ControlLogix EtherNet/IP Network Devices

Catalog Numbers 1756-EN2F, 1756-EN2FK, 1756-EN2T, 1756-EN2TK, 1756-EN2TP, 1756-EN2TPK, 1756-EN2TPXT, 1756-EN2TR, 1756-EN2TRK, 1756-EN2TXT, 1756-EN2TRXT, 1756-EN3TR, 1756-EN3TRK, 1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT, 1756-ENBT, 1756-ENBTK, 1756-EWEB

AB QUALITY

Allen-Bradley

by **ROCKWELL AUTOMATION**

User Manual

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

⚠	**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

⚠	**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

These labels may also be on or inside the equipment to provide specific precautions.

⚡	**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

♨	**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

☢	**ARC FLASH HAZARD:** Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

The following icon may appear in the text of this document.

💡	Identifies information that is useful and can help to make a process easier to do or easier to understand.

ControlLogix Network Device Status Indicators

Appendix A

Notes:

About This Publication

This manual describes how you can use ControlLogix® EtherNet/IP™ communication modules with a Logix 5000® controller and communicate with various devices on the Ethernet/IP network.

Use this manual if you program applications that use EtherNet/IP networks with ControlLogix controllers.

Conventions

Be sure to understand these concepts and tools:

- FactoryTalk® Linx
- Studio 5000 Logix Designer® application
- ControlFLASH Plus™
- HMIs
- SNMP tools

Download Firmware, AOP, EDS, and Other Files

Download firmware, associated files (such as Add-on Profiles, Electronic Data Sheets, Device Type Manager), and access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc.

Summary of Changes

This manual contains new and updated information. Changes throughout this revision are marked by change bars, as shown to the right of this paragraph.

This manual was revised to add or update the information that is listed in this table.

Topic	Page
Added chapter on Concurrent Communication.	23

Additional Resources

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

Resource	Description
1756 EtherNet/IP Communication Modules Installation Instructions, publication 1756-IN050	Provides information on how to install EtherNet/IP™ modules.
1756 ControlLogix Communication Modules Specifications, publication 1756-TD003	Specifications for ControlLogix communication modules.
Redundancy Systems User Manual, publication 1756-UM015	Describes how to set up, configure, program, monitor, and troubleshoot Logix SIS, ControlLogix 5580, and ControlLogix 5570 redundancy systems.
Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD015	Highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases within the CPwE framework.
Ethernet Design Considerations Reference Manual, publication ENET-RM002	Provides details about how to use EtherNet/IP communication modules with Logix 5000 controllers and communicate with other devices on the EtherNet/IP network.
EtherNet/IP Device Level Ring Application Technique, publication ENET-AT007	Describes DLR network operation, topologies, configuration considerations, and diagnostic methods.
EtherNet/IP Media Planning and Installation Manual This manual is available from the Open DeviceNet® Vendor Association (ODVA) at: http://www.odva.org.	Provides details about how to install, configure, and maintain linear and Device Level Ring (DLR) networks by using Rockwell Automation EtherNet/IP devices that are equipped with embedded switch technology.
EtherNet/IP Network Devices User Manual, publication ENET-UM006	Describes how to use EtherNet/IP communication modules in Logix 5000 control systems.
EtherNet/IP Parallel Redundancy Protocol Application Technique, publication ENET-AT006	Describes how you can configure a Parallel Redundancy Protocol (PRP) network with a compatible device or switch.
EtherNet/IP Socket Interface Application Technique, publication ENET-AT002	Describes the socket interface that you can use to program MSG instructions to communicate between a Logix 5000 controller via an EtherNet/IP module and Ethernet devices that do not support the EtherNet/IP application protocol, such as barcode scanners, RFID readers, or other standard Ethernet devices.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.
Troubleshoot EtherNet/IP Networks Application Technique, publication ENET-AT003	Provides details about how to assign IP addresses to and how to troubleshoot EtherNet/IP networks and devices.

You can view or download publications on Literature Library: rok.auto/literature.

ControlLogix EtherNet/IP Network Device Overview

Topic	Page
Overview	9
ControlLogix Network Device Features	9
EtherNet/IP Network Specifications	11
Device Properties Information	14
Simple Network Management Protocol (SNMP)	14
Electronic Keying	15
Protected Mode	16
Protected Mode in a Redundant Adapter Pair	17
Secure Digital Card	18
CIP Security	19
Parallel Redundancy Protocol	21
Device Level Ring (DLR)	21

Overview

EtherNet/IP™ networks are communication networks that offer a comprehensive suite of messages and services for many automation applications.

This open network standard uses commonly available Ethernet communication products to support real-time I/O messaging, information exchange, and general messaging.

ControlLogix Network Device Features

The ControlLogix® EtherNet/IP network devices:

- Facilitate high-speed data transfer between Logix 5000® controllers and remote I/O modules.
- Connect to multiple EtherNet/IP network topologies.

Figure 1 shows how Rockwell Automation EtherNet/IP communication modules fit into a control system.

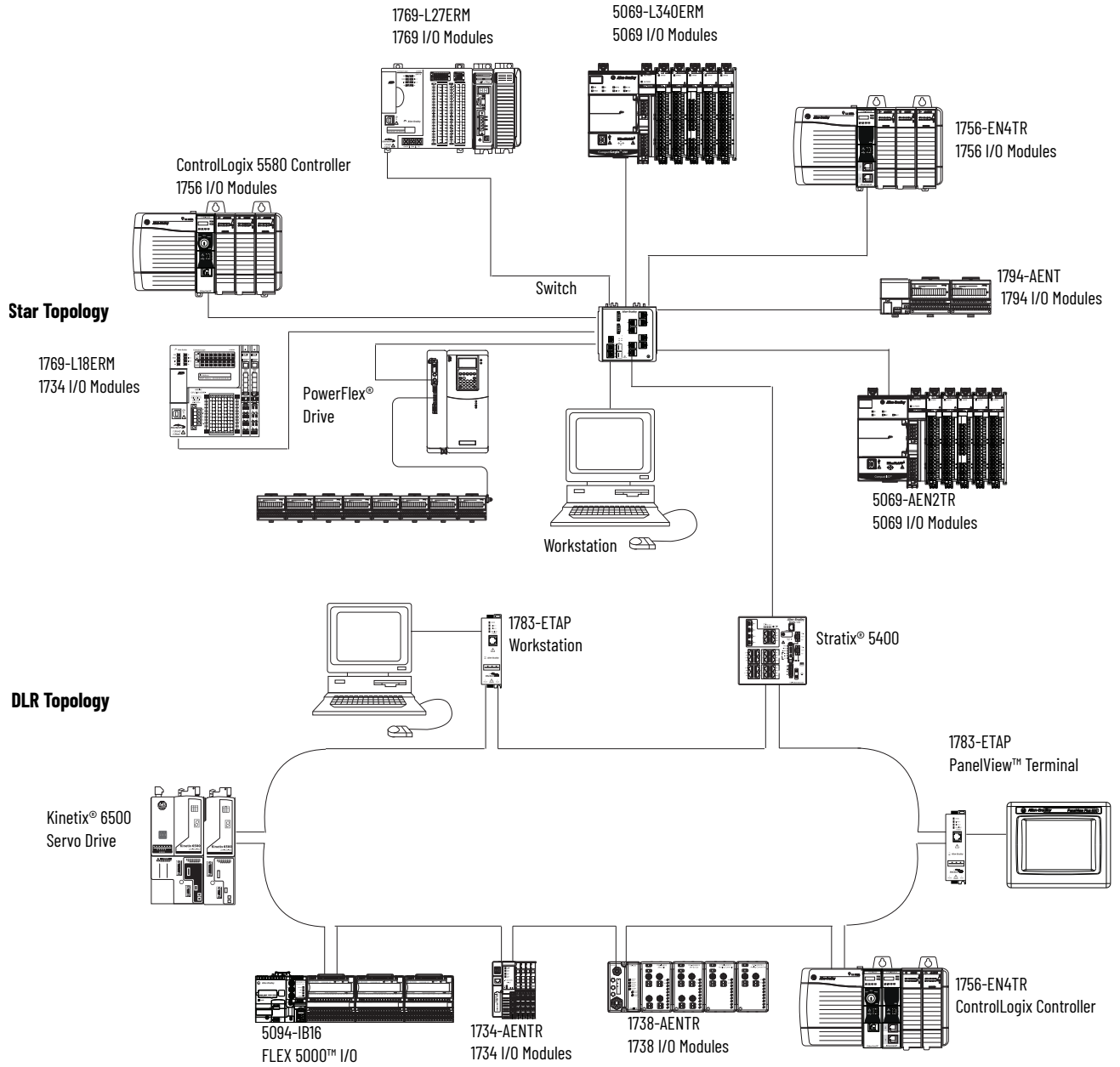**Figure 1 - EtherNet/IP Communication Modules in a Control System**

Table 1 - EtherNet/IP Communication Modules

Cat. No.[1]	Description	Media	Communication Rate
1756-EN2F, 1756-EN2FK	EtherNet/IP bridge, fiber	Fiber	100 Mbps, no auto-negotiation.
1756-EN2T 1756-EN2TK	EtherNet/IP bridge, copper	Copper	10/100 Mbps
1756-EN2TP, 1756-EN2TPK	EtherNet/IP bridge, PRP support, copper	Dual Copper	10/100 Mbps
1756-EN2TPXT	ControlLogix-XT™, extended temperature EtherNet/IP bridge, PRP support	Dual Copper	10/100 Mbps
1756-EN2TR, 1756-EN2TRK	EtherNet/IP bridge, embedded switch, copper	Dual copper	10/100 Mbps
1756-EN2TXT	ControlLogix-XT, extended temperature EtherNet/IP bridge, copper, for extreme environments	Copper	10/100 Mbps
1756-EN2TRXT	ControlLogix-XT, extended temperature EtherNet/IP bridge, embedded switch, copper	Dual copper	10/100 Mbps
1756-EN3TR, 1756-EN3TRK	EtherNet/IP bridge, embedded switch, copper	Dual copper	10/100 Mbps
1756-EN4TR, 1756-EN4TRK	EtherNet/IP bridge, embedded switch, copper	Dual Copper	10/100 Mbps 1 Gbps
1756-EN4TRXT	ControlLogix-XT, extended temperature EtherNet/IP bridge, embedded switch, copper	Dual Copper	10/100 Mbps 1 Gbps
1756-ENBT, 1756-ENBTK	EtherNet/IP bridge, copper	Copper	10/100 Mbps
1756-EWEB	Ethernet web server module	Copper	10/100 Mbps

(1)   A catalog number ending in a K denotes a conformal coating.

EtherNet/IP Network Specifications

Table 2 - ControlLogix EtherNet/IP Connections Specifications[1]

Cat. No.	Connections		CIP™ Unconnected Messages (backplane + Ethernet)
	TCP	CIP[2]	
1756-ENBT	64	128	64 + 64
1756-EN2F	128	256	128 + 128
1756-EN2T	128	256	128 + 128
1756-EN2TP	128	256	128 + 128
1756-EN2TR	128	256	128 + 128
1756-EN3TR	128	256	128 + 128
1756-EN4TR	512	1000 I/O, 528 messaging/HMI	256+256
1756-EWEB	64	128	128 + 128

(1)   Includes the K conformal coating catalog numbers and the XT extreme environment catalog numbers.
(2)   Except for the 1756-EN4TR, which has separate I/O and messaging/HMI CIP connections, these connections can be used for any combination of I/O and messaging/HMI.

Table 3 - ControlLogix EtherNet/IP Data Specifications[1]

Cat. No.	Produced/Consumed Tags		Socket Services	Duplicate IP Detection (starting revision)
	Number of Multicast Tags, Max[2]	Unicast Available in RSLogix 5000® Software		
1756-EN2F		Version 16.03.00 or later	Yes	
1756-EN2T		Version 16.03.00 or later	Yes	
1756-EN2TP		Version 24.00.00 or later	Yes	
1756-EN2TR	32	Version 17.01.02 or later	Yes	All Revisions
1756-EN3TR		Version 18.02.00 or later	Yes	
1756-EN4TR		Version 24.00.00 or later	Yes	
1756-ENBT		Version 16.03.00 or later	No	Revision 3.3
1756-EWEB	N/A	Version 16.03.00 or later	Yes	Revision 2.2

(1)   Includes the K conformal coating catalog numbers and the XT extreme environment catalog numbers.
(2)   Each controller can send a maximum of 32 multicast produced tags to one single consuming controller. If these same tags are sent to multiple consumers, the maximum number is 31.

Table 4 - ControlLogix EtherNet/IP Specifications[1]

Cat. No.	Firmware Revision	RSLogix 5000 Software Version	RSLinx® Software Version	Packet Rate Capacity (packets/second)[2]		Support for Extended Environment[3]	Integrated Motion on the EtherNet/IP Network Axes
				I/O	HMI/MSG		
1756-ENBT	Any	8.02.00 or later	2.30 or later	5000	900	No	N/A
1756-EN2F	2.x	15.02.00 or later	2.51 or later	10,000	2000	No	N/A
	3.6 or later	18.02.00 or later[4]		25,000[5]			Up to 8 axes supported[5]
1756-EN2T	2.x or earlier	15.02.00 or later	2.51 or later	10,000	2000	No	N/A
	3.6 or later	18.02.00 or later[4]		25,000[5]			Up to 8 axes supported[5]
1756-EN2TXT	2.x	15.02.00 or later	2.51 or later	10,000	2000	Yes	N/A
	3.6 or later	18.02.00 or later[4]		25,000[5]			Up to 8 axes supported[5]
1756-EN2TP	Any	24.00.00 or later[4]	4.10 or later	25,000[5]	2000	No	Up to 8 axes supported[5]
1756-EN2TPXT	10.x or later	24.00.00 or later	4.10 or later	25,000[5]	2000	Yes	Up to 8 axes supported[5]
1756-EN2TR	2.x	17.01.02 or later	2.55 or later	10,000	2000	No	N/A
	5.x or later	18.02.00 or later[4]	2.56 or later	25,000[5]			Up to 8 axes supported[5]
1756-EN2TRXT	5.028 or later	20.01.00 or later	2.56 or later	25,000[5]	2000	Yes	Up to 8 axes supported[5]
1756-EN3TR	3.6 or later	18.02.00 or later[4]	2.56 or later	25,000[5]	2000	No	Up to 256 axes supported[5]
1756-EN4TR	Any	24.00.00 or later[6]	4.10 or later	• 50,000 without CIP Security™ • 25,000 with integrity • 15,000 with integrity and confidentiality	• 3,700 without CIP Security • 2,700 with integrity • 1,700 with integrity and confidentiality	No	Up to 256 axes supported[5]
1756-EN4TRXT	Any	24.00.00 or later[6]	4.10 or later	• 50,000 without CIP Security • 25,000 with integrity • 15,000 with integrity and confidentiality	• 3,700 without CIP Security • 2,700 with integrity • 1,700 with integrity and confidentiality	Yes	Up to 256 axes supported[5]

(1) Includes the K conformal coating catalog numbers.

(2) I/O numbers are maximums; they assume no HMI/MSG. HMI/MSG numbers are maximums, they assume no I/O. Packet rates vary depending on packet size. For more details, see Troubleshoot EtherNet/IP Application Technique, publication ENET-AT003, and the EDS file for a specific catalog number.

(3) Module operates in a broad temperature spectrum, -20…+70 ºC (-4…+158 ºF), and meets ANSI/ISA-S71.04-1985 Class G1, G2 and G3, and cULus, Class 1 Div 2, C-Tick, CE, ATEX Zone 2 and SIL 2 requirements for increased protection against salts, corrosives, moisture/condensation, humidity, and fungal growth.

(4) This version is required to use CIP Sync™ technology, Integrated Motion on the EtherNet/IP Network, or Exact Match keying.

(5) This value assumes the use of a 1756-L8x or a 1756-L7x ControlLogix controller. For a 1756-L6x ControlLogix controller, see ControlLogix Controllers User Manual, publication 1756-UM001.

(6) CIP Security requires FactoryTalk® Linx version 6.11.00 or later.

EtherNet/IP Network

The Ethernet Industrial (EtherNet/IP) network protocol is an open industrial-networking standard that supports both real-time I/O messaging and message exchange. The EtherNet/IP network uses off-the-shelf Ethernet communication chips and physical media.

If you need to	Select this interface
Control I/O modules and drives Act as an adapter for I/O on remote EtherNet/IP links Communicate with other EtherNet/IP devices (messages and HMI) Bridge EtherNet/IP links to route messages to devices on other networks	1756-EN2F, 1756-EN2FK 1756-EN2T, 1756-EN2TK, 1756-EN2TXT 1756-EN2TP, 1756-EN2TPK, 1756-EN2TPXT 1756-EN2TR, 1756-EN2TRK, 1756-EN2TRXT 1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT 1756-ENBT, 1756-ENBTK
Support Device Level Ring (DLR) and linear topologies	1756-EN2TR, 1756-EN2TRK, 1756-EN2TRXT 1756-EN3TR, 1756-EN3TRK 1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT
Support for Parallel Redundancy Protocol	1756-EN2TP, 1756-EN2TPK, 1756-EN2TPXT 1756-EN4TR[1], 1756-EN4TRK[1], 1756-EN4TRXT[1]
Support for Redundant Adapters[2]	1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT
Provide control in environments where temperatures range from -25...+70 °C (-13...+158 °F)	1756-EN2TPXT 1756-EN2TRXT 1756-EN2TXT 1756-EN4TRXT
Secure access to a control system from within the plant network	1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT
Use an Internet browser to access tags remotely in a ControlLogix controller Communicate with other EtherNet/IP or generic Ethernet devices (messaging only; no I/O control) Bridge EtherNet/IP links to route messages to devices on other networks	1756-EWEB, 1756-EWEBK web server

(1)   Starting with firmware revision 4.001.

(2)   Redundant Adapters require version 3.001 and higher firmware. See the Product Compatibility and Download Center (PCDC) for that firmware.

Device Properties Information

You can use FactoryTalk Linx Network Browser to view:

- Catalog Number
- Manufacture Date
- Warranty Number
- Series

This applies to:

- 1756-EN2x modules manufactured with firmware revision 12.001 or later.
- 1756-EN4TR modules manufactured in July 2022 or later with firmware revision 4.001 or later.

Example Module Manufactured with Earlier Firmware	Module Manufactured with Later Firmware
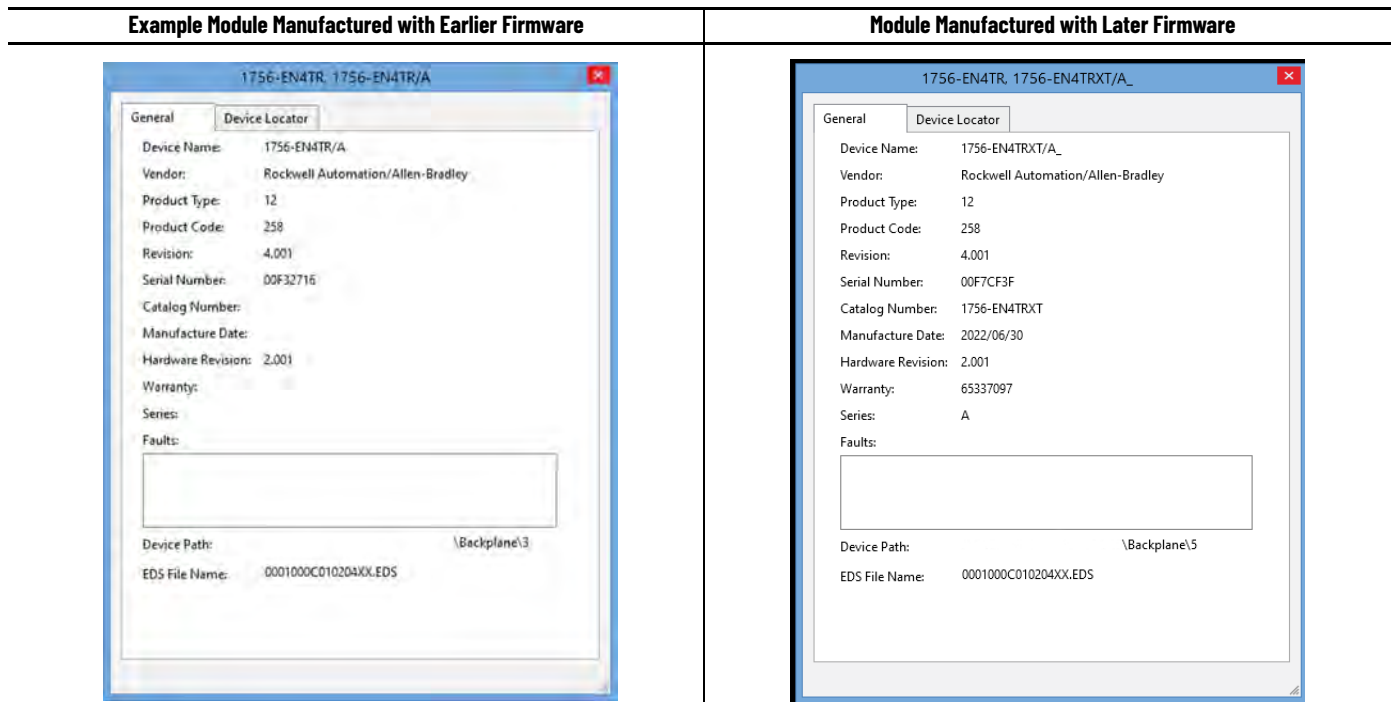
Simple Network Management Protocol (SNMP)

SNMP enables the device to be remotely managed through other network management software. SNMP defines the method of communication among the devices and also denotes a manager for the monitoring and supervision of the devices. For more information about SNMP, see the Ethernet Reference Manual, publication ENET-RM002.

Cat. No.	Default Status	Ability to Disable SNMP
1756-EN2F	**Off** with firmware revision 12.001 or later **On** with firmware revision 11.004 or earlier	**Yes** with firmware revision 12.001 or later **No** with firmware revision 11.004 or earlier
1756-EN2T		
1756-EN2TP		
1756-EN2TR		
1756-EN3TR		
1756-EN4TR	Off	Yes

SNMP Passwords for these modules can be changed. For information on how to change the SNMP Password, see the Knowledgebase Technote *SNMP Password and MIB Configuration*.

Disable SNMP

To disable SNMP, see Disable/Enable Simple Network Management Protocol (SNMP) on page 74.

Electronic Keying

Electronic Keying reduces the possibility that you use the wrong device in a control system. It compares the device that is defined in your project to the installed device. If keying fails, a fault occurs. These attributes are compared in the following table.

Attribute	Description
Vendor	The device manufacturer.
Device Type	The general type of the product, for example, digital I/O module.
Product Code	The specific type of the product. The Product Code maps to a catalog number.
Major Revision	A number that represents the functional capabilities of a device.
Minor Revision	A number that represents behavior changes in the device.

The following Electronic Keying options are available.

Keying Option	Description

Compatible Module	Lets the installed device accept the key of the device that is defined in the project when the installed device can emulate the defined device. With Compatible Module, you can typically replace a device with another device that has the following characteristics:
	• Same catalog number
	• Same or higher Major Revision
	• Minor Revision as follows:
	  – If the Major Revision is the same, the Minor Revision must be the same or higher.
	  – If the Major Revision is higher, the Minor Revision can be any number.

Disable Keying	Indicates that the keying attributes are not considered when attempting to communicate with a device. With Disable Keying, communication can occur with a device other than the type specified in the project. **ATTENTION:** Be cautious when using Disable Keying; if used incorrectly, this option can lead to personal injury or death, property damage, or economic loss. We strongly recommend that you do not use Disable Keying. If you use Disable Keying, you must take full responsibility for understanding whether the device being used can fulfill the functional requirements of the application.
Exact Match	Indicates that all keying attributes must match to establish communication. If any attribute does not match precisely, communication with the device does not occur.

Carefully consider the implications of each keying option when selecting one.

IMPORTANT	Changing Electronic Keying parameters online interrupts connections to the device and any devices that are connected through the device. Connections from other controllers can also be broken. If an I/O connection to a device is interrupted, the result can be a loss of data.

For more detailed information on Electronic Keying, see Electronic Keying in Logix 5000 Control Systems Application Technique, publication LOGIX-AT001.

Protected Mode

The 1756-EN2F, 1756-EN2T, 1756-EN2TP, 1756-EN2TR, 1756-EN3TR, and 1756-EN4TR support explicit protected mode.[1] When in this mode, the module does not allow any configuration changes.

The only exception is for CIP Security devices such as the 1756-EN4TR. For those, if a security policy has already been deployed to the module, then that security policy can be modified while in explicit protected mode. If a security policy has not yet been deployed to the module, then explicit protected mode w prevents an initial policy from being deployed.

Enabling Explicit Protected Mode

To enable the module in an "explicit protected mode state", follow these steps.

1. Set the rotary switches to position '900'.
2. Power up the device, and wait for the display to scroll, "Protected Mode – Change Switch Settings".
3. Power down the device.
4. Set the switches for normal operation.
5. Power up the device.
6. The device is now in Explicit Protected Mode.

Operation in Explicit Protected Mode

While operating in protected mode, the module rejects any CIP explicit messages that would change the configuration of the module. For example, you cannot change the IP address, speed, or duplex settings when the module had Explicit Protected Mode enabled.

IMPORTANT	When used in a Redundant Chassis Pair (RCP) with ControlLogix controllers, the 1756-EN2x/1756-EN4x EtherNet/IP communication modules have a special case for the Time Sync object, where the PTP_Enable attribute is allowed to be set from the backplane.
	This is needed to allow the controller to set the PTP enable using unconnected messaging in the secondary (it is set via a class 1 connection in the primary controller, and in non-RCP cases).

Disabling Explicit Protected Mode

To disable the "explicit protected mode state", follow these steps.

1. Set the rotary switches on position '000'.
2. Power up the device, and wait for the display to scroll, "Unprotected Mode – Change Switch Settings".
3. Power down the device.
4. Set the switches for normal operation.
5. Power up the device.
6. The device is now in Unprotected Mode.

(1) For 1756-EN2F, 1756-EN2T, EN3TR, and 1756-EN2TR Versions 11.001 and later.
       For 1756-EN2TP and 1756-EN4TR all versions

Protected Mode in a Redundant Adapter Pair

The 1756-EN4TR supports explicit protected mode in a redundant adapter pair. In this mode, the module does not allow any configuration changes.

Enabling Explicit Protected Mode in a Redundant Adapter Pair (RAP)

To enable the module in an "explicit protected mode state in RAP", follow these steps.

1. Put your system in a qualified state.
2. Remove the secondary device from the chassis, put it in explicit mode using the methods that are found on , and insert the module back into the chassis.

   The system is qualified with the message "Explicit Protected Mode Mismatch" on the module display.
3. Force a switchover either using AOP service or disconnect the cable.
4. Remove secondary (previous primary) device, put it in explicit mode and insert module back.

   The system has enabled explicit protected mode.

Disabling Explicit Protected Mode in a Redundant Adapter Pair

To disable the module in an "explicit protected mode state in RAP", follow these steps.

1. Put your system in a qualified state.
2. Remove the secondary device from the chassis, put it in non-protected mode using the methods that are found on , and insert the module back into the chassis.

   The system is qualified with the message "Explicit Protected Mode Mismatch" on the module display.
3. Force a switchover either using AOP service or disconnect the cable.
4. Remove secondary (previous primary) device, put it in non-protected mode and insert module back.

   The system has disabled explicit protected mode.

How to Determine if the Module is in Explicit Protected Mode

To determine if your module is in explicit protected mode, either view the AOP Module information page, or create a Generic CIP message. Set the following parameters:

- Service Type: Get Single Attribute
- Class = 1
- Instance = 1
- Attribute = 13(Hex)

The Destination Element Tag must be the INT type. Bit 3 is explicit protected mode and a value of 1 indicates that protected mode is enabled.
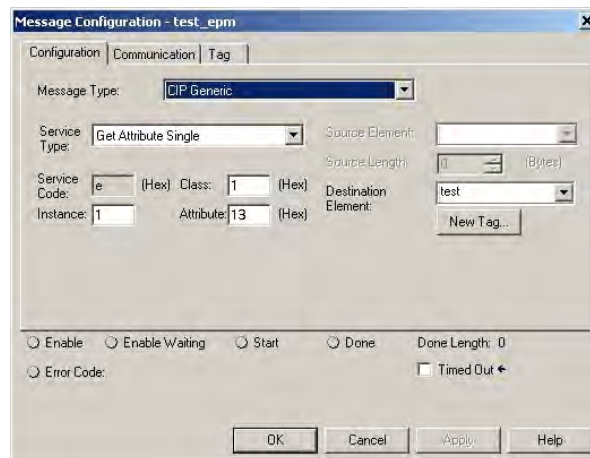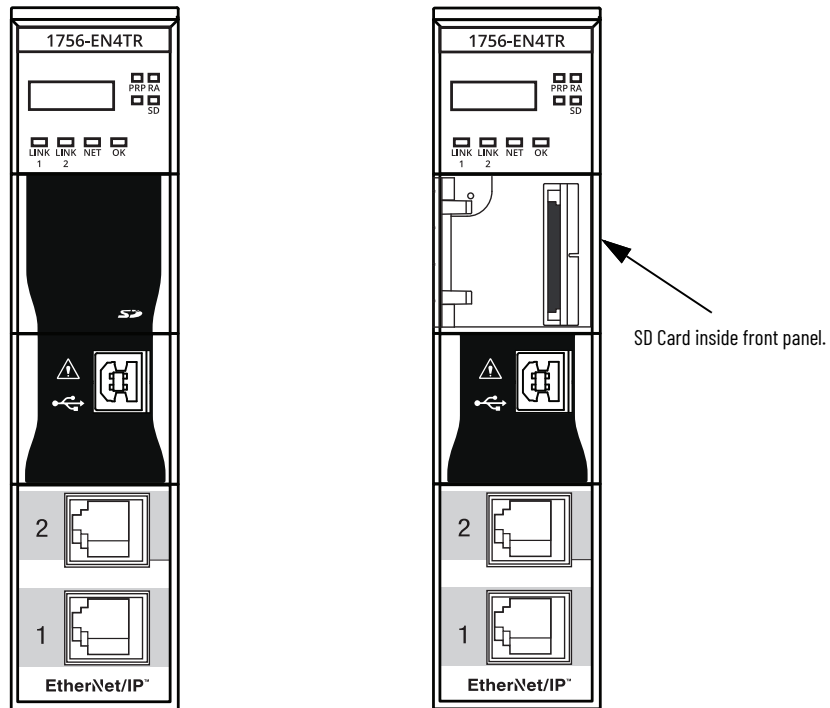
Secure Digital Card

The 1756-EN4TR uses a Secure Digital (SD) card to store:

- Module firmware
- Module configuration
- Fault logs

  You can provide the fault logs to technical support rather than shipping then entire module.

The SD card slot is inside the front panel of the module.

SD Card inside front panel.

When the device is powered up, the device uses the configuration from the SD card if the configuration does not exist in the device. When a blank SD card is inserted, or powered up, the configuration is copied from the device to the SD card that was inserted.

If the module powers up with a configuration that does not match the configuration on the already inserted SD card, the configuration on the SD card is used and copied to the module.

IMPORTANT	The 1756-EN4TR does not save the CIP Security configuration information to the SD card. On power-up, the CIP Security setting returns to the module default setting.

If the module is already powered, and an SD card is inserted, a warning message is displayed.

To see other potential error messages, see Table 12 on page 80.

To change these results, do one of two things. One option is to do an out of box reset on the module, if you want to use the configuration on the SD card. A second option is to modify one of the configuration settings on the device, if you want to use the configuration on the device.

IMPORTANT	If an SD card with a valid configuration is inserted into a 1756-EN4TR module that does not match, an error is displayed on the status display on the front of the module warning of this mis-configuration. If the SD card is intended to be used in the 1756-EN4TR module it must be cleared by external means and reinserted. If this is not done before the next power cycle of the 1756-EN4TR with the non-matching configuration, this configuration is copied to the 1756-EN4TR with all settings including the IP address from the original module. This can possibly cause an IP address conflict.

The 1756-EN4TR supports the use of a 1784-SD1 (1 GB) and 1784-SD2 (2 GB) card. You can use third-party SD cards with the device. You can use SD cards with as much as 32 GB of memory.

IMPORTANT	Rockwell Automation does not test the use of third-party SD cards with the device.

If you use an SD card other than those cards that are available from Rockwell Automation, unexpected results can occur. For example, you can experience data corruption or data loss.

SD cards that are not provided by Rockwell Automation can have different industrial, environmental, and certification ratings as those cards that are available from Rockwell Automation. These cards can have difficulty with survival in the same industrial environments as the industrially rated versions available from Rockwell Automation.

Disable Secure Digital Card

To disable the SD card, see .

CIP Security

CIP Security™ is a standard, open communication mechanism that is defined by the Open DeviceNet® Vendors' Association (ODVA) that helps to provide a secure data transport across an EtherNet/IP™ network. It lets CIP-connected devices authenticate each other before transmitting and receiving data.

CIP Security uses the following security properties to help devices protect themselves from malicious communication:

- Device Identity and Authentication
- Data Integrity and Authentication
- Data Confidentiality

Rockwell Automation uses the following products to implement CIP Security:

- FactoryTalk Services Platform, version 6.11 or later, with the following components enabled:
  - FactoryTalk Policy Manager
  - FactoryTalk System Services
- FactoryTalk Linx, version 6.11 or later
- Studio 5000® Design Environment, version 31.00.00 or later
- CIP Security-enabled Rockwell Automation products, for example, the product described in this publication

For more information on CIP Security, including which products support CIP Security, see the CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001.

IMPORTANT	Redundant Chassis Pair
	1756-EN4TR modules with firmware revision 4.001 support CIP Security when used in a **redundant chassis pair** with ControlLogix 5580 controllers that have firmware revision 34.011 or later. This supports program upload/download/monitor/HMI (not I/O).
	• The 1756-EN4TR pair must be configured for non-IP address swapping.
	• The 1756-EN4TR pair cannot be configured for redundant adapter mode while used in a **redundant chassis pair** with ControlLogix 5580 controllers.
	• The 1756-EN4TR pair that is configured for CIP security cannot be used to communicate with remote I/O, because I/O in ControlLogix redundancy requires multi-cast. A second 1756-EN4TR pair is required for I/O.
	Redundant Adapter Mode
	CIP Security is not yet supported when the 1756-EN4TR is in **redundant adapter mode** for remote I/O.
	If a 1756-EN4TR is installed and using CIP Security, and it is reconfigured to be part of a **redundant adapter pair** for remote I/O, the module loses its CIP Security configuration. When this occurs, the I/O chassis will lose communication with the controller. At this point, the CIP Security policy must be redeployed.[1]

(1) CIP Security is not supported in redundant adapters. See <u>Chapter 4</u> on <u>page 45</u>.

Syslog Event Logging

The 1756-EN4TR module supports syslog event logging. Do not use FactoryTalk AssetCentre for logging if you want to use a syslog collector.

Choose a syslog collector that supports the following:

- RFC-5424 syslog protocol
- Ability to receive messages from the 1756-EN4TR module

To set the IP address of the syslog collector, use FactoryTalk Policy Manager software.

IMPORTANT	The 1756-EN4TR module must be connected to the same network as the syslog collector.

For more information, see:

- CIP Security with Rockwell Automation Products Application Technique, publication <u>SECURE-AT001</u>.
- Logix 5000 Controller and I/O Fault Codes and Syslog Messages, publication <u>1756-RD001</u>.

Parallel Redundancy Protocol

Parallel Redundancy Protocol (PRP) is defined in international standard IEC 62439-3 and provides high-availability in Ethernet networks. PRP technology creates seamless redundancy by sending duplicate frames to two independent network infrastructures, which are known as LAN A and LAN B.

A PRP network includes the following components.

Component	Description
LAN A and LAN B	Redundant, active Ethernet networks that operate in parallel.
Double attached node (DAN)	An end device with PRP technology that connects to both LAN A and LAN B.
Single attached node (SAN)	An end device without PRP technology that connects to either LAN A or LAN B. A SAN does not have PRP redundancy.
Redundancy box (RedBox)	A switch with PRP technology that connects devices without PRP technology to both LAN A and LAN B.
Virtual double attached node (VDAN)	An end device without PRP technology that connects to both LAN A and LAN B through a RedBox. A VDAN has PRP redundancy and appears to other nodes in the network as a DAN.
Infrastructure switch	A switch that connects to either LAN A or LAN B and is not configured as a RedBox.

For more information about PRP, see the EtherNet/IP Parallel Redundancy Protocol Application Technique, publication ENET-AT006.

Device Level Ring (DLR)

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.

Table 5 -

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 are connected to one DLR network and also connected 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.

For more information about DLR, see the EtherNet/IP Device Level Ring Application Technique, publication ENET-AT007.

Notes:

Concurrent Communication

Concurrent communication is available with FLEXHA 5000™ I/O modules and FLEX 5000® safety I/O modules with redundant ControlLogix® 5580 or with Logix SIS controllers, respectively. Concurrent communication provides for **seamless failover** for any redundant pair of hardware components.

You must configure a 1756-EN4TR EtherNet/IP™ communication module in each Logix 5000® controller redundant chassis pair to use concurrent communication and not to use IP swapping mode.

With concurrent communication, data transmission between redundant ControlLogix 5580 and FLEXHA 5000 I/O modules or Logix SIS controllers and FLEX 5000 safety I/O modules is redundant at the logical and physical levels.

There are differences to how concurrent communication works with FLEXHA 5000 I/O module and FLEX 5000 safety I/O modules.

Concurrent Communication with FLEXHA 5000 I/O Modules

You can only use concurrent communication with FLEXHA 5000 I/O modules if you use the following components in your system.

Component		Software Version	Firmware Revision
Software	Studio 5000 Logix Designer® application	**Version 37.00.00 or later**	–
	FactoryTalk® Linx software	Version 6.31.00 or later	–
	ControlFLASH Plus™ software	Version 5.00.00 or later	–
ControlLogix 5580 System	ControlLogix 5580 controllers	–	Revision 37.xxx or later
	1756-EN4TR ControlLogix EtherNet/IP Communication Modules	–	Revision 7.001 or later
FLEXHA 5000 I/O System	FLEXHA 5000 EtherNet/IP adapter	–	Revision 3.011 or later
	FLEXHA 5000 I/O Modules	–	Revision 3.011 or later

Logical Level

Concurrent communication uses one logical CIP connection with two legs to the fault-tolerant I/O modules. Duplicate copies of the I/O data are transmitted across both legs. That is, there is one duplicated packet for each I/O module.

Redundant ControlLogix 5580 controllers operate in parallel to synchronize the data. As a result, the same output values occur simultaneously. The controllers open the concurrent communication path to the FLEXHA 5000 I/O modules.

Via a 1756-EN4TR EtherNet/IP communication module, ControlLogix 5580 controllers send duplicate data to the FLEXHA 5000 I/O modules that work as a redundant pair.

Each duplicate is targeted for one of the FLEXHA 5000 I/O modules in the redundant pair. The paired I/O modules receive duplicate data, compare the data, and establish one signal value that is set on the terminal screws.

A similar pattern is followed for input data that is transmitted from the paired FLEXHA 5000 I/O modules to the redundant ControlLogix 5580 controllers. Both of the controllers and I/O modules process the same data in parallel. Consequently, a failure and dropout of one device does not require a switchover and synchronization of the partner device.

Physical Level

During transmission, the duplicated data passes along physical connections from the 1756-EN4TR EtherNet/IP communication modules and the FLEXHA 5000 EtherNet/IP adapter. Physical network redundancy is provided whether the system is operating in a PRP or DLR topology. Thus, the system has increased resiliency.

The physical network redundancy is achieved via redundant paths between the 1756-EN4TR EtherNet/IP communication module and the FLEXHA 5000 EtherNet/IP adapter as follows:

- PRP network - Duplicated data at the physical level for each path.
- DLR network - Providing redundant paths.

Communication Module Configuration

To use concurrent communication with FLEXHA 5000 I/O modules, you must configure the 1756-EN4TR ControlLogix EtherNet/IP communication module on the Device Definition dialog box in your Studio 5000 Logix Designer application project to use concurrent communication.

1756-EN4TR Communication Module Configuration

IMPORTANT	You can configure the 1756-EN4TR EtherNet/IP communication module for concurrent communication, to use with I/O modules such as FLEXHA 5000 I/O modules. Or you can configure the 1756-EN4TR EtherNet/IP communication module for standard I/O, for example, remote 1756 ControlLogix I/O modules. You can only configure the module for one or the other.
	If the 1756-EN4TR EtherNet/IP communication module is configured for concurrent communication, you can still use it for class 3 communications, for example, HMI, program upload/download/monitor.
	You must disable IP address swapping in the 1756-EN4TR EtherNet/IP communication modules in the redundant chassis pair.

Concurrent Communication in a PRP Topology

This section shows how data is transmitted from one ControlLogix 5580 controller in a redundant controller pair to a duplex pair of FLEXHA 5000 I/O modules.

In this scenario, concurrent communication transmits data as follows.

1. The controller establishes concurrent communication to the 1756-EN4TR EtherNet/IP communication module in the same chassis.

   At this point, the communication is not redundant.

2. Redundant communication starts at the communication module. The communication module opens two legs of the concurrent communication and transmits duplicates of the data across those legs.

   Additionally, the communication module is connected to a redundant PRP network, that is, LAN A and LAN B. The PRP network redundancy introduces further data duplication.

   - Numbers 1A and 2A represent the two legs of the concurrent communication on one physical cable between the communication module and the LAN A switch.
   - Numbers 1B and 2B represent the physical duplication of the two legs of the concurrent communication between the communication module and the LAN B switch.

3. Duplicate data is transmitted across the two legs, and physical duplication of these legs, to the FLEXHA 5000 EtherNet/IP adapters.
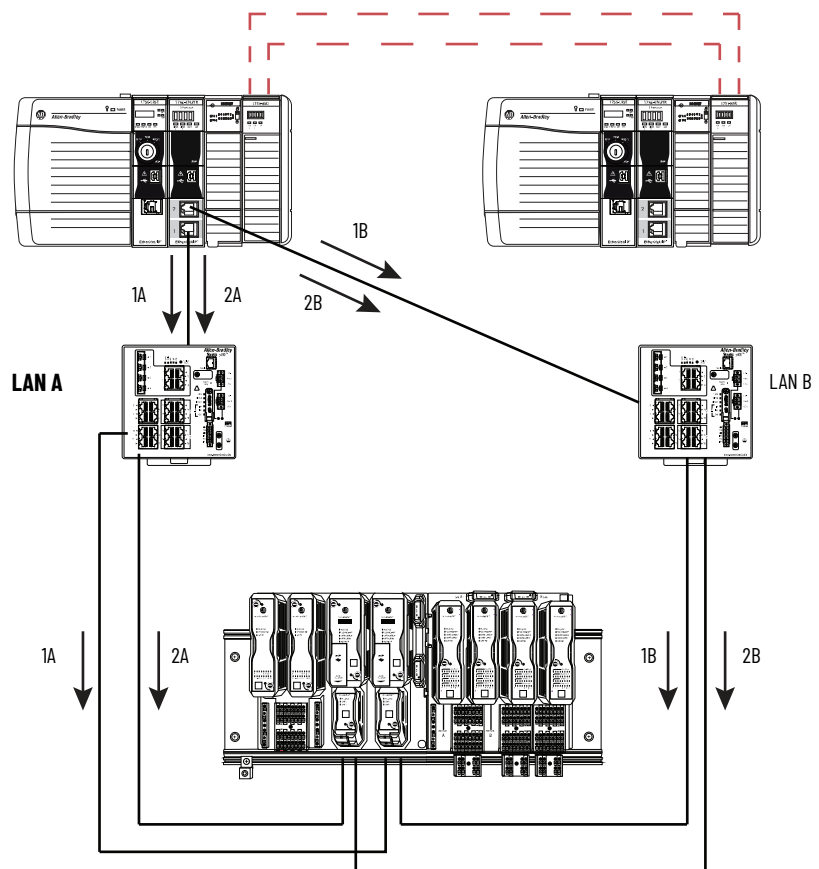
This section expands on the previous section to show that the same data is transmitted from the secondary ControlLogix 5580 controller in the redundant controller pair to the duplex pair of FLEXHA 5000 I/O modules. Data is transmitted from the secondary controller based on the logic state cross loaded from the primary controller.

In this scenario, concurrent communication transmits data as follows.

1. The ControlLogix 5580 controller establishes concurrent communication to the 1756-EN4TR EtherNet/IP communication module in the same chassis.

    At this point, the communication is not redundant.

2. Redundant communication starts at the 1756-EN4TR EtherNet/IP communication module. The 1756-EN4TR EtherNet/IP communication module opens two legs of the concurrent communication and transmits duplicates of the data across those legs.

    Additionally, the 1756-EN4TR EtherNet/IP communication module is connected to a redundant PRP network, that is, LAN A and LAN B. The PRP network redundancy introduces further data duplication.

    -   Numbers 1B' and 2B' represent the two legs of the concurrent communication on one physical cable between the 1756-EN4TR EtherNet/IP communication module and the LAN B switch.

    -   Numbers 1A' and 2A' represent the physical duplication of the two legs of the concurrent communication between the 1756-EN4TR EtherNet/IP communication module and the LAN A switch.

3. Duplicate data is transmitted across the two legs, and physical duplication of these legs, to the FLEXHA 5000 EtherNet/IP adapters.

The following graphic shows how duplicate data is transmitted from each controller across LANs A and B, respectively, simultaneously. That is, this shows what is happening when you consider both of the previous sections.

Concurrent Communication in a PRP Topology

IMPORTANT:
- Each 1756-EN4TR EtherNet/IP communication module in the redundant chassis pair sends duplicated data on each LAN simultaneously.
- Data with the similar designations, for example, 1A and 1A', are the same but from different controllers with the only difference being a small identifier. In this case, it is the prime (') designation.

This occurs because the controllers work as a redundant pair that is synchronized via ControlLogix Redundancy Modules.
- All data transmission starts simultaneously. The duplicated data that reaches the adapters first is what's used in the FLEXHA 5000 I/O system. The other data is disregarded.
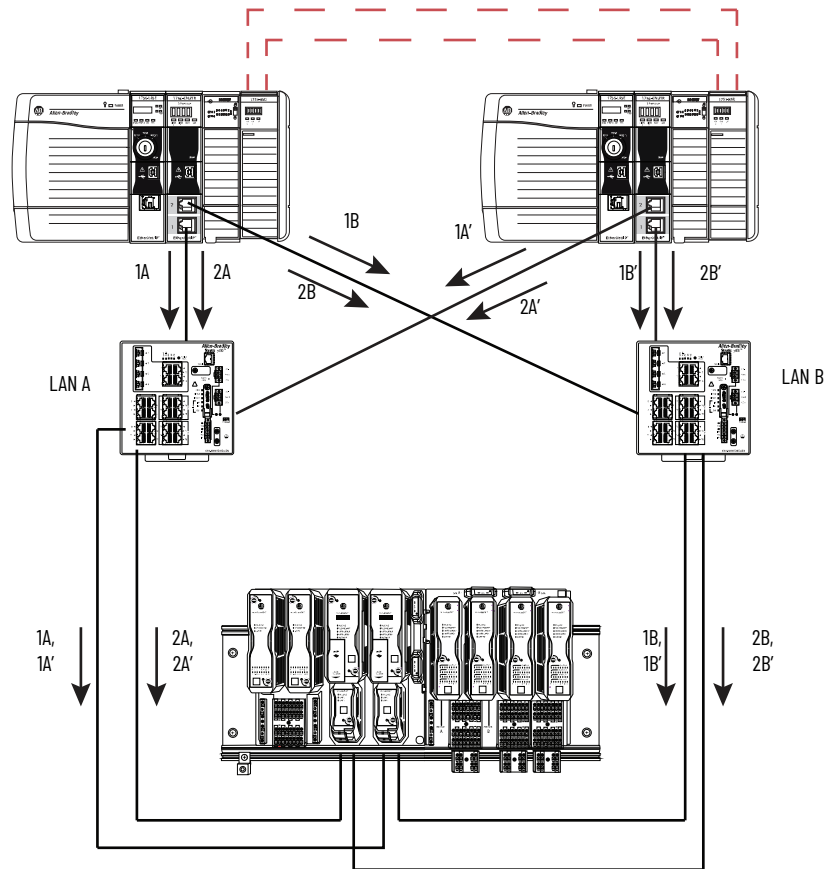
When duplicate data arrives at a FLEXHA 5000 EtherNet/IP adapter, the adapter combines the PRP duplicates and accepts the first uncorrupted PRP duplicate. The second PRP duplicate is rejected.

So from each pair of data duplicates 1A/1B, 2A/2B and 1A'/1B', 2A'/2B' become only 1/1', 2/2'.

The FLEXHA 5000 I/O adapters combine the concurrent communication legs' duplicates and only accept the first valid duplicates from the pair of 1/1' and 2/2'. After that, each adapter only processes the single packet.

The FLEXHA 5000 EtherNet/IP adapters then function in the same way as the 1756-EN4TR EtherNet/IP communication modules. The FLEXHA 5000 EtherNet/IP adapter transmits duplicated data across two legs of the concurrent communication to the FLEXHA 5000 I/O modules.

Additionally, the backplane physical redundancy establishes additional duplication of the data, in a similar way to how the PRP does it for the network. Each adapter transmits four identical data packets, one to each of two I/O modules across each of the two redundant backplanes.

The following graphic presents the idea of concurrent backplane communication. Numbers 1, 1' and 2, 2' represent the concurrent connection duplicates. Postfixes A and B are related to physical duplication.

The I/O modules receive repeated data packets. The physical redundancy layer of the slot 0 I/O module combines the duplicates and accepts the first uncorrupted duplicate of 1A, 1B to 1 and 1A', 1B' to 1'. The concurrent communication layer combines the duplicates, accepting the first uncorrupted packets. The 1 and 1' is reduced to 1.

The slot 1 I/O module executes an identical process. The redundant data are reduced to a single instance, that is, 2.

Once one or both I/O modules receive valid data, the data is applied to the terminal.

Data Transmission in FLEXHA 5000 I/O System

> **IMPORTANT**: This graphic shows how data is transmitted from FLEXHA 5000 EtherNet/IP adapters to the I/O module duplex pair. Remember, only one packet is selected per adapter from the network. From there the adapters distribute that packet information as shown.

Adapter	Transmits Across	Number of Data Packets	
		I/O Module (Slot 0)	I/O Module (Slot 1)
A	BIM A/ Backplane A	1	-
		-	1
	BIM B/ Backplane B	1	-
		-	1
B	BIM A/ Backplane A	1	-
		-	1
	BIM B/ Backplane B	1	-
		-	1
Number of instances of the same data received: 8		4	4

Concurrent Communication in a DLR Topology

A DLR topology provides a means to detect, manage, and recover from single faults in a ring-based network. The following graphic shows a DLR network in which redundant ControlLogix 5580 controllers provide high availability when they are connected to FLEXHA 5000 I/O systems in a DLR network.

In this scenario, concurrent communication transmits data as follows.

1. The ControlLogix 5580 controller establishes concurrent communication to the 1756-EN4TR EtherNet/IP communication module in the same chassis. At this point, the communication is not redundant.

2. The 1756-EN4TR EtherNet/IP communication module then transmits duplicate data across two legs of the concurrent communication to the FLEXHA 5000 EtherNet/IP adapters.

   Numbers 1…4 and 1'…4' represents four concurrent communications opened to four I/O modules in two pairs in two separate chassis (1, 2 and 3, 4). Each of these communications has two redundant legs. All this occurs on single cable.

Concurrent Communication in a DLR Topology
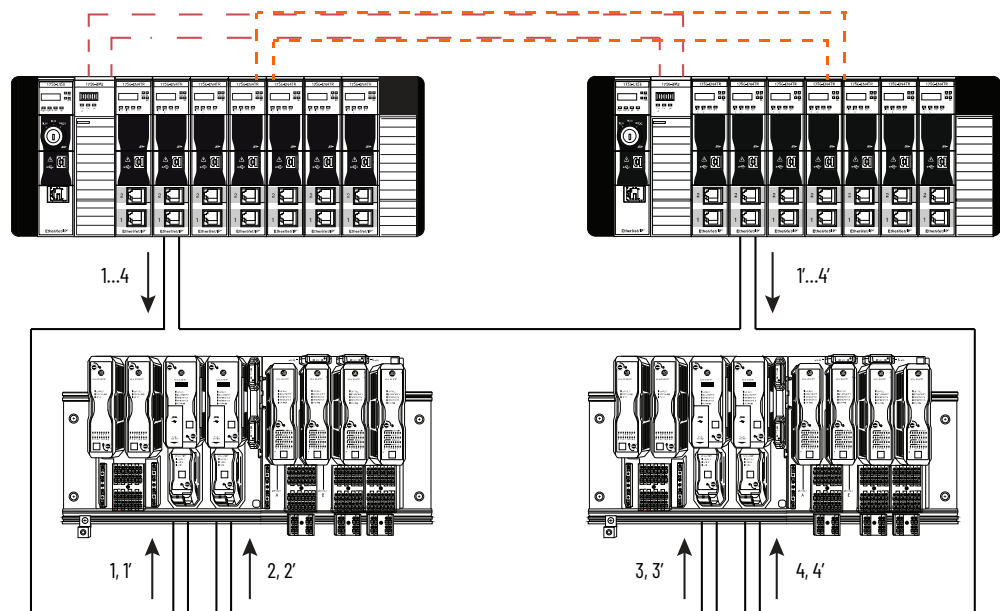
When duplicate data arrives at the FLEXHA 5000 EtherNet/IP adapters, the adapters combine concurrent communication leg duplicates, accepting only the first valid duplicates from the pair—in the first chassis 1/1' and 2/2', and in the second chassis 3/3' and 4/4'.

After that, each adapter only processes the single packet that is targeted for every I/O module in the chassis. It is packets 1 and 2 in first chassis. Packet 1 is targeted to the first I/O in the redundant I/O module pair. Packet 2 is targeted to the second I/O in the redundant I/O module pair.

The FLEXHA 5000 EtherNet/IP adapters then function in the same way as the 1756-EN4TR EtherNet/IP communication modules. The FLEXHA 5000 EtherNet/IP adapters transmit duplicated data across two legs of the concurrent communication to the FLEXHA 5000 I/O modules.

Additionally, the backplane physical redundancy establishes additional duplication of the data in a similar way to how the PRP does it for the network. Each adapter transmits four identical data packets, one to each of two I/O modules across each of the two redundant backplanes.

The following graphic presents the idea of concurrent backplane communication. Numbers 1, 1' and 2, 2' represent the concurrent connection duplicates. Postfixes A and B are related to physical duplication.

The I/O modules receive repeated data packets. The physical redundancy layer of the slot 0 I/O module combines the duplicates and accepts the first uncorrupted duplicate of 1A, 1B become 1. Also, 1A', 1B' become 1'. The concurrent communication layer combines the duplicates, accepting the first uncorrupted packets. The 1 and 1' become 1.

The slot 1 I/O module executes an identical process. The redundant data are reduced to a single instance, that is, 2.

Once one or both I/O modules receive valid data, the data is applied to the terminal.

Data Transmission in Each FLEXHA 5000 I/O System

IMPORTANT: This graphic shows how data is transmitted from FLEXHA 5000 EtherNet/IP adapters to the I/O module duplex pair. Remember, only one packet is selected per adapter from the network. From there the adapters distribute that packet information as shown.

Adapter	Transmits Across	Number of Data Packets	
		I/O Module (Slot 0)	I/O Module (Slot 1)
A	BIM A/ Backplane A	1	-
		-	1
	BIM B/ Backplane B	1	-
		-	1
B	BIM A/ Backplane A	1	-
		-	1
	BIM B/ Backplane B	1	-
		-	1
Number of instances of the same data received: 8		4	4

Concurrent Communication with FLEX 5000 Safety I/O Modules

Concurrent communication is available with FLEX 5000 safety I/O modules. It occurs between Logix SIS controllers and the I/O modules via an EtherNet/IP network.

IMPORTANT	The only safety I/O modules that Logix SIS controllers can communicate with are FLEX 5000 safety I/O modules.

You must configure a 1756-EN4TR EtherNet/IP communication module in each redundant chassis to use concurrent communication and not to use IP swapping mode.

With concurrent communication, data transmission between 1756-EN4TR EtherNet/IP communication modules and the FLEX 5000 EtherNet/IP adapter is redundant at the logical and physical levels.

IMPORTANT	FLEX 5000 I/O systems can include a mix of safety and standard I/O modules. FLEX 5000 standard I/O modules **don't support** concurrent communication, but Logix SIS controllers can still communicate with them. The first part of this section focuses on concurrent communication. For more information on how Logix SIS controllers communicate with FLEX 5000 standard I/O modules, see page 37.

You can only use concurrent communication with FLEX 5000 safety I/O modules if you use the following components in your system.

Component		Software Version	Firmware Revision
Software	Studio 5000 Logix Designer application	**Version 37.00.00 or later**	–
	FactoryTalk Linx software	Version 6.31.00 or later	–
	ControlFLASH Plus software	Version 5.00.00 or later	–
Logix SIS Components	GuardLogix® 5580 controllers	–	Revision 37.xxx or later
	1756-EN4TR ControlLogix EtherNet/IP Communication Modules	–	Revision 7.001 or later
FLEX 5000 Safety I/O System Components	FLEX 5000 EtherNet/IP adapter	–	Revision 6.011 or later
	FLEX 5000 Safety I/O Modules	–	Any

Logical Level

Concurrent communication uses a logical CIP connection to the I/O module. Logix SIS controllers open the concurrent communication path to the FLEX 5000 EtherNet/IP adapter.

The controllers operate in parallel to synchronize the data. Each controller sends a data packet to the 1756-EN4TR EtherNet/IP adapter in its local chassis. The data packets are identical. The adapters transmit the data on the EtherNet/IP network. As a result, the same output values occur simultaneously. Thus, data is duplicated.

When data arrives at the FLEX 5000 EtherNet/IP adapter, it converts the concurrent communication to standard communication and sends one data packet to the I/O module. The I/O module establishes a signal value that is set on the terminal screws.

A similar pattern is followed for input data that is transmitted from the FLEX 5000 safety I/O module to the Logix SIS controllers. The I/O module sends one data packet to the FLEX 5000 EtherNet/IP adapter, the adapter then sends identical data packets onto the 1756-EN4TR EtherNet/IP adapters in the redundant chassis. Thus, the data is duplicated. Each adapter then sends a single data packet to the GuardLogix 5580 controller in its chassis.

Physical Level

During transmission, the duplicated data passes along physical connections between the 1756-EN4TR EtherNet/IP communication modules and the FLEX 5000 EtherNet/IP adapter. The physical network redundancy is achieved via redundant paths between the 1756-EN4TR EtherNet/IP communication module and the FLEX 5000 EtherNet/IP adapter as follows:

- PRP network - Duplicated data at the physical level for each path.
- DLR network - Providing redundant paths.

Communication Module Configuration - FLEX 5000 Safety I/O Modules

To use concurrent communication with FLEX 5000 safety I/O modules, you must configure the 1756-EN4TR ControlLogix EtherNet/IP communication module on the Device Definition dialog box in your Studio 5000 Logix Designer application project to use concurrent communication.

1756-EN4TR Communication Module Configuration - Communicate with FLEX 5000 Safety I/O Modules

	IMPORTANT	You can configure the 1756-EN4TR EtherNet/IP communication module for concurrent communications, to use with I/O modules such as FLEX 5000 safety I/O modules. Or you can configure the 1756-EN4TR EtherNet/IP communication module for standard I/O, for example, remote 1756 ControlLogix I/O modules. You can only configure the module for one or the other.
		If the 1756-EN4TR EtherNet/IP communication module is configured for concurrent communication, you can still use it for class 3 communications, for example, HMI, program upload/download/monitor.
		You must disable IP address swapping in the 1756-EN4TR EtherNet/IP communication modules in the redundant chassis pair.

Concurrent Communication in a PRP Topology

This section shows how data is transmitted from one controller in a Logix SIS to a FLEX 5000 safety I/O module.

In this scenario, concurrent communication transmits data as follows.

1. The controller establishes concurrent communication to the 1756-EN4TR EtherNet/IP communication module in the same chassis.

    At this point, the communication is not redundant.

2. Redundant communication starts at the communication module. The communication module opens a leg of the concurrent communication.

    The communication module is connected to a redundant PRP network, that is, LAN A and LAN B. The PRP network redundancy introduces data duplication.

    -   Number 1A represents the leg of the concurrent communication on one physical cable between the communication module and the LAN A switch.
    -   Number 1B represents the physical duplication of the leg of the concurrent communication between the communication module and the LAN B switch.

3. Duplicate data is transmitted to the FLEX 5000 EtherNet/IP adapter.
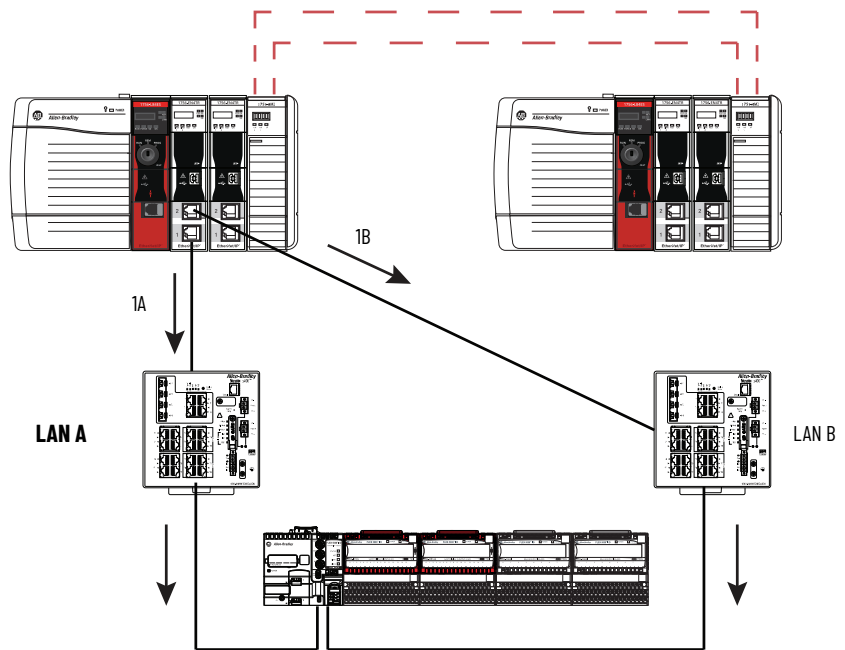
This section expands on the previous section to show that the same data is transmitted from the secondary controller in the Logix SIS to the FLEX 5000 safety I/O module. Data is transmitted from the secondary controller based on the logic state cross loaded from the primary controller.

In this scenario, concurrent communication transmits data as follows.

1. The controller establishes concurrent communication to the 1756-EN4TR EtherNet/IP communication module in the same chassis.

    At this point, the communication is not redundant.

2. Redundant communication starts at the communication module. The communication module opens a leg of the concurrent communication.

    The communication module is connected to a redundant PRP network, that is, LAN A and LAN B. The PRP network redundancy introduces data duplication.

    -   Number 1B' represents the leg of the concurrent communication on one physical cable between the 1756-EN4TR EtherNet/IP communication module and the LAN B switch.

    -   Number 1A' represents the physical duplication of the leg of the concurrent communication between the 1756-EN4TR EtherNet/IP communication module and the LAN A switch.

3. Duplicate data is transmitted to the FLEX 5000 EtherNet/IP adapter.

The following graphic shows how duplicate data is transmitted from each controller across LANs A and B, respectively, simultaneously. That is, this shows what is happening when you consider both of the previous sections.

Concurrent Communication to FLEX 5000 Safety I/O Modules in a PRP Topology

IMPORTANT:
- Each 1756-EN4TR EtherNet/IP communication module in the redundant chassis pair sends duplicated data on each LAN simultaneously.
- Data with the similar designations, for example, 1A and 1A', are the same but from different controllers with the only difference being a small identifier. In this case, it is the prime (') designation.

This occurs because the controllers work as a redundant pair that is synchronized via ControlLogix Redundancy Modules.

- All data transmission starts simultaneously. The duplicated data that reaches the adapters first is what's used in the FLEX 5000 I/O system. The other data is disregarded.
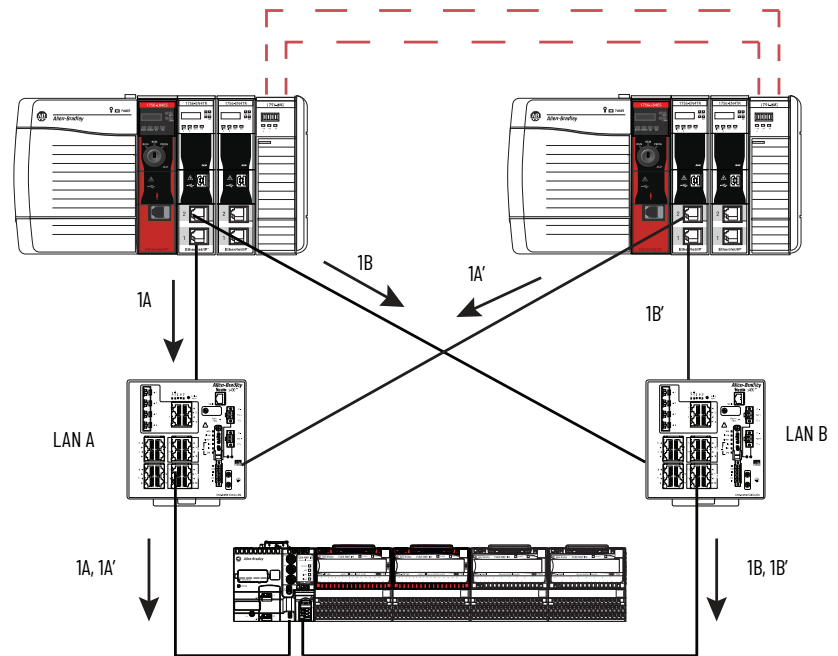
When the data arrives at the FLEX 5000 EtherNet/IP adapter, it converts the concurrent communication to standard communication and sends one data packet to the safety I/O module.

Concurrent Communication in a DLR Topology

A DLR topology provides a means to detect, manage, and recover from single faults in a ring-based network. The following figure shows a DLR network in which Logix SIS controllers provide high availability when they are connected to FLEX 5000 I/O systems in a DLR network.

In this scenario, concurrent communication transmits data as follows.

1. The controller establishes concurrent communication to the 1756-EN4TR EtherNet/IP communication module in the same chassis. At this point, the communication is not redundant.

2. The 1756-EN4TR EtherNet/IP communication modules then transmit duplicate data across a leg of the concurrent communication to the FLEX 5000 EtherNet/IP adapters.

   Numbers 1 and 1' represent concurrent communication opened to the adapter in the first FLEX 5000 I/O system. Number 2 and 2' represent concurrent communication opened to the adapter in the second FLEX 5000 I/O system. Each of these communications has two redundant legs. All this occurs on single cable.

Concurrent Communication to FLEX 5000 Safety I/O Modules in a DLR Topology
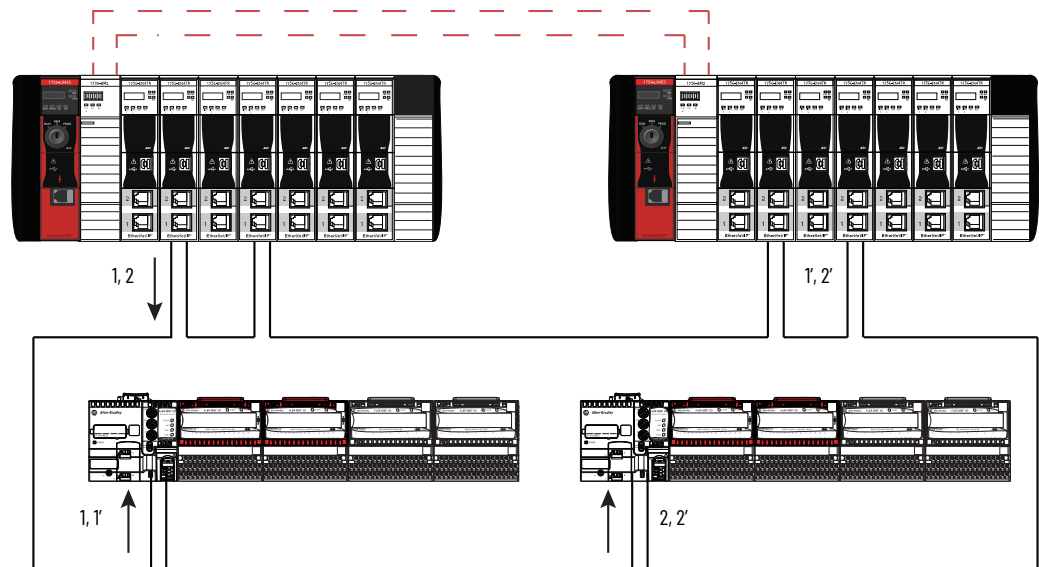
When the data arrives at the FLEX 5000 EtherNet/IP adapter in each system, it converts the concurrent communication to standard communication and sends one data packet to the I/O module.

Standard Communication Between Logix SIS Controllers and FLEX 5000 Standard I/O Modules

FLEX 5000 I/O systems can include a mix of safety and standard I/O modules. FLEX 5000 standard I/O modules don't support concurrent communication. However, Logix SIS controllers can still communicate with FLEX 5000 standard I/O modules in the FLEX 5000 I/O system that includes safety I/O modules.

The Logix SIS controllers communicate with the FLEX 5000 standard I/O modules via a second 1756-EN4TR EtherNet/IP communication module in each redundant chassis.

Communication Module Configuration - FLEX 5000 Standard I/O Modules

You must configure the second 1756-EN4TR EtherNet/IP communication module in each chassis to not use concurrent communication on the Device Definition dialog box and to use IP swapping.

> To use IP Swapping, assign the same IP address and Subnet mask values to the partnered 1756-EN4TR EtherNet/IP communication modules in the redundant chassis. When the redundancy system begins operating, the primary module uses the assigned IP address and the secondary module changes its IP address to the next highest value.

1756-EN4TR Communication Module Configuration - Communicate with FLEX 5000 Standard I/O Modules

The following graphic shows the standard communication in a PRP topology from the Logix SIS controllers to the FLEX 5000 standard I/O modules via a 1756-EN4TR EtherNet/IP communication module in each redundant chassis.

IMPORTANT	In a redundancy system that includes FLEX 5000 standard I/O modules, only the primary controller sends data to the FLEX 5000 standard I/O modules. The second controller doesn't send data. It only sends data if there is a switchover and it becomes the primary controller.
	Both controllers receive data from the I/O modules.

The standard communication passes along the physical connection from the redundant chassis to the switches.

The concurrent communication and the standard communication to the FLEX 5000 I/O modules share the same EtherNet/IP network. Concurrent communication to the FLEX 5000 safety I/O modules and standard communication to the FLEX 5000 standard I/O modules pass along the same cable from the switches to the FLEX 5000 I/O system.

At that point, data is passed along the FLEX 5000 I/O system backplane to the safety I/O modules and standard I/O modules separately.

Communication to FLEX 5000 Safety I/O and Standard I/O Modules and FLEXHA 5000 I/O Modules in a PRP Topology

—— Concurrent communication passes along these cables.

—— • Standard communication to FLEX 5000 I/O standard modules passes along these cables when they connect the 1756-EN4TR module to the switch.
• Standard and concurrent communication to FLEX 5000 I/O modules pass along these cables when they connect the switch to the FLEX 5000 I/O EtherNet/IP adapter.
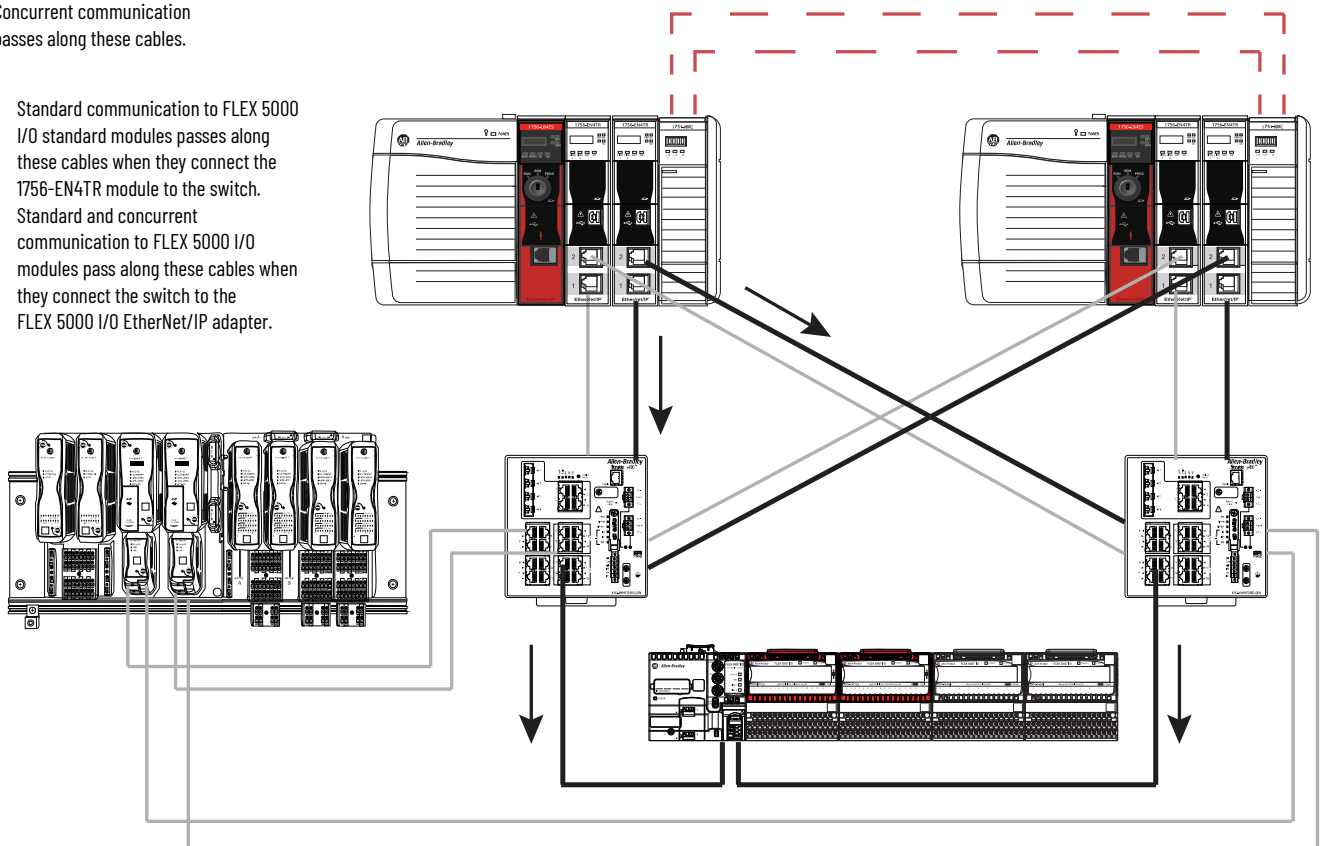
IMPORTANT:
• The 1756-EN4TR module in slot 1 of the ControlLogix chassis can only be used for concurrent communication.
This example include FLEXHA 5000 I/O modules to illustrate that the concurrent communication with FLEX 5000 safety I/O modules and FLEXHA 5000 I/O modules passes along the same cable between the 1756-EN4TR module and the switch.
• The 1756-EN4TR module in slot 2 of the ControlLogix chassis can only be used for standard communication.
• The controllers use concurrent communication with the FLEX 5000 safety I/O modules in slots 1 and 2 of the FLEX 5000 I/O system.
• The controllers use standard communication with the FLEX 5000 I/O standard modules in slots 3 and 4 of the FLEX 5000 I/O system.

The following graphic shows the standard communication in a DLR topology from the Logix SIS controllers to the FLEX 5000 standard I/O modules via the second 1756-EN4TR EtherNet/IP communication module in the chassis.

IMPORTANT	In a redundancy system that includes FLEX 5000 standard I/O modules, only the primary controller sends data to the FLEX 5000 standard I/O modules. The second controller doesn't send data. It only sends data if there is a switchover and it becomes the primary controller.
	Both controllers receive data from the I/O modules.

The standard communication passes along the physical connection from the redundant chassis to the switches.

The concurrent communication and the standard communication to the FLEX 5000 I/O modules share the same EtherNet/IP network. Concurrent communication to the FLEX 5000 safety I/O modules and standard communication to the FLEX 5000 standard I/O modules pass along the same cable from the switches to the FLEX 5000 I/O system.

At that point, data is passed along the FLEX 5000 I/O system backplane to the safety I/O modules and standard I/O modules separately.

Communication to FLEX 5000 Safety I/O and Standard I/O Modules in a DLR Topology

IMPORTANT:
- The 1756-EN4TR module in slot 1 of the ControlLogix chassis can only be used for concurrent communication.
- The 1756-EN4TR module in slot 2 of the ControlLogix chassis can only be used for standard communication.
- The controllers use concurrent communication with the FLEX 5000 safety I/O modules in slots 1 and 2 of the FLEX 5000 I/O systems.
- The controllers use standard communication with the FLEX 5000 I/O standard modules in slots 3 and 4 of the FLEX 5000 I/O systems.

Notes:

Connect to the EtherNet/IP Network

Topic	Page
Set the IP Address	41
Set the IP Address with Rotary Switches	42
Other Methods to Set the Address	43
Reset the Module to Factory Default Value	43
Redundant Adapter Considerations Setting the IP Address	44

EtherNet/IP™ networks are communication networks that offer a comprehensive suite of messages and services for many automation applications.

The following are examples of applications that use EtherNet/IP networks:

- Real-Time Control
- Time Synchronization
- Motion

This open network standard uses commonly available Ethernet communication products to support real-time I/O messaging, information exchange, and general messaging.

EtherNet/IP networks also support CIP Safety™, which makes the simultaneous transmission of safety and standard control data and diagnostics information over a common network possible.

Set the IP Address

The following conditions are required to set the IP address.

Requirements

To set the IP address, have the following:

- EtherNet/IP or USB drivers that are installed on the programming workstation
- MAC ID from the device, which is on the label on the side of the device
- Recommended IP address for the device

Set the IP Address with Rotary Switches

This graphic shows the rotary switches on a 1756 EtherNet/IP communication module. The three rotary switches at the bottom of the module, labeled X, Y, and Z, can be used for setting the IP address. If the rotary switches are not set to a valid number, the module attempts to use the BOOTP/DHCP server to set the IP address.
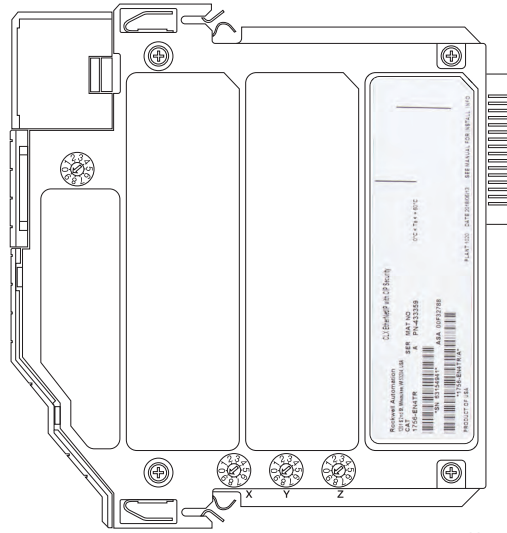
At power-up, the module reads the rotary switches to determine if they are set to a valid number for the last portion of the IP address. Valid numbers range from 001…254.

If the settings are a valid number, these conditions result:

- IP address = 192.168.1.xxx (where xxx represents the switch settings)
- Subnet mask = 255.255.255.0
- Gateway address = 192.168.1.1

> 💡 Some modules now provide a gateway address of 0.0.0.0 when the network address is set with rotary switches.

- The module does not have a host name that is assigned to it, nor does it use any Domain Name System

We recommend that you set the rotary switches to a valid number before installing the module.

IMPORTANT	For more information on how to use the BOOTP/DHCP server to set the IP address, see EtherNet/IP Network Configuration Manual, publication ENET-UM006

1756-EN4TR Mode Rotary Switch

The rotary switch in the upper left corner of the module is reserved for DLR, PRP, and redundancy features.

- For modules built with firmware revision 4.001 or later, the default position of the switch is 0.
- For modules built with firmware revision 3.002 and earlier, the default position of the switch set to 9 for DLR, linear, or star topologies.

> **ATTENTION:** If the mode rotary switch is set to 9 (DLR), and you insert the module into a PRP network, it can disable the network because it will directly connect PRP LAN A and PRP LAN B.

- The switch must be set to 7 for a redundant adapter with DLR or star topologies.
- The switch must be set to 6 for a redundant adapter with PRP.
- Set the switch to the appropriate mode according to Table 6.

  If the switch is in a position that is not implemented, the module displays the message "Unsupported mode. Change rotary switch setting" on the status display. The module does not respond on any port until the mode switch is set to the correct position and is power-cycled.

Table 6 shows the capabilities of the mode rotary switch.

Table 6 - Mode Rotary Switch Capabilities

Switch Position	Capability
9	DLR or Single-port
8	PRP or Single-port
7	Redundant Adapter and DLR or single-port topologies
6	Redundant Adapter and PRP or single-port topologies

> **IMPORTANT** If you use a redundant adapter pair, the mode rotary switches of both modules in the redundant adapter pair must be set to the same value.

Other Methods to Set the Address

The modules support the following additional methods to change the IP address:

- RSLinx® Classic software
- EtherNet/IP Commissioning Tool
- FactoryTalk® Linx Network Browser software
- Studio 5000 Logix Designer® Application
- Using Secure Digital Card (1756-EN4TR only)
- For more information on how to use these methods, see EtherNet/IP Network Configuration Manual, publication ENET-UM006.

Reset the Module to Factory Default Value

You can reset the configuration of the module to its factory default value with the following method.

If the module has rotary switches, set the switches to 888 and cycle power.

Redundant Adapter Considerations Setting the IP Address

The following are considerations when using two 1756-EN4TR modules as a Redundant Adapter Pair.

- DHCP is not supported in Redundant Adapter Mode.
- Default Class C addresses like 192.168.1.x can be set using rotary switches on the module in any mode.
- IP address assignments other than default Class C can only be set in non-redundant adapter mode, where the switch is set to 8 or 9.
- Both 1756-EN4TR modules must be set to the same IP address before switching to Redundant Adapter Mode, where the switch is set to 6 or 7.
- You must reserve an IP+1 address that is taken automatically by the secondary.

  For example, if the primary address is 192.168.1.1, the address 192.168.1.2 must be reserved.

To set the IP address for redundant adapters use the following steps.

1. Insert one module into the chassis in the standard mode (rotary mode switch set to 8 or 9).
2. Set the IP address on the module.
3. Remove the module from the chassis.
4. Insert a second module into the chassis.
5. Set the same IP address on the second module as you set on the first module.
6. Set the rotary mode switches to 6 or 7 on both modules to put the modules in redundant adapter mode, and put the modules in slots 0 and 1.

Connect Redundant EtherNet/IP Adapters

Topic	Page
Redundant Design Considerations	45
Redundant System Components	46
Redundant Switchovers	46
Configure a 1756-EN4TR Redundant Adapter Pair	48
Redundant Architecture	53
Redundant Architecture Network Considerations	55
PRP Architecture with RedBox Switches	57
PRP Architecture without RedBox Switches	58

Redundant 1756-EN4TR adapters can be used for added resiliency at the adapter level. One adapter acts as the primary and controls the I/O, while the other adapter acts as a secondary and can take over as the primary if needed. Redundant Adapter functionality is available starting in revision 3.001 firmware.

Redundant Design Considerations

There are some details and rules to consider with redundant design considerations in the following list.

- Do not exceed 80% of the maximum allowed packet rate capacity (max: 50,000 pps).
- Only I/O modules are supported in the redundant adapter chassis. The redundant chassis does not support the following.
  - motion modules
  - communication modules such as DHRIO and DeviceNet®
  - controllers
- Redundant adapters must reside in slots 0 and 1 only.
- The fourth rotary switch on the redundant 1756-EN4TR adapter must be set to number 7 for a redundant adapter with DLR, or 6 for a redundant adapter with PRP. Note that PRP is available starting with firmware revision 4.001.

> ⚠️ **ATTENTION:** For redundant adapter functionality, two 1756-EN4TR adapters must have configurations that match, including IP addresses and rotary switches, in both slot 0 and 1.
> If you are using one 1756-EN4TR adapter, it functions as one adapter.
>
> If a redundant adapter is in slot 0 or slot 1, then both of those slots must contain a redundant adapter. No other types of modules can be part of the pair.

Redundant System Components

The following features are supported with the 1756-EN4TR redundant adapter pair in firmware revision 4.001 or later:

- PRP

The following features are not currently supported with the 1756-EN4TR redundant adapter pair.

- CIP Safety™ modules
- CIP Security™

Redundant adapters can be used with redundant controllers or one controller.

For more information on redundancy, see the Redundancy Systems User Manual, publication 1756-UM015.

Redundant Switchovers

During redundant adapter operation, if certain conditions occur to the primary adapter, control is switched to the secondary adapter. These conditions cause a switchover:

- Major fault/assert on the adapter
- Failure of the adapter
- Removal of the adapter
- A program-prompted command to switchover
- An AOP-prompted command to switchover
- The adapter loses both Ethernet links

Switchover Considerations

Each 1756-EN4TR adapter uses one IP address as the primary IP address for all communication on the EtherNet/IP™ network. The redundant adapter pair consists of one active and one stand-by adapter.

The two adapters negotiate which is the primary, depending on the status of the system. If the primary adapter is unable to perform its role, for example, if a fault occurs in the primary adapter, then the secondary adapter becomes the new primary, assuming the IP address of the first primary adapter and taking over the role of communication. The primary adapter is the only adapter of the pair that produces data on the EtherNet/IP network.

On power-up, the primary is chosen from a pair of devices. The secondary adapter uses the primary IP address +1. For example, if the primary adapter has an IP address of 'N', then the secondary adapter has an IP address of 'N+1'.

The primary adapter is always active and is responsible for monitoring all inputs and outputs, monitoring diagnostics in the system, and reading and writing data to and from I/O simultaneously. The secondary adapter is waiting to take over communication, if the primary switches over.

If there is a switchover, the IP address swapping between the primary adapter and the secondary adapter takes no longer than 50 ms from the time of the initiating fault. The secondary adapter is the new primary and handles all communication. Depending on the RPIs configured, the observed switchover time can appear longer. Transmission time that is imposed by network infrastructure has to be considered when calculating overall switchover time. No connection drops occur during this switchover process.

This IP address swap is transparent to the user. You can detect which adapter the primary adapter is by examining the four character display indicator near the top of each adapter. On the primary adapter, the network status indicator is steady green. On the secondary adapter, the network status indicator flashes green.

Once a swap occurs, the 'new' primary adapter remains the primary unless there is a reason to swap over again. When the previous primary adapter is reinserted or reconnected, both adapters start the qualification process again with the adapter that was reconnected becoming the new qualified secondary.

Status Display Codes

Table 7 shows the different Redundant Adapter status codes that can appear on the adapter.

Table 7 - Primary and Secondary Operation Modes

Status Code	Description
PwrUp	Power Up/ Unknown
DS	Disqualified secondary
QS	Qualified secondary
PwQs	Primary with qualified secondary partner
PwDS	Primary with disqualified secondary
PwNS	Primary with no secondary
DSwP	Disqualified secondary with primary

Adapter Qualification

In a Redundant Adapter configuration, one adapter takes the Primary role and a second adapter becomes the Qualified Secondary ready to take I/O control when the primary becomes disqualified.

To complete the qualification process the following conditions must be met. The modules must:

- have the same firmware revision.
- reside in slots 0 and 1 of the same chassis.
- be initially set to the same IP address.
- have at least one Ethernet port link active.
- be connected to the same Ethernet network.

Configure a 1756-EN4TR Redundant Adapter Pair

To configure a 1756-EN4TR redundant adapter pair, use the following steps.

1. To set the IP address, see .
2. Make sure you are using the Studio 5000 Logix Designer® application in offline mode.
3. In the I/O configuration tree, add the 1756-EN4TR in slot 0.
4. Name your module and enter the IP address.
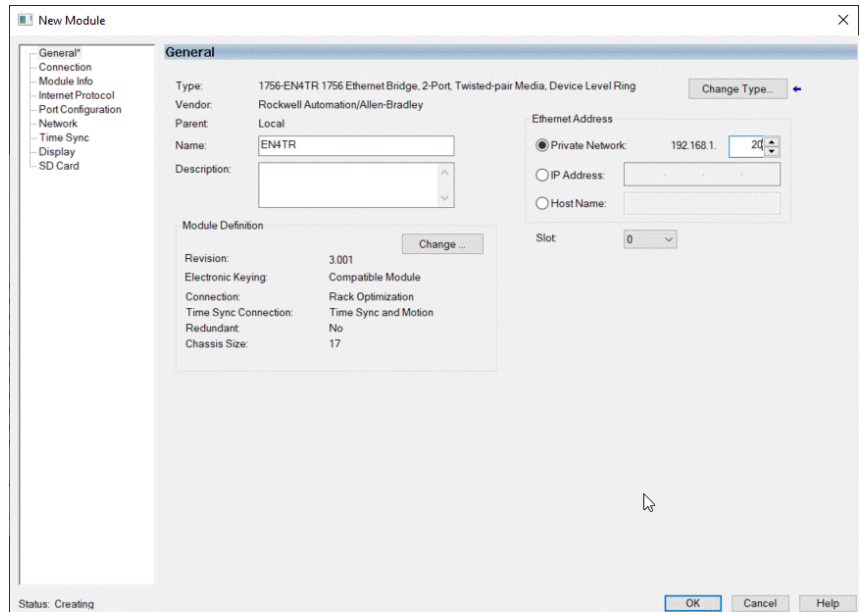
IMPORTANT	Do not put any devices in slot 1 in the I/O configuration tree.

5. Click change under the module definition pane, and select "Yes" for redundancy.
6. If you have one of the following modules in your chassis, Select Time Sync and Motion.
   - 1756-IB16IF
   - 756-OB16IEF
   - 1756-OB16IEFS

   When a chassis is configured for a 1756-EN4TR redundant adapter pair and the I/O chassis contains any of the preceding modules, then the 1756-EN4TR modules must be configured as Time Sync and Motion or unexpected connection drops can occur.
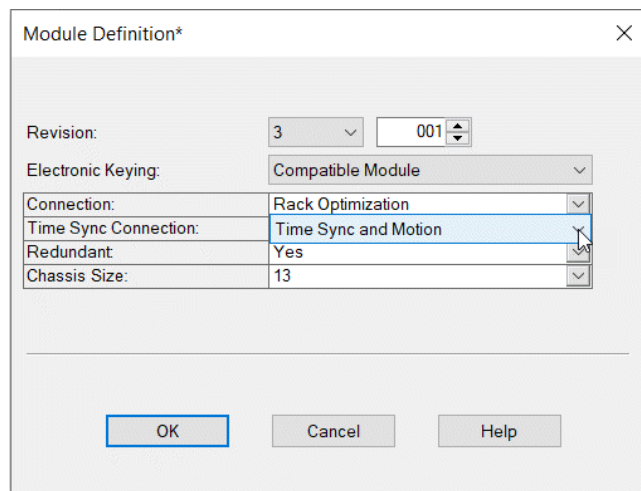
7. Power the adapters, and the synchronization process starts. Once synchronization has completed, one adapter reports as PwQS and the other adapter reports as QS. This status displays on the adapter.

    The adapter that reports as QS has an IP address that was incremented by one, which was incremented by the firmware in the module.

8. Go online with the project and click Download.
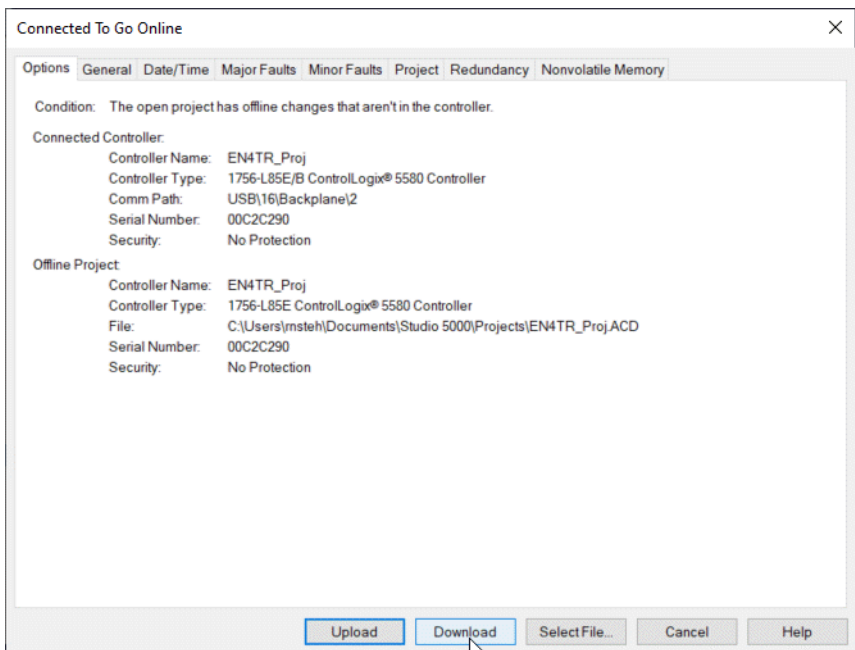
9. Examine the AOP screens by right-clicking on the module and select Properties.

You can now see options in your configuration tree for Module Info Primary, Module Info Secondary, and Redundancy.

The image below shows the Module Info Primary Tab.
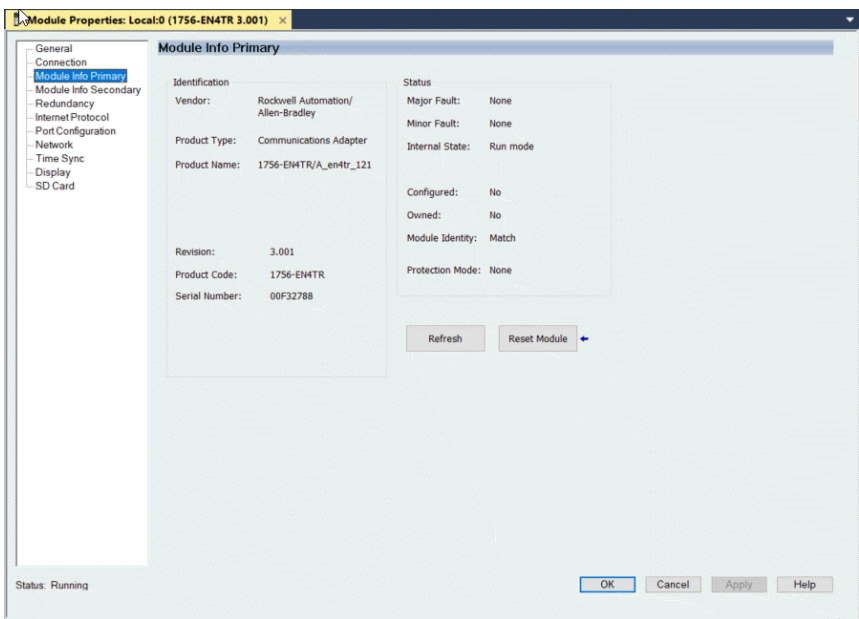
10. Under the Redundancy tab, click Qualify Secondary.
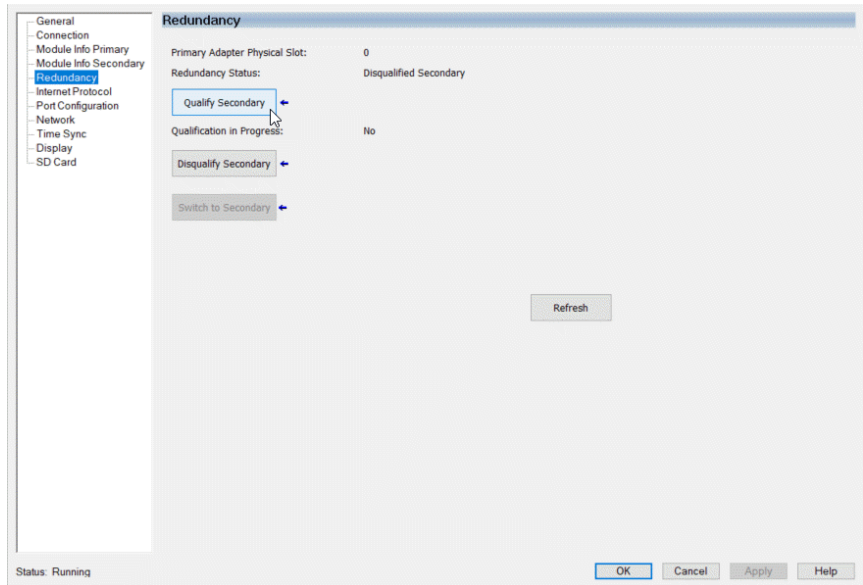
11. Click the Module Info Secondary page and examine the information.

    In the Status table, the Configured section says "No" if it is not qualified.
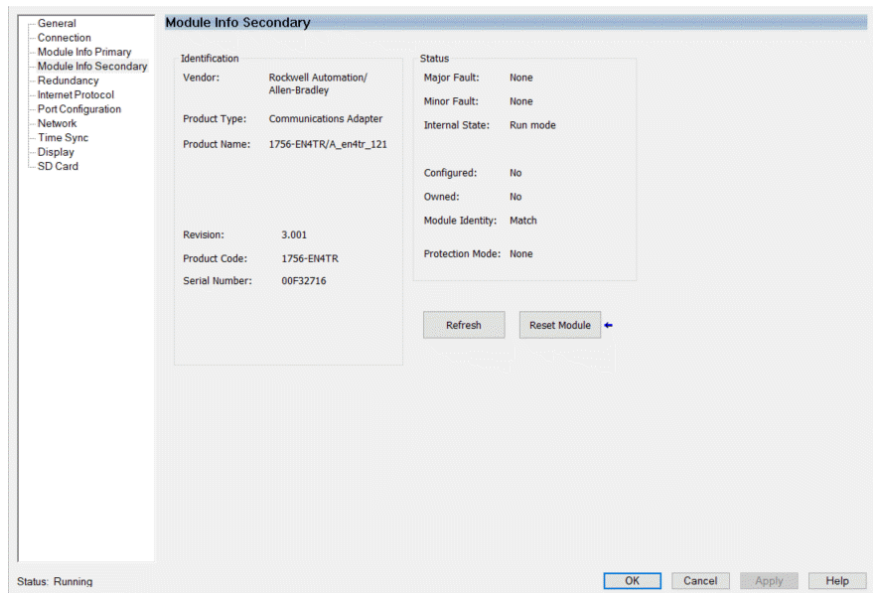
12. To verify that the redundancy feature created a redundant adapter system, click the General tab.

You should see the properties for the module defined with both Slot 0 and Slot 1.
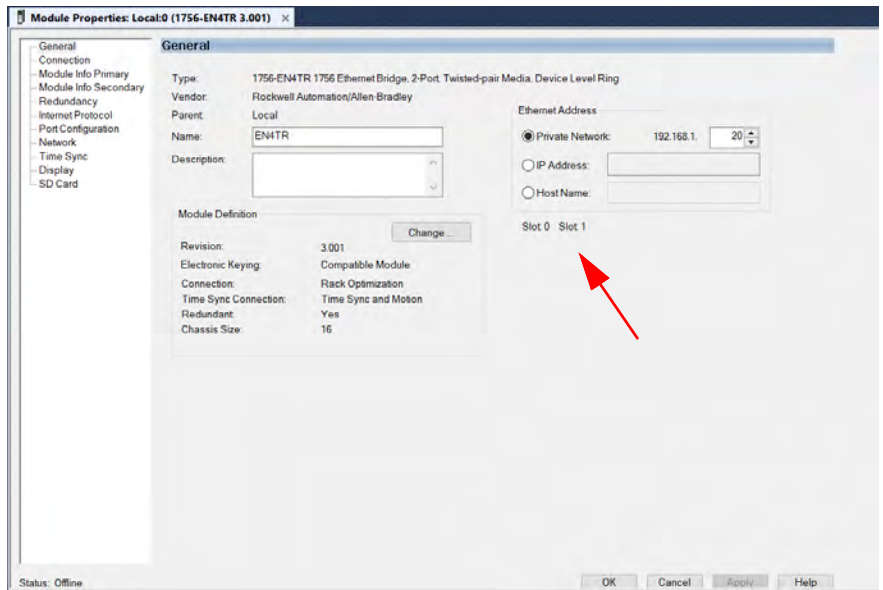
If the primary module was in slot 1 and a switchover occurred, you can see a change in the serial number of the module to match the module in slot 1.
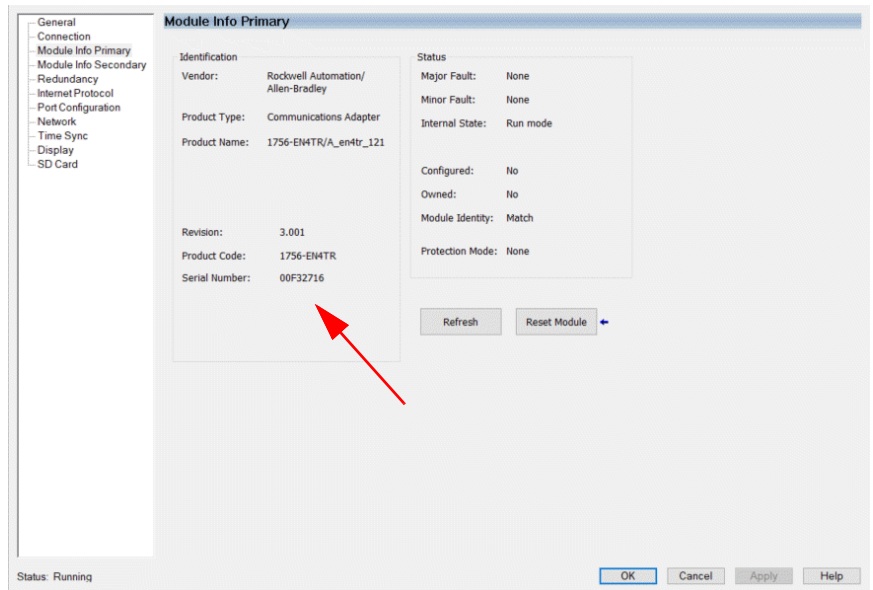
13. To confirm that a switchover occurred and there is no longer a secondary, on the redundancy page, click refresh. You should see "No Secondary" appear.
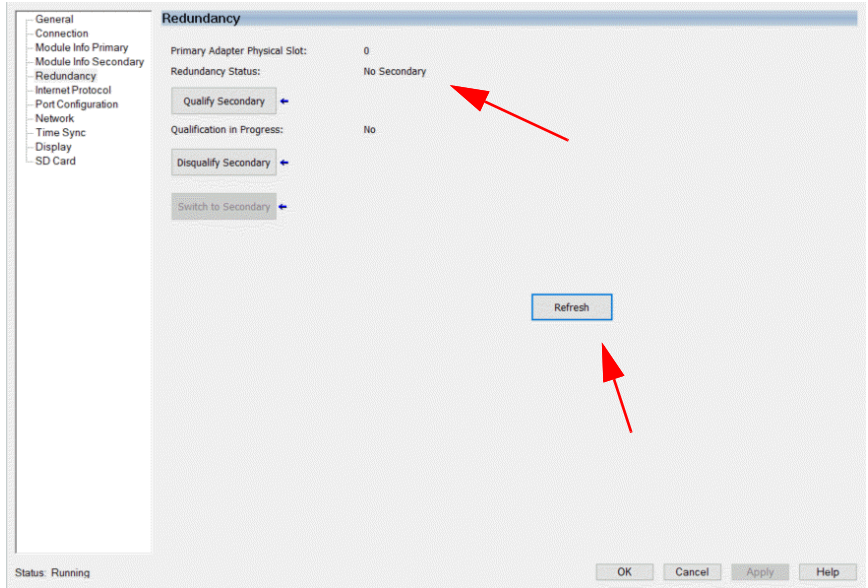
In the following figure, there is an example of an I/O module in slot 1. Even with a 1756-EN4TR in slot 0, with any other module apart from a second 1756-EN4TR in slot 1 (in this example it is the 1756-IF8) you cannot enable redundancy. On the module redundancy page, any attempt that is made to change the redundant function to "yes" results in the following error.
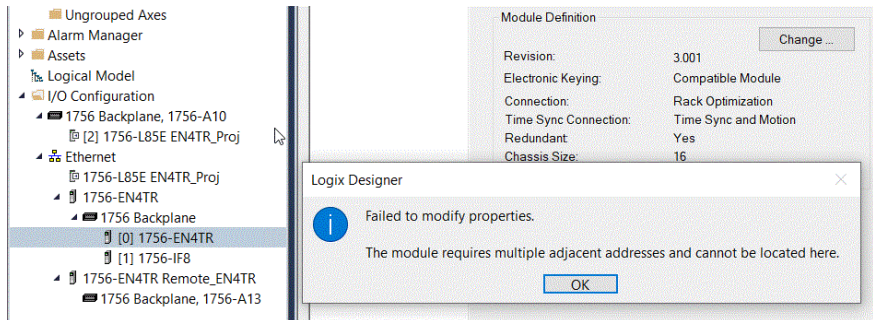
If you try to make a redundancy system starting in any other slot in the chassis other than slot 0, the redundancy option will not be available on the module definition configuration screen. The redundant adapter must be present in slot 0.
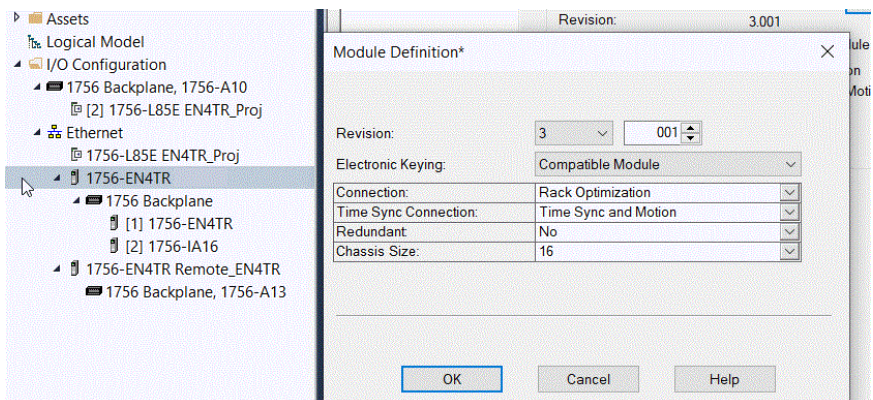
Redundant Architecture

The following figures show DLR and Star Topology with the 1756-EN4TR module. DLR provides higher resiliency than a single star. Linear topologies are not recommended because any break or firmware updating of devices in the line causes loss of communications to downstream devices.

Figure 2 - Redundant 1756-EN4TR Adapters in DLR Topology

1756-EN2TR
(can also be a 1756-EN4TR)

1756-EN4TR pair
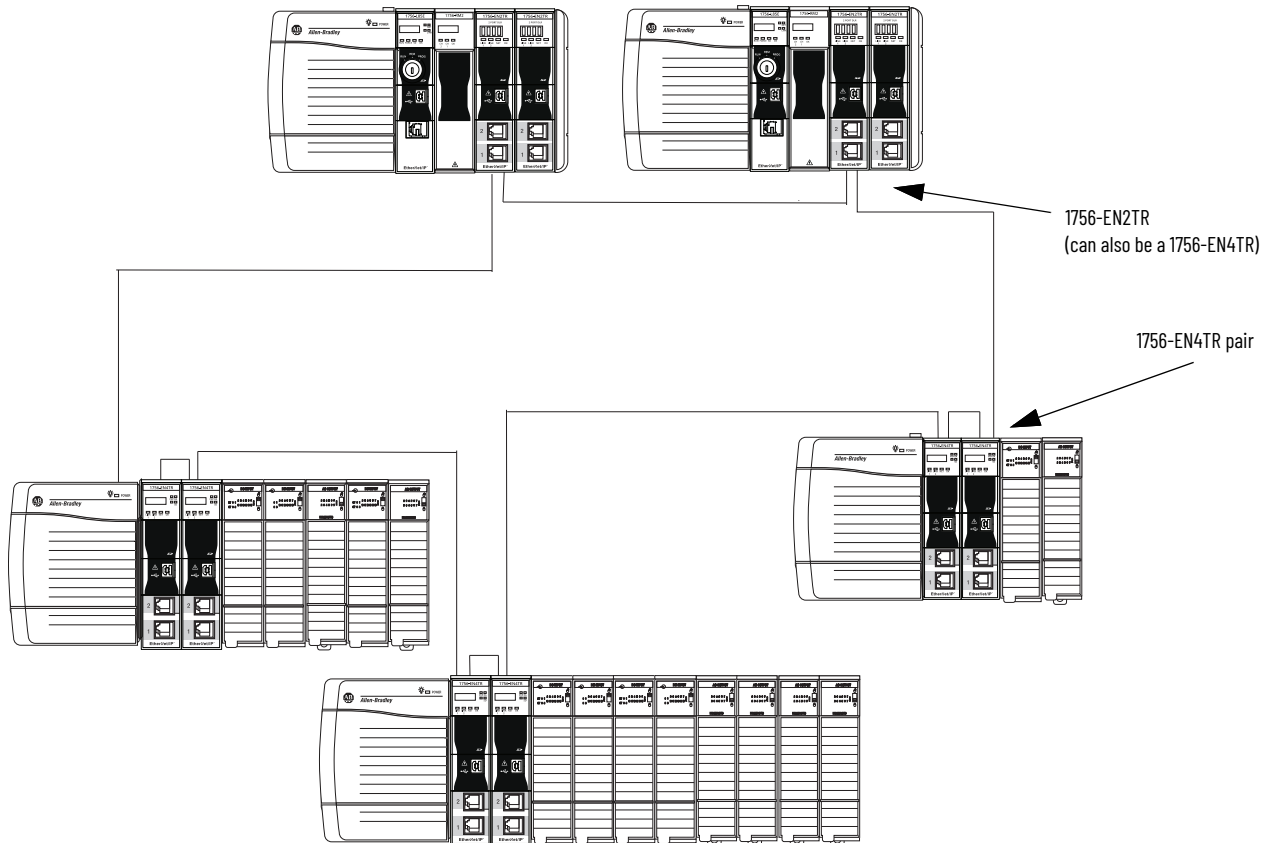
> Configure all DLR devices on the ring to be at the same speed on all links as defined in the Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture design and implementation guide, ENET-TD015.

Redundant adapters can be used in a star configuration, as shown in [Figure 3](). However, the switch at the center of the star is a single point of failure. DLR provides for higher resiliency.

Figure 3 - Redundant 1756-EN4TR Adapters in Star Topology with a Single Switch

1756-EN4TR or
1756-EN2T

1756-EN4TR pair
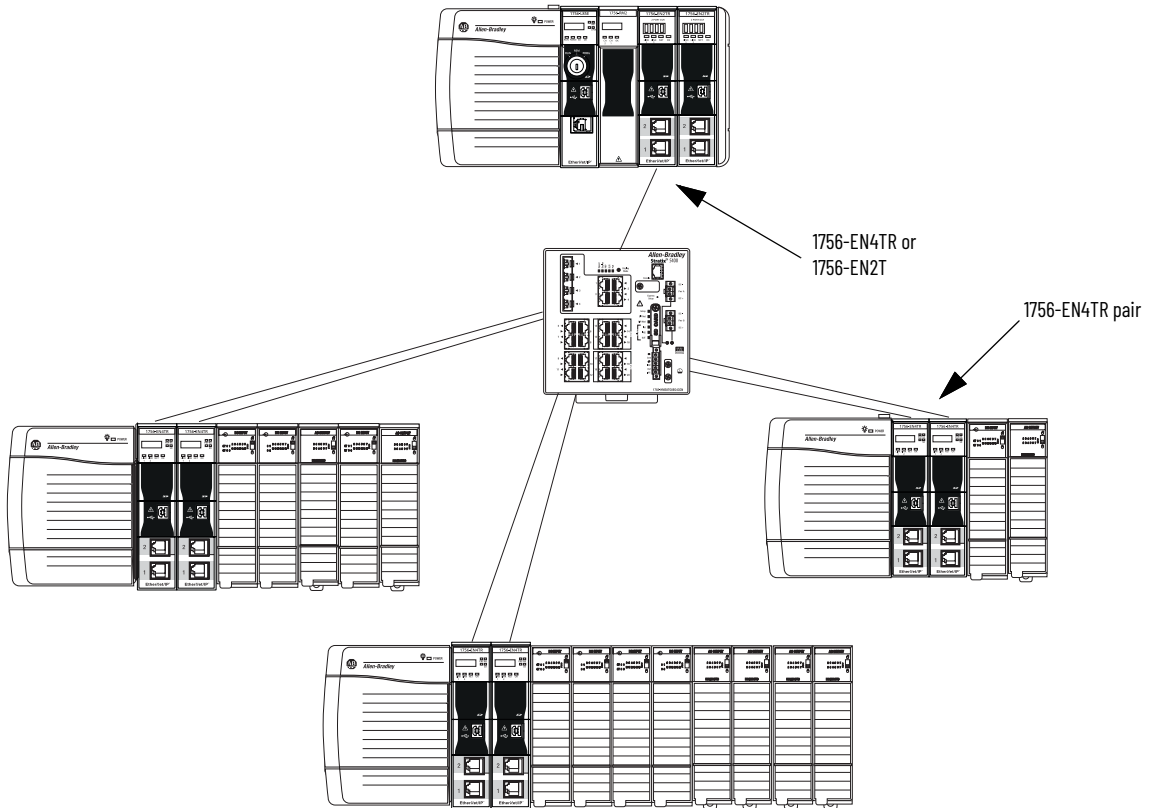
Redundant Architecture Network Considerations

In a star topology with a single switch, if a link is broken between the switch and the primary redundant adapter, a switchover occurs. With multiple switches, for example as shown in , if a link is broken between two switches, a switchover does not occur because the link to the redundant adapter is still in place.

Figure 4 - Invalid Topology: Network Break Does not Cause Switchover
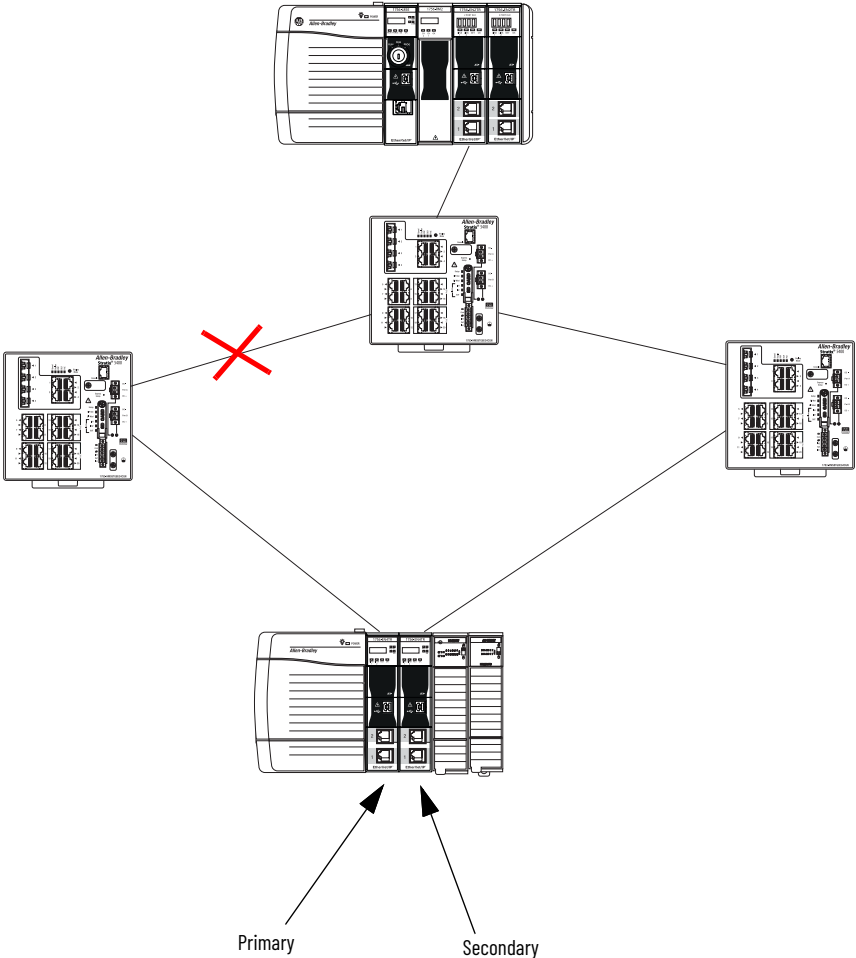
Primary   Secondary

The Primary Adapter does not detect data connection loss on non-directly connected links. For example in Figure 5, the secondary adapter disqualifies because it cannot detect the primary adapter.

This action occurs even though the secondary adapter still has a healthy path to the primary controller.

Similarly, the secondary controller in the redundant controller pair disqualifies because it cannot detect the primary.

Figure 5 - Invalid Topology: Network Break Results in Loss of Control

Secondary

Primary

Primary

Secondary
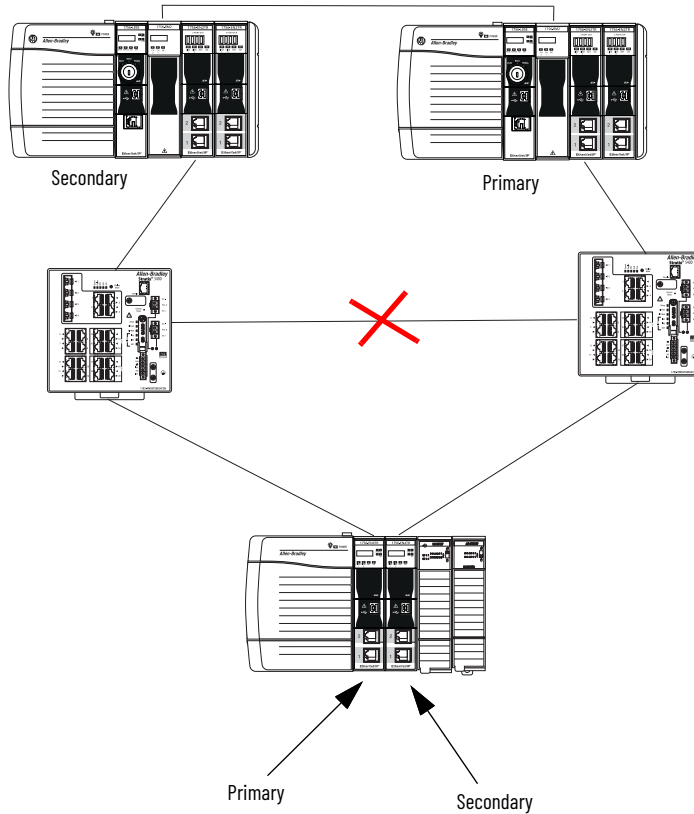
PRP Architecture with RedBox Switches

PRP, including RedBox switches, must be properly designed, built, and configured based on CPwE guidelines. For more information, see the Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture Technical Data.

With Logix Designer application version 33 and 1756-EN4TR firmware 3.001, you can use 1756-EN4TR redundant adapters in the I/O chassis with PRP as shown in Figure 6.

- The 1756-EN4TR firmware 3.001 does not natively support PRP, which is why the 1756-EN4TRs must be connected to RedBox switches.
- The 1756-EN4TR firmware 3.001 does not support the 1756-EN4TR being placed in the redundant chassis pair, so the 1756-EN2TP is the module being used to connect the redundant chassis pair to the PRP LAN A and LAN B.

Figure 6 – PRP Network with RedBox Switches and Redundant Adapters
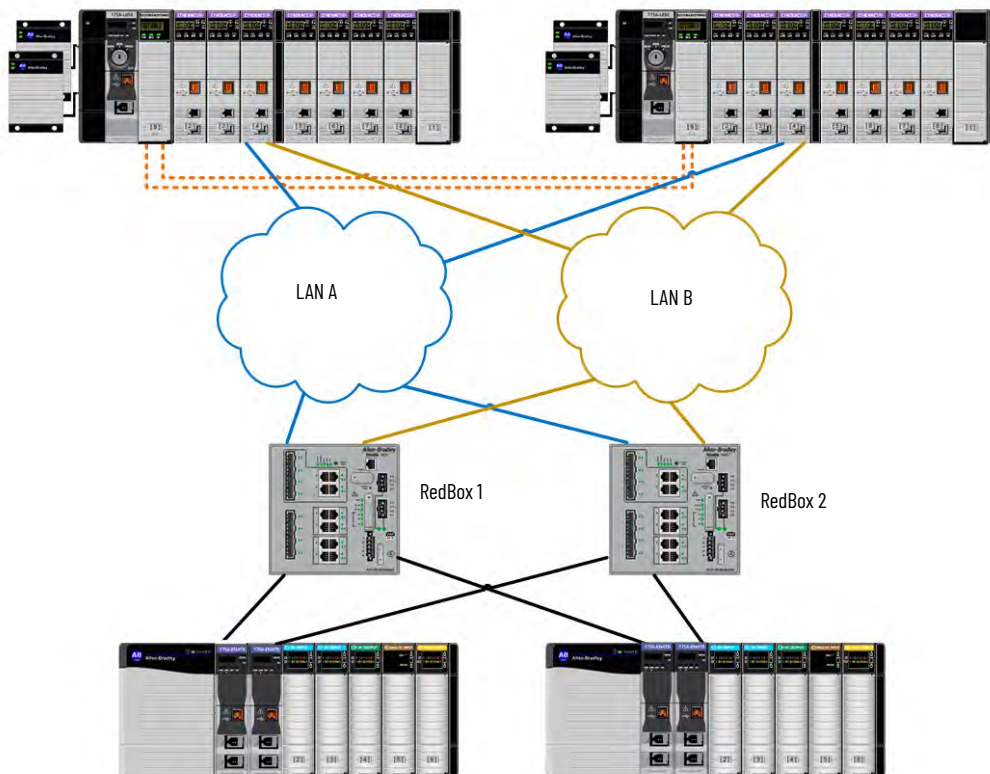
PRP Architecture without RedBox Switches

PRP must be properly designed, built, and configured based on CPwE guidelines. For more information, see the Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture Technical Data.

With Studio 5000 Logix Designer application version 34 and later, and 1756-EN4TR firmware 4.001 and later, the 1756-EN4TR can be used in the ControlLogix® 5580 redundant chassis pair.

- The 1756-EN4TR cannot be placed in a ControlLogix 5570 redundant chassis pair.
- Redundant 1756-EN4TR adapters can also be placed in the remote I/O chassis, as they could starting with firmware 3.001.
- RedBox switches are no longer needed because the 1756-EN4TR natively supports PRP with firmware 4.001 and later.

Follow these guidelines:

- Use EtherNet/IP modules that support the redundant adapter feature.
- Connect the redundant adapters in the I/O chassis to LAN A and LAN B.

Figure 7 - PRP Network with Redundant Adapters

1756-EN4TR Redundant Adapter Pair

1756-EN4TR as a single adapter
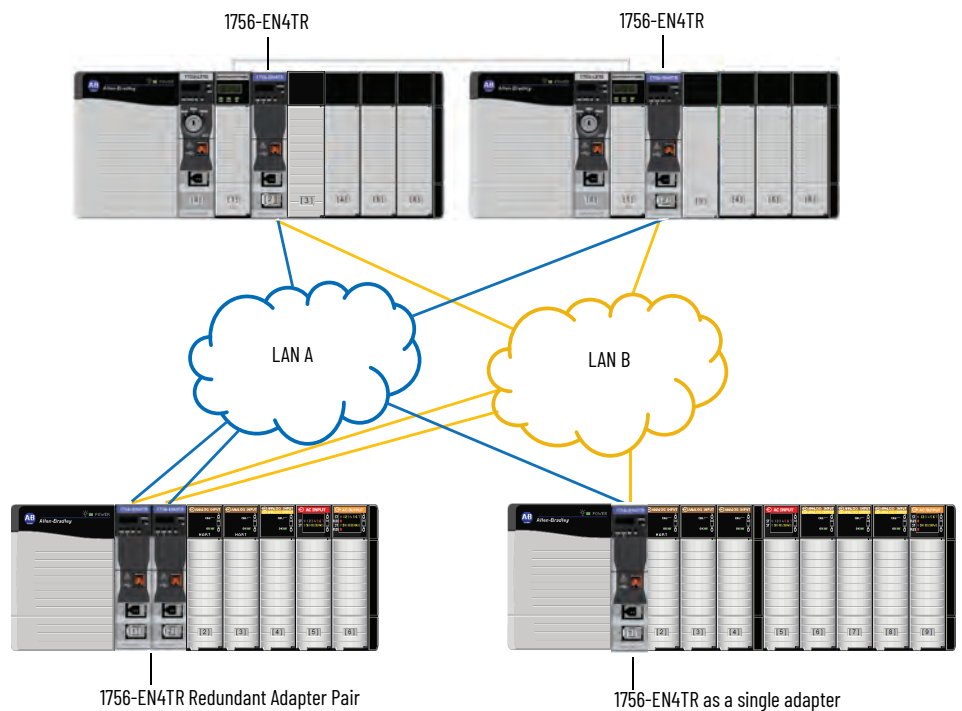
Security Options

Topic	Page
MSG Instruction	59
Disable/Enable an Ethernet Port	61
Disable the CIP Security Ports	64
Disable/Enable LLDP	66
Disable the USB Port	67
Disable/Enable the SD Card	68
Disable/Enable the 4-character Status Display	70
Disable/Enable the Webpages	72
Disable/Enable Simple Network Management Protocol (SNMP)	74
Disable the Socket Object	76
Disable the Email Object	76

For enhanced security, you can disable specific functionalities on an Ethernet communication module as desired.

MSG Instruction

You can use a CIP™ Generic MSG to disable many of the functionalities on a module. This CIP Generic MSG originates in the controller and is sent to the communication module receiving the change.

Configure the MSG Communication Path

While the Configuration tab on the Message Configuration dialog requires specific information to disable or enable a specific feature, the method for configuring the message communication path is the same for all features.

Communication goes through the backplane and Ethernet ports. When you configure the communication path, the values in the path specify backplane or Ethernet port:

- 1 - Backplane
- 2 - Ethernet port

Module In The Local Chassis

To disable or enable functionality in a module in the Local Chassis, the path is:
1, slot number of local module.

The path below is 1,1 denoting that the message originating in the controller is going to the backplane (the first 1) over to slot 1 (the second 1), which is the location of the local_EN2TR module that is receiving the change.
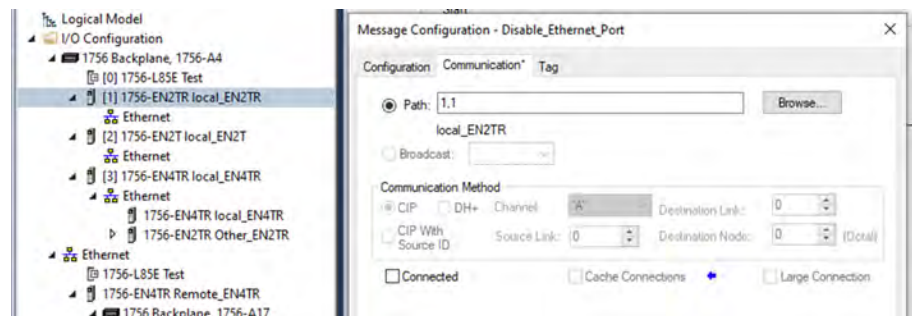
Remote Module Connected Through A Controller Ethernet Port

To disable or enable functionality in a module in a remote chassis that is connected through the front port of a controller, the path is:
2 (denoting out the Ethernet port), IP address of the remote module that is receiving the change.
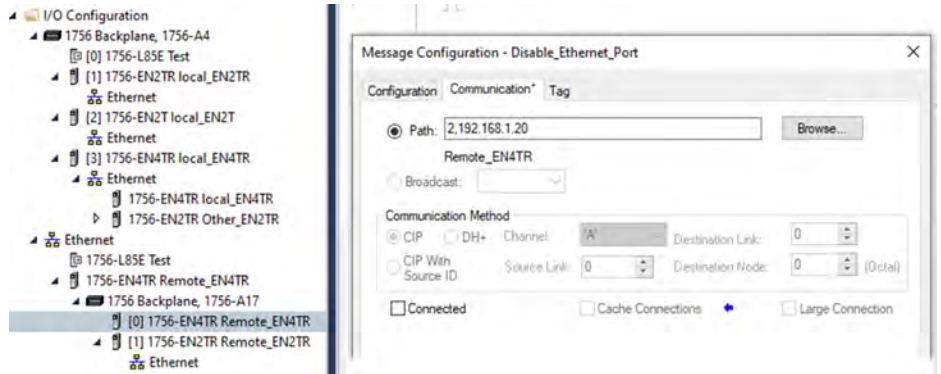
Remote Module Connected to Controller Through a Module in the Local Chassis

To disable or enable functionality in a module in a remote chassis that is connected through an Ethernet module in the local chassis, the path is:
1 (denoting from the controller to the backplane), slot number of local communication module, 2 (denoting out the Ethernet port of the communication module), IP address of remote module that is receiving the change.
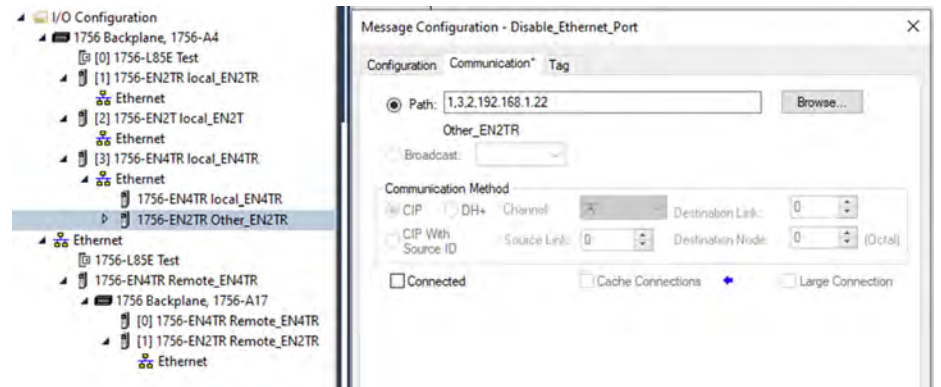
Disable/Enable an Ethernet Port

Applies to these modules:

1756-EN2x
1756-EN4x

You can disable or enable an Ethernet port three ways:

Ethernet ports return to the default setting after the module is reset to factory defaults. You must reconfigure the settings to disable an Ethernet port after the port returns to its default settings.

IMPORTANT	Remember the following: • Once a port is disabled, you lose any connection that is established through the controller Ethernet port. • You cannot disable Ethernet ports if the controller keyswitch is in Run mode or if the FactoryTalk® Security settings deny this editing option.

Disable/Enable an Ethernet Port with FactoryTalk Linx Network Browser

You can disable or enable an Ethernet port with FactoryTalk® Linx software, version 6.30.00 or later.

1. On the Factory Talk Linx Network Browser, select the Ethernet module, and click Configure Device.
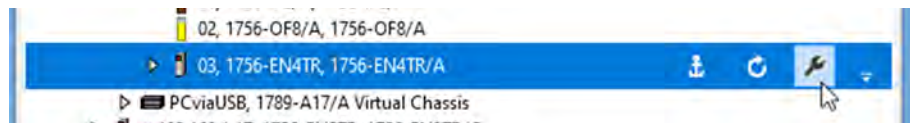
2. On the Port Configuration category:
- To disable an Ethernet port, clear the Enabled checkbox.
- To enable an Ethernet port, select the Enabled checkbox.
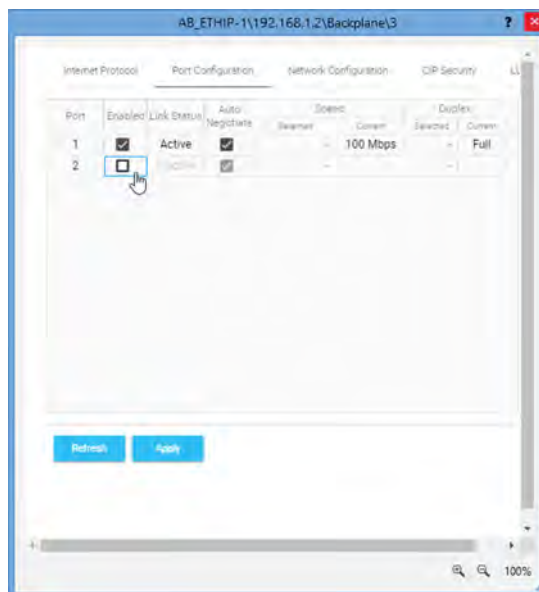
3. Click Apply.
4. Click Yes on the confirmation messages that appear. The change takes effect immediately.
5. Click Refresh.

Disable/Enable an Ethernet Port on the Port Configuration Tab

You can disable or enable an Ethernet port with the Studio 5000 Logix Designer® application, version 28.00.00 or later.

IMPORTANT	To disable an Ethernet port, the Link Status for one port must be Active.

This method retains the setting in the project every time you download the project to the controller.

1. Go online with the controller.
2. To open the module properties, double-click the Ethernet module.
3. On the Port Configuration category:
- To disable an Ethernet port, clear the Enable checkbox.
- To enable an Ethernet port, select the Enable checkbox.
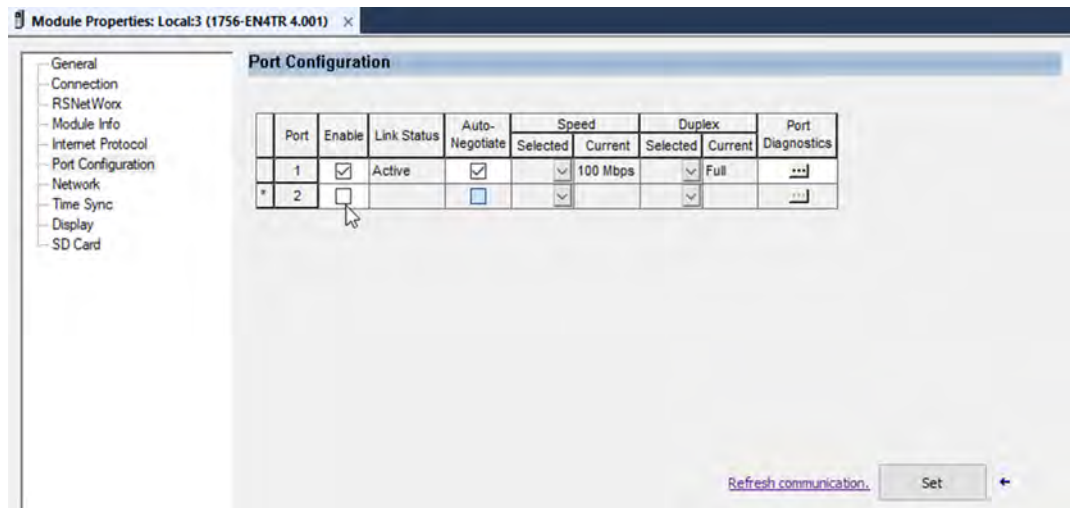
4. On the Port Configuration tab, click Set.
5. On the dialog box, click Yes. The change takes effect immediately.
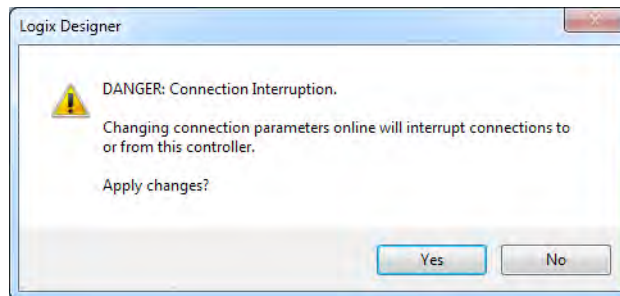
6. On the Port Configuration category, click OK.

Disable an Ethernet Port with a MSG Instruction

You can disable an Ethernet port with the Studio 5000 Logix Designer application, version 28.00.00 or later. You cannot use this MSG instruction to disable the Ethernet port on a different controller.

1. Add a MSG instruction to your program.

    This message only has to execute once, it does not need to execute with every program scan.

IMPORTANT	• These values are stored to NVS memory in such a way that the MSG instruction is not required to execute each time the controller powers up.
	• You cannot add a MSG instruction to your program if the controller keyswitch is in Run mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as follows:

Table 1 – Disable an Ethernet Port

Message Type:	CIP Generic
Service Type:	Set Attribute Single
Instance:	1 for single port modules 1 for Port 1, 2 for Port 2 on dual-port modules
Class:	f6
Attribute:	9
Source Element:	Controller tag of SINT data type. In this example, the controller tag is named Port_Configuration.
Source Length:	1
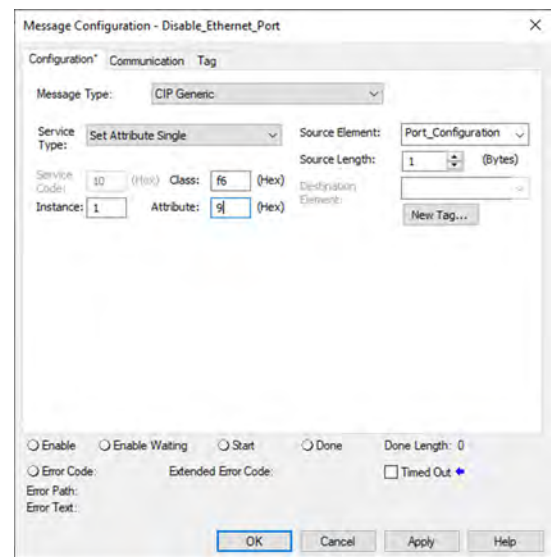
3. On the Communication tab, configure the Path. See .

4. Before you enable the MSG instruction, make sure that the Source Element tag value is 2.

    To re-enable the port, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure that the Source Element tag value is 1.

Disable the CIP Security Ports

Applies to these modules:

1756-EN4x

There are two ways to disable CIP Security™ ports:

- Use the Disable CIP Security checkbox in FactoryTalk Linx software, version 6.30.00 or later. See Disable the CIP Security Ports with FactoryTalk Linx Network Browser on page 64
- Disable the CIP Security Ports with a MSG Instruction on page 65

IMPORTANT	These procedures disable the CIP Security ports. To re-enable the ports, you must use the rotary switches to return the controller to a factory default state. See Reset the Module to Factory Default Value on page 43.

Disable the CIP Security Ports with FactoryTalk Linx Network Browser

You can disable the CIP Security ports with FactoryTalk Linx Network Browser, version 6.30.00 or later.

1. On the Factory Talk Linx Network Browser, select 1756-EN4TR, and click Configure Device.
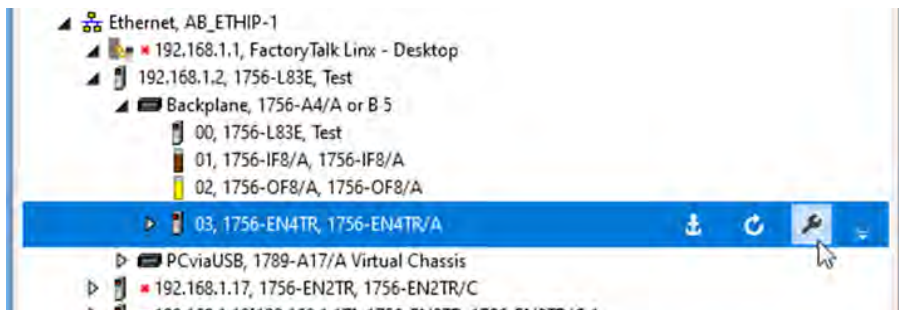
2. Click CIP Security.
3. Select the Disable CIP Security (Port 2221) checkbox.
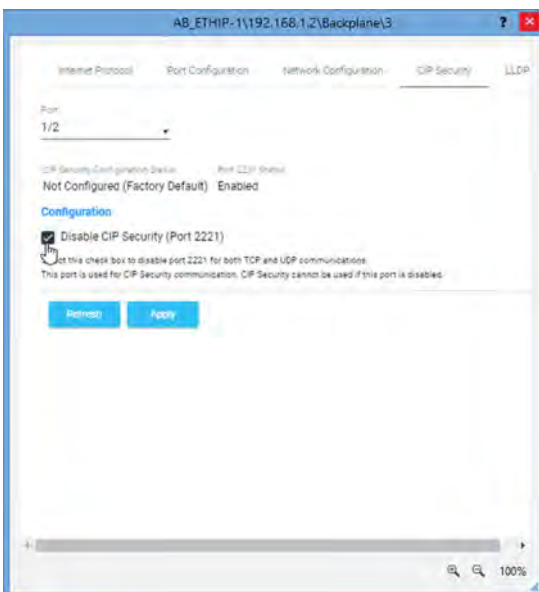
4. Click Apply.
5. Click Yes on the confirmation messages that appear.

Disable the CIP Security Ports with a MSG Instruction

With the Studio 5000 Logix Designer application, version 32.00.00 or later, use a CIP Generic MSG to execute this option. The message only has to execute once, it does not need to execute with every program scan.

1. Create a controller tag of SINT[9] data type.

   In this example, the controller tag is named CIPSEC_DISABLE and must match the following graphic.

Name		Value	Style	Data Type	D
▲ CIPSEC_DISABLE		{...}	Hex	SINT[9]	
▷ CIPSEC_DISABLE[0]		16#02	Hex	SINT	
▷ CIPSEC_DISABLE[1]		16#ad	Hex	SINT	
▷ CIPSEC_DISABLE[2]		16#08	Hex	SINT	
▷ CIPSEC_DISABLE[3]		16#11	Hex	SINT	
▷ CIPSEC_DISABLE[4]		16#00	Hex	SINT	
▷ CIPSEC_DISABLE[5]		16#ad	Hex	SINT	
▷ CIPSEC_DISABLE[6]		16#08	Hex	SINT	
▷ CIPSEC_DISABLE[7]		16#06	Hex	SINT	
▷ CIPSEC_DISABLE[8]		16#00	Hex	SINT	

Before you enable the MSG instruction, consider the following:

- The element CIPSEC_DISABLE[4] is responsible for disabling UDP port 2221 and EtherNet/IP™ over DTLS, transport class 0/1.
- The element CIPSEC_DISABLE[8] is responsible for disabling TCP port 2221 and EtherNet/IP over TLS, UCMM, and transport class 3.
- To disable the controller CIP Security™ ports, the elements CIPSEC_DISABLE[4] and CIPSEC_DISABLE[8] in the SINT array for the Source Element CIPSEC_DISABLE must be 0.

2. Add a MSG instruction to your program.

> **IMPORTANT** You cannot add a MSG instruction to your program if the controller keyswitch is in RUN mode, or if the FactoryTalk Security settings deny this editing option.

3. Configure the Configuration tab on the Message Configuration dialog box as follows:

Table 2 - Disable the CIP Security Ports

Message Type:	CIP Generic
Service Type:	Custom
Service Code:	4c
Instance:	1
Class:	f5
Attribute:	0
Source Element:	Controller tag of SINT[9] data type. This is the controller tag that you created in step 1.
Source Length:	9
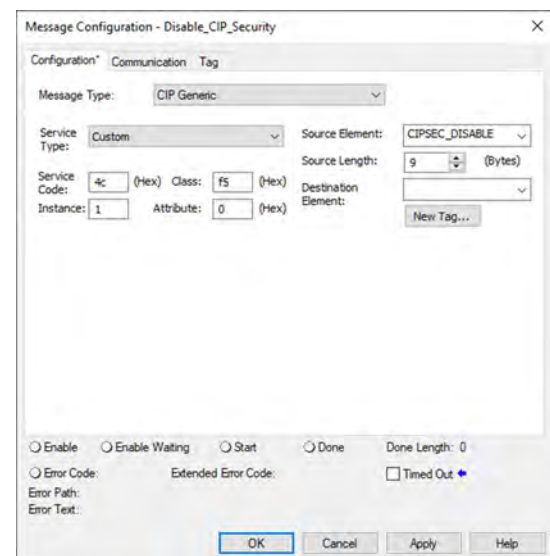
4. On the Communication tab, configure the Path. See [Configure the MSG Communication Path on page 59](#).
5. Cycle power on the controller for the configuration to take effect.

Disable/Enable LLDP

Applies to these modules:

1756-EN2x
1756-EN4x

Link Layer Discovery Protocol (LLDP) is used by network devices to advertise their identity, capabilities, and neighbors on a local area network.

You can disable or enable LLDP with FactoryTalk Linx Network Browser, version 6.30.00 or later.

1. On the Factory Talk Linx Network Browser, select the module, and click Configure Device.
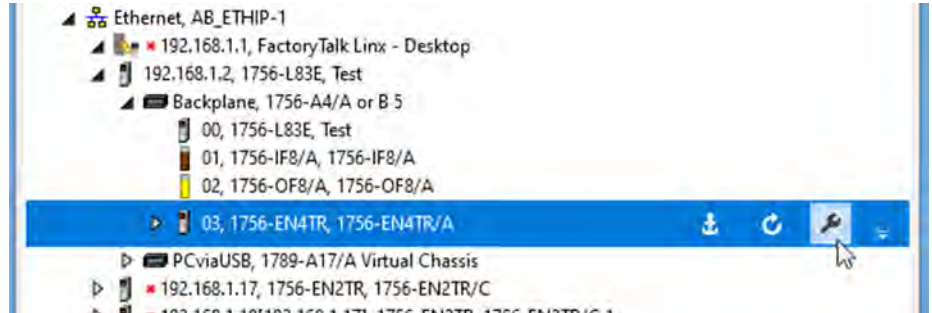
2. On the LLDP category:
- To disable LLDP, clear the Enabled checkbox.
- To enable LLDP, select the Enabled checkbox..
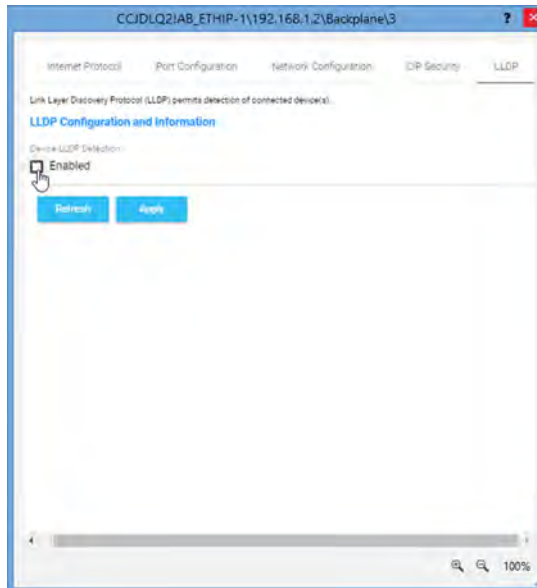
3. Click Apply.
4. Click Yes on the confirmation messages that appear.

Disable the USB Port

Applies to these modules:

1756-EN2x
1756-EN4x

With the Studio 5000 Logix Designer application, version 32.00.00 or later, use a CIP Generic MSG to execute this option.

1. Add a MSG instruction to your program.

   This message only has to execute once, it does not need to execute with every program scan.

IMPORTANT	• These values are stored to NVS memory in such a way that the MSG instruction is not required to execute each time the controller powers up. • You cannot add a MSG instruction to your program if the controller keyswitch is in Run mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as follows:

Table 3 - Disable the USB Port

Message Type:	CIP Generic
Service Type:	Set Attribute Single
Instance:	1
Class:	33a
Attribute:	4
Source Element:	Controller tag of SINT data type. In this example, the Source Element is named Port_Configuration.
Source Length:	1
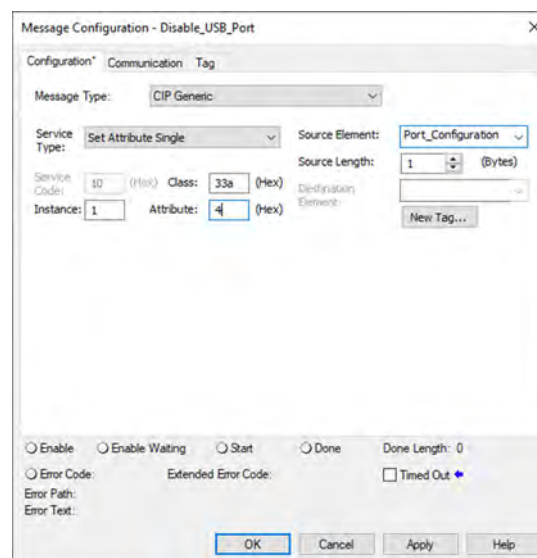
3. On the Communication tab, configure the Path. See .

Disable/Enable the SD Card

Applies to these modules:

1756-EN4x

You can disable or enable the SD card two ways:

- Disable/Enable the SD Card on the Module Properties Dialog on page 68
- Disable/Enable the SD Card with a MSG Instruction on page 69

IMPORTANT	Remember the following:
	- Once an SD Slot is disabled, you lose all and any ability to communicate to an SD Card inserted into the slot. This includes any diagnostic information.
	- To re-enable the SD card again:
	- Use the rotary switches to rest the module to factory defaults.
	- Use a MSG instruction.

Disable/Enable the SD Card on the Module Properties Dialog

This method retains the setting in the project every time you download the project to the controller.

On the SD Card category in the module properties dialog:

- To disable the SD card, clear the Enable SD Card checkbox and click Set.
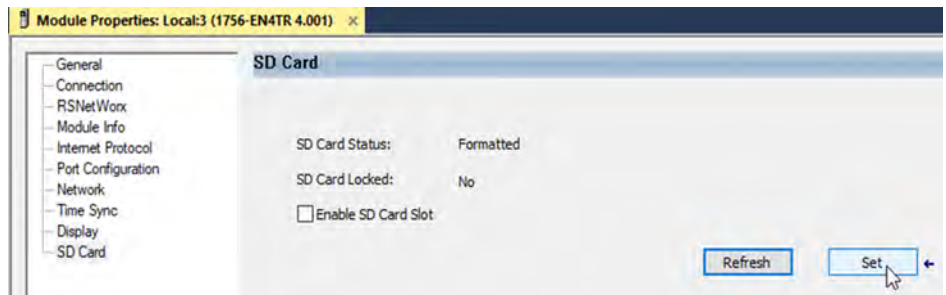
- To enable the SD card, select the Enable SD Card checkbox and click Set.

Disable/Enable the SD Card with a MSG Instruction

1. Add a MSG instruction to your program.

   This message only has to execute once, it does not need to execute with every program scan.

IMPORTANT
- These values are stored to NVS memory in such a way that the MSG instruction is not required to execute each time the controller powers up.
- You cannot add a MSG instruction to your program if the controller keyswitch is in Run mode, or if the FactoryTalk Security settings deny this editing option.

---

2. Configure the Configuration tab on the Message Configuration dialog box as follows:

   - To Enable: set source tag value to 0
   - To Disable: set source tag value to 1

Table 4 – Disable/Enable the SD Card

Message Type:	CIP Generic
Service Type:	Set Attribute Single
Instance:	1
Class:	3a4
Attribute:	4
Source Element:	Controller tag of SINT Array. In this example, the Source Element is named src_array.
Source Length:	1
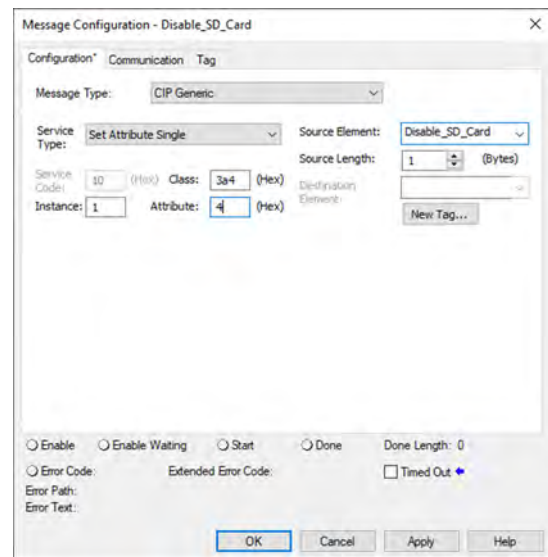
3. On the Communication tab, configure the Path. See [Configure the MSG Communication Path on page 59](#).

Disable/Enable the 4-character Status Display
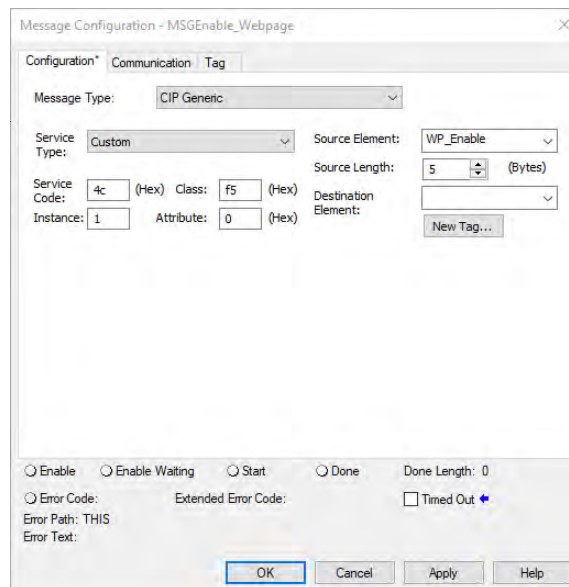
Applies to these modules:

1756-EN4x

With the Studio 5000 Logix Designer application, version 29.00.00 or later, you can disable or enable certain categories of messages on the 4-character status display:

- Disable/Enable All Categories of Messages on page 70
- Disable/Enable Individual Categories of Messages on page 71

You use a CIP Generic MSG to execute each option.

IMPORTANT	You cannot disable these system messages, and they always display:
	• Power-up messages (such as TEST, PASS, CHRG)
	• Catalog number message
	• Firmware revision message
	• Major / Critical failure messages

The 4-character status display returns to the default setting after the module is reset to factory defaults. You must reconfigure the settings to disable the 4-character status display after it returns to its default settings.

Disable/Enable All Categories of Messages

When you disable all categories of messages, this information no longer shows:

- Link status
- Port status
- IP address

Complete these steps.

1. Add a MSG instruction to your program.

IMPORTANT	You cannot add a MSG instruction to your program if the controller keyswitch is in Run mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box:

Table 5 - Disable/Enable All Categories of Messages

Message Type:	CIP Generic
Service Type:	Set Attribute Single
Instance:	1
Class:	3a5
Attribute:	1
Source Element:	Controller tag of SINT data type. In this example, the controller tag is named Display_SINT.
Source Length:	1
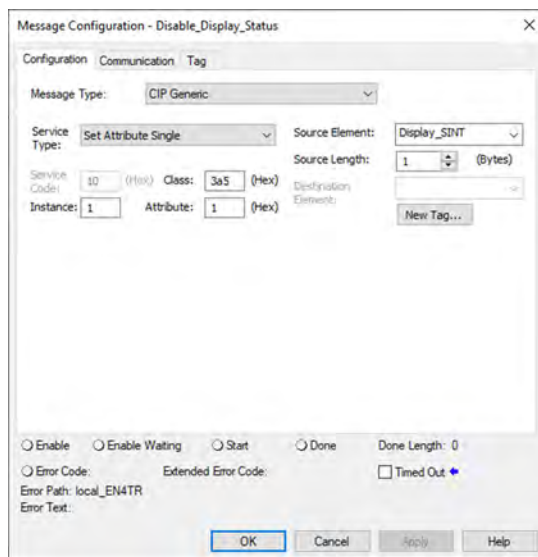
3. On the Communication tab, configure the Path. See Configure the MSG Communication Path on page 59.
4. Before you enable the MSG instruction, make sure that the Source Element tag value is 1.

IMPORTANT	You can re-enable the 4-character display after it is disabled.
	To re-enable the 4-character display, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure that the Source Element tag value is 0.

Disable/Enable Individual Categories of Messages

You can disable a subset of the information that scrolls across the 4-character display. You can disable these subsets:

- Link status
- Port status and IP address

Complete these steps.

1. Add a MSG instruction to your program.

   This message only has to execute once, it does not need to execute with every program scan.
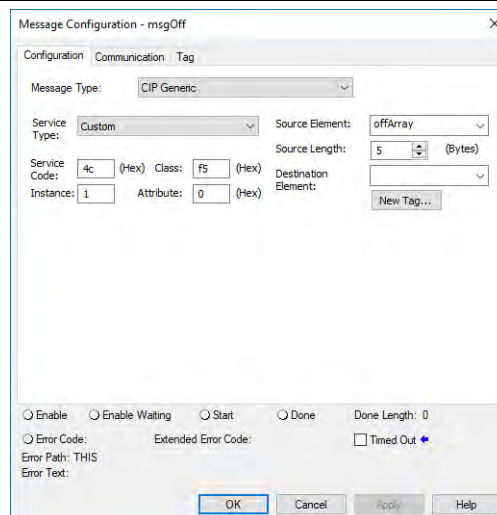
IMPORTANT	You cannot add a MSG instruction to your program if the controller keyswitch is in Run mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as follows:

Table 6 - Disable/Enable Individual Categories of Messages

Message Type:	CIP Generic
Service Type:	Set Attribute Single
Instance:	1
Class:	3a5
Attribute:	2
Source Element:	Controller tag of DINT data type. In this example, the controller tag is named Line_MASK.
Source Length:	4
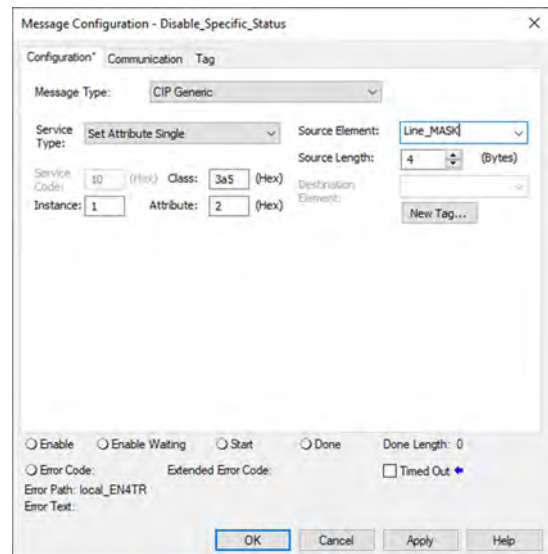
3. On the Communication tab, configure the Path. See Configure the MSG Communication Path on page 59.

4. Before you enable the MSG instruction, make sure that the Source Element uses one of the following tag values that are based on what information that you want to disable:
   - Link status - Bit 0 of the Source Element = 1
   - Port status and IP address - Bit 1 of the Source Element = 1

IMPORTANT	You can re-enable the subsets of information on the 4-character display after they are disabled.
	To re-enable the subsets, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure the appropriate bit in the Source Element tag value is 0.

Disable/Enable the Webpages

Applies to these modules:

1756-EN2x
1756-EN4x

You can disable or enable the module webpages.

Use a CIP Generic MSG to Disable the Webpages

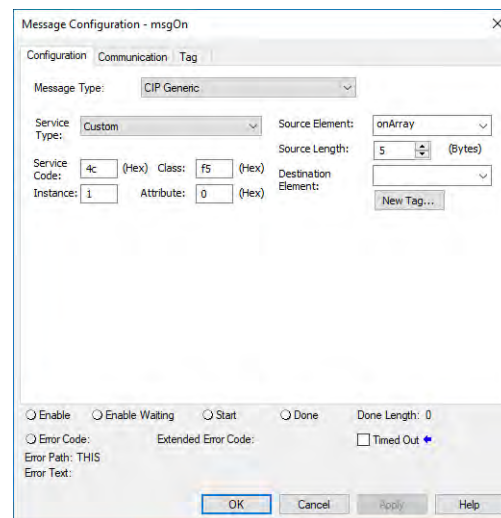| **IMPORTANT**	If you use FactoryTalk Policy Manager to disable the webpages in a CIP Security application, the CIP generic message-to-self overrides the FactoryTalk Policy Manager setting.

1. Add a MSG instruction to your program.

IMPORTANT	You cannot add a MSG instruction to your program if the controller keyswitch is in RUN mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as follows:

Table 7 - Disable the Webpages

Message Type:	CIP Generic
Service Type:	Custom
Service Code:	4c
Instance:	1
Class:	f5
Attribute:	0
Source Element:	Controller tag of SINT[5] data type. In this example, the controller tag is named WP_Disable and must match the following graphic: ![WP_Disable table showing WP_Disable {...} Decimal SINT[5]; WP_Disable[0] 1 Decimal SINT; WP_Disable[1] 80 Decimal SINT; WP_Disable[2] 0 Decimal SINT; WP_Disable[3] 6 Decimal SINT; WP_Disable[4] 0 Decimal SINT] **IMPORTANT:** The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, the controller webpages are not disabled.
Source Length:	5

3. On the Communication tab, configure the Path. See <u>Configure the MSG Communication Path on page 59</u>.

Use a CIP Generic MSG to Enable the Webpages

1. Add a MSG instruction to your program.

> **IMPORTANT**   You cannot add a MSG instruction to your program if the controller keyswitch is in RUN mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as follows:

Table 8 - Enable the Webpages

Message Type:	CIP Generic
Service Type:	Custom
Service Code:	4c
Instance:	1
Class:	f5
Attribute:	0
Source Element:	Controller tag of SINT[5] data type. In this example, the controller tag is named WP_Enable and must match the following graphic: **IMPORTANT:** The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, the controller webpages are not enabled.
Source Length:	5

3. On the Communication tab, configure the Path. See Configure the MSG Communication Path on page 59.

Disable/Enable Simple Network Management Protocol (SNMP)

Applies to these modules:

1756-EN2x
1756-EN4x

SNMP enables the module to be remotely managed through other network management software. SNMP defines the method of communication among the devices and also denotes a manager for the monitoring and supervision of the devices.

- For 1756-EN2x modules: With firmware revision 12.001 or later, SNMP is disabled on the Ethernet module by default.
- For 1756-EN4x modules: SNMP is disabled on the Ethernet module by default will all firmware revisions

For more information about SNMP, see the Ethernet Reference Manual, publication ENET-RM002.

Use a CIP Generic MSG to Disable SNMP

1. Add a MSG instruction to your program.

IMPORTANT	You cannot add a MSG instruction to your program if the controller keyswitch is in RUN mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as follows:

Table 9 – Disable SNMP

Message Type:	CIP Generic
Service Type:	Custom
Service Code:	4c
Instance:	1
Class:	f5
Attribute:	0
Source Element:	Controller tag of USINT[5] data type. In this example, the controller tag is named offArray and must match this graphic: IMPORTANT: The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, SNMP will not be disabled.
Source Length:	5

3. On the Communication tab, configure the Path. See .

Use a CIP Generic MSG to Enable SNMP

1. Add a MSG instruction to your program.

IMPORTANT   You cannot add a MSG instruction to your program if the controller keyswitch is in RUN mode, or if the FactoryTalk Security settings deny this editing option.

---

2. Configure the Configuration tab on the Message Configuration dialog box as follows:

Table 10 – Enable SNMP

Message Type:	CIP Generic
Service Type:	Custom
Service Code:	4c
Instance:	1
Class:	f5
Attribute:	0
Source Element:	Controller tag of USINT[5] data type. In this example, the controller tag is named onArray and must match this graphic: **IMPORTANT:** The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, SNMP will not be enabled.
Source Length:	5

3. On the Communication tab, configure the Path. See .

There are two additional tables to store the result of the IANA port administrator state change operation.

Figure 8 – onArrayOut

Disable the Socket Object

Applies to these modules:

1756-EN2x
1756-EN4x

The module can use socket interfaces to communicate with Ethernet devices that do not support the EtherNet/IP application protocol. The socket interface is implemented via the Socket Object. The socket object is enabled by default. You can use a CIP Generic MSG instruction to disable the socket object.

For more information on the socket interface, see EtherNet/IP Socket Interface Application Technique, publication ENET-AT002.

Disable the Email Object

Applies to these modules:

1756-EN2x
1756-EN4x

A Logix controller can send a generic CIP™ message instruction to the EtherNet/IP communication module that instructs the module to send an email message to an SMTP mail relay server that uses the standard SMTP protocol. This process automatically communicates controller data and application conditions to appropriate personnel.

The controller communicates with the Email Object via MSG instructions.

For more information on the Email Object, see EtherNet/IP Network Devices User Manual, publication ENET-UM006.

ControlLogix Network Device Status Indicators

Topic	Page
Status Indicators	77
Diagnostic Web Pages	82
Access the Diagnostic Web Pages	82

Status Indicators

The following graphics show the status indicators for these modules (extended-temperature versions not shown).

Figure 9 - 1756-EN2F, 1756-EN2T (Single-port Modules)
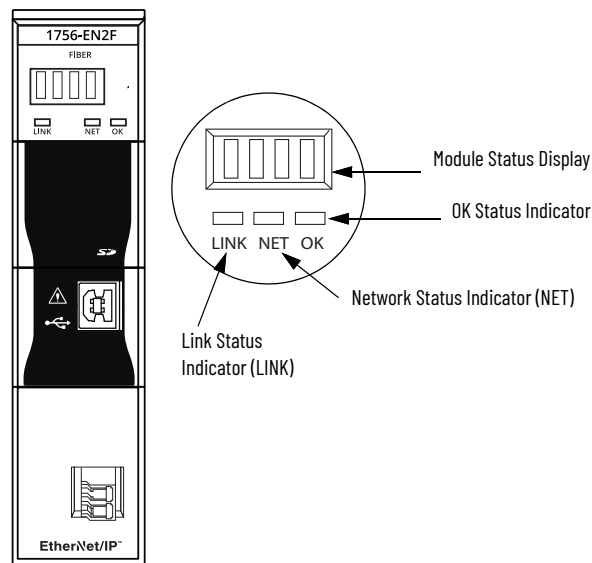
Figure 10 - 1756-EN2TR, 1756-EN3TR (Dual-port Modules)
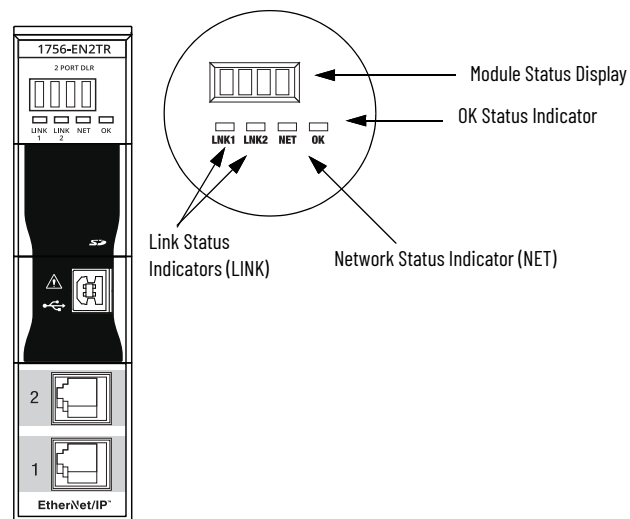
Figure 11 - 1756-EN2TP (Dual-port Module)

- Module Status Display
- OK Status Indicator
- Network Status Indicator (NET)
- Link Status Indicators (LINK)
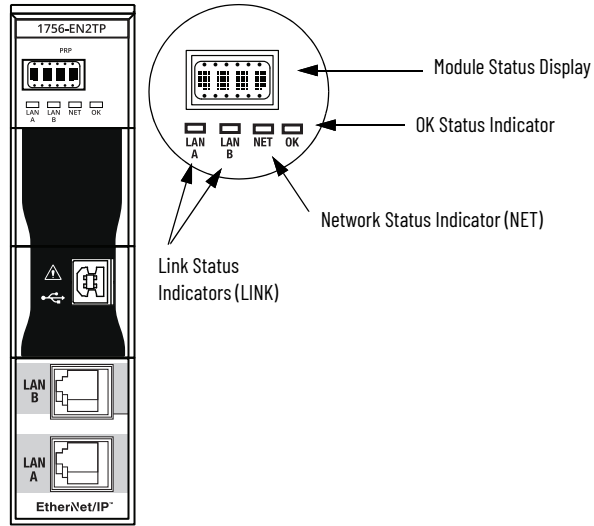
Figure 12 - 1756-EN4TR (Dual-port Module)[1]

- Module Status Display
- Parallel Redundant Protocol Status Indicator
- Redundant Adapter Status Indicator
- SD Card Status Indicator
- OK Status Indicator
- Network Status Indicator (NET)
- Link Status Indicators (LINK)
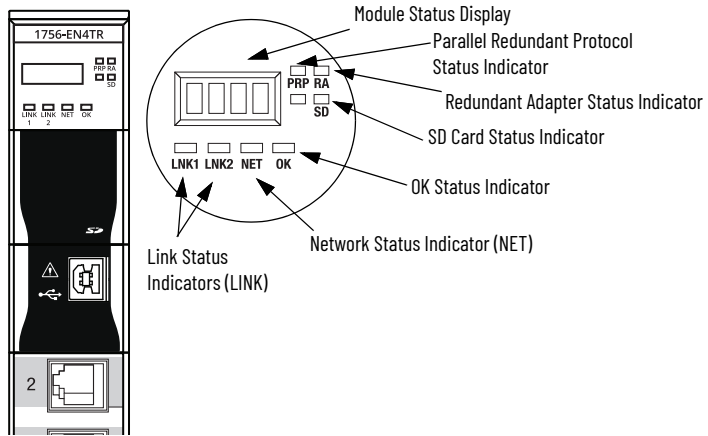
Figure 13 - 1756-ENBT (Single-port Module)

- Module Status Display
- OK Status Indicator
- Network Status Indicator (NET)
- Link Status Indicator (LINK)
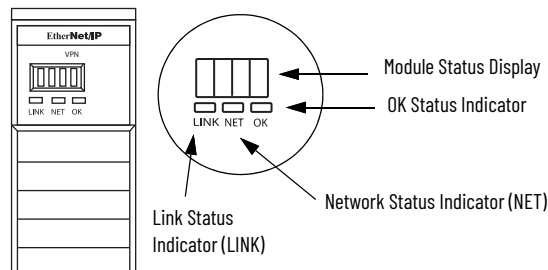
Figure 14 - 1756-EWEB (Single-port Module)

- Module Status Display
- OK Status Indicator
- Network Status Indicator (NET)
- Link Status Indicator (LINK)

---
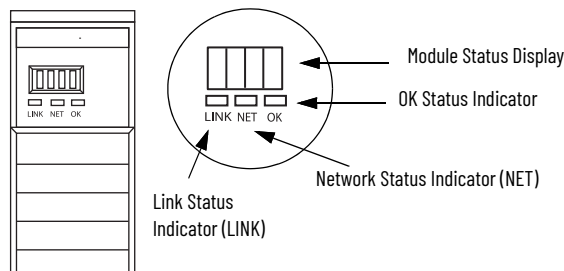
(1)   Parallel Redundant Protocol and Redundant Adapter features are not available in the initial release. Check the Product Compatibility and Download Center (PCDC) to see if it is available in your firmware revision.

Single-Port Module Status Indicators

Table 11 - Single-port Module Status Indicators

Status Indicator	Description	Status	State
Module Status Display	Alphanumeric display that scrolls messages. For example, when a module is operating normally, the display scrolls the module's IP address.	–	–

Link Status (LINK)	Indicates the current state of the module regarding transmission of data on the EtherNet/IP™ network.	Off	One of these conditions exists:
			• The module is not powered.
			  – Verify that there is chassis power.
			  – Verify that the module is completely inserted into the chassis and backplane.
			  – Make sure that the module has been configured.
			• No link exists on the port.

		Flashing green	Activity exists on the port.
		Green	The port is active, but not receiving traffic.
OK Status (OK)	Indicates the current state of the module. For example, this status indicator indicates if the module is executing power-up testing, in the process of a firmware update or operating normally.	Off	The module is not powered. • Verify that there is chassis power. • Verify that the module is completely inserted into the chassis and backplane. • Make sure that the module has been configured.
		Flashing green	The module is not configured. The Module Status display scrolls: BOOTP or DHCP<Mac_address_of_module> For example: BOOTP 00:0b:db:14:55:35 Configure the module.
		Green	The module is operating correctly. The IP address scrolls across the Module Status display.
		Flashing red	The module detected a recoverable minor fault. Check the module configuration. If necessary, reconfigure the module.
		Red	The module detected an unrecoverable major fault. Cycle power to the module. If this power cycle does not clear the fault, replace the module.

Network Status (NET)	Indicates if CIP™ connections are established.	Off	One of these conditions exists:
			• The module is not powered.
			  – Verify that there is chassis power.
			  – Verify that the module is completely inserted into the chassis and backplane.
			  – Make sure that the module has been configured.
			• The module is powered but does not have an IP address. Assign an IP address to the module.

		Flashing green	The controller has an IP address and one of these conditions exists: • The module has not established any CIP connections. If connections are configured for this module, check the connection originator for the connection error code. • All connections to the device have timed out or been closed.
Network Status (NET)	Indicates if CIP connections are established.	Green	The module has established at least 1 CIP connection and is operating properly. The IP address scrolls across the Module Status display.
		Red	The module is in conflict mode. It shares an IP address with another device on the network. The current IP address scrolls across the Module Status display. The display scrolls: OK <IP_address_of_this_module> Duplicate IP <Mac_address_of_duplicate_node_detected> For example: OK 10.88.60.196 Duplicate IP - 00:00:BC:02:34:B4 Change the IP address of the module.
		Flashing green/flashing red	The module is performing its power-up testing.

Dual-Port Module Status Indicators

Table 12 - Dual-port Module Status Indicators

Status Indicator	Description	Status	State
Module Status Display	Alphanumeric display that scrolls messages. For example, when a module is operating normally, the display scrolls the module's IP address.	—	—
OK	Indicates the current state of the module. For example, this status indicator indicates if the module is executing power-up testing, in the process of a firmware update or operating normally.	Off	The module is not powered. • Verify that there is chassis power. • Verify that the module is completely inserted into the chassis and backplane. • Make sure that the module has been configured.
		Flashing green	The module is not configured. The Module Status display scrolls: BOOTP or DHCP<Mac_address_of_module> For example: BOOTP 00:0b:db:14:55:35 Configure the module.
		Green	The module is operating correctly. The Module Status display scrolls: OK <IP_address_of_this_module> For example: OK 10.88.60.160
		Flashing red	The module detected a recoverable minor fault. Check the module configuration. If necessary, reconfigure the module.
		Red	The module detected an unrecoverable major fault. Cycle power to the module. If this power cycle does not clear the fault, replace the module.
		Both of these conditions exist: • Status Indicator is Red • Module Status Display is scrolling: Image Update Needed	The module's main firmware image must be updated. Follow these steps: 1. Update the firmware image. 2. Cycle power to the module.
		Flashing red and green	The module is performing its power-up testing.

Network Status (NET)	Indicates if CIP connections are established.
	IMPORTANT: The new-series 1756-EN2TR and 1756-EN3TR modules have a NET status indicator. The older-series 1756-EN2TR and 1756-EN3TR modules do not have a NET status indicator.
		Off	One of these conditions exists:
			• The module is not powered.
			  – Verify that there is chassis power.
			  – Verify that the module is completely inserted into the chassis and backplane.
			  – Make sure that the module has been configured.
			• The module is powered but does not have an IP address. Assign an IP address to the module.

		Flashing green	The controller has an IP address and one of these conditions exists: • The module has not established any CIP connections. If connections are configured for this module, check the connection originator for the connection error code. • All connections to the device have timed out or been closed.
		Green	The module has established at least 1 CIP connection and is operating properly. The IP address scrolls across the Module Status display.
		Red	The module is in conflict mode. It shares an IP address with another device on the network. The module's current IP address scrolls across the Module Status display. The display scrolls: OK <IP_address_of_this_module> Duplicate IP <Mac_address_of_duplicate_node_detected> For example: OK 10.88.60.196 Duplicate IP - 00:00:BC:02:34:B4 Change the module's IP address.
		Flashing green/flashing red	The module is performing its power-up testing.

Table 12 - Dual-port Module Status Indicators (Continued)

Status Indicator	Description	Status	State

Link Status (LINK 1, LINK 2)		Off	One of these conditions exists:
			• The module is not powered.
			  – Verify that there is chassis power.
			  – Verify that the module is completely inserted into the chassis and backplane.
			  – Make sure that the module has been configured.
			• No link exists on the port.
			• The port is administratively disabled.
			• The port is disabled due to rapid ring faults (LNK2).

		Flashing green	Activity exists on the port.
		Green	One of these conditions exists: • A link exists on the port, but no traffic is being received. • The ring network is operating normally on active ring supervisor (LNK2). • A ring partial network fault was detected on the active ring supervisor (LNK2).
Link Status (LAN A, LAN B)		Flashing red	When the corresponding LAN A/B Parallel Redundancy Protocol (PRP) Warning bit is set.
SD[1]	The SD indicator shows if the SD card is in use	Off	No activity is occurring with the SD card. You can safely remove the card, if necessary.
		Flashing green	The module is reading from or writing to the SD card.
		Solid green	**IMPORTANT**: Do not remove the SD card while the module is reading or writing. Let the read/write complete without interruption. If you interrupt the read/write, data corruption or loss can occur.
		Flashing red	One of the following exists: • The SD card does not have a valid file system. • The SD card drew excessive current and power has been removed from the card.
		Solid red	The module does not recognize the SD card.
Parallel Redundancy Protocol (PRP)[1]	Check Firmware Revision for availability of this feature.		
Redundant Adapter (RA)[1]	Major revision 3.001 or higher.		

(1)   Status indicators only available on the 1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT.

Diagnostic Web Pages

The number and type of diagnostic fields vary by module catalog number, series, and revision number.

IMPORTANT	The diagnostic web pages have many fields that you can use to monitor the operating state of your EtherNet/IP module.
	To troubleshoot problems, you diagnose as a result of monitoring the diagnostic web pages of the EtherNet/IP modules, see Troubleshoot EtherNet/IP Networks, publication ENET-AT003.

Access the Diagnostic Web Pages

To troubleshoot most possible problems with your EtherNet/IP communication module, you must access the diagnostic web pages for the module.

To access the EtherNet/IP communication module diagnostic web pages, follow these steps.

1. Open your web browser.
2. In the Address field, type your EtherNet/IP communication module Internet Protocol (IP) address and press Enter.

    The diagnostic web home page appears.
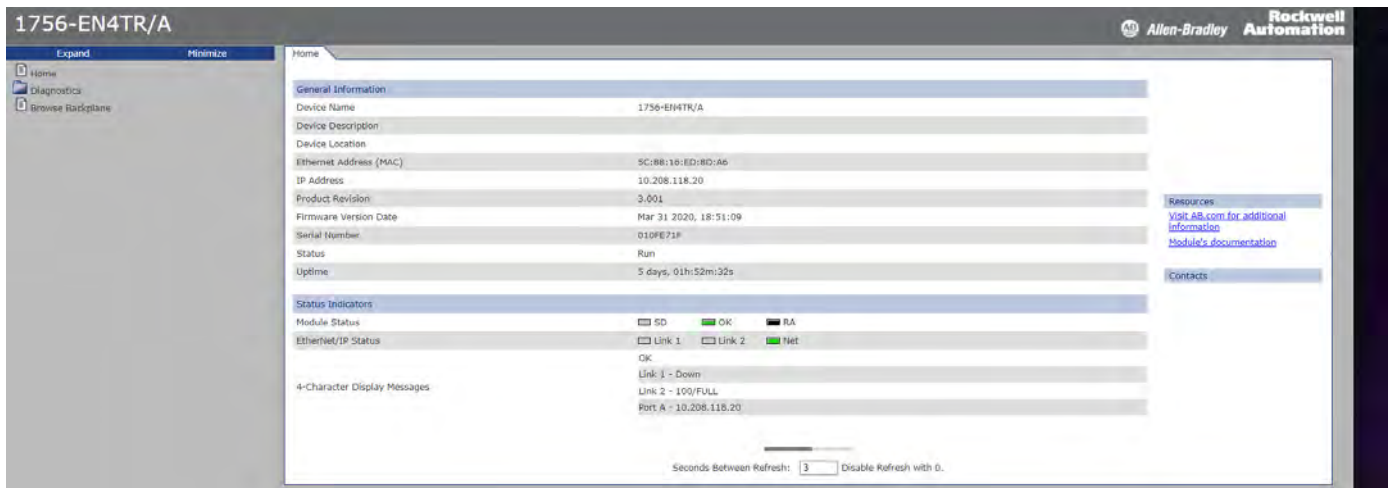
3. Open the Diagnostics folder in the left-most navigation bar and click the link for each diagnostic web page you must monitor.
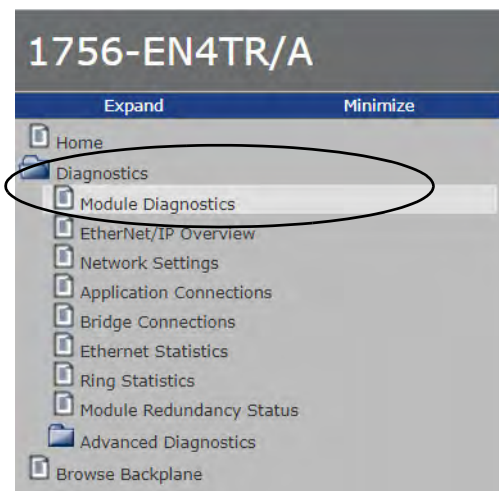
For more information on diagnostics, see Troubleshoot EtherNet/IP Networks, publication ENET-AT003.

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)

At the end of life, this equipment should be collected separately from any unsorted municipal waste.

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

Connect with us.