Label Switching
MQC	Modular QoS CLI
MSE	Mobile Service Engine
MSS	Maximum Segment Size
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDES	Network Device Enrollment Service
NHRP	Next Hop Routing Protocol
NMT	Network Monitoring Tool
NOC	Network Operation Center
NPS	Microsoft Network Policy Server
NSP	Native Supplicant Profile
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
ODVA	Open DeviceNet Vendors Association
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
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
REP	Resilient Ethernet Protocol
RPI	Request Packet Interval
RTT	Round Trip Time
SA	Security Association
SaaS	Software-as-a-Service
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
SV	Stackwise Virtual
SYN	Synchronization
TCN	Topology Change Notification
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
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

About the Cisco Validated Design (CVD) Program

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

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

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

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

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

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

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

www.panduit.com

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

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

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

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

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

www.cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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

www.rockwellautomation.com

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

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

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

Allen-Bradley, ArmorStratix, Compact 5000, CompactLogix, ControlLogix, Integrated Architecture, FactoryTalk, FactoryTalk Network Manager, Flex 5000, GuardLogix, POINT I/O, Rockwell Automation, Stratix and Studio 5000 Logix Designer are trademarks of Rockwell Automation, Inc.
Trademarks not belonging to Rockwell Automation are property of their respective companies.

CIP, CIP Motion, CIP Safety, CIP Sync, ControlNet and EtherNet/IP are trademarks of the ODVA, Inc.