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
New guidance for ring speed	11
Added support for redundant gateway topologies with VLAN trunking	42
Added descriptions of supervisor fields for 1756-EN2TR	55
Added information to monitor the network via MSG instructions	81

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 the Open DeviceNet® Vendors' Association (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 nodes on a DLR network. Only 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.

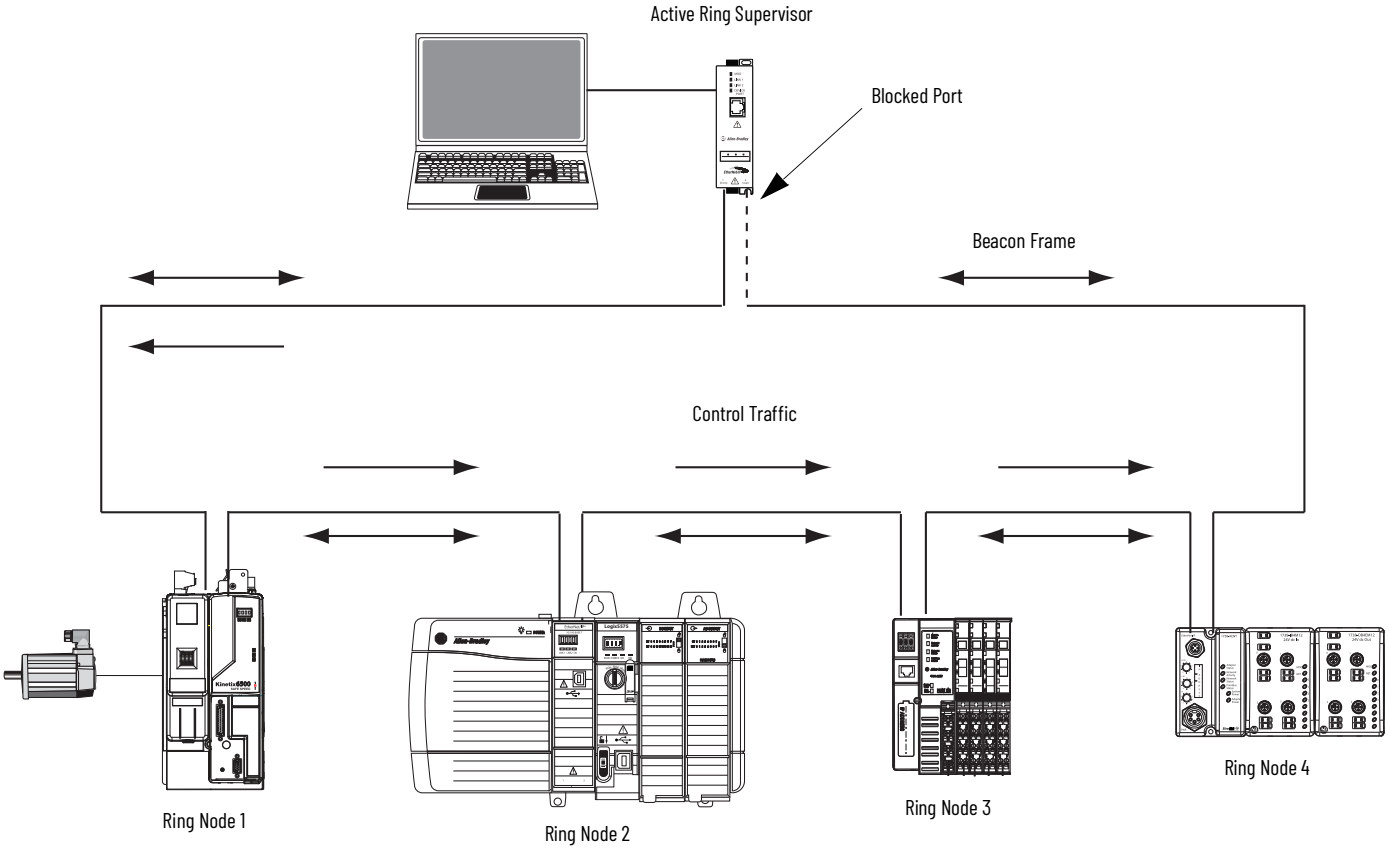
A DLR configuration includes the following beacon-related parameters:

- 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:

- Helps prevent and 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)*.

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 tap.

Additional Features

Some Stratix switches support these DLR features:

- Redundant gateways—Stratix switches configured as redundant gateways provide redundant paths from a DLR network to the outside network. Refer to Ring with Redundant Gateways on page 17.
- Multiple rings—Stratix 5400 switches support as many as three rings. Depending on the number of switches in the network and their configuration, VLAN restrictions can apply. Refer to Multiple Rings on page 31.
- DHCP for ring devices—On some Stratix switches, you can configure DHCP to assign IP addresses to devices connected to a ring based on their positions in the ring. This feature makes sure that a replaced device receives the expected IP address. Refer to Ring with a DHCP Server on page 24.

For more information about how to configure these features on Stratix switches, see the online Help or user manual for the switch.

DLR Network Requirements and Restrictions

Be aware of these requirements and restrictions for DLR networks.

Topic	Page
Number of Ring Nodes	10
Switch Ports	10
Multicast Groups	10
Ring Speed	11
CIP Sync Time Synchronization/Precision Time Protocol (PTP)	12

Number of Ring Nodes

For all types of rings, we recommend that you limit a DLR network to fewer than 50 nodes. If your application requires 50 or more 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 for a switch, 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	Multiport Automation Device or None
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

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

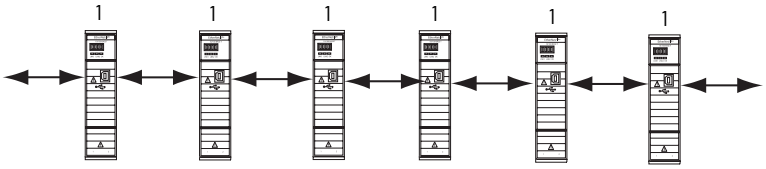
A ring must operate at **one speed**: either 100 Mbps or 1 Gbps. Ring nodes cannot communicate at different speeds within the same ring. A uniform ring speed is required to make sure each connection in a ring functions and to help prevent packet loss from buffer overruns.

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.

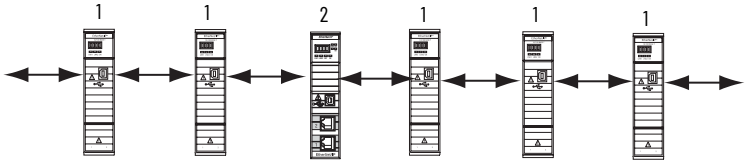
  For example, if all ring nodes are 1756-EN2TR devices, configure all connected ports to auto-negotiate.



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.

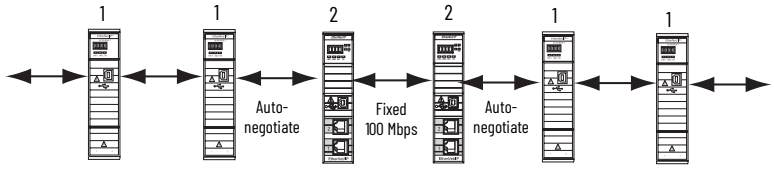
  For example, if you insert one 1756-EN4TR device into a ring of 1756-EN2TR devices, configure all connected ports to auto-negotiate.



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 the ports 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.

Fault Management

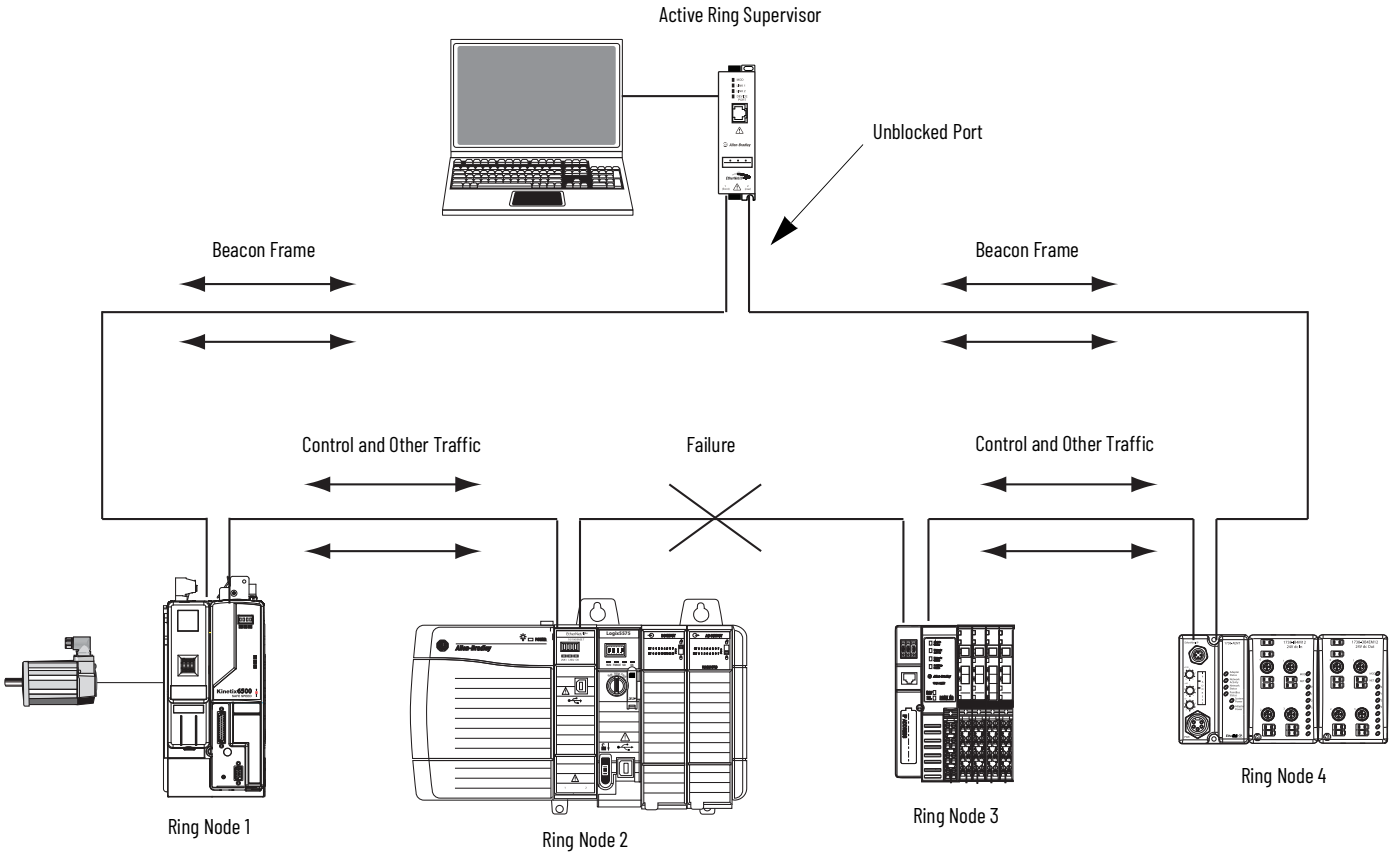
A DLR network can help protect your application from interruptions that are caused by a fault. To maintain the resiliency of a ring, configure your application so that it monitors the health of the ring itself. The ring can be faulted while all higher-level network functions, such as I/O connections, 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 3, Monitor a DLR Network.

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.

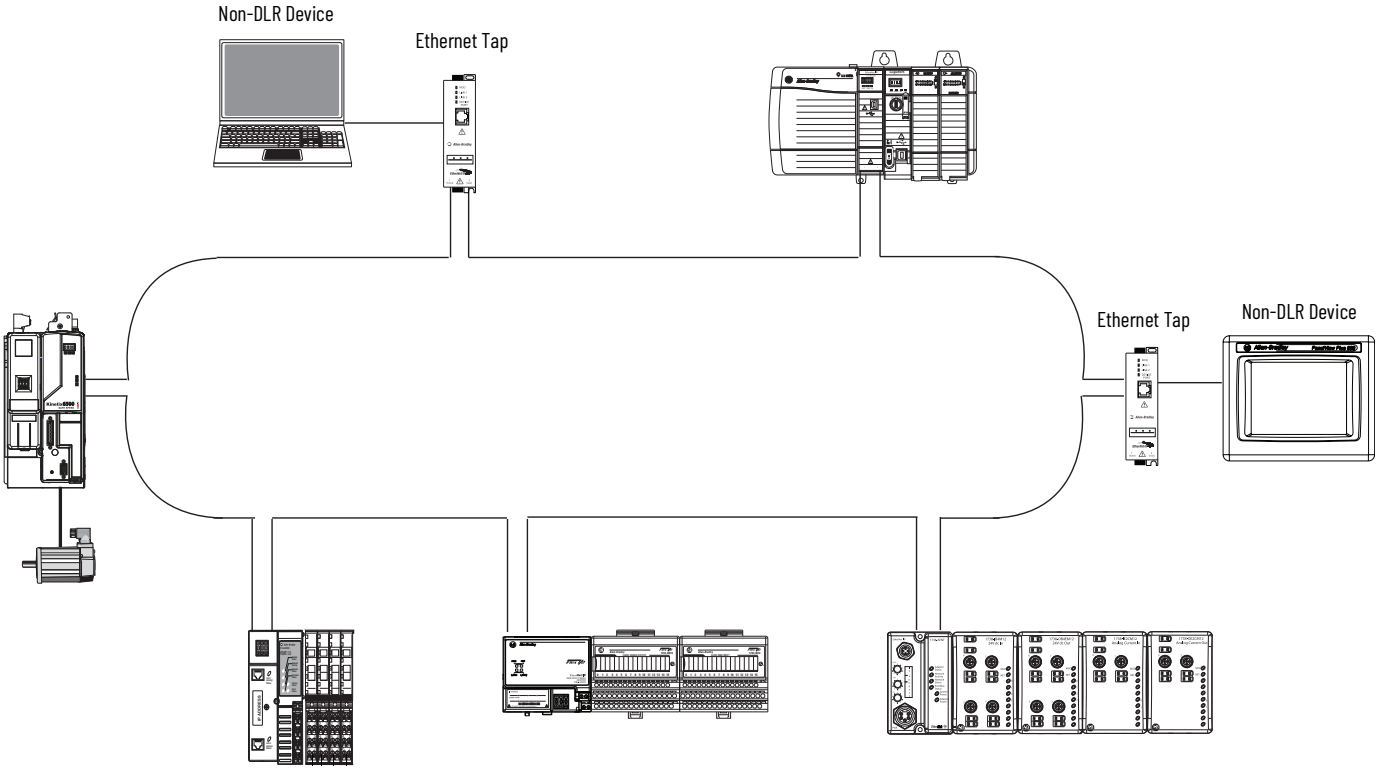
Figure 2 - Network Reconfiguration After Fault



Ring of Devices

The most basic implementation of DLR is a ring of DLR-capable devices. In Figure 3, devices without DLR capability connect to the ring via Ethernet taps.

Figure 3 - Ring of Devices

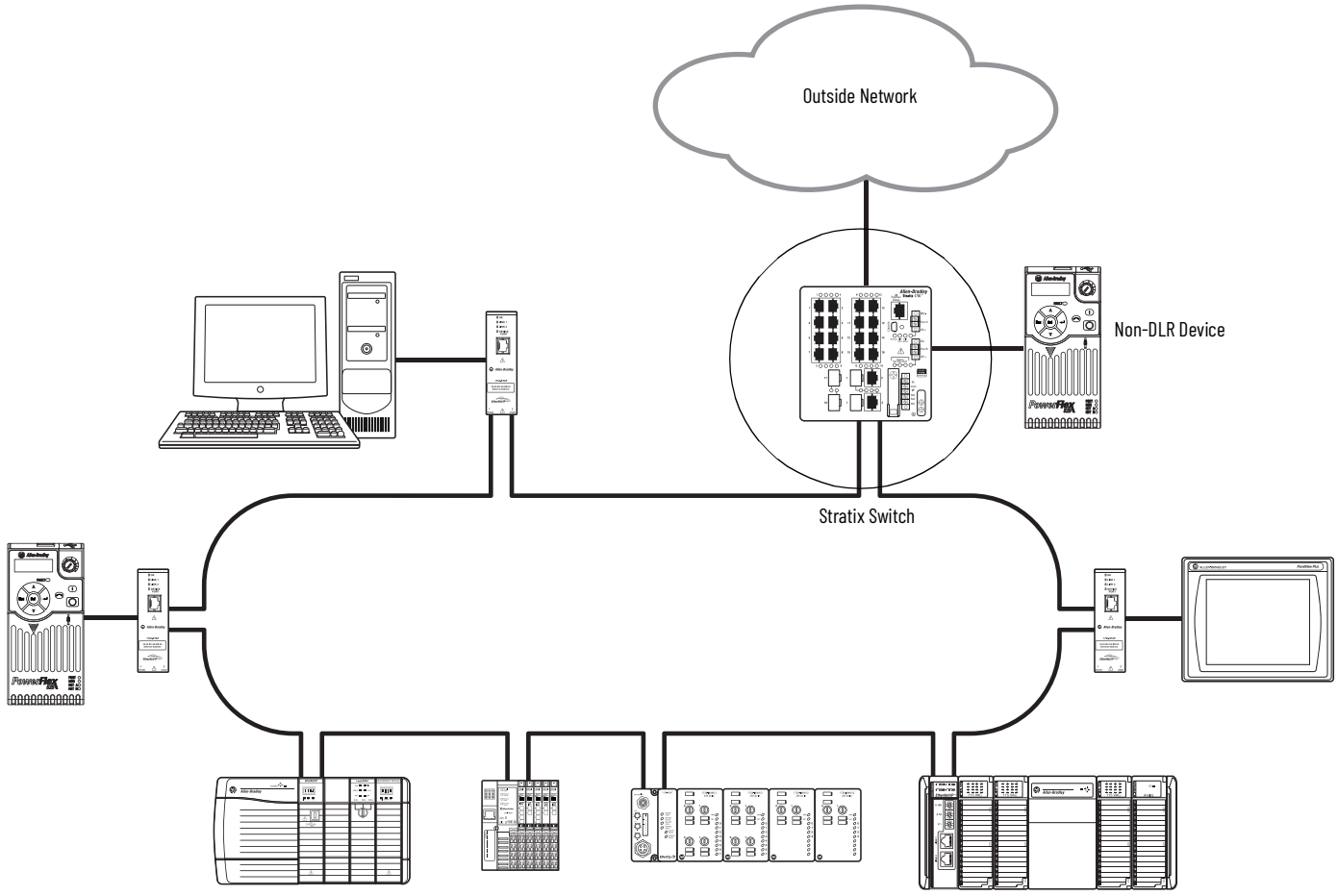


Ring of Devices with a Switch

In Figure 4, a DLR-capable Stratix switch is connected directly to the ring. The switch connects the ring to the rest of the network. If the switch is configured as the ring supervisor, the switch also provides consolidated status and diagnostics for the DLR network.

Like an Ethernet tap, a DLR-capable switch can also connect non-DLR devices to the ring.

Figure 4 - Ring of Devices with Switch

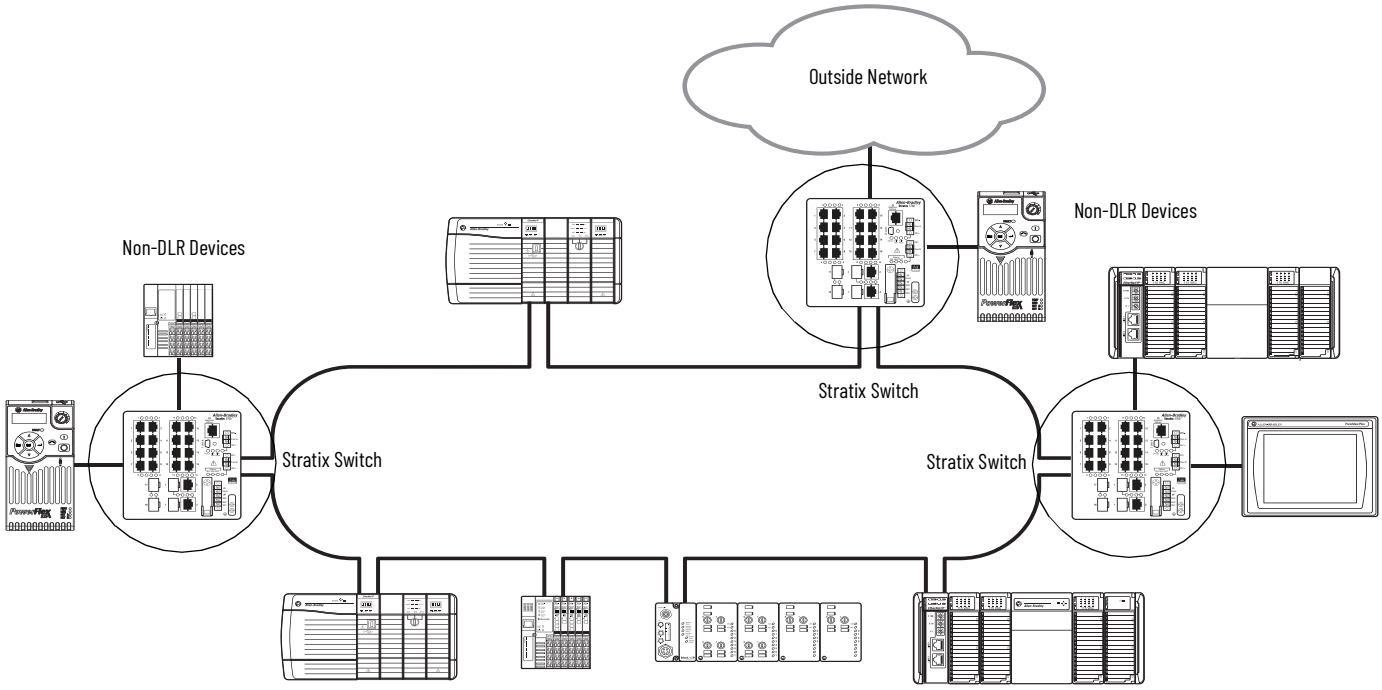


Ring of Devices with Multiple Switches

When multiple DLR-capable switches connect directly to a ring (Figure 5), they can serve different purposes:

- One or more of the switches that are configured as redundant gateways can connect to the outside network.
- One or more of the switches can connect non-DLR devices to the ring.

Figure 5 - Ring of Devices with Multiple Switches

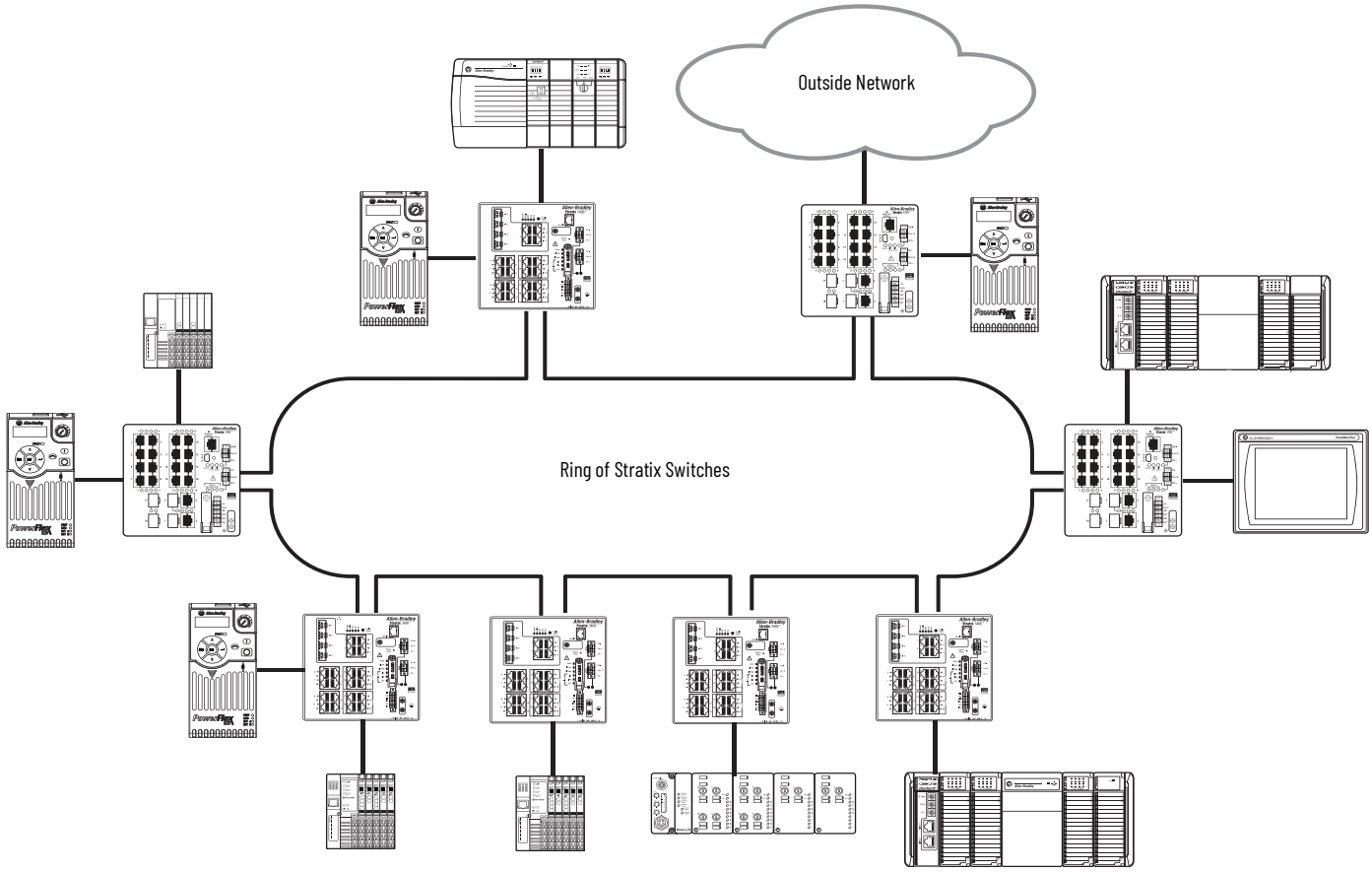


Ring of Switches

A DLR network can consist of solely DLR-capable switches (Figure 6) and still support a high-speed convergence time of 3 ms or less with these restrictions:

- Limit one ring to no more than 24 switches and 230 end devices.
- Use only one VLAN in a ring.

Figure 6 - Ring of Switches

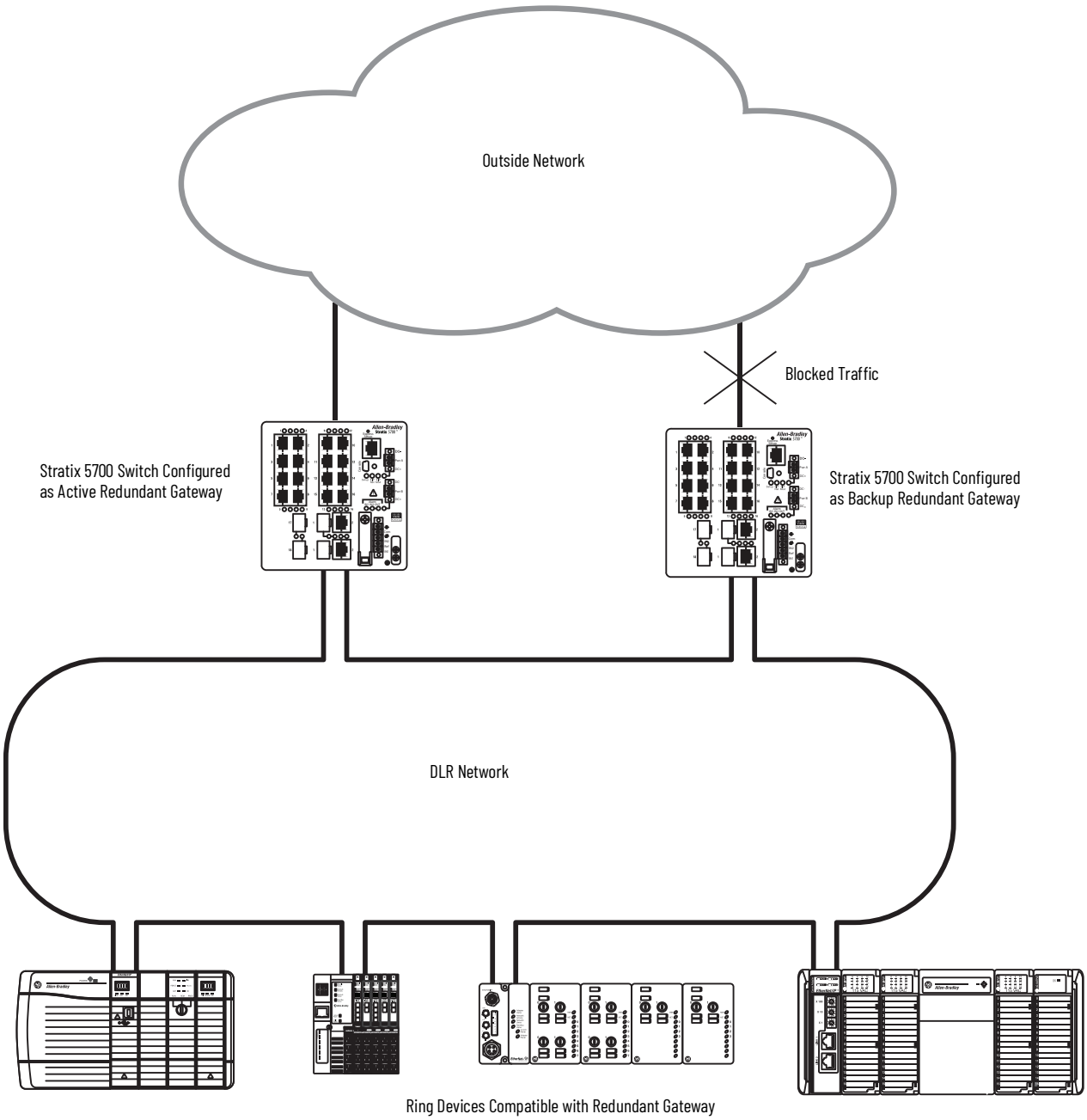


Ring with Redundant Gateways

A DLR network with redundant gateways uses multiple switches to provide multiple connections from a ring to the outside network infrastructure (Figure 7). If you only need 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.

Figure 7 - 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. For example, two 1783-ETAP modules in the same DLR network cannot use their device ports to connect to a common switch or network.

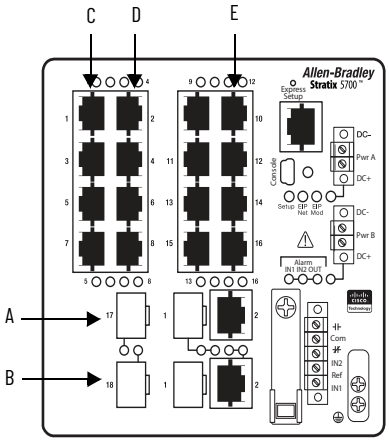
IMPORTANT The redundant gateway feature requires all devices on the ring to be compatible with redundant gateway. Connections to devices wired to or through a DLR network can be lost upon a gateway changeover if all DLR network devices are not compatible with redundant gateway.

For more information about redundant gateway compatibility, see Knowledgebase article *Using Device Level Ring (DLR) Redundant Gateway*.

Redundant Gateway Traffic Flow

Figure 8 is an example of a switch that is configured for redundant gateway. All ports are assigned to VLAN 1.

Figure 8 - Redundant Gateway Switch Ports



E

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

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

When the switch acts as a **backup** redundant gateway, traffic on the switch that is assigned to VLAN 1 can flow as follows:

- Between only Ports A and B
- Between only Ports C, D, and E
- To join the ring, traffic on Ports C, D, and E must flow through the non-DLR port, through devices connected to the backup redundant gateway, and then through the active redundant gateway.

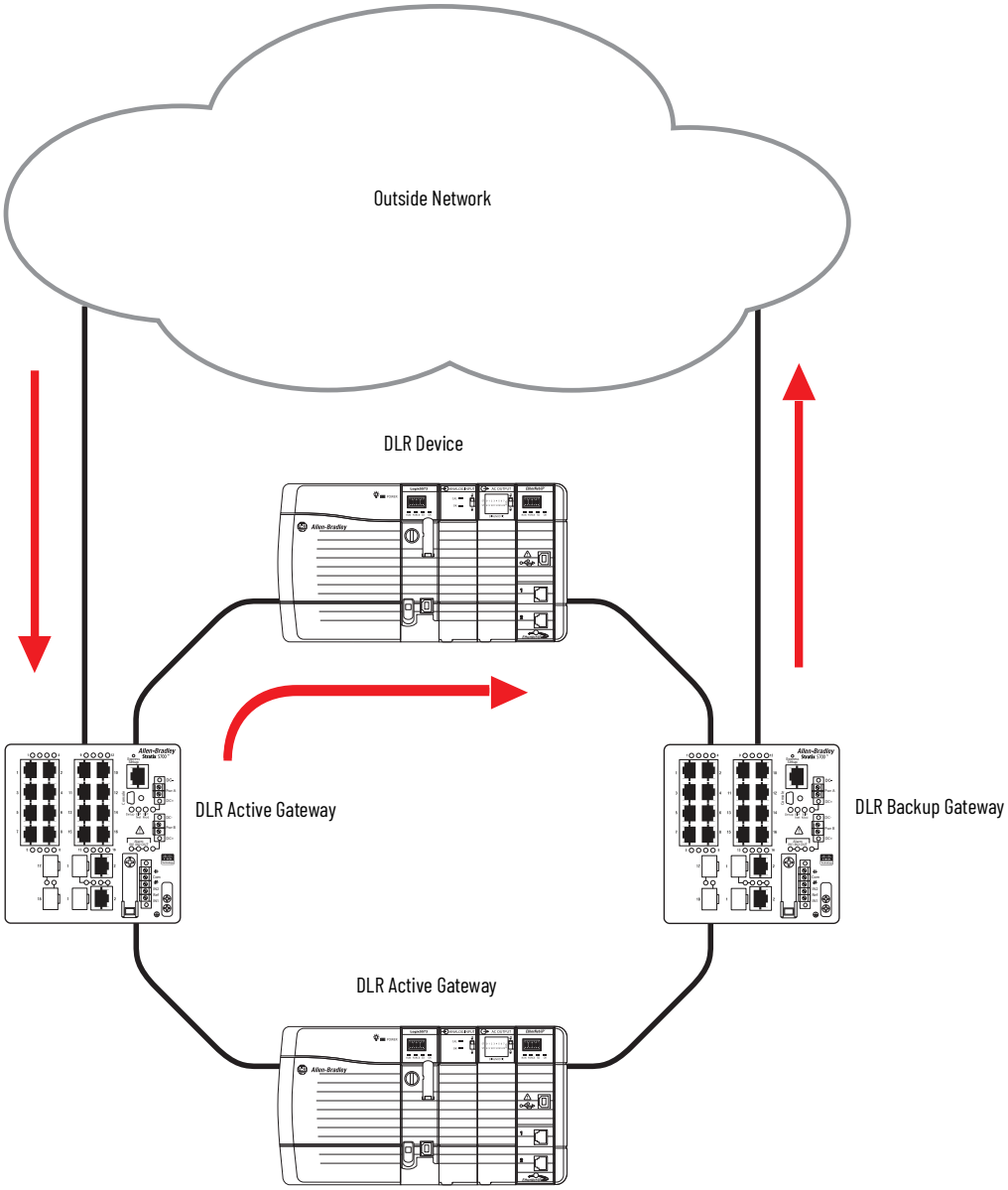
IMPORTANT Traffic flow restrictions from the backup gateway to the ring include CIP™ and Device Manager traffic. As a result, all traffic that flows from a ring device to the backup gateway must use this path:

- 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.

Figure 9 shows traffic flow from the backup gateway to the ring.

Figure 9 - Traffic from Backup Gateway to Ring



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 article *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:
  - Multicast I/O (examples are ControlLogix® Redundancy I/O and IEEE 1588 CIP Sync traffic)
  - Multicast produce/consume tags

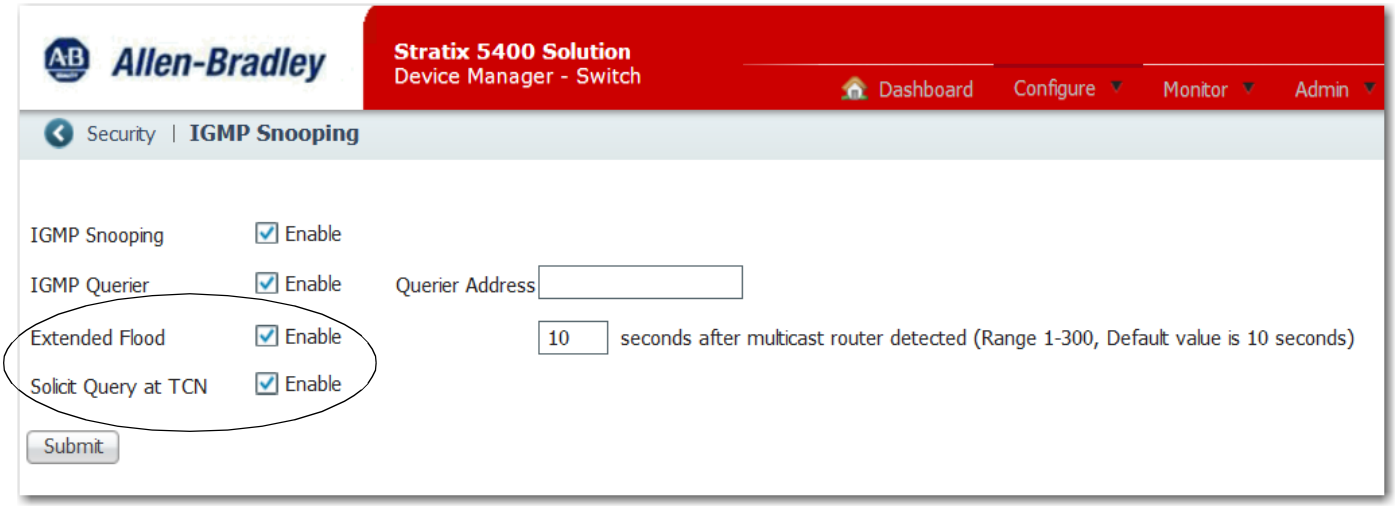
Multicast Traffic and Redundant Gateways

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 10):

- 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 10 - 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.

Ring with 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)
- Hot Standby Router Protocol (HSRP)

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

Single Switch Uplink to the Outside Network

Figure 11 shows a Stratix switch with an uplink port that is connected to a network that uses STP for resiliency.

Figure 11 - Single Switch Uplink to Network with STP

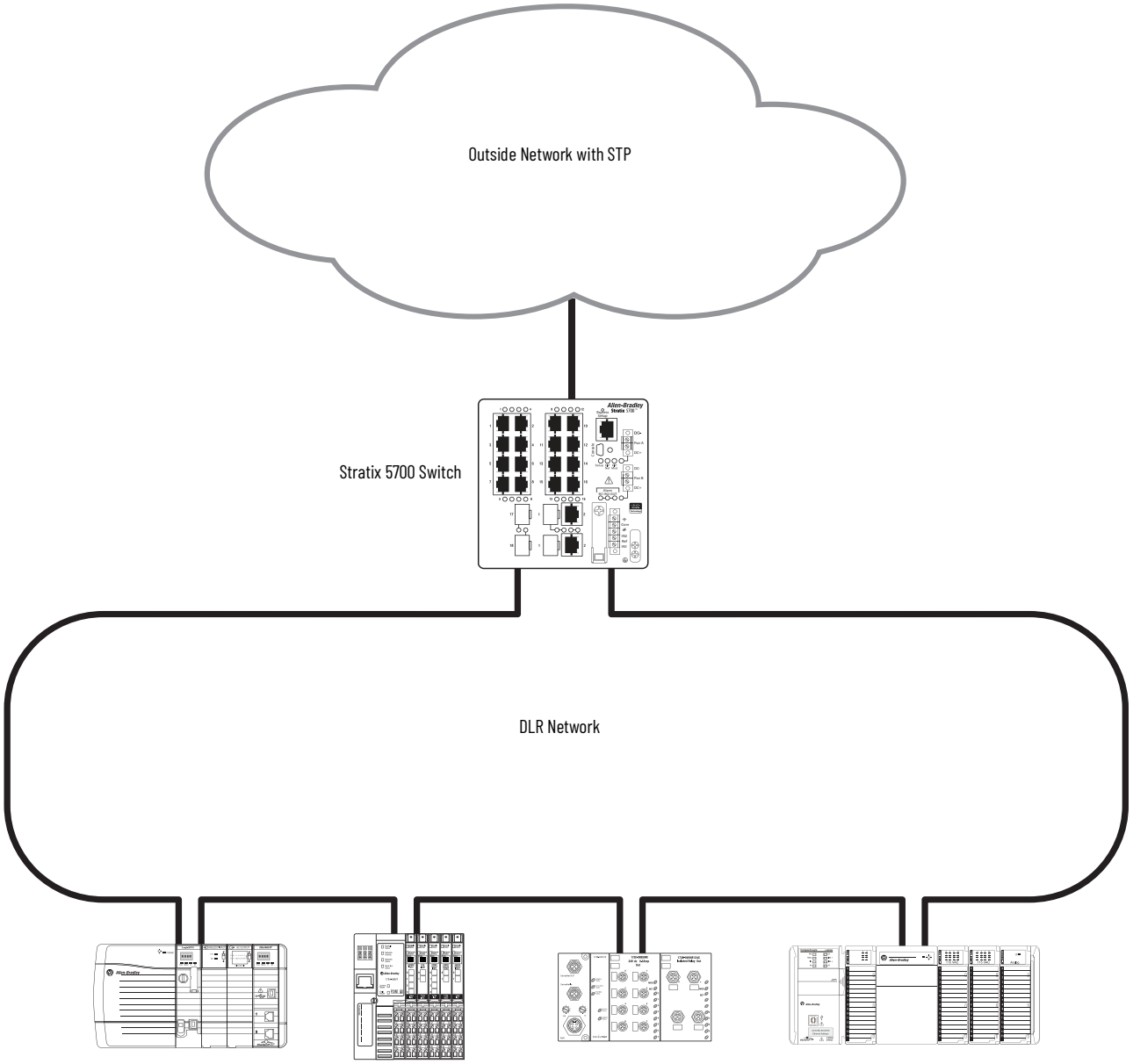
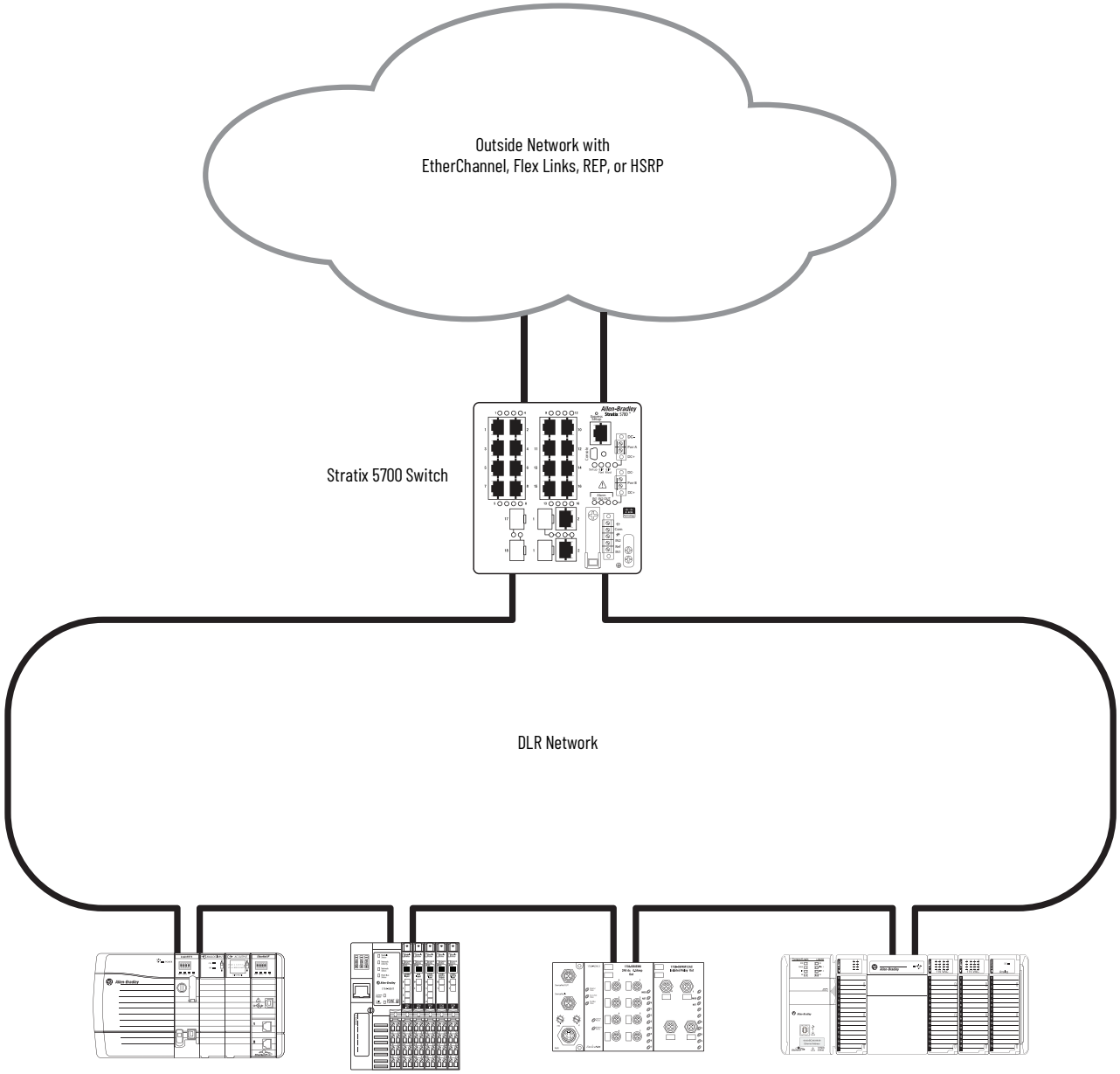


Figure 12 shows a Stratix switch with two uplink ports that are connected to a network that uses EtherChannel, Flex Links, REP, or HSRP for resiliency.

Figure 12 - Single Switch Uplink to Network with EtherChannel, Flex Links, REP, or HSRP

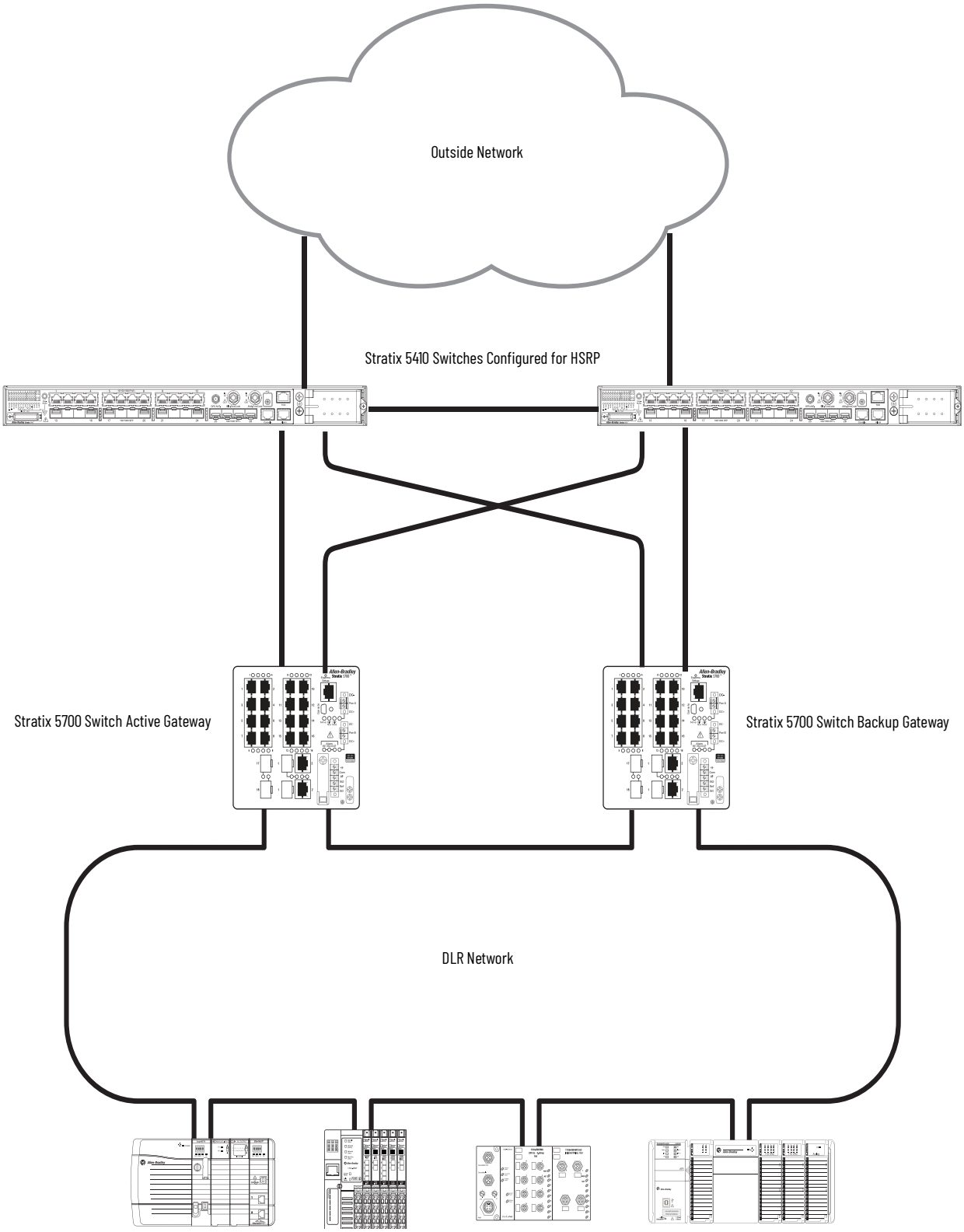


Redundant Gateways with Uplinks to Outside Network via HSRP

In the example shown in Figure 13, 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 13 - Redundant Gateways to Outside Network via HSRP



Ring with a DHCP Server

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 symmetric devices. The controller cannot detect incorrect IP addresses of identical devices in the wrong position.

DLR DHCP Example

Figure 14 shows an example of a Stratix 5700 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 Gi1/1, so the device connected to Gi1/1 has an index number of 2.

In Figure 14, the primary DLR DHCP server recognizes IP address requests from ring devices 3, 4, and 6 and responds with the position-based IP address that is specified in the DHCP table.

Figure 14 - DLR DHCP Example

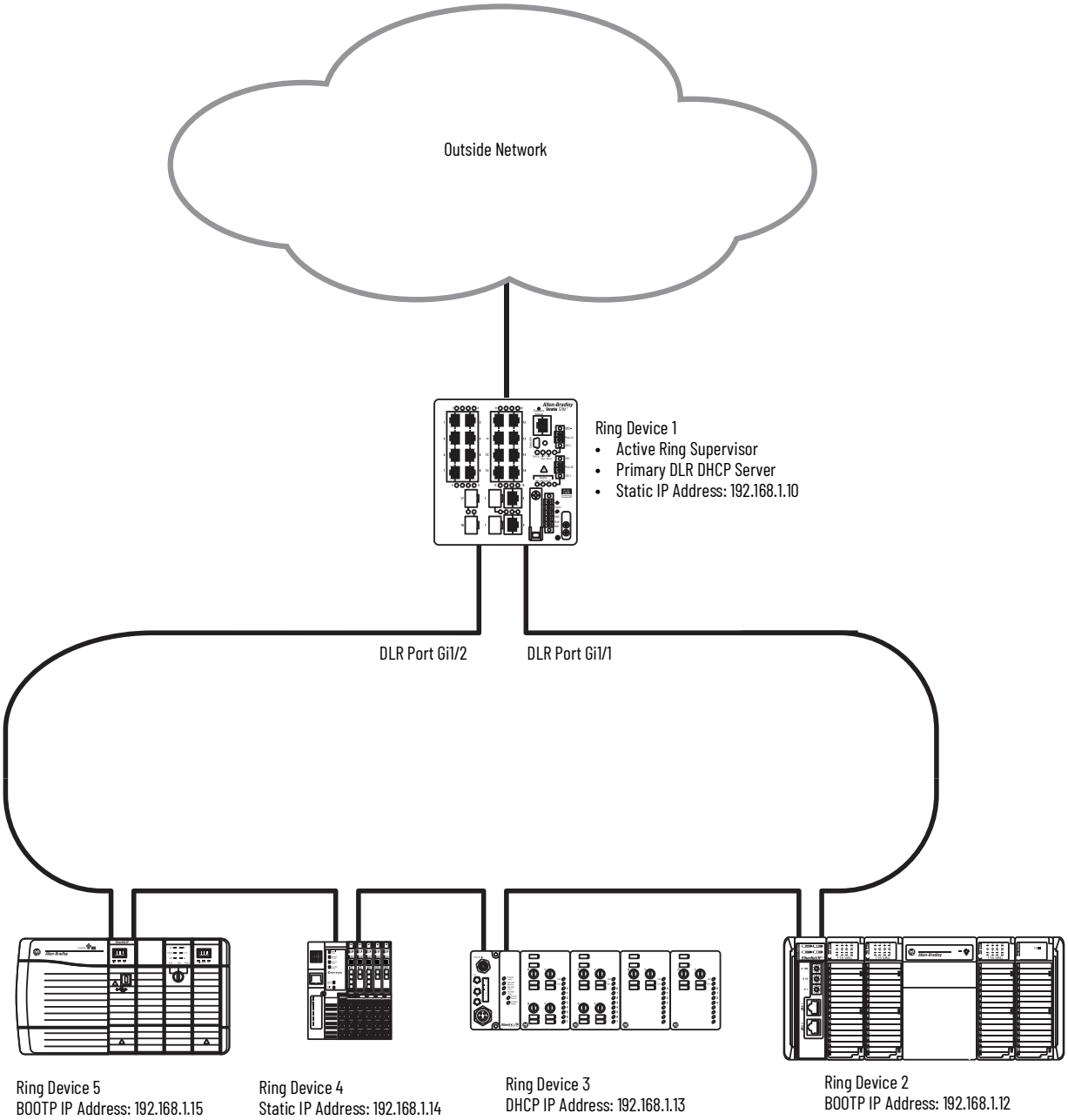


Table 1 - Example DHCP Table for Ring Devices

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.

For an example of how to configure a DLR network with DHCP, see page 56.

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.

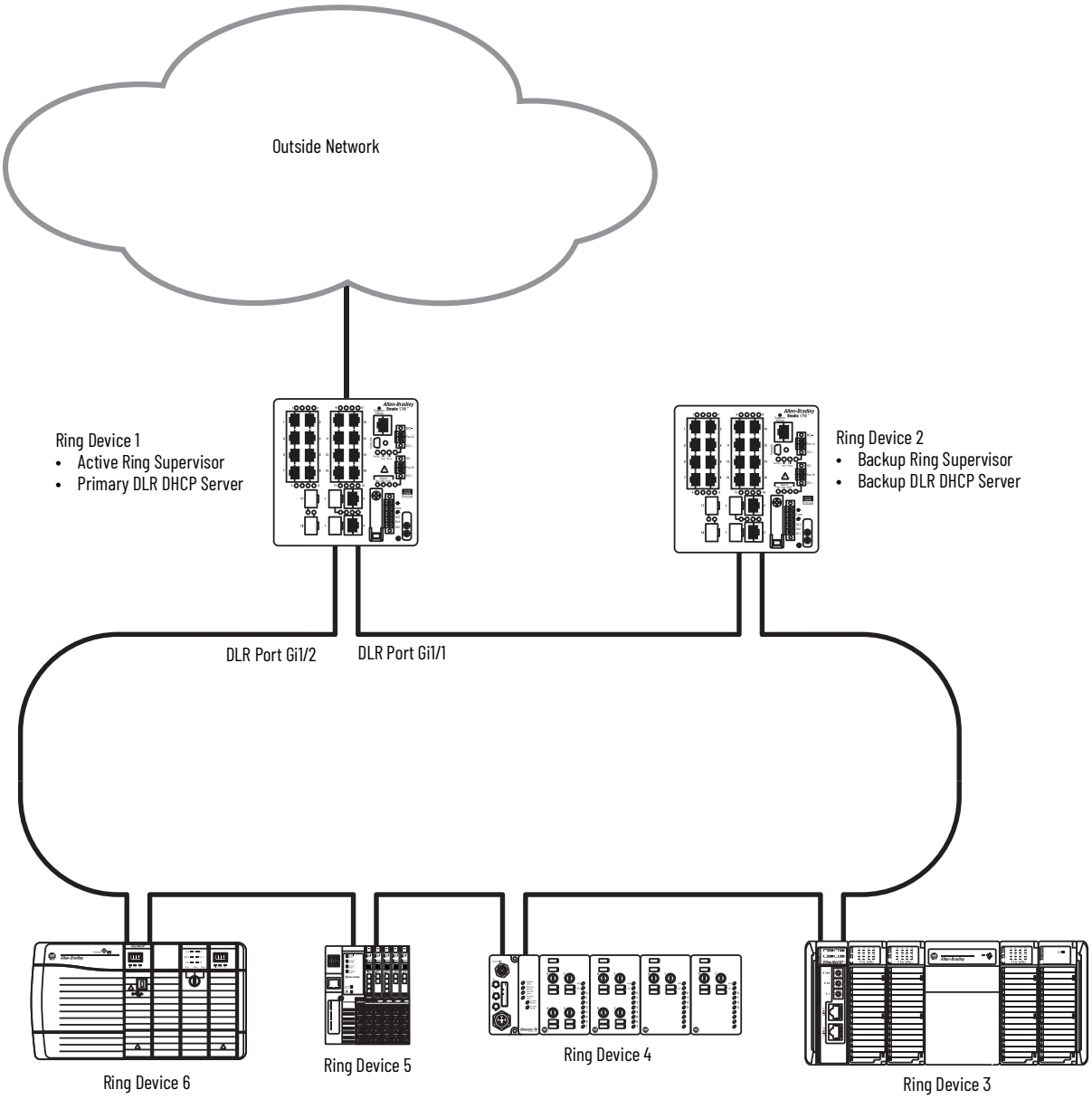
If the primary DLR DHCP server fails, the following happens:

- 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 15 shows a topology that includes a backup DLR DHCP server. A backup DLR DHCP server is an optional configuration.

Figure 15 - Optional Backup DLR DHCP Server



DHCP Snooping

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

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.

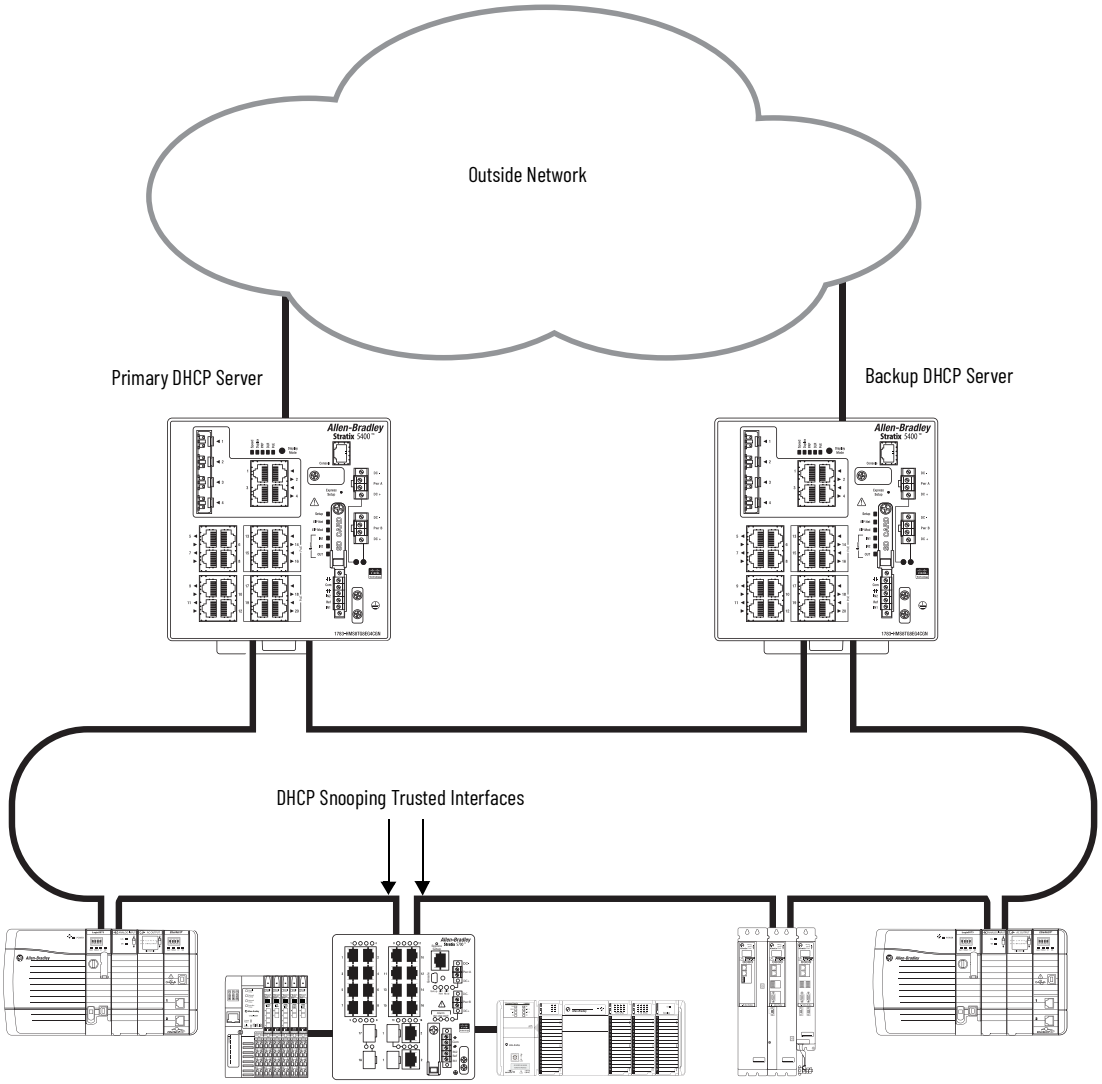
If DHCP snooping is disabled, DHCP address requests become broadcast messages and ring participants can receive an IP address from the first offer from a DHCP server within or outside of the ring.

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 16).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. To configure a DLR port as trusted interface, apply the following command to the port by using the command-line interface (CLI):

ip dhcp snooping trust

For information about how to access a Stratix switch via the CLI, see Knowledgebase article *Access CLI on a Stratix Switch*.

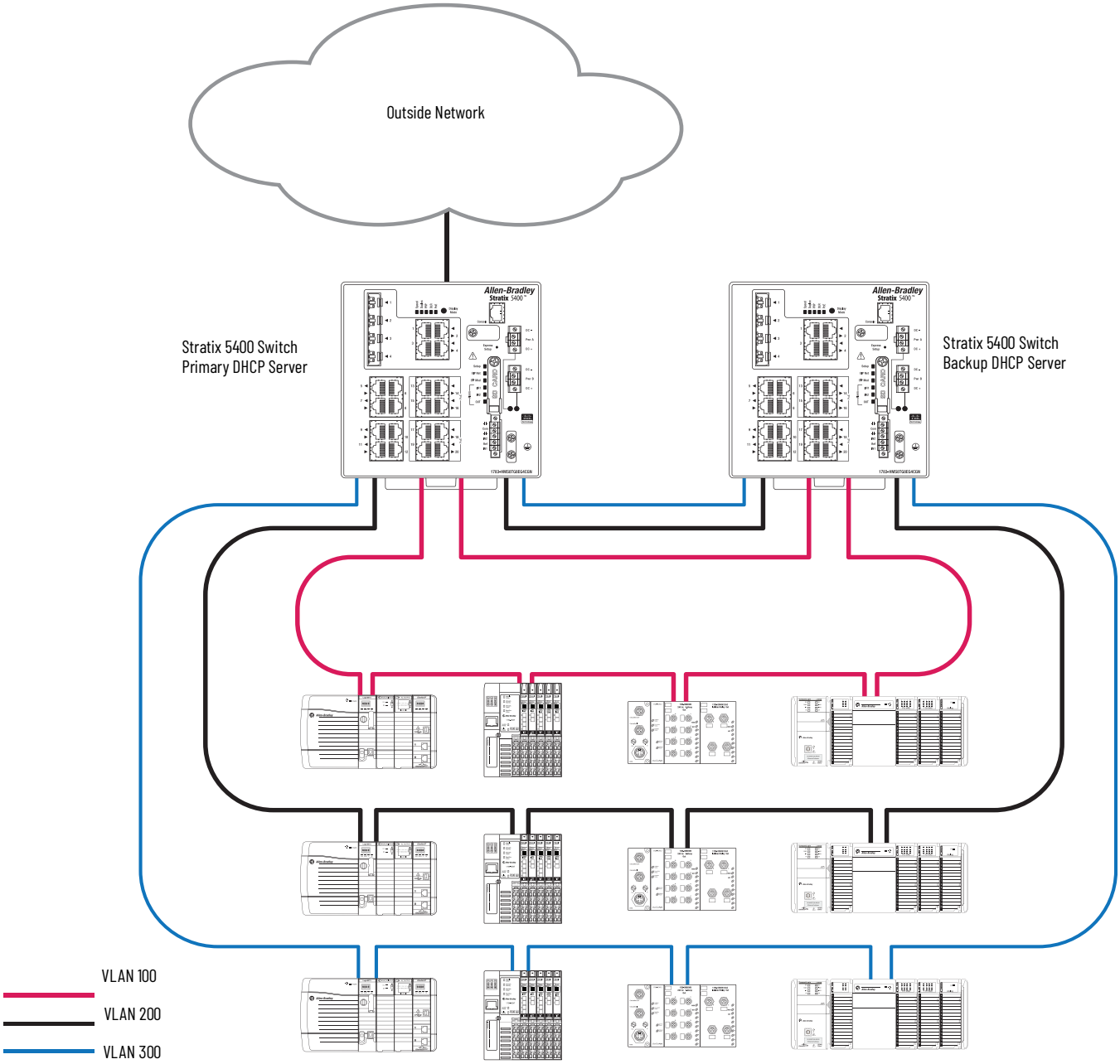
Figure 16 - DHCP Snooping Trusted Interfaces



DLR DHCP with Multiple VLANs and Multiple Rings

By using a Stratix 5400 switch, you can use DLR DHCP with multiple VLANs and multiple rings, as shown in Figure 17. In this example, both the primary and backup DHCP servers share the same CIP™ VLAN.

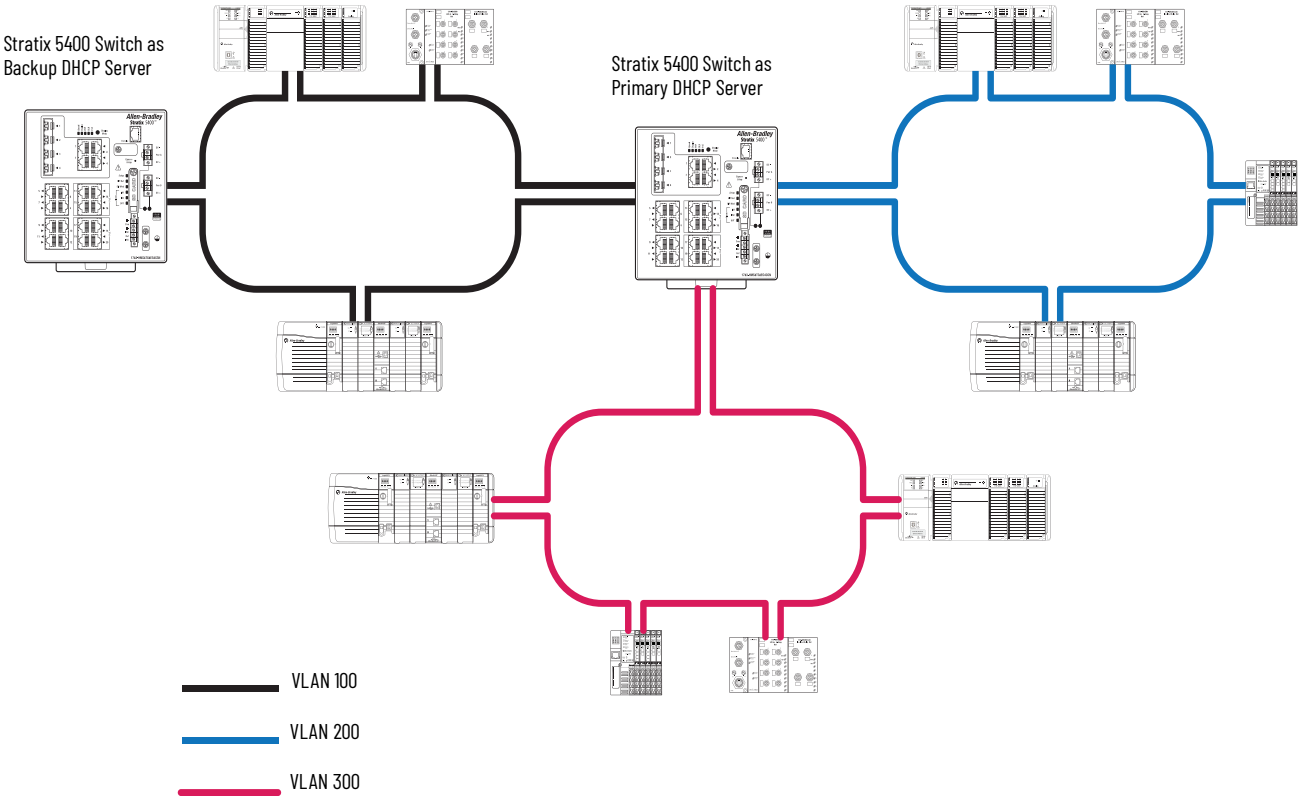
Figure 17 - DLR DHCP with Multiple Rings, Multiple VLANs, Same CIP VLAN



In some DLR topologies, the primary and backup DHCP servers must be use different CIP VLANs. Figure 18 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.

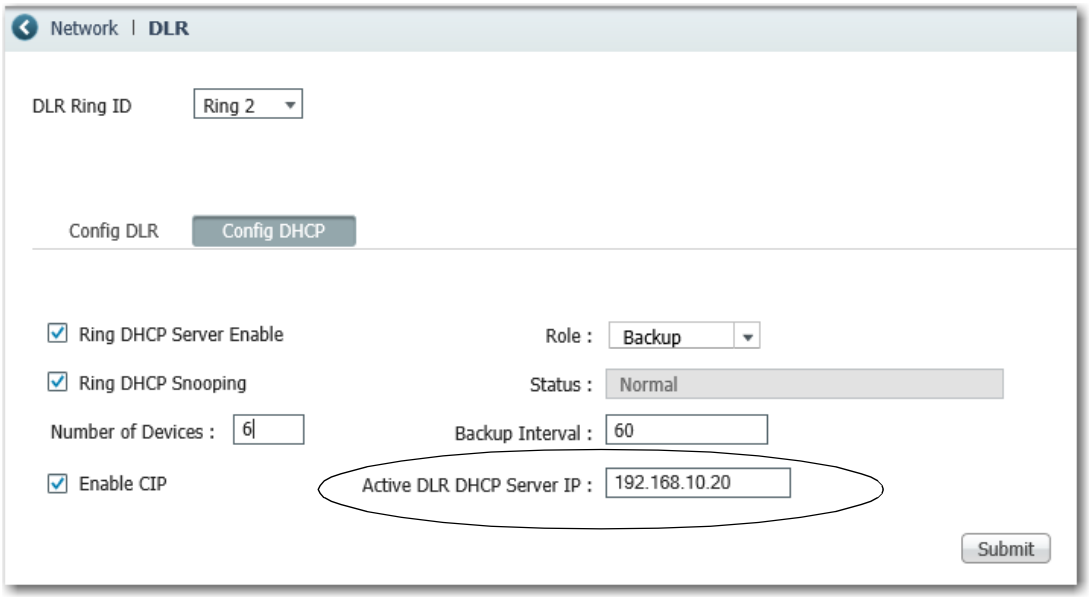
Figure 18 - DLR DHCP with Multiple Rings, Multiple VLANs, Different CIP VLANs



CIP VLAN Configuration

When both primary and backup DLR DHCP servers are used, you must specify the CIP VLAN IP address of primary server in the configuration for the backup server (Figure 19). The IP address enables the backup server to receive the DHCP configuration from the primary server if a switchover occurs.

Figure 19 - CIP VLAN IP Address of Primary Server in Configuration of Backup Server



In Figure 18, the primary DHCP server has the following IP addresses:

- 10.10.10.1 (CIP VLAN)
- 192.168.1.1
- 10.203.66.1

The backup DHCP server has IP address 192.168.1.4. The DHCP configuration for the backup DHCP server must include the CIP VLAN IP address for the active DHCP server: 10.10.10.1.

Multiple Rings

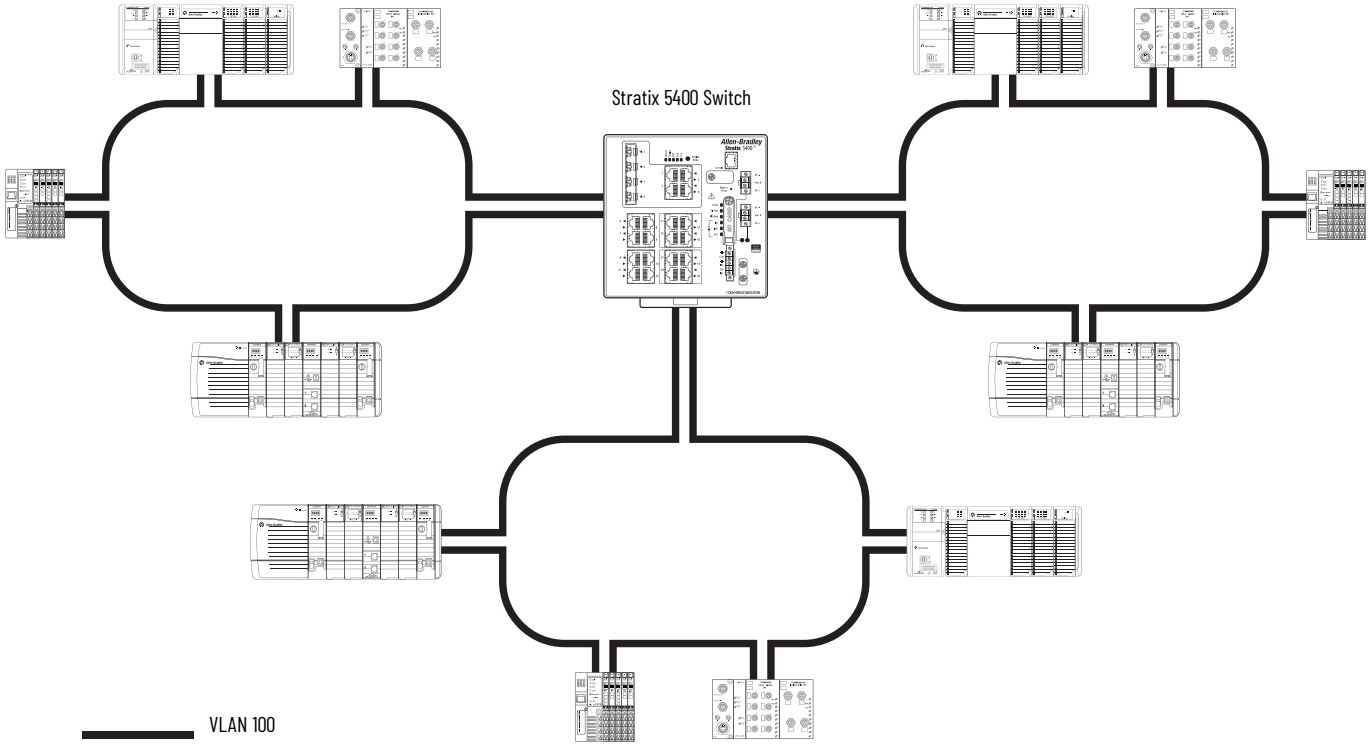
Stratix 5400 switches support as many as three rings with these restrictions:

- 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.

Multiple Rings Connected to a Single Switch

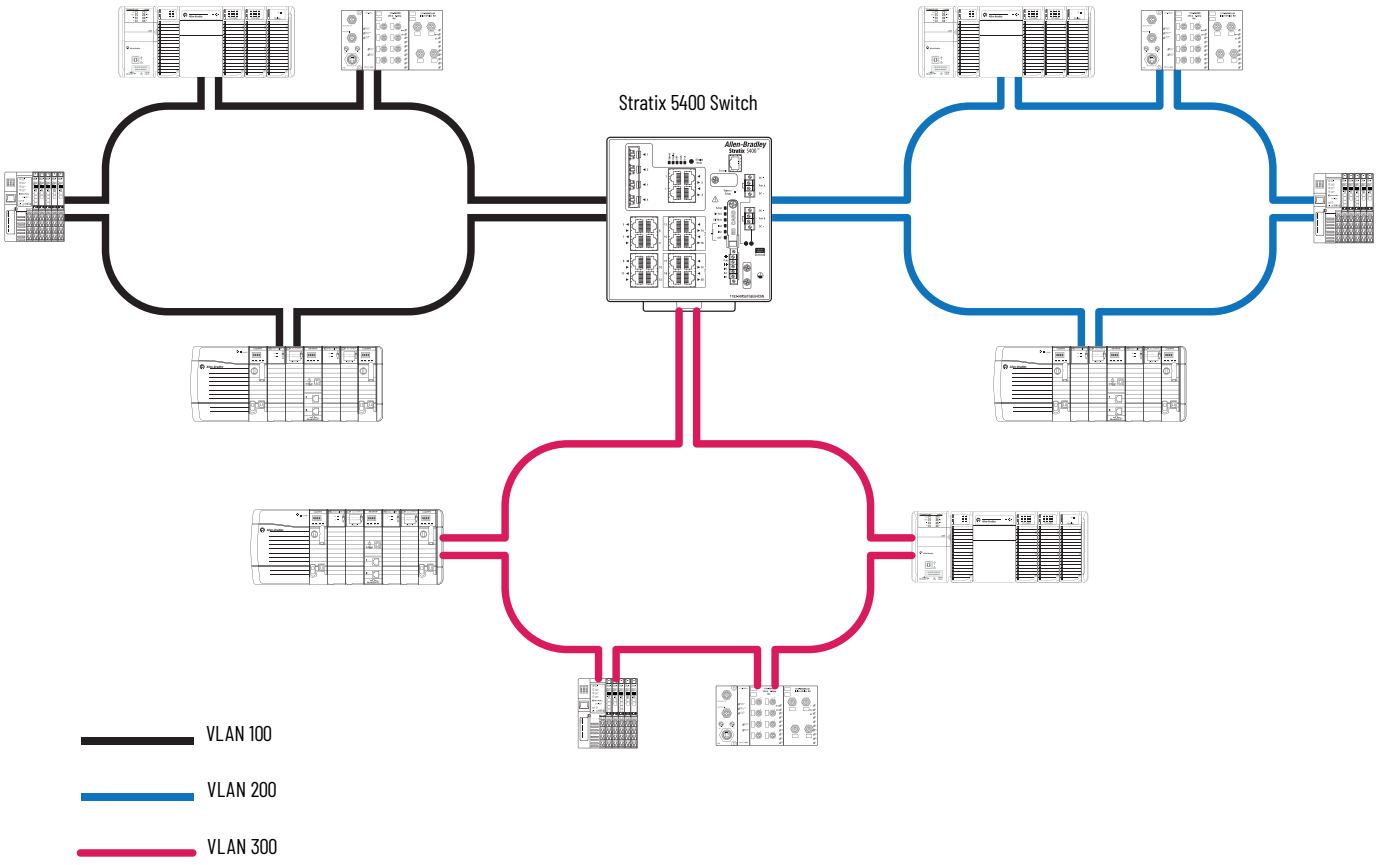
In Figure 20, multiple rings are connected to one switch on one VLAN.

Figure 20 - Multiple Rings, Single Switch, Single VLAN



Each ring can also be on a separate VLAN, as shown in Figure 21.

Figure 21 - Multiple Rings, Single Switch, Multiple VLANs

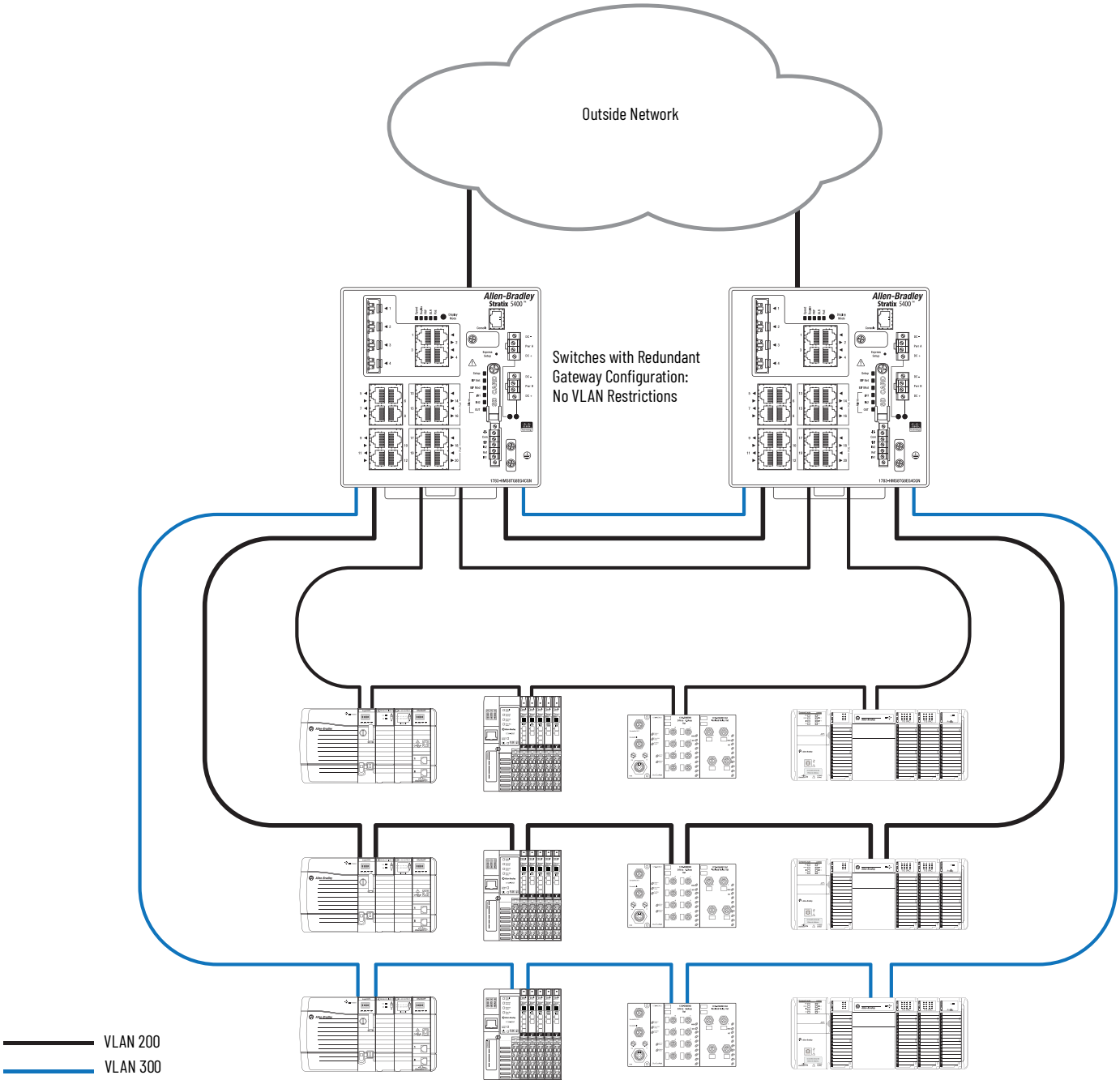


Multiple Rings Connected to Multiple Switches

You can also use multiple rings with multiple Stratix 5400 switches, as shown in Figure 22. Depending on the configuration of the switches, VLAN restrictions can apply.

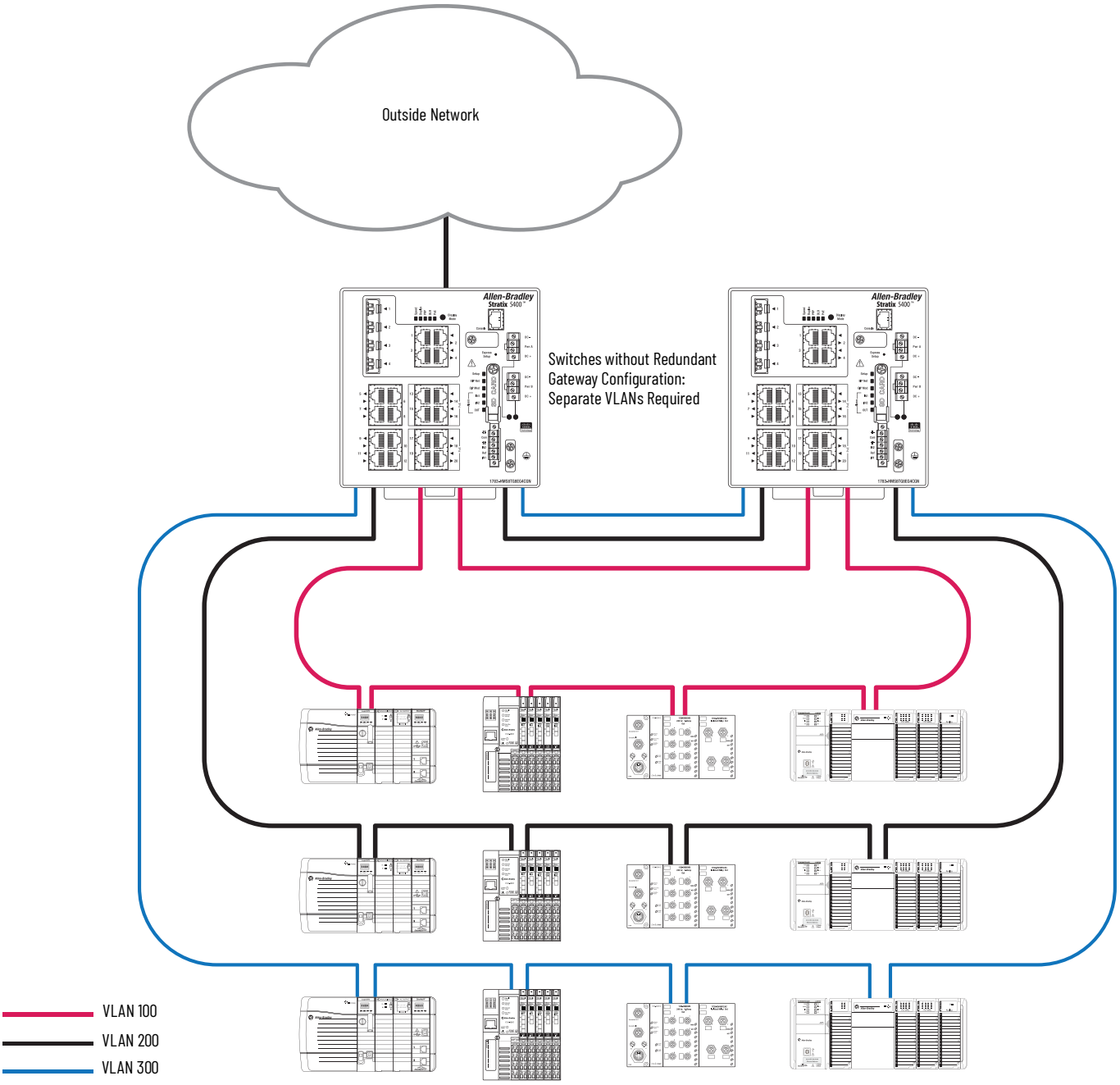
If the two switches are configured as redundant gateways on the same VLAN, no VLAN restrictions exist. The following example shows two rings on the same VLAN and one VLAN on a separate VLAN. However, because there are no VLAN restrictions, you could also configure all three rings on the same VLAN or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

Figure 22 - 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 23.

Figure 23 - VLANs Required



Multiple Rings with DHCP and Redundant Gateways

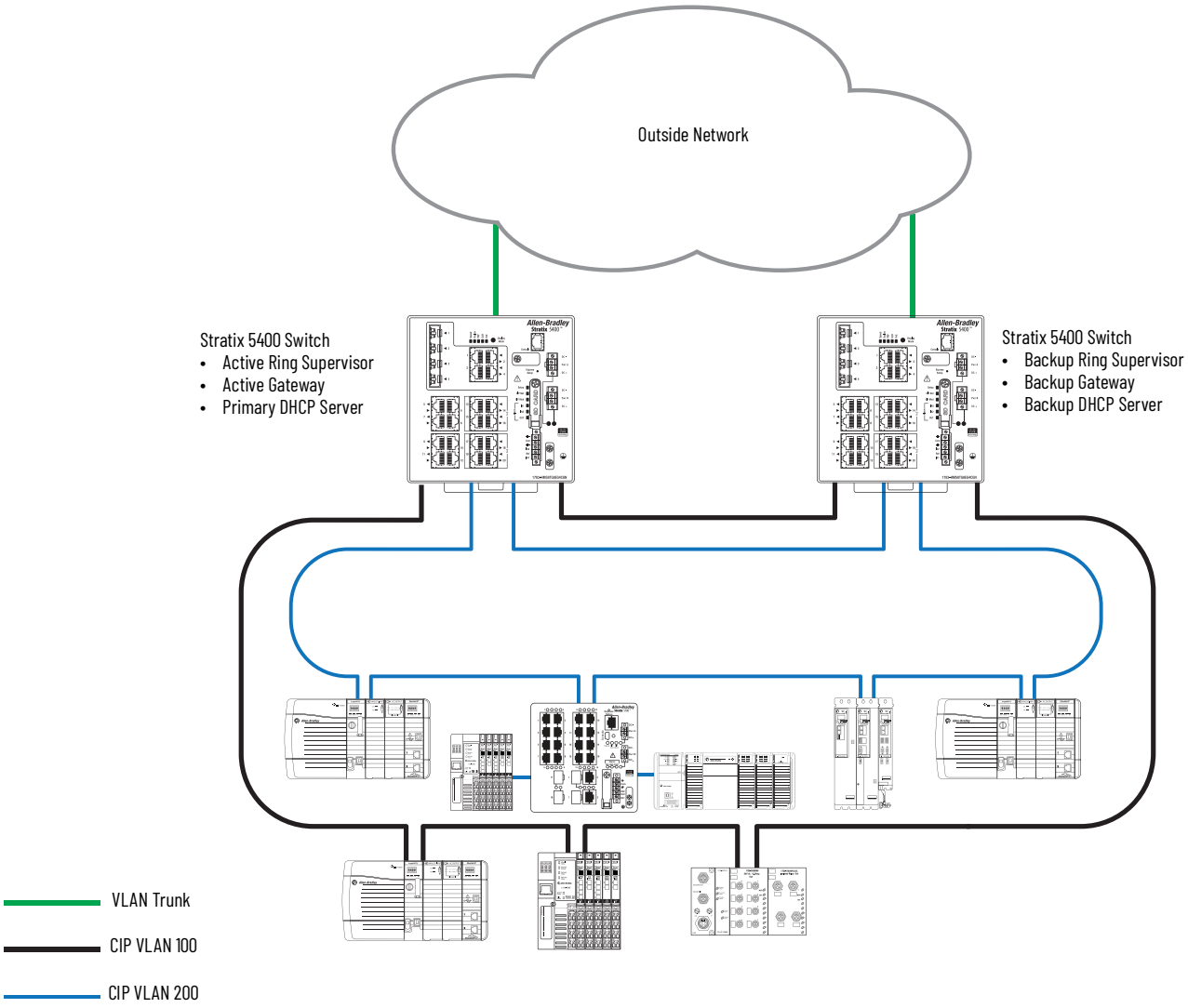
A DLR network with multiple rings can operate with all of these features (Figure 24):

- Multiple or single VLANs
- DLR DHCP
- Redundant gateways

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 24 - Multiple Rings, DLR DHCP, Redundant Gateways



ControlLogix Redundancy System with DLR

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

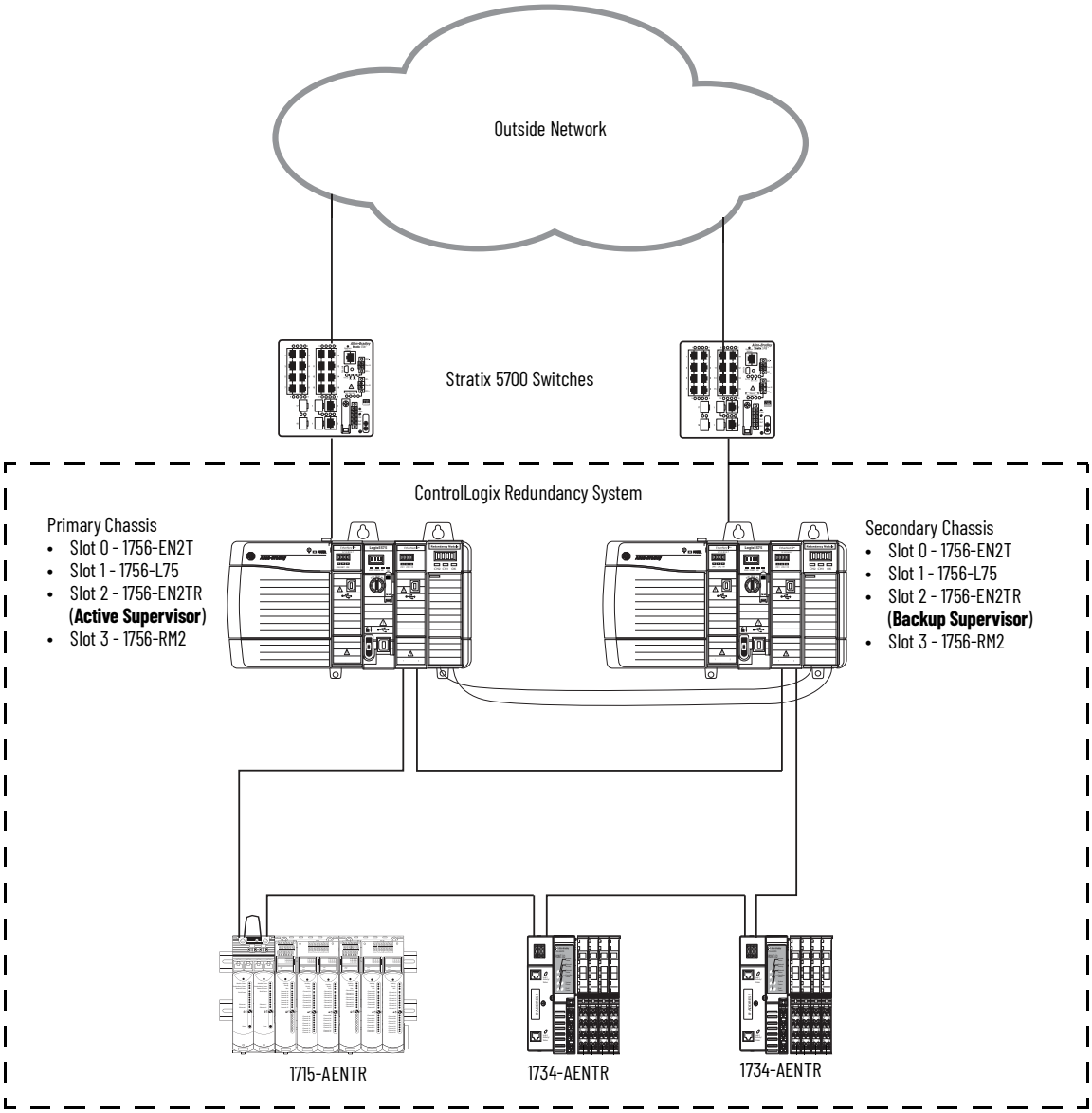
For more information about ControlLogix redundancy with DLR networks, see the following resources:

- 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*

In the example shown in Figure 25, the 1756-EN2TR module in the primary chassis is the active supervisor node, and the 1756-EN2TR module in the secondary chassis is the backup supervisor node.

IMPORTANT Do not connect a redundant chassis pair to a pair of switches that are configured as redundant gateways.

Figure 25 - DLR with Redundant Chassis Pair



ControlLogix Redundancy Crossload, Synchronization, and Switchover

A ControlLogix redundancy system uses the following functionality:

- Crossloading and synchronization transfer data from the primary controller to the secondary controller, so that the secondary controller can assume control if there is a switchover.

IMPORTANT	Crossloading and synchronization transfer DLR network configuration parameters. The active supervisor role is independent of the ControlLogix redundancy system and does not directly follow the primary chassis. It is possible that the active supervisor role does not transfer. We recommend that you verify that the active supervisor role that transfers with redundancy system data transfers from a primary controller to a secondary controller.

- In a switchover, the primary chassis and controller become the secondary chassis and controller, and the secondary chassis and controller become the primary chassis and controller. When the switchover occurs, partnered sets of EtherNet/IP™ communication modules can swap IP addresses, depending on the configuration.

  Switchovers result in a network break only if the primary chassis is no longer online. If a break occurs, the transition of the active supervisor role takes less than 3 ms. Keep in mind, the 3 ms time does not represent the time to change the primary and secondary chassis in the redundancy system.

Switchover That Does Not Break the DLR Network

If the switchover does not break the DLR network, the following occurs (Figure 26):

- The active and backup supervisor roles remain with the same physical devices, despite the chassis changing roles from primary to secondary and secondary to primary.
- As a function of redundancy, the active and backup supervisors swap IP addresses, but the MAC address values remain the same.

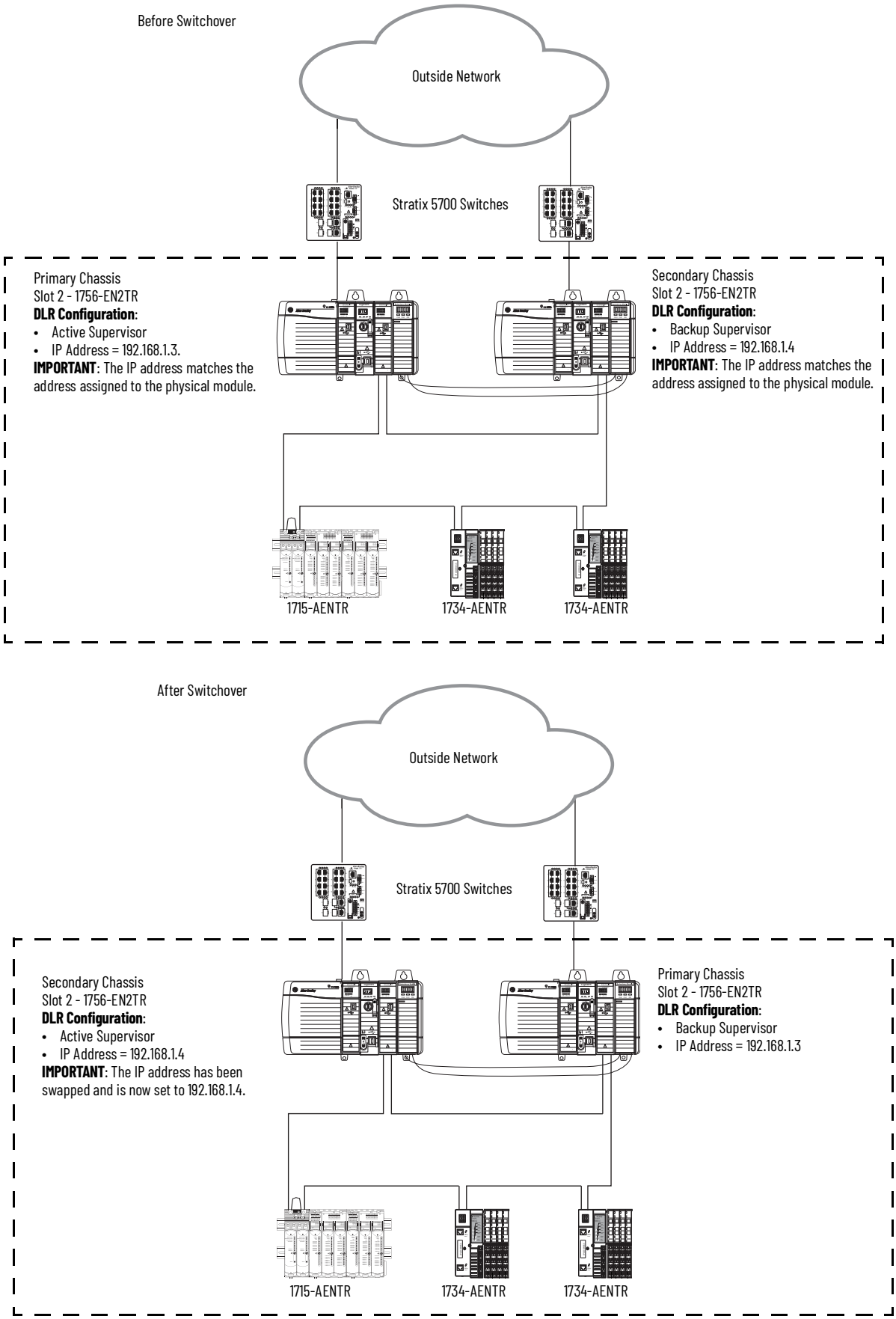
  The swapping of IP addresses does not break the DLR ring and does not cause active supervisor status to switch to the backup supervisor.

You can monitor the active supervisor node for status, as described in Command-line Interface on page 78. In this case, we recommend the following:

- Write your application code so it switches over to monitoring the active supervisor node at its new IP address.
- Write application code that monitors the active supervisor node and backup supervisor node.

  The application code checks the ring supervisor status of the active supervisor node and backup supervisor node to determine from which node to read diagnostic information.

Figure 26 - Switchover That Does Not Break DLR Network



Switchover That Breaks the DLR Network at the Active Supervisor

If the switchover breaks the DLR network at the active supervisor node, the following occurs (Figure 27):

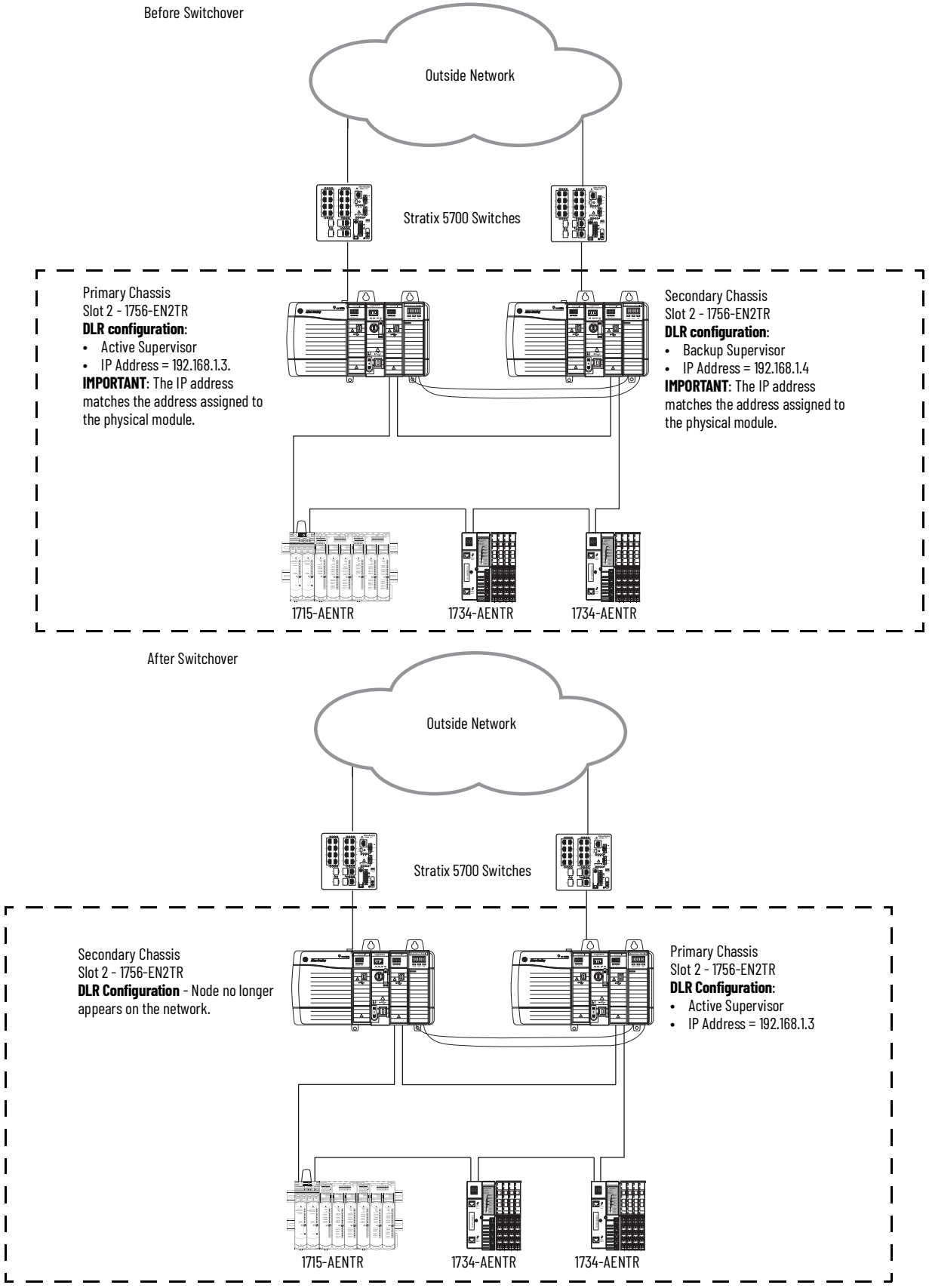
- The DLR network ring experiences a fault and transitions to a linear network.
- The backup supervisor node becomes the active supervisor node.
- Convergence time on the network is less than 3 ms, making the switchover seamless for the application.
- The partnered pair of EtherNet/IP modules that function as active and backup supervisor nodes swap IP addresses.

  The new active supervisor node uses the same IP address as the previous active supervisor node. This IP address swap is part of the redundancy system operation. In this case, the MAC address values remain the same.

If your application code is monitoring the active supervisor node for network status information, as described in Command-line Interface on page 78 continues to read that information from the same network address despite the fact that the active supervisor node is now a different physical node.

IMPORTANT In this example, the break in the DLR network at the active supervisor node is not a physical disconnection from the network.

Figure 27 - Switchover That Breaks DLR Network at Active Ring Supervisor



DLR 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.

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 to allow on each DLR-enabled trunk port.

IMPORTANT By default, trunk ports carry traffic from any VLAN. Be sure to 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, configure DLR VLAN trunking on Stratix 5400 switches.

DLR VLAN Trunking Examples

The following examples show DLR VLAN trunking in these network topologies:

- One ring with routing in the outside network (Figure 28)
- Multiple rings with routing within each ring (Figure 29)
- Multiple rings with a routing in the outside network (Figure 30)

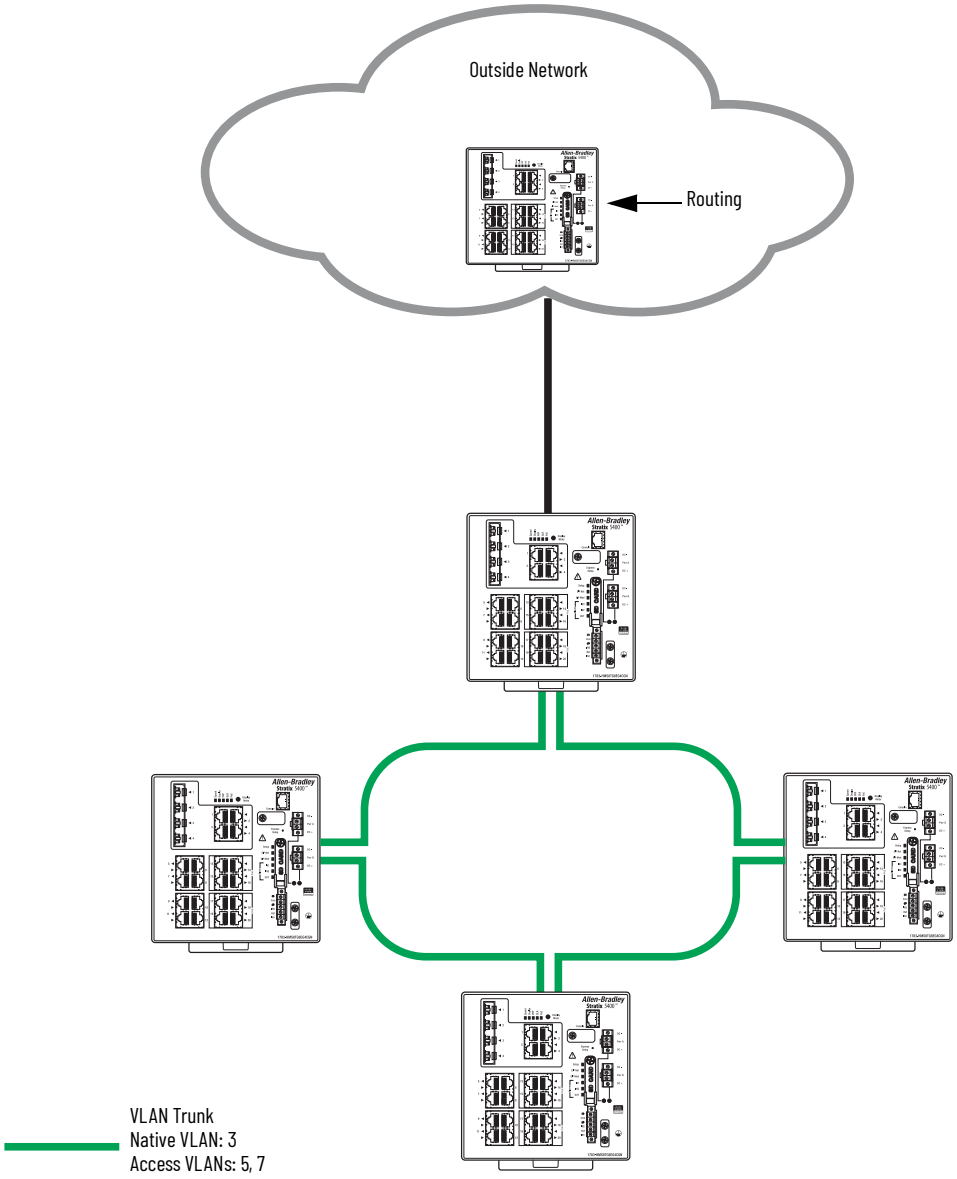
Each network includes Stratix 5400 switches for best performance.

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

Figure 28 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

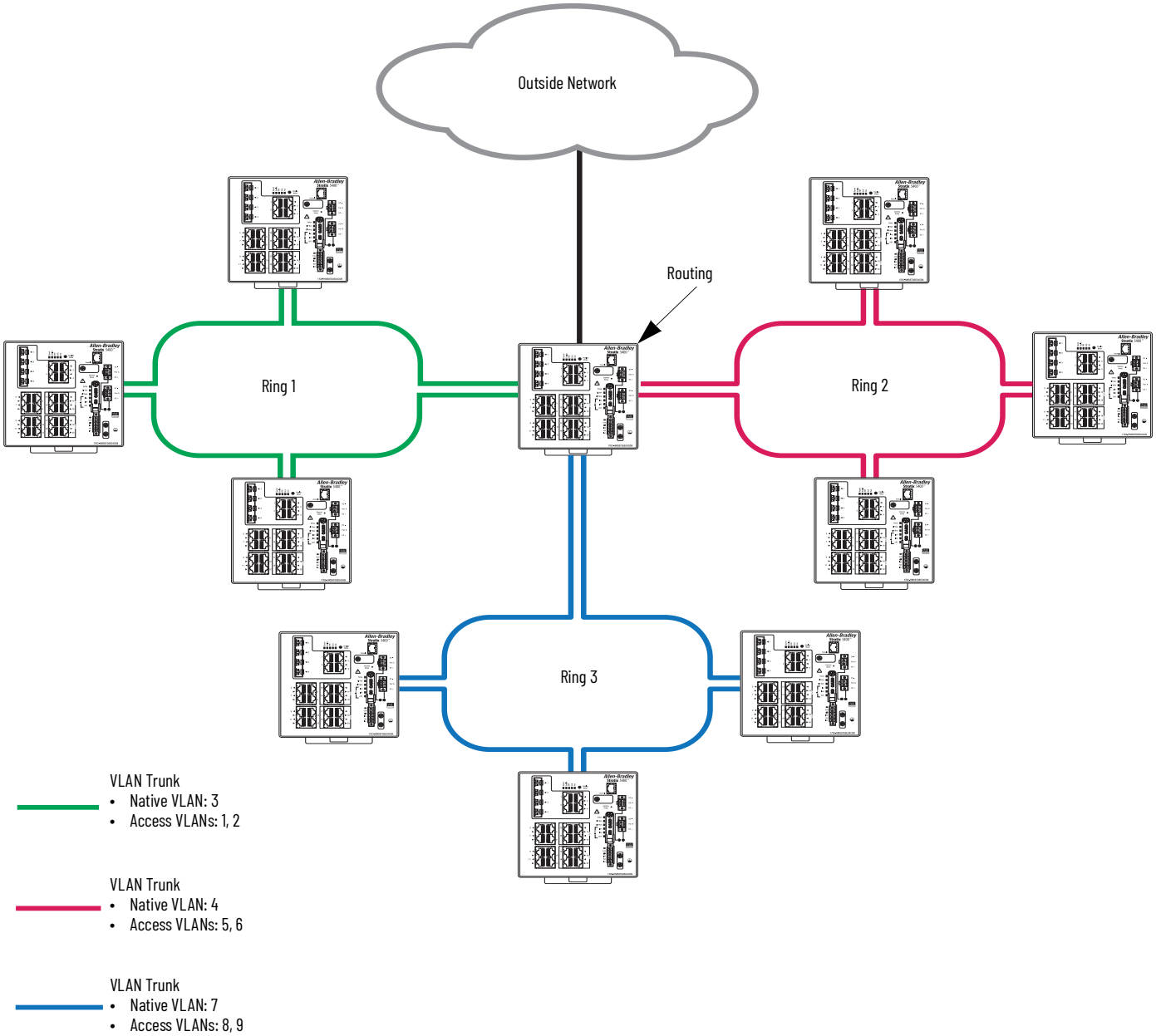
Figure 28 - DLR VLAN Trunking—One Ring



In the example shown in Figure 29, routing is performed within each ring:

- 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.

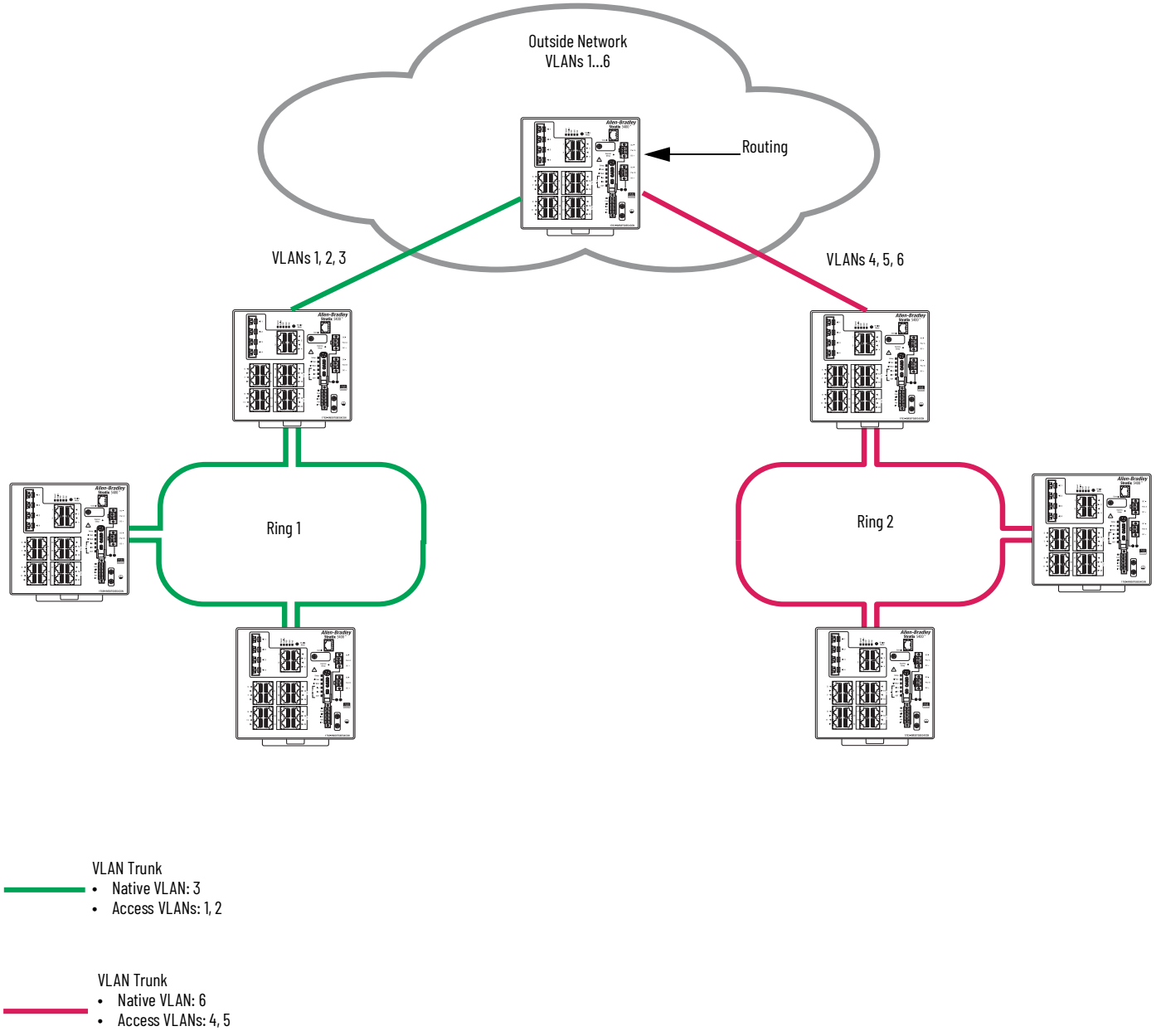
Figure 29 - DLR VLAN Trunking—Multiple Rings, Switch with Routing within Rings



In the example shown in Figure 30, 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.

Figure 30 - DLR VLAN Trunking—Routing in Outside Network



Unsupported Topologies

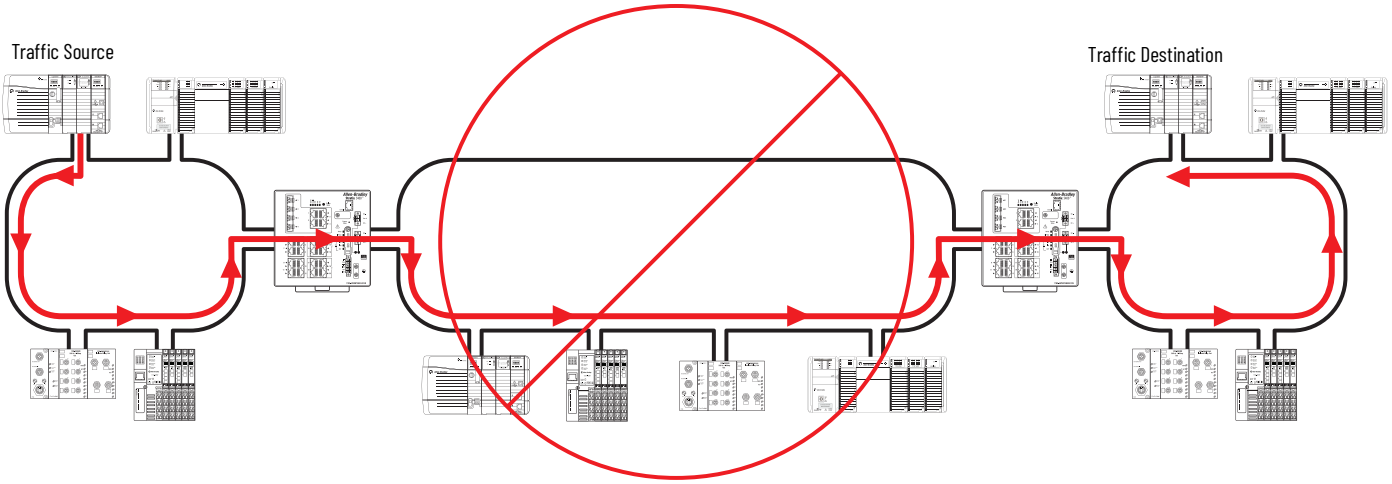
IMPORTANT Depending on your network architecture, DLR topology limitations can exist.
Be sure to validate your DLR topology within the larger network before production use.

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

For networks that do not use DLR VLAN trunking, a topology where traffic flows nonstop through one or more rings is not supported. For example, in Figure 31, traffic flows from its source in ring 1 through ring 2 without stopping before it reaches its destination in ring 3.

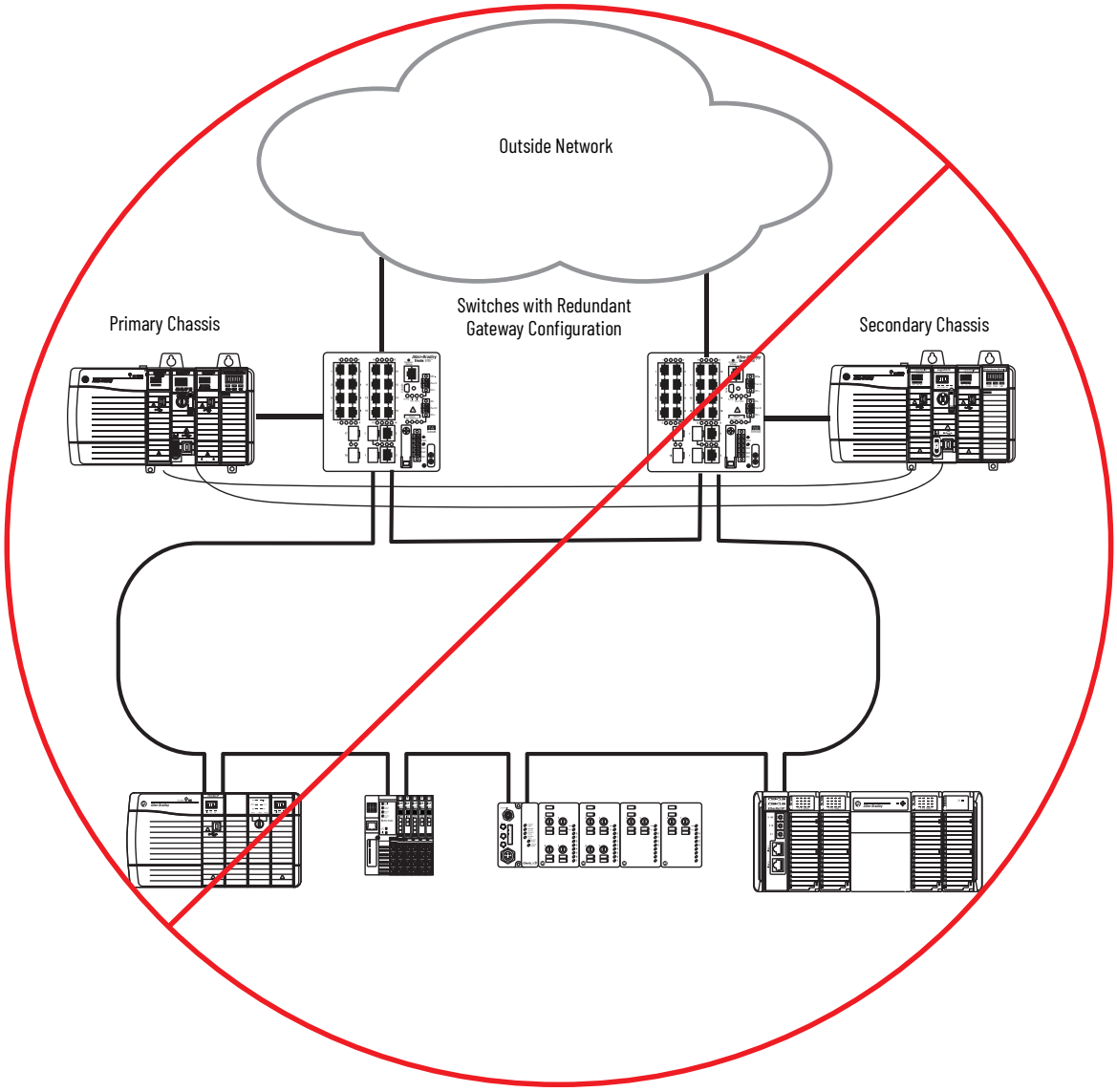
For networks that use DLR VLAN trunking, a topology where traffic flows nonstop through a series of trunked rings is not supported. However, traffic can flow nonstop through one trunked ring.

Figure 31 - Nonstop Traffic Through One or More Rings



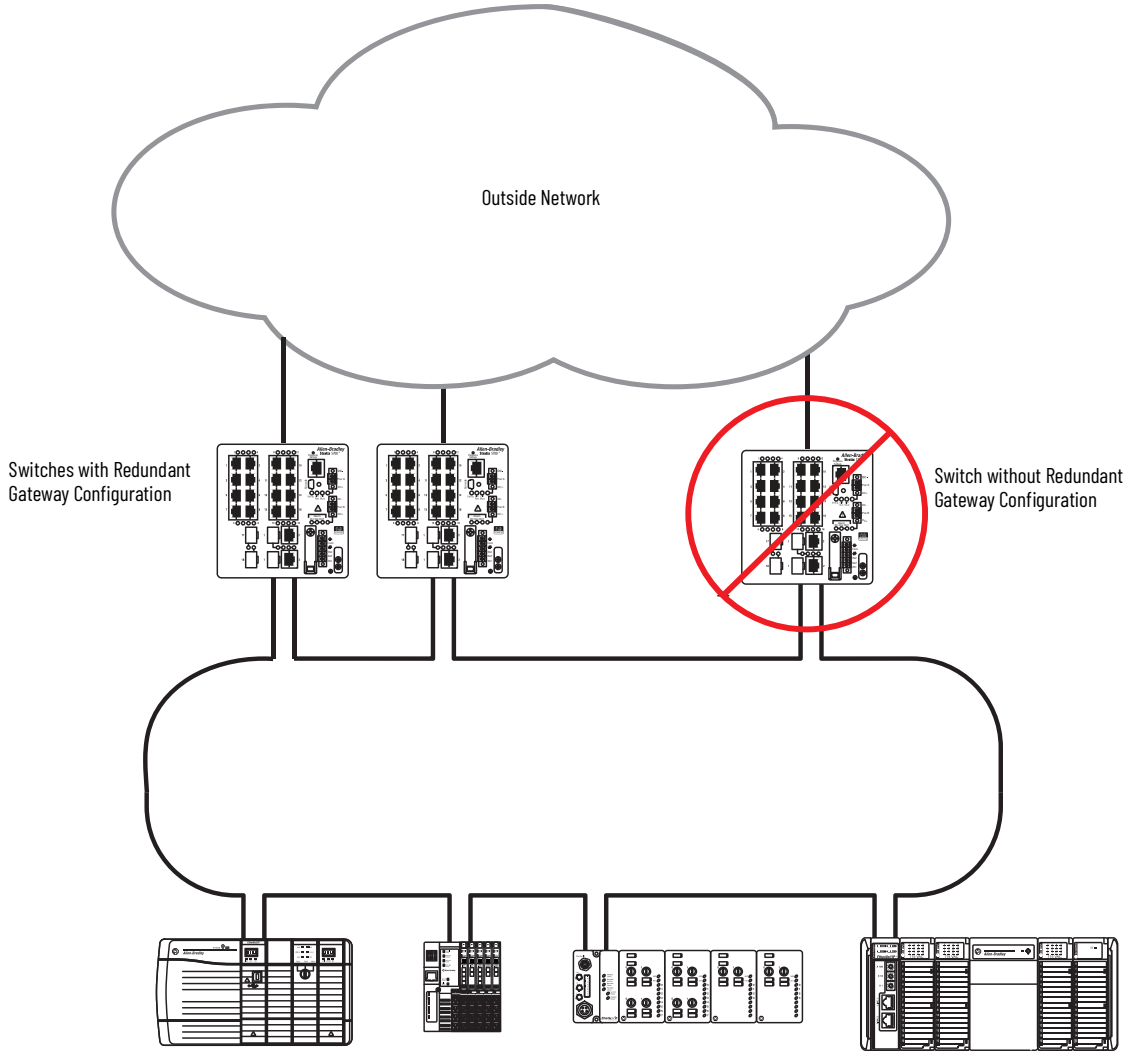
In a ControlLogix redundancy system, do not connect redundant chassis pairs to DLR redundant gateways (Figure 32).

Figure 32 - 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 33).

Figure 33 - Uplink via Redundant Gateways and Non-Redundant Gateway Switch



Media

DLR network connections can be copper, fiber, or a combination of both. To find specifications for Ethernet taps, Stratix switches, and SFP modules, see the Stratix Ethernet Device Specifications Technical Data, 1783-TD001. To choose a cable type, use the following guidelines.

Cable Type	Data Rate	Distance, max	Device Compatibility
Singlemode fiber (SMF)	100 Mbps 1 Gbps 10 Gbps	10 km (32,808 ft); 1 Gbps 10 km (32,808 ft); 10 Gbps	Stratix switches
Multimode fiber (MMF)	100 Mbps 1 Gbps 10 Gbps	2000 m (6561 ft); 1 Gbps 400 m (1312 ft);10 GBps	Ethernet taps (100 Mbps only) Stratix switches
Copper	100 Mbps 1 Gbps 10 Gbps	100 m (328 ft)	Ethernet taps (100 Mbps only) Stratix switches

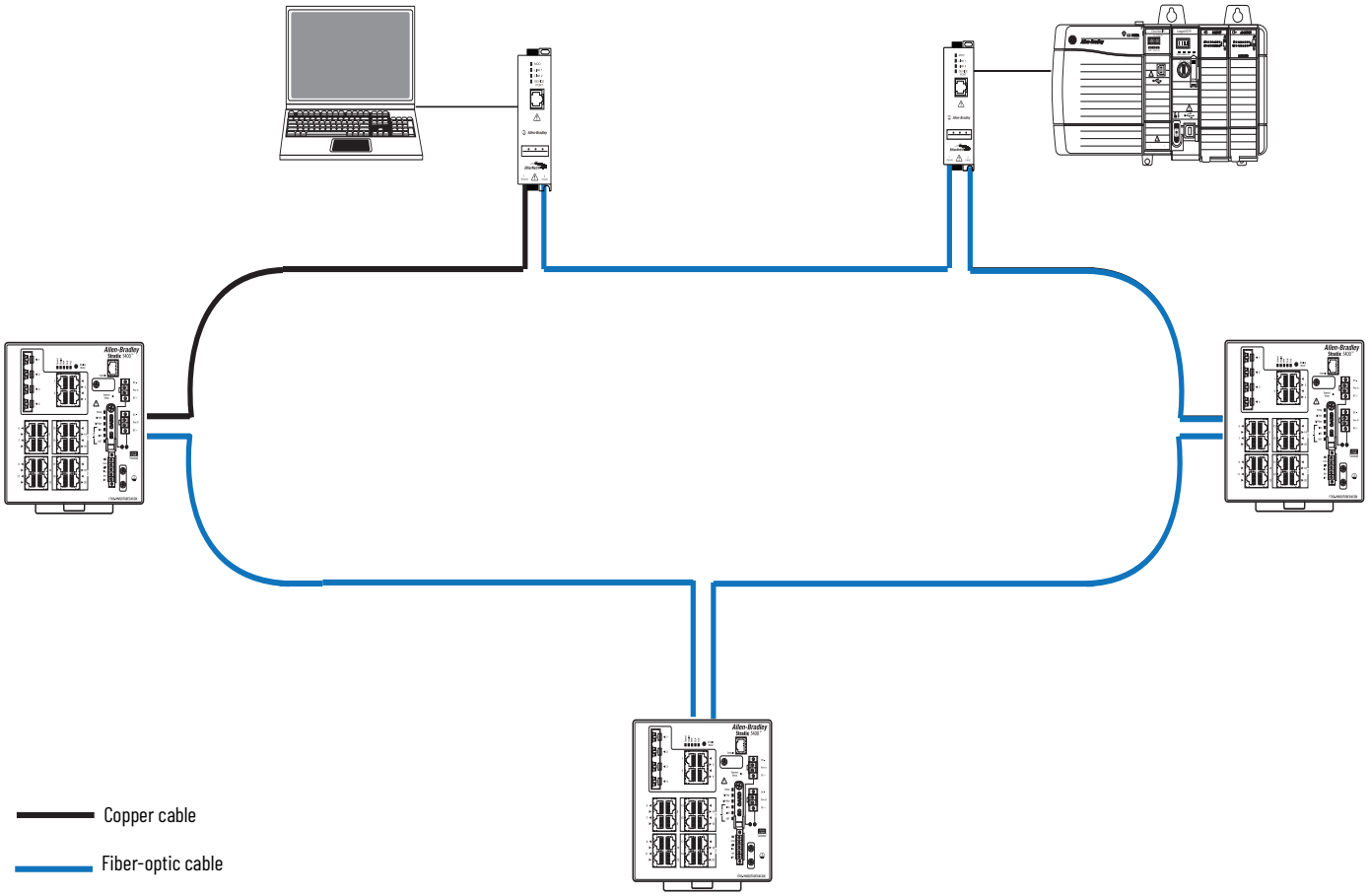
Figure 34 shows devices and switches in a DLR network with a mix of media.

Fiber-optic cable is used to connect these devices:

- Ethernet tap to Ethernet tap
- Ethernet tap to Stratix switch
- Stratix switch to Stratix switch

Copper cable is used to connect the Stratix switch to the Ethernet tap.

Figure 34 - Mixed Media in DLR Network



For more information on using fiber media to extend a DLR network across long distances, see the Deploying a Fiber Optic Physical Infrastructure within a Converged Plantwide Ethernet Architecture Application Guide, publication ENET-TD003.

Notes:

Configure a DLR Network

Configure a DLR network in this order:

1. Install Devices on a DLR Network.
2. Configure a Ring Supervisor.
3. Complete the Physical Connections of the Network.

See the following examples for step-by-step instructions:

- Configuration Example for a 1756-EN2TR Device on page 54
- Configuration Example for Stratix Switches on page 56

Install Devices on a DLR Network

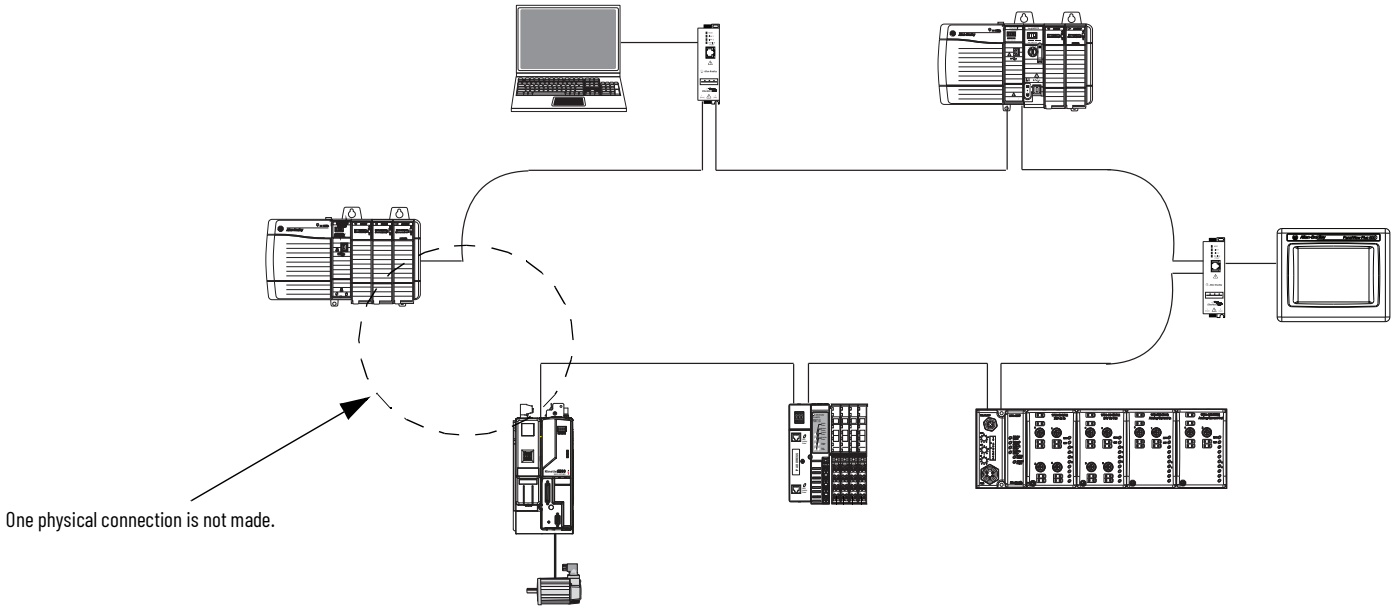
To configure a DLR network, start with a linear network by temporarily leaving the Ethernet segment between two nodes disconnected from each other.

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 35 - 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/.

Configure a Ring Supervisor

You must configure at least one ring supervisor.

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.

Rockwell Automation recommends the following configuration guidelines for supervisor nodes:

- Configure at least one backup ring supervisor.
- Configure the active ring supervisor with a numerically higher precedence value than the backup supervisors.
- Know the supervisor-precedence values for all supervisor-enabled nodes in your network.

Depending on whether the ring supervisor is a device or a switch, you can use the following methods to enable a ring supervisor.

Figure 36 - Methods to Enable Ring Supervisor

Enable Method	Device	Switch
Logix Designer application	Yes	Yes
RSLinx® Classic software	Yes	No
DIP switches(1)	Yes	No
Device Manager web interface	No	Yes
Command-line interface (CLI)	No	Yes

(1) DIP switches are available only on some devices. To use the DIP switches on a device to enable the ring supervisor function, see the installation guide for the device.

For configuration instructions, refer to the user manual or Help for the device or switch.

For an Ethernet tap operating as a ring supervisor, follow these guidelines:

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

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.

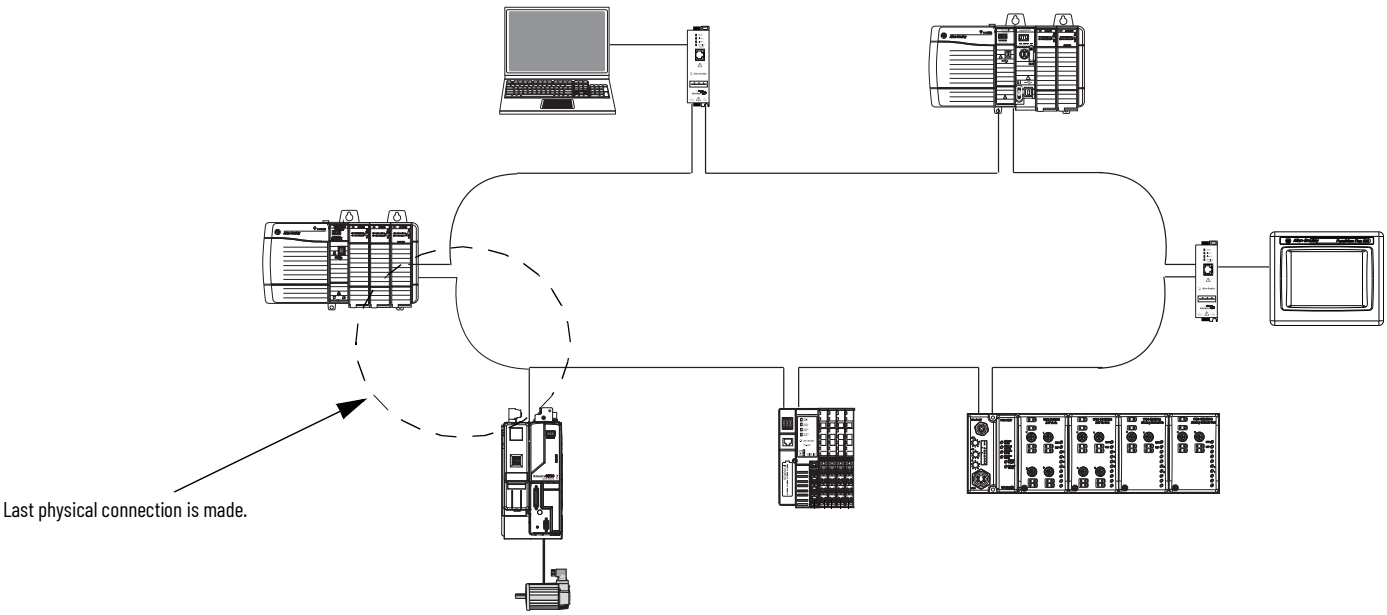
IMPORTANT If you fully connect your DLR network without a supervisor configured, a network storm can result. A network storm can render the network unusable until one link is disconnected and at least one supervisor is enabled.

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.

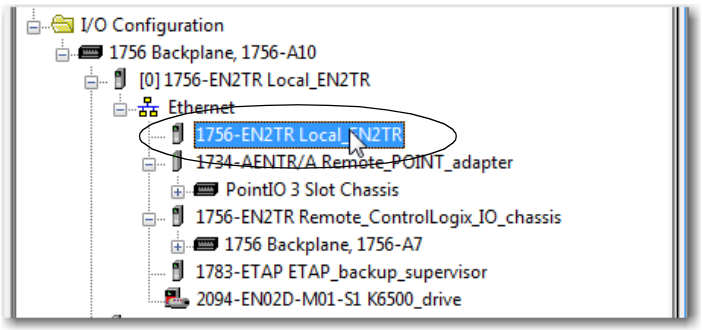
Figure 37 - DLR Network with All Links Connected



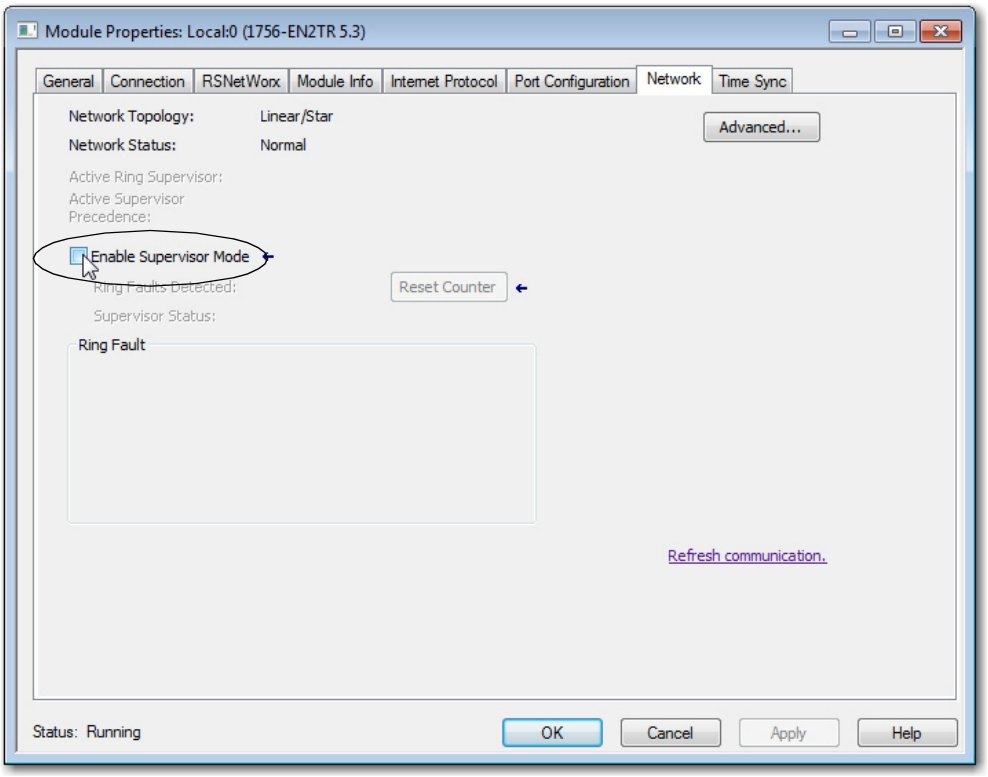
Configuration Example for a 1756-EN2TR Device

The following instructions show an example of how to configure a 1756-EN2TR device as a ring supervisor via the Logix Designer application.

1. With your controller project online, double-click a supervisor-capable device in the I/O configuration tree.

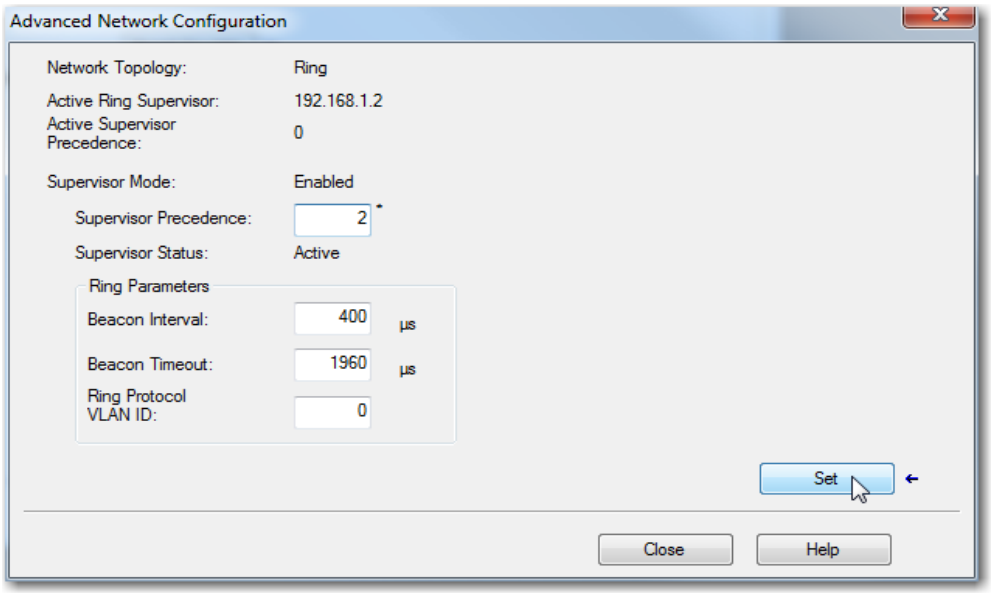


2. On the Network tab, check Enable Supervisor Mode.



3. To set supervisor-related parameters, click Advanced.

   For Beacon Interval, Beacon Timeout and Ring Protocol VLAN ID, we recommend that you use the default values.



Field	Description
Network Topology	Displays the current network topology: Valid values: • Linear/Star • Ring
Active Ring Supervisor	Displays the IP address or MAC address of the active ring supervisor.
Active Ring Supervisor Precedence	Displays the precedence that is currently assigned to the active ring supervisor.
Supervisor Mode	Displays whether the Supervisor mode of the device is enabled or disabled.
Supervisor Precedence	Specifies the supervisor precedence number when Supervisor mode is enabled. Valid values: 0…255 When multiple nodes are enabled as supervisor, the node with the highest precedence value is assigned as the active ring supervisor. The other nodes automatically become back-up supervisors. We recommend the following: • Configure at least one back-up supervisor node. • Set the desired active ring supervisor with a relatively high supervisor-precdence value compared to the back-up nodes. • Keep track of the supervisor-precedence values of a network.
Supervisor Status	Displays the status of the supervisor when Supervisor mode is enabled. Valid values: • Active—The device is the active ring supervisor. • Backup—The device is the backup ring supervisor. • Cannot support current Beacon Interval or Timeout—The device cannot support the beacon interval or timeout values of the current active ring supervisor.
Beacon Interval	Specifies the frequency at which the active ring supervisor transmits a beacon frame through both of its ring ports. Available when Supervisor mode is enabled. Valid values: 100…100000
Beacon Timeout	Specifies the amount of time that supervisor or ring nodes wait before timing out the reception of beacon frames and taking appropriate action. Available when Supervisor mode is enabled. The beacon timeout value must be at least 2 times the beacon interval value but not exceed 500,000.
Ring Protocol VLAN ID	Specifies the VLAN ID to use in the ring protocol message when Supervisor mode is enabled. Valid values: 0…4094

Configuration Example for Stratix Switches

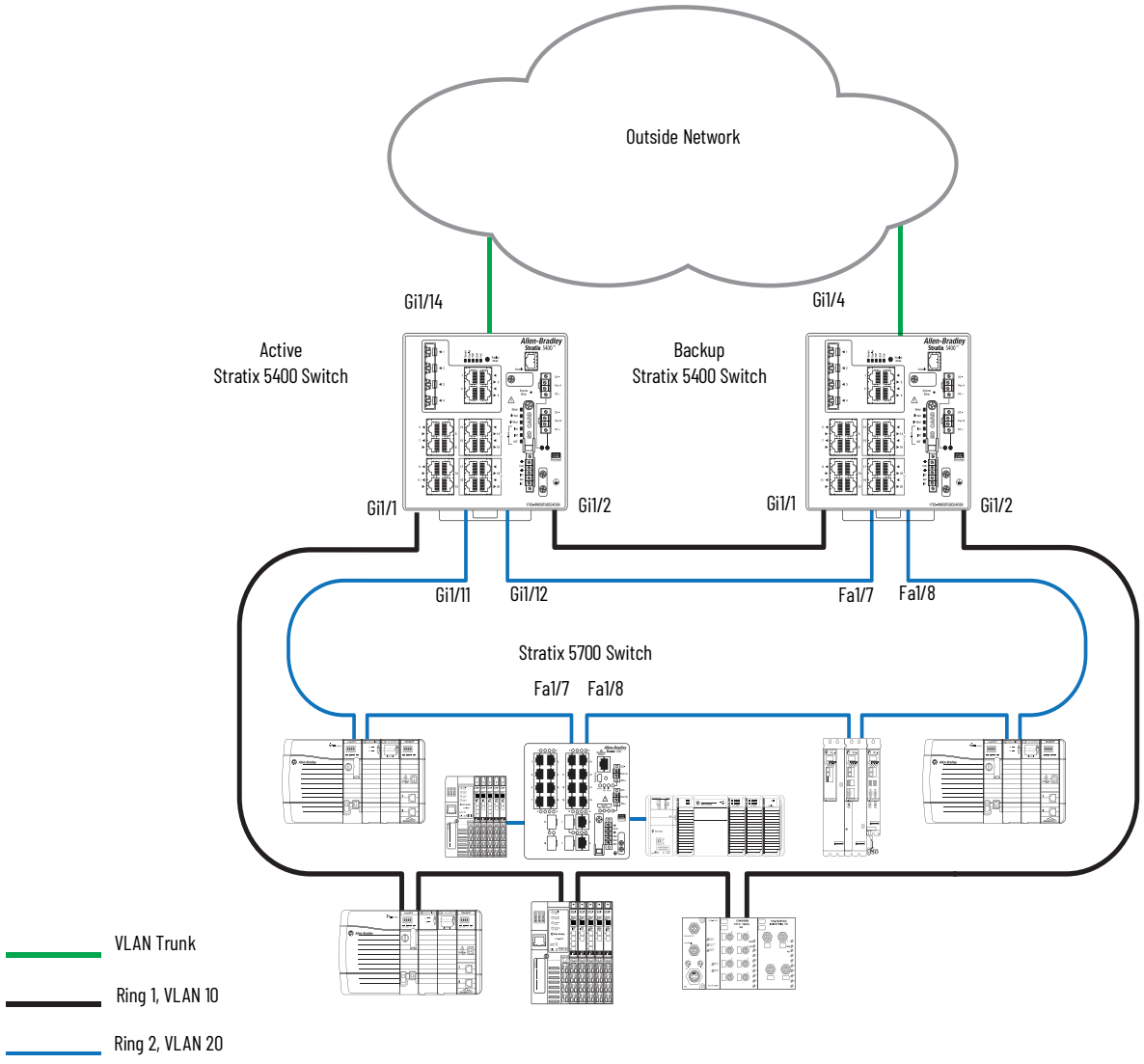
The following instructions show an example of how to configure Stratix® switches in a DLR network. As shown in Figure 38, the example DLR network includes these components:

- Two rings each on separate a VLAN
- Stratix 5400 switch as active ring supervisor, active redundant gateway (optional configuration), and primary DHCP server
- Stratix 5400 switch as backup ring supervisor, backup redundant gateway (optional configuration), and backup DHCP server
- Stratix 5700 switch as a ring participant on Ring 2

Configuration of the switches is completed via Device Manager.

IMPORTANT CIP™ is required for this topology and must be enabled on each switch.

Figure 38 - DLR Network with Redundant Gateways, Multiple CIP VLANs, and DHCP



To configure the example DLR network in Figure 38, complete the following procedures.

1. Configure the active Stratix 5400 switch (see page 57).
2. Configure the backup Stratix 5400 switch (see page 67).
3. Configure the Stratix 5700 switch on Ring 2 (see page 73).

Configure the Active Stratix 5400 Switch

In this example, the active switch is configured with these roles:

- Active redundant gateway (optional configuration)
- Active ring supervisor
- Active DHCP server for Ring 2

The active switch uses the configurations in the following tables.

Table 2 - Active Switch Port Configurations

Port	Connected Ring	VLAN
Gi1/1	Ring 1	10
Gi1/2	Ring 1	10
Gi1/11	Ring2	20
Gi1/12	Ring 2	20
Gi1/14	–	10 20

Table 3 - VLAN IP Addresses

VLAN	IP Address
10	192.168.10.20
20	192.168.20.20

The following table represents the DHCP table for Ring 2:

- Index 1 represents the active ring DHCP server and is not configurable.
- Index 4 represents a Stratix 5700 switch on Ring 2, which receives a statically assigned IP address during Express Setup.
- Index 6 represents the backup switch, which receives a statically assigned IP address during Express Setup.

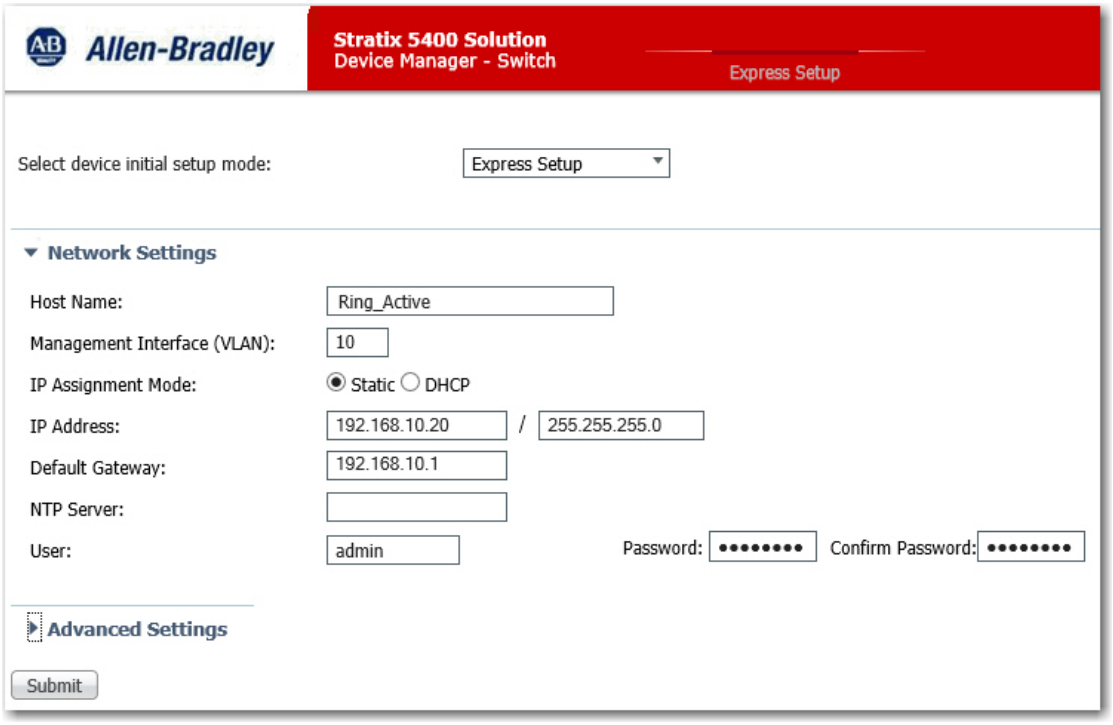
Table 4 - DHCP Table for Ring 2

Ring Device Index	IP Address	Host Name	DHCP Pool
2	192.168.20.30	DLR_Device_20_30	DLR_DHCP_POOL
3	192.168.20.31	DLR_Device_20_30	DLR_DHCP_POOL
4	Not applicable	Not applicable	Not applicable
5	192.168.20.32	DLR_Device_20_30	DLR_DHCP_POOL
6	Not applicable	Not applicable	Not applicable

To configure the active switch in this example, follow these steps.

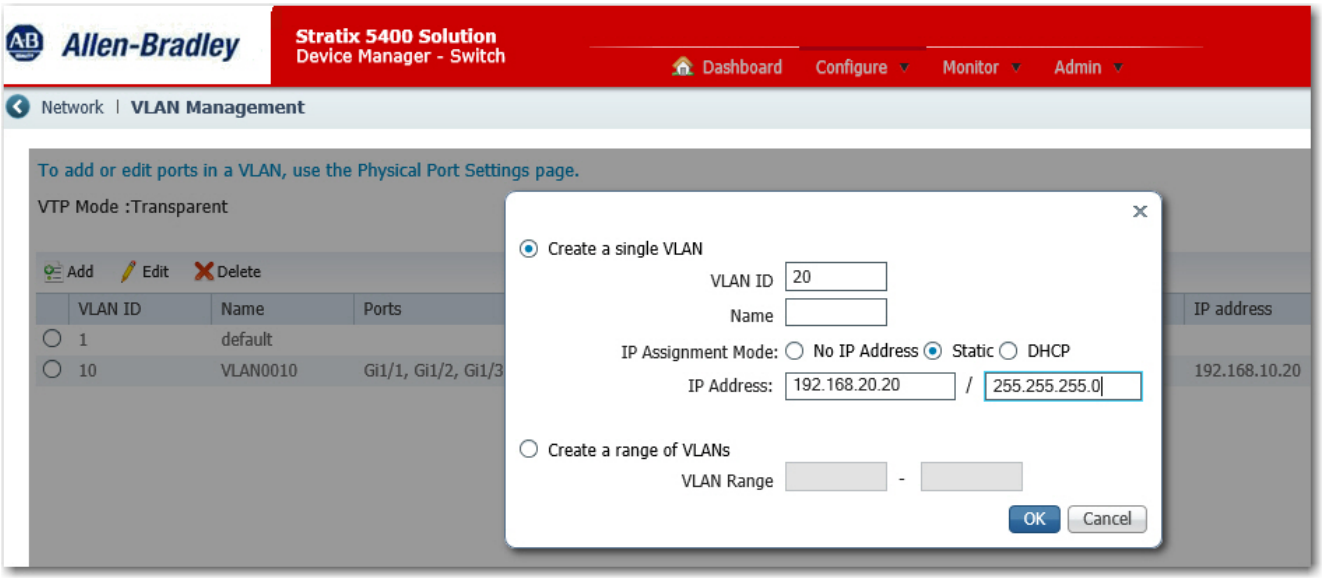
1. Run Express Setup on the switch and assign a static IP address.

   By default, the IP address that is configured during Express Setup is the CIP interface (192.168.10.20). Once Express Setup is complete, you can verify or change the CIP interface and IP address by going to Admin > Express Setup > Advanced Settings.

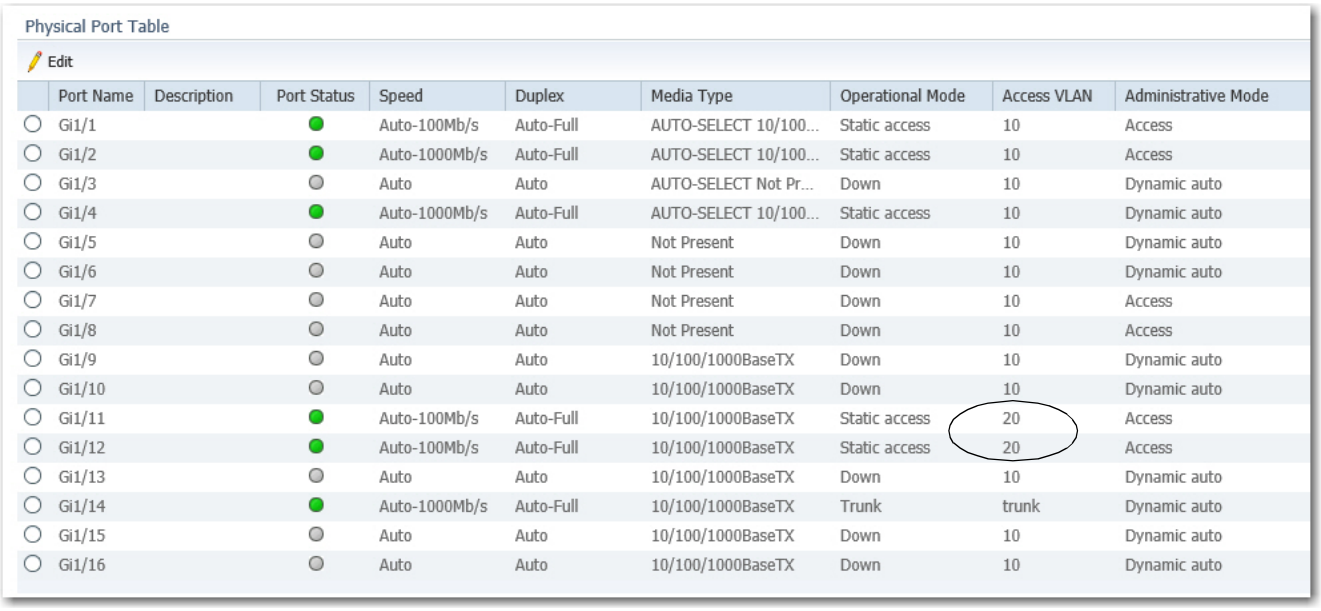


2. Access Device Manager for the switch.

3. Create VLAN ID 20 with IP address 192.168.20.20.



4. In Port Settings, assign VLAN 20 to the DLR ports for Ring 2 (Gi1/11 and Gi1/12).

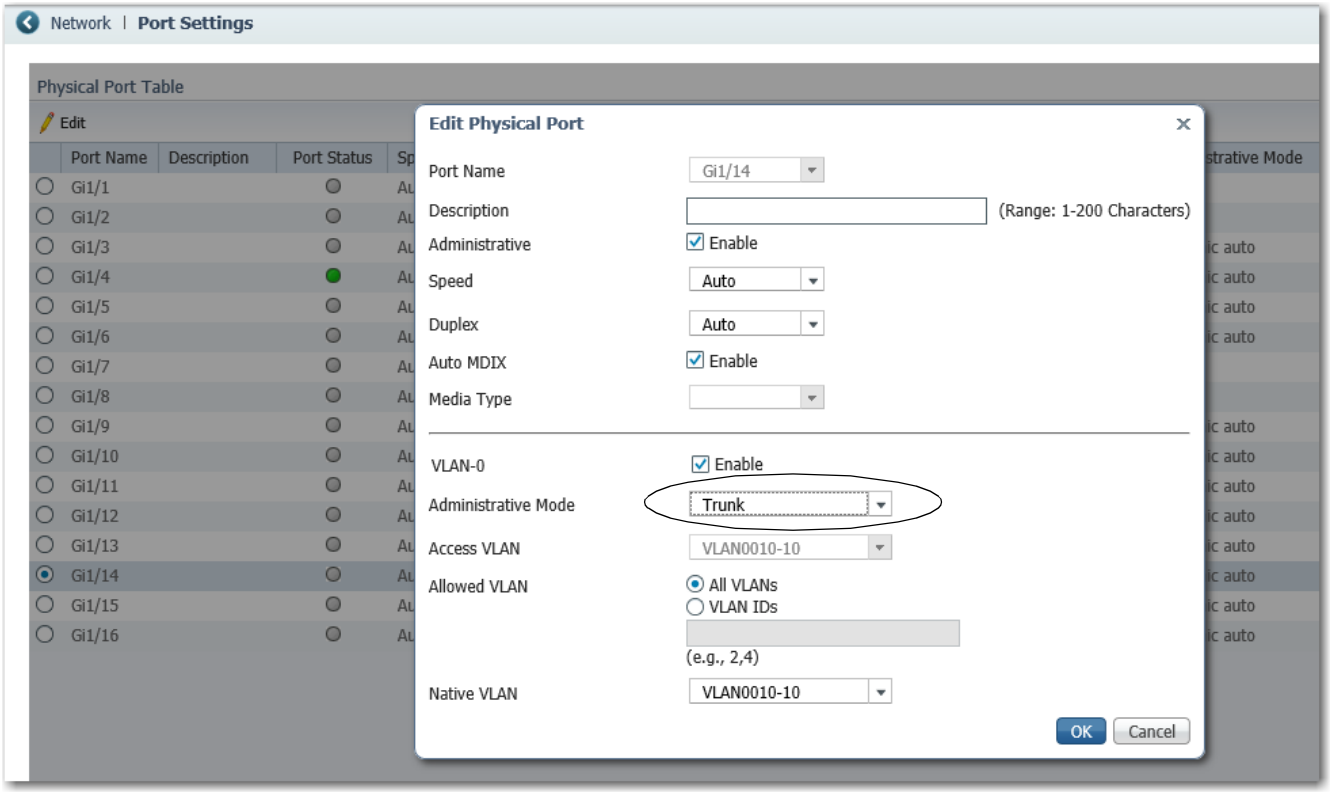


Physical Port Table

Edit

Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
Gi1/1			Auto-100Mb/s	Auto-Full	AUTO-SELECT 10/100...	Static access	10	Access
Gi1/2			Auto-1000Mb/s	Auto-Full	AUTO-SELECT 10/100...	Static access	10	Access
Gi1/3			Auto	Auto	AUTO-SELECT Not Pr...	Down	10	Dynamic auto
Gi1/4			Auto-1000Mb/s	Auto-Full	AUTO-SELECT 10/100...	Static access	10	Dynamic auto
Gi1/5			Auto	Auto	Not Present	Down	10	Dynamic auto
Gi1/6			Auto	Auto	Not Present	Down	10	Dynamic auto
Gi1/7			Auto	Auto	Not Present	Down	10	Access
Gi1/8			Auto	Auto	Not Present	Down	10	Access
Gi1/9			Auto	Auto	10/100/1000BaseTX	Down	10	Dynamic auto
Gi1/10			Auto	Auto	10/100/1000BaseTX	Down	10	Dynamic auto
Gi1/11			Auto-100Mb/s	Auto-Full	10/100/1000BaseTX	Static access	20	Access
Gi1/12			Auto-100Mb/s	Auto-Full	10/100/1000BaseTX	Static access	20	Access
Gi1/13			Auto	Auto	10/100/1000BaseTX	Down	10	Dynamic auto
Gi1/14			Auto-1000Mb/s	Auto-Full	10/100/1000BaseTX	Trunk	trunk	Dynamic auto
Gi1/15			Auto	Auto	10/100/1000BaseTX	Down	10	Dynamic auto
Gi1/16			Auto	Auto	10/100/1000BaseTX	Down	10	Dynamic auto

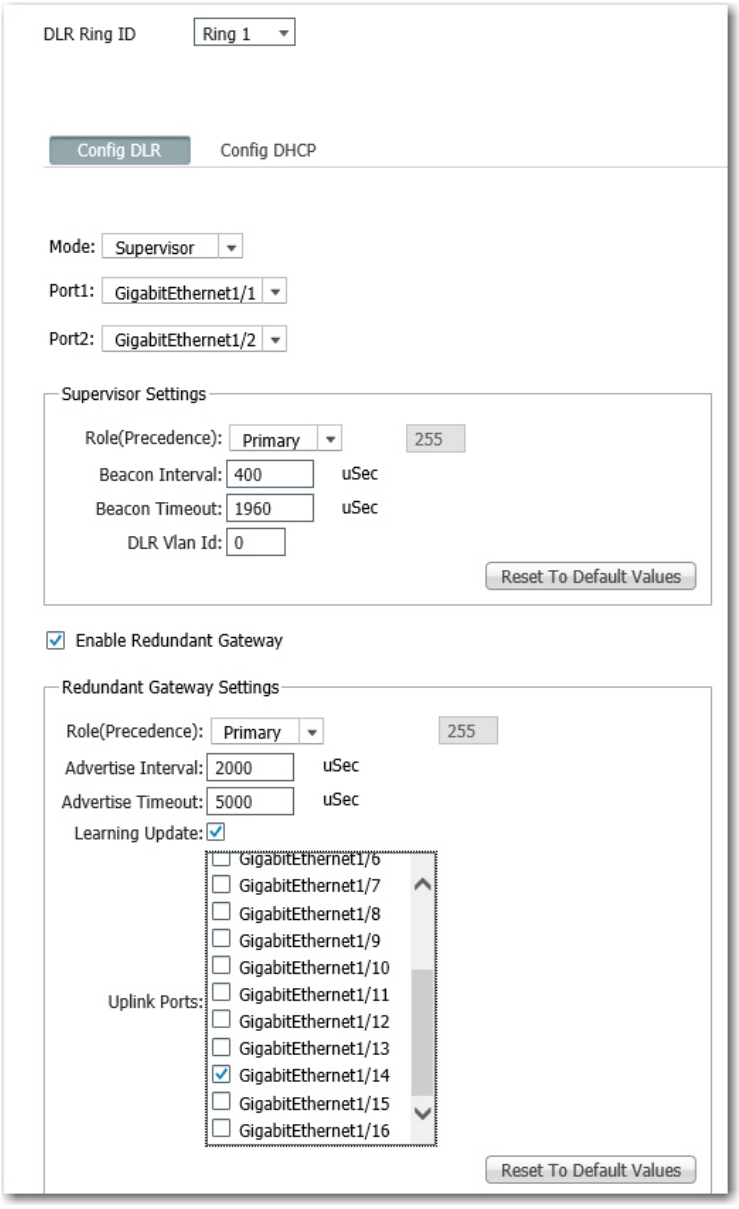
5. Assign Trunk mode to the uplink port (Gi1/14).



6. Configure Precision Time Protocol (PTP) in Boundary mode.

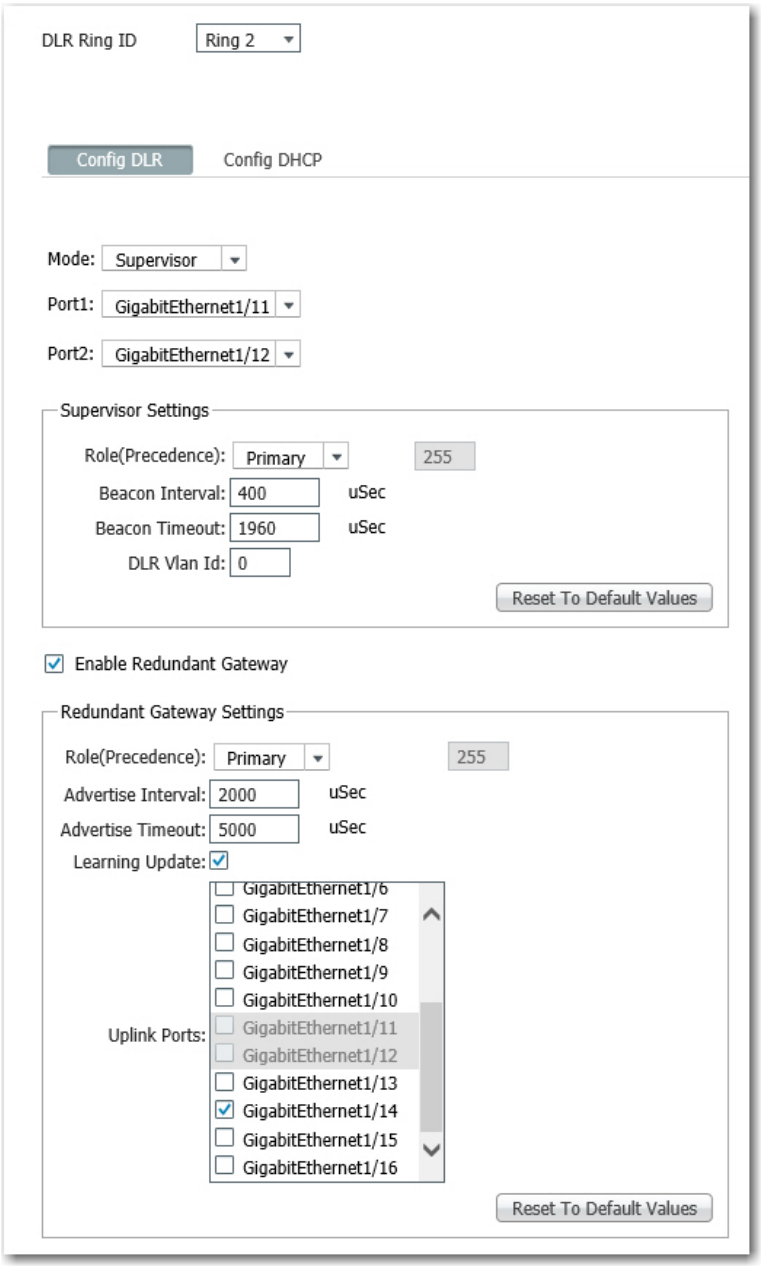
7. Configure Ring 1 with the following settings.

Field	Value
DLR Ring ID	Ring 1
Mode	Supervisor
Port1	GigabitEthernet1/1
Port2	GigabitEthernet1/2
Supervisor Settings	
Role (Precedence)	Primary
DLR Vlan ID	0 (default)
Enable Redundant Gateway	Checked
Redundant Gateway Settings	
Role (Precedence)	Primary
Uplink Ports	GigabitEthernet1/14

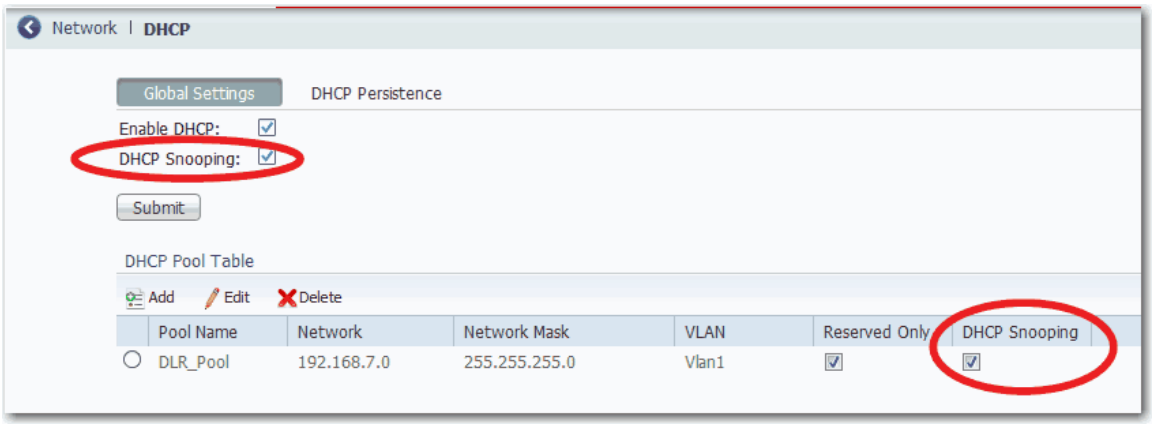


8. Configure Ring 2 with the following settings.

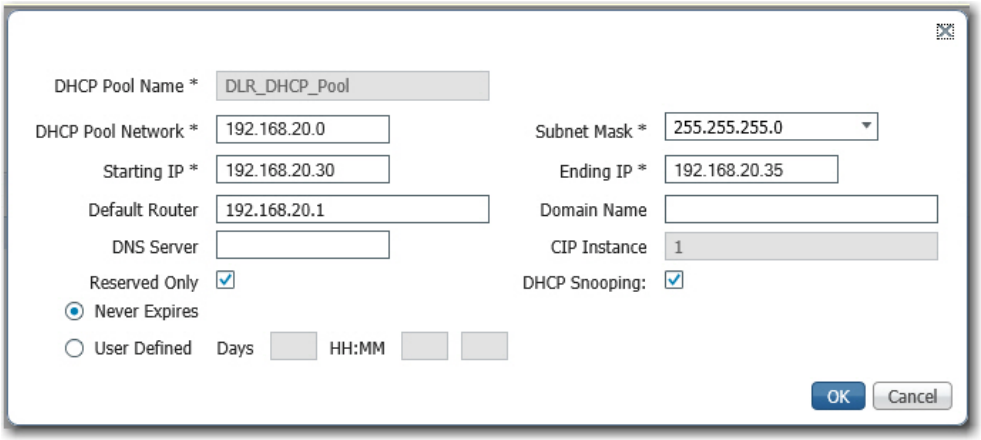
Field	Value
DLR Ring ID	Ring 2
Mode	Supervisor
Port1	GigabitEthernet1/11
Port2	GigabitEthernet1/12
Supervisor Settings	
Role (Precedence)	Primary
DLR Vlan ID	0 (default)
Enable Redundant Gateway	Checked
Redundant Gateway Settings	
Role (Precedence)	Primary
Uplink Ports	GigabitEthernet1/14



9. Configure the switch for DHCP.
   a. Enable DHCP and DHCP snooping.
   b. In the DHCP Pool Table, check Reserved Only.

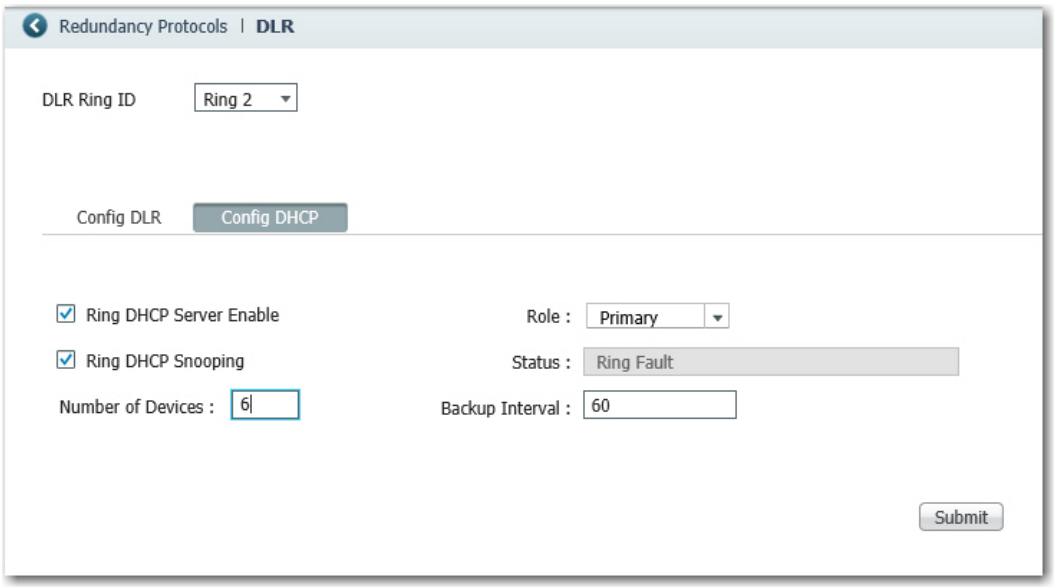


   c. Configure an IP address pool for ring devices.



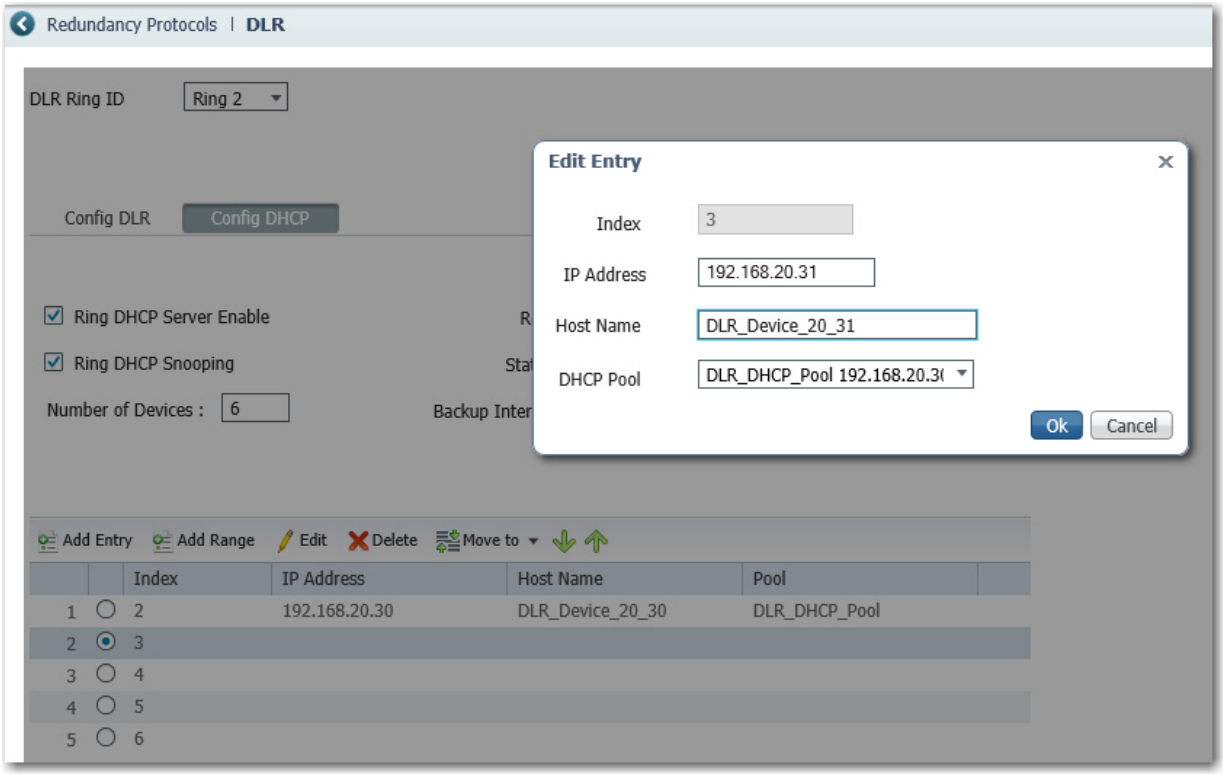
10. Configure the switch as a primary DHCP server for devices on Ring 2 with the following settings.

Field	Value
Ring DHCP Server Enable	Checked
Role	Primary
Ring DHCP Snooping	Checked
Number of Devices	6

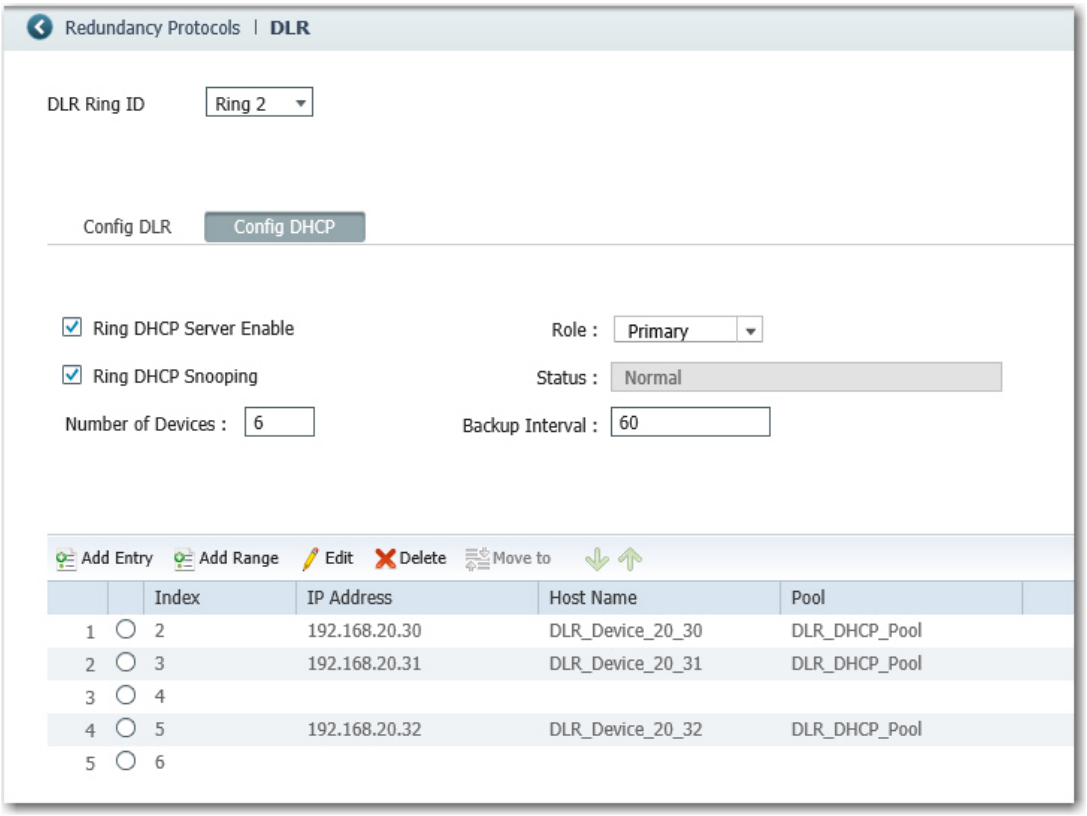


11. Add entries to represent each device on Ring 2 to the index table and assign IP addresses to each index entry, except for entries 4 and 6.

    Entries 4 and 6 are other switches on the ring, which have static IP addresses that you assign during Express Setup.

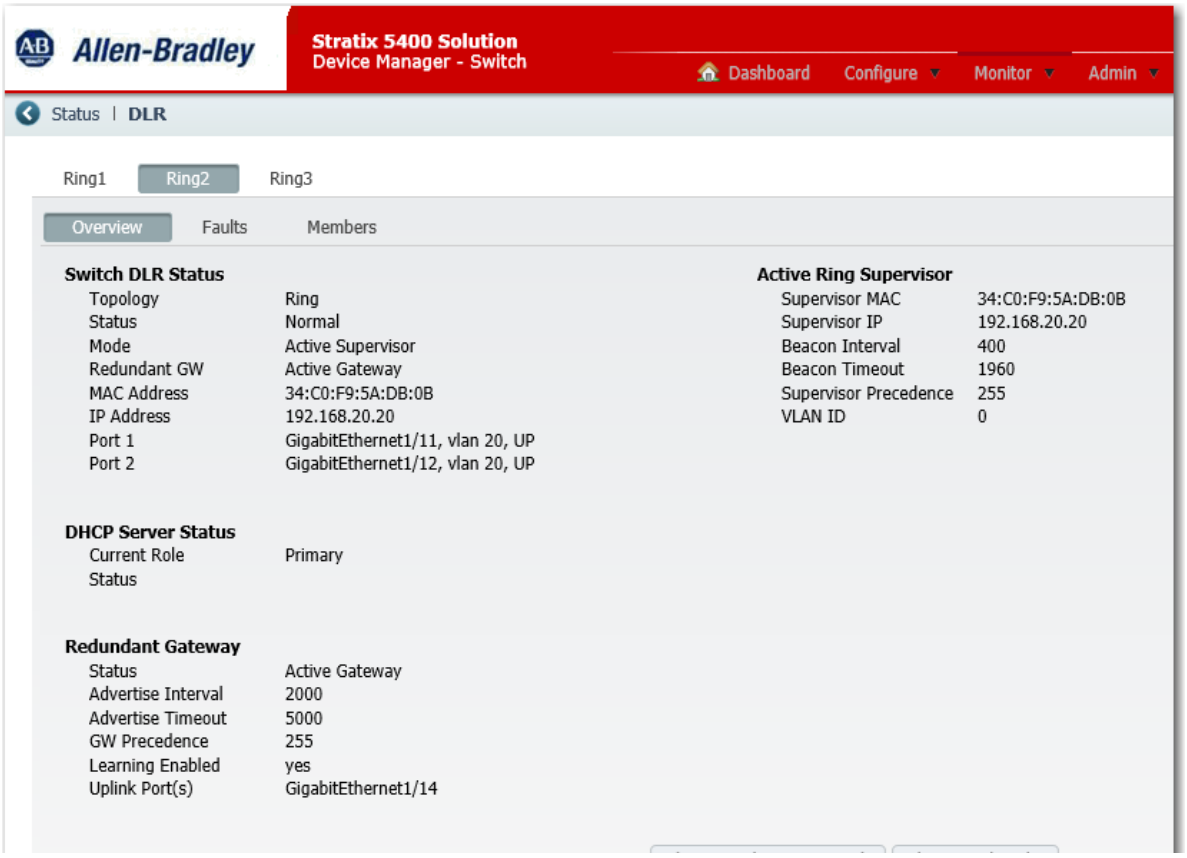


The following image shows the completed DHCP table for Ring 2.

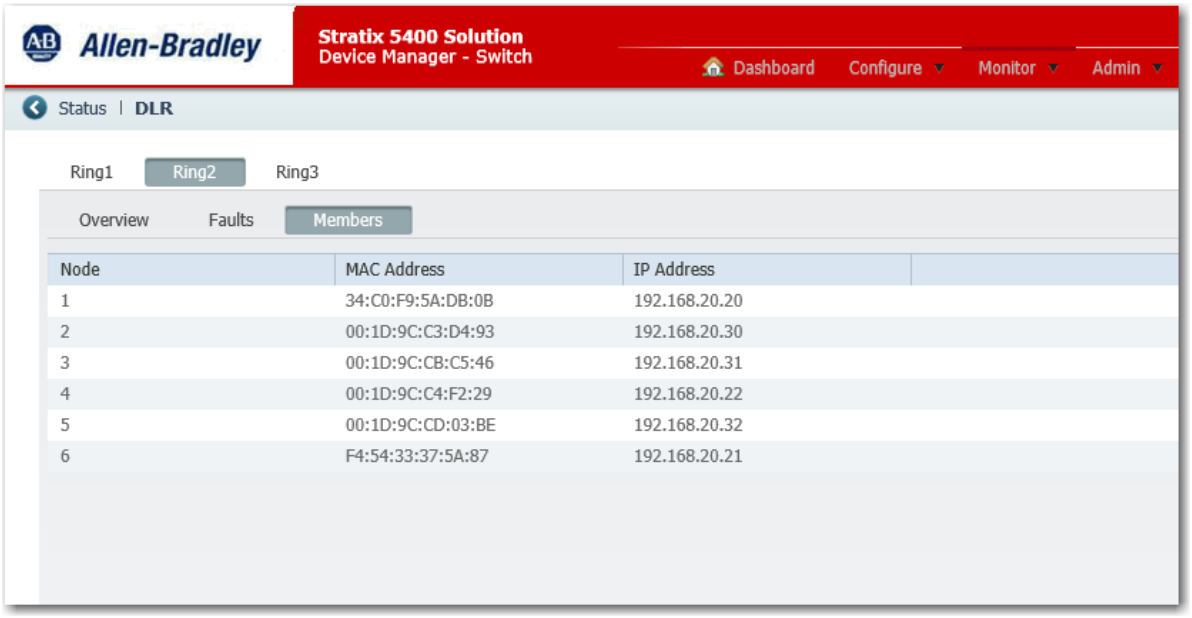


12. On the Monitor > DLR page, verify the configuration of Ring 2.

    Verify that Ring 2 ports are correctly configured.



    Verify that all ring members have IP addresses.



Configure the Backup Stratix 5400 Switch

In this example, the backup switch is configured with these roles:

- Backup redundant gateway (optional configuration)
- Backup ring supervisor
- Backup DHCP server for Ring 2

The backup switch uses the configurations in the following tables.

Table 5 - Backup Switch Port Configurations

Port	Connected Ring	VLAN
Gi1/1	Ring 1	10
Gi1/2	Ring 1	10
Fa1/7	Ring2	20
Fa1/8	Ring 2	20
Gi1/4	–	10 20

Table 6 - VLAN IP Addresses

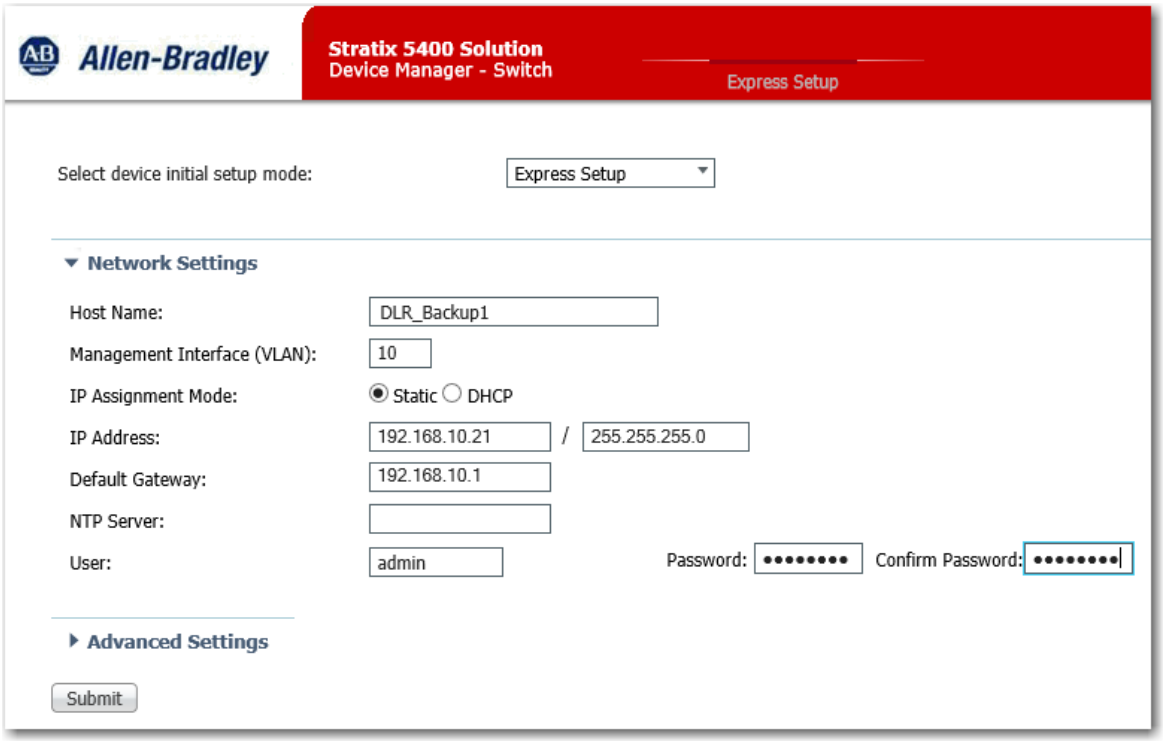
VLAN	IP Address
10	192.168.10.21
20	192.168.20.21

Because the backup switch receives the DHCP table that is configured on the active switch during a switchover, you do not configure DHCP on the backup switch.

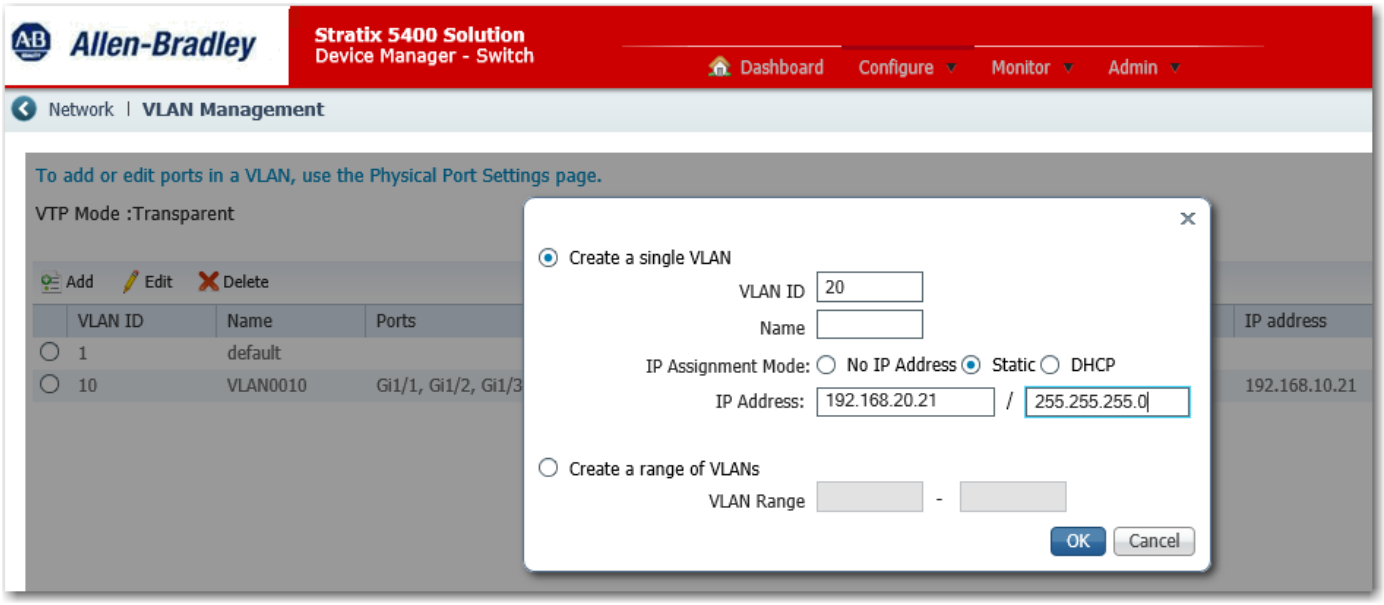
To configure the backup switch in this example, follow these steps.

1. Run Express Setup on the switch and assign a static IP address.

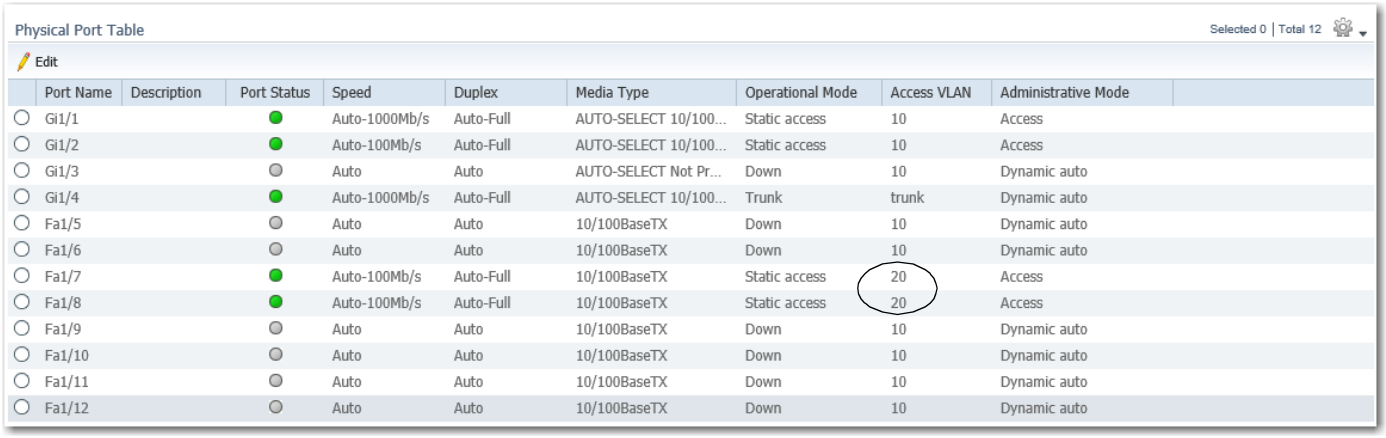
   By default, the IP address that is configured during Express Setup is the CIP interface (192.168.10.21). Once Express Setup is complete, you can verify or change the CIP interface and IP address by going to Admin > Express Setup > Advanced Settings.



2. Create VLAN 20 with IP address 192.168.20.21.

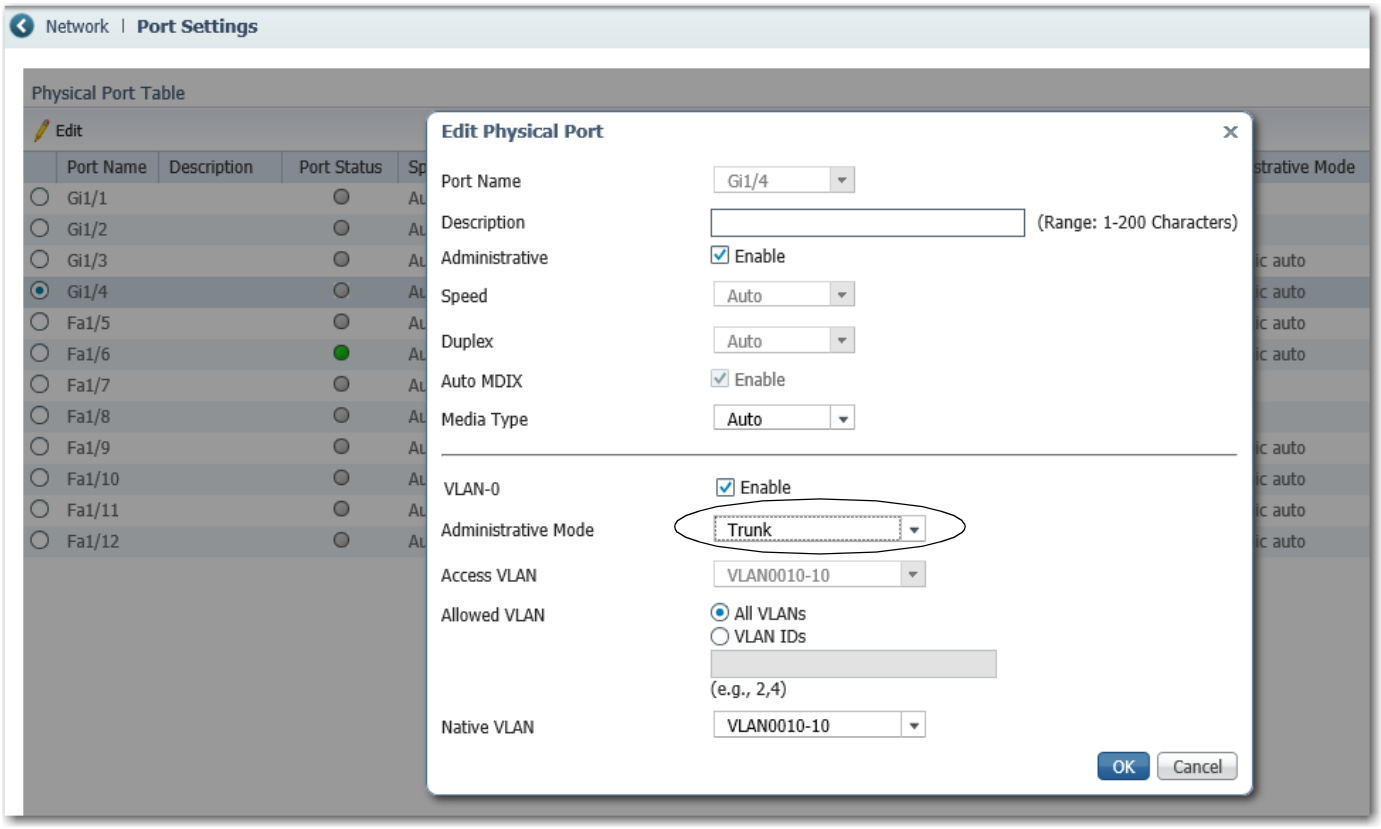


3. In Port Settings, assign VLAN 20 to the DLR ports for Ring 2 (Fa1/7 and Fa1/8).



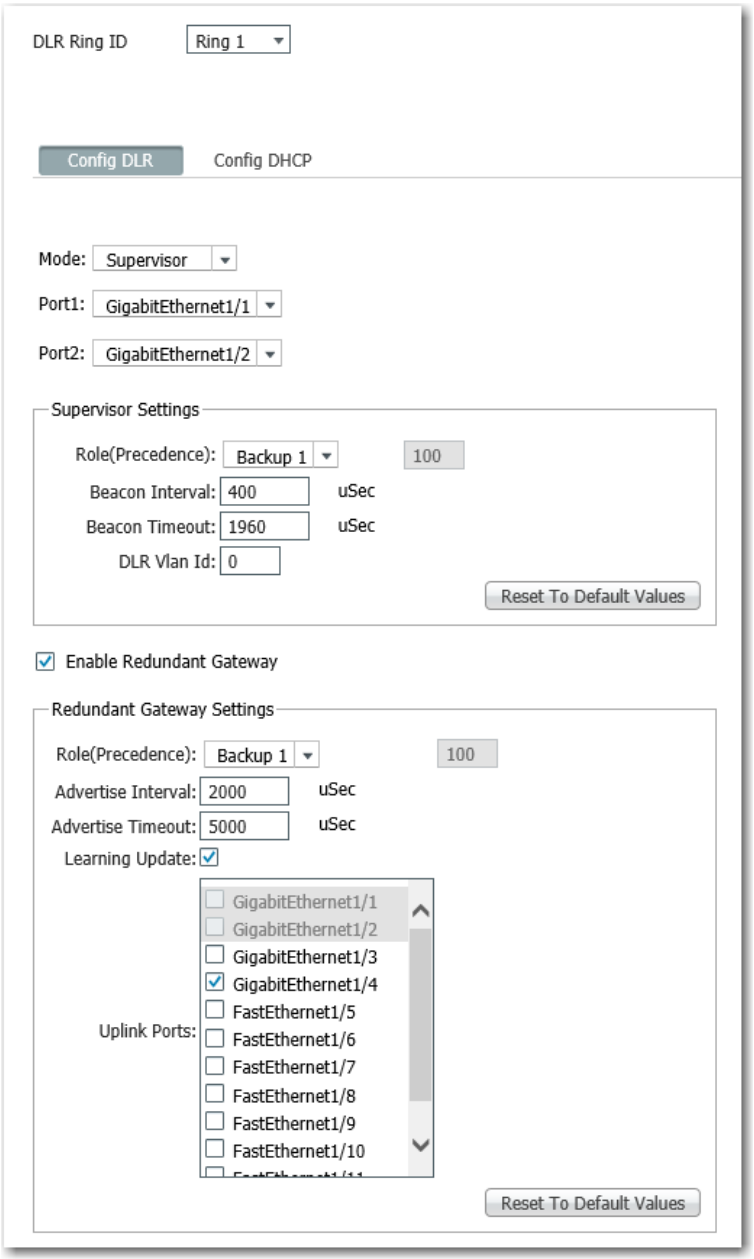
Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
Gi1/1			Auto-1000Mb/s	Auto-Full	AUTO-SELECT 10/100...	Static access	10	Access
Gi1/2			Auto-100Mb/s	Auto-Full	AUTO-SELECT 10/100...	Static access	10	Access
Gi1/3			Auto	Auto	AUTO-SELECT Not Pr...	Down	10	Dynamic auto
Gi1/4			Auto-1000Mb/s	Auto-Full	AUTO-SELECT 10/100...	Trunk	trunk	Dynamic auto
Fa1/5			Auto	Auto	10/100BaseTX	Down	10	Dynamic auto
Fa1/6			Auto	Auto	10/100BaseTX	Down	10	Dynamic auto
Fa1/7			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	20	Access
Fa1/8			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	20	Access
Fa1/9			Auto	Auto	10/100BaseTX	Down	10	Dynamic auto
Fa1/10			Auto	Auto	10/100BaseTX	Down	10	Dynamic auto
Fa1/11			Auto	Auto	10/100BaseTX	Down	10	Dynamic auto
Fa1/12			Auto	Auto	10/100BaseTX	Down	10	Dynamic auto

4. Assign Trunk mode to the uplink port (Gi1/4).



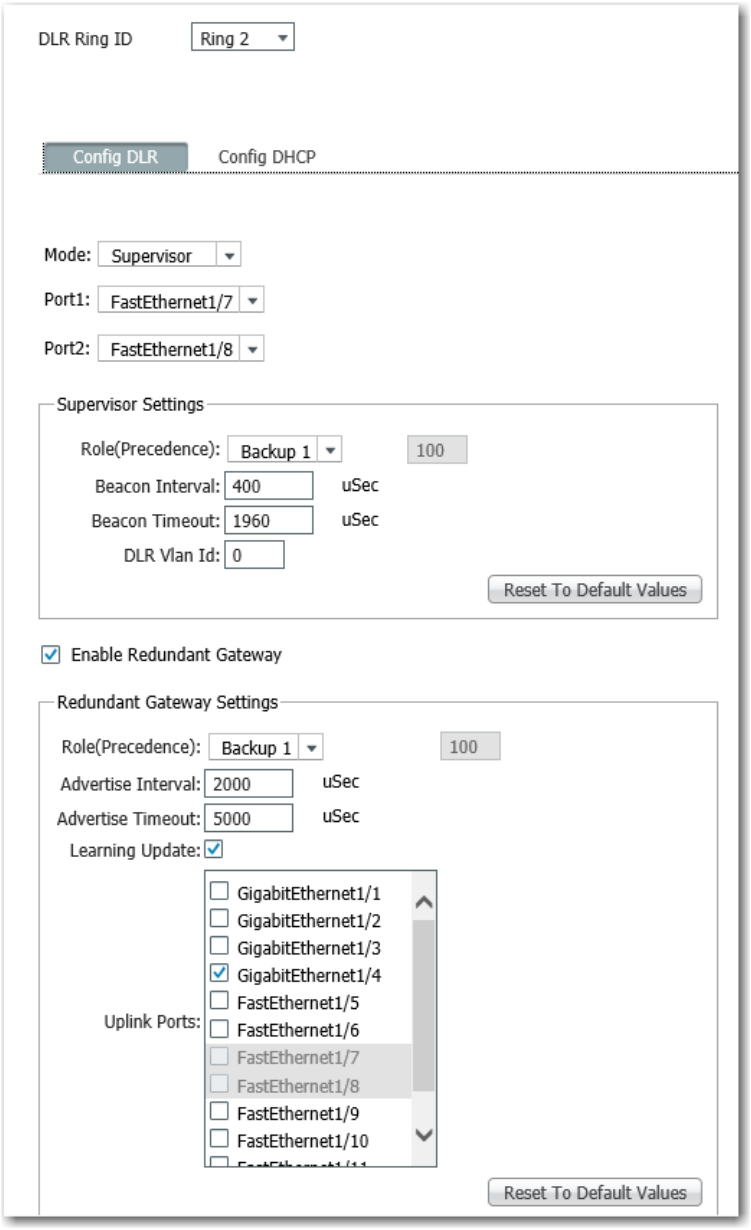
5. Configure Ring 1 with the following settings.

Field	Value
DLR Ring ID	Ring 1
Mode	Supervisor
Port1	GigabitEthernet1/1
Port2	GigabitEthernet1/2
Supervisor Settings	
Role (Precedence)	Backup 1
DLR Vlan ID	0 (default)
Enable Redundant Gateway	Checked
Redundant Gateway Settings	
Role (Precedence)	Backup 1
Uplink Ports	GigabitEthernet1/4



6. Configure Ring 2 with the following settings.

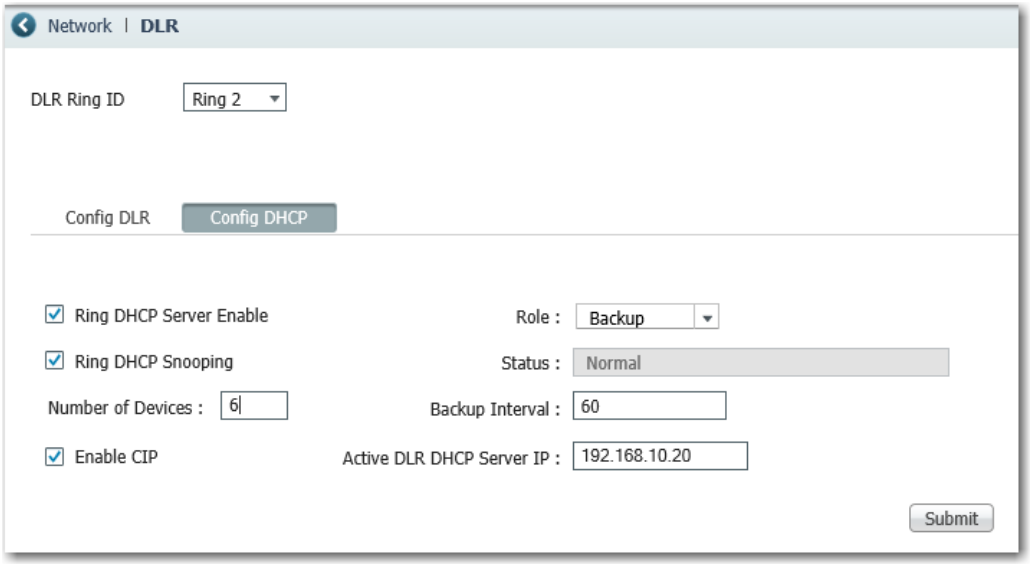
Field	Value
DLR Ring ID	Ring 2
Mode	Supervisor
Port1	FastEthernet1/7
Port2	FastEthernet1/8
Supervisor Settings	
Role (Precedence)	Backup 1
DLR Vlan ID	0 (default)
Enable Redundant Gateway	Checked
Redundant Gateway Settings	
Role (Precedence)	Backup 1
Uplink Ports	GigabitEthernet1/4



7. Configure the switch as a backup DHCP server for devices on Ring 2 with the following settings.

IMPORTANT You must check Enable CIP and enter the IP address of the primary ring DHCP server. These settings enable the backup DHCP ring server to receive the DHCP configuration from the primary ring DHCP server if a switchover occurs.

Field	Value
Ring DHCP Server Enable	Checked
Role	Backup
Ring DHCP Snooping	Checked
Number of Devices	6
Enable CIP	Checked
Active DLR DHCP Server IP	192.168.10.20

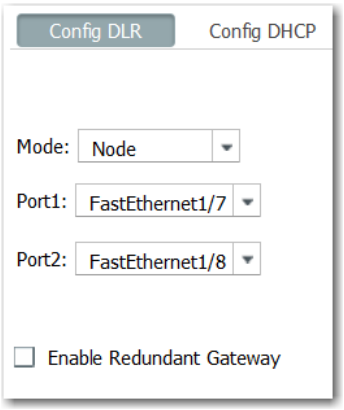


Configure the Stratix 5700 Switch on Ring 2

To enable the Stratix 5700 switch on Ring 2 to participate on the ring and pass DHCP server messages through its ports, complete these configuration steps.

1. In Device Manager, configure these DLR settings on the switch.

Field	Value
Mode	Node
Port1	FastEthernet1/7
Port2	FastEthernet1/8



2. By using the Cisco command-line interface (CLI), execute the following command on DLR ports Fa1/7 and Fa1/8 to make the ports DHCP snooping trusted interfaces: **ip dhcp snooping trust**

   This command allows DHCP server messages to flow through the DLR ports on the switch. For more information, see DHCP Snooping on page 28.

Notes:

Monitor a DLR Network

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.

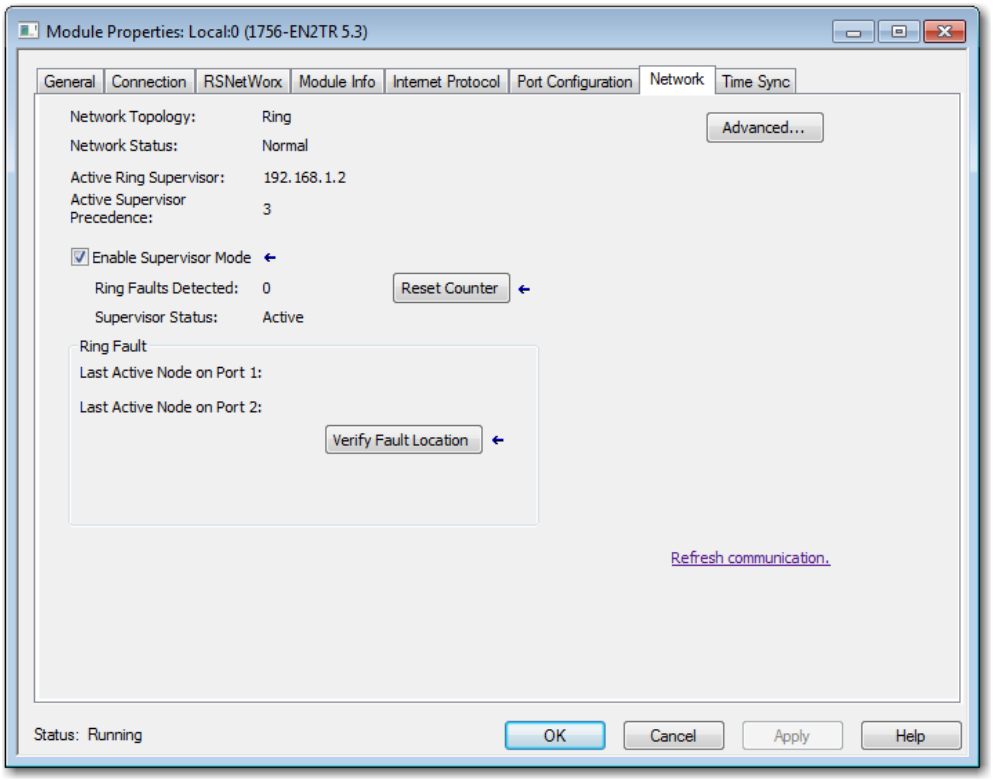
Depending on whether the ring node is a device or a switch, you can use the following software tools to monitor and diagnose a DLR network.

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
FactoryTalk® Network Manager™	Yes	Yes
MSG instructions	Yes	Yes

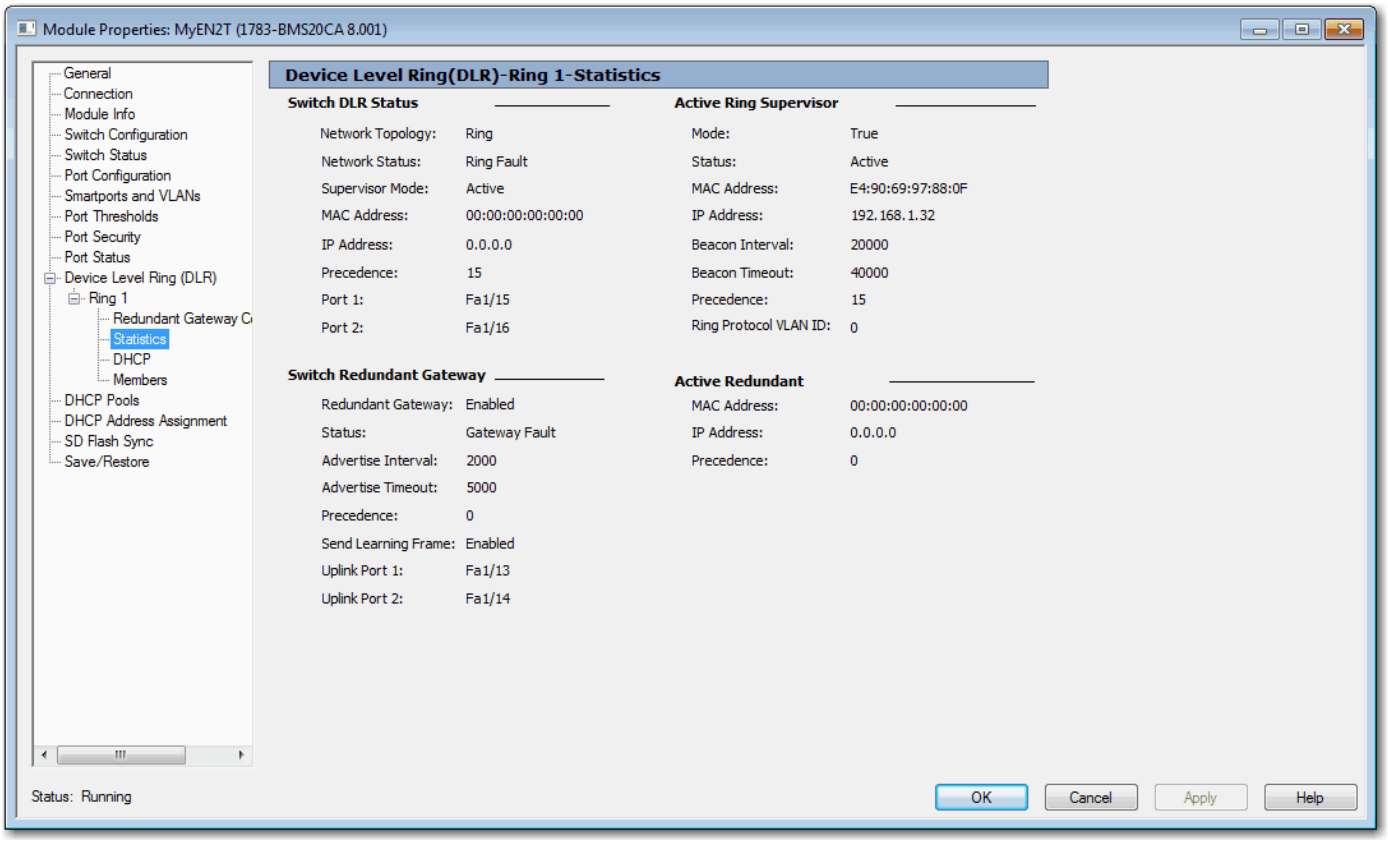
Logix Designer Application

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.



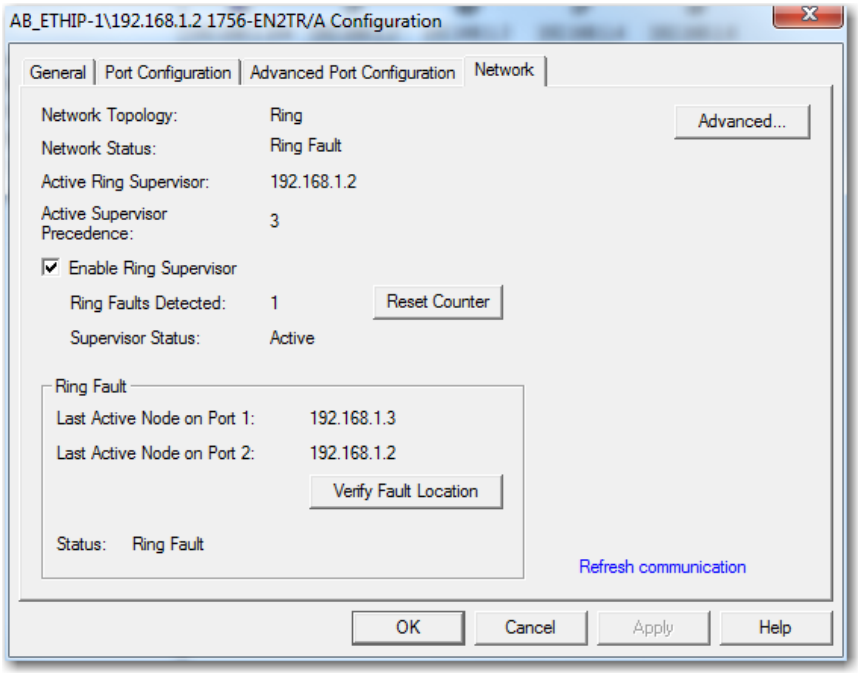
For switches, open the Module Properties dialog box, expand Device Level Ring (DLR) and click Statistics.



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.

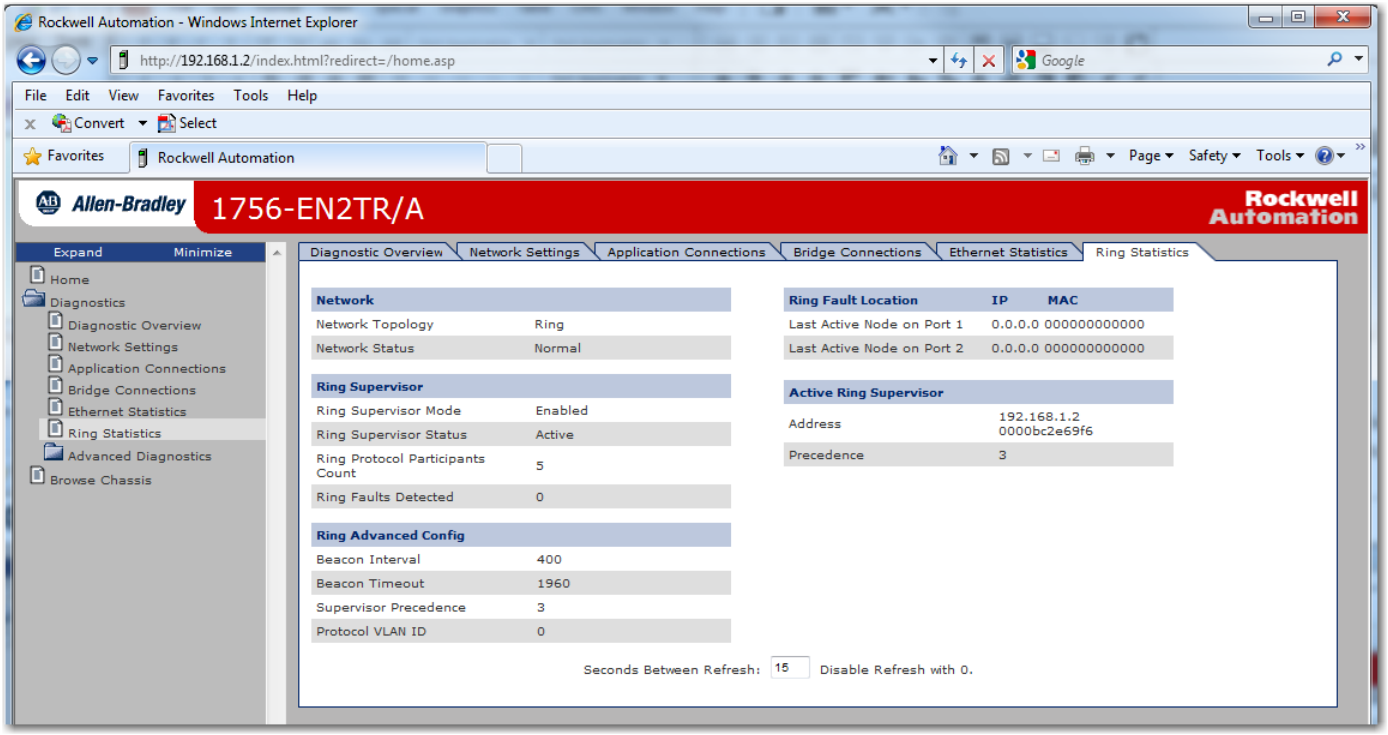
The following example shows a ring fault between nodes at IP addresses 192.168.1.3 and 192.168.1.2.



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.

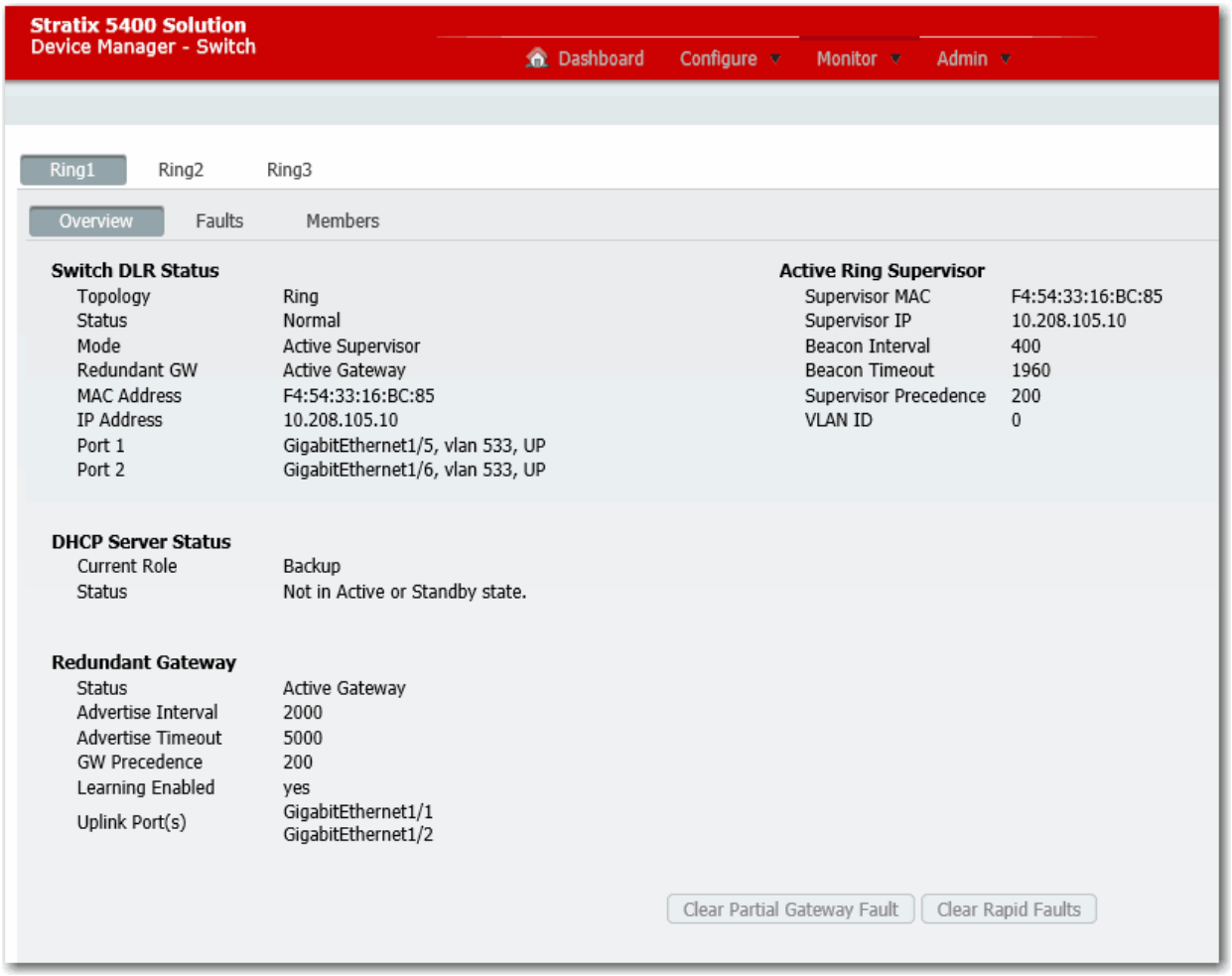


Device Manager

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

Enter the IP address of the switch in a web browser and log on 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.

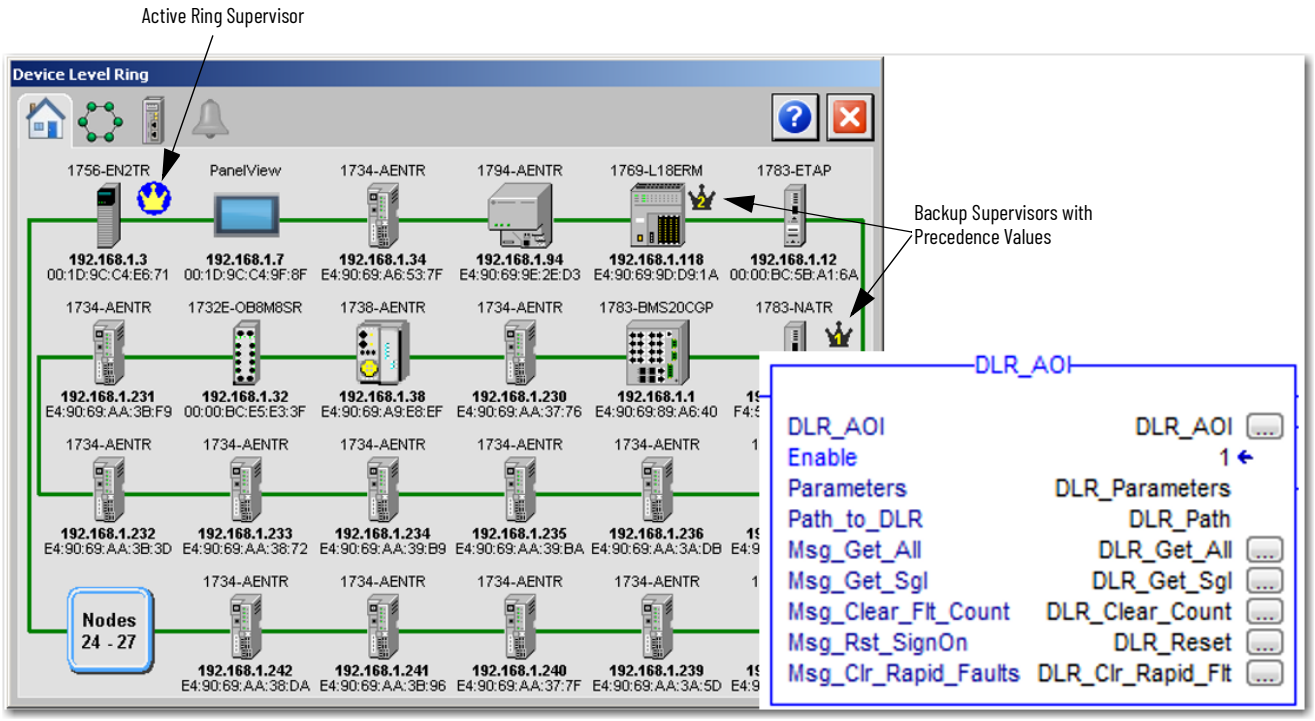
For details about CLI commands for DLR, see the Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD015.

```
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:A4:5D   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
```

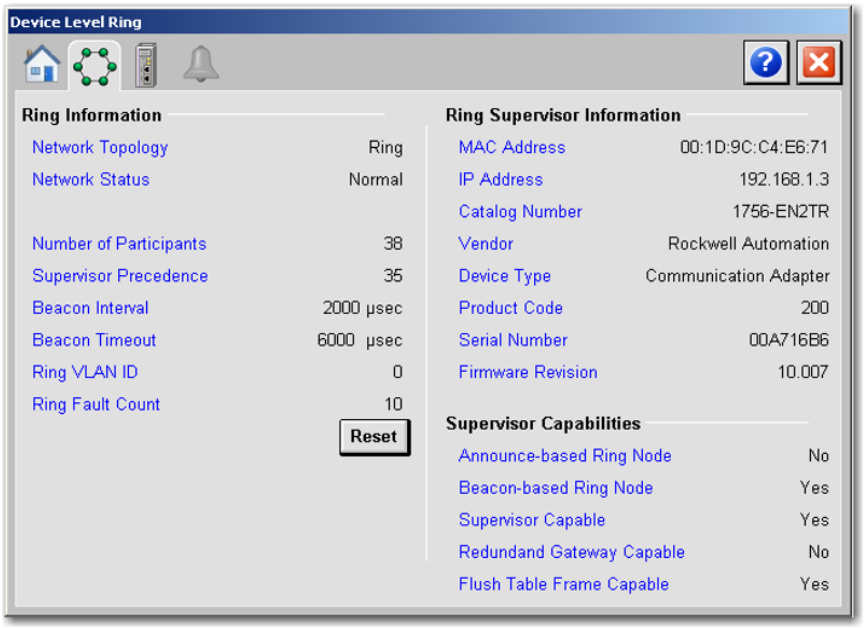
DLR Faceplate

The EtherNet/IP Device Level Ring Network Diagnostics faceplate with Add-On Instruction code enables a controller to retrieve real-time DLR network status information. HMI faceplate graphics allow the data to be visualized on an operator interface.

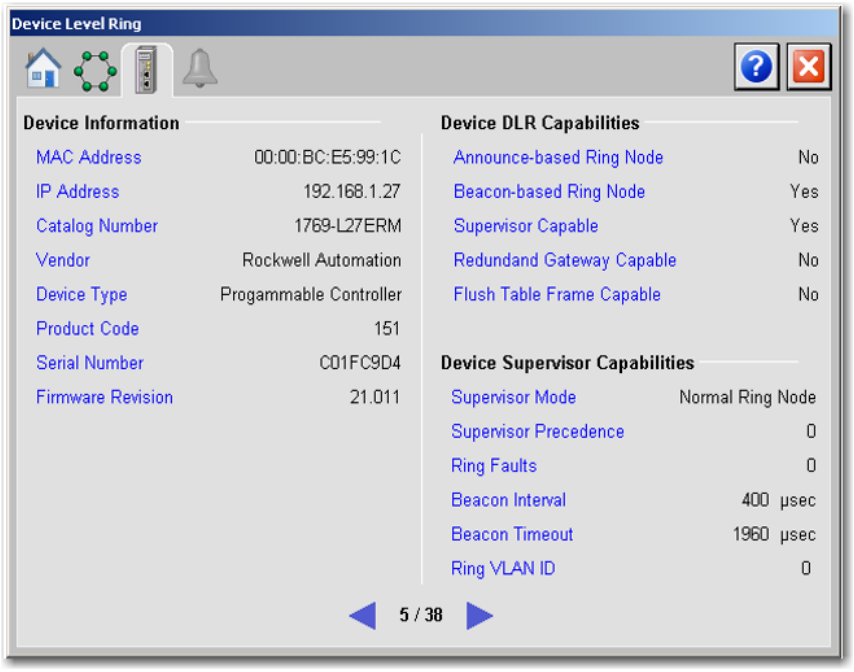
For Stratix switches that support multiple rings, the faceplate retrieves data from ring 1 only.



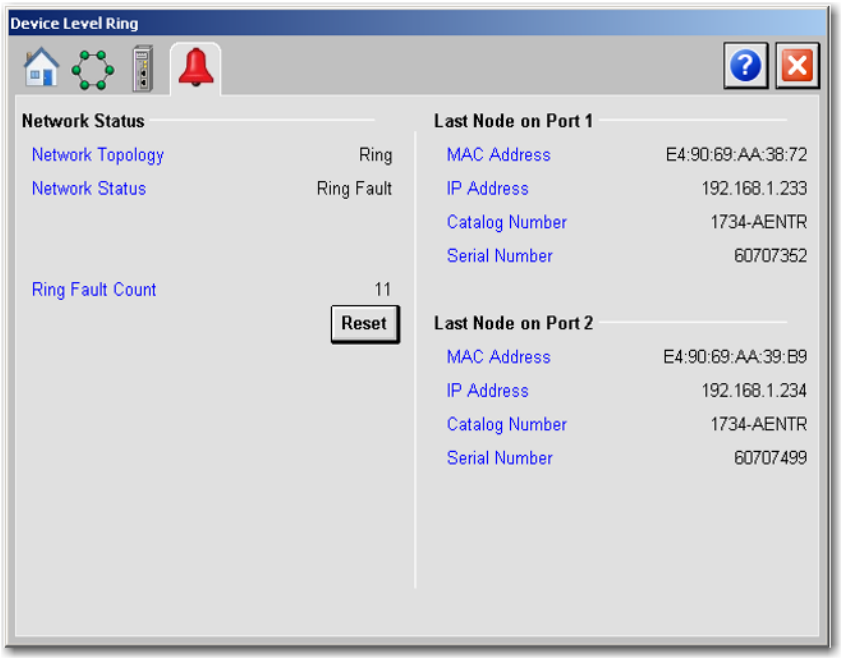
The Network tab provides detailed network parameters and information about the active ring supervisor.



The Node tab provides detailed information about the selected ring participant.



The Alarm tab shows ring fault information that is obtained from the active ring supervisor.

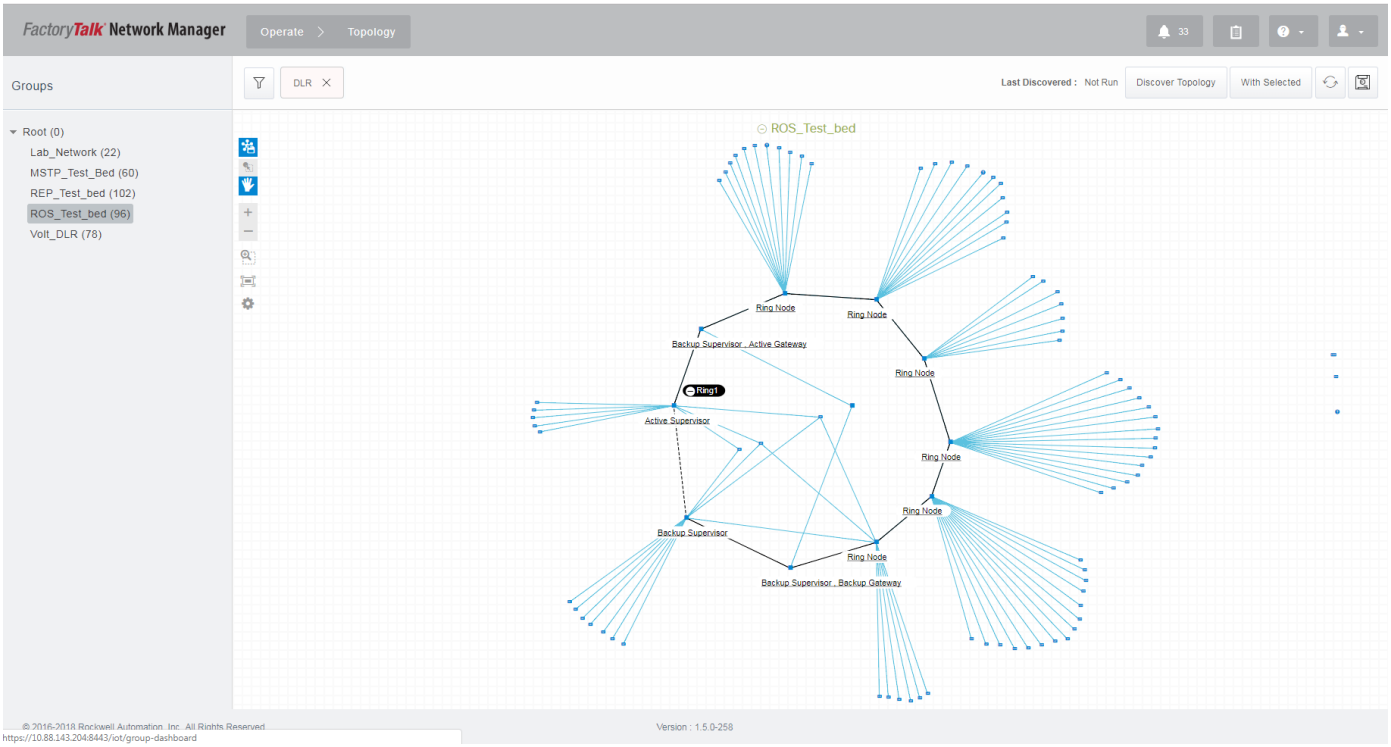


The EtherNet/IP Device Level Ring Network Diagnostics faceplate is available for download in the Sample Code Library. You can access the Sample Code Library from the Rockwell Automation Download Center:

https://www.rockwellautomation.com/en-us/support/product/product-downloads.html

FactoryTalk Network Manager

In FactoryTalk Network Manager, you can view a DLR network on a topology map. The software also shows ring faults, blocked ports on the active supervisor, roles of ring nodes, and other DLR parameters and statistics.



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 chain through port 1 of an active ring supervisor during a ring fault
- Get the last active node at the end of 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 83.

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.

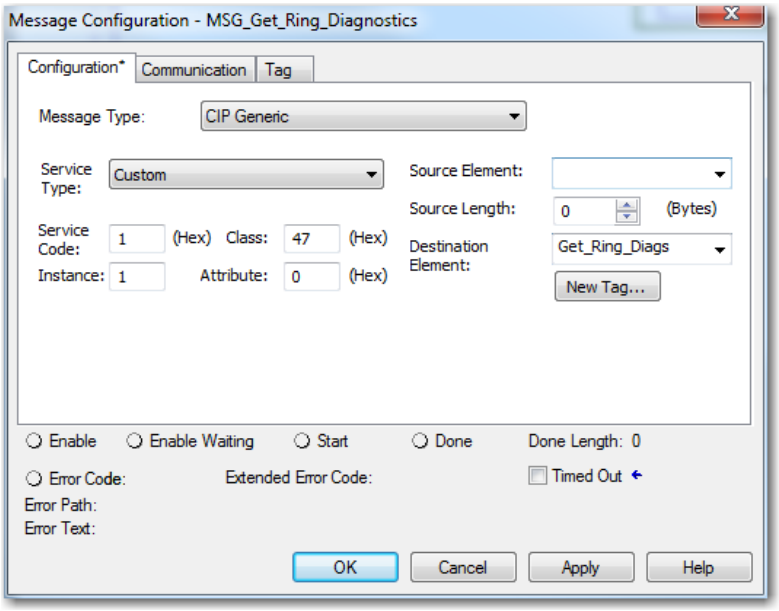
For information about how to program MSG instructions for Logix 5000™ controllers, see the Logix 5000 Controllers Messages Programming Manual, publication 1756-PM012.

Example Use of MSG Instruction

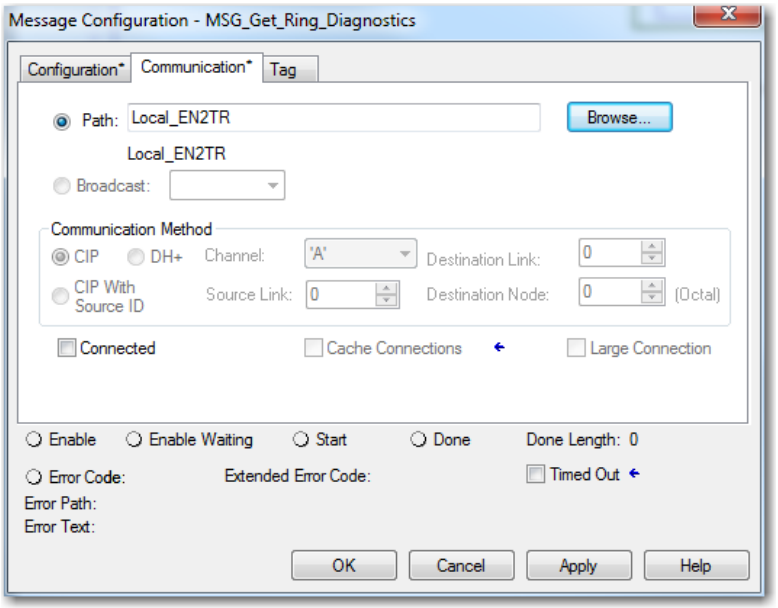
The following steps describe how to configure an MSG instruction.

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 7 on page 83.

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 7 on the Configuration tab of an MSG instruction.

Table 7 - MSG Instruction Configuration Values

Attribute and Service Names	Description	Message Type	Service Code	Attribute Code (HEX)	Class (HEX)	Instance[1]	Destination Element	Destination Length (Bytes)
Network Topology	Current network topology mode	CIP Generic	E	1	47	1 = ring 1 2 = ring 2 3 = ring 3	user-defined tag name	1
Network Status	Status of network	CIP Generic	E	2	47	1 = ring 1 2 = ring 2 3 = ring 3	user-defined tag name	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	6	47	1 = ring 1 2 = ring 2 3 = ring 3	user-defined tag name	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	7	47	1 = ring 1 2 = ring 2 3 = ring 3	user-defined tag name	10
Verify a Fault Location	Causes ring supervisor to verify	CIP Generic	4B	0	47	1 = ring 1 2 = ring 2 3 = ring 3	user-defined tag name	2
Clear Rapid Faults	Clears the Rapid Fault/Restore	CIP Generic	4C	0	47	1 = ring 1 2 = ring 2 3 = ring 3	user-defined tag name	2
Clear Gateway Partial Fault	Clears the partial network fault	CIP Generic	4E	0	47	1 = ring 1 2 = ring 2 3 = ring 3	user-defined tag name	2

(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 executes the state machine.

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.

Notes:

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 following to take place:

1. The supervisor node recognizes that a fault ex ists 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 other node conditions exist, such as a node operating at 10 Mbps full-duplex, or 10/100 Mbps half-duplex, 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

O

P

R

S

T

U

V

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

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.

You can view or download publications at rok.auto/literature.

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
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.

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) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication ENET-AT007D-EN-P - August 2021
ENET-AT007C-EN-P - August 2019