Application Technique

Original Instructions

Allen-Bradley
by ROCKWELL AUTOMATION

EtherNet/IP Device Level Ring

Rockwell Automation

Summary of Changes

This publication contains the following new or updated information. This list includes substantive updates only and is not intended to reflect all changes.

Topic	Page
Added support for Stratix® 5800 switches	throughout
Moved content about installing devices and completing physical connections to Chapter 1: Device Level Networks	7
Moved content about types of rings to new Chapter 2: Typical Implementations	17
Moved content about Stratix features into new Chapter 3: DLR Features for Stratix Switches	21
Revised Redundant Gateway Traffic Flow section	23
Revised Uplink to Other Resiliency Technologies section	41
Added Chapter 3: Stratix Switch Configuration Examples	47
Updated DLR Faceplate section in Chapter 5: DLR Network Monitoring	92
Updated Table 13: MSG Instruction Configuration Values	94

About This Publication

This publication describes DLR network operation, topologies, configuration considerations, and diagnostic methods.

Download Firmware, AOP, EDS, and Other Files

Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc.

Notes:

Device Level Ring Networks

Device Level Ring (DLR) is an EtherNet/IP™ protocol that is defined by ODVA. DLR provides a means to detect, manage, and recover from single faults in a ring-based network.

A DLR network includes the following types of ring nodes.

Node	Description
Ring supervisor	A ring supervisor provides these functions: • Manages traffic on the DLR network • Collects diagnostic information for the network A DLR network requires at least one node to be configured as ring supervisor. By default, the supervisor function is disabled on supervisor-capable devices.
Ring participants	Ring participants provide these functions: • Process data that is transmitted over the network. • Pass on the data to the next node on the network. • Report fault locations to the active ring supervisor. When a fault occurs on the DLR network, ring participants reconfigure themselves and relearn the network topology.
Redundant gateways (optional)	Redundant gateways are multiple switches that connect to a DLR network and also connect together through the rest of the network. Redundant gateways provide DLR network resiliency to the rest of the network.

Depending on their firmware capabilities, both devices and switches can operate as supervisors or ring participants on a DLR network. Only some DLR devices, such as switches, can operate as redundant gateways.

DLR Network Operation

During normal network operation, an active ring supervisor uses beacon and other DLR protocol frames to monitor the health of the network. The backup ring supervisor and other ring participants monitor the beacon frames to track transitions between normal and faulted connections in the ring.

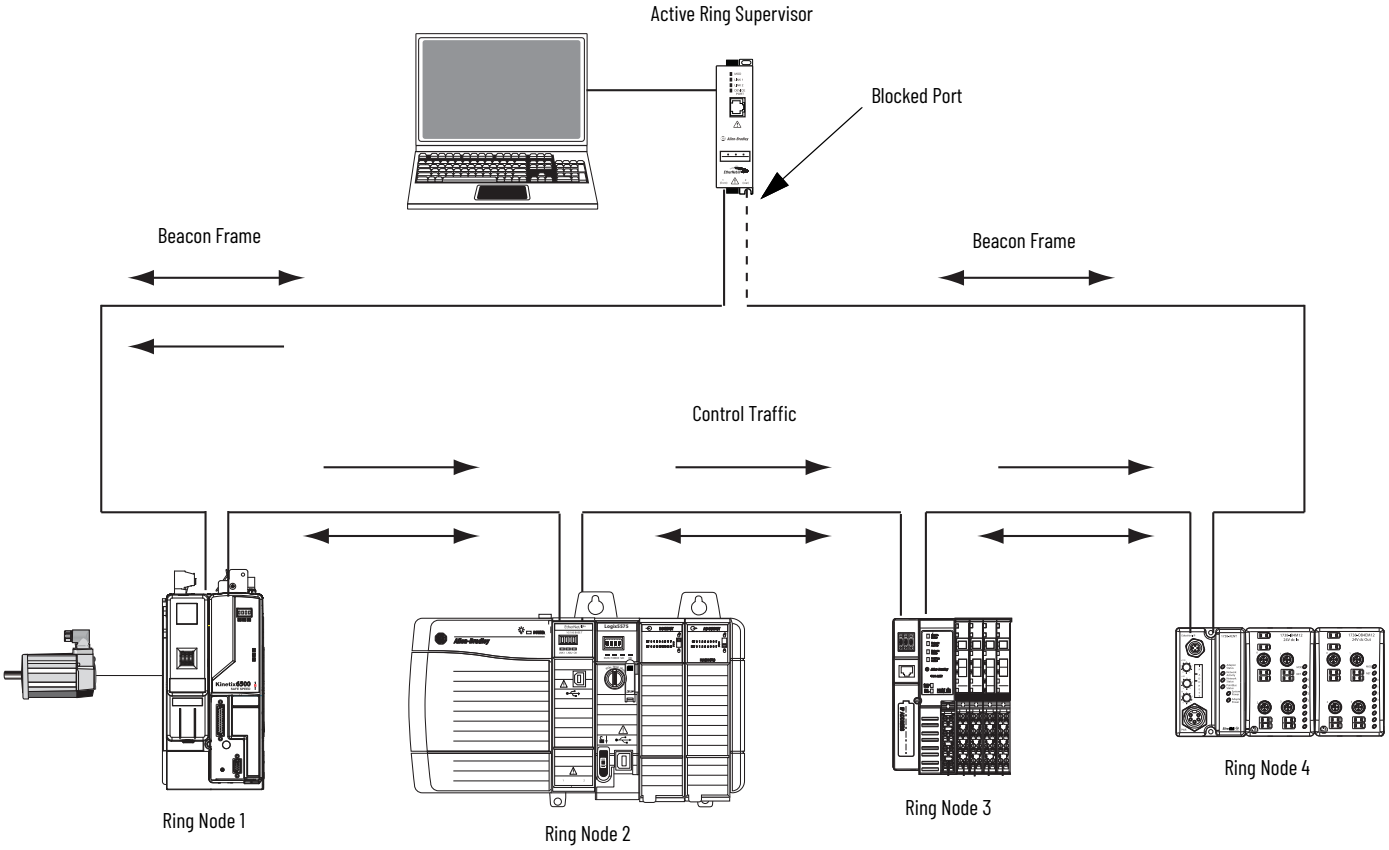
A DLR configuration includes the following beacon-related parameters:

- Beacon interval—The frequency the active ring supervisor uses when transmitting a beacon frame through both of its ring ports.
- Beacon timeout—The amount of time that supervisor or ring nodes wait for the reception of beacon frames before they time out and take an action.

These parameters impact network recovery performances. For information on recovery performance times, see Appendix A.

During normal operation, one of the network ports on the active supervisor is blocked for DLR protocol frames. However, both network ports continue to send beacon frames to monitor network health. Figure 1 shows the transmission of beacon frames from the active ring supervisor.

Figure 1 - Normal DLR Network Operation



While Allen-Bradley® products with DLR technology support beacon frames, there is another category of ring nodes that supports announce frames. The active supervisor sends announce frames out one of its ports once per second or upon detection of a ring fault. DLR networks with announce that frame nodes have slightly longer recovery times than beacon frame nodes.

Ring Supervisor

A DLR network requires at least one node to be configured as ring supervisor. The ring supervisor provides these functions:

- Manages network loops
- Determines active or backup status
- Verifies ring integrity
- Reconfigures the ring to recover from a network fault
- Performs ring diagnostics
- Provides IP addresses to ring nodes when configured as a DLR DHCP server

At any point in time, there is only one active supervisor on a DLR network:

- When multiple nodes are enabled as supervisor, the node with the numerically highest precedence value becomes the active ring supervisor. The other nodes automatically become backup supervisors.
- If multiple supervisors are configured with the same precedence value, the node with the numerically highest MAC address becomes the active supervisor.

A limited number of devices can operate as a DLR supervisor. For a complete list of supervisor-capable devices, see Knowledgebase article *Devices That Can Be a Supervisor on Device Level Ring (DLR)*.

IMPORTANT A ring that is configured without a supervisor constitutes an unmanaged network loop. This loop can result in unicast, multicast, or broadcast storms that cause disruptions to network communication. The ring supervisor maintains loop-free topologies by blocking on one of its two DLR ring ports. The supervisor only opens the port when a ring topology change is detected.

For an EtherNet/IP tap operating as a ring supervisor, follow these guidelines:

- Only configure an EtherNet/IP tap in your I/O configuration if you plan to enable the tap as a ring supervisor.
- If you do not plan to use an EtherNet/IP tap as a ring supervisor, we recommend that you do not add it to your I/O configuration.

If you plan to configure an EtherNet/IP tap as a ring supervisor via software, you must first assign it an IP address. An IP address is not required for an EtherNet/IP tap in a ring that is not a ring supervisor or that uses a DIP switch to enable its supervisor function.

Backup Supervisor

While a backup supervisor is not required on a DLR network, we recommend that you configure at least one backup ring supervisor for your ring network.

During normal operation, a backup supervisor operates as a ring participant. If the active supervisor node operation is interrupted, the backup supervisor with the next numerically highest precedence value becomes the active supervisor.

Ring Participants

A ring participant is a node that processes data that is transmitted over the network or passes on data to the next node on the network. When a fault occurs on the DLR network, ring participants reconfigure themselves and relearn the network topology. Ring participants also report fault locations to the active ring supervisor.

A limited number of devices can operate as ring participants. For a complete list of DLR-capable ring participants, see Knowledgebase article *List of Embedded Switch DLR Capable Devices*.

IMPORTANT Only connect DLR-capable devices directly to the ring network. Connect non-DLR devices to the ring network via a DLR-capable Stratix® switch or EtherNet/IP tap.

Advanced DLR Features

Some Stratix switches support the following advanced features.

- Redundant gateways
- Multiple rings
- DHCP for ring devices
- DLR VLAN trunking

For more information about implementing these features, see Chapter 3.

DLR Network Requirements and Restrictions

Know the requirements and restrictions for the following aspects of a DLR network:

- Number of ring nodes
- Switch ports
- Multicast groups
- Ring speed
- CIP Sync™ Time Synchronization/Precision Time Protocol (PTP)

Number of Ring Nodes

For all types of rings, we recommend that you limit a DLR network to 50 or fewer nodes. If your application requires more than 50 nodes, we recommend that you segment the nodes into separate DLR networks. For rings of only switches, we recommend that you use no more than 24 switches and 230 end devices.

IMPORTANT If you use more than 50 nodes in a DLR network, be sure to test your application before production.

Too many ring nodes can result in a higher probability of multiple faults, slower fault detection and recovery time, and decreased network performance.

Switch Ports

Only predesignated ports on a switch can connect to the DLR network. To determine valid DLR ports, refer to the user manual for the switch.

The following table lists required settings for DLR ports.

Port Parameter	Setting
Administrative mode	Access or Trunk mode
Smartport role	None, Multiport Automation Device, or Switch for Automation
Duplex	Full-duplex mode

Certain features are not supported on DLR ports. Unsupported features include, but are not limited to, the following. Do not configure these features on DLR-enabled ports:

- EtherChannel
- Network Address Translation (NAT)
- Resilient Ethernet Protocol (REP)
- Spanning Tree Protocol (STP)
- Parallel Redundancy Protocol (PRP)
- Flex Links
- 802.1x Security
- MAC ID-based port security

Non-DLR ports on the same switch still support these features.

Multicast Groups

Exceeding the multicast group threshold for a switch can result in the following network issues:

- Dropped traffic
- Poor port performance
- Poor error recovery
- Intermittent performance issues
- Poor handling of bursts in traffic

For multicast group limits, refer to the user manual for the switch.

Ring Speed

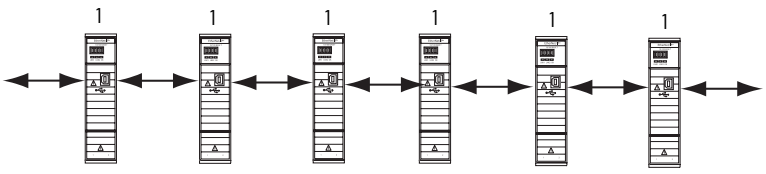
A ring must operate at **one speed**: either 100 Mbps or 1 Gbps. Ring nodes cannot communicate at different speeds within the same ring. A uniform ring speed is required to make sure each connection in a ring functions and to help prevent packet loss from buffer overruns.

A switch that supports multiple rings, such as a Stratix 5400 switch, can have each ring operate at different speeds. For example, Ring 1 can operate at 100 Mbps, Ring 2 can operate at 1 Gbps, and Ring 3 can operate at 100 Mbps.

To achieve a uniform ring speed, follow these configuration rules for ring nodes:

- If **all ring nodes** can operate at the same highest speed (100 Mbps or 1 Gbps), set all connected ports to auto-negotiate speed.

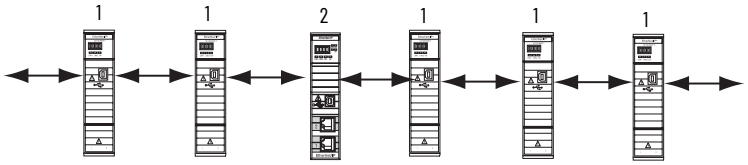
  For example, if all ring nodes are 1756-EN2TR devices, configure all connected ports to auto-negotiate.



Device		Capability	Port Speed Configuration
1	1756-EN2TR	100 Mbps	Auto-negotiate

- If **one ring node** can operate at a higher speed (1 Gbps) than the others, but adjacent ring nodes on both sides can only operate at 100 Mbps, set all connected ports to auto-negotiate speed. The 1 Gbps-capable device can negotiate to 100 Mbps and does not require you to fix its speed to 100 Mbps.

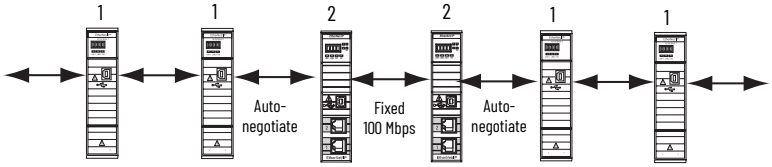
  For example, if you insert one 1756-EN4TR device into a ring of 1756-EN2TR devices, configure all connected ports to auto-negotiate.



Device		Capability	Port Speed Configuration
1	1756-EN2TR	100 Mbps	Auto-negotiate
2	1756-EN4TR	100 Mbps or 1 Gbps	Auto-negotiate

- If a **pair of adjacent ring nodes** can operate at a higher speed (1 Gbps) than others that can only operate at 100 Mbps, fix the port speed between the pair of 1 Gbps-capable devices to 100 Mbps to keep them from communicating at 1 Gbps with each other.

  For example, if two adjacent 1756-EN4TR ring nodes are redundant adapters in slots 0 and 1 of a ControlLogix® I/O chassis, and the ring contains devices running at 100 Mbps, then facing ports on both devices between the two 1756-EN4TR ring nodes must use a fixed speed of 100 Mbps.



Device		Capability	Port Speed Configuration
1	1756-EN2TR	100 Mbps	Auto-negotiate
2	1756-EN4TR	100 Mbps or 1 Gbps	The connection between the pair of 1756-EN4TR devices is fixed at 100 Mbps. The connection between each 1756-EN4TR and 1756-EN2TR device is set to auto-negotiate.

Unlike speed/duplex settings, auto-MDIX is not required on both ends of a connection. If one end device has auto-MDIX enabled, then a cross-over cable is not required.

CIP Sync Time Synchronization/Precision Time Protocol (PTP)

DLR networks support control applications that require the IEEE 1588 standard for Precision Time Protocol (PTP), also known as CIP Sync™ Time Synchronization. For example, DLR networks can be used with time-centric motion applications that include drives.

These PTP modes are supported on switches in a DLR network:

- Switches that are configured as redundant gateways must be configured for Boundary mode. In Boundary mode, the switch participates in selecting the best master clock.
- Other switches that are not configured as redundant gateways support both Boundary mode and End-to-End Transparent mode.

IMPORTANT Not all DLR-capable switches support the IEEE 1588 standard. To make sure that delays are compensated in a time-critical application in a ring, we recommend that you select a switch that supports the IEEE 1588 standard.

ControlLogix Redundancy System with DLR

You can use ControlLogix redundancy with DLR for network resiliency in a high availability system.

For more information about ControlLogix redundancy with DLR networks, see the following resources:

- High Availability Systems Reference Manual, publication HIGHAV-RM002
- Knowledgebase article *Using ControlLogix Redundancy 1756-EN2TR Modules as the DLR Supervisor*

- Knowledgebase article *DLR Active Supervisor IP Address Not Updated After Redundancy Switchover*

Fault Management

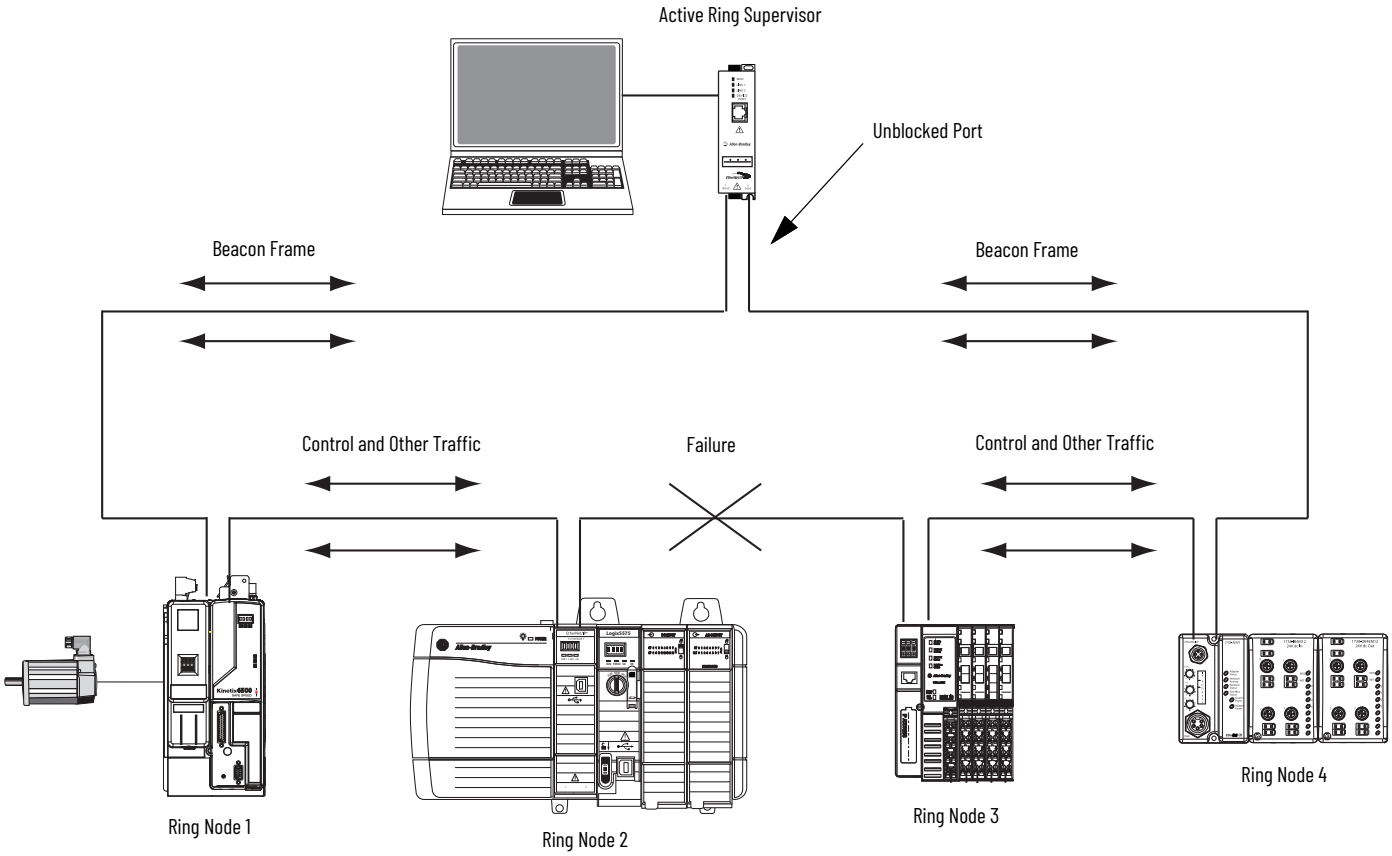
A DLR network can help protect your application from interruptions that are caused by a fault. To maintain the resiliency of a ring, configure your application so that it monitors the health of the ring itself. The ring can be faulted while all higher-level network functions, such as I/O connections, operate normally.

You can obtain fault location information from the active supervisor or the DLR faceplate, if installed. For more information on how to obtain fault location information, see Chapter 5, DLR Network Monitoring.

After a fault occurs, the active supervisor reconfigures the network to continue sending data on the network.

Figure 2 shows the network configuration after a failure occurs. The active ring supervisor passes traffic through both of its ports and maintains communication on the network.

Figure 2 - Network Reconfiguration After Fault



Media

DLR network connections can be copper, fiber, or a combination of both. To find specifications for EtherNet/IP taps, Stratix switches, and SFP modules, see the Stratix Ethernet Device Specifications Technical Data, 1783-TD002. To choose a cable type, use the following guidelines.

Cable Type	Data Rate	Device Compatibility
Singlemode fiber (SMF)	100 Mbps 1 Gbps	Stratix switches
Multimode fiber (MMF)	100 Mbps 1 Gbps	EtherNet/IP taps (100 Mbps only) Stratix switches
Copper	100 Mbps 1 Gbps	EtherNet/IP taps (100 Mbps only) EtherNet/IP devices (100/1 Gb) Stratix switches

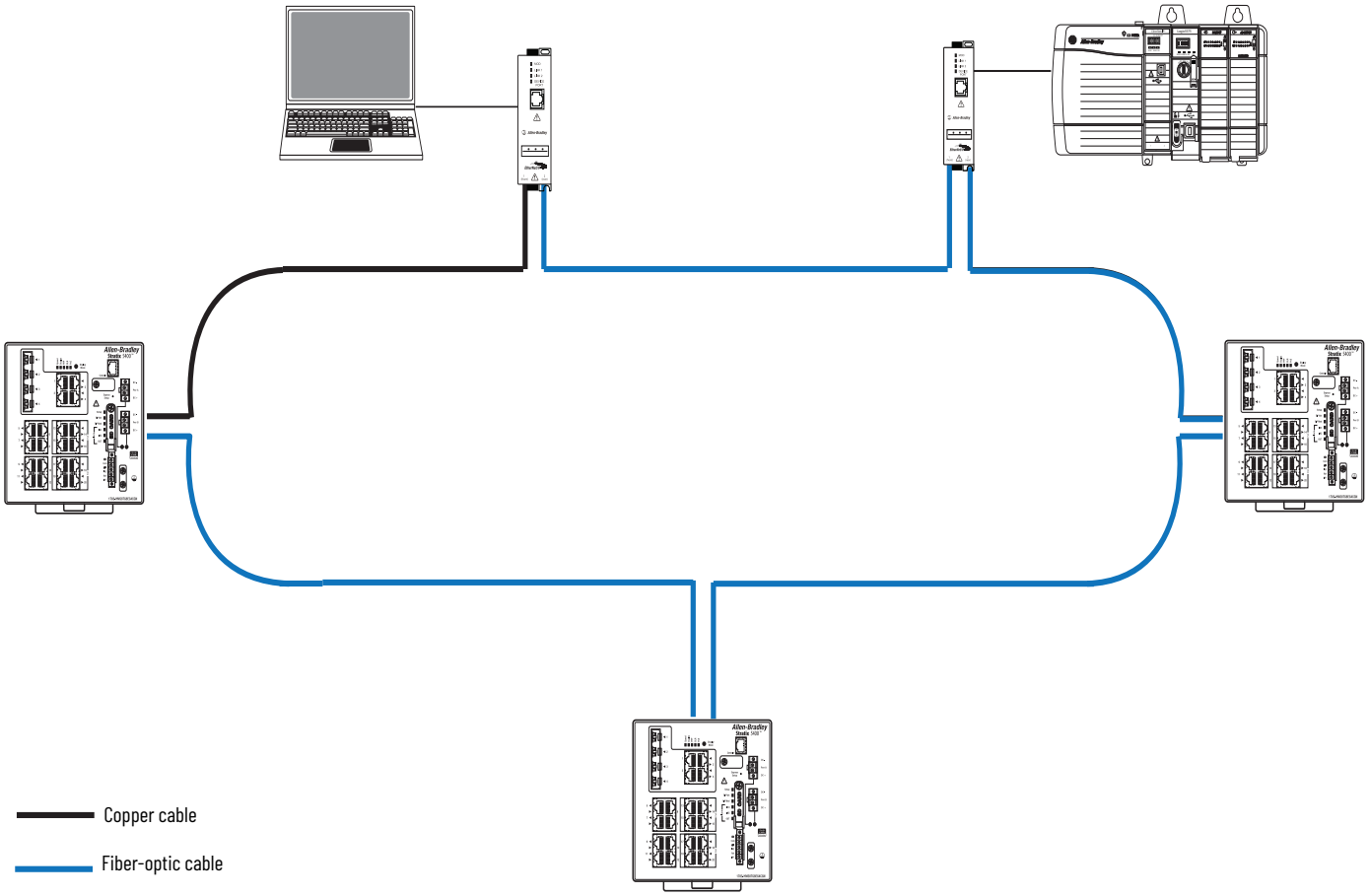
Figure 3 shows devices and switches in a DLR network with a mix of media.

Fiber-optic cable is used to connect these devices:

- EtherNet/IP tap to EtherNet/IP tap
- EtherNet/IP tap to Stratix switch
- Stratix switch to Stratix switch

Copper cable is used to connect the Stratix switch to the EtherNet/IP tap.

Figure 3 - Mixed Media in DLR Network



For more information about how to use fiber media to extend a DLR network across long distances, see the Physical Infrastructure for the Converged Plantwide Ethernet Architecture Application Guide, publication ENET-TD020.

Order of Configuration

To configure a DLR network, you must complete these steps in the following order:

1. Install and Configure Devices on a DLR Network.
2. Complete the Physical Connections of the Network on page 15.

Install and Configure Devices on a DLR Network

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

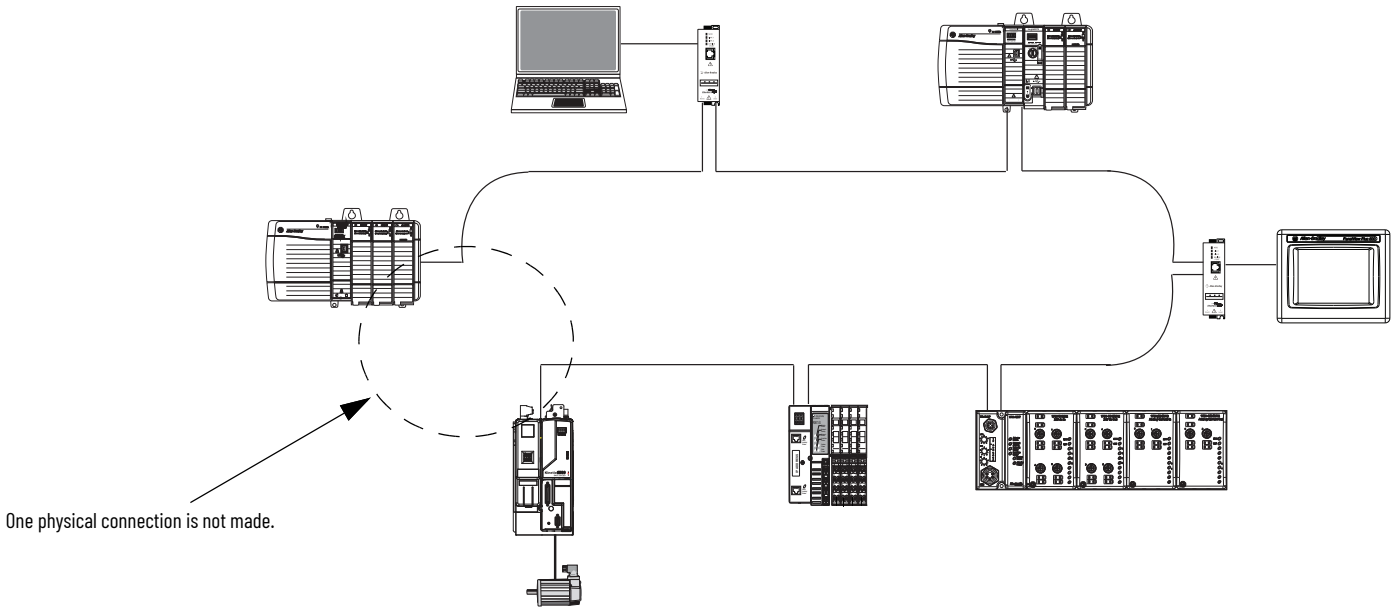
IMPORTANT Before you fully connect all ring nodes, you must do the following:

- Configure a ring supervisor
- Complete the DLR configuration of all switches in the ring

If you fully connect your DLR network without a supervisor configured, the network can experience a network storm. A network storm can render the network unusable until one link is disconnected and at least one supervisor is enabled.

IMPORTANT If your DLR network includes redundant gateways, you must complete the redundant gateway configuration before you connect the uplink ports to the outside network.

Figure 4 - DLR Network with One Link Disconnected



Use the installation instructions for each device to connect it to the network. You can view or download Rockwell Automation publications at http://www.rockwellautomation.com/literature/.

Complete the Physical Connections of the Network

After you configure a ring supervisor, you must complete the physical connection between all nodes to establish a complete and functioning DLR network.

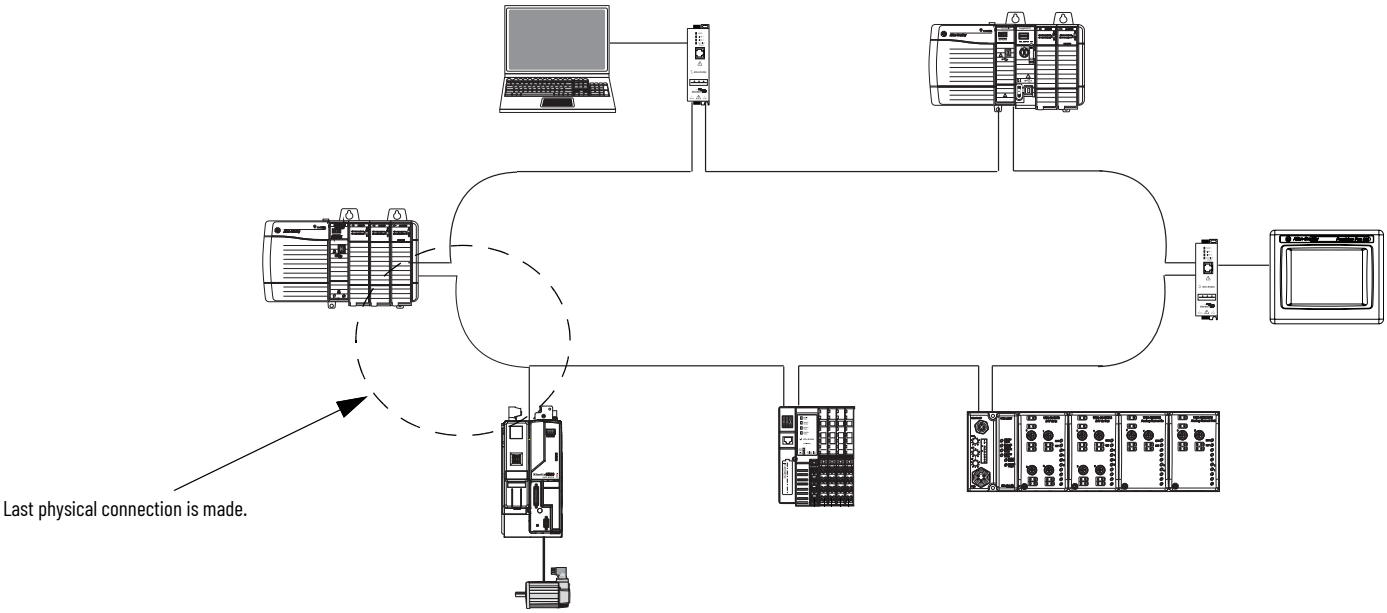
IMPORTANT If you fully connect your DLR network without a supervisor configured, a network storm can result. A network storm can render the network unusable until one link is disconnected and at least one supervisor is enabled.

IMPORTANT If your DLR network includes switches, you must complete the DLR configuration of all switches before you complete the physical connection between all nodes.

IMPORTANT If your DLR network includes redundant gateways, you must complete the redundant gateway configurations before you connect the uplink ports to the outside network.

The following figure shows an example DLR network with all physical connections complete.

Figure 5 - DLR Network with All Links Connected



Notes:

DLR Implementations

There are three typical implementations of a DLR network:

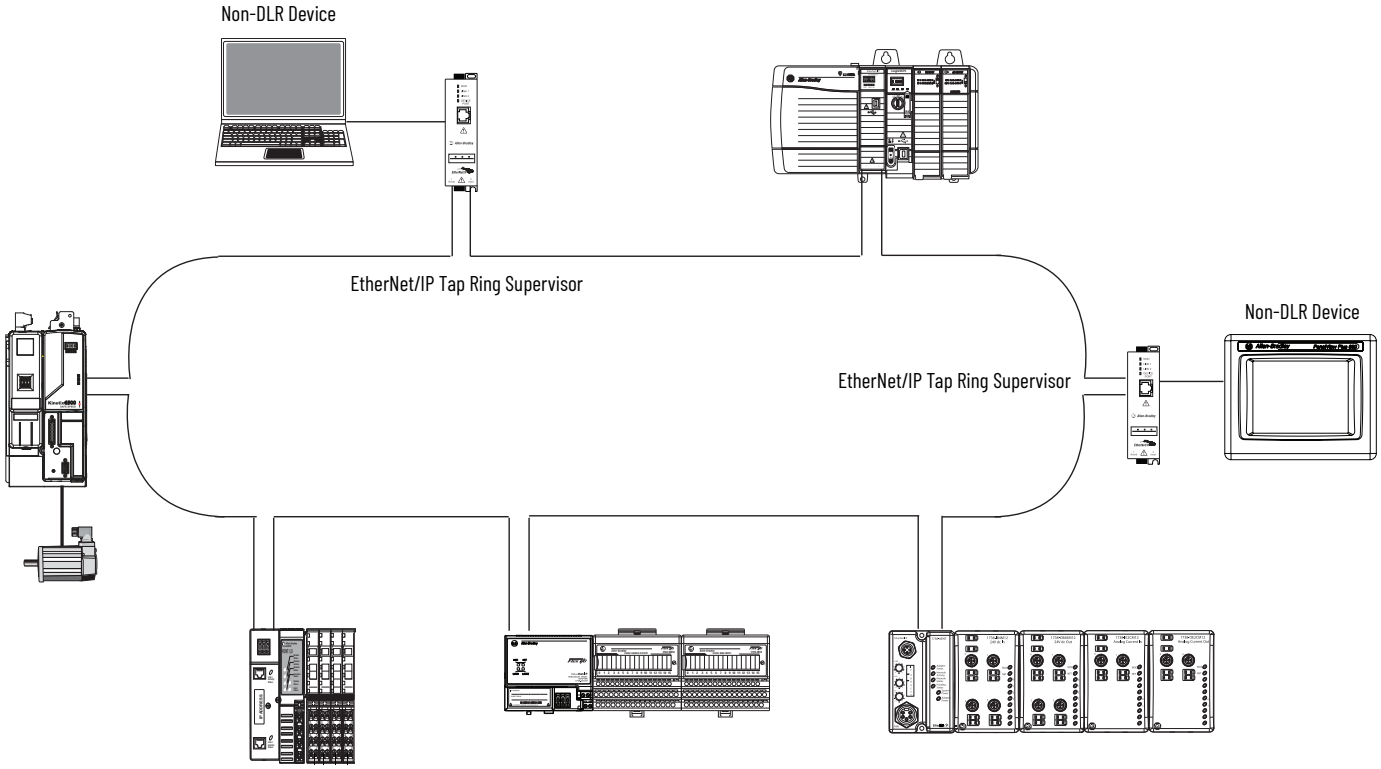
- Ring of Devices
- Ring of Devices and Switches
- Ring of Switches

Ring of Devices

A simplistic implementation of DLR is a ring of DLR-capable devices. In Figure 6, devices without DLR capability connect to the ring via EtherNet/IP taps. In this example, EtherNet/IP taps are configured as ring supervisors.

For configuration examples, see Chapter 4 on page 47.

Figure 6 - Ring of Devices



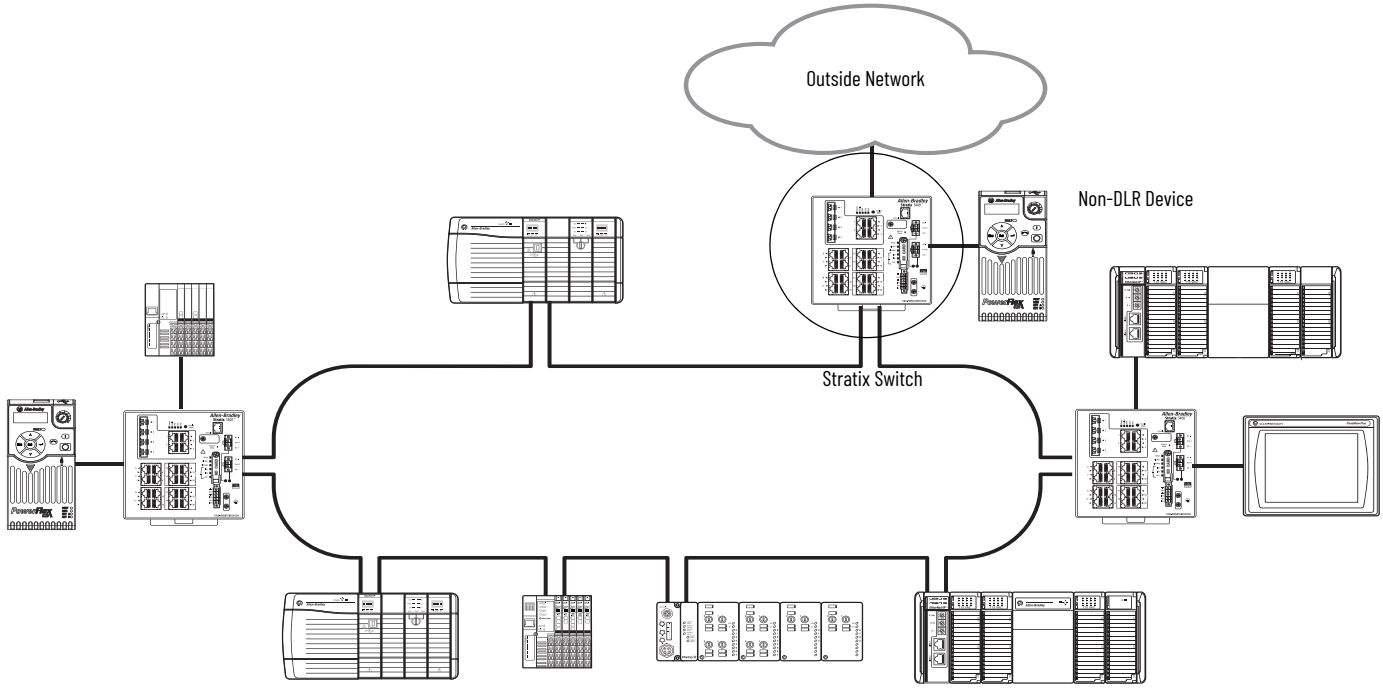
Ring of Devices and Switches

Figure 7 shows a ring of both DLR-capable devices and switches:

- If configured as a ring supervisor, a Stratix® switch provides consolidated status and diagnostics for the DLR network.
- A Stratix switch connects the ring to the outside network and also connects a non-DLR device to the ring.

For configuration examples, see Chapter 4 on page 47.

Figure 7 - Ring of Devices and Switches



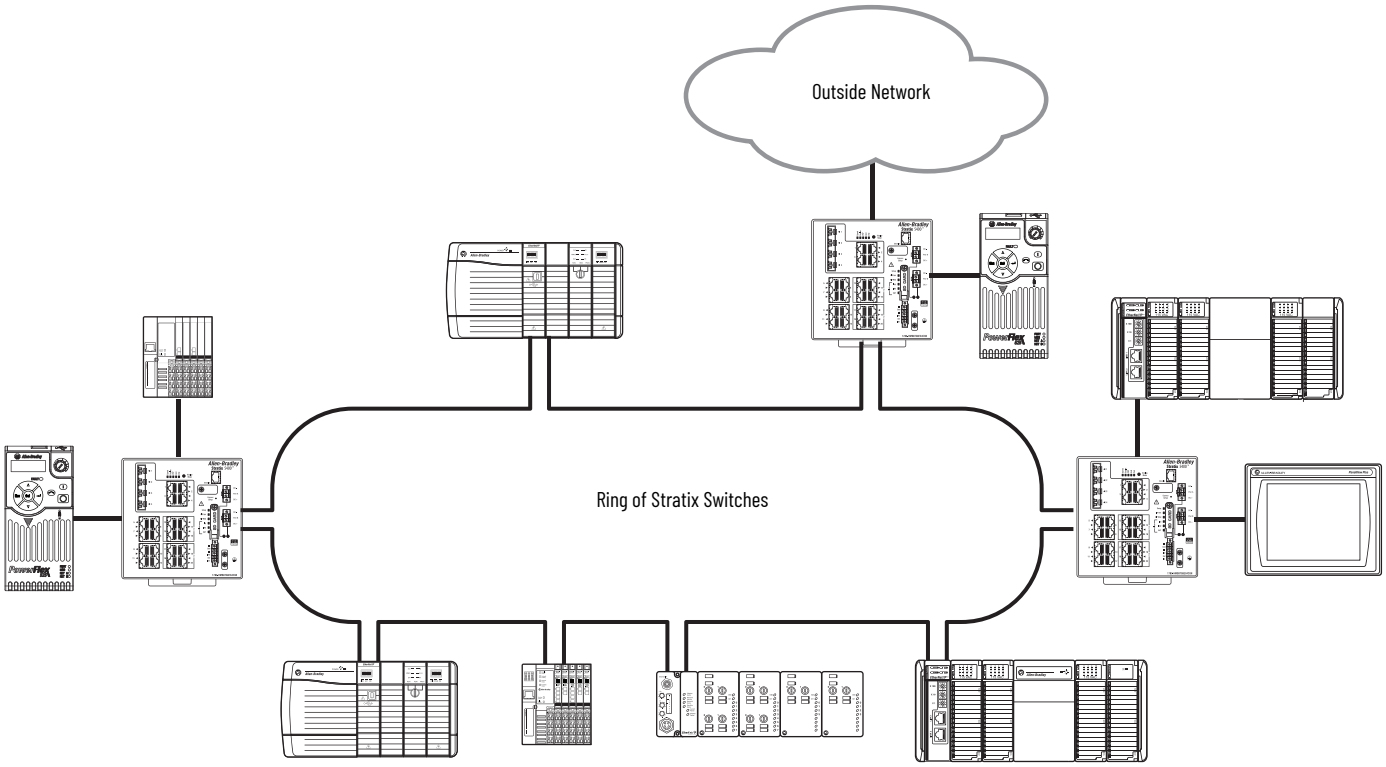
Ring of Switches

A DLR network can consist solely of DLR-capable switches and still support a high-speed convergence time of 3 ms or less.

Limit one ring to no more than 24 switches and 230 end devices.

For configuration examples, see Chapter 4 on page 47.

Figure 8 - Ring of Switches



Notes:

DLR Features for Stratix Switches

Some Stratix® switches support these DLR features:

- Redundant Gateways
- DLR DHCP
- Multiple Rings
- VLAN Trunking

To determine the supported features on a switch, refer to the switch user manual.

IMPORTANT When using the DLR features described in this chapter, be aware of the unsupported network architectures that are described on page 44.

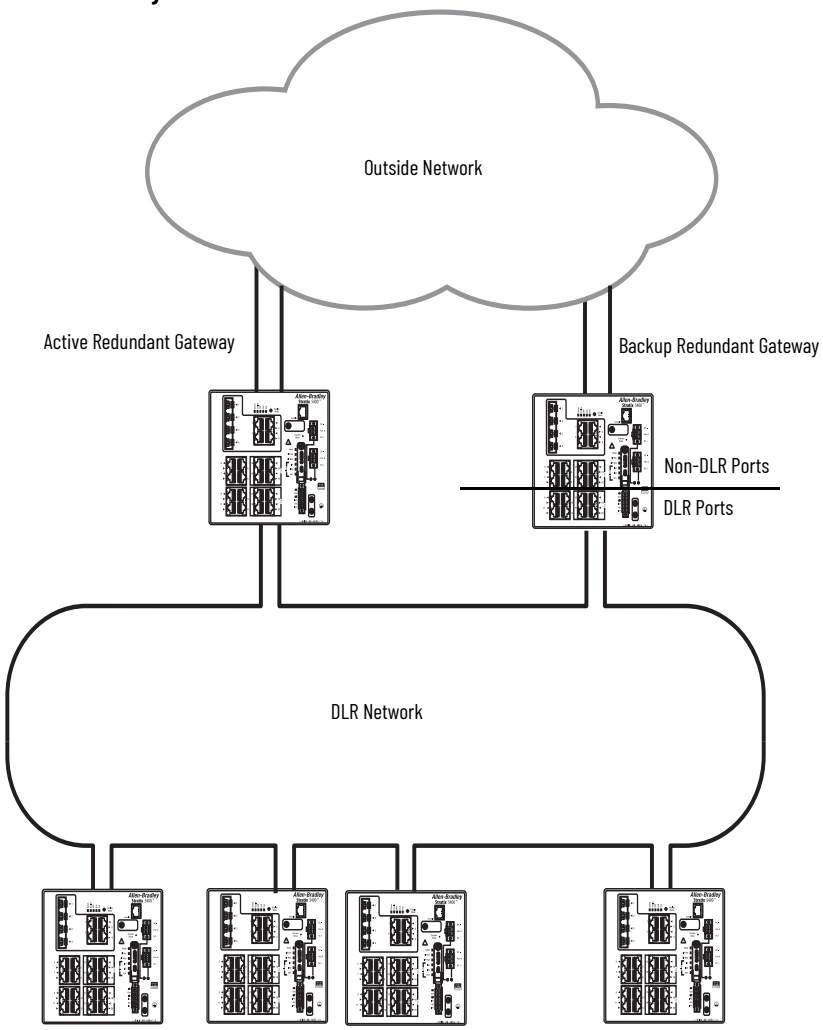
Redundant Gateways

A ring with redundant gateways uses multiple switches to provide multiple connections from a ring to the outside network infrastructure (Figure 9). If you need only one connection to the outside network, redundant gateways are not necessary. However, they provide an additional layer of network resiliency for the loss of an uplink connection.

Switches that function as redundant gateways can be either ring supervisors or ring participants. DLR must be enabled and configured on both gateway switches.

For configuration examples, see Stratix Switch Configuration Examples on page 47.

Figure 9 - Ring with Redundant Gateways



You can configure multiple gateways and assign each gateway a precedence value. Only one gateway can be active at any given time. A backup gateway uses the configuration of the active gateway if the active gateway becomes inactive. The network can switch from the active gateway to a backup gateway within 14 ms...6.1 seconds depending on the uplink network redundancy protocol.

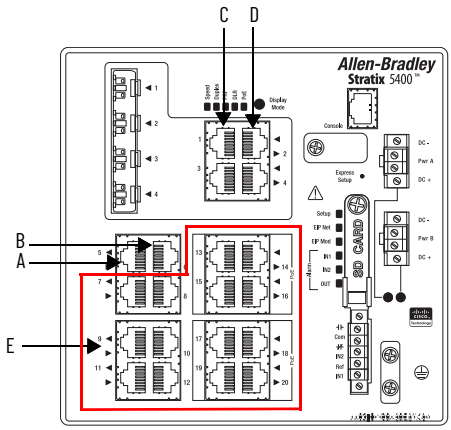
IMPORTANT	Redundant gateway uplink functionality is limited to Stratix switches.

IMPORTANT	The redundant gateway feature requires all devices on the ring to be compatible with redundant gateway. Connections to devices wired to or through a DLR network can be lost upon a gateway changeover if all DLR network devices are not compatible with redundant gateway. For more information about redundant gateway compatibility, see Knowledgebase Technote *Using Device Level Ring (DLR) Redundant Gateway*.

Redundant Gateway Traffic Flow

Figure 10 is an example of a switch that is configured for redundant gateway. All ports are assigned to VLAN 1.

Figure 10 - Redundant Gateway Switch Ports



Port	Configuration
A	DLR access port
B	DLR access port
C	Redundant gateway uplink port
D	Redundant gateway uplink port
E	Non-DLR ports

When the switch acts as the **active** redundant gateway, traffic on the switch that is assigned to VLAN 1 can flow between all ports (A, B, C, D, and E).

When the switch acts as a **backup** redundant gateway, traffic can no longer flow between the DLR ports (A, B) and the other ports on the switch (C, D, and E). To reach the ring, traffic on non-DLR ports (E) must flow through the uplink ports (C, D) to the outside network, and then through the active redundant gateway.

IMPORTANT Traffic flow restrictions from the backup gateway to the ring include Common Industrial Protocol (CIP™) and Device Manager traffic. As a result, management traffic from a ring device to the backup gateway (CIP or webpage data) must use this path:

- Exit the ring through the active gateway
- Flow through the outside network above the ring
- Enter the backup gateway through the uplink port.

If the backup gateway later becomes the active gateway, traffic then begins to flow between all ports.

Redundant Gateway Device Requirements

IMPORTANT Both the active and backup gateway switches and all devices on the ring must have firmware that supports redundant gateways.

Connections to devices wired to or through a DLR network can be lost upon a gateway changeover if all DLR devices do not support redundant gateways.

To support redundant gateways, compatible Stratix switches require IOS release 15.2(4)EA or later.

To determine whether a device supports redundant gateways, see Knowledgebase Technote *Using Device Level Ring (DLR) Redundant Gateway*.

Redundant Gateway Considerations

For the best performance with DLR redundant gateways, keep in mind these considerations:

- Keep critical data within the ring.
- Do not directly connect devices that must communicate with DLR to either the active or backup redundant gateway switch. You can connect devices in a linear or star topology to the redundant gateway switch if the devices can tolerate long periods of network isolation.
- Multicast convergence times can be higher than expected for the following types of traffic on gateway uplink ports:
  - IEEE 1588 CIP Sync™ traffic
  - Multicast produce/consume tags

Multicast Traffic and Redundant Gateways

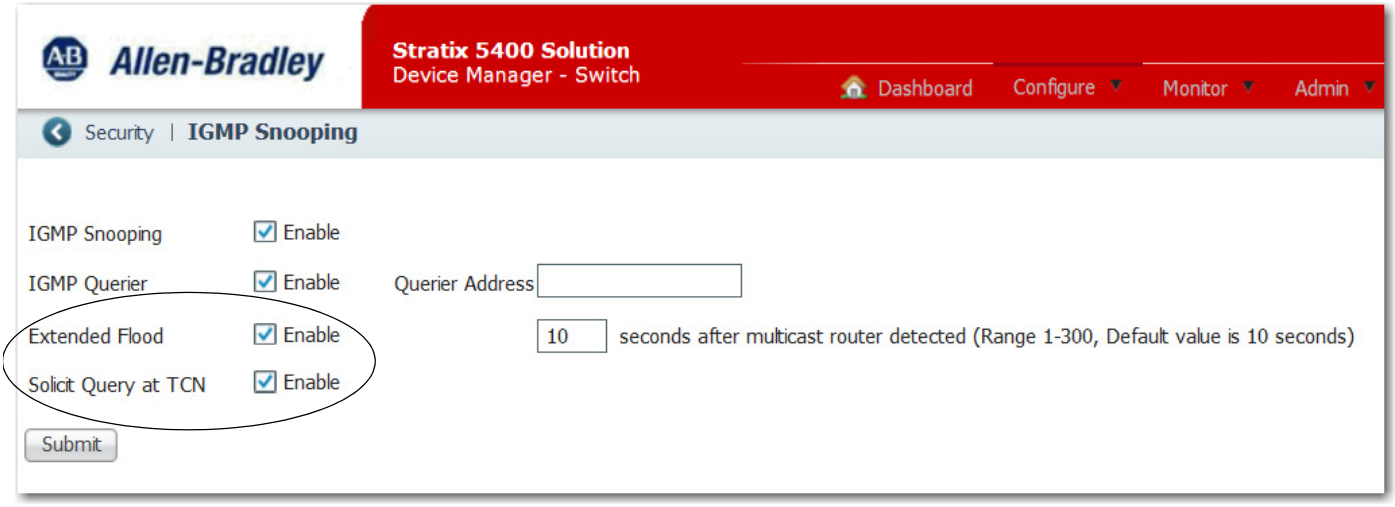
In redundant gateway applications, we recommend unicast for traffic moving between the DLR network and the outside network. However, if your application requires that you use multicast traffic, we recommend that you enable the following IGMP features in Device Manager (Figure 11):

IMPORTANT These options are not available and are not required to be configured on a Stratix 5800 switch because the behavior is enabled by default.

- Extended Flood—Enable this IGMP feature to help prevent the switch from dropping multicast packets before they reach the hosts when IGMP snooping querier experiences a disruption.
- Solicit Query at TCN—Enable this IGMP feature to speed convergence time when an STP topology change occurs in the outside network. When the feature is enabled on a non-root bridge switch in the spanning tree domain, the switch sends a topology change notification (TCN) message to the active IGMP snooping querier. The querier then issues a general query message that causes hosts to subscribe to multicast streams via report messages.

For more information about configuring these features, refer to the user manual for the switch.

Figure 11 - Recommended Features in Device Manager for Multicast Traffic



Although the IGMP snooping querier is typically enabled only on the distribution switch, it is possible in some applications to enable multiple IGMP snooping queriers per VLAN on these switches:

- Distribution switch
- Access switch

This scenario is outside the scope of this publication.

DLR DHCP

You can configure some Stratix switch models as a DLR DHCP server for devices in a ring. This feature provides IP addresses for devices in the ring, but not other switches in the ring. A DLR DHCP server assigns IP addresses to devices based on their positions in the ring. This feature makes sure that a replaced device receives the expected IP address. Replacement devices must be configured in DHCP or BOOTP mode and placed in the same position in the ring as the previous device.

A switch can only assign IP addresses to ring devices when these conditions are met:

- DLR DHCP is properly configured on the switch.
- The switch is configured as a ring supervisor.
- All connections in the ring are complete.
- The ring is in a healthy state with no faults.

Ring devices receive IP address changes from the switch when the ring converges after the loss of a network connection. If you assign a new IP address to an active device, the new address does not take effect until the current address lease expires or the device restarts.

A mismatch between the number of configured devices and the number of physical ring devices triggers an alarm. This mismatch can be a result of a topology change or a configuration change.

IMPORTANT	Use caution with automatic IP address assignment when wiring DLR with similar devices. The controller cannot detect incorrect IP addresses of identical devices in the wrong position.

Figure 12 shows an example of a Stratix 5400 switch that is configured as a primary DHCP server in a ring. All devices on the ring have assigned index numbers:

- The primary DHCP server is always index number 1.
- Starting from the primary DHCP server, the index numbers increment around the ring in order from the device connected to the lowest DLR port on the primary server. In this example, the lowest DLR port on the primary server is Gi1/5, so the device connected to Gi1/5 has an index number of 2.

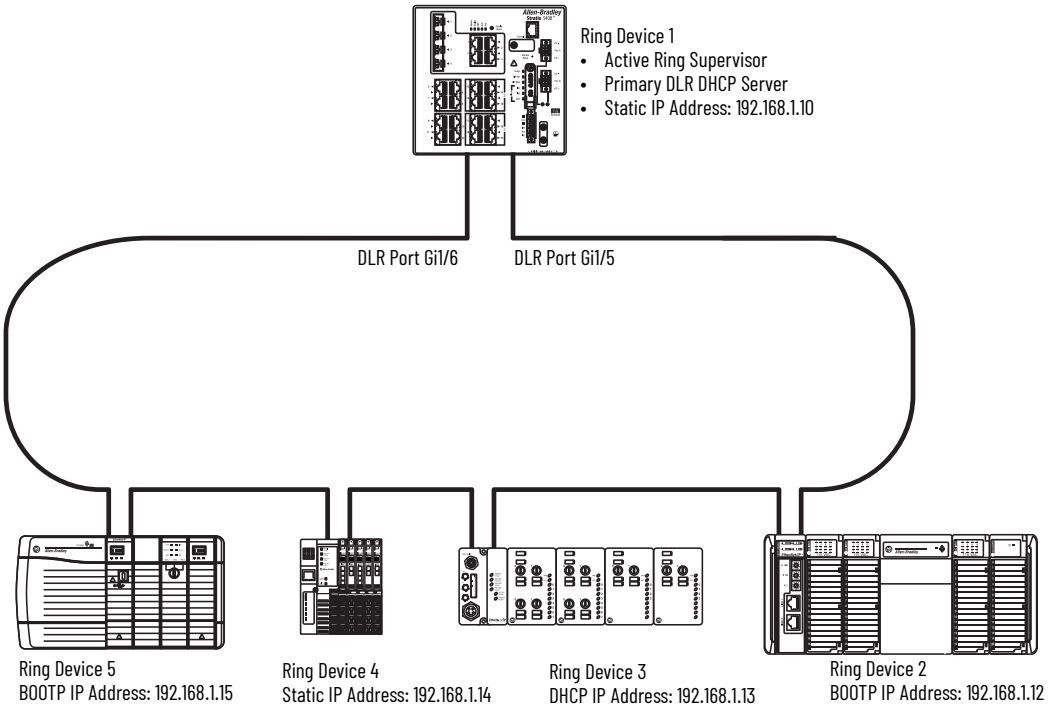
In this example, the primary DLR DHCP server recognizes IP address requests from ring devices 2, 3, and 5 and responds with the position-based IP address that is specified in the DHCP table.

Table 1 - Example DHCP Table for Ring Devices

Ring Device Index(1)	IP Address	Host Name	DHCP Pool
2	192.168.1.12	Rack 2	Pool 1
3	192.168.1.13	Rack 3	Pool 1
4			
5	192.168.1.15	Rack 5	Pool 1

(1) Device 1 represents the primary DLR DHCP server and is not configurable. Because device 4 does not have an entry in the DHCP table, the DHCP server does not provide an IP address for that device.

Figure 12 - DLR DHCP Example



For step-by-step configuration examples, see Stratix Switch Configuration Examples on page 47.

Backup DHCP Server (Optional)

IMPORTANT If you have an application that includes a backup DLR DHCP server, other DHCP features (including DHCP persistence) are not supported on the primary DHCP server or the backup DHCP server.

If enabled, a backup DLR DHCP server runs on the backup ring supervisor and obtains its reference table automatically from the active DLR DHCP server on the active ring supervisor. There can be multiple backup DLR DHCP servers in the ring.

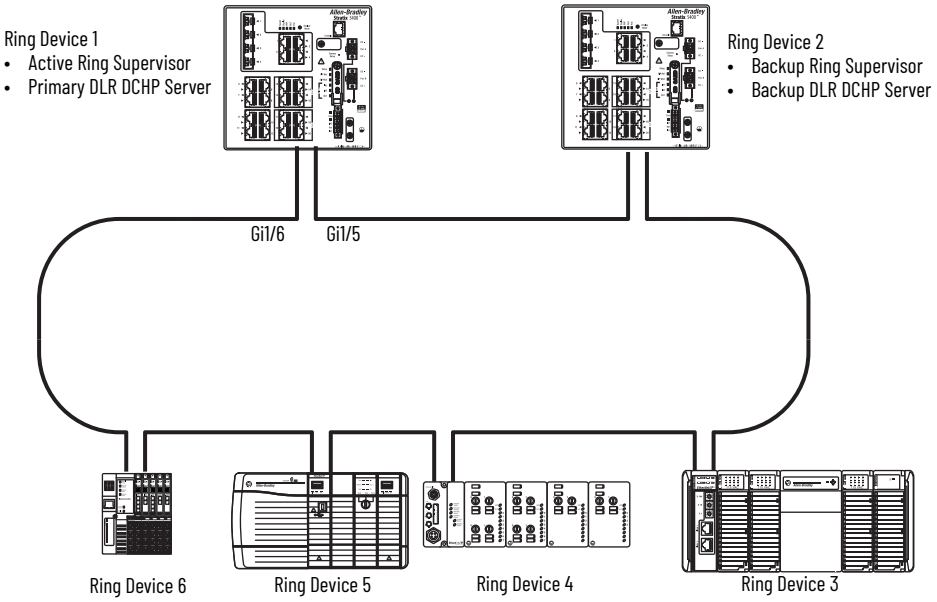
If the primary DLR DHCP server fails, the following happens:

- The backup ring supervisor becomes the active supervisor.
- The backup DLR DHCP server on the backup ring supervisor becomes the active DLR DHCP server.
- The new active DLR DHCP server begins IP assignment and renewal for the ring until one of the following happens:
  - The original active DLR DHCP server is restored.
  - A new active DLR DHCP server is manually configured.

IMPORTANT Do not configure a DHCP table or DHCP address pool on the backup DLR DHCP server. Only configure DHCP on the active DLR DHCP server.

Figure 13 shows a DLR network that includes a backup DLR DHCP server. A backup DLR DHCP server is an optional configuration.

Figure 13 - Optional Backup DLR DHCP Server



DHCP Snooping

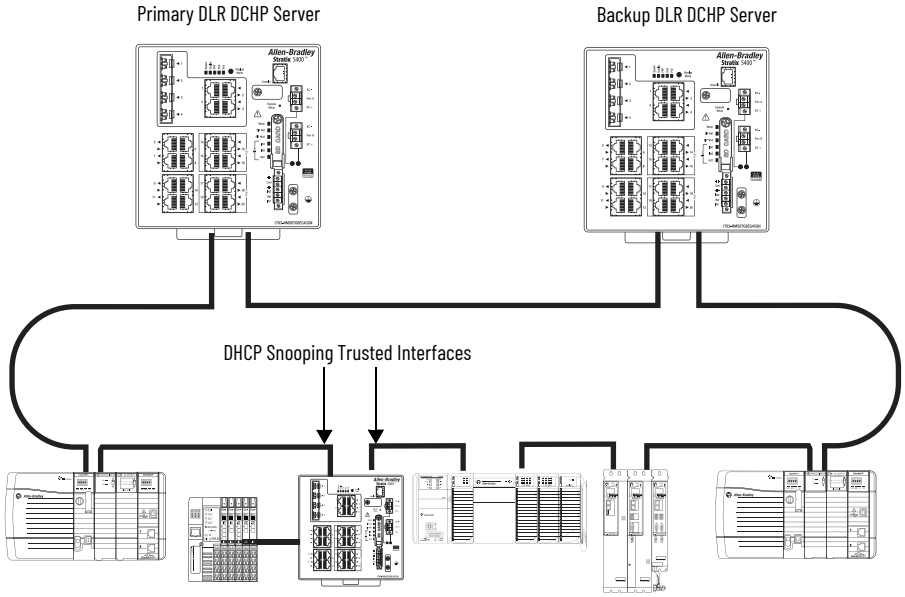
IMPORTANT DHCP snooping must be enabled for ring participants to receive IP addresses from a DLR DHCP server reliably.

DHCP snooping is enabled by default on switches that are configured as DHCP servers. When DHCP snooping is enabled, DHCP address assignments are restricted to the primary ring DCHP server and ring participants. DHCP requests from another server cannot enter the ring, and DHCP requests from the primary ring DCHP server cannot leave the ring.

If DHCP snooping is disabled, DHCP address requests become broadcast messages and ring participants can receive an IP address from the first offer from a DHCP server within or outside of the ring.

If a ring contains a switch operating as a ring participant rather than a primary or backup DHCP server, you must configure the DLR ports on the switch as Trusted® interfaces (Figure 14).Otherwise, DHCP server messages are dropped when they reach the DLR ports on the switch. Once the DLR ports are configured as Trusted interfaces, DHCP server messages can flow through the ports to offer IP addresses to ring participants.

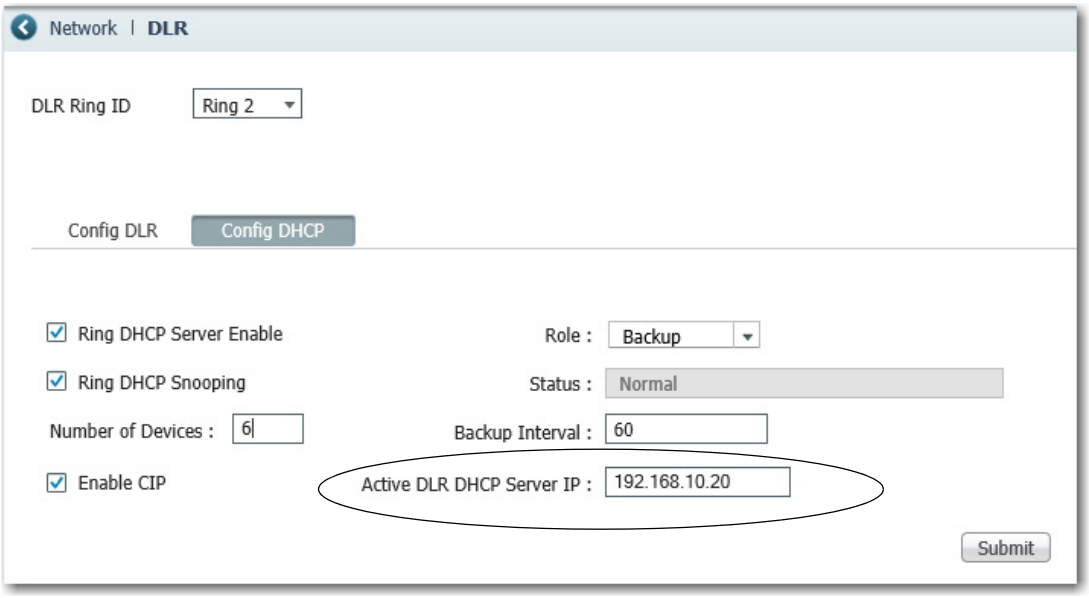
Figure 14 - DHCP Snooping Trusted Interfaces



CIP VLAN Configuration

When both primary and backup DLR DHCP servers are used, you must specify the CIP VLAN IP address of the primary server in the configuration for the backup server (Figure 15). The IP address enables the backup server to receive the DHCP configuration from the primary server if a switchover occurs.

Figure 15 - CIP VLAN IP Address of Primary Server in Configuration of Backup Server



Multiple Rings

Stratix 5400 and 5800 switches support as many as three rings.

For configuration examples, Stratix Switch Configuration Examples on page 47.

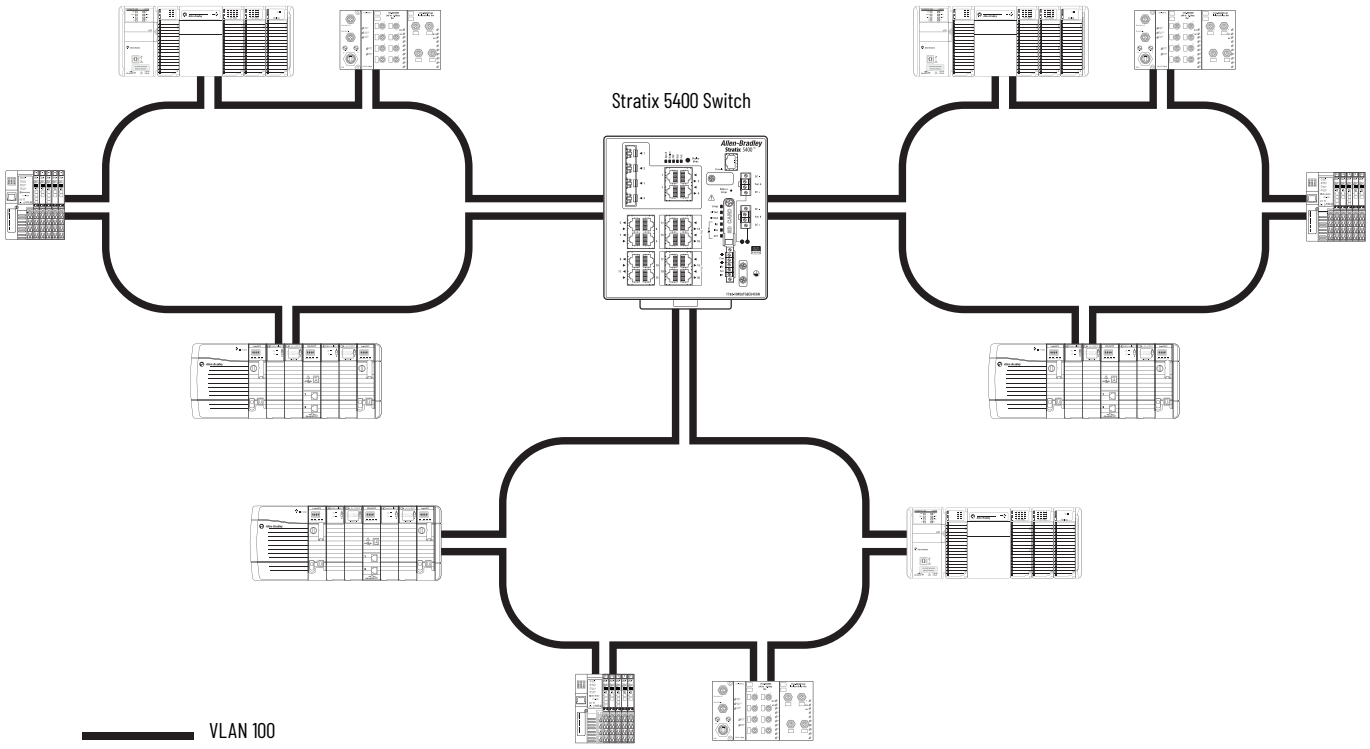
Multiple Rings, Single Switch, Single VLAN

The following restrictions apply to multiple rings that are connected to one switch without VLAN trunking:

- Multiple rings cannot share the same ring ports.
- Ring ports function only as access ports.
- All ring ports within the same ring must be assigned to the same access VLAN.
- All ring ports within the same ring must be configured for the same speed.

In Figure 16, multiple rings are connected to one switch on one VLAN.

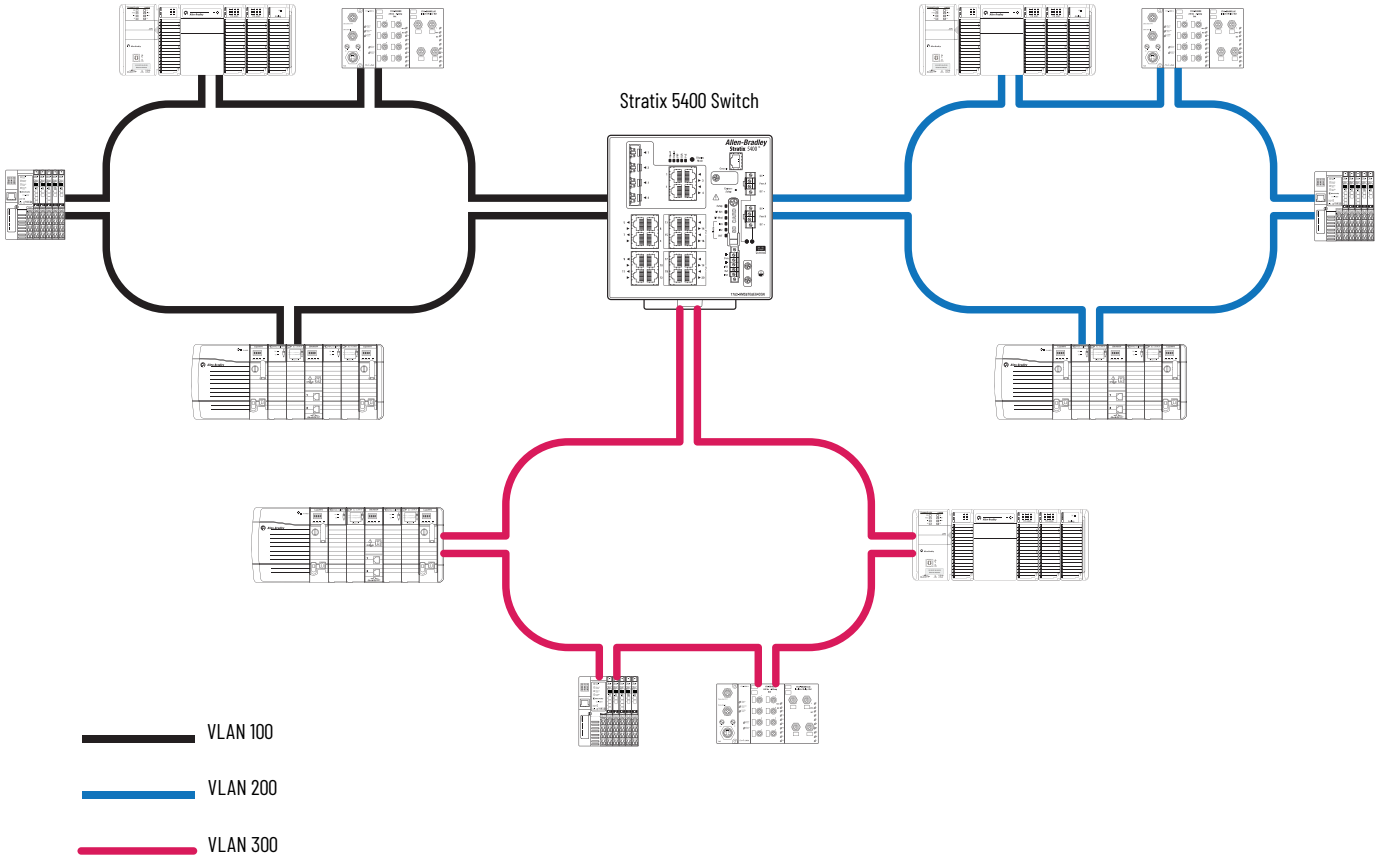
Figure 16 - Multiple Rings, Single Switch, Single VLAN



Multiple Rings, Single Switch, Multiple VLANs

Each ring can also be on a separate VLAN, as shown in Figure 17.

Figure 17 - Multiple Rings, Single Switch, Multiple VLANs

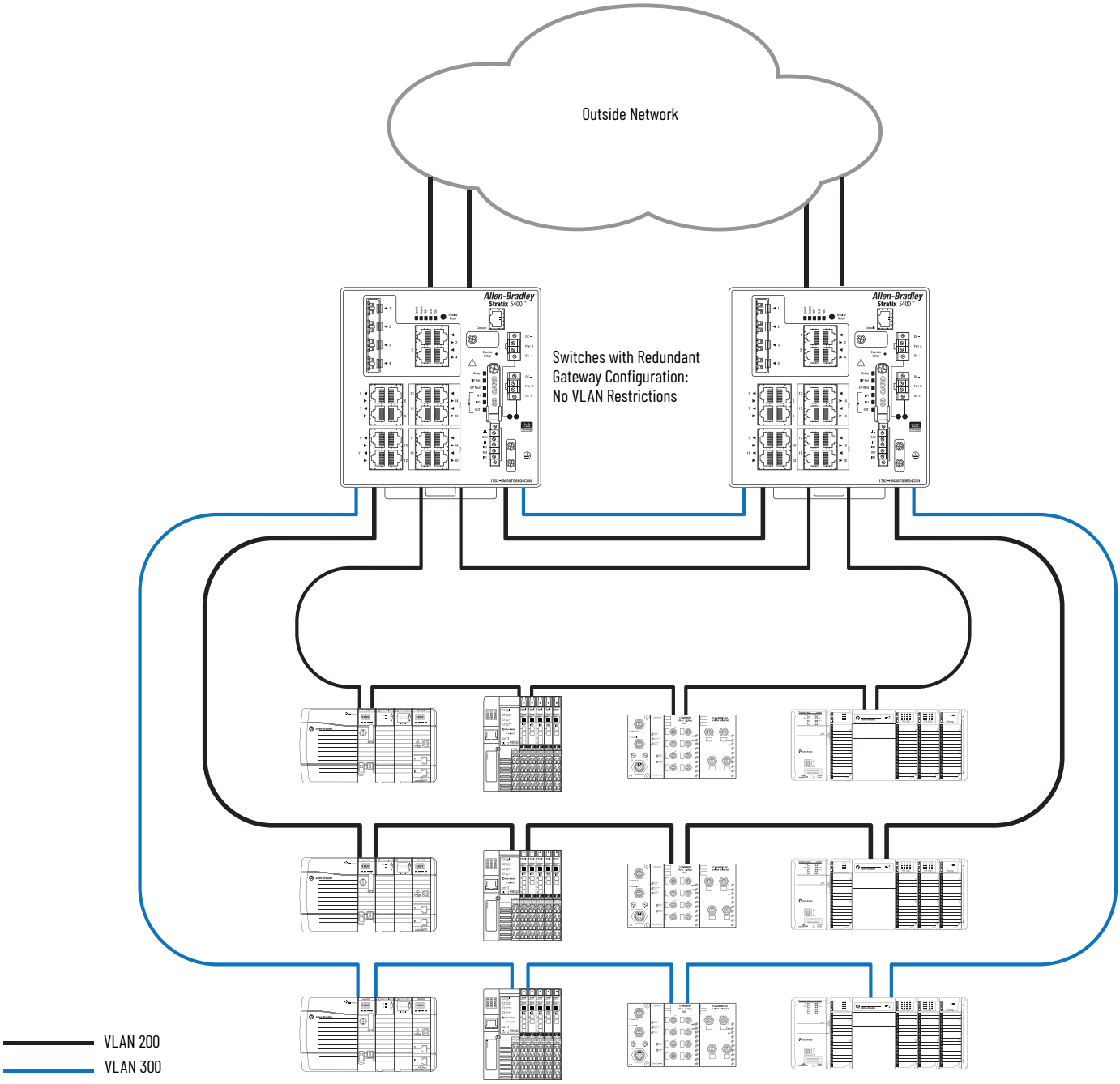


Multiple Rings Connected to Multiple Switches

You can also use multiple rings with multiple Stratix 5400 switches, as shown in Figure 18. Depending on the configuration of the switches, VLAN restrictions can apply.

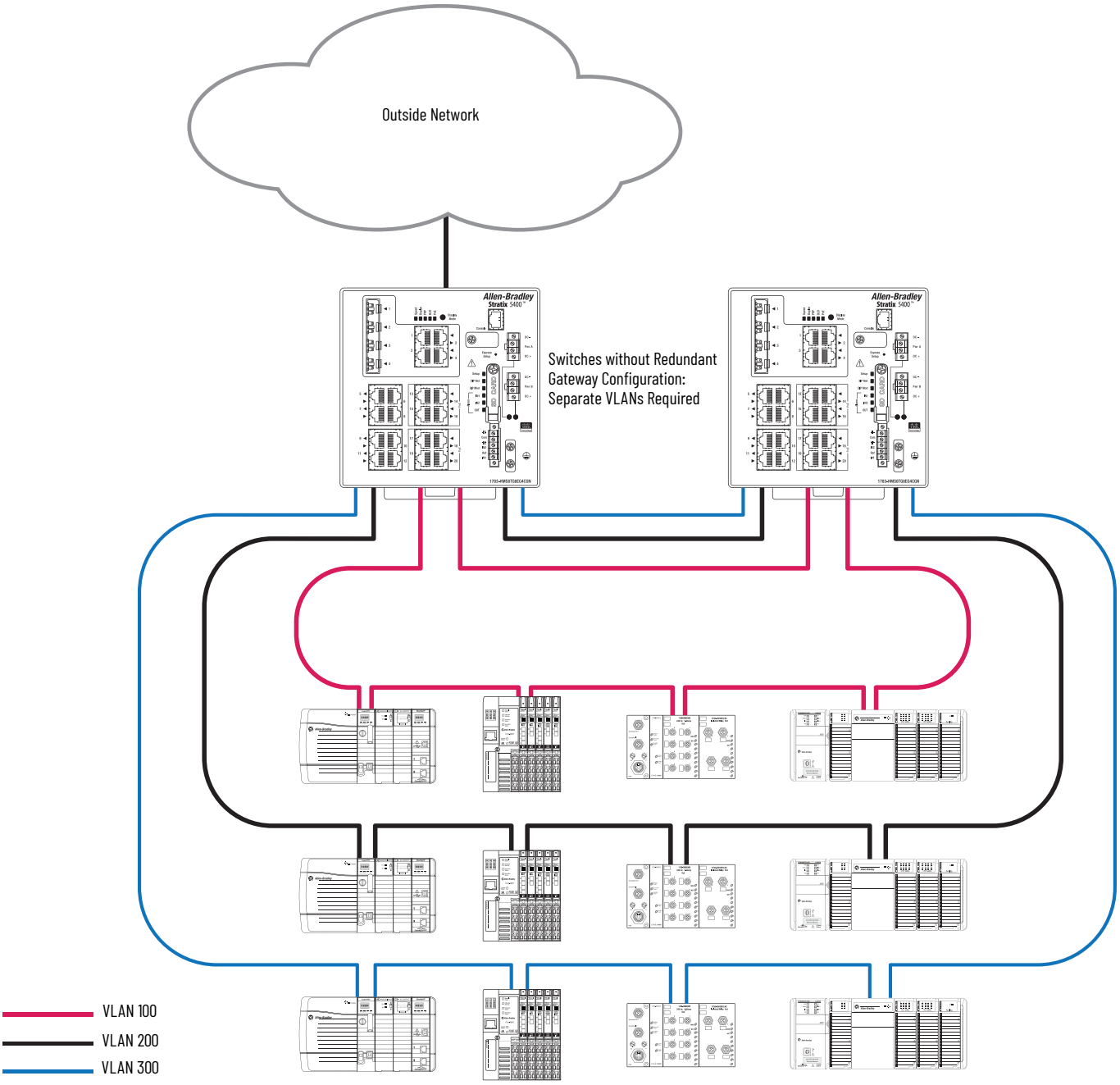
If the two switches are configured as redundant gateways for the same set of rings, no VLAN restrictions exist. The following example shows two rings on the same VLAN and one ring on a separate VLAN. However, because there are no VLAN restrictions, you can also configure all three rings on the same VLAN or all three on separate VLANs.

Figure 18 - Multiple Rings, Multiple Switches, No VLAN Restrictions



If the two switches are not configured as redundant gateways, then each ring must be on a separate VLAN, as shown in Figure 19.

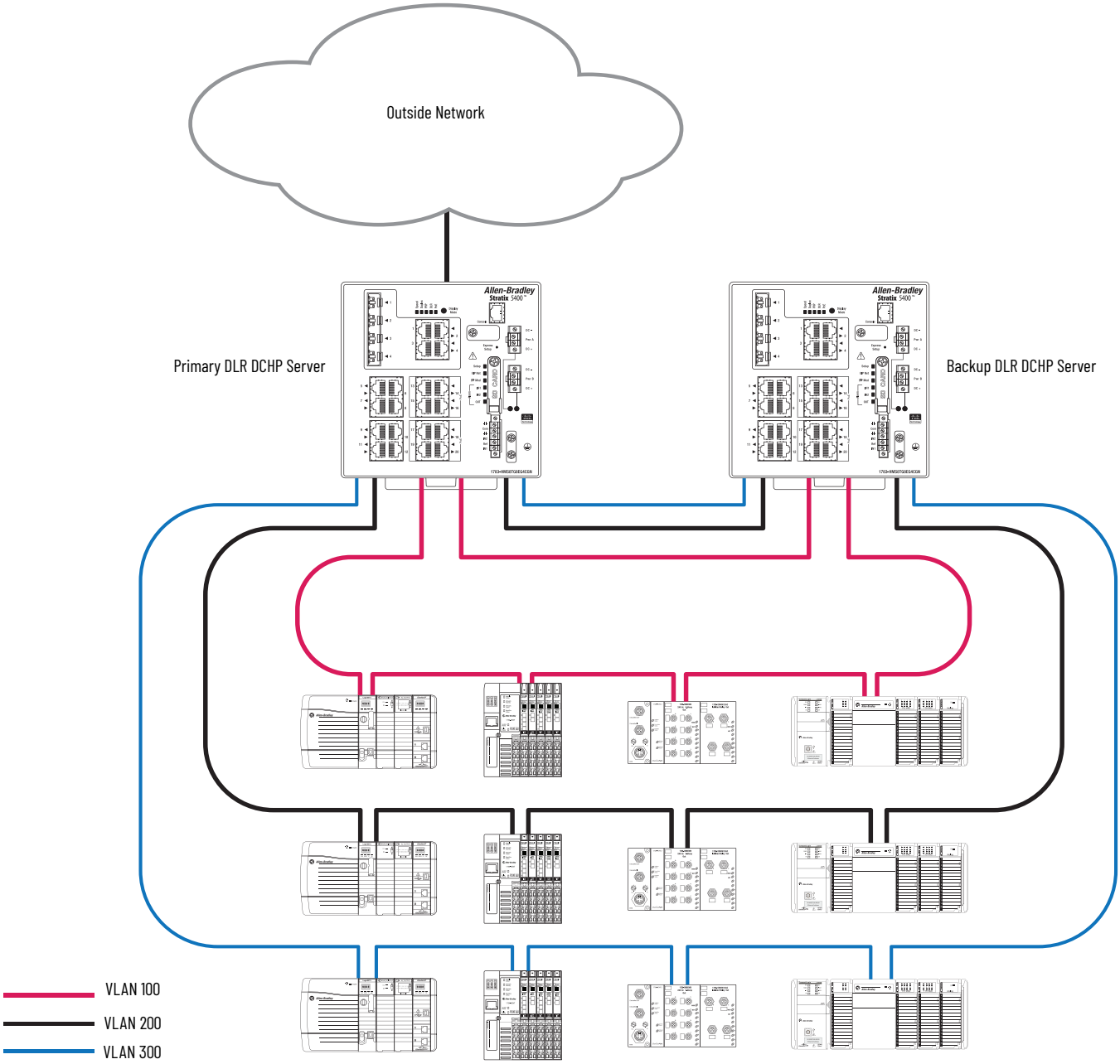
Figure 19 - VLANs Required



Multiple Rings with DLR DHCP

Multiple ring architectures can also include a DHCP server as shown in Figure 20. In this example, both the primary and backup DHCP servers share a CIP™ VLAN.

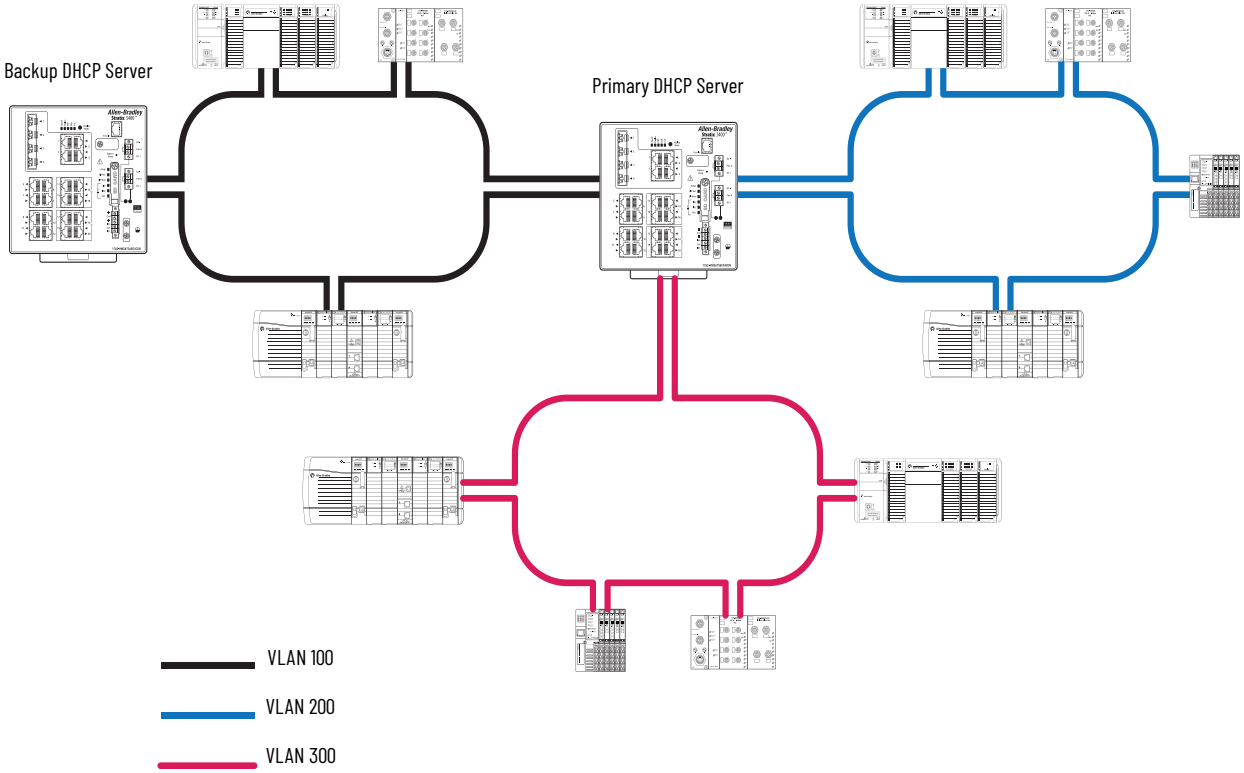
Figure 20 - Multiple Rings with DHCP Server and Multiple VLANs



In some DLR networks, the primary and backup DHCP servers must use different CIP VLANs. Figure 21 shows an example of this scenario:

- One Stratix 5400 switch connects to three rings with three different VLANs. The same switch also operates as the primary DHCP server for ring devices on CIP VLAN 100.
- Another Stratix 5400 switch is located within the ring with CIP VLAN 100 and operates as the backup DHCP server for that ring.

Figure 21 - DLR DHCP with Multiple Rings, Multiple VLANs, Different CIP VLANs



VLAN Trunking

A trunk is a connection between switches that carries traffic from multiple VLANs configured on the switches. DLR VLAN trunking allows switches with multiple VLANs to be connected in a DLR network. As traffic passes from one switch to the next in a ring, the traffic can either remain on the same VLAN or pass to different VLANs via routing. For more information about configuring VLAN trunking on a switch, refer to the user manual for the switch.

For configuration examples, Stratix Switch Configuration Examples on page 47.

Requirements and Restrictions

When configuring DLR VLAN trunking, observe these guidelines:

- All devices in your DLR network must be switches.
- All switches in your DLR network must have DLR-enabled trunk ports.
- Routing traffic to different VLANs requires one of the following:
  - A Layer 2 switch using connected routing in the ring or in the outside network
  - A Layer 3 switch or router in the ring or in the outside network

IMPORTANT Do not use multiple routing devices per ring and VLAN.

- You cannot extend the same VLAN across multiple rings.
- To avoid problems with Spanning Tree Protocol (STP), you must specify which VLANs, including native VLANs, to allow on each DLR-enabled trunk port.

IMPORTANT By default, trunk ports carry traffic from any VLAN. Change the default port setting on each trunk port to allow only the required VLANs.

- The same capability and restrictions that apply to VLANs and resiliency protocols, like REP and STP, also apply to DLR VLAN trunking.
- For best performance, use Stratix 5400 or 5800 switches with DLR VLAN trunking.

VLAN Trunking Architecture Examples

The following examples show DLR VLAN trunking with these network architectures:

- One ring with routing in the outside network (Figure 22)
- Multiple rings with routing on the DLR switch that connects all rings (Figure 23)
- Multiple rings with a routing in the outside network (Figure 24)

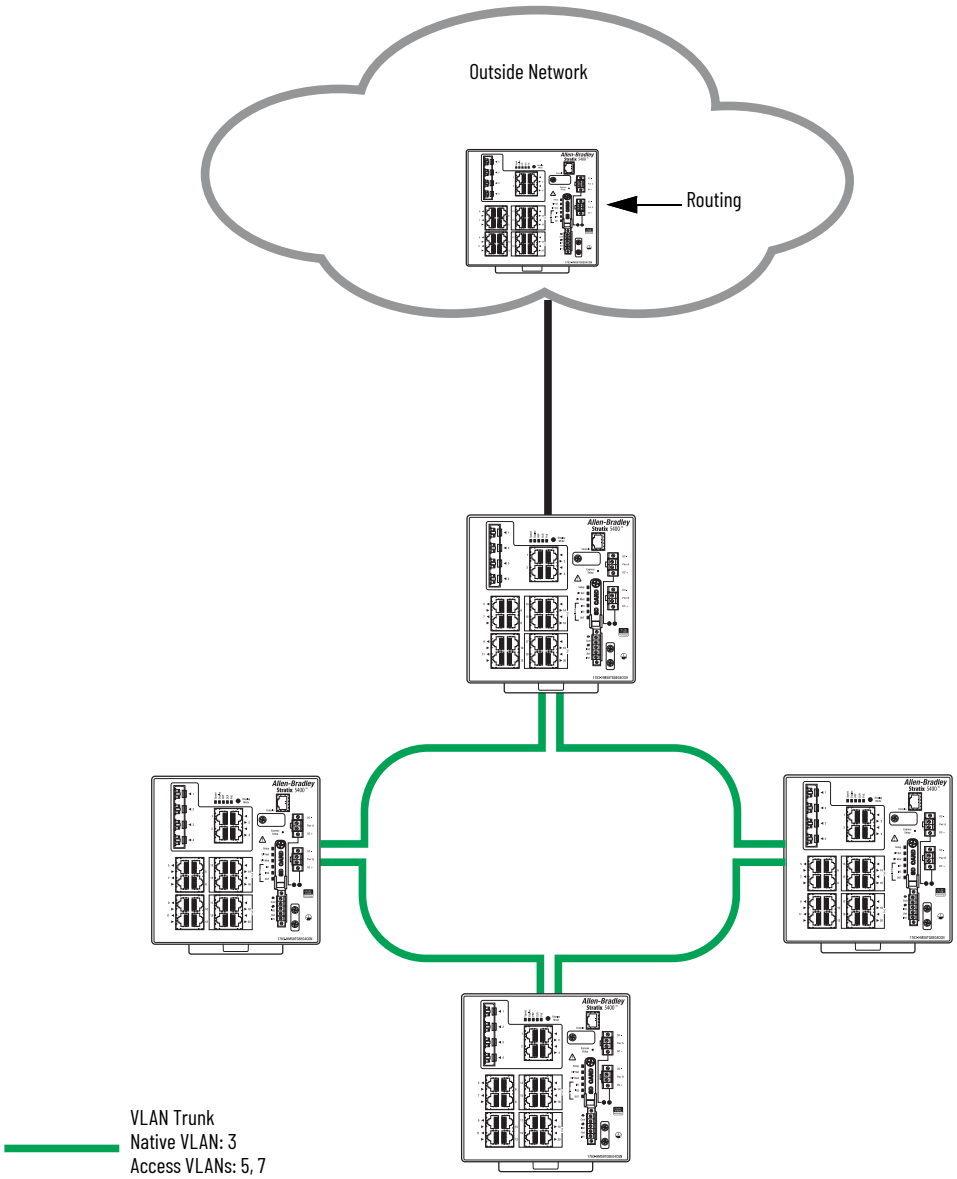
While not shown, redundant gateways are also supported in DLR networks with VLAN trunking.

Figure 22 shows DLR VLAN trunking in one ring with no routing functionality:

- Traffic remains on the same VLAN as it passes through each switch in the ring.
- All DLR-enabled trunk ports allow traffic from only VLANs 3, 5, and 7

IMPORTANT Control data or management traffic on the native VLAN is not recommended.

Figure 22 - DLR VLAN Trunking—One Ring

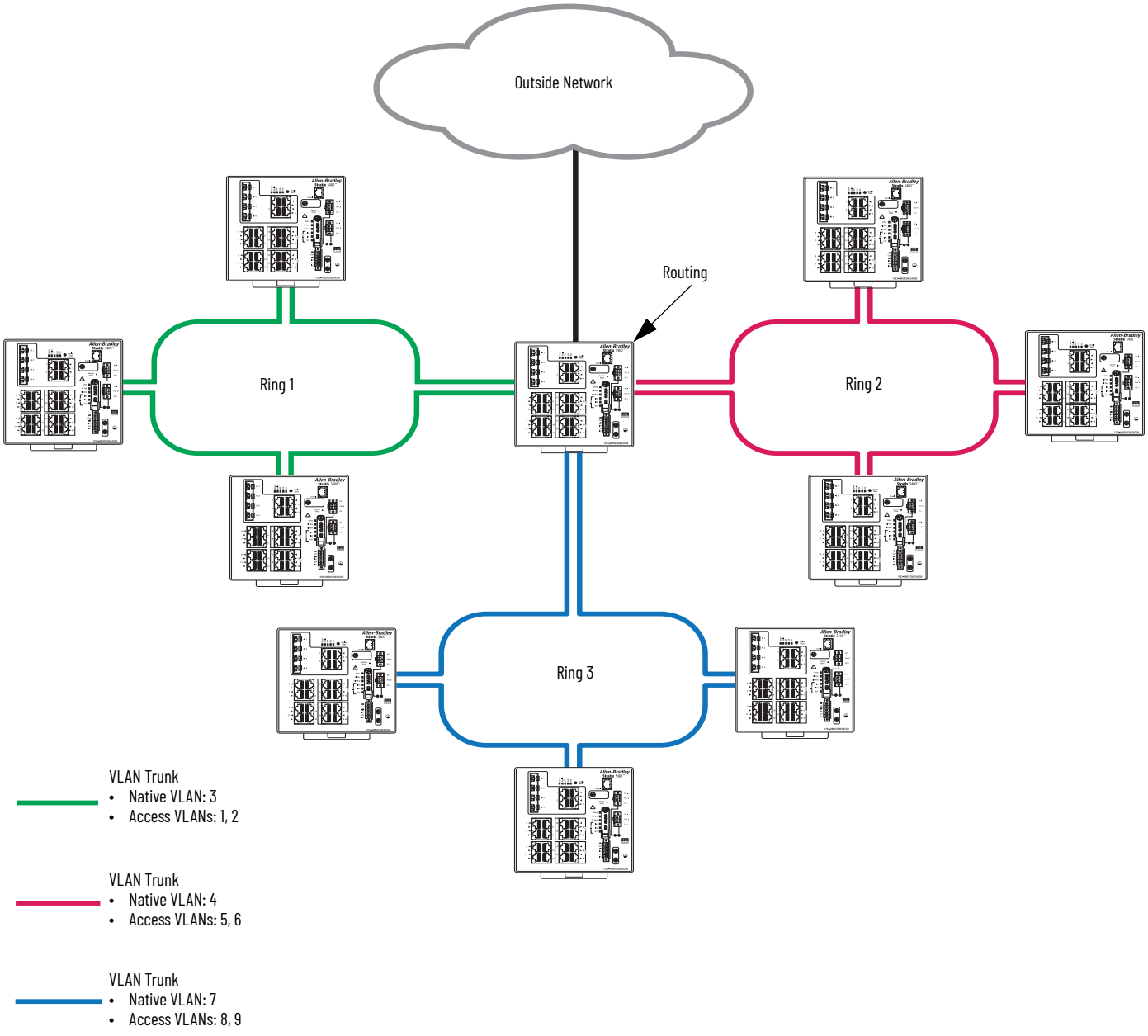


In the example shown in Figure 23, routing is performed on the switch that connects all rings:

- In ring 1, all DLR-enabled trunk ports allow traffic from only VLANs 1, 2, and 3
- In ring 2, all DLR-enabled trunk ports allow traffic from only VLANs 4, 5, and 6
- In ring 3, all DLR-enabled trunk ports allow traffic from only VLANs 7, 8, and 9
- No VLANs overlap between rings.

IMPORTANT Control data or management traffic on the native VLAN is not recommended.

Figure 23 - DLR VLAN Trunking—Multiple Rings, Switch with Routing

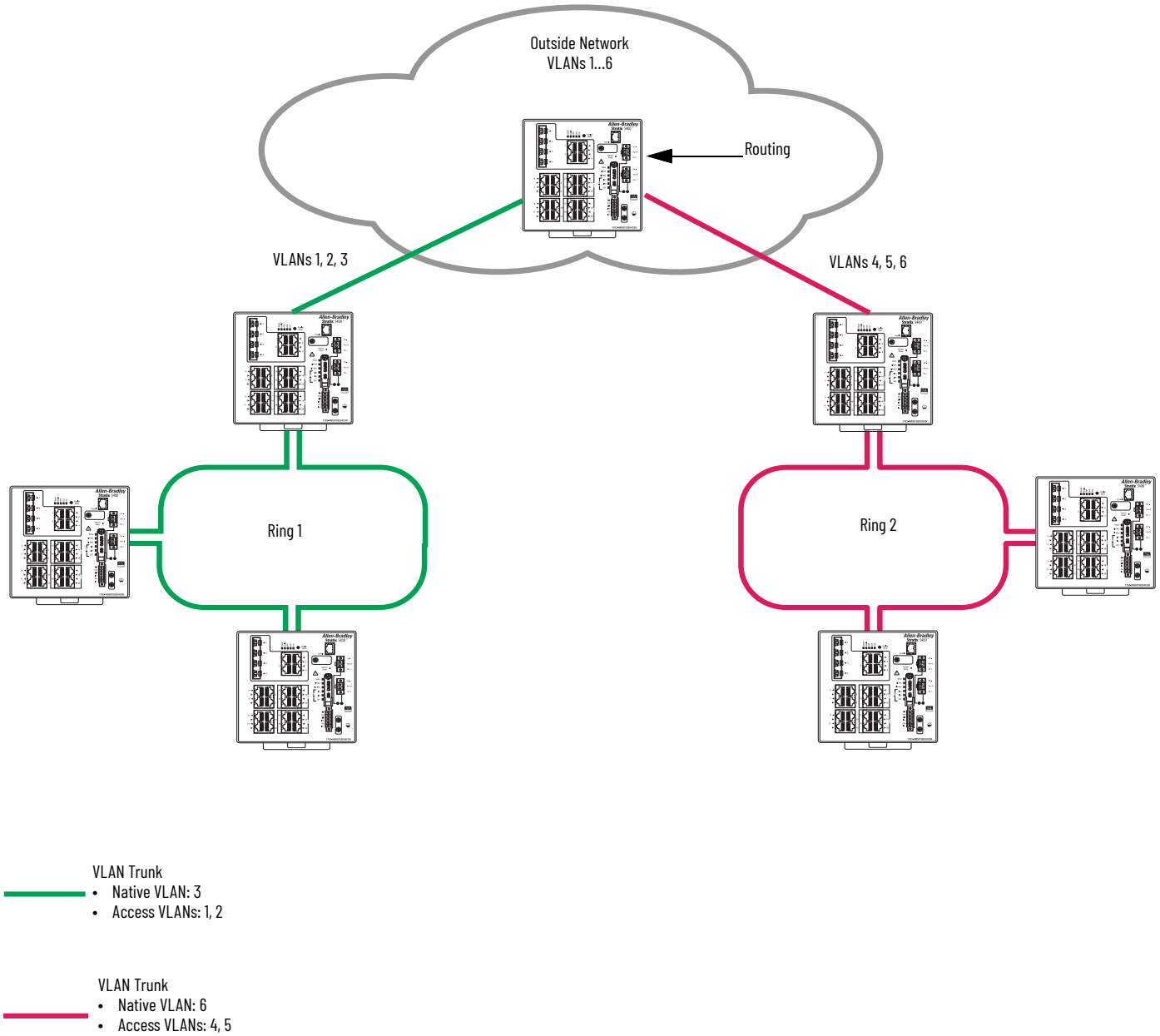


In the example shown in Figure 24, routing is performed in the outside network:

- In ring 1, all DLR-enabled trunk ports allow traffic from only VLANs 1, 2, and 3
- In ring 2, all DLR-enabled trunk ports allow traffic from only VLANs 4, 5, and 6
- The remote ports on the routing device in the outside network are configured to allow the same VLANs as the connected local ports.
- No VLANs overlap between rings.

IMPORTANT Traffic on the native VLAN is not recommended.

Figure 24 - DLR VLAN Trunking—Routing in Outside Network



All Features in One DLR Network

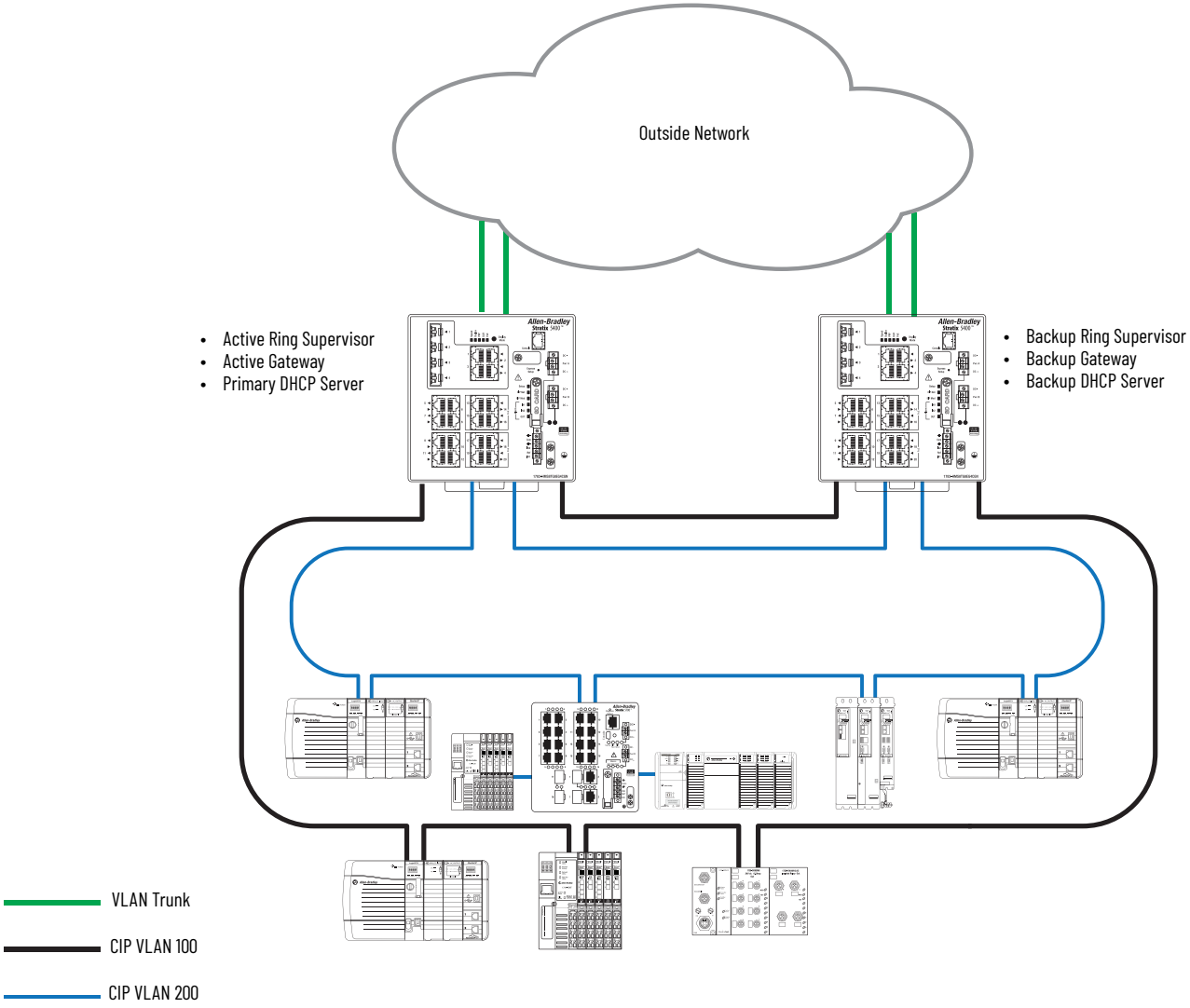
One DLR network can operate with all of these features together (Figure 25):

- Redundant gateways
- DLR DHCP
- Multiple rings
- VLAN trunking

In a network with both redundant gateways and multiple rings, the same Stratix switch must be the active gateway for all rings. The same Stratix switch must also be the backup gateway for all rings.

While this example illustrates the use of multiple VLANs, you can also use one VLAN for both rings.

Figure 25 - Redundant Gateways, DLR DHCP, Multiple Rings, VLAN Trunking



Uplink to Other Resiliency Technologies

For a DLR network that connects to an existing outside network, Stratix switch uplink ports support these resiliency technologies:

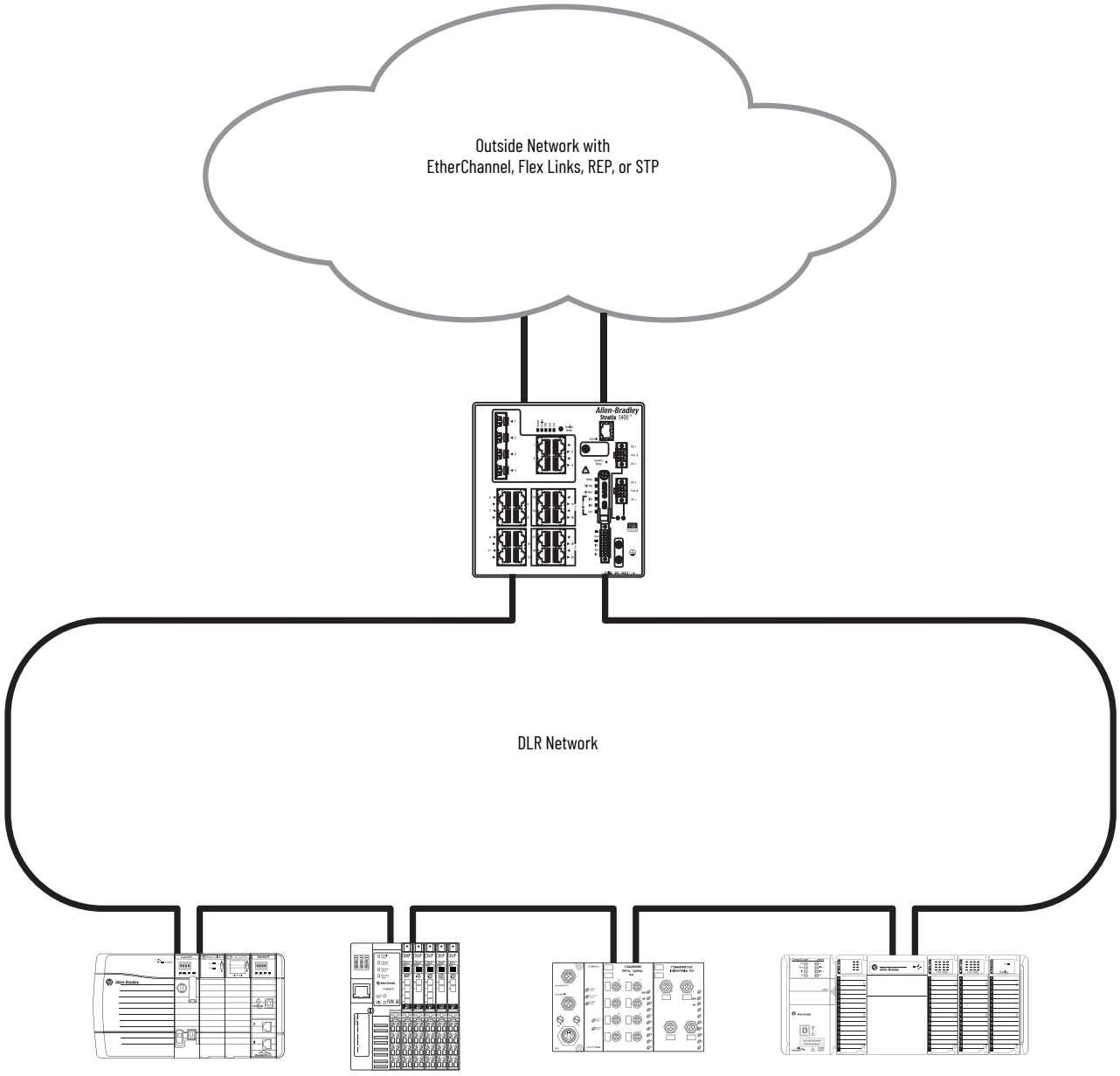
- Spanning Tree Protocol (STP)
- EtherChannel
- Flex Links
- Resilient Ethernet Protocol (REP)

IMPORTANT Network resiliency protocols are valid only on uplink ports and not on DLR ports.

Single Switch Uplink to the Outside Network

Figure 26 shows a Stratix switch with two uplink ports that are connected to a network that uses EtherChannel, Flex Links, REP, or STP for resiliency.

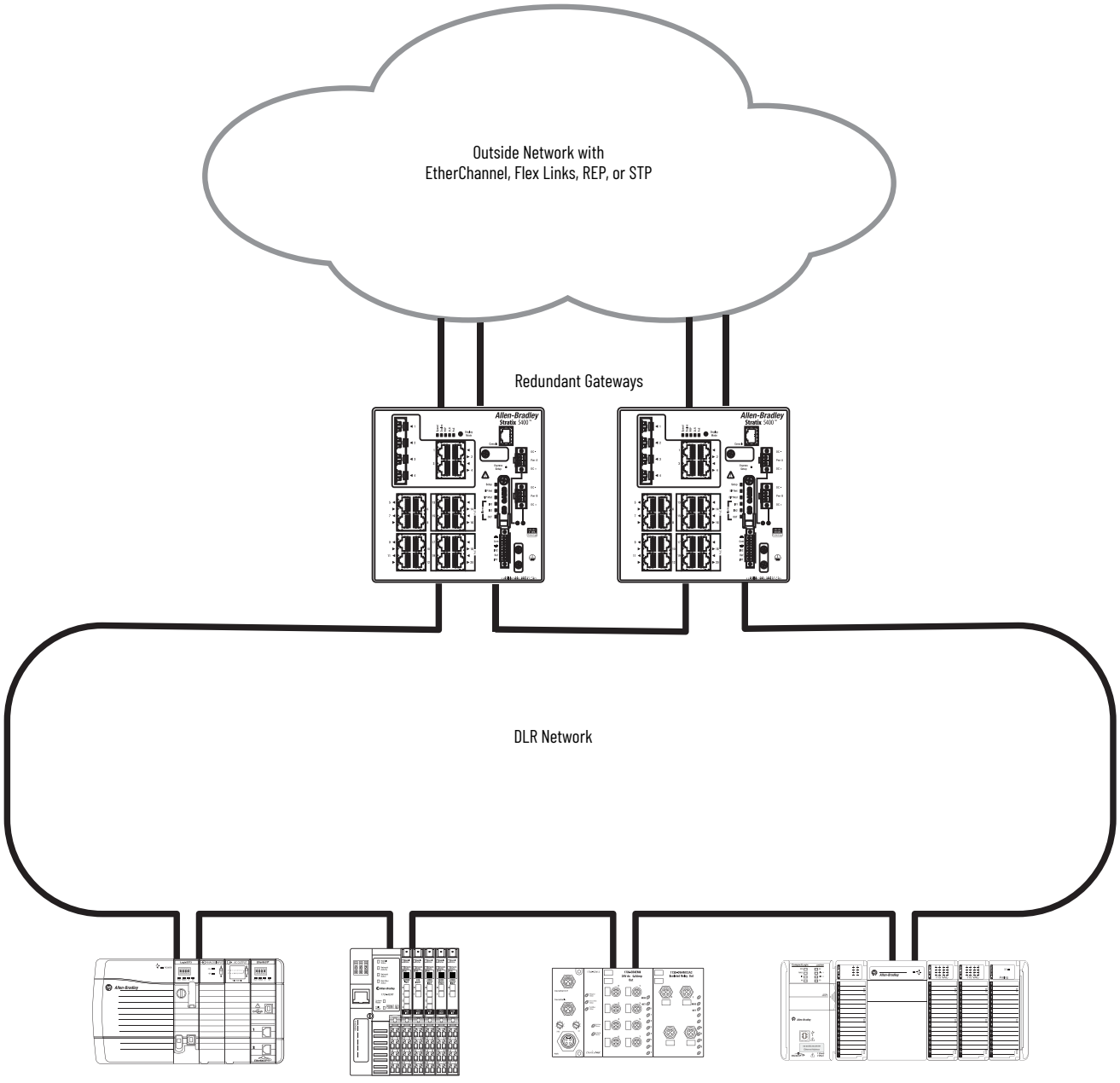
Figure 26 - Single Switch Uplink to Network with EtherChannel, Flex Links, REP or STP



Redundant Gateways with Uplinks to Outside Network

Figure 27 shows Stratix redundant gateways with two uplink ports that are connected to a network that uses EtherChannel, Flex Links, REP, or STP for resiliency.

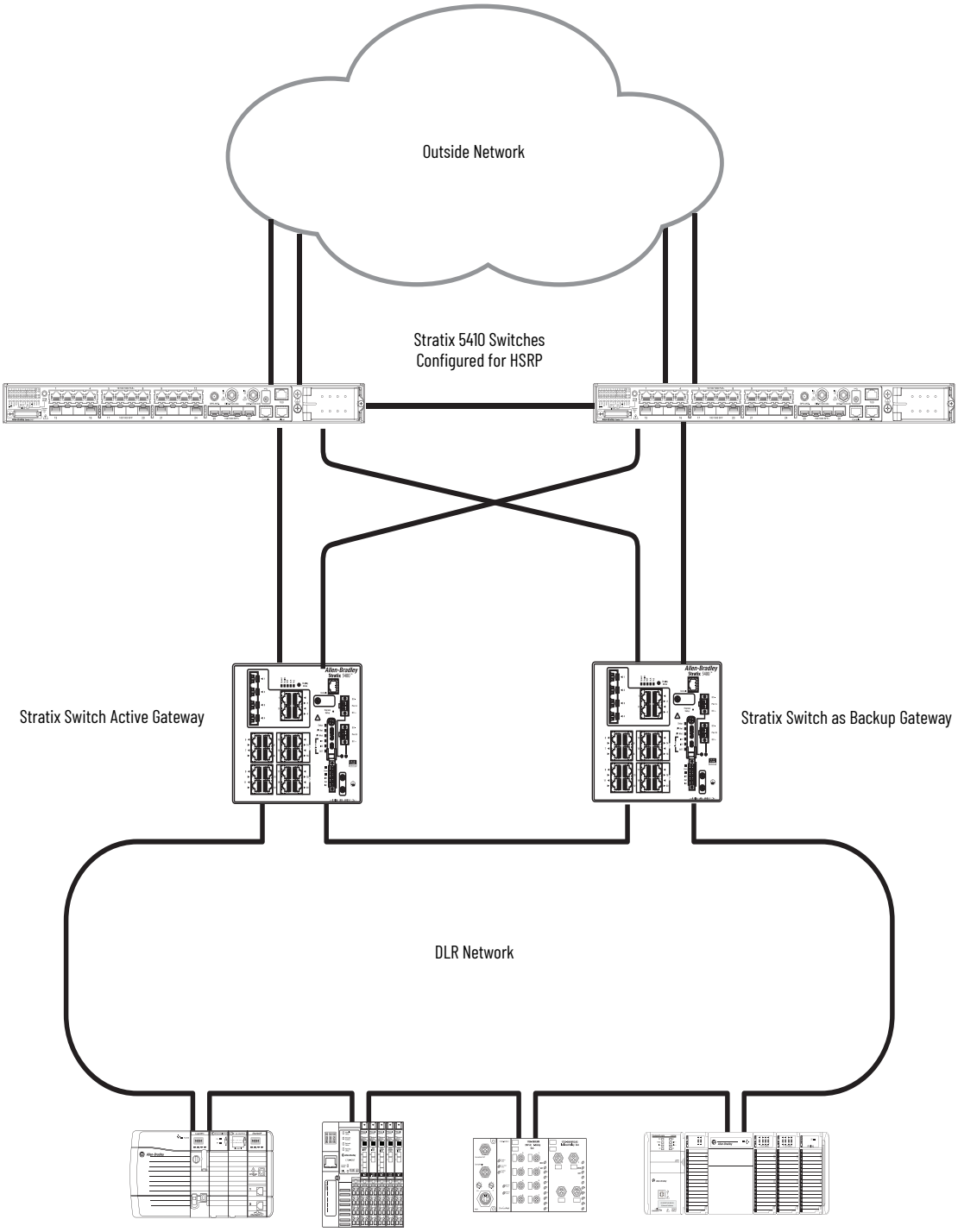
Figure 27 - Redundant Gateways - Uplink to Network with EtherChannel, Flex Links, REP or STP



In the example shown in Figure 28, HSRP provides redundancy from the uplink ports on the redundant gateways to the outside network.

HSRP is a gateway redundancy solution that is developed by Cisco®. It allows a high-available network to recover from the failure of the device acting as a default gateway.

Figure 28 - Redundant Gateways to Outside Network via HSRP



Unsupported Network Architectures

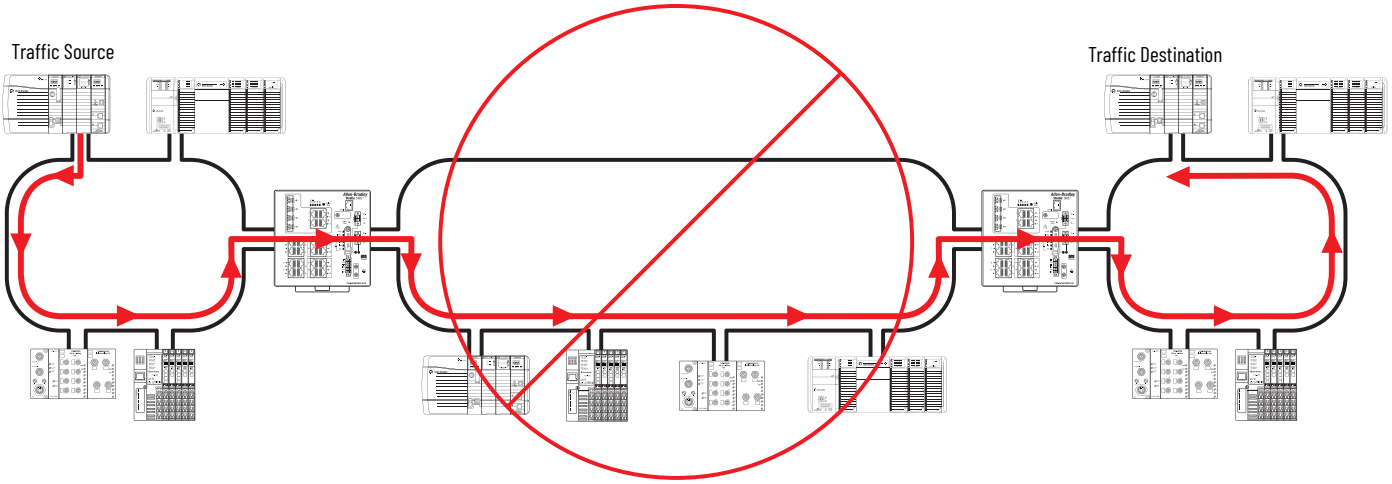
IMPORTANT Depending on your network architecture, limitations can exist.
Be sure to validate your DLR architecture within the larger network before production use.

The following architectures can have an adverse effect on network performance and are not supported.

For networks that do not use DLR VLAN trunking, an architecture where traffic flows nonstop through one or more rings is not supported. For example, in Figure 29, traffic flows from its source in ring 1 through ring 2 without stopping before it reaches its destination in ring 3.

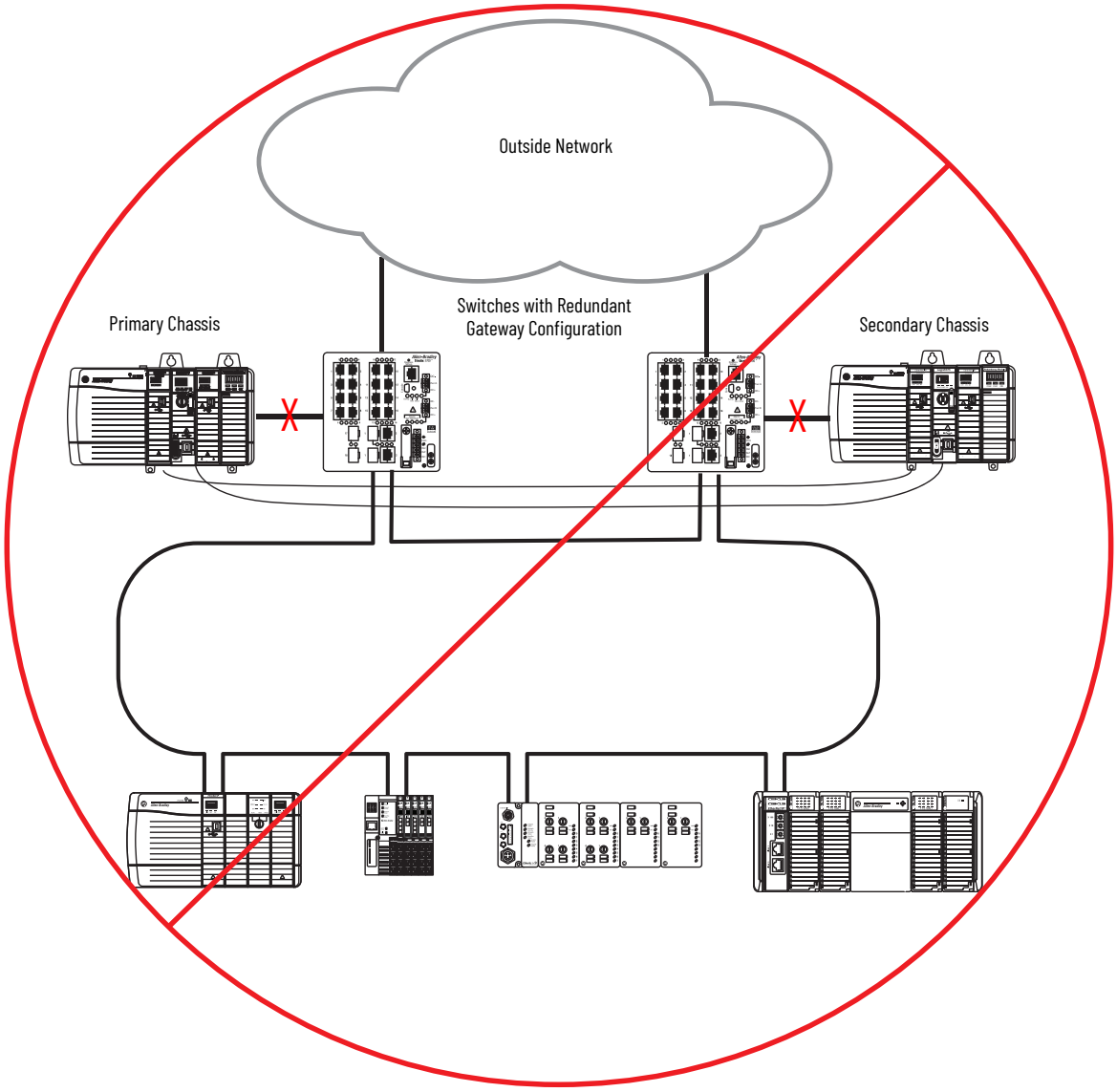
For networks that use DLR VLAN trunking, an architecture where traffic flows nonstop through a series of trunked rings is not supported. However, traffic can flow nonstop through one trunked ring.

Figure 29 - Nonstop Traffic Through One or More Rings



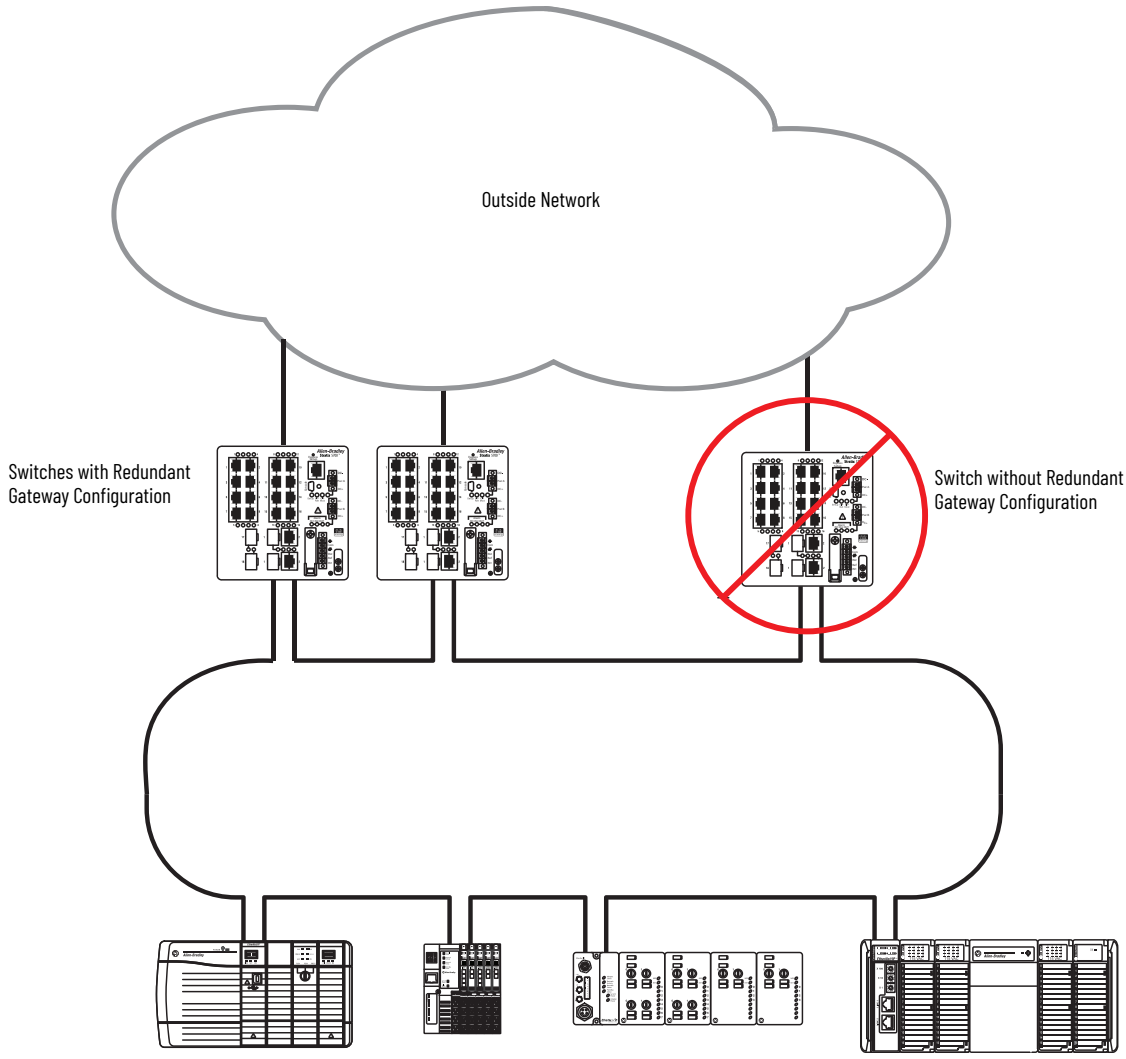
In a ControlLogix® redundancy system, do not connect redundant chassis pairs to DLR redundant gateways (Figure 30).

Figure 30 - Redundant Chassis Pair Connected to Redundant Gateways



When using redundant gateways, do not connect another Stratix switch in the ring to the outside network (Figure 31).

Figure 31 - Uplink via Redundant Gateways and Non-Redundant Gateway Switch



Stratix Switch Configuration Examples

This chapter provides step-by-step configuration examples for typical DLR implementations and DLR features described in the preceding chapters. Note the following:

- The examples use multiple software tools. Choose a tool that is suitable for your application and skill set.
- For details about how to run Express Setup, see the user manual for the switch.
- There are no DLR parameters to configure for non-Stratix® ring participants.
- The examples use either Stratix 5400 or 5800 switches and three rings.

Table 2 - DLR Implementations

Implementation		Configuration Process
A	Ring of Devices	1. Non-Stratix Configuration Examples. 2. Configure Non-Stratix Ring Participants.
B	Ring of Devices and Switches	1. Run Express Setup on Switches. 2. Non-Stratix Configuration Examples. 3. Configure Non-Stratix Ring Participants. 4. Configure Stratix 5400 Ring Supervisors or Configure Stratix 5800 Ring Supervisors. 5. Configure Stratix 5400 Ring Participants or Configure Stratix 5800 Ring Participants.
C	Ring of Switches	1. Run Express Setup on Switches. 2. Configure Stratix 5400 Ring Supervisors or Configure Stratix 5800 Ring Supervisors. 3. Configure Stratix 5400 Ring Participants or Configure Stratix 5800 Ring Participants.

Table 3 - DLR Features

Implementation	Configuration Process
Redundant Gateways	1. Use implementation B or C in Table 2. 2. Configure Stratix 5400 Redundant Gateways or Configure Stratix 5800 Redundant Gateways.
DLR DHCP	1. Use implementation B in Table 2. 2. Configure DLR DHCP on a Stratix 5400 Switch or Configure DLR DHCP on Stratix 5800 Switches.
VLAN Trunking	1. Use implementation C in Table 2. 2. Configure VLAN Trunking on a Stratix 5400 Switch or Configure VLAN Trunking on Stratix 5800 Switches.

Non-Stratix Configuration Examples

You can modify these 1756-EN2TR examples to use with any non-Stratix device with DLR ring supervisor capability.

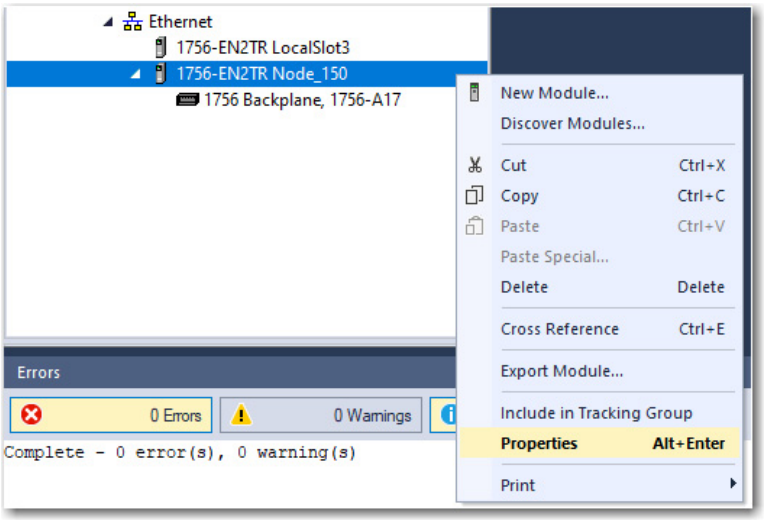
Configure Non-Stratix Ring Supervisors

Use any of the following tools to configure a non-Stratix device as a ring supervisor:

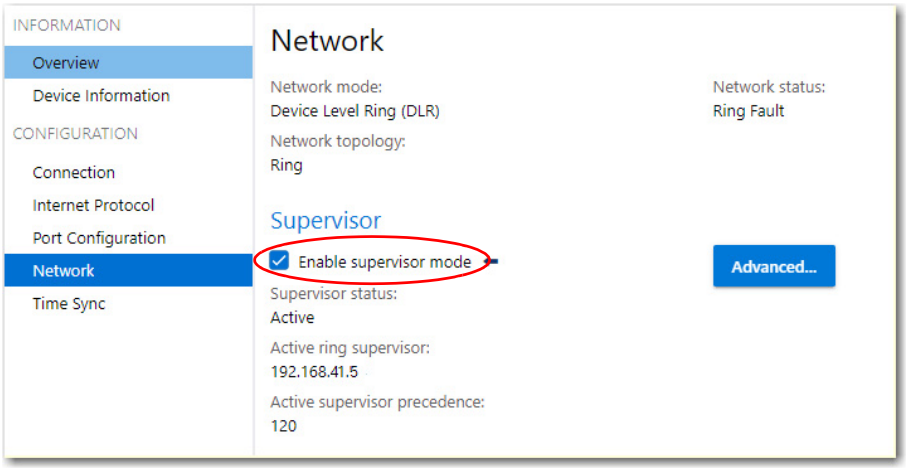
- Logix Designer application
- FactoryTalk® Linx
- RSLinx® Classic

Non-Stratix Ring Supervisor via Logix Designer Application

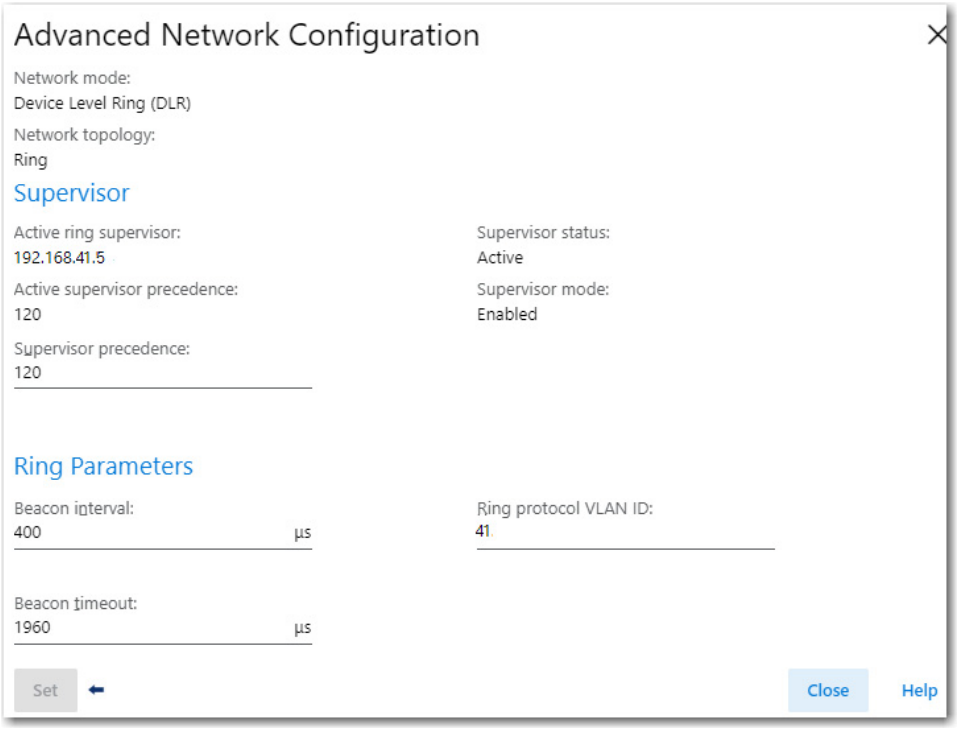
1. Access the properties for the device.



2. Enable Supervisor mode.



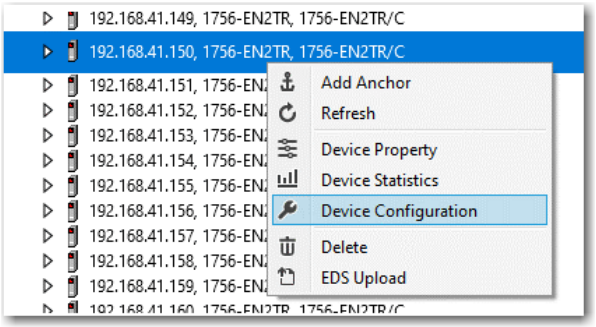
3. Configure supervisor parameters.



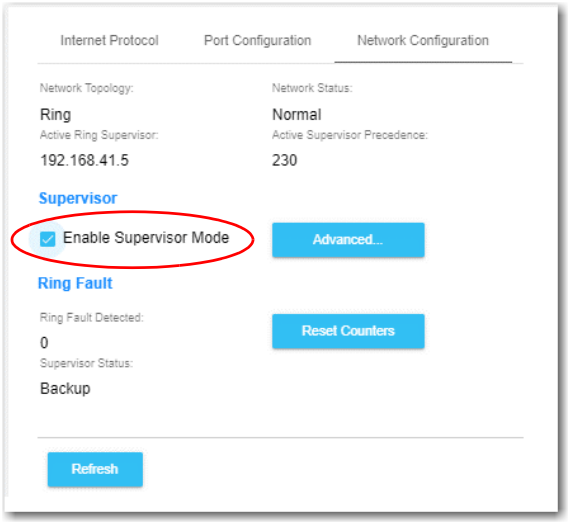
4. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Non-Stratix Ring Supervisor via FactoryTalk Linx

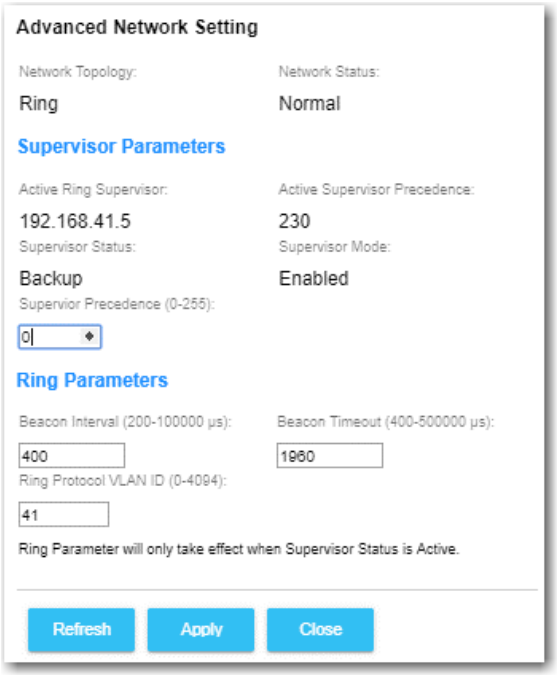
1. Access the configuration for the device.



2. Enable Supervisor mode.



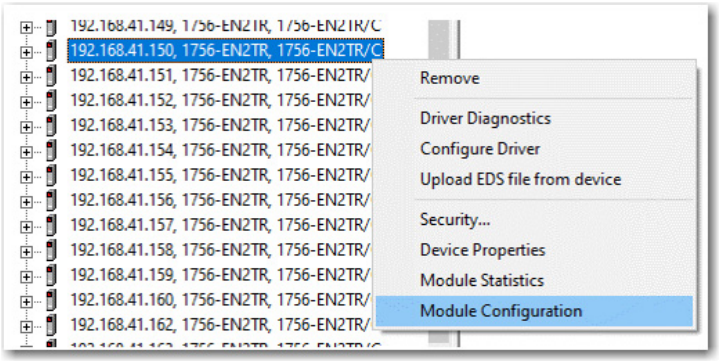
3. Configure supervisor parameters.



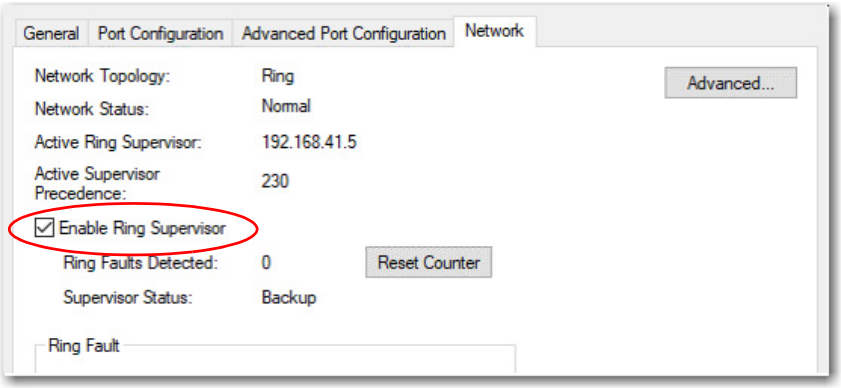
4. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Non-Stratix Ring Supervisor via RSLinx Classic

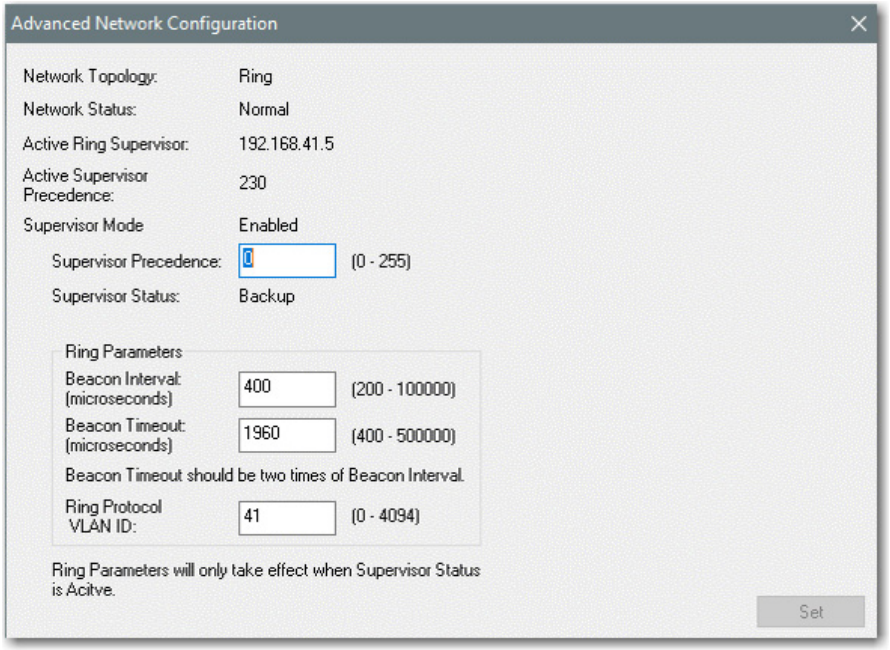
1. Access the configuration for the device.



2. Enable Supervisor mode.



3. Configure supervisor parameters.



4. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Stratix 5400 Configuration Examples

You can modify these Stratix 5400 examples to use with a DLR-capable Stratix 5700 switch by using one ring and one VLAN.

Configure Stratix 5400 Ring Supervisors

Use any of the following tools to configure a Stratix 5400 switch as a ring supervisor:

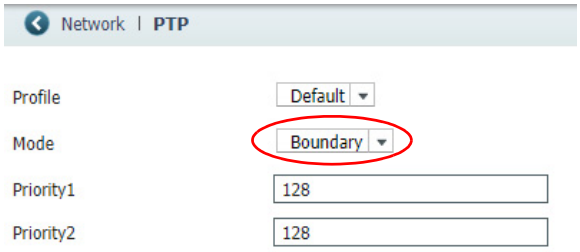
- Device Manager
- Logix Designer application
- Command-line interface (CLI)

Table 4 - Stratix Ring Supervisor Configuration Example

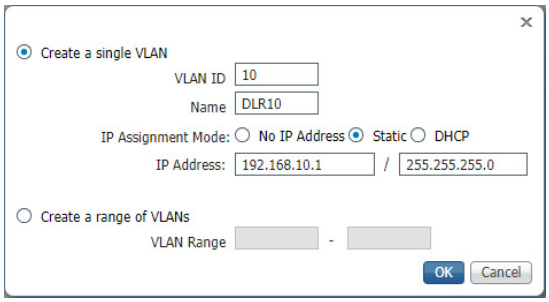
Switch	Ring	VLAN ID	IP Address	DLR Ports
Stratix 5400	1	10	192.168.10.1	Gi1/5, Gi1/6
	2	20	192.168.20.1	Gi1/7, Gi1/8
	3	30	192.168.30.1	Gi1/9, Gi1/10

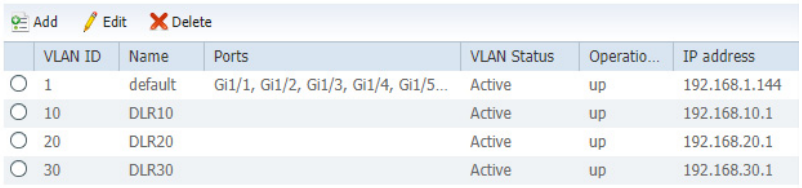
Stratix 5400 Ring Supervisor via Device Manager

1. Configure Precision Time Protocol (PTP) for Boundary mode.

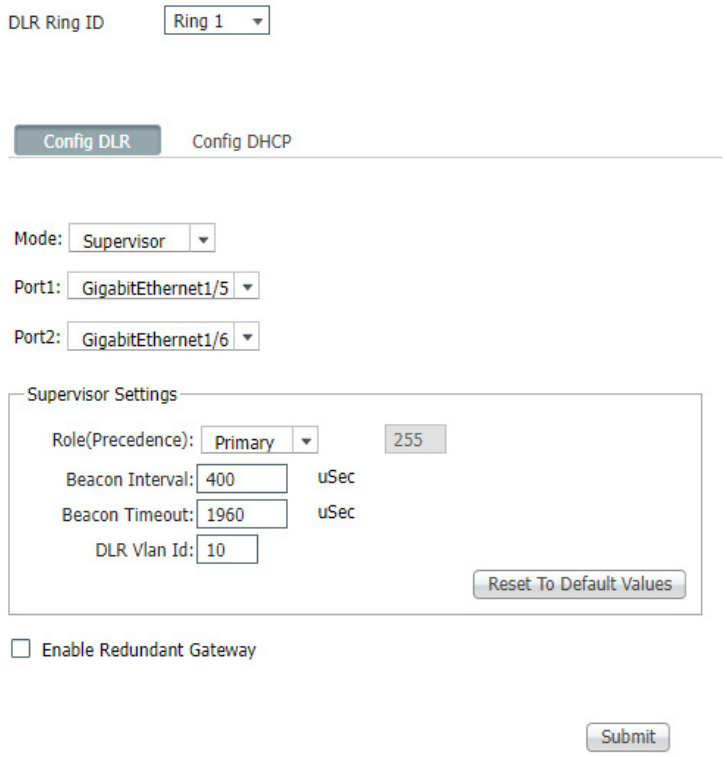


2. Create VLANs 10, 20, and 30 and assign each VLAN an IP address.

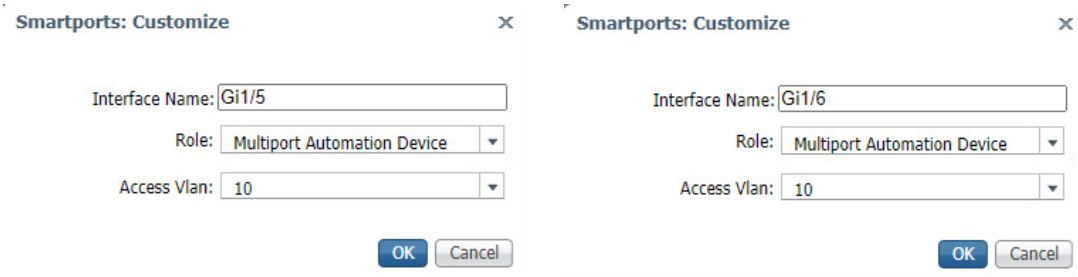




3. For each ring, enable Supervisor mode, select DLR ports, and configure primary or backup supervisor settings.



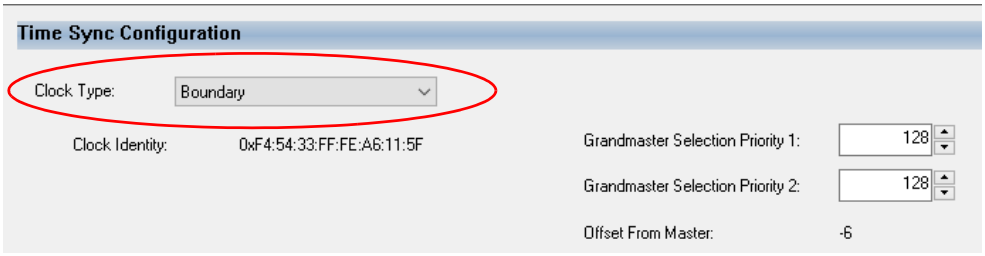
4. For each ring, apply the Multiport Automation Device Smartport role to DLR-enabled ports.



5. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

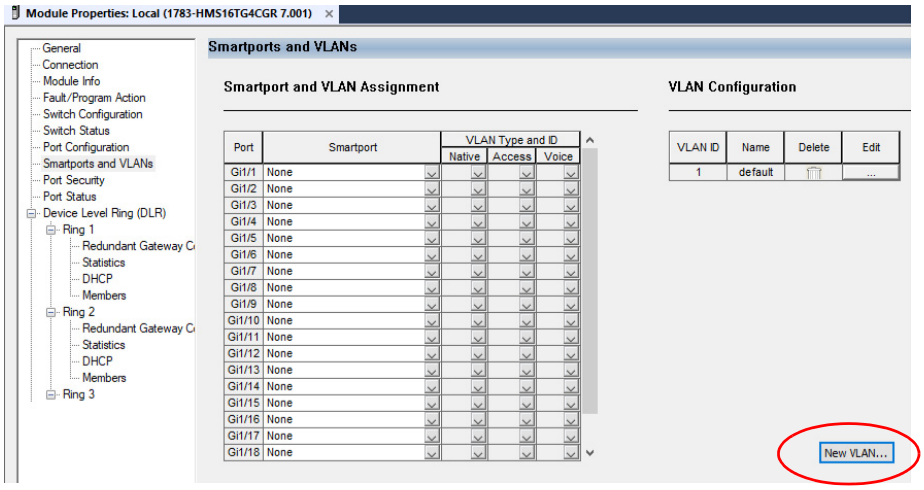
Stratix 5400 Ring Supervisor via Logix Designer Application

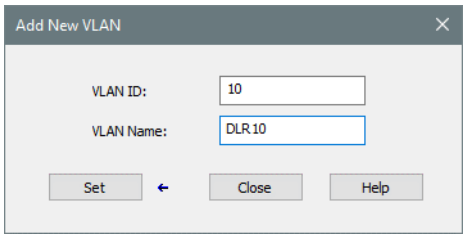
1. Configure Precision Time Protocol (PTP) for Boundary mode.

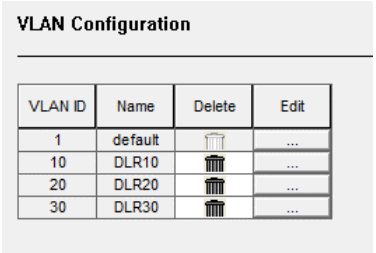


2. Create VLANs 10, 20, and 30.

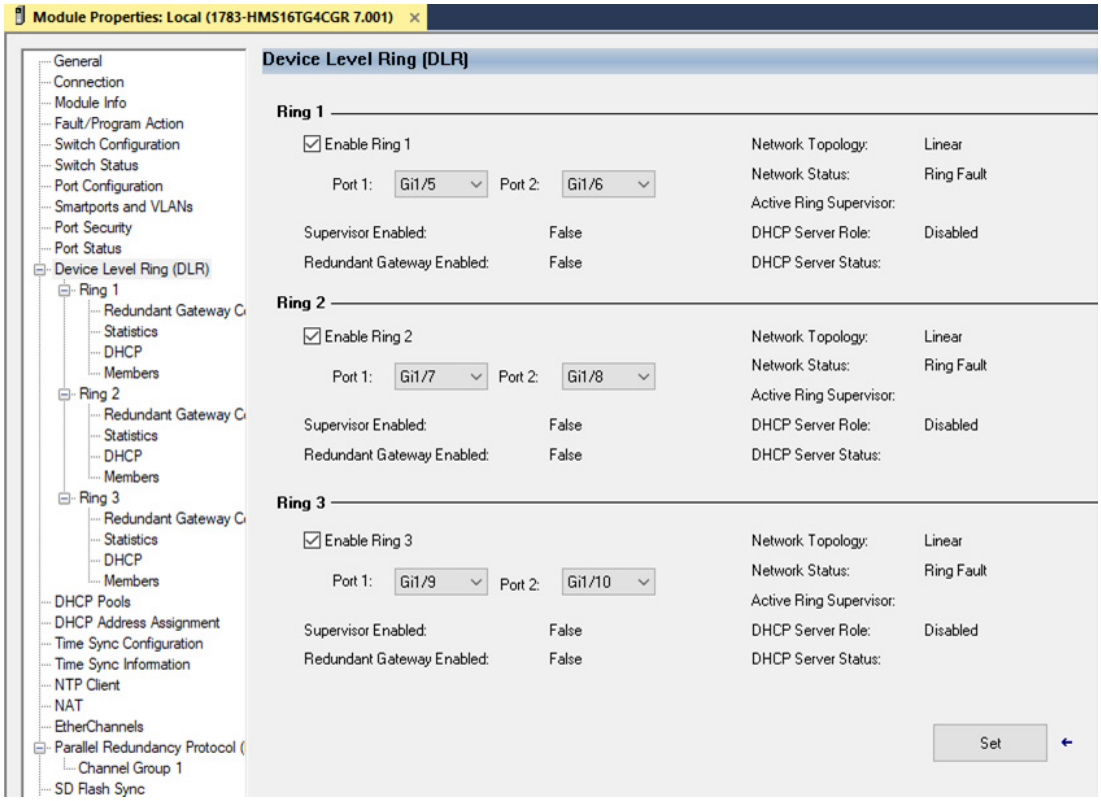
IMPORTANT To assign the VLAN an IP address, you must use Device Manager or the CLI.



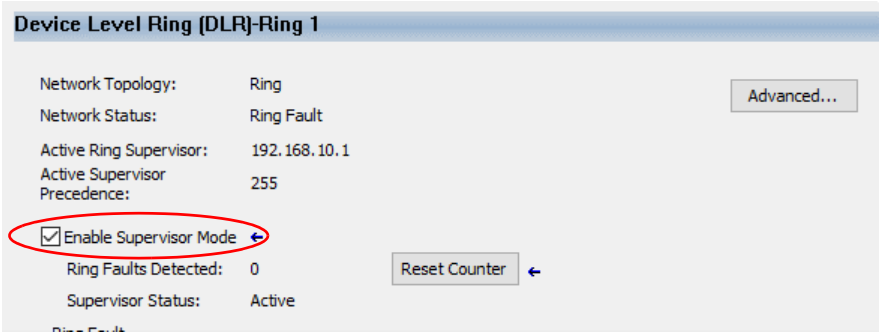




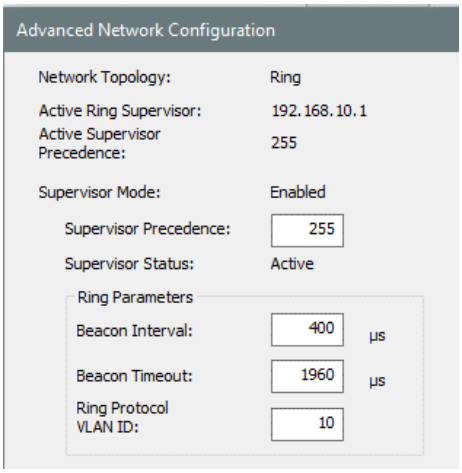
3. For each ring, enable DLR and select DLR ports.



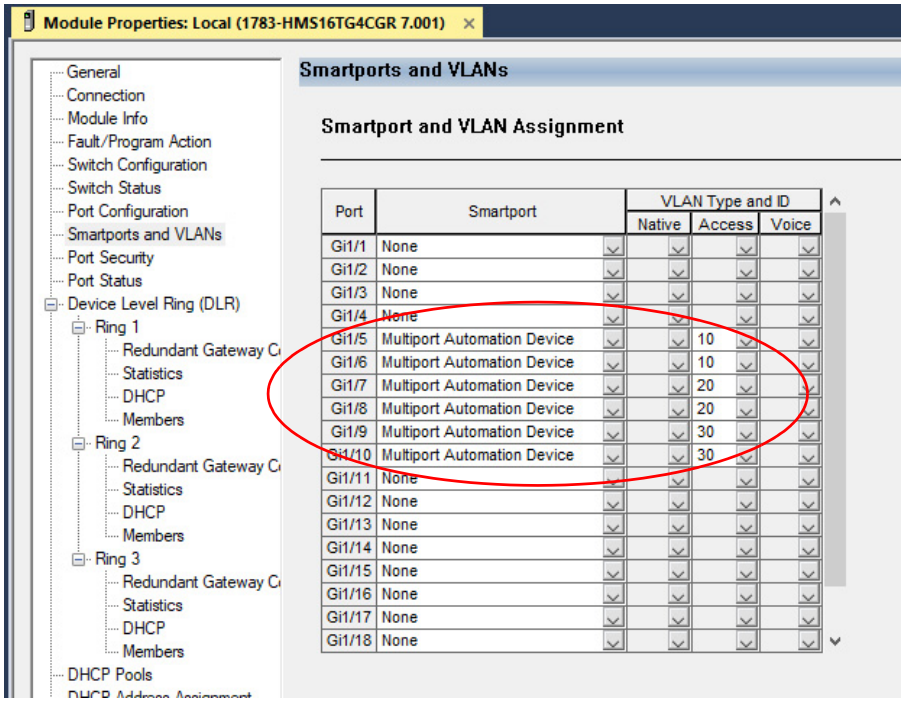
4. For each ring, enable Supervisor mode.



5. For each ring, configure primary or backup supervisor settings.



6. For each VLAN, apply the Multiport Automation Device Smartport role to DLR-enabled ports.



7. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Stratix 5400 Ring Supervisor via CLI

```
config t

ptp mode boundary

! Create VLANs 10, 20, and 30
VLAN 10
name DLR10

VLAN 20
name DLR20

VLAN 30
name DLR30

! Assign an IP address to VLANs 10, 20, and 30
interface VLAN 10
IP address 192.168.10.1 255.255.255.0
exit

interface VLAN 20
IP address 192.168.20.1 255.255.255.0
exit

interface VLAN 30
IP address 192.168.30.1 255.255.255.0
exit

! Configure primary or backup supervisor parameters
! Use precedence value 255 for a primary supervisor
! Use precedence value 100 or some other value for
! a backup Supervisor

DLR Ring 1
mode supervisor
control-vlan-ID 10
precedence 255
exit
exit

DLR Ring 2
mode supervisor
default beacon-interval
default beacon-timeout
control-vlan-ID 20
precedence 255
exit
exit

DLR Ring 3
mode supervisor
default beacon-interval
default beacon-timeout
control-vlan-ID 30
precedence 255
exit
exit

! Apply Smartport roles to DLR ports on each ring
interface range Gi1/5-6
macro apply ab-multiport-device $access_vlan 10
DLR Ring 1
ip dhcp snooping trust
exit

interface range Gi1/7-8
macro apply ab-multiport-device $access_vlan 20
DLR Ring 2
ip dhcp snooping trust
exit

interface range Gi1/9-10
macro apply ab-multiport-device $access_vlan 30
DLR Ring 3
ip dhcp snooping trust
exit
end
!
```

Proceed to the next step in your implementation.

See Stratix Switch Configuration Examples on page 47.

Configure Stratix 5400 Ring Participants

Use any of the following tools to configure a Stratix switch as a ring participant:

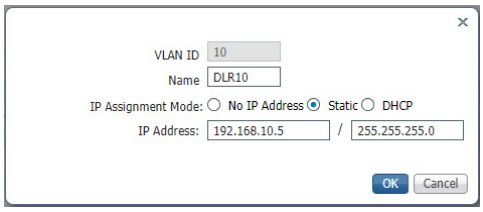
- Device Manager
- Logix Designer application
- Command-line interface (CLI)

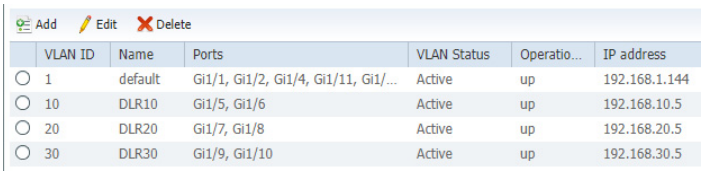
Table 5 - Stratix Ring Participant Configuration Example

Switch	Ring	VLAN ID	IP Address	DLR Ports
Stratix 5400	1	10	192.168.10.5	Gi1/5, Gi1/6
	2	20	192.168.20.5	Gi1/7, Gi1/8
	3	30	192.168.30.5	Gi1/9, Gi1/10

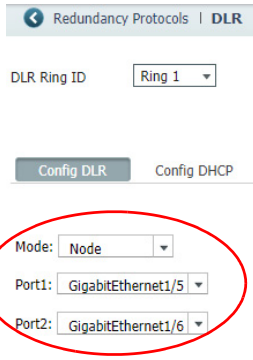
Stratix 5400 Ring Participant via Device Manager

1. Create VLANs 10, 20, and 30 and assign each VLAN an IP address.

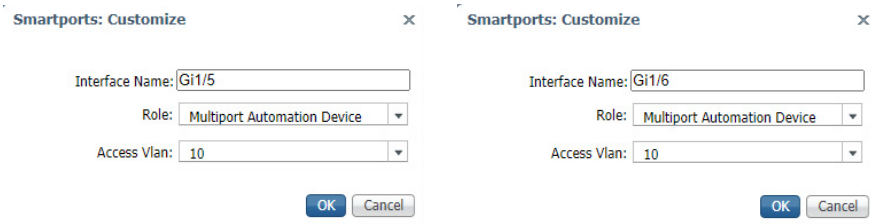




2. For each ring, enable Node mode and select DLR ports.



3. For each DLR-enabled port, apply the Multiport Automation Device Smartport.

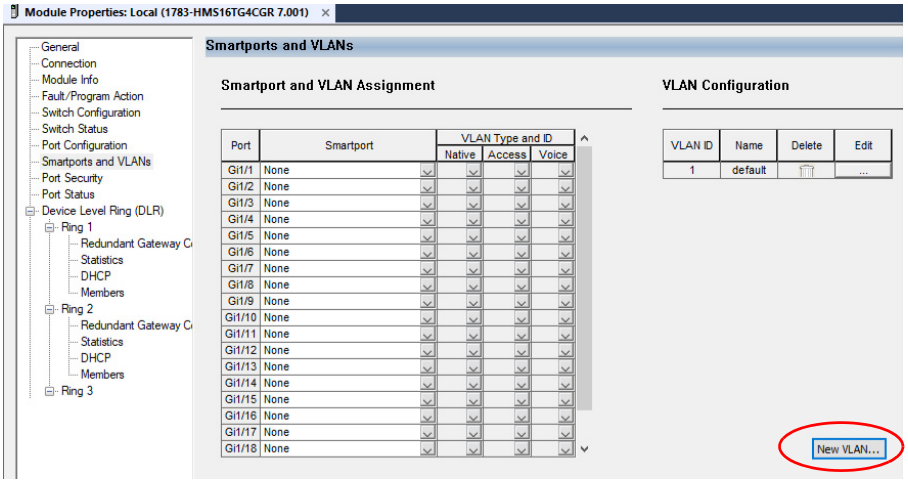


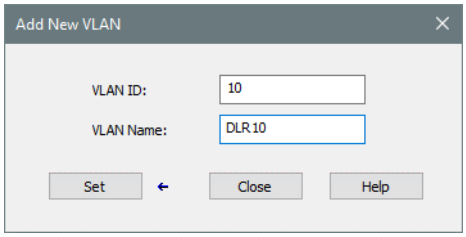
4. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

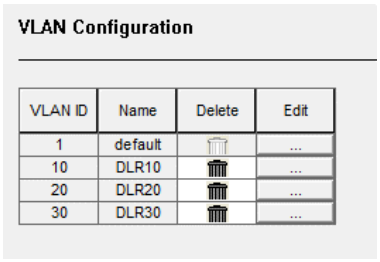
Stratix 5400 Ring Participant via Logix Designer Application

1. Create VLANs 10, 20, and 30.

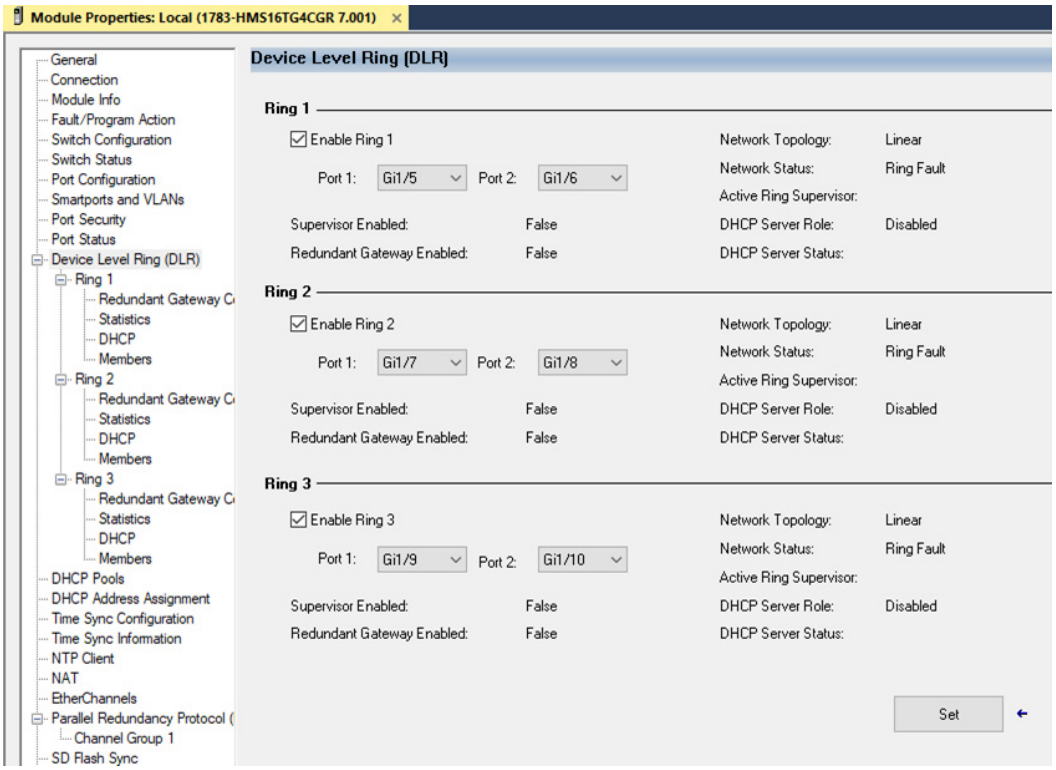
IMPORTANT To assign the VLAN an IP address, you must use Device Manager or the CLI.



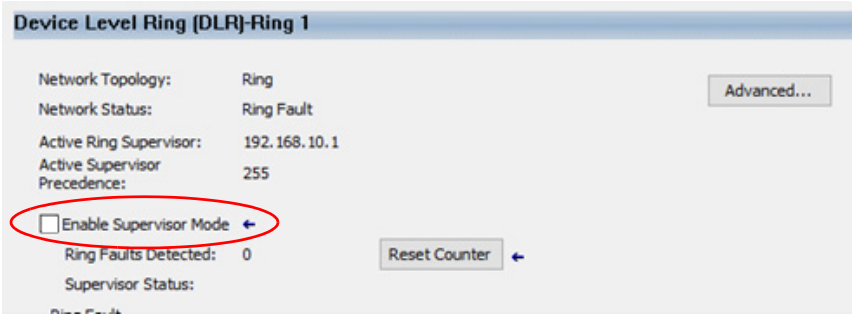




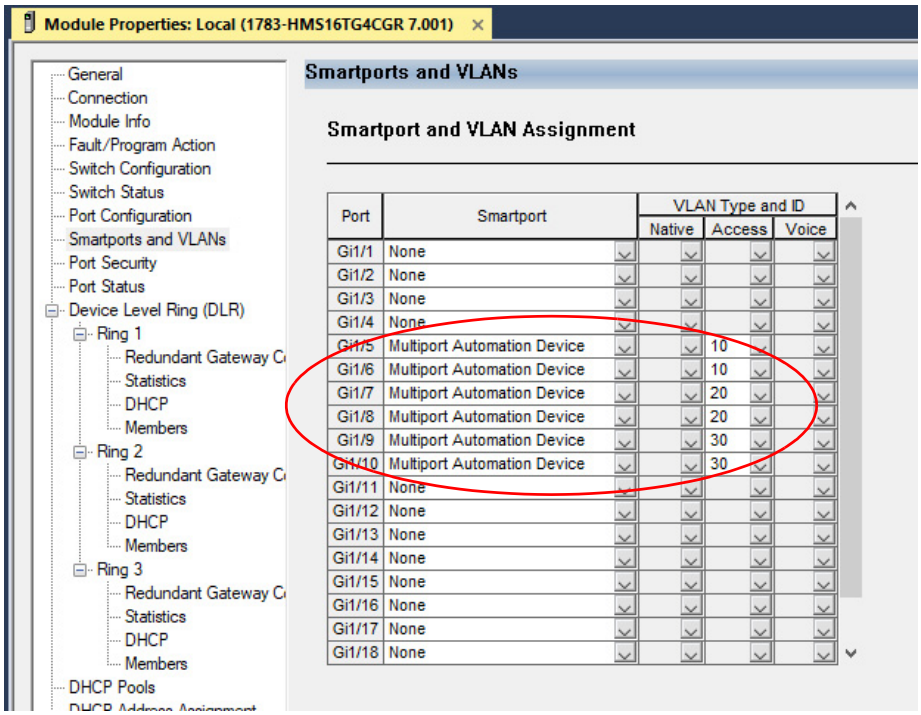
2. For each ring, enable DLR and select DLR ports.



3. For each ring, disable Supervisor mode.



4. For each VLAN, apply the Multiport Automation Device Smartport role to DLR-enabled ports.



5. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Stratix 5400 Ring Participant via CLI

```
config t

ptp mode boundary

! Create VLANs 10, 20, and 30
VLAN 10
name DLR10

VLAN 20
name DLR20

VLAN 30
name DLR30

! Assign an IP address to each VLAN
interface VLAN 10
IP address 192.168.10.5 255.255.255.0
exit

interface VLAN 20
IP address 192.168.20.5 255.255.255.0
exit

interface VLAN 30
IP address 192.168.30.5 255.255.255.0
exit

! Configure DLR parameters for each ring

DLR Ring 1
mode beacon-node
exit

DLR Ring 2
mode beacon-node
exit

DLR Ring 3
mode beacon-node
exit

! Apply Smartport roles for DLR ports on each ring
interface range Gi1/5-6
macro apply ab-multiport-device $access_vlan 10
DLR Ring 1
ip dhcp snooping trust
exit

interface range Gi1/7-8
macro apply ab-multiport-device $access_vlan 20
DLR Ring 2
ip dhcp snooping trust
exit

interface range Gi1/9-10
macro apply ab-multiport-device $access_vlan 30
DLR Ring 3
ip dhcp snooping trust
exit
end
!
```

Proceed to the next step in your implementation.

See Stratix Switch Configuration Examples on page 47.

Configure Stratix 5400 Redundant Gateways

Use any of the following tools to configure a Stratix switch as a redundant gateway:

- Device Manager
- Logix Designer application
- Command line interface (CLI)

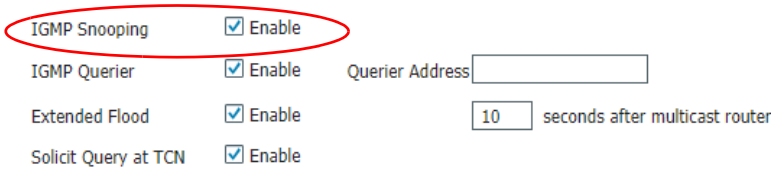
Table 6 - Redundant Gateway Configuration Example

Switch	Ring	VLAN ID	IP Address	DLR Ports	Uplink Ports
Stratix 5400	1	10	192.168.10.1	Gi1/5, Gi1/6	Gi1/1, Gi1/2
	2	20	192.168.20.1	Gi1/7, Gi1/8	
	3	30	192.168.30.1	Gi1/9, Gi1/10	

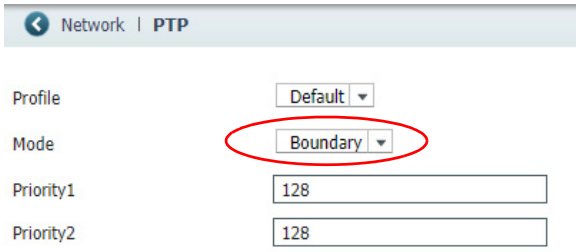
Stratix 5400 Redundant Gateway via Device Manager

1. Enable IGMP snooping.

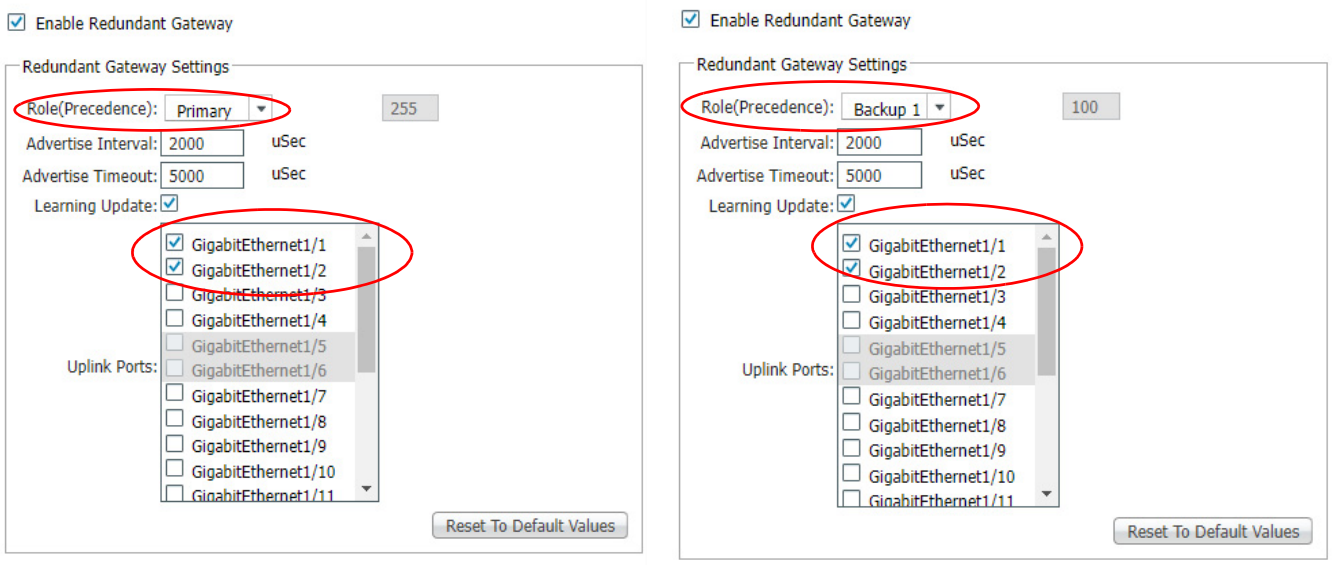
IMPORTANT To determine whether to enable Extended Flood or Solicit Query at TCN, see Multicast Traffic and Redundant Gateways on page 24.



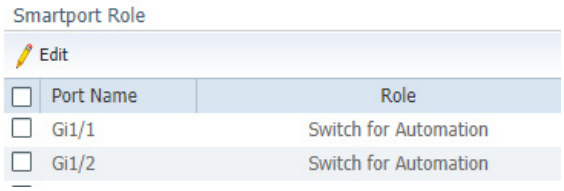
2. Verify that PTP Boundary mode is enabled.



3. For each ring, enable and configure a primary or backup redundant gateway.



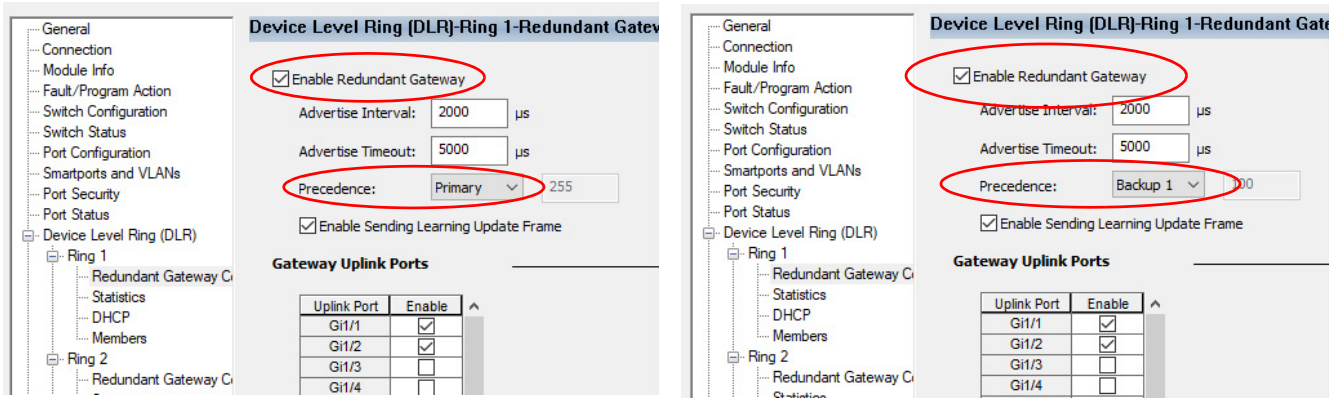
4. For each uplink port, apply the Switch for Automation Smartport role.



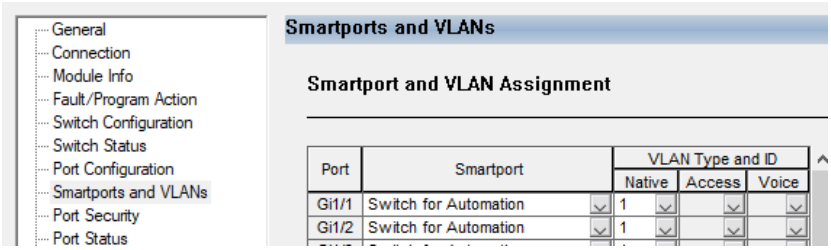
5. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Stratix 5400 Redundant Gateway via Logix Designer Application

1. For each ring, enable and configure a primary or backup redundant gateway.



2. For each uplink port, apply the Switch for Automation Smartport role.



3. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Stratix 5400 Redundant Gateway via CLI

```
config t

! Configure IGMP snooping
ip igmp snooping mrouter-ext-flood 10
ip igmp snooping tcn query solicit

! Configure ptp boundary mode
ptp mode boundary

! Enable and configure a primary or
! backup redundant gateway for each ring
! Use precedence value 255 for a primary gateway
! Use precedence value 100 or some other value
! for a backup gateway

DLR ring 1
gateway enable
default advertise-interval
default advertise-timeout
gateway-precedence 255
exit
exit

DLR ring 2
gateway enable
default advertise-interval
default advertise-timeout
gateway-precedence 255
exit
exit

DLR ring 3
gateway enable
default advertise-interval
default advertise-timeout
gateway-precedence 255
exit
exit

! Configure the uplink ports for each ring
interface range Gi1/1-2
dlr ring 1 uplink
dlr ring 2 uplink
dlr ring 3 uplink
macro apply switch-automation $native_vlan 1
exit
end
!
```

Proceed to the next step in your implementation.

See Stratix Switch Configuration Examples on page 47.

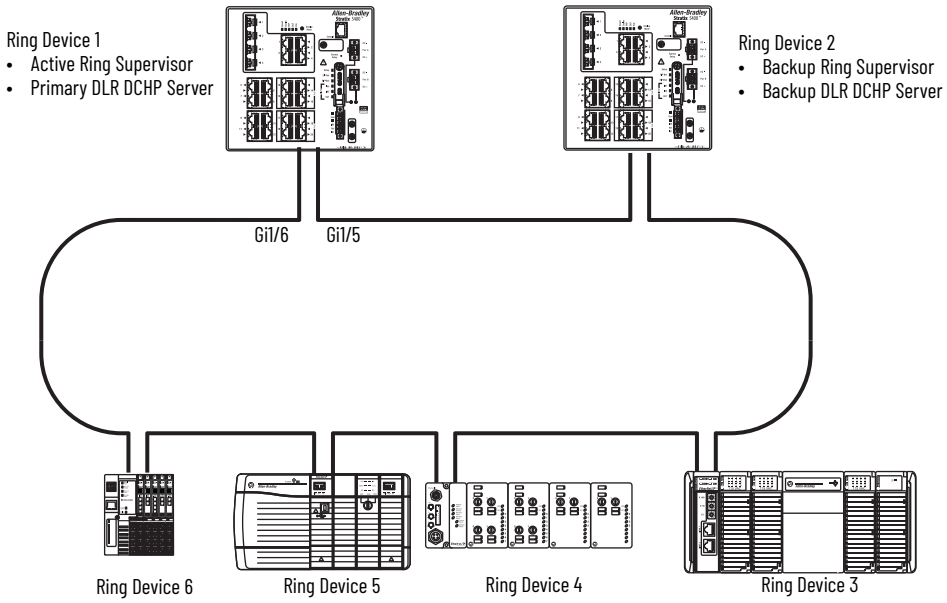
Configure DLR DHCP on a Stratix 5400 Switch

Use any of the following tools to configure DLR DHCP:

- Device Manager
- Logix Designer application
- Command-line interface (CLI)

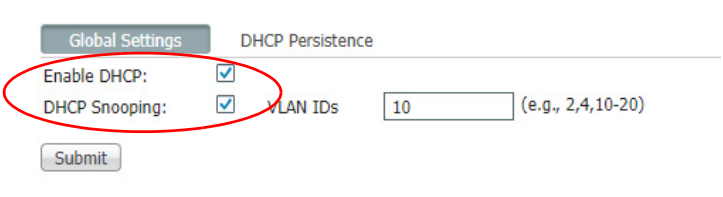
Table 7 - DLR DHCP Example

Ring Device Index	IP Address	Host Name	DHCP Pool
2	Not applicable	Not applicable	Not applicable
3	192.168.10.100	Device_10_100	DLR_DHCP_POOL
4	192.168.10.101	Device_10_101	DLR_DHCP_POOL
5	Not applicable	Not applicable	Not applicable
6	192.168.10.103	Device_10_103	DLR_DHCP_POOL

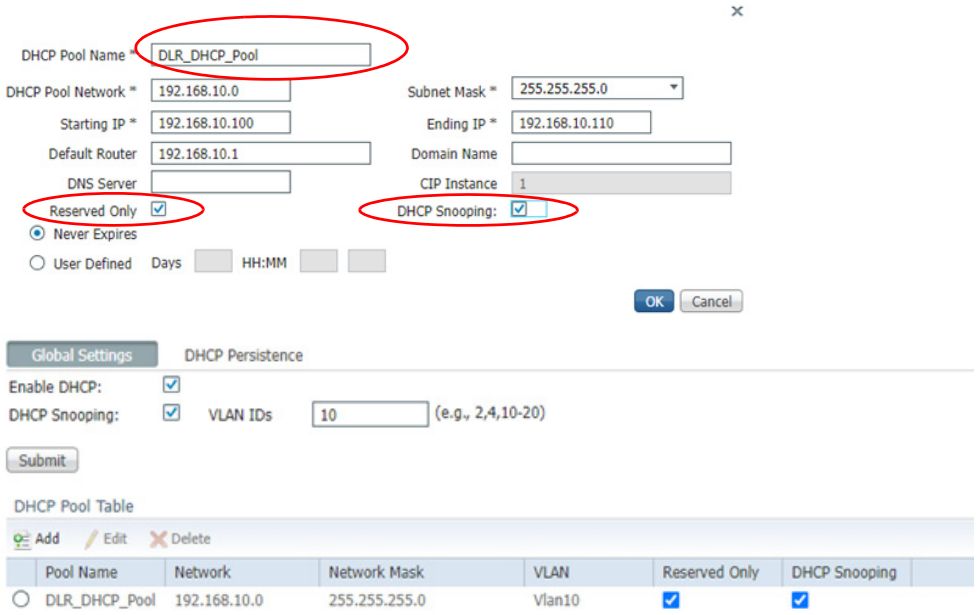


DLR DHCP on a Stratix 5400 Switch via Device Manager

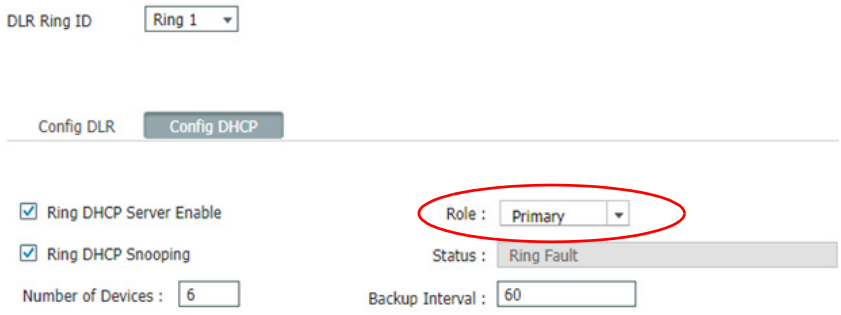
1. Enable DHCP and DHCP Snooping.



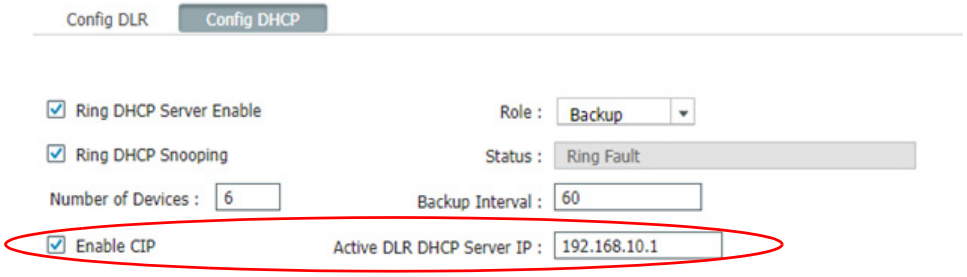
2. Configure a DHCP pool for ring devices.
   Select Reserved Only and DHCP Snooping.



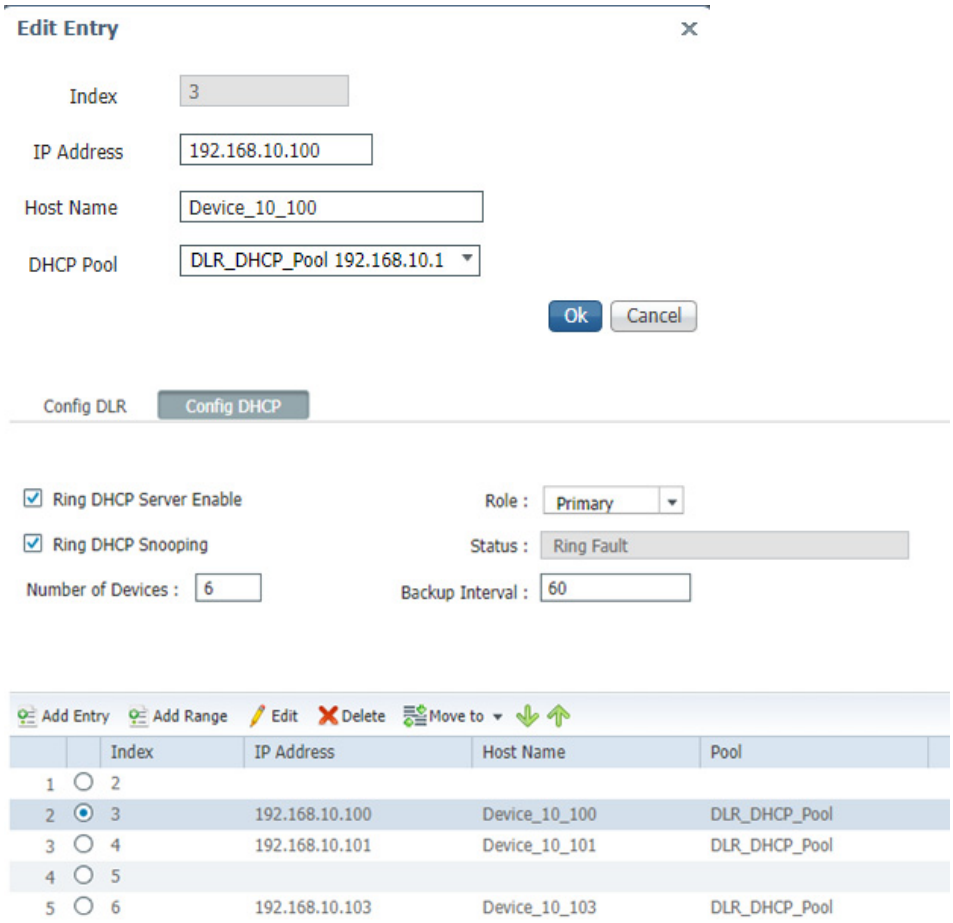
3. Configure the switch as a primary or backup DLR DHCP server.



For a **backup** configuration, you must select Enable CIP™ and enter the IP address of the primary DLR DHCP server. These settings enable the backup server to receive the DHCP configuration from the primary server if a switchover occurs.



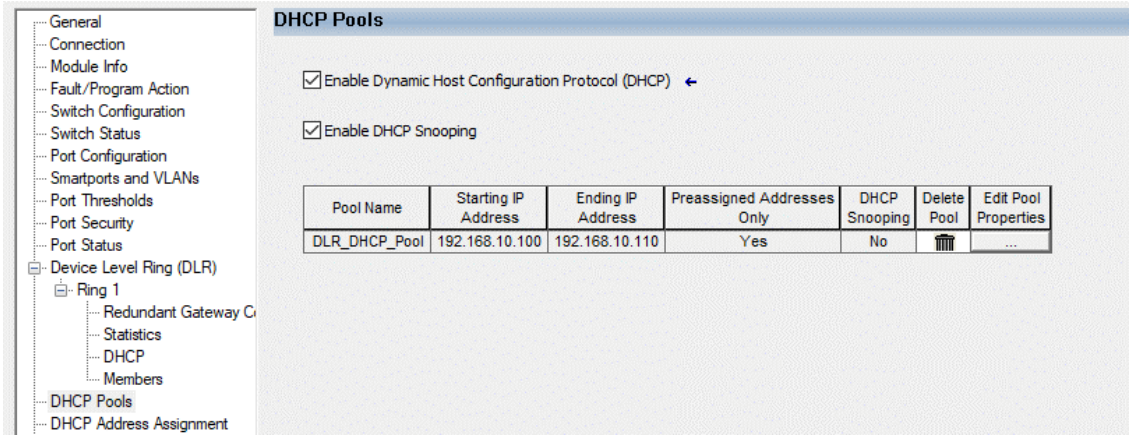
4. For each device on Ring 1, add entries to the index table and assign IP addresses to each entry, except for entries 2 and 5. In this example, entries 2 and 5 have static IP addresses.



5. Proceed to the next step in your implementation.
See Stratix Switch Configuration Examples on page 47.

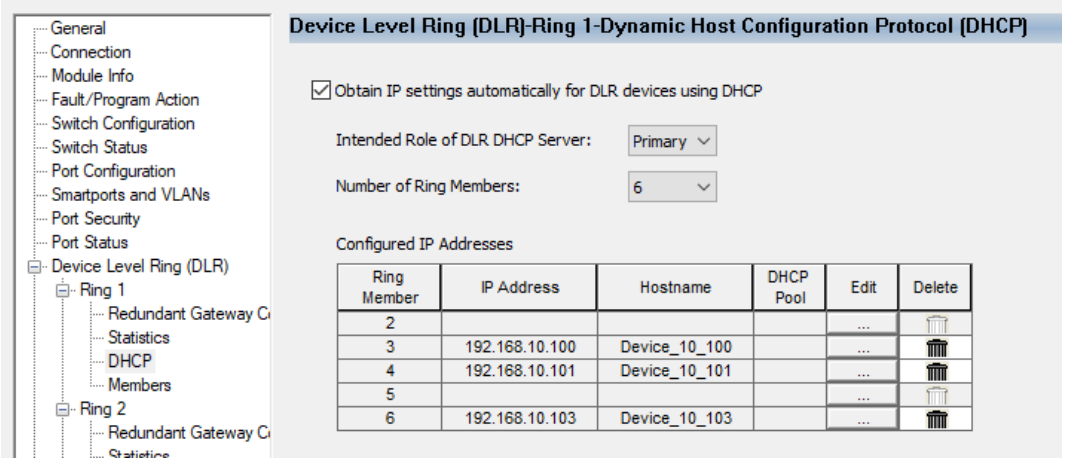
DLR DHCP on a Stratix 5400 Switch via Logix Designer Application

1. Configure DLR DHCP:
   - Enable DHCP
   - Enable DHCP Snooping
   - Create a DHCP pool for ring devices



2. Configure the switch as a primary or backup DLR DHCP server.

   For each device on Ring 1, add entries to the index table and assign IP addresses to each entry, except for entries 2 and 5. In this example, entries 2 and 5 have static IP addresses.



3. Proceed to the next step in your implementation.

   See Stratix Switch Configuration Examples on page 47.

DLR DHCP on a Stratix 5400 Switch via CLI

Primary DHCP Server

```
config t

! Exclude the ring devices with static IP addresses

ip dhcp excluded-address 192.168.10.0 192.168.10.99
ip dhcp excluded-address 192.168.10.111 192.168.10.255

! Configure an IP address pool
ip dhcp pool DLR_DHCP_Pool
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
lease infinite
reserved-only
cip instance 1

! Enable DHCP snooping
ip dhcp snooping vlan 10
ip dhcp snooping

! Configure the switch as a primary DLR DHCP server
dlr ring 1
ring-dhcp
snooping enable
dhcp-server enable
intended-role primary
number-of-devices 6

! Assign IP addresses to devices in the DLR DHCP address pool.
entry 3 add 192.168.10.100 DLR_DHCP_Pool Device_10_100
entry 4 add 192.168.10.101 DLR_DHCP_Pool Device_10_101
entry 6 add 192.168.10.103 DLR_DHCP_Pool Device_10_103

exit
exit
end
!
```

Backup DHCP Server

```
config t

! Exclude the ring devices with static IP addresses
ip dhcp excluded-address 192.168.10.0 192.168.10.99
ip dhcp excluded-address 192.168.10.111 192.168.10.255

! Configure an IP address pool
ip dhcp pool DLR_DHCP_Pool
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
lease infinite
reserved-only
cip instance 1

! Enable DHCP snooping
ip dhcp snooping vlan 10
ip dhcp snooping

! Configure the switch as a backup DLR DHCP server
dlr ring 1
ring-dhcp
snooping enable
dhcp-server enable
intended-role backup
active-cip-addr 192.168.10.1
number-of-devices 6

exit
exit
end
!
```

Proceed to the next step in your implementation.

See Stratix Switch Configuration Examples on page 47.

Configure VLAN Trunking on a Stratix 5400 Switch

Use any of the following tools to configure VLAN trunking:

- Device Manager
- Command line interface (CLI)

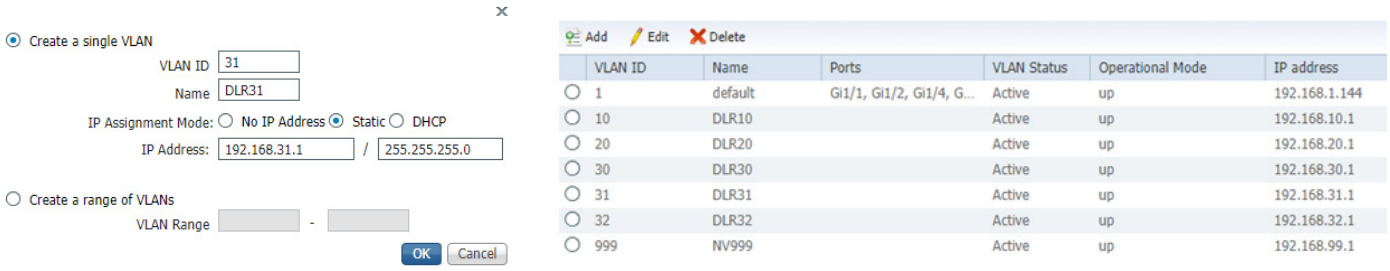
This example shows how to configure DLR VLAN trunking on Ring 3 and assumes that Ring 1 and Ring 2 are already configured for one VLAN.

Table 8 - VLAN Trunking Configuration Example

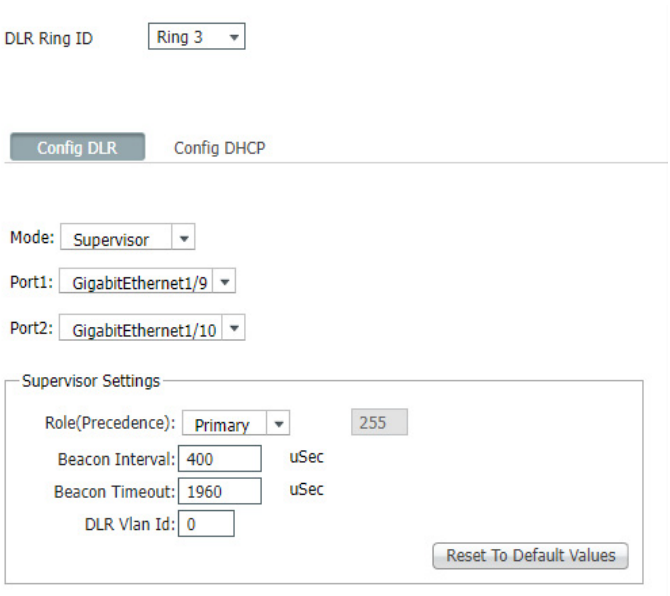
Switch	Ring	VLAN	IP Address	DLR Ports
Stratix 5400	1	10	192.168.10.1	Gi1/5, Gi1/6
	2	20	192.168.20.1	Gi1/7, Gi1/8
	3	Trunk 30, 31, 32, 999	Multiple, native VLAN 192.169.99.1	Gi1/9, Gi1/10

VLAN Trunking on a Stratix 5400 Switch via Device Manager

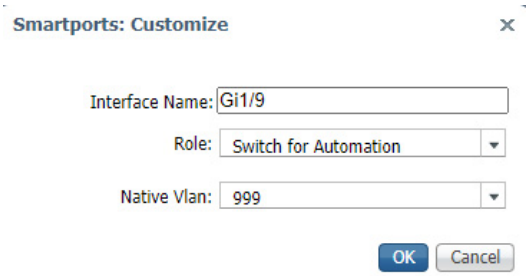
1. To configure Rings 1 and 2 with single VLANs, follow the steps for Implementation C, as shown on page 47.
2. Create VLANs 30, 31, 32, and 999 and assign each VLAN a static IP address.
   Assigning an IP address to the native VLAN is not required, but recommended for diagnostic purposes.

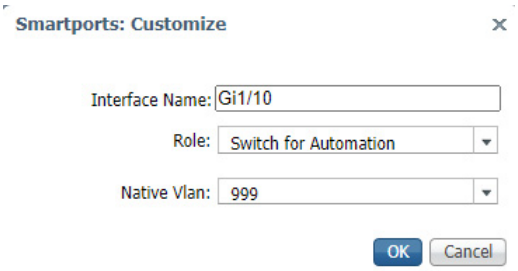


3. For Ring 3, do the following:
   - Enable Supervisor mode.
   - Enable DLR on two DLR-capable switch ports.
   - Configure primary or backup supervisor parameters.

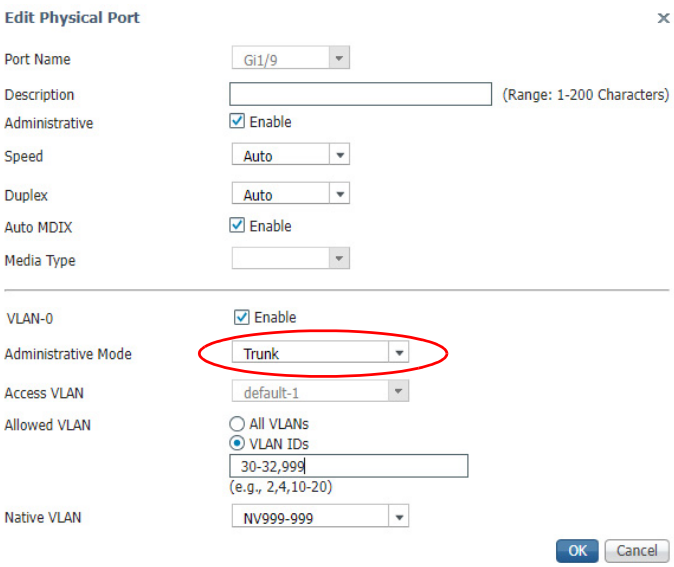


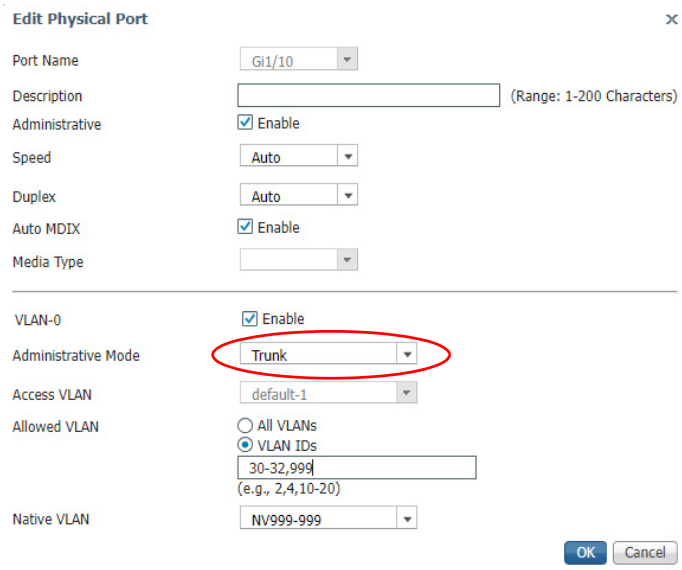
4. For Ring 3, apply the Switch for Automation Smartport role to DLR-enabled ports.





5. For Ring 3, configure VLAN trunking on DLR-enabled ports.





6. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

VLAN Trunking on a Stratix 5400 Switch via CLI

```
config t

!create VLANs for Ring 3 and assign addresses
VLAN 30
name DLR30

VLAN 31
name DLR31

VLAN 32
name DLR32

VLAN 999
name NV999

interface VLAN 30
IP address 192.168.30.1 255.255.255.0
exit

interface VLAN 31
IP address 192.168.31.1 255.255.255.0
exit

interface VLAN 32
IP address 192.168.32.1 255.255.255.0
exit

interface VLAN 999
IP Address 192.168.99.1 255.255.255.0
exit

! configure supervisor settings for Ring 3
! for backup use precedence 100
DLR Ring 3
mode supervisor
default beacon-interval
default beacon-timeout
control-vlan-ID 30
precedence 255
exit
exit

!configure VLAN trunking on Ring 3
interface range Gi1/9-10
macro apply switch-automation $native_vlan 999
switchport trunk allowed vlan 30,31,32,999
DLR Ring 3
ip dhcp snooping trust
exit

end
!
```

Proceed to the next step in your implementation.

See Stratix Switch Configuration Examples on page 47.

Stratix 5800 Configuration Examples

DLR configuration for Stratix 5800 switches requires IOS release 17.12.01 or later.

You can modify these Stratix 5800 examples to use with a DLR-capable Stratix 5200 switch.

Configure Stratix 5800 Ring Supervisors

Use any of the following tools to configure a Stratix 5800 switch as a ring supervisor:

- Device Manager
- Command-line interface (CLI)

DLR configuration via the Logix Designer application will be available in a future release.

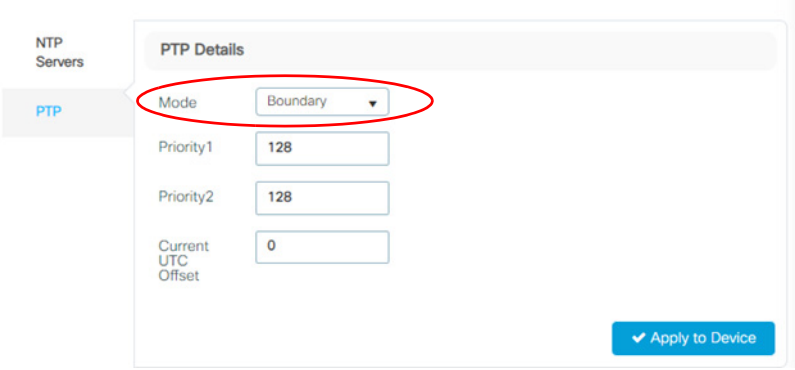
Table 9 - Stratix Ring Supervisor Configuration Example

Switch	Ring	VLAN ID	IP Address	DLR Ports
Stratix 5800	1	10	192.168.10.1	Gi1/5, Gi1/6
	2	20	192.168.20.1	Gi1/7, Gi1/8

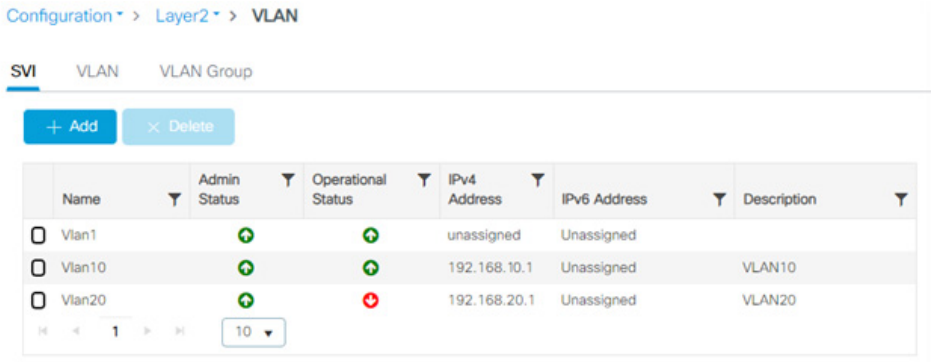
IMPORTANT Stratix 5800 switches support as many as three rings with the third ring only on the expansion module. Ring 3 configuration is not a part of this example.

Stratix 5800 Ring Supervisor via WebUI

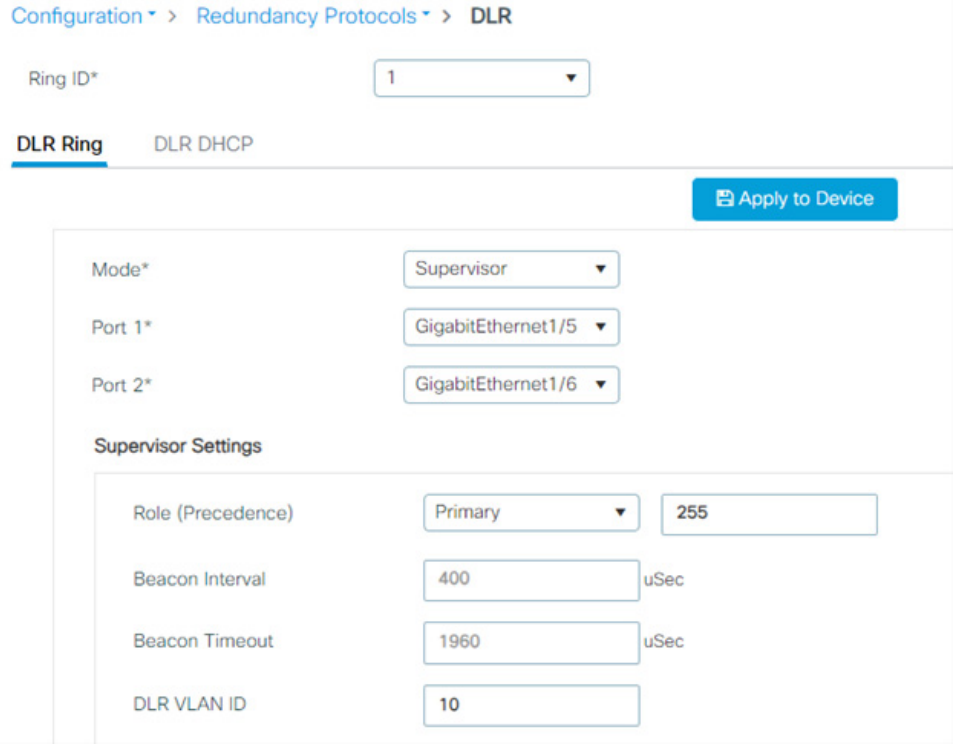
1. Configure Precision Time Protocol (PTP) for Boundary mode.



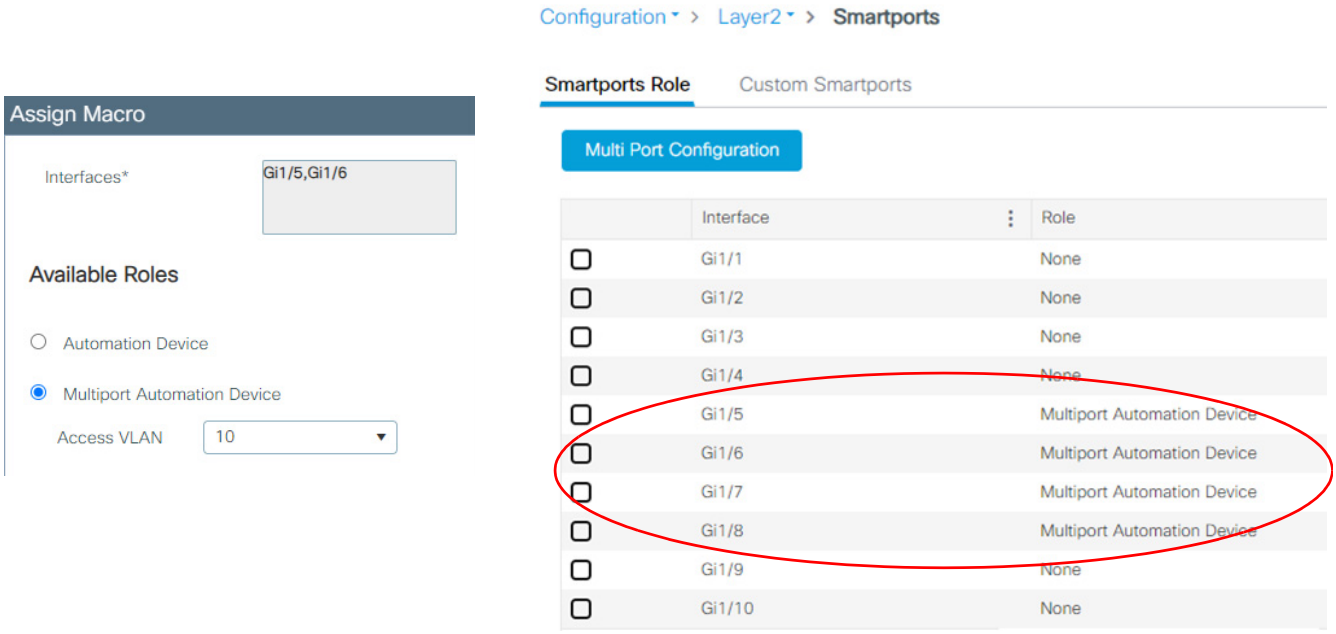
2. Create VLANs 10 and 20 and assign each VLAN an IP address.



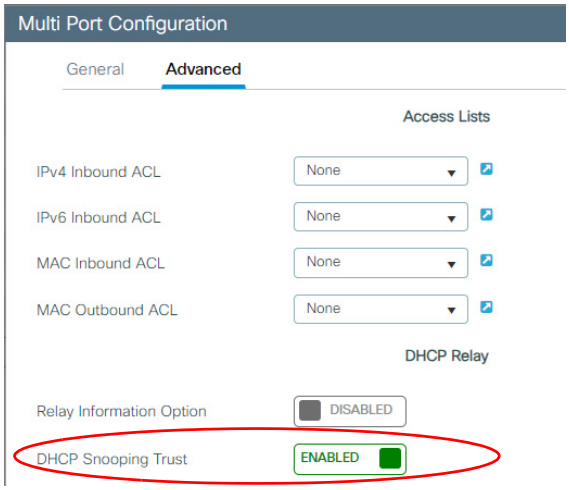
3. For each ring, enable Supervisor mode, select DLR ports, and configure primary or backup supervisor settings.



4. For each VLAN, apply the Multiport Automation Device Smartport role to DLR-enabled ports.



5. For each DLR-enabled port, enable DHCP Snooping Trust.



6. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Stratix 5800 Ring Supervisor via CLI

```
config t
ptp mode boundary

! Create VLANs 10, 20
VLAN 10
name DLR10
VLAN 20
name DLR20

! Assign an IP address to VLANs 10 and 20
interface VLAN 10
IP address 192.168.10.1 255.255.255.0
exit
interface VLAN 20
IP address 192.168.20.1 255.255.255.0
exit

! Configure primary or backup supervisor parameters
! Use precedence value 255 for a primary supervisor
! Use precedence value 100 or some other value for
! a backup Supervisor
DLR Ring 1
mode supervisor
control-vlan-ID 10
precedence 255
exit
exit
DLR Ring 2
mode supervisor
default beacon-interval
default beacon-timeout
control-vlan-ID 20
precedence 255
exit
exit

! Apply Smartport roles to DLR ports on each ring
interface range Gi1/5-6
macro apply ab-multiport-device $access_vlan 10
DLR Ring 1
ip dhcp snooping trust
exit
interface range Gi1/7-8
macro apply ab-multiport-device $access_vlan 20
DLR Ring 2
ip dhcp snooping trust
exit
end
!
```

Configure Stratix 5800 Ring Participants

Use any of the following tools to configure a Stratix switch as a ring participant:

- Device Manager
- Command-line interface (CLI)

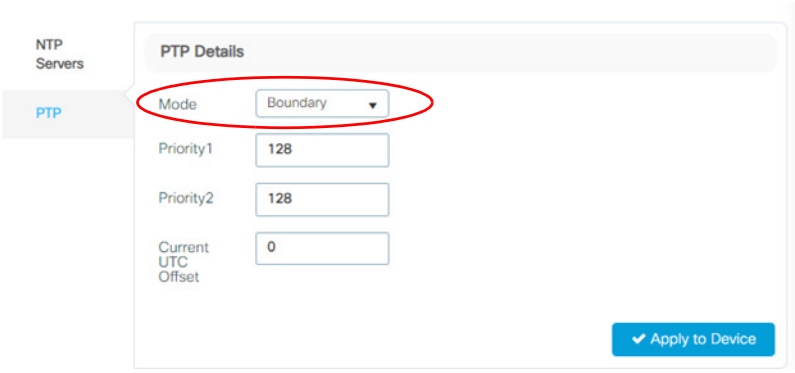
DLR configuration via the Logix Designer application will be available in a future release.

Table 10 - Stratix Ring Participant Configuration Example

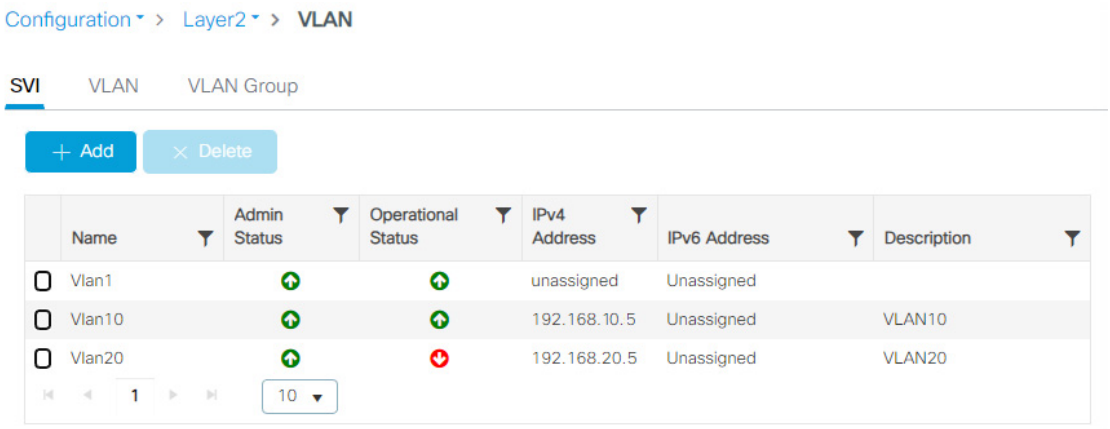
Switch	Ring	VLAN ID	IP Address	DLR Ports
Stratix 5800	1	10	192.168.10.5	Gi1/5, Gi1/6
	2	20	192.168.20.5	Gi1/7, Gi1/8

Stratix 5800 Ring Participant via WebUI

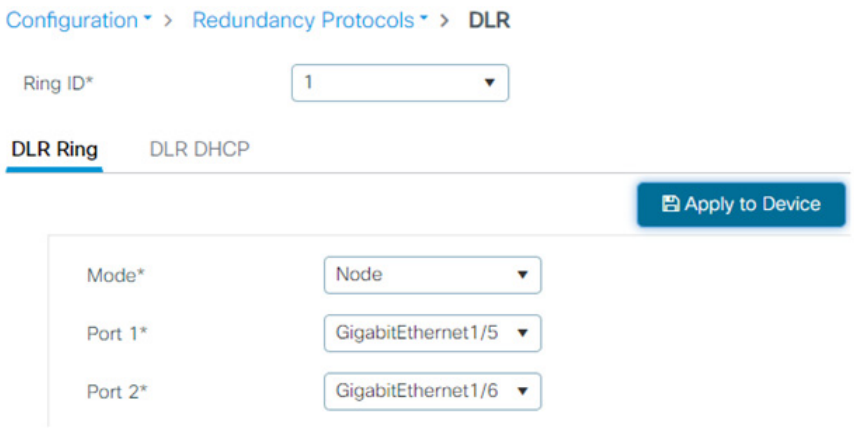
1. Configure Precision Time Protocol (PTP) for Boundary mode.



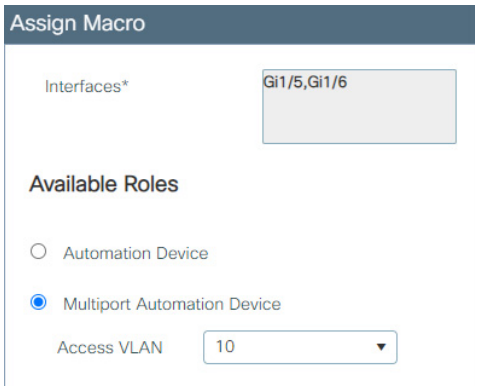
2. Create VLANs 10 and 20 and assign each VLAN an IP address.

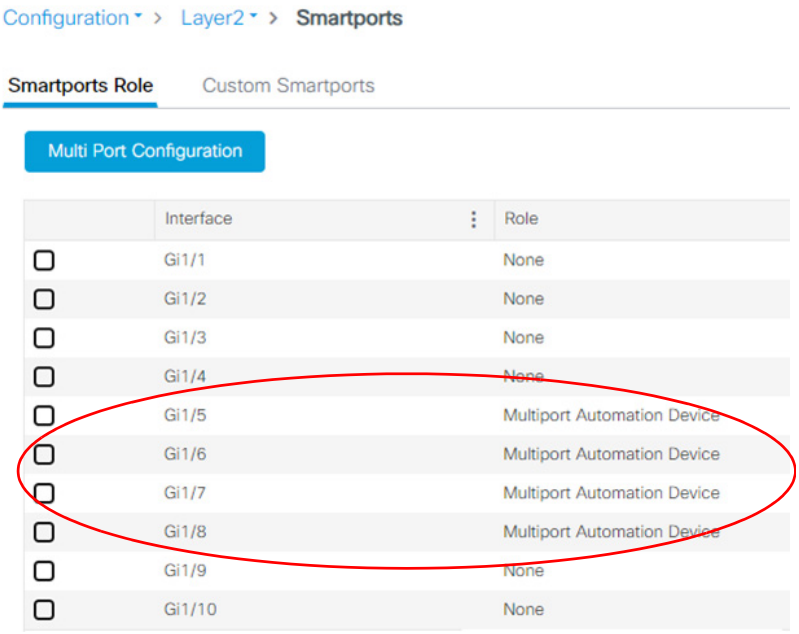


3. For each ring, enable Node mode and select DLR ports.



4. For each VLAN, apply the Multiport Automation Device Smartport role to DLR-enabled ports.





5. Proceed to the next step in your implementation.
See Stratix Switch Configuration Examples on page 47.

Stratix 5800 Ring Participant via CLI

```
config t
ptp mode boundary

! Create VLANs 10 and 20
VLAN 10
name DLR10
VLAN 20
name DLR20

! Assign an IP address to each VLAN
interface VLAN 10
IP address 192.168.10.5 255.255.255.0
exit
interface VLAN 20
IP address 192.168.20.5 255.255.255.0
exit

! Configure DLR parameters for each ring
DLR Ring 1
mode beacon-node
exit
DLR Ring 2
mode beacon-node
exit

! Apply Smartport roles for DLR ports on each ring
interface range Gi1/5-6
macro apply ab-multiport-device $access_vlan 10
DLR Ring 1
ip dhcp snooping trust
exit
interface range Gi1/7-8
macro apply ab-multiport-device $access_vlan 20
DLR Ring 2
ip dhcp snooping trust
exit
end
!
```

Configure Stratix 5800 Redundant Gateways

Use any of the following tools to configure a Stratix switch as a redundant gateway:

- Device Manager
- Command line interface (CLI)

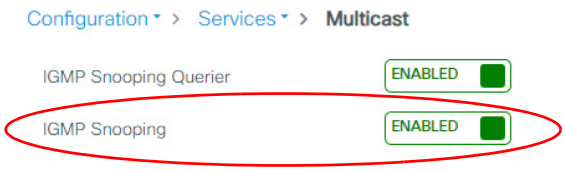
DLR configuration via the Logix Designer application will be available in a future release.

Table 11 - Redundant Gateway Configuration Example

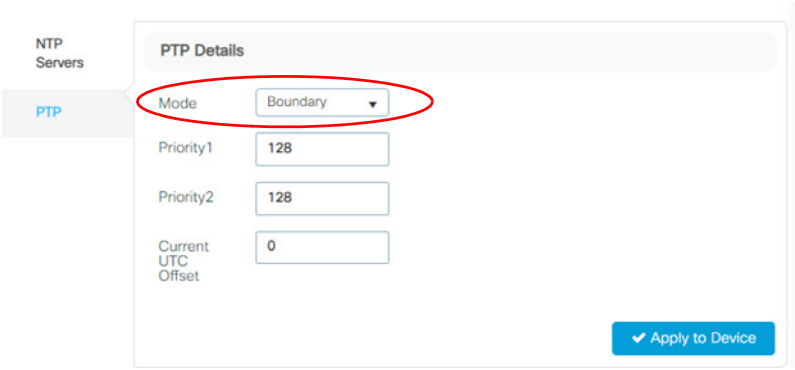
Switch	Ring	VLAN ID	IP Address	DLR Ports	Uplink Ports
Stratix 5800	1	10	192.168.10.1	Gi1/5, Gi1/6	Gi1/1, Gi1/2
	2	20	192.168.20.1	Gi1/7, Gi1/8	

Stratix 5800 Redundant Gateway via Device Manager

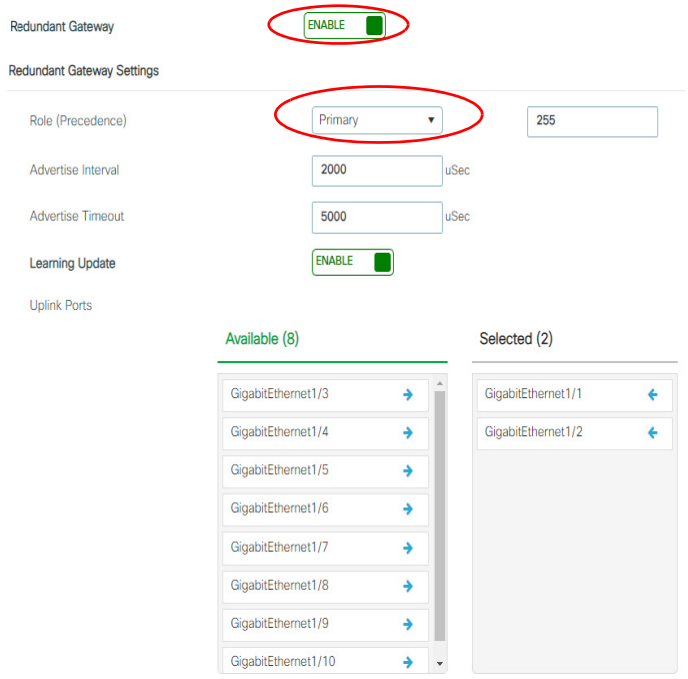
1. Enable IGMP snooping.

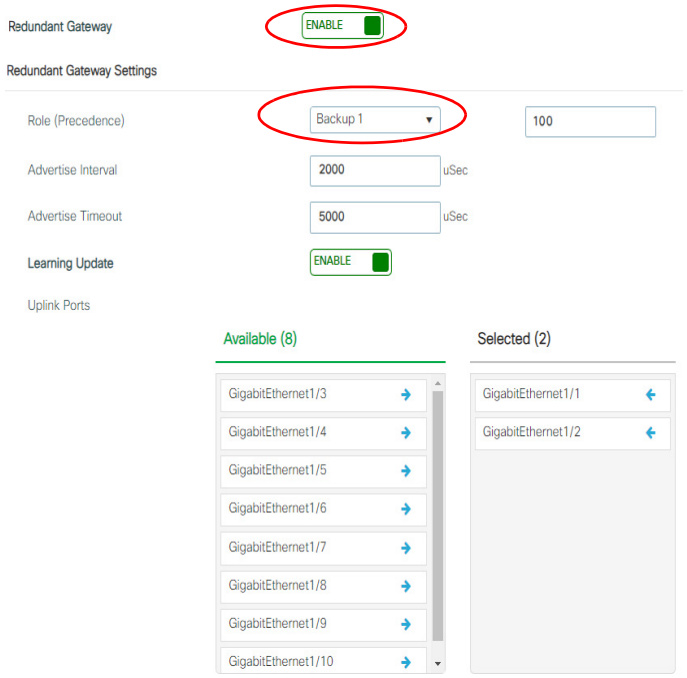


2. Verify that PTP Boundary mode is enabled.

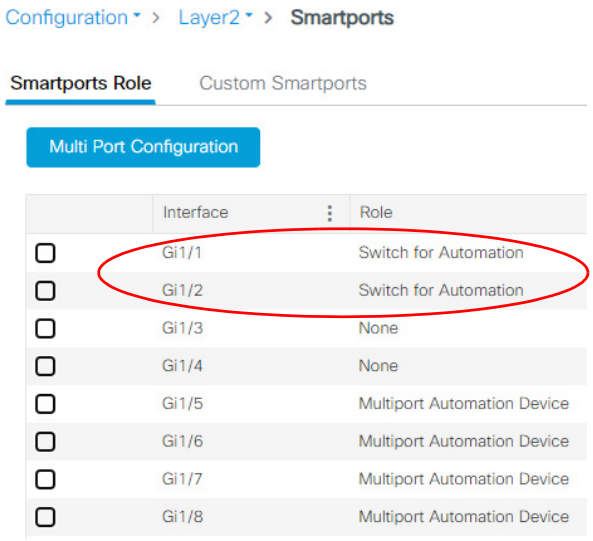


3. For each ring, enable and configure a primary or backup redundant gateway.





4. For each uplink port, apply the Switch for Automation Smartport role.



5. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Stratix 5800 Redundant Gateway via CLI

```
config t

! Configure IGMP snooping
ip igmp snooping tcn query solicit

! Configure ptp boundary mode
ptp mode boundary

! Enable and configure a primary or
! backup redundant gateway for each ring
! Use precedence value 255 for a primary gateway
! Use precedence value 100 or some other value
! for a backup gateway
DLR ring 1
gateway enable
default advertise-interval
default advertise-timeout
gateway-precedence 255
exit
exit
DLR ring 2
gateway enable
default advertise-interval
default advertise-timeout
gateway-precedence 255
exit
exit

! Configure the uplink ports for each ring
interface range Gi1/1-2
dlr ring 1 uplink
dlr ring 2 uplink

macro apply switch-automation $native_vlan 1
exit
end
!
```

Configure DLR DHCP on Stratix 5800 Switches

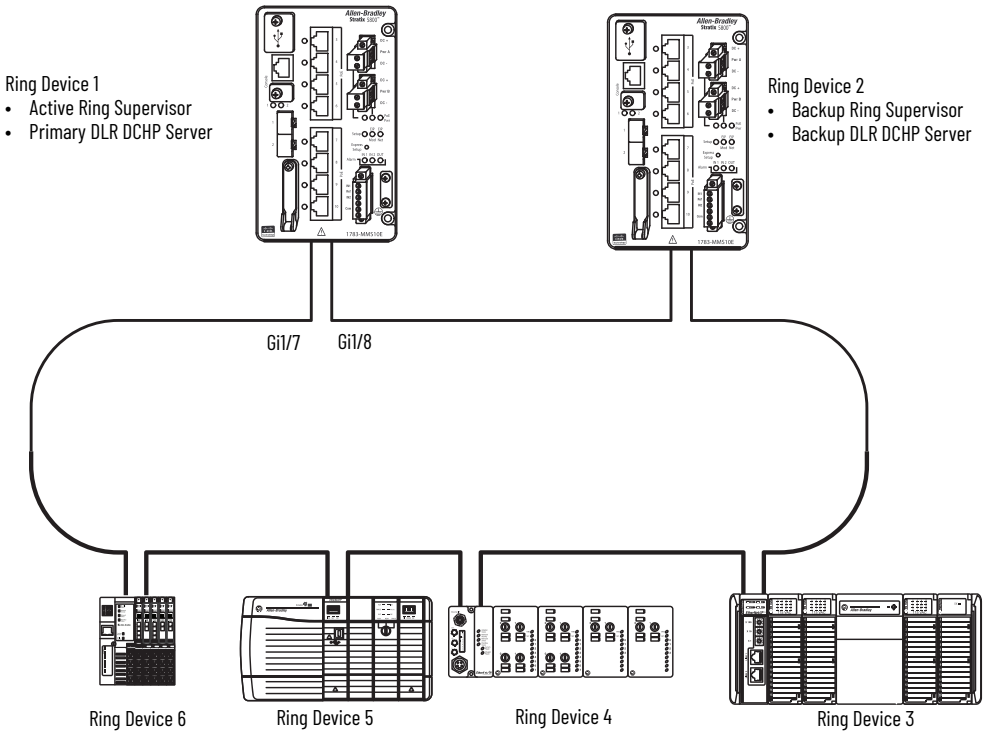
Use any of the following tools to configure DLR DHCP:

- Device Manager
- Command-line interface (CLI)

DLR configuration via the Logix Designer application will be available in a future release.

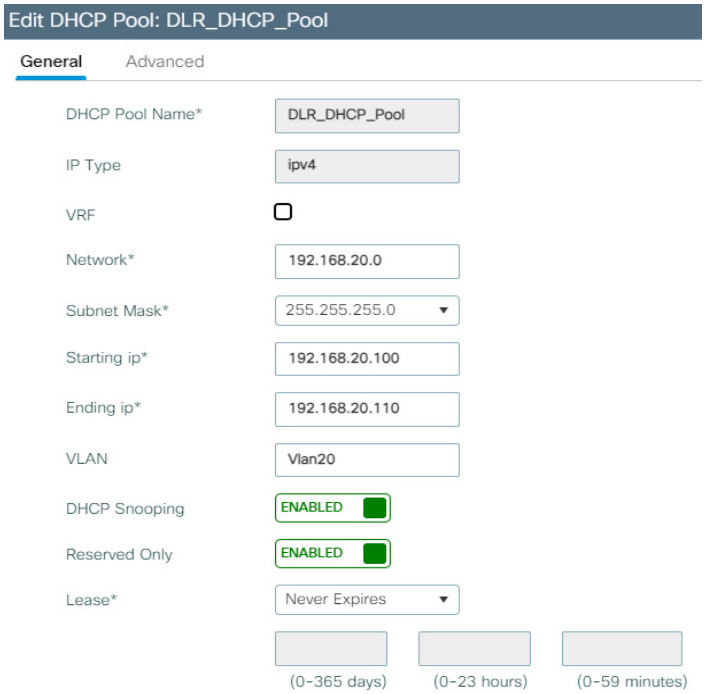
Table 12 - DLR DHCP Example

Ring Device Index	IP Address	Host Name	DHCP Pool
2	Not applicable	Not applicable	Not applicable
3	192.168.20.100	Device_20_100	DLR_DHCP_POOL
4	192.168.20.101	Device_20_101	DLR_DHCP_POOL
5	Not applicable	Not applicable	Not applicable
6	192.168.20.103	Device_20_103	DLR_DHCP_POOL

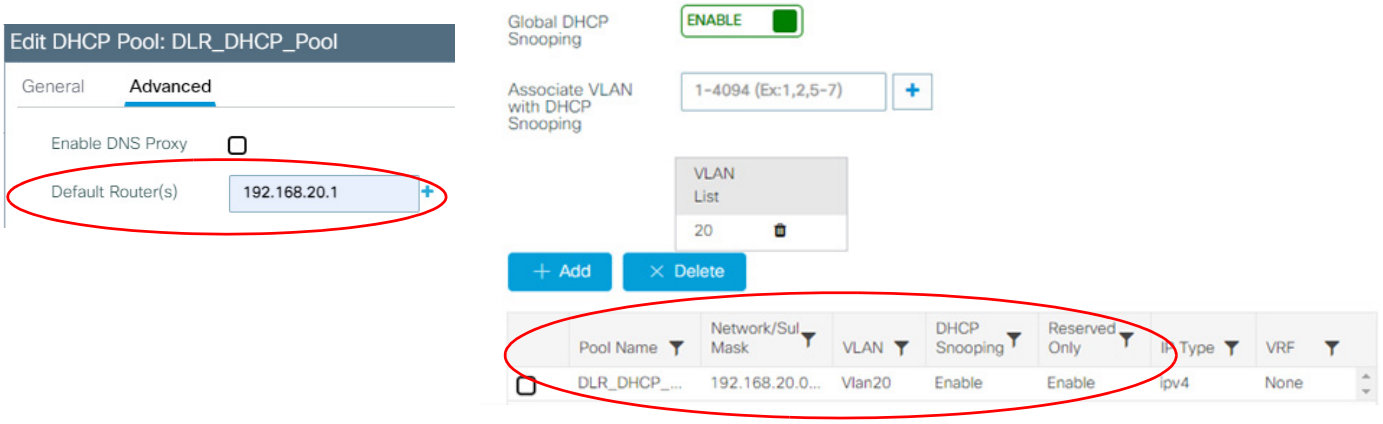


DLR DHCP on a Stratix 5800 Switch via Device Manager

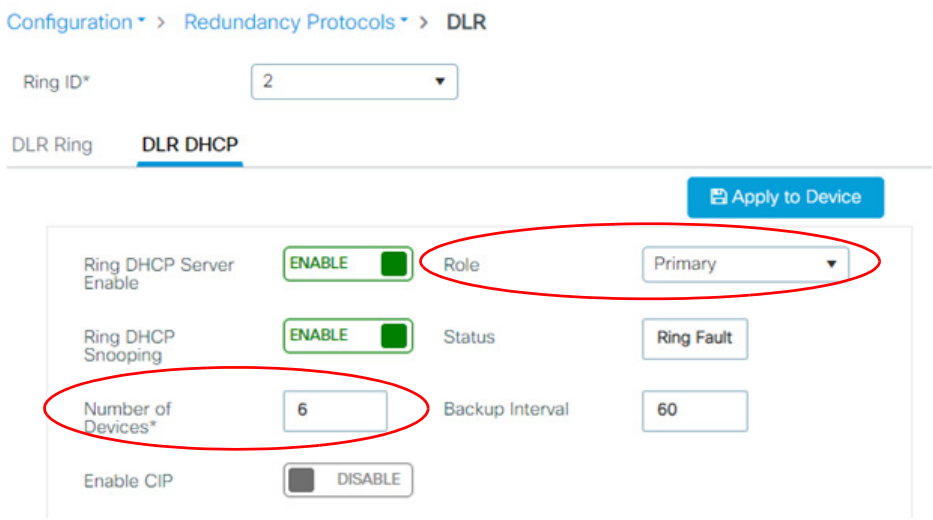
1. Enable DHCP and DHCP Snooping:
   - Configure a DHCP pool for ring devices.
   - Enable DHCP Snooping and Reserved Only.



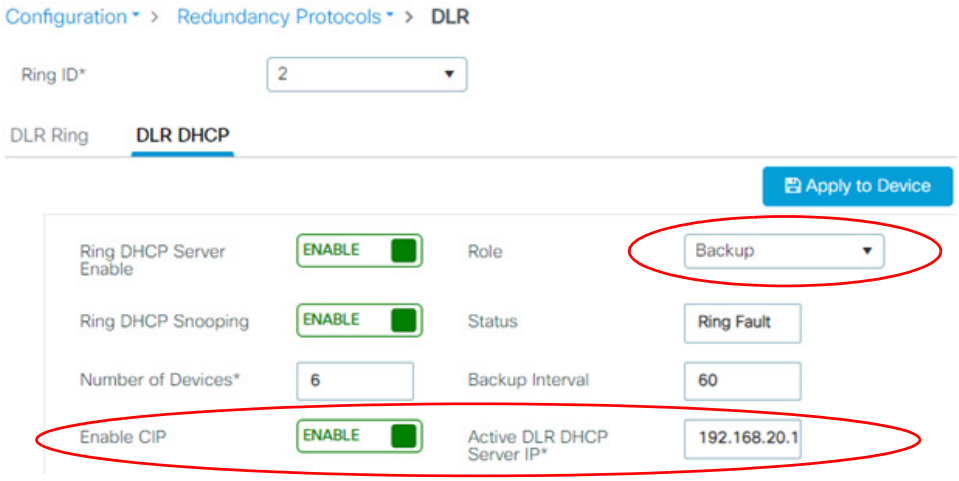
2. Specify a default router.



3. Configure the switch as a primary or backup DLR DHCP server.



For a **backup** configuration, you must select Enable CIP and enter the IP address of the primary DLR DHCP server. These settings enable the backup server to receive the DHCP configuration from the primary server if a switchover occurs.



4. (Primary DHCP server only). For each device on Ring 2, add entries to the index table and assign IP addresses to each entry, except for entries 2 and 5.

   In this example, entries 2 and 5 have static IP addresses.

Index	IP Address	Host Name	DHCP Pool
2			
3	192.168.20.100	Device_20_100	DLR_DHCP_Pool
4	192.168.20.101	Device_20_101	DLR_DHCP_Pool
5			
6	192.168.20.103	Device_20_103	DLR_DHCP_Pool

5. Proceed to the next step in your implementation.

   See Stratix Switch Configuration Examples on page 47.

Stratix 5800 DLR DHCP via CLI

Primary

```
config t
! Exclude the ring devices with static IP addresses
ip dhcp excluded-address 192.168.20.0 192.168.20.99
ip dhcp excluded-address 192.168.20.111 192.168.20.255
! Configure an IP address pool
ip dhcp pool DLR_DHCP_Pool
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
lease infinite
reserved-only
cip instance 1
! Enable DHCP snooping
ip dhcp snooping vlan 20
ip dhcp snooping
! Configure the switch as a primary DLR DHCP server
dlr ring 2
ring-dhcp
snooping enable
dhcp-server enable
intended-role primary
number-of-devices 6
! Assign IP addresses to devices in the DLR DHCP address pool.
entry 3 add 192.168.20.100 DLR_DHCP_Pool Device_20_100
entry 4 add 192.168.20.101 DLR_DHCP_Pool Device_20_101
entry 6 add 192.168.20.103 DLR_DHCP_Pool Device_20_103
exit
exit
end
!
```

Backup

```
config t
! Exclude the ring devices with static IP addresses
ip dhcp excluded-address 192.168.20.0 192.168.20.99
ip dhcp excluded-address 192.168.20.111 192.168.20.255
! Configure an IP address pool
ip dhcp pool DLR_DHCP_Pool
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
lease infinite
reserved-only
cip instance 1
! Enable DHCP snooping
ip dhcp snooping vlan 20
ip dhcp snooping
! Configure the switch as a backup DLR DHCP server
dlr ring 2
ring-dhcp
snooping enable
dhcp-server enable
intended-role backup
active-cip-addr 192.168.20.1
number-of-devices 6
exit
exit
end
!
```

Configure VLAN Trunking on Stratix 5800 Switches

Use any of the following tools to configure VLAN trunking:

- Device Manager
- Command line interface (CLI)

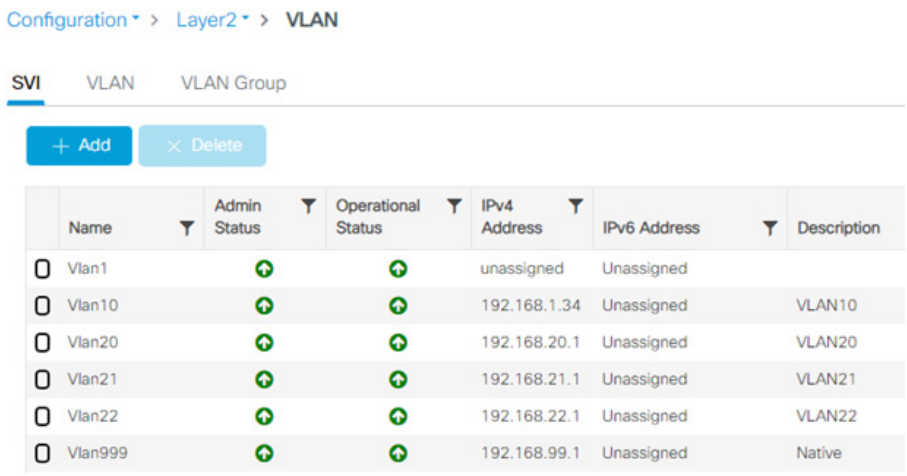
This example shows how to configure DLR VLAN trunking on Ring 2 and assumes that Ring 1 is already configured for one VLAN.

Table 13 - VLAN Trunking Configuration Example

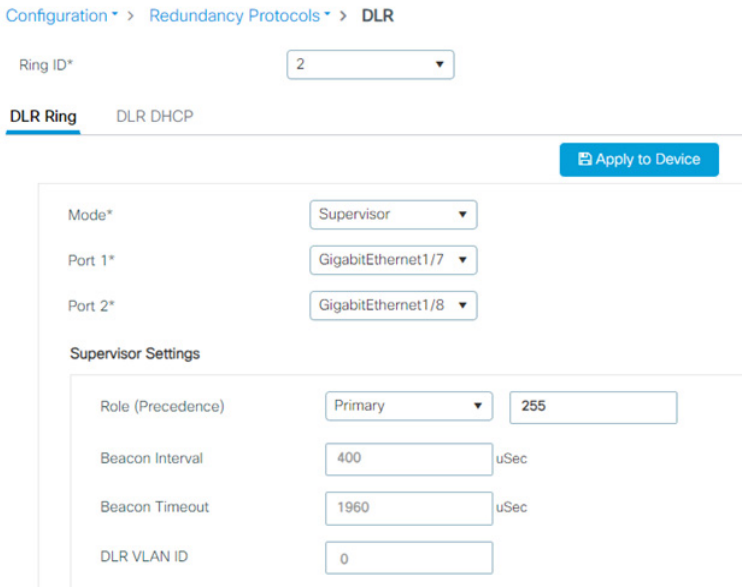
Switch	Ring	VLAN	IP Address	DLR Ports
Stratix 5800	1	10	192.168.10.1	Gi1/5, Gi1/6
	2	Trunk VLANs 20, 21, 22, and 999	Multiple, native VLAN 192.169.99.1	Gi1/7, Gi1/8

VLAN Trunking on a Stratix 5800 Switch via Device Manager

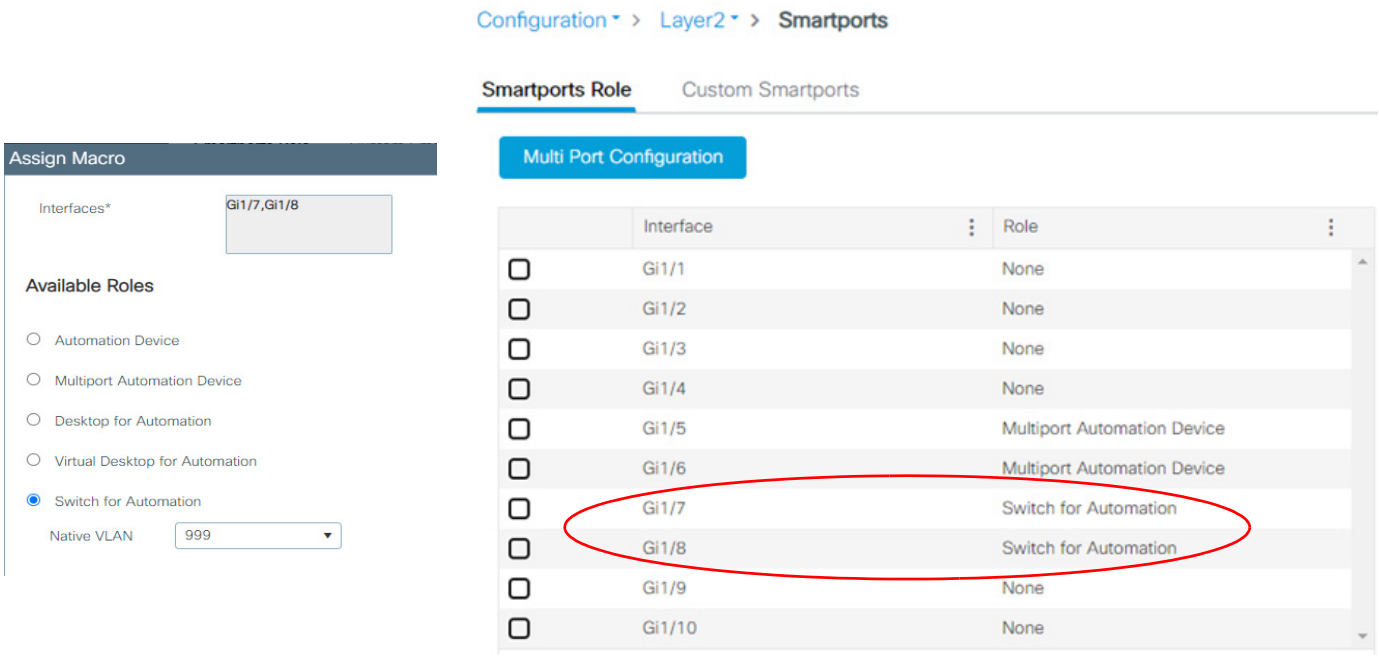
1. To configure Ring 1 with a single VLAN, follow the steps for Implementation C, as shown on page 47.
2. Create VLANs 20, 21, 22, and 999 and assign each VLAN a static IP address.
   Assigning an IP address to the native VLAN is not required, but recommended for diagnostic purposes.



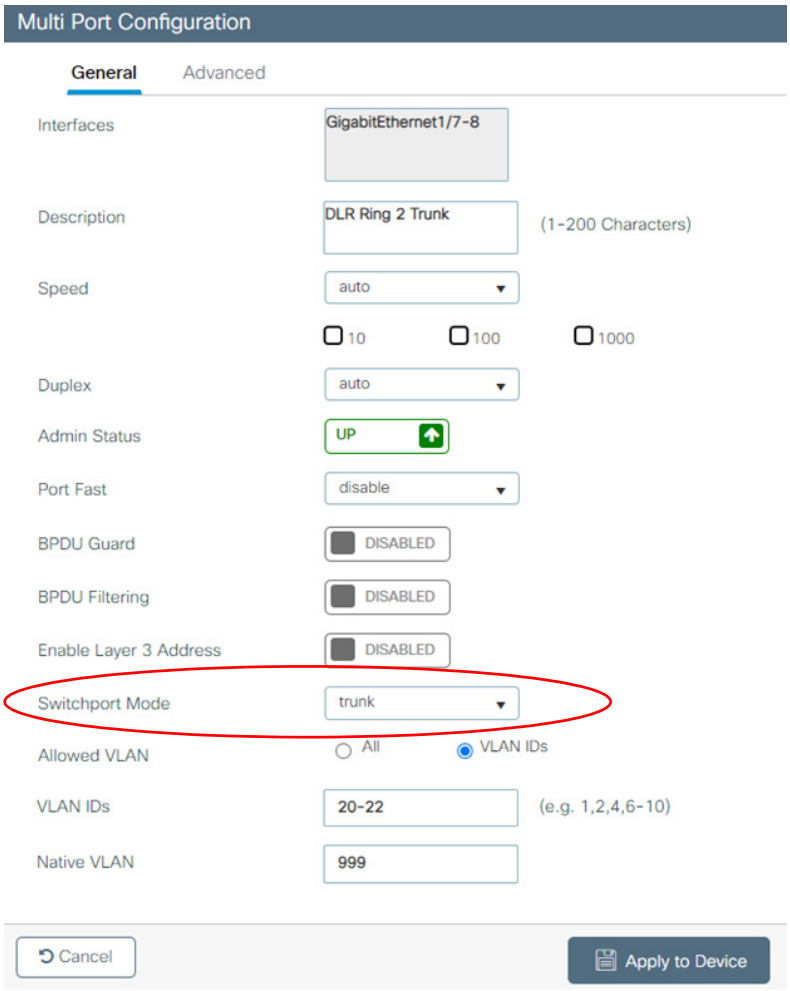
3. For Ring 2, do the following:
   - Enable Supervisor mode.
   - Enable DLR on two DLR-capable switch ports.
   - Configure primary or backup supervisor parameters.



4. For Ring 2, apply the Switch for Automation Smartport role to DLR-enabled ports Gi1/7 and Gi1/8 with native VLAN 999.



5. For Ring 2, configure VLAN trunking on DLR-enabled ports.



6. Proceed to the next step in your implementation.
   See Stratix Switch Configuration Examples on page 47.

Stratix 5800 VLAN Trunking via CLI

```
config t
!create VLANs for Ring 2 and assign addresses
VLAN 20
name DLR20
VLAN 21
name DLR21
VLAN 22
name DLR22
VLAN 999
name NV999
interface VLAN 20
IP address 192.168.20.1 255.255.255.0
exit
interface VLAN 21
IP address 192.168.21.1 255.255.255.0
exit
interface VLAN 22
IP address 192.168.22.1 255.255.255.0
exit
interface VLAN 999
IP Address 192.168.99.1 255.255.255.0
exit
! configure supervisor settings for Ring 2
! for backup use precedence 100
DLR Ring 2
mode supervisor
default beacon-interval
default beacon-timeout
control-vlan-ID 20
precedence 255
exit
exit
!configure VLAN trunking on Ring 2
interface range Gi1/7-8
macro apply switch-automation $native_vlan 999
switchport trunk allowed vlan 20,21,22,999
DLR Ring 2
ip dhcp snooping trust
exit
end
!
```

Notes:

DLR Network Monitoring

You can retrieve DLR network information through various software and tools that are described in this chapter.

For more information about how to troubleshoot products on EtherNet/IP™ networks, see the Troubleshoot EtherNet/IP Networks Application Technique, publication ENET-AT003.

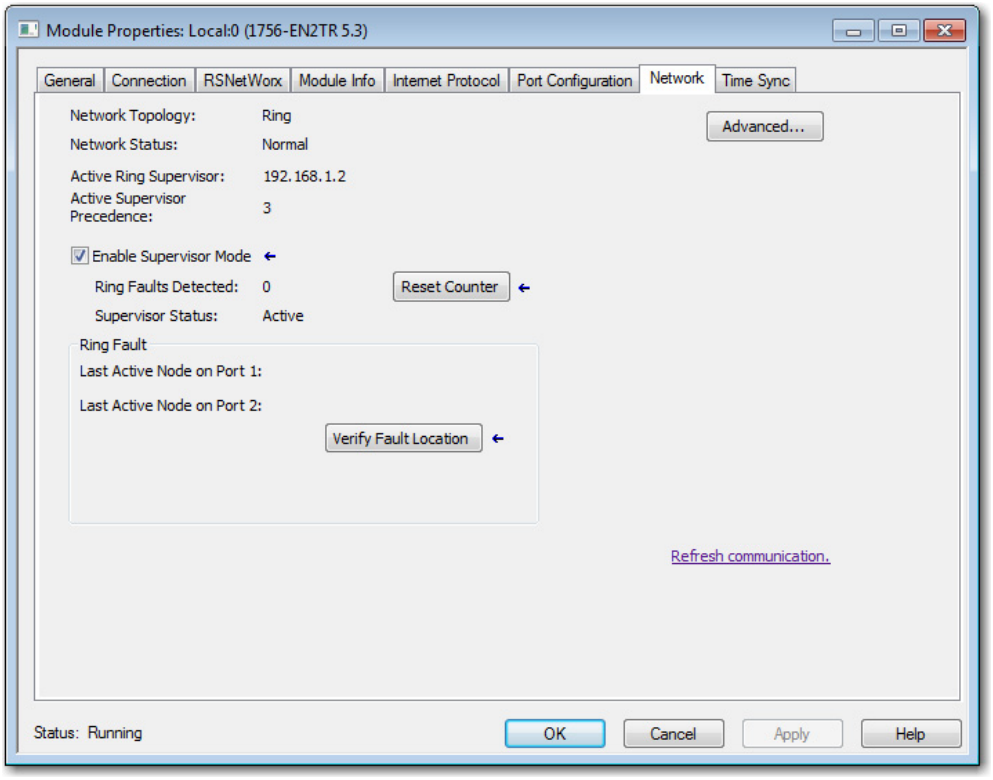
Depending on whether the ring node is a device or a switch, you can use the following software tools to monitor and diagnose a DLR network.

Software Tools	Device	Switch
Studio 5000 Logix Designer® application	Yes	Yes
RSLinx® Classic software	Yes	No
Device webpages	Yes	No
Device Manager web interface	No	Yes
Command-line interface (CLI)	No	Yes
DLR faceplate	Yes	Yes
MSG instructions	Yes	Yes

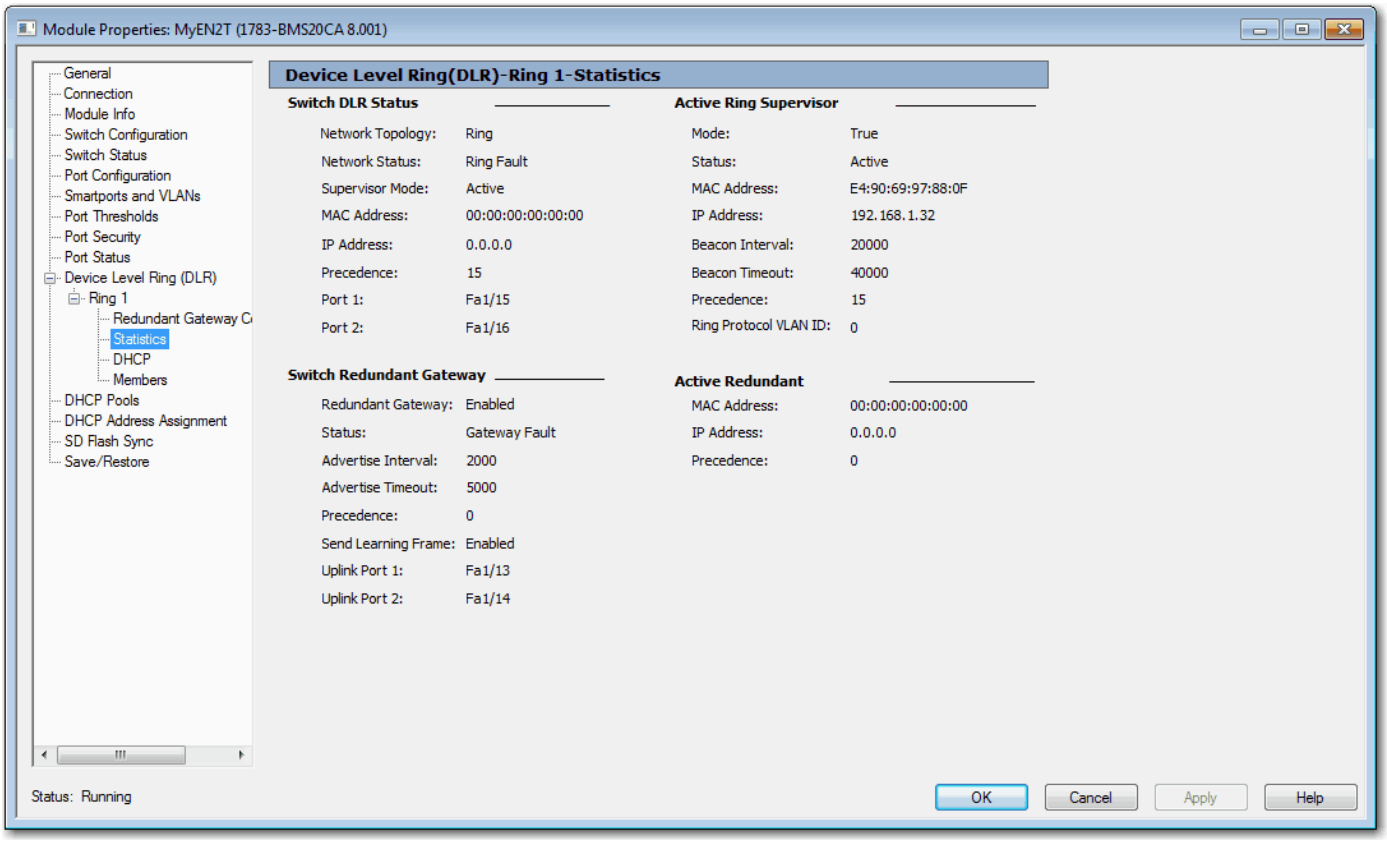
Logix Designer Application

You can view information about a DLR network in the Logix Designer application when your controller project is online.

For supervisor-cable devices, open the Module Properties dialog box and click the Network tab.



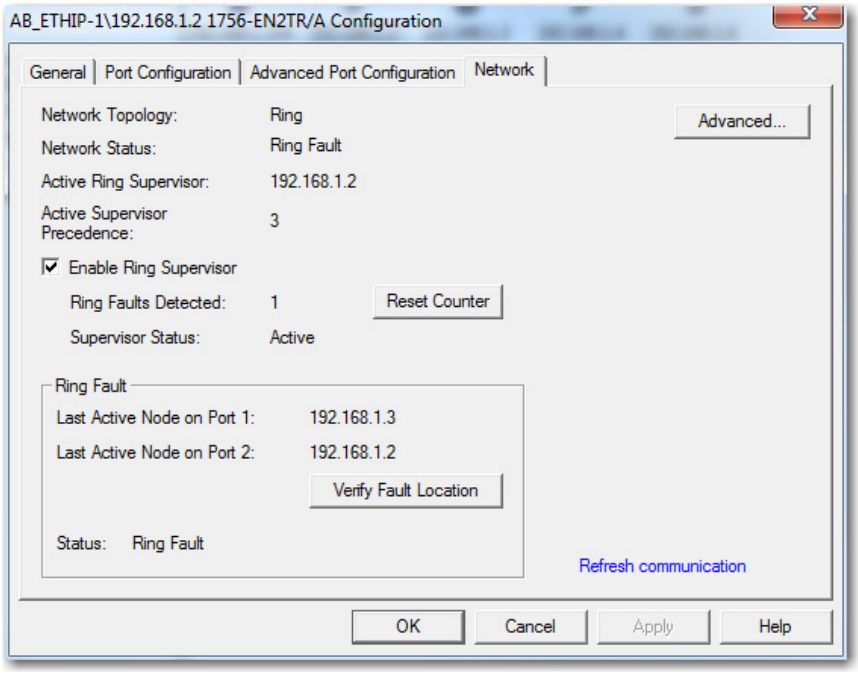
For switches, open the Module Properties dialog box, expand Device Level Ring (DLR) and click Statistics.



RSLinx Classic Software

In RSLinx® Classic software, browse the network to find the supervisor-cable device. Open the Module Configuration dialog box and click the Network tab.

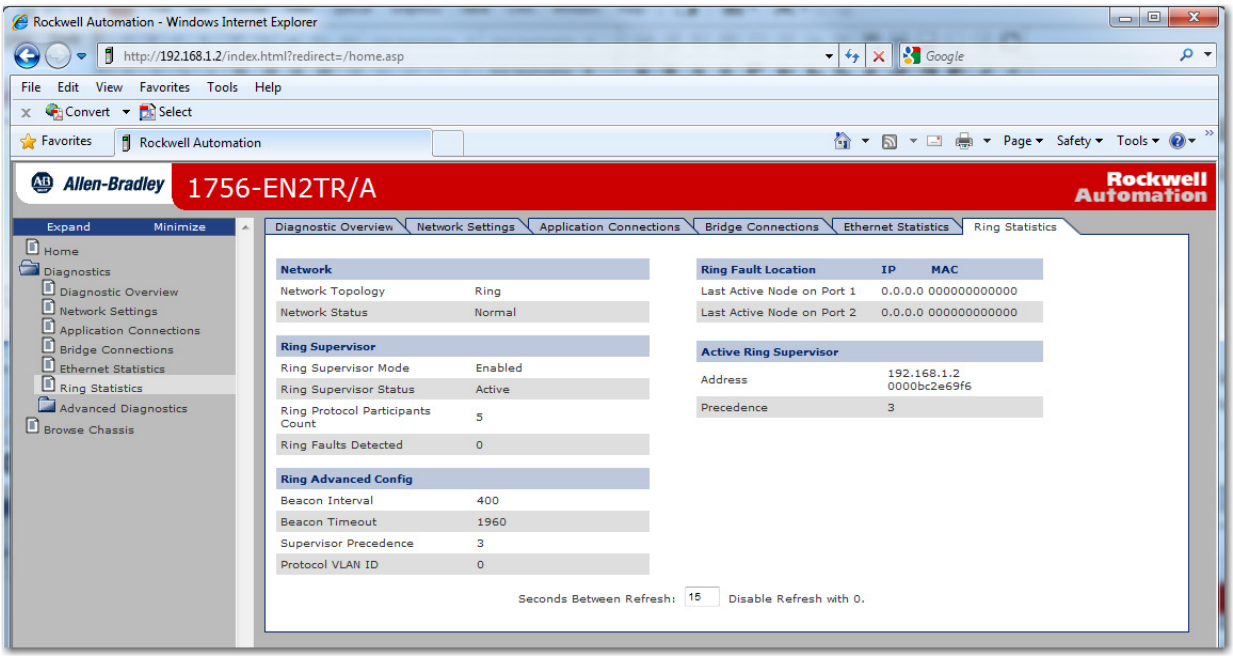
The following example shows a ring fault between nodes at IP addresses 192.168.1.3 and 192.168.1.2.



Device Webpages

Another method to monitor DLR network information with supervisor-capable devices is to use the diagnostic webpages for the device. This example uses a 1756-EN2TR module.

Enter the IP address of the device in a web browser to open the device webpage. Under the Diagnostics folder, click Ring Statistics.

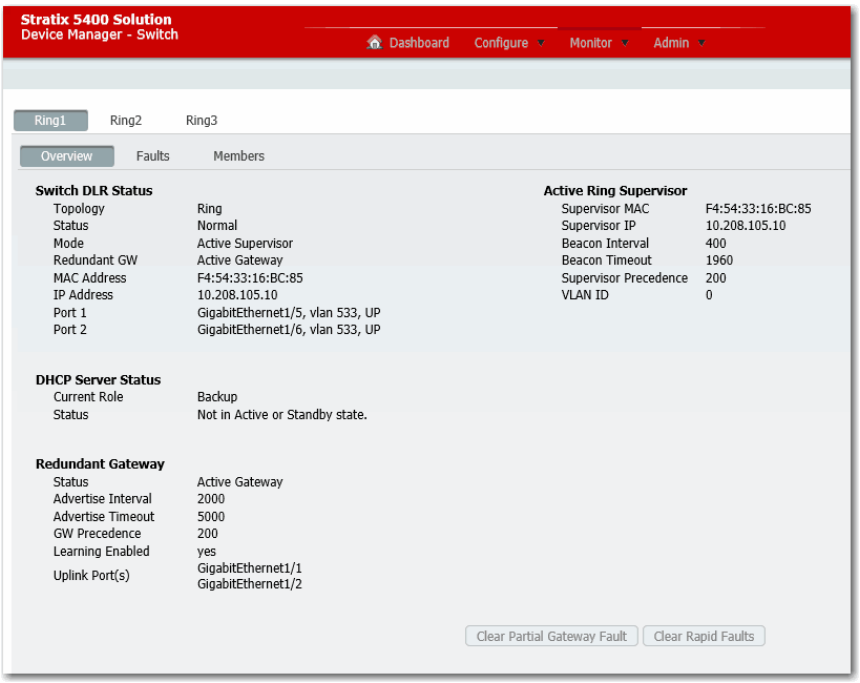


Device Manager

The Device Manager web interface is available for Stratix® managed switches.

Enter the IP address of the switch in a web browser and sign in to Device Manager. From the Monitor menu, choose DLR.

The following example shows DLR network information for the Stratix 5400 switch. You can view network information on the Overview, Faults, and Members tabs for each configured ring.



Command-line Interface

The Cisco IOS® command-line interface (CLI) enables you to execute Cisco IOS commands to configure and monitor DLR networks.

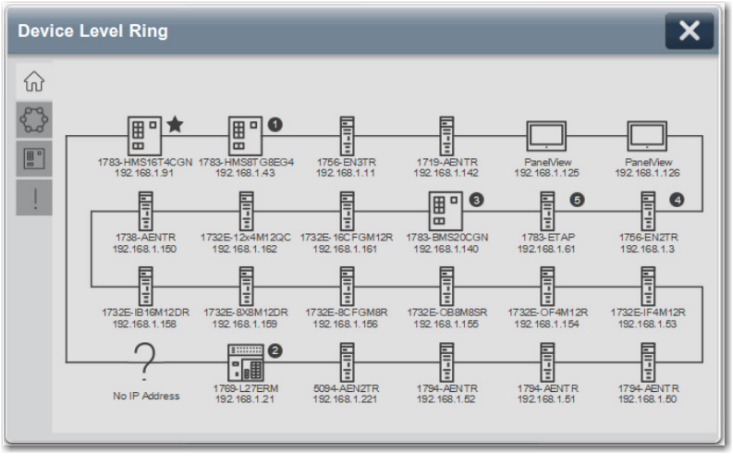
For details about CLI commands for DLR, see the Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD015.

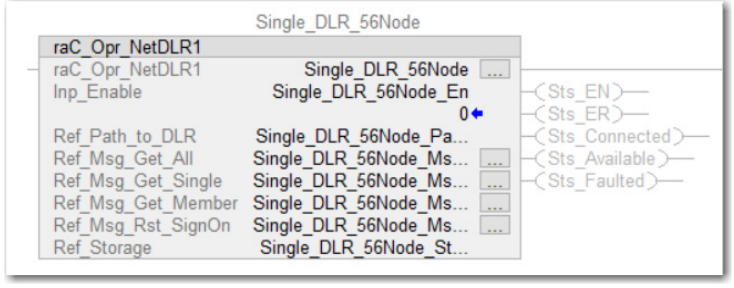
```
5700#sh dlr ring 1
DLR ring 1

mode: Active Supervisor
Network Topology: Ring                  Network Status: Normal
IOS state: NORMAL_ACTIVE                Hardware State: NORMAL_ACTIVE
Mac-Addr: E4:90:69:89:41:40             IP-Addr: 192.168.2.2
Port1: GigabitEthernet1/1, vlan 1, UP   Port2: GigabitEthernet1/2, vlan 1, 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: E4:90:69:89:41:40             IP-Addr: 192.168.2.2

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

Ring Protocol Participants Count: 8
No          Mac-Addr                    IP-Addr
1           E4:90:69:89:41:40           192.168.2.2
2           E4:90:69:9B:04:5D           192.168.2.18
3           00:00:BC:D0:18:4E           192.168.2.30
4           00:00:BC:D0:0A:9A           192.168.2.8
5           00:1D:9C:BF:5E:8B           192.168.2.83
6           E4:90:69:9D:85:4D           192.168.2.17
7           00:00:BC:CF:E5:CF           192.168.2.31
8           00:00:BC:61:1E:7D           192.168.2.240

Fault Statistics:
Ring Faults since power up: 1
Time of last fault: 21:53:58 UTC Mon Mar 2 2015
Ring Fault Location                     Mac-Addr                IP-Addr
Last Active Node on Port 1              00:00:00:00:00:00       0.0.0.0
Last Active Node on Port 2              00:00:00:00:00:00       0.0.0.0
```

DLR Faceplate

The EtherNet/IP Device Level Ring Network Diagnostics Faceplate enables a controller to retrieve real-time DLR network status information. The Logix Add-On Instruction automatically collects DLR information and HMI faceplate graphics allow the data to be visualized on an operator interface. Faceplate supports applications with as many as three DLR rings for FactoryTalk® View SE/ME and View Designer displays with Logix controllers. Faceplate files are available in the Network Device Library accessible from the Product Compatibility and Download Center at rok.auto/pcdc.

For more details, see the Network Device Library Reference Manual, publication DEVICE-RM400.





MSG Instructions

By using MSG instructions in the Logix Designer application, you can perform the following functions to monitor your DLR network:

- Get the current network topology mode
- Get the status of the network
- Get the last active node at the end of a chain through port 1 of an active ring supervisor during a ring fault
- Get the last active node at the end of a chain through port 2 of an active ring supervisor during a ring fault
- Verify a ring fault location
- Clear rapid ring faults
- Clear partial network faults

These functions are described in detail in Attribute and Service Return Values on page 95.

You can display this information on an HMI device or manipulate it in your project code.

Sample DLR network diagnostic application code, for example, Add-On Instruction or HMI faceplate graphics, is available on the Rockwell Automation Sample Code Library.

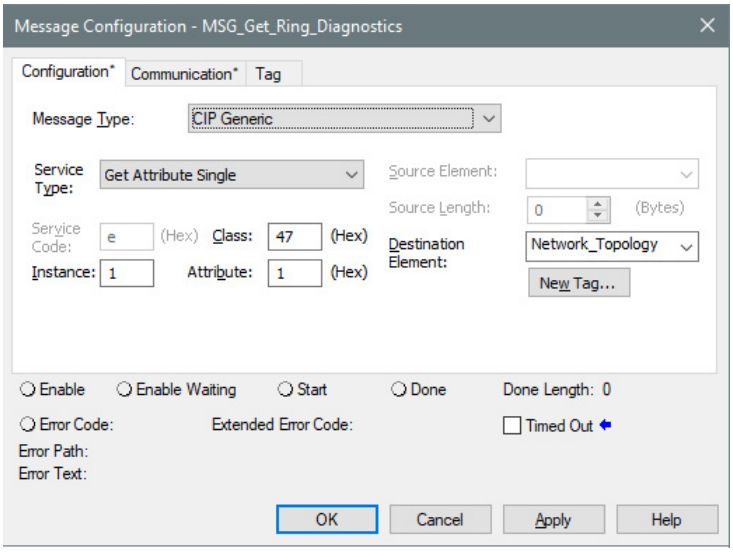
For information about how to program MSG instructions for Logix 5000® controllers, see the Logix 5000 Controllers Messages Programming Manual, publication 1756-PM012.

Example Use of MSG Instruction

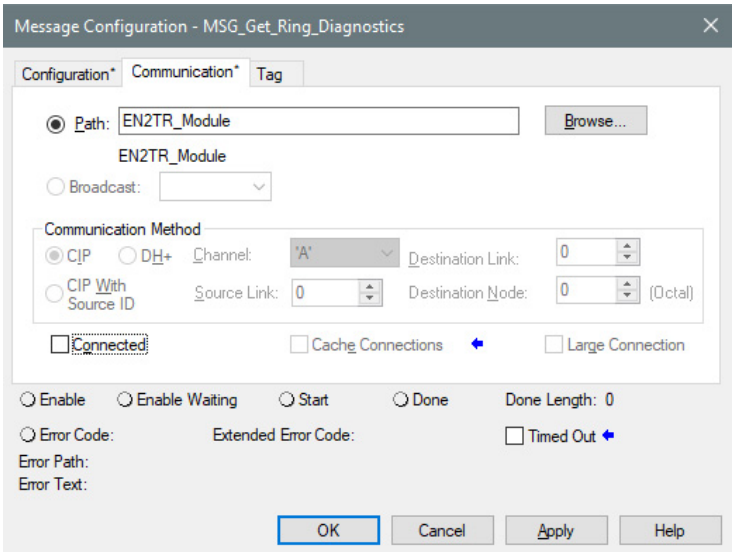
The following steps describe how to configure an MSG instruction.

1. Enter an MSG instruction into your rung of logic.
2. Configure the MSG instruction to retrieve the desired diagnostic service or attribute, as described in Table 14 on page 94.

Make sure the tag that you create is sized appropriately to hold all data.



3. Configure the communication path to point to the active supervisor node.



MSG Instruction Configuration Values

To obtain DLR diagnostic information, enter the configuration values that are described in Table 14 on the Configuration tab of an MSG instruction.

Table 14 - MSG Instruction Configuration Values

Attribute and Service Names	Description	Message Type	Service Code	Class (HEX)	Instance(1)	Attribute Code (HEX)	Destination Element	Destination Length (Bytes)
Network Topology	Current network topology mode	CIP™ Generic	E	47	1 = ring 1 2 = ring 2 3 = ring 3	1	SINT tag	1
Network Status	Status of network	CIP Generic	E	47	1 = ring 1 2 = ring 2 3 = ring 3	2	SINT tag	1
Last Active Node on Port 1	Last active node at the end of chain through port 1 of active ring supervisor during ring fault	CIP Generic	E	47	1 = ring 1 2 = ring 2 3 = ring 3	6	SINT[10] tag	10
Last Active Node on Port 2	Last active node at the end of chain through port 2 of active ring supervisor during ring fault	CIP Generic	E	47	1 = ring 1 2 = ring 2 3 = ring 3	7	SINT[10] tag	10
Verify a Fault Location	Causes ring supervisor to verify	CIP Generic	4B	47	1 = ring 1 2 = ring 2 3 = ring 3	0	None	–
Clear Rapid Faults	Clears the Rapid Fault/Restore	CIP Generic	4C	47	1 = ring 1 2 = ring 2 3 = ring 3	0	None	–
Clear Gateway Partial Fault	Clears the partial network fault	CIP Generic	4E	47	1 = ring 1 2 = ring 2 3 = ring 3	0	None	–

(1) For DLR-capable devices that are not Stratix switches, use instance 1.

Attribute and Service Return Values

Network Topology

The Network Topology attribute returns the current network topology mode.

Value	Mode	Description
0	Linear	The Network Topology attribute indicates Linear mode (0) when any of these conditions are true: • A supervisor-capable device is not enabled as a ring supervisor. • A supervisor-capable device is enabled as a ring supervisor, but cannot support the current operating ring parameters. • The device is not a supervisor-capable device[1].
1	Ring	The Network Topology attribute indicates Ring mode (1) when a supervisor-capable device is enabled as a ring supervisor, except when the device cannot support the current operating ring parameters.

(1) If the device is not a supervisor-capable device, the Topology mode is initially Linear, but then transitions between Ring and Linear modes.

Network Status

The Network Status attribute returns the status of the network based the view of the network by the device.

Value	Status	Description
0	Normal Operation	The devices detect that the network is operating normally in both ring and linear topology modes.
1	Ring Fault	The device detects a ring fault. Valid only when Network Topology is Ring.
2	Unexpected Loop Detected	The device detects a loop in the network. Valid only when the Network Topology mode is Linear.
3	Partial Network Fault	The device detects a network fault in one direction only. Valid only when the Network Topology mode is Ring and the node is the active ring supervisor.
4	Rapid Fault/Restore Cycle	The device detects a series of rapid ring fault/restore cycles. The supervisor remains in a state with forwarding blocked on its ring ports. The condition must be cleared explicitly via the Clear Rapid Faults service.

Last Active Node on Port 1

The Last Active Node on Port 1 attribute contains the IP address and Ethernet MAC address of the last node reachable through port 1 of an active ring supervisor. The value of the attribute is obtained via the Link_Status/Neighbor Status frames:

- The first 4 bytes represent the IP address.
- The next 6 bytes represent the MAC address.

The attribute value is 0 for these conditions:

- The initial value of the IP address and MAC address is 0.
- When no IP address is configured, the address is 0.
- When the device is not enabled as a ring supervisor or is operating as the backup supervisor, the IP address and Ethernet MAC address is 0.

On transition to FAULT_STATE, this attribute remains clear until the supervisor receives Link/Neighbor Status information.

On transition from FAULT_STATE to NORMAL_STATE, the value of the attribute is retained to help diagnose the previous ring fault.

Last Active Node on Port 2

The Last Active Node on Port 2 attribute contains the IP address and Ethernet MAC address of the last node reachable through port 2 of an active ring supervisor. The value of the attribute is obtained via the Link_Status/Neighbor Status frames:

- The first 4 bytes represent the IP address.
- The next 6 bytes represent the MAC address.

The attribute value is 0 for these conditions:

- The initial value of the IP address and MAC address is 0.
- When no IP address is configured, the address is 0.
- When the device is not enabled as a ring supervisor, or is operating as the backup supervisor, the IP address and Ethernet MAC address is 0.

On transition to FAULT_STATE, this attribute remains clear until the supervisor receives Link/Neighbor Status information.

On transition from FAULT_STATE to NORMAL_STATE, the value of the attribute is retained to help diagnose the previous ring fault.

Verify a Fault Location

The Verify Fault Location service causes an active ring supervisor to verify a ring fault location by retransmitting the Locate_Fault frame to ring nodes. The Last Active Node 1 and Last Active Node 2 attributes are updated based on the response to the Locate_Fault frame.

There are no parameters for the request. A success response results in all zeros.

If the Verify_Fault_Location service is received when the supervisor is not enabled, or is the backup supervisor, or is the active supervisor but not in fault state, status code 0x0C (Object State Conflict) is returned, and the Last Active Node 1 and Last Active Node 2 attributes is set to 0.

Clear Rapid Faults

The Clear Rapid Faults service clears the condition where the ring supervisor has detected a cycle of rapid ring fault/restore. Upon clearing the condition, the ring supervisor returns to normal operation.

There are no parameters for the request.

If the Clear Rapid Faults service is received when the supervisor is not enabled, or is the backup supervisor, or is the active supervisor but not in the rapid fault/restore condition, status code 0x0C (Object State Conflict) is returned.

Clear Gateway Partial Faults

The Clear Gateway Partial Fault service clears the condition where the gateway has detected a partial network fault. Upon clearing the condition, the gateway resumes normal operation.

There are no parameters for the request.

If the Clear Gateway Partial Fault service is received when the gateway is not enabled, or is not in partial network fault condition, status code 0x0C (Object State Conflict) is returned.

Network Recovery Performance

When you measure the performance of your network during fault conditions, we recommend that you consider the network recovery time. Network recovery is the time for all of the following to take place:

1. The supervisor node recognizes that a fault exists on the network.
2. The supervisor node reconfigures the network appropriately because of the fault.
3. The supervisor node communicates to the network nodes that a fault condition exists.
4. The network nodes reconfigure themselves appropriately because of the fault.

With the default beacon interval value of 400 µs and beacon timeout value of 1960 µs, the worst-case time for network recovery times are as follows:

- 2890 µs for a **copper DLR network**. This recovery time is based on 100 m (328 ft) copper segments between nodes on the network.
- 3140 µs for a **fiber-optic DLR network**. This recovery time is based on 2 km (6561 ft) fiber-optic cable segments between nodes on the network.

When considering these values, keep in mind the following:

- Recovery time can actually occur faster than the times listed.
- The recovery times assume that your network nodes are operating at 100 Mbps speed and full-duplex mode.
- If nodes operate at a different speed or duplex mode, the recovery times can differ.

  In this scenario, you must change the beacon interval and beacon timeout. If you think you must change these parameters, we recommend that you first call Rockwell Automation technical support.
- The value assumes that most of the traffic on your network is EtherNet/IP™ traffic.

Notes:

Numerics

A

B

C

D

E

F

H

I

L

M

N

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation. You can view or download publications at rok.auto/literature.

Resource	Description
Stratix Ethernet Device Specifications Technical Data, 1783-TD001	Provides specifications for Stratix® Ethernet switches and other devices.
Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD015	Represents a collaborative development effort from Rockwell Automation and Cisco Systems®. Provides application requirements, technology, and design considerations to deploy Device Level Ring (DLR) technology through a plant-wide Industrial Automation and Control System (IACS) network infrastructure.
High Availability Systems Reference Manual, HIGHAV_RM002	Provides guidelines for high availability systems, including redundant system components, networks, and other hardware and software considerations.
Stratix Managed Switches User Manual, 1783-UM007	Describes how to configure, monitor, and troubleshoot Stratix® 5400, 5410, 5700, 8000, 8300, and ArmorStratix™ 5700 managed switches.
ControlLogix EtherNet/IP Network Devices User Manual, 1756-UM004	Describes how to configure and use EtherNet/IP devices to communicate on the EtherNet/IP network.
Ethernet Reference Manual, publication ENET-RM002	Describes basic Ethernet concepts, infrastructure components, and infrastructure features.
Troubleshoot EtherNet/IP Networks Application Technique, publication ENET-AT003	Describes troubleshooting techniques for Integrated Architecture products on EtherNet/IP networks.
Online Help (provided with the switch)	Provides context-sensitive information about how to configure and use the switch.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general installation guidelines for a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, Knowledgebase, and product notification updates.	rok.auto/support
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Technical Documentation Center	Quickly access and download technical specifications, installation instructions, and user manuals.	rok.auto/techdocs
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Allen-Bradley, ArmorStratix, Compact I/O, ControlLogix, expanding human possibility, FactoryTalk Network Manager, Logix 5000, Rockwell Software, Rockwell Automation, RSLinx, Stratix, and Studio 5000 Logix Designer are trademarks of Rockwell Automation, Inc.

CIP, CIP Sync, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc.

Cisco and Cisco Systems are trademarks of Cisco Systems, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Automation maintains current product environmental compliance information on its website at rok.auto/pec.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608, FAX: (65) 6510 6699
UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication ENET-AT007E-EN-P - June 2023
Supersedes Publication ENET-AT007D-EN-P - August 2021

Copyright © 2023 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.