User Manual

Original Instructions

Allen-Bradley

Stratix Managed Switches

Stratix 5400 Switches (1783-HMS)

Stratix 5410 Switches (1783-IMS)

Stratix 5700 Switches (1783-BMS)

ArmorStratix 5700 Switches (1783-ZMS)

Stratix 8000 and 8300 Switches (1783-MS, 1783-RMS, 1783-MX)









Allen-Bradley • Rockwell Software

Rockwell Automation

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.

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).

Preface **13**
Access Product Release Notes 13
Additional Resources 13

Summary of Changes **15**

Chapter 1

About the Switches

EtherNet/IP CIP Interface 19
CIP Network Connections 19
EtherNet/IP QuickConnect Technology 19
Lite Versus Full Firmware Features (Stratix 5700 Switches) 20
Software Features 21
Hardware Features 22
Memory Allocation 25
Stratix 5400 Templates 25
Stratix 5410 Templates 26
Stratix 5700 and ArmorStratix 5700 Templates 27
Stratix 8000 and 8300 Templates 28

Chapter 2

Get Started

Express Setup Overview 30
Express Setup Requirements 30
Express Setup Button 32
Multi-mode Express Setup 34
Run Multi-mode Express Setup in Short Press Mode 35
Run Multi-mode Express Setup in Medium Press Mode 36
Run Multi-mode Express Setup in Long Press Mode 37
Single-mode Express Setup 38
Configure Network Settings via Device Manager 39
Configure Network Settings via the Logix Designer Application 42
Default Global Macro 44
RSLinx Software and Network Who Support 44
Electronic Data Sheet (EDS) Files 44
Data Accessible with CIP 45
Configuration via Device Manager 47
Access Device Manager 48
Configure Port Settings 51
Configuration via the Studio 5000 Environment 53
General Properties 55
Connection Properties 57
Switch Configuration 58
Port Configuration 59
User Administration via Device Manager 61

Configuration Files 62
Manage Configuration Files via Device Manager 62
Manage Configuration Files via the Logix Designer Application . . 63
Secure Digital (SD) Card 64
Synchronize the SD Card via Device Manager 65
Synchronize the SD Card via the Logix Designer Application 67
CompactFlash Memory Card (Stratix 8000/8300 Switches) 68
Firmware Updates 68
Cisco Network Assistant 69
Command-line Interface 70

Chapter 3

Install Stratix 5400 Switches

Specifications 75
Overview 75
Parts List and Required Tools 76
Install or Remove the SD Card 78
Verify Switch Operation 79
Mount the Switch on a DIN Rail 80
Remove the Switch from the DIN Rail 81
Ground the Switch 81
Wire the Switch DC Power Source 83
Attach the Switch Power Connectors 85
Install an SFP Module 87
Remove an SFP Module from an SFP Slot 89
Wire the External Alarms 90
Attach the Alarm Relay Connector to the Switch 93
Connect to 10/100 and 10/100/1000 Ports 93
Connect to 10BASE-T, 100BASE-TX, or 1000BASE-T Ports 94
Connect to PoE Ports 95
Connect to SFP Module Ports 95
Connect to a Dual-purpose Port 96

Chapter 4

Install Stratix 5410 Switches

Switch Specifications 101
Power Supply Specifications 101
Overview 102
Parts List and Required Tools 103
Install or Remove the SD Card 105
Verify Switch Operation 107
Mount the Switch on a Rack 107
Attach Brackets 108
Mount the Switch 110
Mount the Switch on a Wall 111
Attach the Brackets 111
Mount the Switch 113
Ground the Switch 114

Install a Power Supply Module in the Switch 115
Wire the Power Source 116
Remove a Power Supply Module from the Switch 120
Install an SFP Module 120
Remove an SFP Module from an SFP Slot 122
Wire the External Alarms 123
Attach the Alarm Relay Connector to the Switch 124
Connect to 10/100/1000 Ethernet, PoE/PoE+ Ports 124
Connect to SFP/SFP+ Ports 126

Chapter 5

Install Stratix 5700 Switches

Specifications 130
Overview 130
Parts List and Required Tools 132
Install or Remove the SD Card 133
Verify Switch Operation 134
Mount the Switch on a DIN Rail 135
Remove the Switch from the DIN Rail 137
Ground the Switch 137
Wire the Switch DC Power Source 139
Attach the Switch Power Connectors 143
Wire the Power over Ethernet DC Power Source 144
Attach the PoE Power Connector 145
Install an SFP Module 146
Remove an SFP Module from an SFP Slot 148
Wire the External Alarms 149
Attach the Alarm Relay Connector to the Switch 152
Connect to 10/100 and 10/100/1000 Ports 152
Connect to 10BASE-T, 100BASE-TX, or 1000BASE-T Ports . . . 153
Connect to PoE Ports 154
Connect to SFP Module Ports. 154
Connect to a Dual-purpose Port 155

Chapter 6

Install Stratix 8000 and 8300 Switches

Specifications 159
Overview 160
Parts List and Required Tools 162
Attach Expansion Modules. 164
Mount the Switch 166
Mount the Switch on a DIN Rail 166
Mount the Switch on a Wall or Panel 168
Install an SFP Module 169
Ground the Switch 171
Wire the DC Power Source for the Switch 172
Wire the DC Power Source for the PoE Expansion Module. 174
Attach the Power and Relay Connector to the Switch 176

Attach the Power Connector to the PoE Expansion Module 178
Wire External Alarms..... 178
Connect to 10/100 Copper Ports..... 180
Connect to a PoE Expansion Module Port 180
Connect to Dual-purpose Uplink Ports 181
Connect to 10/100/1000 Uplink Ports..... 181
Connect to SFP Fiber Ports 181
Connect to 100BaseFX Ports..... 182
Install or Remove the CompactFlash Card 182

Chapter 7

Configure Switch Features

Access Control Lists (ACLs) 184
Configure ACLs via Device Manager..... 185
Alarms 189
Configure Alarms via Device Manager..... 190
CIP Sync Time Synchronization (Precision Time Protocol) 194
Boundary Mode 194
End to End Transparent Mode 195
Forward Mode 195
NTP-PTP Clock Mode (Stratix 5400 and 5410 Switches) ... 195
Configure Time Synchronization via Device Manager 196
Configure Time Synchronization
via the Logix Designer Application..... 204
View Time Sync Information in the Logix Designer Application... 209
Cryptographic IOS..... 212
Device-level Ring (DLR)..... 212
Overview 213
DLR Port Choices..... 215
DLR Considerations..... 216
Redundant Gateways 217
DHCP for Ring Devices 222
Multiple Rings 225
Configure DLR via Device Manager 226
Configure DLR via the Logix Designer Application 230
Dynamic Host Configuration Protocol (DHCP) Persistence 238
Configure DHCP via Device Manager 238
Configure DHCP via the Logix Designer Application 243
EtherChannels..... 244
Configure EtherChannels via Device Manager 246
Configure EtherChannels via the Logix Designer Application 247
Motion Prioritized QoS Macros..... 248
Configure Motion Prioritized QoS Macros via Device Manager ... 249
Horizontal Stacking..... 250
Internet Group Management Protocol (IGMP)
Snooping with Querier 252
Configure IGMP Snooping via Device Manager..... 253

Network Address Translation (NAT) 254
Configuration Overview 254
VLAN Assignments 260
Configuration Considerations 261
Traffic Permits and Fixups 262
Configure NAT via Device Manager 262
Configure NAT via the Logix Designer Application 274
Configure NAT via the Logix Designer Application (Stratix 5410 Switches) 286
View Address Translations in RSLinx Software 294
Network Time Protocol (NTP) 295
Configure NTP in Device Manager 295
Parallel Redundancy Protocol (PRP) 297
Configure PRP via Device Manager 298
Port Mirroring 301
Configure Port Mirroring in Device Manager 302
Port Security 303
Dynamic Secure MAC Address (MAC ID) 303
Static Secure MAC Address (MAC ID) 304
Security Violations 304
Configure Port Security via Device Manager 304
Configure Port Security via the Logix Designer Application . . 307
Port Thresholds 309
Incoming (storm control) 309
Outgoing (rate limiting) 310
Default Port Thresholds Configuration 310
Configure Port Thresholds via Device Manager 311
Configure Port Thresholds via the Logix Designer Application 312
Power over Ethernet (PoE) 314
Powered Device Detection and Initial Power Allocation 315
Power Management Modes 316
Configure PoE Ports via Device Manager 319
Configure PoE via the Logix Designer Application 322
Resilient Ethernet Protocol (REP) 325
REP Open Segment 326
REP Ring Segment 327
Access Ring Topologies 327
Link Integrity 328
Configure REP via Device Manager 329
Layer 3 Routing 330
Types of Routing 331
Enhanced Interior Gateway Routing Protocol (EIGRP) 332
Configure EIGRP via Device Manager 333
Open Shortest Path First (OSPF) 337
Configure OSPF via Device Manager 339

Static and Connected Routing. 344
Reallocate Switch Memory for Routing via Device Manager . . 345
Enable and Configure Routing via Device Manager. 346
Simple Network Management Protocol (SNMP) 347
Supported MIBs. 348
Configure SNMP via Device Manager. 349
Use SNMP Management Applications 350
Smartports. 350
Custom Smartport Roles 351
Avoid Smartport Mismatches. 351
Configure Smartports via Device Manager 352
Customize Port Role Attributes 353
Manage Custom Smartport Macros 354
Assign Smartports and VLANs via the Logix Designer Application 358
Spanning Tree Protocol (STP) 361
Configure STP via Device Manager 362
Configure STP via the Logix Designer Application 364
Virtual Local Area Networks (VLANs) 365
Isolate Traffic and Users 366
Isolate Different Traffic Types. 367
Group Users 367
Configure VLANs via Device Manager 368
Configure VLANs via the Logix Designer Application. 369

Chapter 8

Monitor the Switch

Switch Status via Device Manager 372
Front Panel 373
Switch Information. 385
Switch Health. 386
Port Utilization 387
Switch Status via the Logix Designer Application 388
Port Status. 391
System Log Messages 392
Trends 394
Port Statistics 395
NAT Statistics. 396
Monitor NAT Statistics via Device Manager. 396
Monitor NAT Statistics via the Logix Designer Application. . 399
Private-to-Public Translation Diagnostics 401
Public-to-Private Translation Diagnostics 402
REP Status. 403
CIP Status. 403
DHCP Clients. 405
DLR Status 406
Monitor DLR Status via Device Manager. 406
Monitor DLR Status via the Logix Designer Application. 408

PRP Status. 410
Port Diagnostics 412
Cable Diagnostics 414
Diagnose Cables via Device Manager 414
Diagnose Cables via the Logix Designer Application 415
DHCP Pool Display. 416

Chapter 9

Troubleshoot the Switch

Troubleshoot the Installation 418
Switch POST Results 418
POST Results with a Terminal 418
Bad or Damaged Cable. 419
Ethernet and Fiber Cables. 419
Link Status. 420
Transceiver Issues 420
Port and Interface Settings 420
Verify Boot Fast. 421
Troubleshoot IP Addresses. 421
Troubleshoot Device Manager 421
Troubleshoot Switch Performance. 422
Access Direct Managed Mode 423
Restart or Reset the Switch. 424
Restart the Switch from Device Manager 424
Restart the Switch from the Logix Designer Application 425
Reset the Switch to Factory Defaults 425
Recover the Switch Firmware 426
Reset the Switch to Factory Defaults 426
Reset a Stratix 5400, Stratix 5410, Stratix 5700, or ArmorStratix 5700 Switch 426
Reset a Stratix 8000/8300 Switch 427
Troubleshoot a Firmware Update. 427
Collect System and Configuration Information for Technical Support 428

Appendix A

Data Types

Stratix 5400 Data Types 430
8-port Switches. 430
12-port Switches 432
12-port Gigabit Switches 434
16-port Switches 436
16-port Gigabit Switches 439
20-port Switches 442
20-port Gigabit Switches 445
Stratix 5410 Data Types 449
Stratix 5700 and ArmorStratix 5700 Data Types. 454
6-port Gb Switches 454

6-port Switches 455
8-port Switches 457
10-port Gb Switches 458
10-port Switches 460
16-port Switches 462
20-port Gb Switches 465
18-port Gb Switches 467
20-port Gb Switches 471
20-port Switches 474
24-port Switches 477
Stratix 8000 and 8300 Data Types 481

Appendix B

Port Assignments for CIP Data

Stratix 5400 Port Assignments 488
Stratix 5410 Port Assignments 490
Stratix 5700 Port Assignments 491
ArmorStratix 5700 Port Assignments 492
Stratix 8000 and 8300 Port Assignments 493

Appendix C

Port Numbering

Stratix 5400 Port Numbering 496
Stratix 5410 Port Numbering 504
Stratix 5700 Port Numbering 505
ArmorStratix 5700 Port Numbering 512
Stratix 8000 and 8300 Port Numbering 515

Appendix D

Cables and Connectors

Stratix 5410 Cables and Connectors 517
10/100/1000 Ports 517
Connect to 10BASE-T- and 100BASE-TX-Compatible Devices . . 518
Console Ports 520
Alarm Port 522
Ethernet, PoE Port Cable Specifications 522
Stratix 5400 and 5700 Cables and Connectors 523
10/100 and 10/100/1000 Ports 523
Connect to 10BASE-T- and 100BASE-TX-Compatible Devices . . 524
Dual-purpose Ports (combo ports) 525
Console Ports 526
Alarm Ports 528
PoE Port Cable Specifications 528
ArmorStratix 5700 Cables and Connectors 529
10/100 Ports 529
100/1000 Ports 529
Connect to 10BASE-T- and 100BASE-TX-Compatible Devices . . 530
Console Port 532
Alarm Ports 533

PoE Port Cable Specifications 534
Stratix 8000/8300 Cables and Connectors 534
10/100 and 10/100/1000 Ports. 534
Connect to 10BASE-T- and 100BASE-TX-compatible Devices. . . 535
100Base-FX Ports 537
SFP Transceiver Ports. 537
Dual-purpose Ports 537
Console Port 538
PoE Port Cable Specifications 539

Index 541

Notes:

This publication describes the embedded software features and tools for configuring and managing Stratix™ managed switches. In addition, this publication provides troubleshooting information to help you resolve basic switch and network issues.

This manual assumes that you understand the following:

- Local area network (LAN) switch fundamentals
- Concepts and terminology of the Ethernet protocol and local area networking

Access Product Release Notes

Access product release notes from the Product Compatibility and Download Center at http://www.rockwellautomation.com/rockwellautomation/support/pcdc.page.

Additional Resources

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

Resource	Description
Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001	Provides specification information for the switches.
Ethernet Design Considerations Reference Manual, publication ENET-RM002	Provides information about implementing a system based on the EtherNet/IP platform.
Device Manager web interface online help (provided with the switch)	Provides context-sensitive information on configuring and using the switch, including system messages.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, http://www.rockwellautomation.com/global/certification/overview.page	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http://www.rockwellautomation.com/global/literature-library/overview.page. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

For information on additional software features or further configuration, see Cisco publications for Industrial Ethernet series switches at http://www.Cisco.com.

Notes:

This manual contains new and updated information as indicated in the following table.

Topic	Page
Software features include multiple DLR rings, global QoS macros, horizontal stacking, and PRP	21
Enable CIP VLAN and Enable SSH checkboxes added to Express Setup window	40
Motion Prioritized QoS macros	44, 248
Access Device Manager via a secure connection	48
Connect to the command-line interface (CLI) via Secure Shell (SSH), Telnet disabled	70
Configure time syncronization in the Logix Designer application	204
View time sync information in the Logix Designer application	209
Crytpographic IOS	212
Device-level ring (DLR) with three ring support for Stratix 5400 switches	212, 215, 225
Configure redundant gateways and DHCP for DLR in the Logix Designer application	230
Configure EtherChannels in the Logix Designer application	247
Horizontal stacking for Stratix 5410 switches	250
Parallel Redundancy Protocol (PRP) for 5400 and 5410 switches	297
Monitor DHCP clients	405
Monitor DLR	406
Monitor PRP for Stratix 5400 and 5410 switches	410
Collect system and configuration information for Technical Support	428

Notes:

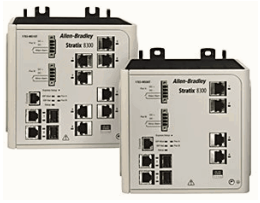
About the Switches

Topic	Page
EtherNet/IP CIP Interface	19
Lite Versus Full Firmware Features (Stratix 5700 Switches)	20
Software Features	21
Hardware Features	22
Memory Allocation	25

Stratix® managed switches provide a secure switching infrastructure for harsh environments. You can connect the switches to network devices such as servers, routers, and other switches. In industrial environments, you can connect Ethernet-enabled industrial communication devices, including programmable logic controllers (PLCs), human machine interfaces (HMIs), drives, sensors, and I/O.

Table 1 on page 18 describes the Stratix switch families.

Table 1 - Stratix Switches

Switch Family	Description
Stratix 5400 switches 	Layer 2 and Layer 3 scalable managed switches. Available in 8…20 port versions, including all Gigabit port versions.
Stratix 5410 switches 	Layer 2 and Layer 3 scalable managed switches. Available in 28-port versions.
Stratix 5700 switches 	Layer 2 scalable managed switches. Available in 6…20 port versions.
ArmorStratix™ 5700 switches 	Layer 2 managed switches with IP67-rating for protection in extreme conditions. Available in 8…24 port versions.
Stratix 8000 switches 	Layer 2 modular managed switches available with copper, fiber, small form-factor pluggable (SFP), and Power over Ethernet (PoE) expansion modules. Available in 6…26 port versions.
Stratix 8300 switches 	Layer 3 modular managed switches available with copper, fiber, SFP, and Power over Ethernet (PoE) expansion modules. Available in 6…26 port versions.

EtherNet/IP CIP Interface

Stratix switches contain an EtherNet/IP network interface. The EtherNet/IP network is an industrial automation network specification from the Open DeviceNet Vendor Association (ODVA). The network uses the Common Industrial Protocol (CIP) for its application layer and TCP/UDP/IP for its transport and network layers. This interface is accessible via any of the Ethernet ports by using the IP address of the switch.

CIP Network Connections

CIP is an object-oriented, connection-based protocol that supports two basic types of messaging:

- Explicit
- Implicit (I/O)

A maximum of 32 connections is available. Both connection types must use the switch password before any switch parameters can be written. The password is the same one you enter during Express Setup.

Connection	Description
Explicit Messaging	Explicit Messaging connections provide generic, multi-purpose communication paths between two devices. These connections are often referred to as messaging connections. Explicit messages provide request/response-oriented network communication. Each request is typically directed at another data item. Explicit messages can be used to configure, monitor, and troubleshoot the switch. The Explicit Messaging interface is used by the Studio 5000 Logix Designer® application.
Implicit messaging (I/O connections)	I/O connections provide dedicated, special purpose communication paths between a producing application and one or more consuming applications. The application-specific I/O data that moves through these connections is typically a fixed, cyclical structure. The switch supports two I/O connection choices. • Input Only • Exclusive Owner Both connections are cyclic and adjustable from 300...5000 ms. The Input Only connection contains a data structure with status information on the switch in general and specific status on each of the ports. This connection is multicast. Multiple controllers can share the connection. The Exclusive Owner connection uses the same Input data structure as the Input Only connection, but adds an Output data structure. The Output data contains a bit for each port that lets you enable or disable each port separately. While the Input data on this connection can be shared via multicast by multiple controllers, only one controller can own the Output data. If a second controller attempts to open this connection, the connection is rejected.

IMPORTANT Because the controller sends output data cyclically, the output data overrides attempts by other software tools or visualization stations to enable or disable a port.

EtherNet/IP QuickConnect Technology

EtherNet/IP QuickConnect technology enables EtherNet/IP devices to quickly power up and join an EtherNet/IP network. Stratix switches can be a part of a network configuration that uses QuickConnect technology. To use the switches in a network that supports QuickConnect technology, you must apply specific port settings to the switch. To configure the switch and apply the port settings for QuickConnect technology, refer to the Ethernet QuickConnect Application Technique, publication ENET-AT001.

Lite Versus Full Firmware Features (Stratix 5700 Switches)

Some features for Stratix 5700 switches depend on whether the switches have Full or Lite firmware. All Stratix 8000 and ArmorStratix 5700 switches have Full firmware.

To determine the firmware type available for specific catalog numbers, see the Stratix 5700 switch descriptions in Table 166 on page 505.

Feature	Lite Firmware	Full Firmware
CIP Sync (IEEE 1588)		Separate option
Resilient Ethernet Protocol (REP)	•	•
FlexLinks		•
Quality of Service (QoS)		•
Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), MST (instances)	64	128
Internet Group Management Protocol (IGMP) Snooping with querier	•	•
Virtual Local Area Networks (VLANs) with trunking	64	255
EtherChannel (link aggregation)		•
Port Threshold (Storm control and traffic shaping)		•
IPv6 support		•
Access Control Lists (ACL)		•
Static and interVLAN routing		•
CIP port control and fault detection	•	•
MAC ID Port security		•
IEEE 802.1x security		•
TACACS+, RADIUS authentication	•	•
Encryption (SSH, SNMPv3, HTTPS)	Separate IOS firmware available as a separate item	
Port mirroring	•	•
Syslog	•	•
Broken wire detection	•	•
Duplicate IP address detection	•	•
Simple Network Management Protocol (SNMP)	•	•
Smartports	•	•
Dynamic Host Configuration Protocol (DHCP) per port	•	•
Command-line interface (CLI)	•	•
Compatible with Cisco tools: Cisco Network Assistant (CNA); CiscoWorks	•	•
EtherNet/IP (CIP) interface	•	•
Device-level ring (DLR)	Available on specific models that are listed on page 215	

Software Features

Switch software features can be configured via Device Manager, the Logix Designer application, or both:

- See Configuration via Device Manager on page 47
- See Configuration via the Studio 5000 Environment on page 53

All features can be configured via the command-line interface (CLI).

Some features are available only on select switches and expansion modules.

Table 2 - Software Features

Feature	Switches	Device Manager	Logix Designer
Access Control Lists (ACLs)	All	•	—
Alarms	All	•	—
CIP Sync Time Synchronization/ Precision Time Protocol (PTP)	All Stratix 5400 switches All Stratix 5410 switches Stratix 5700 switches: 1783-BMS10CGN, 1783-BMS10CGP, 1783-BMS12T4E2CGNK, 1783-BMS12T4E2CGP, 1783-BMS20CGN, 1783-BMS20CGP, 1783-BMS20CGPK ArmorStratix 5700 switches: 1783-ZMS4T4E2TGP, 1783-ZMS8T8E2TGP, 1783-ZMS4T4E2TGN, 1783-ZMS8T8E2TGN All Stratix 8000/8300 switch base units (PTP traffic can be only forwarded through expansion modules)	•	•
Device-level Ring (DLR)	All Stratix 5400 switches Stratix 5700 switches: 1783-BMS10CGP, 1783-BMS10CGN, 1783-BMS12T4E2CGL, 1783-BMS12T4E2CGP, 1783-BMS12T4E2CGNK,1783-BMS20CL, 1783-BMS20CA, 1783-BMS20CGL, 1783-BMS20CGP, 1783-BMS20CGN, 1783-BMS20CGPK ArmorStratix 5700 switches: 1783-ZMS4E4T2GP, 1783-ZMS8E8T2GP, 1783-ZMS8E8T2GN, 1783-ZMS8E8T2GN	•	•
Dynamic Host Configuration Protocol (DHCP) Persistence	All	•	•
DHCP for Ring Devices	Stratix 5700 and ArmorStratix 5700 switches	•	
Enhanced Interior Gateway Routing Protocol (EIGRP)	Stratix 5400 switches with Layer 3 firmware Stratix 5410 switches with Layer 3 firmware Stratix 8300 base units	•	—
EtherChannels	All	•	—
Motion Prioritized QoS macros	Stratix 5400 switches Stratix 5410 switches Stratix 5700 switches with Full firmware ArmorStratix 5700 switches	•	—
Horizontal stacking	Stratix 5410 switches: 1783-IMS28NAC, 1783-IMS28RAC, 1783-IMS28NDC, 1783-IMS28RDC	—	—
Internet Group Management Protocol (IGMP) Snooping with Querier	All	•	—
Multi-mode Express Setup	Stratix 5400, 5410, 5700, ArmorStratix 5700, and Stratix 8000 switches	•	•
Network Address Translation (NAT)	All Stratix 5400 switches All Stratix 5410 switches Stratix 5700 switches: 1783-BMS10CGN, 1783-BMS20CGN, 1783-BMS12T4E2CGNK ArmorStratix 5700 switches: 1783-ZMS4T4E2TGN, 1783-ZMS8T8E2TGN	•	•
Network Time Protocol	Stratix 5400 switches Stratix 5410 switches Stratix 5700 switches ArmorStratix 5700 switches Stratix 8000/8300 switches	•	—

Table 2 - Software Features (Continued)

Feature	Switches	Device Manager	Logix Designer
Parallel Redundancy Protocol (PRP)	Stratix 5400 switches Stratix 5410 switches	•	—
Port Mirroring	All	•	—
Port Security	All	•	•
Port Thresholds	All	•	•
Power over Ethernet (PoE)	Stratix 5400 switches: 1783-HMS4T4E4CGN, 1783-HMS4S8E4CGN, 1783-HMS4EG8CGN, 1783-HMS8TG8EG4CGN, 1783-HMS4SG8EG4CGN,1783-HMS4EG8CGR, 1783-HMS8TG8EG4CGR, 1783-HMS4SG8EG4CGR All Stratix 5410 switches Stratix 5700 switches: 1783-BMS12T4E2CGNK, 1783-BMS12T4E2CGP, 1783-BMS12T4E2CGL ArmorStratix 5700 switches: 1783-ZMS4T4E2TGP, 1783-ZMS8T8E2TGP, 1783-ZMS4T4E2TGN, 1783-ZMS8T8E2TGN Stratix 8000/8300 expansion modules: 1783-MX04E, 1783-MX04T04E	•	•
Resilient Ethernet Protocol (REP)	All	•	—
Static and Connected Routing	All	•	—
Open Shortest Path First (OSPF) Gateway Routing Protocol	Stratix 5400 switches with Layer 3 firmware Stratix 5410 switches with Layer 3 firmware Stratix 8300 base units	•	—
Simple Network Management Protocol (SNMP)	All	•	—
Smartports	All	•	•
Spanning Tree Protocol (STP)	All	•	•
Virtual Local Area Networks (VLANs)	All	•	•

Hardware Features

See the following for a description of hardware features:

- For Stratix 5400, Stratix 5700, ArmorStratix 5700, and Stratix 8000/8300 switches, see Table 3 on page 23.
- For Stratix 5410 switches, see Table 4 on page 24.
- For supported SFP modules, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Table 3 - Hardware Features for Stratix 5400, Stratix 5700, ArmorStratix 5700, and Stratix 8000/8300 Switches

Feature	Description
Power and relay connectors	You connect the power and alarm signals to the front panel of a switch: • Stratix 5400 switches—One connector provides primary DC power. A second connector provides secondary power. The two connectors are physically identical. You can activate alarms for environmental, power supply, and port status alarm conditions. You can configure an alarm to indicate open or closed contacts. There is no separate power connector for PoE. • Stratix 5700 switches—One connector provides primary DC power and a second connector provides secondary power. The two connectors are physically identical. You can activate alarms for environmental, power supply, and port status alarm conditions. You can configure an alarm to indicate open or closed contacts. A separate power connector is required for PoE. • ArmorStratix 5700 switches—One cable provides DC power from one or dual power sources. Relay connectors and alarm relays are available for only catalog numbers 1783-ZMS4T4E2TGP, 1783-ZMS8T8E2TGP, 1783-ZMS4T4E2TGN, and 1783-ZMS8T8E2TGN. There is no separate power connector for PoE. • Stratix 8000/8300 switches—One connector provides primary DC power (supply A) and the major alarm signal. A second connector provides secondary power (supply B) and the minor alarm signal. The two connectors are physically identical and are in the upper-left side of the front panel. The power and relay connectors also provide an interface for two independent alarm relays: the major alarm and the minor alarm. You can activate the relays for environmental, power supply, and port status alarm conditions. You can configure an alarm to indicate open or closed contacts. The relay itself is normally open, so under power failure conditions, the contacts are open. From the Command-line interface (CLI), you can associate any alarm condition with one alarm relay or with both relays. When dual power sources are operational for any of the switches, the switch draws power from the DC source with the higher voltage. If one of the two power sources fail, the other continues to power the switch.
Console port	To configure, monitor, and manage a switch, you can connect a switch to a computer through the console port: • Stratix 5400 and Stratix 5700 switches—Connect to the console port with an RJ45-to-DB-9 adapter cable or a mini USB cable. The mini USB driver is available in the firmware download section at http://www.rockwellautomation.com. • ArmorStratix 5700 switches— Connect to the console port with an M12-to-DB-9 cable. See page 532. • Stratix 8000/8300 switches—Connect to the console port with an RJ45-to-DB-9 adapter cable.
Dual-purpose (combo) uplink ports	You can configure the dual-purpose uplink ports available on some models for RJ45 (copper) or SFP (fiber) media types. Only one of these connections in each of the dual-purpose ports can be active at a time. If both ports are connected, the SFP module port has priority. You can set the copper RJ45 ports to operate at 10 Mbps, 100 Mbps, or 1000 Mbps, full-duplex, or half-duplex. You can configure them as fixed 10 Mbps, 100 Mbps, or 1000 Mbps (Gigabit) Ethernet ports and can configure the duplex setting. 1000 Mbps is not supported on all modules with combo ports. You can use approved Gigabit (or 100 Mbps) Ethernet SFP modules to establish fiber-optic connections to other devices. These transceiver modules are field-replaceable and provide the uplink interfaces when inserted into an SFP module slot. You use fiber-optic cables with LC connectors to connect to a fiber-optic SFP module. These ports operate only in full-duplex.
10/100 copper ports	You can set the 10/100 copper ports to operate at 10 Mbps or 100 Mbps, full-duplex, or half-duplex. You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3-2002. The default setting is autonegotiate. When set for autonegotiation, the port senses the speed and duplex settings of the attached device. If the connected device also supports autonegotiation, the switch port negotiates the connection with the fastest line speed that both devices support. The port also negotiates full-duplex transmission if the attached device supports it. The port then configures itself accordingly. In all cases, the attached device must be within 100 m (328 ft) of the switch.
100/1000 SFP ports	The SFP ports on some models provide full-duplex, 100- or 1000-Mbps connectivity. ArmorStratix 5700 switches and Stratix 8000/8300 base switches do not have SFP ports.
PoE/PoE+ ports	The PoE ports available on some switches and expansion modules can be configured for PoE (IEEE 802.3af) or PoE+ (IEEE 802.3at Type 2). You can configure PoE /PoE+ ports in any combination of PoE and PoE+. Stratix 5400 and ArmorStratix 5700 switches use one power connection for both basic power supply and PoE power supply. Stratix 5700 switches and Stratix 8000/8300 expansion modules require a dedicated power supply for PoE. See the following for PoE requirements: • For Stratix 5400 switches, see page 83 • For Stratix 5700 switches, see page 144. • For ArmorStratix 5700 switches, see page 156. • For Stratix 8000/8300 expansion modules, see page 174.
Auto-MDIX	When connecting the switch to workstations, servers, and routers, straight-through cables are typically used. However, the automatic medium-dependent interface crossover (auto-MDIX) feature of the switch is enabled by default and reconfigures the ports to use either a straight-through or crossover cable type. The auto-MDIX feature is enabled by default. When the auto-MDIX feature is enabled, the switch detects the required cable type (straight-through or crossover) for copper Ethernet connections and configures the interfaces accordingly. You can use the Command-line interface (CLI) to disable the auto-MDIX feature. See the online help for more information.

Table 4 - Hardware Features for Stratix 5410 Switches

Feature	Description
Dual power supply modules	Depending on the switch model, one AC or DC power supply module comes pre-installed in the switch. You can order an optional second power supply of any voltage type to provide redundancy and additional power for PoE devices: • One power supply provides 60 W for PoE/PoE+. • Two power supplies provide 185 W for PoE/PoE+. The power-input terminal on the cable-side of the switch provides connections for high-voltage AC, high-voltage DC, or low-voltage DC power for the two power supplies. When dual power sources are operational, the switch draws power from the power source with the higher voltage. If one of the two power sources fail, the other continues to power the switch.
Alarm relay connector	The front panel alarm port uses an RJ45 connector. You can connect four alarm inputs and one alarm output for environmental, power supply, and port status conditions. You can configure an alarm to indicate open or closed contacts.
Console port	To configure, monitor, and manage a switch, you can connect a switch to a computer through the console port: Connect to the console port with an RJ45-to-DB-9 adapter cable or a mini USB cable. The mini USB driver is available in the firmware download section at http://www.rockwellautomation.com.
10/100/1000 Ethernet, PoE/PoE+ ports	You can set the 10/100/1000 ports to operate at 10 Mbps, 100 Mbps, or 1000 Mbps, full-duplex, or half-duplex. You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3-2002. The default setting is autonegotiate. When set for autonegotiation, the port senses the speed and duplex settings of the attached device. If the connected device also supports autonegotiation, the switch port negotiates the connection with the fastest line speed that both devices support. The port also negotiates full-duplex transmission if the attached device supports it. The port then configures itself accordingly. In all cases, the attached device must be within 100 m (328 ft) of the switch. The ports can also be configured for PoE (IEEE 802.3af) or PoE+ (IEEE 802.3at Type 2): • You can configure the ports in any combination of PoE and PoE+. • A second power supply is required to support PoE+. • The ports deliver up to 15.4 W of PoE and 30 W of PoE+. The ports can be designated as high or low priority PoE/PoE+ ports. When two power-supply modules are installed, the system has enough power to support all ports as PoE/PoE+ ports. If one of the power-supply modules fails, the power to the low priority ports is dropped, while power to the high priority ports remains uninterrupted. For more information, see pages 314, 321, and 324. The ports use RJ45 connectors with Ethernet pinouts. The maximum cable length is 100 m (328 ft).
100/1000 SFP ports	100/1000 SFP ports provide full-duplex, 100-Mbps or 1-Gbps connectivity.
1000 SFP ports	1000 SFP ports provide only 1-Gbps connectivity. These uplink ports are available on catalog numbers1783-IMS28GNDC, 1783-IMS28GNAC, 1783-IMS28GRDC, and 1783-IMS28GRAC.
1000/10 Gigabit SFP/SFP+ ports	1000/10 Gigabit SFP/SFP+ ports provide full-duplex, 1-Gbps or 10-Gbps connectivity. The port speed is 1 Gbps when a 1000BASE SFP module is installed and 10 Gbps when an 10GBASE SFP+ module is installed.
Auto-MDIX	When connecting the switch to workstations, servers, and routers, straight-through cables are typically used. However, the automatic medium-dependent interface crossover (auto-MDIX) feature of the switch is enabled by default and reconfigures the ports to use either a straight-through or crossover cable type. The auto-MDIX feature is enabled by default. When the auto-MDIX feature is enabled, the switch detects the required cable type (straight-through or crossover) for copper Ethernet connections and configures the interfaces accordingly. You can use the Command-line interface (CLI) to disable the auto-MDIX feature. See the online help for more information.
Global positioning system (GPS)	Not available in the current release.
Inter-range instrumentation group (IRIG) time codes	
Time of day (ToD) synchronization	

Memory Allocation

You can use Switch Database Management (SDM) templates to configure system resources in the switch to optimize specific features. You can select a template to provide maximum system usage for some functions. For example, use the default template to balance resources, and use the access template to obtain maximum ACL usage. To allocate hardware resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features.

Stratix 5400 Templates

The selected template optimizes the resources in the switch to support features for eight routed interfaces and 1024 VLANs.

Layer 2 firmware models have the IPv4 Default template.

Layer 3 firmware models have these templates:

- IPv4 Default
- Dual IPv4/IPv6 Default
- IPv4 Routing
- Dual IPv4/IPv6 Routing

Table 5 - Stratix 5400 Templates

Feature	Memory Allocation			
	IPv4 Default	Dual IPv4/IPv6 Default	IPv4 Routing	Dual IPv4/IPv6 Routing
Unicast MAC addresses	16K	16K	16K	16K
IPv4 IGMP groups + multicast routes	1K	1K	1K	1K
IPv4 unicast routes	18K	5.25K	24K	6K
IPv6 multicast groups	0	1K	0	1K
IPv6 unicast groups	0	5.25K	0	7K
Directly connected IPv4 hosts	16K	4K	16K	4K
Directly connected IPv6 addresses	0	4K	0	4K
Indirect IPv4 routes	2K	1.25K	8K	2K
Indirect IPv6 unicast routes	0	5.25K	0	3K
IPv4 policy-based routing aces	0.125K	0.25K	0.375K	0.125K
IPv4/MAC QoS aces	1.875K	0.5K	0.5K	0.5K
IPv4/MAC security aces	1.875K	0.75K	1K	0.625K
IPv6 policy-based routing aces	0	0.25K	0	0.125K
IPv6 QoS aces	0	0.375K	0	0.125K
IPv6 security aces	0	0.375K	0	0.125K

Stratix 5410 Templates

The selected template optimizes the resources in the switch to support features for eight routed interfaces and 1024 VLANs.

Layer 2 firmware models have the Default template.

Table 6 - Stratix 5410 Layer 2 Firmware Model Template

Feature	Memory Allocation
Unicast MAC addresses	16K
IPv4 IGMP groups or IPv6 groups	1K IPv4
Direct routes	1K IPv4
Indirect routes	0.25K IPv4
IPv4 or IPv6 policy-based routing ACEs	0
IPv4 or IPv6 QoS ACEs	1K (IPv4 QoS)
IPv4 or IPv6 port or MAC security ACEs	1K (IPv4 ACL)

Layer 3 firmware models have these templates:

- Default
- Dual-default
- IPv4 Routing
- Dual-routing

Table 7 - Stratix 5410 Layer 3 Firmware Model Templates

Feature	Memory Allocation			
	Default	Dual-default	IPv4 Routing	Dual-routing
Unicast MAC addresses	16K	16K	16K	16K
IPv4 IGMP groups or IPv6 groups	1K IPv4	1K IPv4 1K IPv6	1K IPv4	1K IPv4 1K IPv6
Direct routes	16K IPv4	4K IPv4 4K IPv6	16K IPv4	4K IPv4 4K IPv6
Indirect routes	2K IPv4	1.25K IPv4 1.25K IPv6	8K IPv4	2K IPv4 3K IPv6
IPv4 or IPv6 policy-based routing ACEs	0.125K (IPv4 PBR)	0.25K (IPv4 PBR) 0.25K (IPv6 PBR)	0.5K (IPv4 PBR)	0.125K (IPv4 PBR) 0.125K (IPv6 PBR)
IPv4 or IPv6 QoS ACEs	1.75K (IPv4 QoS)	0.5K (IPv4 QoS) 0.5K (IPv6 QoS	0.5K (IPv4 QoS)	0.5K (IPv4 QoS) 0.125K (IPv6 QoS)
IPv4 or IPv6 port or MAC security ACEs	1.75K (IPv4 ACL)	0.75K (IPv4 ACL) 0.5K (IPv6 ACL)	1K (IPv4 ACL)	0.625K (IPv4 ACL) 0.125K (IPv6 ACL)

Stratix 5700 and ArmorStratix 5700 Templates

The following SDM templates are available:

- Default
- Lanbase Routing
- Dual IPv4 and IPv6

If you enable static routing, or if you have more than 180 IGMP groups or multicast routes., consider using the routing template.

If you use IPv6, consider using the Dual IPv4 and IPv6 template.

You can select SDM templates for IP version 4 (IPv4) to optimize these features.

Table 8 - Stratix 5700 and ArmorStratix 5700 Templates

Feature	Memory Allocation		
	Default	**Lanbase Routing**	**Dual IPv4 and IPv6**
Unicast MAC addresses	8K	4K	7.5K
IPv4 IGMP groups + multicast routes	0.25K	0.25K	0.25K
IPv4 unicast routes	0	4.25K	0
IPv6 multicast groups	0	0	0.375K
Directly connected IPv4 hosts	0	4K	
Directly connected IPv6 addresses	0	0	0
Indirect IPv4 routes	0	0.25K	
Indirect IPv6 routes	0	0	0
IPv4 policy-based routing aces	0	0	
IPv4/MAC QoS aces	0.375K	0.375K	0.375K
IPv4/MAC security aces	0.375K	0.375K	0.375K
IPv6 policy-based routing aces	0	0	0
IPv6 QoS aces	0	0	0
IPv6 security aces	0	0	0.125K

Stratix 8000 and 8300 Templates

The following SDM templates are recommended:

- Default
- Lanbase Routing

For static and connected routing, or if you have more than 180 IGMP groups or multicast routes, you can use the Lanbase Routing template. Other SDM templates are available, but are not covered in detail.

You can use SDM templates for IP Version 4 (IPv4) to optimize these features.

Table 9 - Stratix 8000 and ArmorStratix 8300 Templates

Feature	Memory Allocation	
	Default	**Lanbase Routing**
Unicast MAC addresses	8K	4K
IPv4 IGMP groups + multicast routes	0.25K	0.25K
IPv4 unicast routes	0	0.75
Directly connected IPv4 hosts	0	0.75
Indirect IPv4 routes	0	16
IPv4 policy-based routing ACEs	0	0
IPv4/MAC QoS ACEs	0.375K	0.375K
IPv4/MAC security ACEs	0.375K	0.375K

Get Started

Topic	Page
Express Setup Overview	30
Multi-mode Express Setup	34
Single-mode Express Setup	38
Configure Network Settings via Device Manager	39
Configure Network Settings via the Logix Designer Application	42
Default Global Macro	44
RSLinx Software and Network Who Support	44
Configuration via Device Manager	47
Configuration via the Studio 5000 Environment	53
User Administration via Device Manager	61
Configuration Files	62
Secure Digital (SD) Card	64
CompactFlash Memory Card (Stratix 8000/8300 Switches)	68
Firmware Updates	68
Cisco Network Assistant	69
Command-line Interface	70

Express Setup Overview

When you first install the switch, use Express Setup to perform these initial setup tasks:

- Assign the switch an initial IP address. You can then access the switch through the IP address for more configuration.
- Run the global macro to set initial configuration parameters, as described on page 43.

Express Setup Requirements

Multi-mode and single-mode versions of Express Setup are available depending on your switch and IOS version:

- With IOS version **15.2(4)EA3 or later**, the following switches use multi-mode Express Setup, as described on page 34:
  - Stratix® 5400
  - Stratix 5410
  - Stratix 5700
  - ArmorStratix™ 5700
  - Stratix 8000
- With IOS version **15.2(4)EA or earlier**, all switches use single-mode Express Setup, as described on page 38.
- All IOS versions of the Stratix 8300 switch use single-mode Express Setup.

Multi-mode Express Setup enables you to configure network settings in either Device Manager or the Studio 5000 Logix Designer® application. To configure network settings via the Logix Designer application, you must have the Add-on Profile (AOP) for Stratix switches, **version 11.01.xx or later**.

You need this equipment to install the switch.

Component	Requirement
Hardware	
Processor	1 GHz or faster 32-bit (x86) or 64-bit (x64)
RAM	1 GB RAM (32-bit) or 2GB RAM (64-bit)
Hard disk space	16 GB (32-bit) or 20 GB (64-bit)
Software	
Operating system	Windows 7
Web browser	Latest version of Internet Explorer™ or Firefox with JavaScript enabled. Express Setup verifies the browser version when starting a session, and it does not require a plug-in.
Computer-to-switch connection (single-mode Express Setup or multi-mode Express Setup in Short Press mode)	Straight-through or crossover Category 5 Ethernet cable or (ArmorStratix 5700 switches) M12-to-RJ45 patchcord, such as Allen-Bradley® catalog number 1585D-M4TBJM-2

For 1783-BMS4S2SGL or 1783-BMS4S2SGA switches, you also need a Gigabit copper SFP module, such as Allen-Bradley catalog number 1783-SFP1GSX, or a Gigabit fiber-to-Ethernet media converter.

Before you begin, do the following:

- Single-mode Express Setup or multi-mode Express Setup in Short Press mode:
  - Disable other networks in your system.
  - Set your computer to determine its IP address automatically versus statically.
  - Disable static DNS servers.
- Disable any wireless interface on your computer.
- Disable browser proxy settings.
- Make sure at least one switch Ethernet port is available for Express Setup.

  IMPORTANT For catalog numbers 1783-BMS4S2SGL and 1783-BMS4S2SGA, you must use port Gi1/1 for Express Setup.

  Do not use the console port for Express Setup.

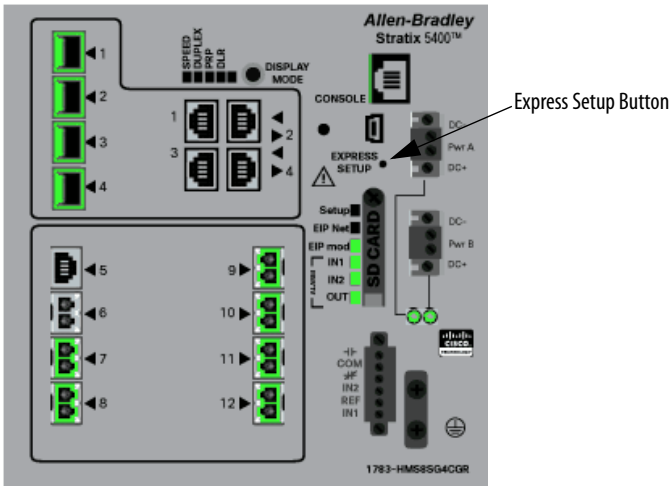
- For Stratix 5700 or ArmorStratix 5700 switches, make sure that the SD card is **not** inserted.

Express Setup Button

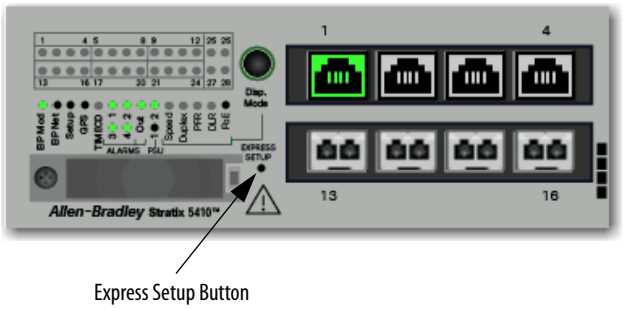
Use the Express Setup button on the physical switch to perform Express Setup. This Express Setup button is recessed behind the panel. To reach the button, use a small tool, such as a paper clip.

WARNING: When you press the Express Setup button while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

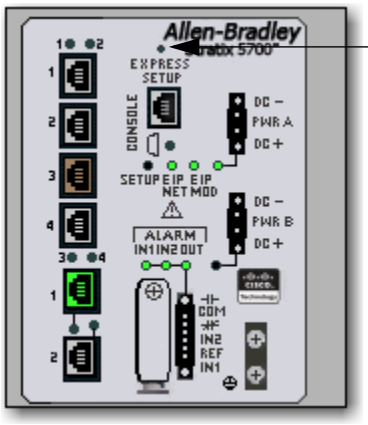
Stratix 5400 Switch



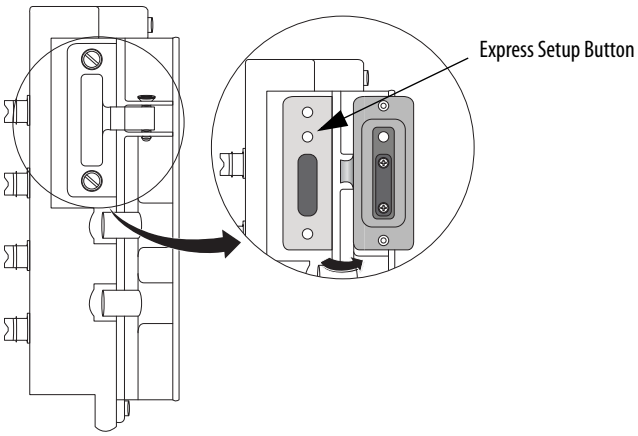
Stratix 5410 Switch



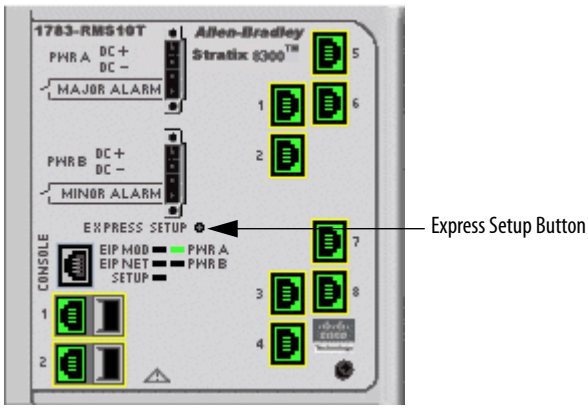
Stratix 5700 Switch



ArmorStratix 5700 Switch



Stratix 8000/8300 Switch



Multi-mode Express Setup

Multi-mode Express Setup has three modes:

IMPORTANT The Studio 5000 Logix Designer® application supports only Medium-press mode.

- Short Press mode—You want to use Express Setup to enter the initial IP address of the switch. You can then configure additional network settings via Device Manager. To run Short Press mode, see page 35.
- Medium Press mode—You want to use a DHCP server to assign the switch an IP address. You can then configure additional network settings via Device Manager or the Logix Designer application. To run Medium Press mode, see page 36.
- Long Press mode—You want to reset the switch to use factory default settings. To run Long Press mode, see page 37.

Table 10 summarizes the function of each mode.

Table 10 - Mulit-mode Express Setup Modes

Attribute	Short Press Mode	Medium Press Mode	Long Press Mode
Enable method	Press and hold the Express Setup button until the Setup status indicator flashes green during seconds 1…5, and then release.	Press and hold the Express Setup button until the Setup status indicator flashes red during seconds 6…10, and then release.	Press and hold the Express Setup button until the Setup status indicator flashes alternating green and red during seconds 16…20, and then release.
		Between seconds 11…15 and after 21 seconds, the Setup status indicator turns off. If you release the Express Setup button while the Setup status indicator is off, no Express Setup mode is enabled.	
Setup status indicator	Flashes green between seconds 1…5.	Flashes red between seconds 6…10.	Flashes green and red between seconds 16…20.
Function	• The Express Setup management interface is selected. • The switch acts as a DHCP server on VLAN 1000 with an address of 169.254.0.1. • Once the DHCP session is successfully established, the switch assigns the computer an IP address of 169.254.0.2 on VLAN 1000. • The default login credentials are set to the following: – User name: [no user name/blank] – Password: **switch** • Express Setup parameters are completed via Device Manager.	• A DHCP client request is sent out of all switch ports on VLAN 1. • VLAN 1 is configured for the IP address returned by DHCP. • The default login credentials are set to the following: – User name: [no user name/blank] – Password: **switch** • CIP is enabled on VLAN 1 with the CIP security password set to **switch**. • Express Setup parameters are completed via Device Manager or the Logix Designer application.	• All configuration settings (config.text, vlan.dat, and private-config.text files) in internal memory or on the SD card or CompactFlash card are reset to factory defaults. • The switch restarts with factory default settings.

Run Multi-mode Express Setup in Short Press Mode

Be aware of the following conditions that cause the switch to exit Short Press mode.

Condition	Status Indicator Behavior
A non-default configuration exists on the switch.	The Setup status indicator turns red for 10 seconds.
You do not connect to the Express Setup port within 2 minutes from when the port status indicator flashes green.	The unconnected port status indicator and the Setup status indicator turn off.
No DHCP request is received for 2 minutes from when you connect to the Express Setup port.	The Setup status indicator turns red for 10 seconds.
No browser session is started for 2 minutes after an IP address is assigned to the computer.	The unconnected port status indicator and the Setup status indicator turn off.
You disconnect your computer from the switch before the setup process is complete.	All temporary configurations that are applied by Express Setup, such as DHCP server, are removed.

To run multi-mode Express Setup in Short Press mode, follow these steps.

1. Apply power to the switch.

   When the switch powers on, it begins its power-on sequence. The power-on sequence can take as many as 90 seconds to complete.

2. Make sure that the power-on sequence has completed by verifying that the EIP Mod and Setup status indicators are flashing green.

   If the switch fails the power-on sequence, the EIP Mod status indicator turns red.

   If you do not press the Express Setup button within 5 minutes after the power-on sequence is complete, the Setup status indicator turns off. However, you can still run Express Setup after the Setup status indicator turns off.

3. Press and hold the Express Setup button until the Setup status indicator flashes green during seconds 1...4, and then release.

   The switch selects a port to use for Express Setup.

4. Connect a Category 5 Ethernet cable from the flashing switch port to the Ethernet port on a computer.

   or

   For 1783-BMS4S2SGL or 1783-BMS4S2SGA switches, do one of the following:

   - Insert a copper SFP module into the Gi1/1 port on the switch. Then connect a Category 5 Ethernet cable from the SFP module to the Ethernet port on the computer.
   - Connect the Gi1/1 port on the switch to the Ethernet port on the computer by using a fiber-to-Ethernet media converter.

   IMPORTANT Port Gi1/1 does not flash during setup, but must be used to connect 1783-BMS4S2SGL or 1783-BMS4S2SGA switches to a computer.

   Once you connect the switch to the computer, the following occurs:

   - The status indicator for the port connected to the computer changes from flashing green to solid green.
   - The switch acts as a DHCP server on VLAN 1000 with an address of 169.254.0.1.

   IMPORTANT The IP address of the switch for multi-mode Express Setup is different than the IP address for single-mode Express Setup.

   - The switch assigns the computer an IP address of 169.254.0.2 on VLAN 1000.
   - The Setup status indicator changes from flashing green to solid green.

5. Proceed to Configure Network Settings via Device Manager on page 39.

Run Multi-mode Express Setup in Medium Press Mode

Be aware of the following conditions that cause the switch to exit Medium Press mode.

Condition	Status Indicator Behavior
A non-default configuration exists on the switch.	The Setup status indicator turns red for 10 seconds.
No DHCP response is received for 10 minutes from when the switch broadcast the request.	

IMPORTANT Before you begin, make sure that your system has a DHCP server configured to assign the switch an IP address. You can configure a switch to be a DHCP server, as described on page 238.

To run multi-mode Express Setup in Medium Press mode, follow these steps.

1. Apply power to the switch.

   When the switch powers on, it begins its power-on sequence. The power-on sequence can take as many as 90 seconds to complete.

2. Make sure that the power-on sequence has completed by verifying that the EIP Mod and Setup status indicators are flashing green:
   - If the switch fails the sequence, the EIP Mod status indicator turns red.
   - If you do not press the Express Setup button within 5 minutes after the sequence completes, the Setup status indicator turns off.

3. Press and hold the Express Setup button until the Setup status indictor flashes red during seconds 6...10, and then release:

   IMPORTANT You must complete the switch setup within 10 minutes of releasing the Express Setup button. Otherwise, the switch exits Express Setup.

   - The Setup status indicator flashes green during seconds 1...5, and then red during seconds 6...10.
   - The switch broadcasts a DHCP request out of all ports on VLAN 1.
   - VLAN 1 is configured with the IP address returned by the DHCP server.
   - The default login credentials are set to the following:
     - User name: [no user name/blank]
     - Password: **switch**
   - CIP is enabled on VLAN 1 with CIP security password set to **switch**.

4. Configure network settings:
   - To complete the configuration via Device Manager, see page 39.
   - To complete the configuration via the Logix Designer application, see page 42.

Run Multi-mode Express Setup in Long Press Mode

IMPORTANT Long Press mode overwrites all existing configuration files in internal or external memory and resets the switch to use factory default settings.

Press and hold the Express Setup button until the Setup status indicator flashes alternating green and red during seconds 16...20, and then release.

Upon release of the Express Setup button, the switch restarts with factory default settings.

Single-mode Express Setup

To run single-mode Express Setup, follow these steps.

1. Make sure that at least one switch Ethernet port is available for Express Setup.
2. Apply power to the switch.

   When the switch powers on, it begins its power-on sequence. The power-on sequence can take up to 90 seconds to complete.
3. Make sure that the power-on sequence has completed by verifying that the EIP Mod and Setup status indicators are flashing green.

   If the switch fails the power-on sequence, the EIP Mod status indicator turns red.
4. Press and release the Express Setup button.

   Unlike multi-mode Express Setup, there is no time requirement for when you release the Express Setup button.
5. Wait a few seconds until the status indicator on one of the unconnected switch ports flashes green.
6. Connect a Category 5 Ethernet cable from the flashing switch port to the Ethernet port on a computer.

   or

   For 1783-BMS4S2SGL or 1783-BMS4S2SGA switches, do one of the following:
   - Insert a copper SFP module into the Gi1/1 port on the switch. Then connect a Category 5 Ethernet cable from the SFP module to the Ethernet port on the computer.
   - Connect the Gi1/1 port on the switch to the Ethernet port on the computer by using a fiber-to-Ethernet media converter.

   IMPORTANT Port Gi1/1 does not flash during setup, but must be used to connect 1783-BMS4S2SGL or 1783-BMS4S2SGA switches to a computer.

   IMPORTANT If you wait too long to connect the cable, the Setup status indicator turns off.
7. Proceed to Configure Network Settings via Device Manager on page 39.

Configure Network Settings via Device Manager

To configure network settings via Device Manager after you run Express Setup, follow these steps.

1. Access Device Manager, as described on page 48.

   If the Express Setup window does not appear, try the following:

   - Verify that your network adapter is set to accept a DHCP address
   - Enter the URL of a well-known website in your browser to be sure that the browser is working correctly. Your browser then redirects to Express Setup.
   - Verify that any proxy settings or pop-up blockers are disabled on your browser.
   - Verify that any wireless interface is disabled on the computer.

2. On the Express Setup window, complete the fields, as described in Table 11.

   To view fields for Common Industrial Protocol (CIP), click Advanced Settings.

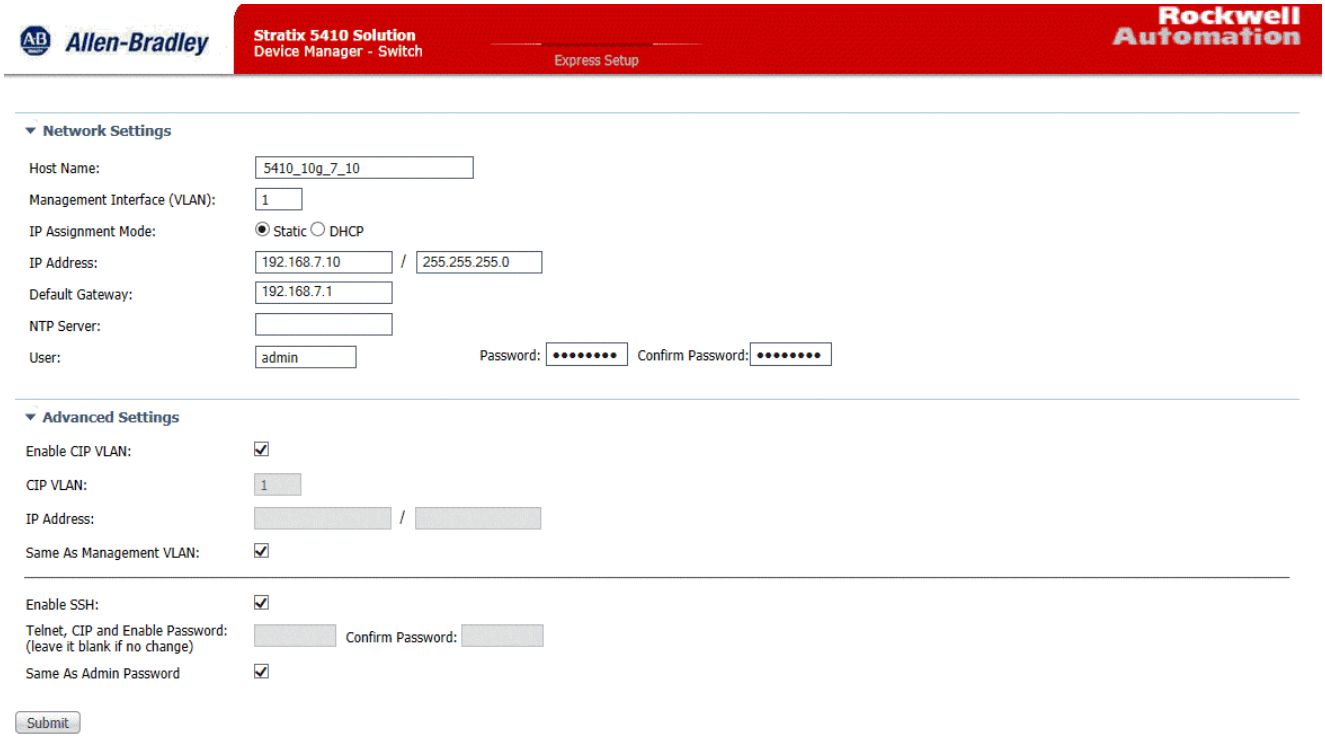


Table 11 - Express Setup Fields

Field	Description
Network Settings	
Host Name	The name of the device.
Management Interface (VLAN ID)	The name and ID of the management VLAN through which the switch is managed. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. It also provides secure administrative access to all devices in the network. Choose an existing VLAN as the management VLAN. The default management VLAN ID is 1 and the VLAN name is default. Valid IDs for single-mode Express Setup: 1…1001 Valid IDs for multi-mode Express Setup: 1…4096 **IMPORTANT:** Be sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch.
IP Assignment Mode	The IP Assignment mode determines whether the switch IP information is manually assigned (static) or is automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you click Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access Device Manager. If you click DHCP, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. Unless restarted, the switch continues to use the DHCP-assigned information, and you are able to use the DHCP-assigned address to access Device Manager. For a manually assigned IP address in a network that uses a DHCP server, make sure that the IP address is not within the range of addresses that the DHCP server assigns. Otherwise, IP address conflicts can occur between the switch and another device.
IP Address	The IP address and associated subnet mask are unique identifiers for the switch in a network: • The IP address format is a 32-bit numeric address that is written as four numbers that are separated by periods. Each number can be from 0…255. • The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The default is 255.255.255.0. **IMPORTANT:** If you run multi-mode Express Setup in Medium Press mode, the IP Address field displays the address received from the DHCP server. If you change the address, the connection drops. To re-establish the connection with the new address, close your web browser and go to the address you specified. Make sure that the IP address that you assign to the switch is not assigned to another device in your network. The IP address and the default gateway cannot be the same.
Default Gateway (optional)	The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address must be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This field is enabled only if the IP assignment mode is Static. If your network management station and the switch are in different networks or subnetworks, you must specify a default gateway. Otherwise, the switch and your network management station cannot communicate with each other.
NTP Server	The IP address of the Network Time Protocol (NTP) server. NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
User	Enter the user name.
Password, Confirm Password (initial setup only)	The password for the switch can have up to 63 alphanumeric characters, can start with a number, is case-sensitive, and can have embedded spaces. The password cannot be one digit, it cannot contain a ? or a tab, and it does not allow spaces at the beginning or the end. The default is **switch**. To complete initial setup, you must change the password from the default password, **switch**. This password is also used as the Control Industrial Protocol (CIP) security password. We recommend that you provide a password to the switch to secure access to Device Manager.
Advanced Settings	
Enable CIP VLAN	Check the checkbox to enable CIP on a VLAN. You can specify the settings required for CIP or check the Same As Management VLAN checkbox.
CIP VLAN	The VLAN on which Common Industrial Protocol (CIP) is enabled. The CIP VLAN can be the same as the management VLAN or you can isolate CIP traffic on another VLAN that is already configured on this device.
IP Address	The IP address and subnet mask for the CPI VLAN if the CIP VLAN differs from the management VLAN. The format is a 32-bit numeric address that is written as four numbers that are separated by periods. Each number can be from 0…255. Make sure that the IP address that you assign to this device is not being used by another device in your network.
Same As Management VLAN	Check the checkbox to make the settings for the CIP VLAN the same as the management VLAN.

Table 11 - Express Setup Fields (Continued)

Field	Description
Enable SSH	Check the checkbox to enable Secure Shell (SSH) sessions on the switch. You can use SSH to access the command-line interface (CLI) for switch configuration. For more information about the CLI, see page 70.
Telnet, CIP and Enable Password (optional), Confirm Password	The password that is used for Telnet and CIP security.
Same As Admin Password	Sets the password that is used for Telnet and CIP security to the same user password specified under Network Settings.

3. Click Submit.

   The switch initializes its configuration for typical industrial EtherNet/IP applications by running the global macro as described on page 43. You can then log on to Device Manager for further configuration or exit the application.

4. Turn off DC or AC power at the source, disconnect any cables to the switch, and install the switch in your network.

   IMPORTANT For 1783-BMS4S2SGL or 1783-BMS4S2SGA switches, make sure that DC power is disconnected before disconnecting Ethernet cables.

5. If you used single-mode Express Setup or multi-mode Express Setup in Short Press mode, refresh the computer IP address:
   - For a dynamically assigned IP address, disconnect the computer from the switch and reconnect the computer to the network. The network DHCP server assigns a new IP address to the computer.
   - For a statically assigned IP address, change it to the previously configured IP address.
6. For Stratix 5400 and Stratix 5410 switches, synchronize the SD card that came with the switch with the internal memory of the switch:
   - To synchronize the SD card via Device Manager, see page 65.
   - To synchronize the SD card via the Logix Designer application, see page 67.

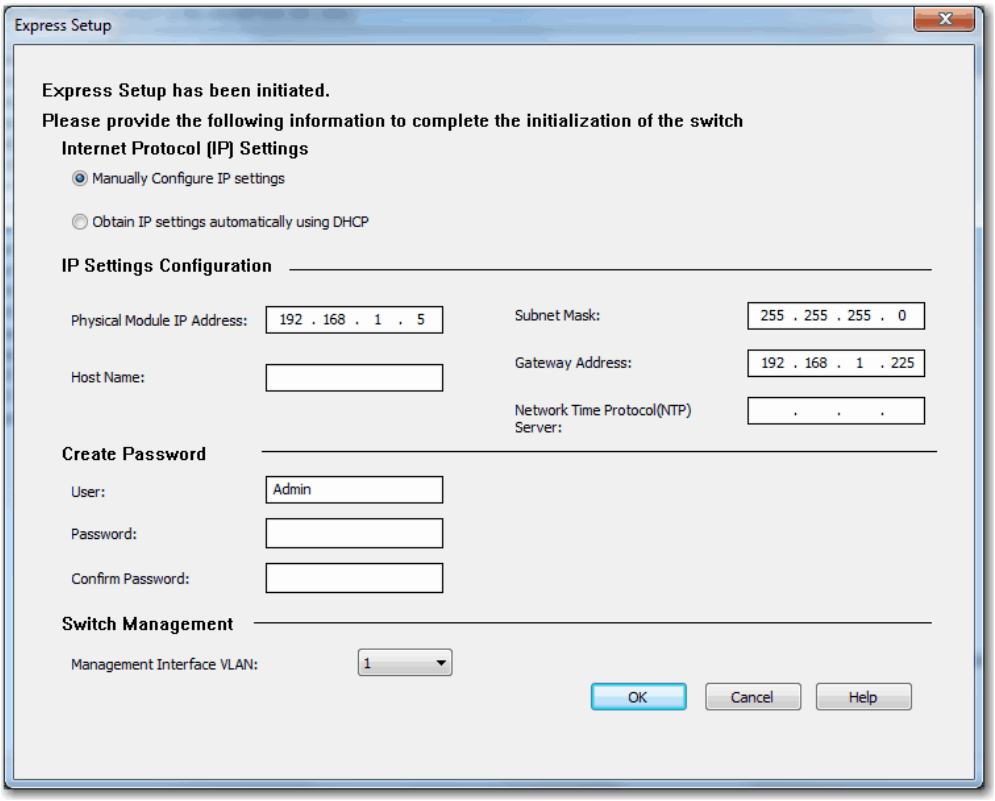
After initial setup with Express Setup, you can change the settings if you want to move the switch to another management VLAN or to another network. To change Express Setup settings after initial setup, from the Admin menu in Device Manager, choose Express Setup.

Configure Network Settings via the Logix Designer Application

To configure network settings via the Logix Designer Application after running multi-mode Express Setup in Medium Press mode, follow these steps.

1. If you have not yet added the switch to a controller project, complete Steps 1...3 on page 53.
2. Configure general properties, as described page 55.

   Be sure to specify the IP address assigned to the switch by the DHCP server.
3. Go online with the controller, and then open the Module Properties dialog box for the switch.
4. In the navigation pane, click Switch Configuration.
5. When the Express Setup dialog box appears, complete the fields.



Field	Description
Internet Protocol (IP) Settings	Click the method to use for assigning the swtich an IP address: • Manually Configure IP settings (default)—The switch uses a manually-assigned, static IP address. If you manually assign the IP address of the switch and your network uses a DHCP server, make sure that the IP address is not within the range of addresses that the DHCP server assigns. Otherwise, IP address conflicts can occur between the switch and another device. • Obtain IP settings automatically using DHCP—A Dynamic Host Configuration Protocol (DHCP) server automatically assigns the switch an IP address, subnet mask, and default gateway. Unless restarted, the switch continues to use the DHCP-assigned information.
Physical Module IP Address	Displays the IP address assigned to the switch by the DHCP server during Express Setup. This value must match the IP address on the General view. If you change the assigned IP address, make sure that the new IP address is not assigned to another device in your network. The IP address and the default gateway cannot be the same. **IMPORTANT:** If you reconfigure your switch with another IP address, you can lose communication with the switch when you click Set. To correct this problem, you must return to the Express Setup and General view, set the new IP address, and download to the controller.

Field	Description
Subnet Mask	Displays the IP address assigned to the switch by the DHCP server during Express Setup. The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The subnet mask is a 32-bit number. Set each octet between 0…255. The default is 255.255.255.0.
Host Name	Type a name to identify the switch. The name can be up to 64 characters and can include alphanumeric and special characters (comma and dash).
Gateway Address	Displays the gateway address assigned to the switch by the DHCP server during Express Setup. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address must be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This field is enabled only if the IP assignment mode is Static. If your network management station and the switch are in different networks or subnetworks, you must specify a default gateway. Otherwise, the switch and your network management station cannot communicate with each other. **IMPORTANT:** Communication is disrupted when you change the gateway (IP) address.
Network Time Protocol (NTP) Server	(Optional). Type the IP address of the NTP server. NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
User	Displays the default user name: **Admin**
Password, Confirm Password	The password for the switch can have up to 63 alphanumeric characters, can start with a number, is case-sensitive, and can have embedded spaces. The password cannot be one digit, it cannot contain a ? or a tab, and it does not allow spaces at the beginning or the end. The default password is **switch**. To complete initial setup, you must change the password from the default password. This password is also used as the Control Industrial Protocol (CIP) security password. You must provide a password to the switch to secure access to Device Manager.
Management Interface (VLAN)	Choose a management VLAN. The default management VLAN ID is 1. The management VLAN through which the switch is managed. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. It also provides secure administrative access to all devices in the network. **IMPORTANT:** Be sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch.

6. Click OK.

   The switch initializes its configuration for typical industrial EtherNet/IP applications by running the global macro as described on page 43. You can then use the AOP for further configuration or exit the application.

7. Turn off DC or AC power at the source, disconnect any cables to the switch, and install the switch in your network.

   IMPORTANT For 1783-BMS4S2SGL or 1783-BMS4S2SGA switches, make sure that DC power is disconnected before disconnecting Ethernet cables.

8. For Stratix 5400 and Stratix 5410 switches, synchronize the SD card that came with the switch with the internal memory of the switch, as described on page 67.

Default Global Macro

Once you complete Express Setup, the switch runs a default global macro (ab-global). This macro configures the switch for industrial automation applications that use the EtherNet/IP protocol. This macro sets many parameters, including these major settings:

- Enable IGMP snooping and querier
- Enable CIP
- Enables alarms, SYSLOG, and SNMP notifications
- Enables Rapid Spanning Tree (RSTP), BPDU Guard, BPDU Filter, and loop guard
- Configure Quality of Service (QoS) settings and classify CIP, PTP, and other traffic (does not apply to switches with lite firmware revisions)

IMPORTANT The default QoS setting applied by the default global macro assigns the same priority to traffic for CIP and traffic for Integrated Motion on the EtherNet/IP network applications. However, you can assign a higher priority to motion traffic by manually applying optional QoS macros after you run Express Setup. For more information, see page 248.

If you do not run Express Setup to initialize the switch, the global macro does not run. You can use the CLI, described on page 70, to run the global macro.

RSLinx Software and Network Who Support

The EtherNet/IP network interface also supports the List Identity command that is used by CIP-based network tools, such as the RSLinx® software RSWho function. RSWho enables you to locate and identify your switch on the network by using the electronic data sheet (EDS) files.

To access the RSWho function, from the RSLinx software toolbar, choose Communications > RSWho.

IMPORTANT After using the RSWho function, if you access the switch and view the Ethernet link counters, you see the counts for only the first port (Port Gi1/1).

Electronic Data Sheet (EDS) Files

Electronic Data Sheet (EDS) files are text files that are used by network configuration tools, such as RSNetWorx™ for EtherNet/IP software. EDS files help you identify products and commission them on a network. EDS files contain details about the readable and configurable parameters of the device. They also provide information about the I/O connections the device supports and the content of the associated data structures.

If you are using the switch in a system without a Rockwell Automation Logix controller, you cannot use the AOP supplied with Logix controllers. You must use information from the EDS files to configure the I/O connection.

EDS files for the Stratix switches are included with the following software packages:

- RSLinx software
- RSLogix 5000® software
- RSNetWorx for EtherNet/IP software

You can also obtain the EDS files in either of these two ways:

- By downloading it from http://www.rockwellautomation.com/resources/eds/.
- By using the RSLinx EDS Hardware Installation tool.

To upload the EDS files directly from the switch over the network, follow these steps.

1. From the Start menu, choose Programs > Rockwell Software >RSLinx >Tools > EDS Hardware Installation Tool.
2. To launch the EDS Wizard and add the selected hardware description and associated files, click Add.

Data Accessible with CIP

The CIP interface lets you access the information in Table 12.

Table 12 - Data Accessible with CIP

Data Type	Details
Input data via I/O connection	• Link status per port: not connected, connected • Unauthorized device per port: OK, not OK • Unicast threshold exceeded per port: OK, exceeded • Multicast threshold exceeded on each port: OK, exceeded • Broadcast threshold exceeded on each port: OK, exceeded • Port bandwidth utilization per port: value in % • Alarm relay major: OK, tripped • Multicast groups active: quantity
Output data via I/O connection	Port disable per port: enabled, disabled

Table 12 - Data Accessible with CIP (Continued)

Data Type	Details
Other status data	• Module identification (vendor ID, device type, product code, product name, revision, serial number) • Major/minor fault status, I/O connection, module identity match • Active alarms • Major alarm relay (open, closed) • Active faults • Switch uptime since last restart • Switch internal temperature in degrees Centigrade • Management CPU utilization in percentage • Power supply A present: yes, no • Power supply B present: yes, no • Number of active multicast groups • IOS release version • DLR ring status, members, and faults • CIP connection counters: open/close requests, open/close rejects, timeouts • Port alarm status per port: OK, Link Fault, Not Forwarding, Not Operating, High Bit Error Rate • Port fault status per port: Error Disable, SFP Error, Native VLAN Mismatch, MAC address Flap Condition, Security Violation • Port diagnostic counters per port: Ethernet interface counters (10), Ethernet media counters (12) • Link status • Traffic threshold exceeded per port: unicast, multicast, broadcast • Cable diagnostics per port selected • DHCP pool display: name, starting and ending IP address • NAT: display name of instance, VLANs assigned per instance • NAT diagnostics: active translations, total translated packets, blocked and pass-through traffic, ICMP and ARP fixups
Configuration data	• Major and minor revision of switch • Electronic keying (Exact Match, Disable Keying) • Connection (Input Data, Data) • Data connection password • Requested packet interval (RPI) • Inhibit module • Major fault on controller if connection fails while in Run mode • Use unicast connections over EtherNet/IP • Module fault display • IP addressing method: Manual, DHCP • IP address, subnet mask, primary and secondary DNS server address, default gateway (all if static) • Host name • Administration: contact name, geographic location • Spanning Tree Mode (MST, RSTP, PVST+, RPVST+) • Dual-power supply alarm enable • Port configuration per port: enable/disable, auto-negotiate, speed, duplex • Power over Ethernet (PoE): mode, status, power limit, power used, total power supported, total power used, remaining power available • Smartports and VLANs: assign roles per port, VLAN ID and name • Port thresholds (incoming: unicast, multicast, broadcast, all outgoing traffic) rate limiting threshold per port: in packets per second, bits per second, or percentage • Port security: enable, allowed MAC IDs per port, dynamic, static • DHCP pool: enable, delete, refresh, create • DHCP address assignment per port • Time sync configuration: enable per port, port state • NAT configuration: create instance (private-to-public, public-to-private, traffic permits, and fixups)
Smartport assignment per port	• Role • VLAN
Save and restore of switch configuration	Via File Obj

Configuration via Device Manager

Device Manager is a web-based management tool for configuring, monitoring, and troubleshooting individual switches. You can display Device Manager from anywhere in your network through a web browser.

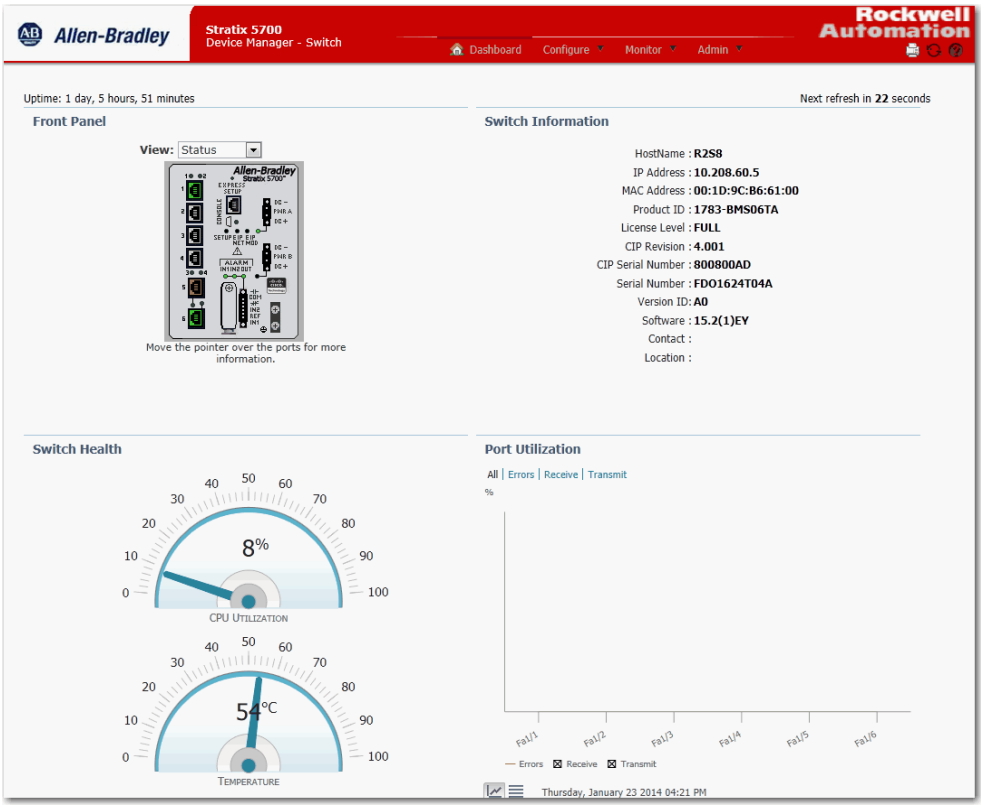
Device Manager displays real-time views of switch configuration and performance. It simplifies configuration tasks with features such as Smartports. It uses graphical, color-coded displays, such as the front panel view, graphs, and animated indicators to simplify monitoring tasks. It provides alert tools to help you to identify and to solve networking problems.

Table 13 - Device Manager Hardware Requirements

Attribute	Requirement
Processor speed	1 GHz or faster (32 bit or 64 bit)
RAM	1 GB (32 bit) or 2 GB (64 bit)
Available hard disk space	16 GB (32 bit) or 20 GB (64 bit)
Number of colors	256
Resolution	1024 x 768
Font size	Small

Table 14 - Device Manager Software Requirements

Web Browser	Version
Microsoft Internet Explorer	Latest version with JavaScript enabled
Mozilla Firefox	Latest version with JavaScript enabled



Access Device Manager

With IOS version 15.2(5)EA.fc4 and later, Device Manager provides a secure connection via the latest version of Internet Explorer or Firefox. Security messages from your browser can appear when you access Device Manager.

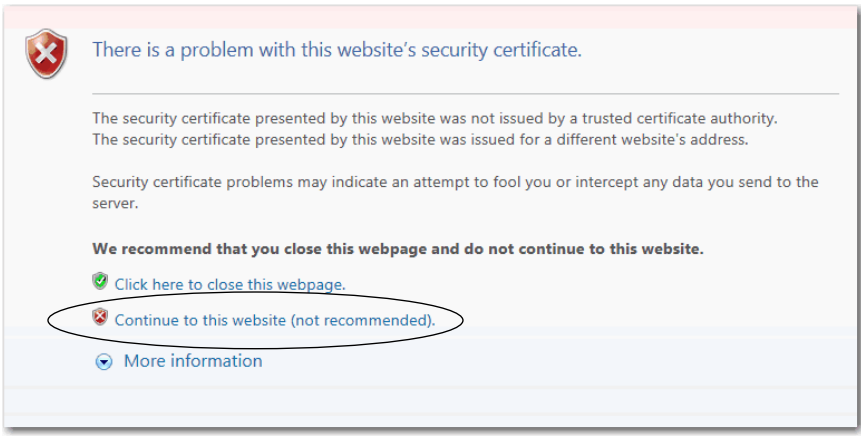
To make sure that Device Manager runs properly, disable any pop-up blockers or proxy settings in your browser and any wireless clients on your computer. Device Manager verifies the browser version when starting a session to be sure that the browser is supported.

To access Device Manager, follow these steps.

1. Start a web browser session and go to the switch IP address.

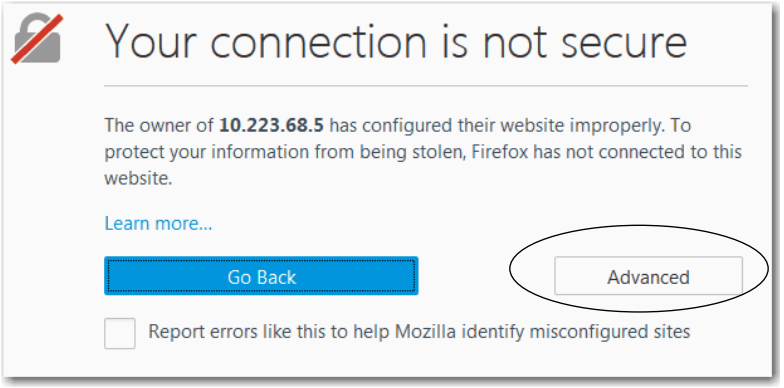
   IMPORTANT If you set up bookmarks for accessing previous versions of Device Manager, be sure to recreate new bookmarks. Addresses that end with /homed.shtml do not provide the latest login authentication method.

2. (Internet Explorer). If the following message appears, click Continue to this website.

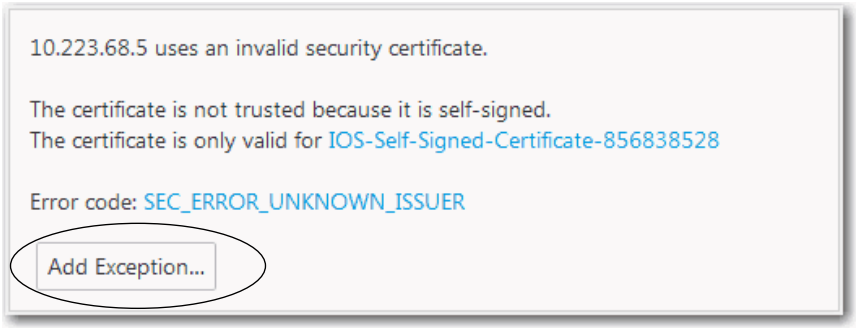


   (Firefox). If the following message appears, do the following:

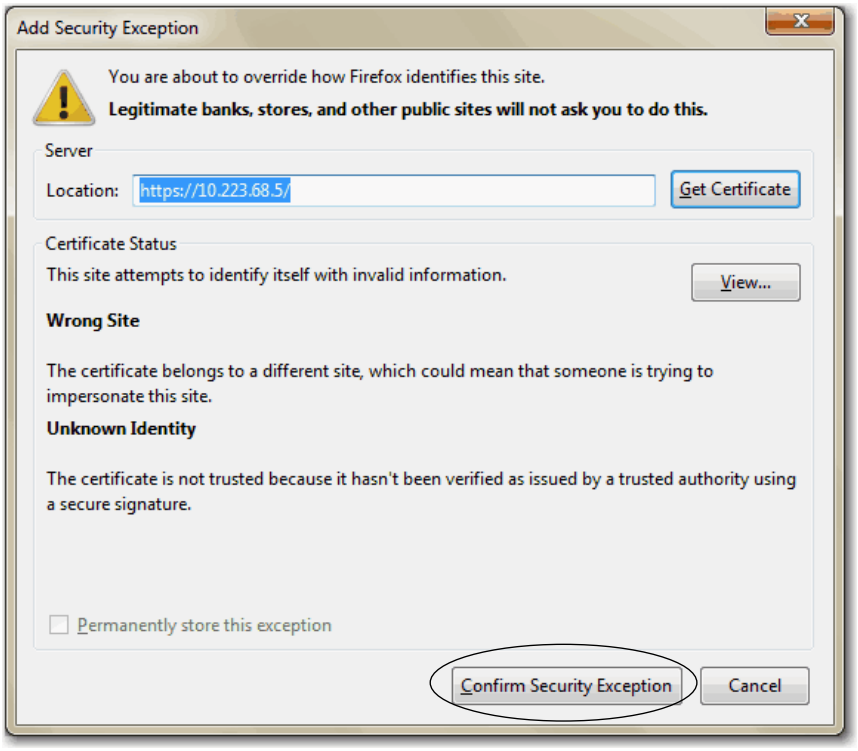
   a. Click Advanced.



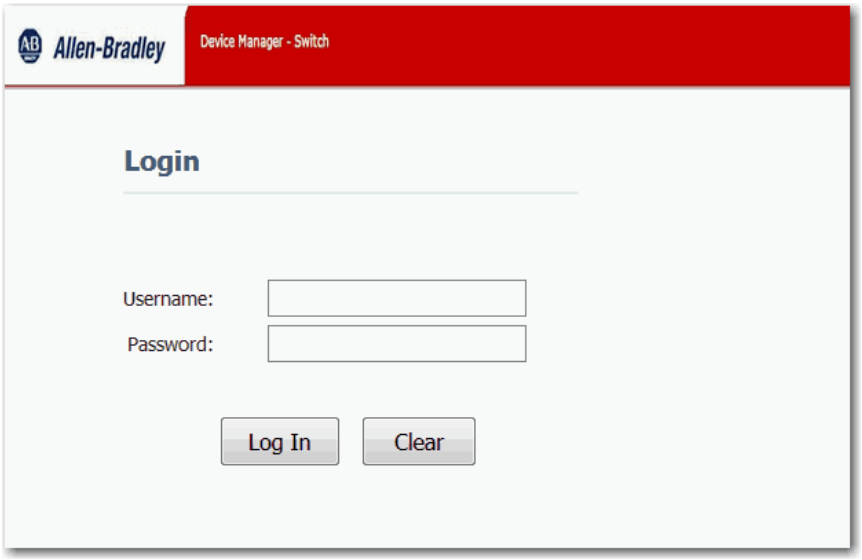
   b. Click Add Exception.



c. Click Confirm Security Exception.



3. On the Device Manager Login window, enter the switch name and password.



Configure Port Settings

The basic port settings determine how data is received and sent between the switch and the attached device. You can change these settings to fit your network needs and to troubleshoot network problems. The settings on a switch port must be compatible with the port settings of the connected device.

To change basic port settings, from the Configure menu, choose Port Settings.

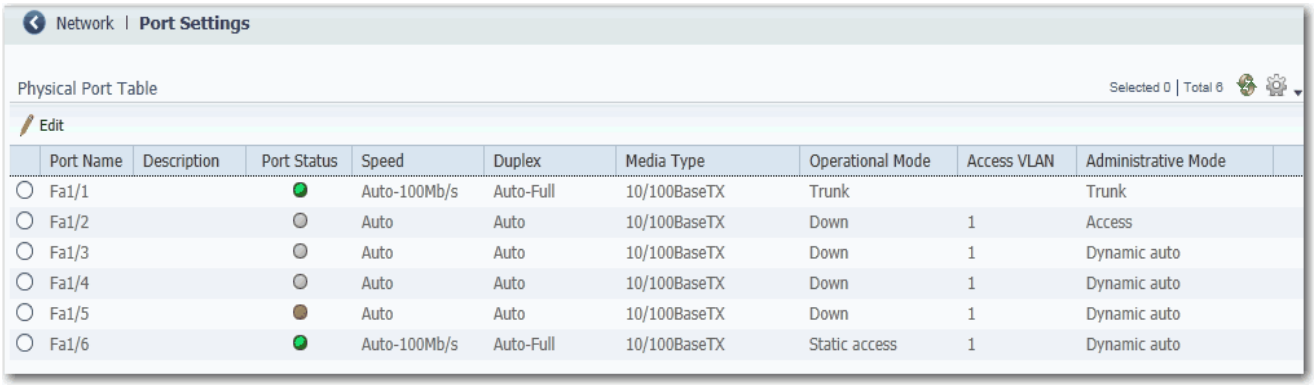


Table 15 lists the basic settings for the switch ports. To change these settings, click the radio button next to the port name and click Edit to display the Edit Physical Port window.

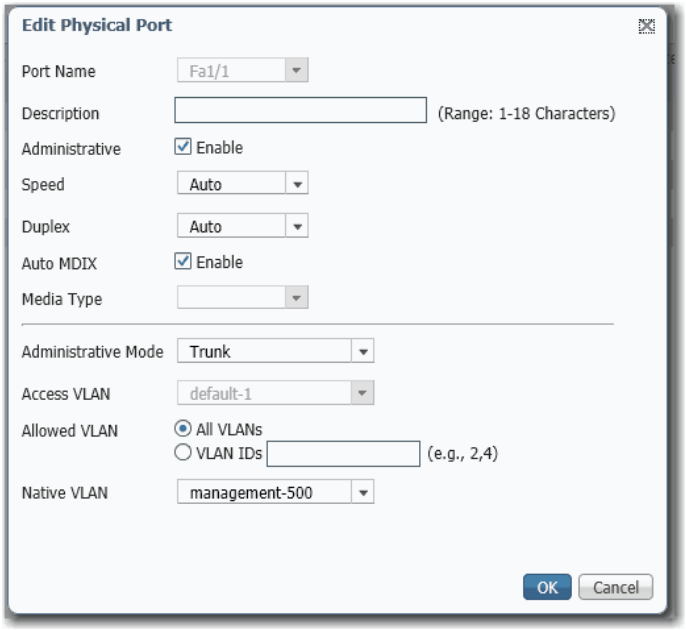


Table 15 - Port Settings

Field	Description
Port Name	The number of the switch port, including port type, such as Fa for Fast Ethernet and Gi for Gigabit Ethernet, and the specific port number: • Gi/1 is the gigabit port 1 of the switch. • Fa1/1 is Fast Ethernet port 1 on the switch.
Description	The description of the switch port. We recommend that you provide a port description to help identify the port during monitoring and troubleshooting. The description can be the location of the connected device or the name of the person using the connected device.
Port Status	The state of the switch port. The default is Enabled. You can change this setting on the Edit Physical Port window by checking or clearing the Administrative checkbox. We recommend disabling the port if the port is not in use and is not attached to a device. An example of when to change this setting is during troubleshooting. You can troubleshoot a suspected unauthorized connection by administratively disabling the port.
Speed	The operating speed of the switch port. You can choose Auto (autonegotiation) if the connected device can negotiate the link speed with the switch port. The default is Auto. We recommend that you use the default so that the speed setting on the switch port automatically matches the setting on the connected device. Change the switch port speed if the connected device requires a specific speed. An example of when to change this setting is during troubleshooting. If you are troubleshooting a connectivity problem, you can change this setting to see if the switch port and connected device have a speed mismatch.
Duplex	The Duplex mode of the switch port: • Auto (autonegotiation) if the connected device can negotiate with the switch. • Full (Full-duplex mode) if both devices can send data simultaneously. • Half (Half duplex mode) if one or both devices cannot send data simultaneously. The default is Auto. On Gigabit Ethernet ports, you cannot set the port to Half-duplex mode if the port speed is set to Auto. We recommend that you use the default so that the duplex setting on the switch port automatically matches the setting on the connected device. Change the Duplex mode on the switch port if the connected device requires a specific mode. An example of when to change this setting is during troubleshooting. If you are troubleshooting a connectivity problem, you can change this setting to verify if the switch port and connected device have a duplex mismatch.
Auto-MDIX	Whether the automatic medium-dependent interface crossover (auto-MDIX) feature can automatically detect the required cable connection type (straight-through or crossover) and configure the connection appropriately. The default is Enable. This setting is not available on the SFP module ports.
Media Type	The active port type (either the RJ45 port or the SFP module port) of a dual-purpose uplink port. By default, the switch detects whether the RJ45 port or SFP module port of a dual-purpose port is connected and uses the port accordingly. Only one port can be active at a time. If both ports are connected, the SFP module port has priority. You cannot change the priority setting. Choose from the following media types: • SFP—The SFP module port is active. If you choose this option, the speed and duplex displays the current settings and auto-MDIX displays N/A. • RJ45—The RJ45 port is active. If you choose this option, you can set the port speed, duplex, and auto-MDIX values. • Auto (autonegotiation)—Either port can be active. If you choose this option, the speed and duplex is set to auto and auto-MDIX displays N/A. The default is Auto.
Operational Mode	The operational state of the port. Displays the administrative mode or Down (if disabled).
Access VLAN	The VLAN that an interface belongs to and carries traffic for, when the link is configured as or is acting as a nontrunking interface.
Administrative Mode	Displays one of the following administrative modes: • Access—The interface is in permanent nontrunking mode and negotiates to convert the neighboring link into a nontrunk link even if the neighboring interface is a trunk interface. If you choose this option, also choose an Access VLAN. An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). • Trunk—The interface is in permanent trunking mode and negotiates to convert the neighboring link into a trunk link even if the neighboring interface is not a trunk interface. If you choose this option, also choose whether to allow All VLANs or specified VLAN IDs. • Dynamic Auto—The interface converts the link to a trunk link if the neighboring interface is set to trunk or desirable mode. This mode is the default setting. If you choose this option, specify an Access VLAN to use when the link is in access mode. Also specify whether to allow All VLANs or specified VLAN IDs when the link is in trunk mode. • Dynamic Desirable—If the neighboring interface is set to Trunk, Dynamic Desirable, or Auto mode, the interface converts the link to a trunk link. If you choose this option, specify an Access VLAN to use when the link is in access mode. Also choose whether to allow All VLANs or specified VLAN IDs when the link is in Trunk mode. • Routed—The interface acts like a port on a router but does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as DTP and STP. Routed ports are supported only on switches running the IP base or IP services image. The default setting is Dynamic Auto.

Configuration via the Studio 5000 Environment

You can manage the switch by using the Logix Designer application in the Studio 5000® environment. The Logix Designer application is IEC 61131-3 compliant and offers relay ladder, Structured Text, function block diagram, and sequential function chart editors for you to develop application programs.

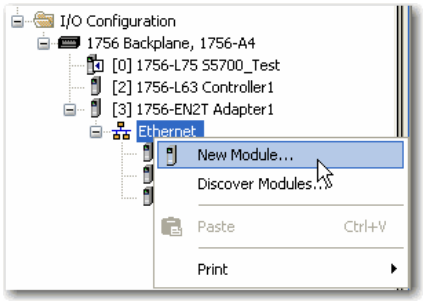
Table 16 - Logix Designer Hardware Requirements

Attribute	Requirement
Processor speed	Pentium II 450 MHz min Pentium III 733 MHz (or better) recommended
RAM	128 MB min 256 MB recommended
Free hard disk space	3 GB
Optical drives	DVD
Video requirements	256-color VGA graphics adapter 800 x 600-min resolution (True Color 1024 x 768 recommended)
Resolution	800 x 600-min resolution (True Color 1024 x 768 recommended)

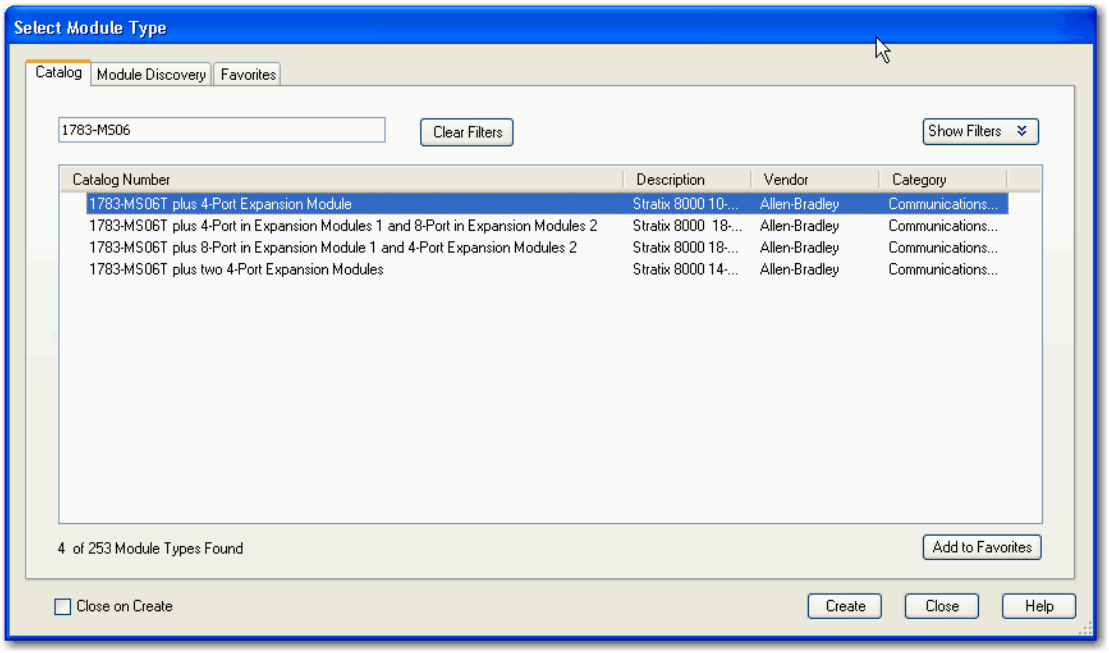
To add the switch to a controller project in the Logix Designer application, follow these steps.

IMPORTANT These steps are required before you can go online to configure and monitor the switch. You must be online to view and configure most switch parameters in the Logix Designer application.

1. Open the project file for the controller to monitor the switch.
2. Right-click Ethernet and choose New Module.



3. On the Select Module Type dialog box, select the switch and click Create.

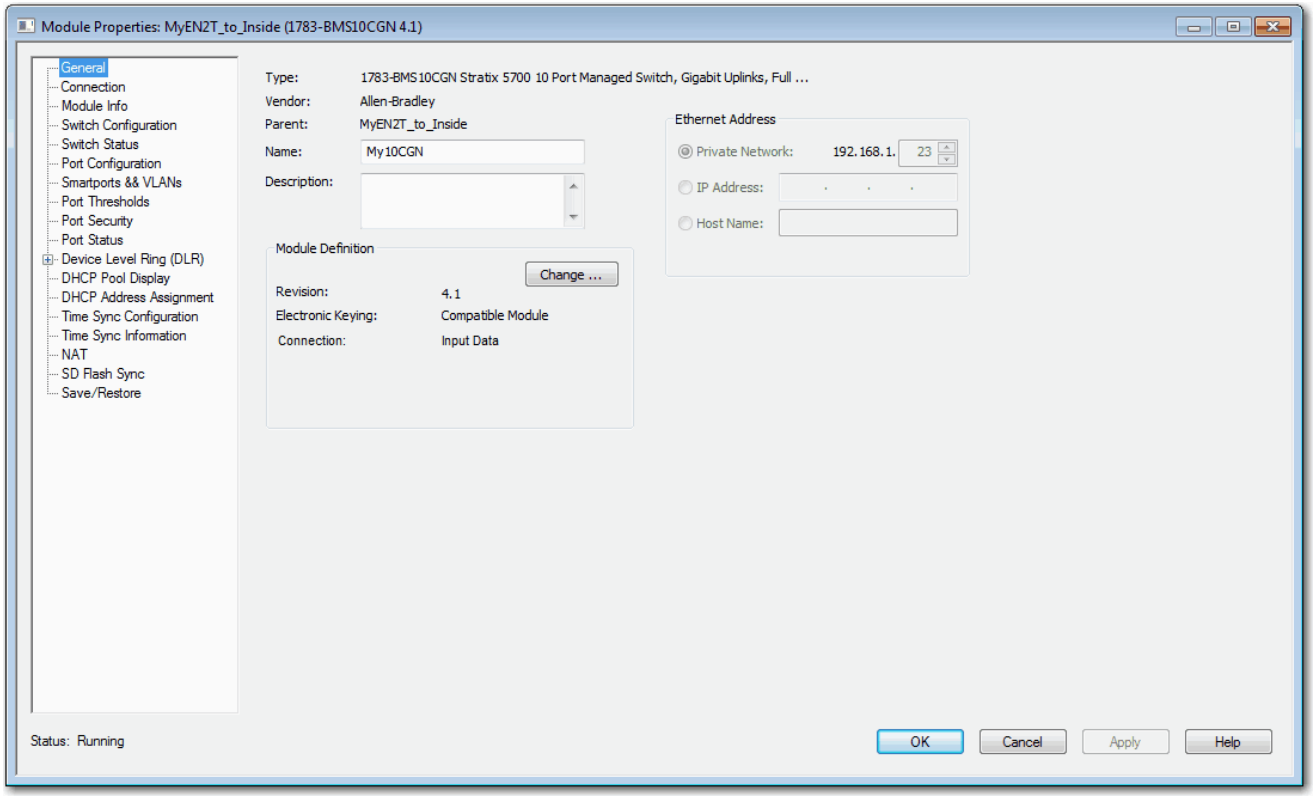


If you do not see the switch on the list, you can obtain the AOP from the Rockwell Automation support website: http://www.rockwellautomation.com/support/

General Properties

To configure general properties, follow these steps.

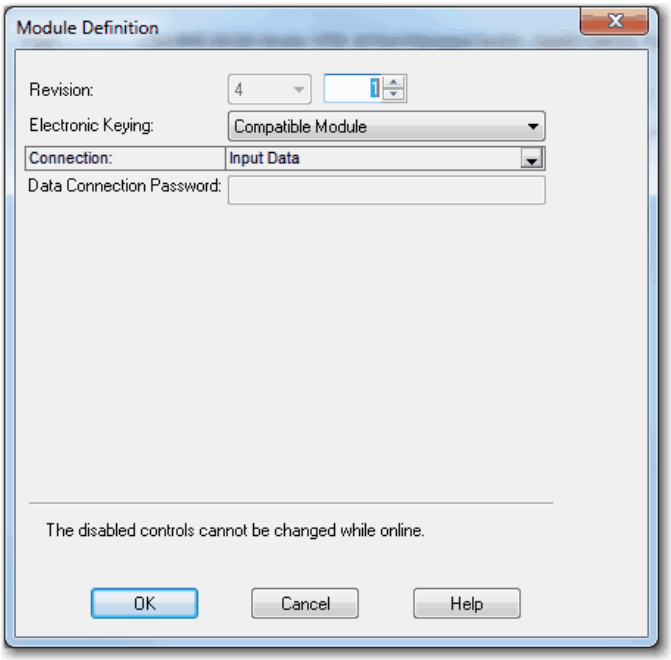
1. In the navigation pane, click General and complete the fields.



IMPORTANT Make sure that the IP address and host name match the values you used during Express Setup. On the Module Properties dialog box, you can choose either an IP address or host name. Only one of these two choices is enabled.

Field	Description
Name	A name that you choose for the switch.
Description	A description that helps you remember something important about the switch.
Ethernet Address	Choose one of the following: • Private Network—The IP address of your private network. • IP Address—The IP address assigned to the switch during Express Setup. • Host Name—The host name that is provided on initial configuration when you performed Express Setup. The host name requires that you have a DNS server that is configured on the network for the Ethernet interface module of the controller.

2. In the Module Definition area, click Change.
3. On the Module Definition dialog box, complete the fields and click OK.



Field	Description
Revision	The major and minor revision of the switch: • Major revision: 1…128 • Minor revision: 1…255
Electronic Keying	Choose one of the following: • Compatible Module (default) • Exact Match • Disable Keying
Connection	Choose one of the following: • Input Data (default): Enables only an input data connection. • Data: Enables an input and output data connection. **ATTENTION:** This selection enables output tags, which can disable ports and interrupt connections to and through the switch. You can disable a switch port by setting the corresponding bit in the output tag. The output bits are applied every time that the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied. If the corresponding output bit is 0, the port is enabled. If you enable or disable a port by using Device Manager or the CLI, the port setting can be overridden by the output bits from the controller on the next cyclic update of the I/O connection. The output bits always take precedence, regardless of whether the Device Manager Web interface or CLI was used to enable or disable the port.
Data Connection Password	(Data connections only). Enter the password for accessing the switch.
Switch Base (Stratix 8000/8300 switches)	Displays the switch base catalog number for the selected module.
Switch Expansion 1 (Stratix 8000/8300 switches)	(14, 18, 22 and 26 port switches only). The catalog number for the copper or fiber expansion modules you are using. For 14 and 18-port switches, user selection of the expansion module is supported. For 22 and 26-port switches, Switch Expansion 1 displays 1783-MX08T. User selection of the expansion module is not supported.
Switch Expansion 2 (Stratix 8000/8300 switches)	(22 and 26 port switches only). The catalog number for the copper or fiber expansion modules you are using. User selection of the expansion module is supported.

Connection Properties

In the navigation pane, click Connection.

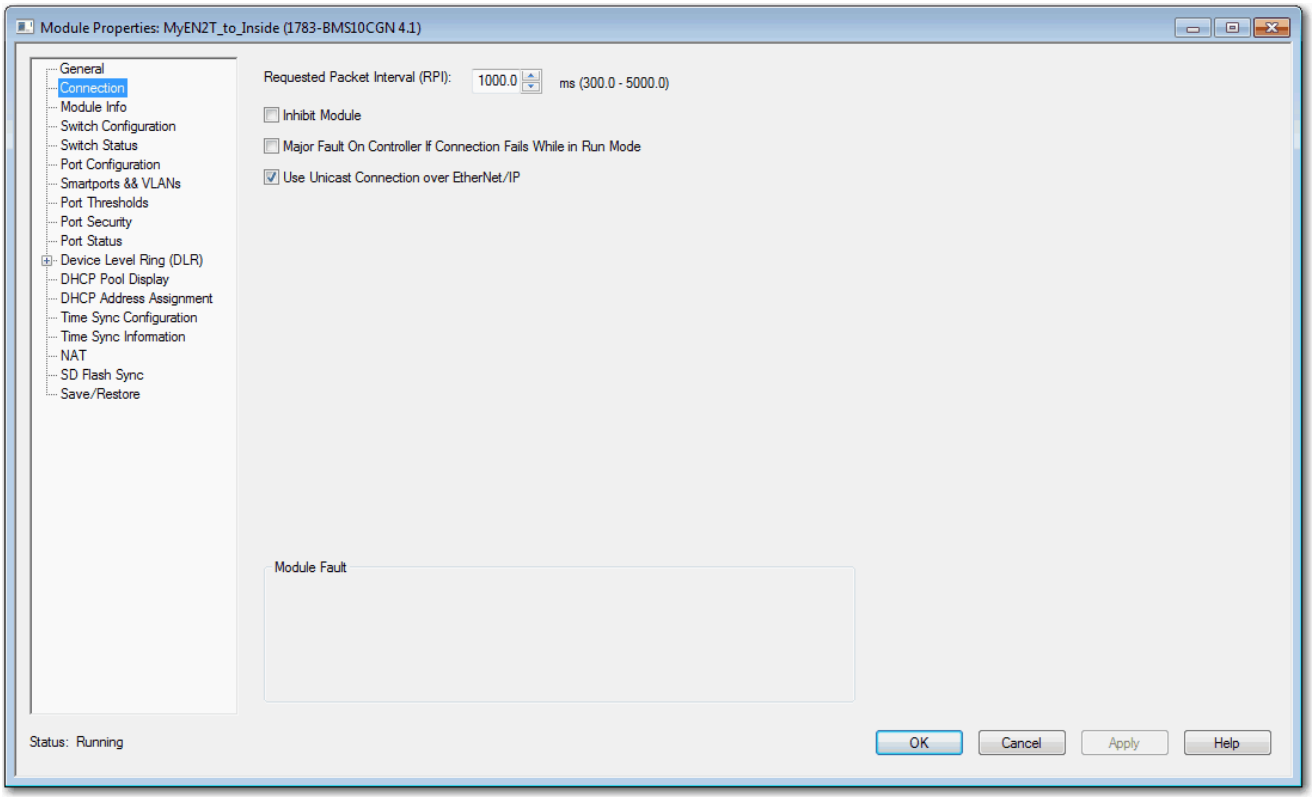


Table 17 - Connection Fields

Field	Description
Requested Packet Interval (RPI)	Enter a value between 300…5000.
Inhibit Module	Check to disable communication between the controller and the switch. Clear the checkbox to restore communication.
Major Fault on Controller If Connection Fails While in Run mode	Check to have the controller create a major fault if connection fails in Run mode.
Use Unicast Connections over EtherNet/IP	Check to use Unicast connections with the EtherNet/IP network.
Module Fault	Displays the fault code from the controller and the text that indicates the module fault has occurred.

Switch Configuration

You can configure IP settings and administrative parameters. The IP address can be manually assigned (static) or it can be automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you choose Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the switch.

- Static—Manually enter the IP address, subnet mask, and gateway.
- DHCP—The switch automatically obtains an IP address, default gateway, and subnet mask from the DHCP server. As long as the switch is not restarted, it continues to use the assigned IP information.

In the navigation pane, click Switch Configuration.

Figure 1 - Switch Configuration

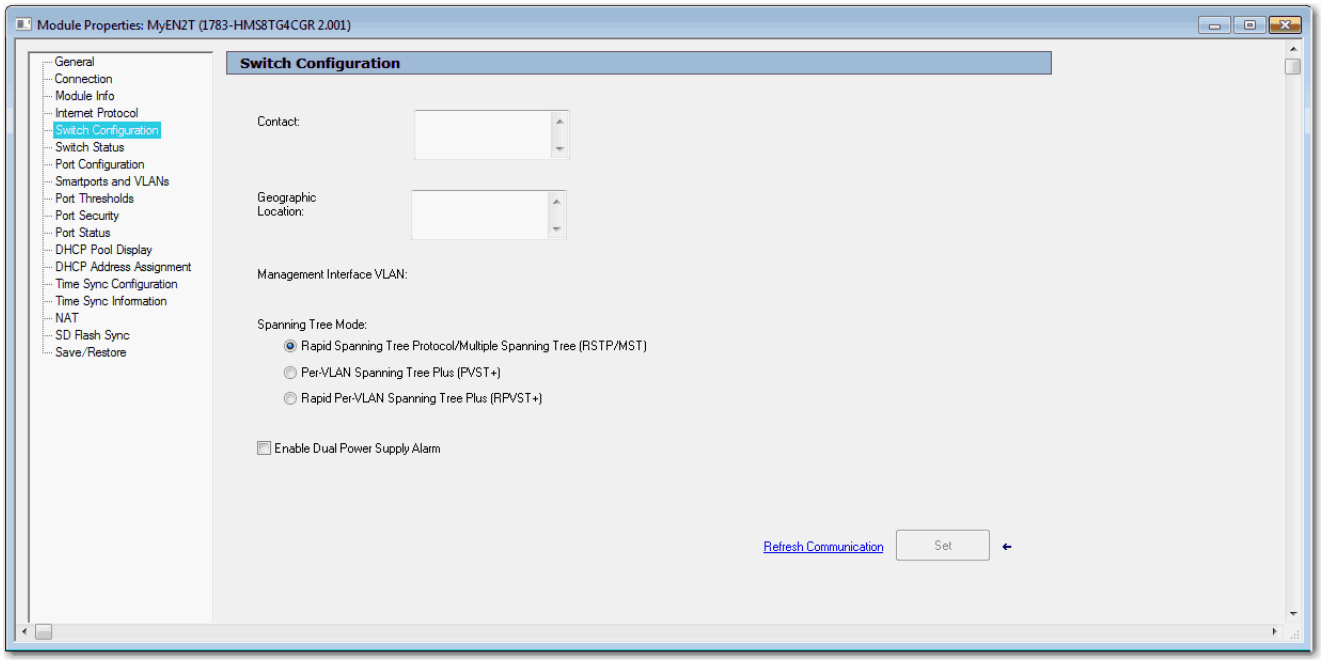


Table 18 - Switch Configuration Fields

Field	Description
Contact	(Optional). Enter contact information for the switch, up to 200 characters. The contact information can include alphanumeric and special characters (dash and comma) and a carriage return.
Geographic Location	(Optional). Enter a geographic location of the switch, up to 200 characters. The geographic location can include alphanumeric and special characters (dash and comma) and a carriage return.
Management Interface VLAN	Displays the VLAN through which the switch is managed. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. It also provides secure administrative access to all devices in the network. **IMPORTANT:** Be sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch.
Spanning Tree Mode (Stratix 5700 and ArmorStratix switches)	See Spanning Tree Protocol (STP) on page 361.
Enable Dual-Power Supply Alarm (Stratix 5700 and ArmorStratix switches)	To enable dual-power supply alarms, check the checkbox. The feature is disabled by default.

Port Configuration

Port settings determine how data is received and sent between the switch and the attached device.

In the navigation pane, click Port Configuration.

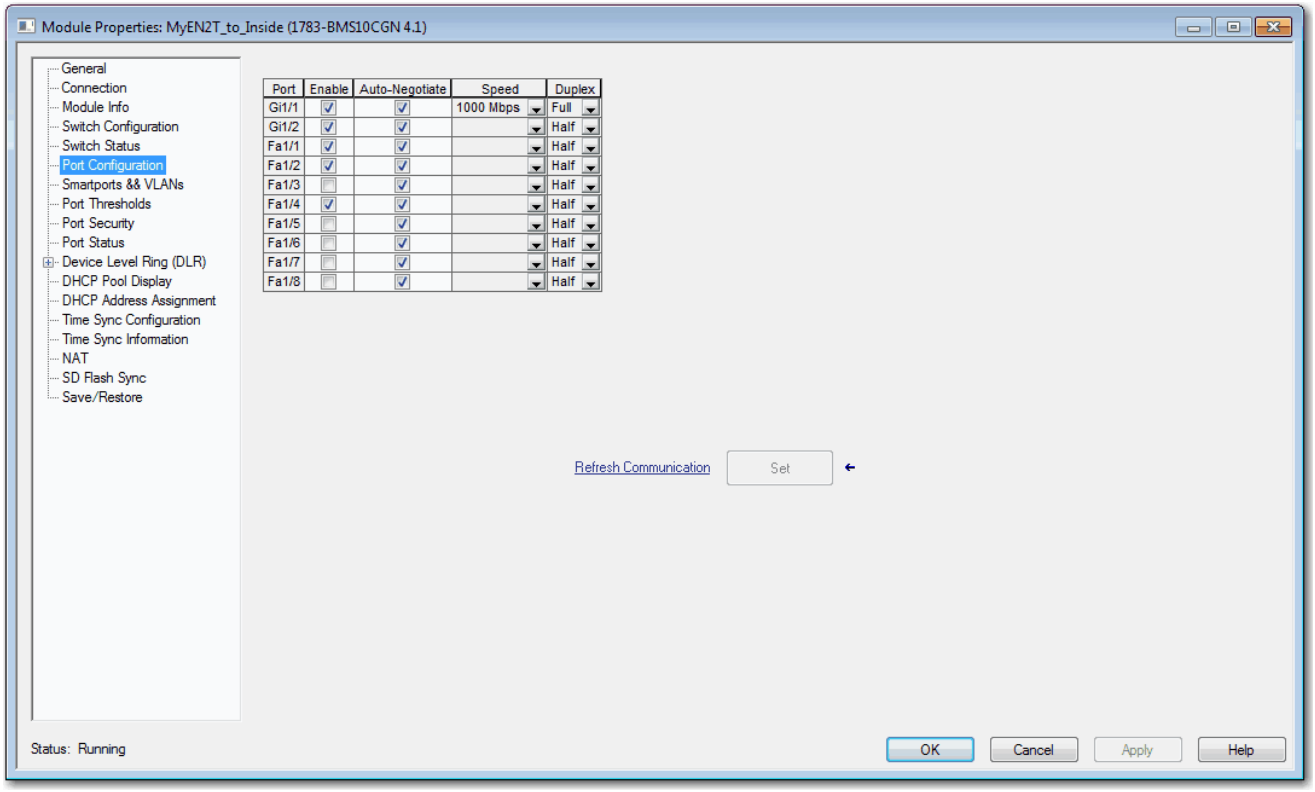


Table 19 - Port Configuration Fields

Field	Description
Unit (Stratix 8000/8300 switches)	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	The port that is selected for configuration. The port number includes the port type (Fa for Fast Ethernet, Gi for Gigabit Ethernet, or Te for Ten Gigabit Ethernet) and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Enable	To enable the port, check the checkbox. To disable the port manually, clear the checkbox. If the port is not in use and is not attached to a device, we recommend that you disable the port. You can troubleshoot a suspected unauthorized connection by manually disabling the port.

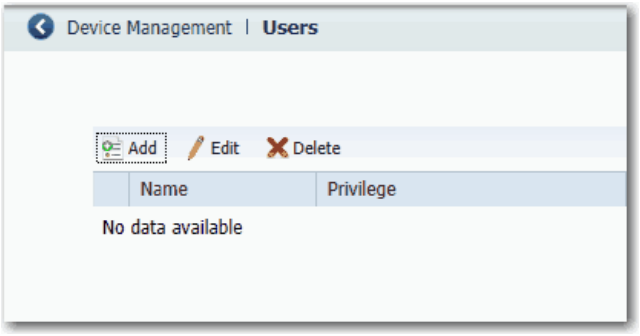
Table 19 - Port Configuration Fields (Continued)

Field	Description
Auto-negotiate	If you want the port and end-device to auto-negotiate the link speed and Duplex mode, check the checkbox. To specify the desired port speed and Duplex mode manually, clear the checkbox. We recommend that you use the default (auto-negotiate) so that the speed and duplex settings on the switch port automatically match the setting on the connected device. Change the switch port speed and duplex if the connected device requires a specific speed and duplex. If you set the speed and duplex for the switch port, the connected device must be configured for the same speed and duplex and not set to auto-negotiate. Otherwise, a speed/duplex mismatch occurs. Fiber-optic interfaces do not support auto-negotiation.
Speed	Choose the operating speed of the port. Gigabit (Gi): • 10 Mbps • 100 Mbps • 1 Gbps Fast Ethernet (Fa): • 10 Mbps • 100 Mbps 10 Gigabit (Te) • 1 Gbps • 10 Gbps
Duplex	Choose one of these Duplex modes: • Half-duplex—Both devices cannot send data simultaneously. Half-duplex is not available when speed is set to 1 Gbps or higher. • Full-duplex—Both devices can send data simultaneously.

User Administration via Device Manager

You can add, modify, or delete users and user login information for the switch via Device Manager.

From the Admin menu, choose Users.



For each user, you can specify the information in Table 20.

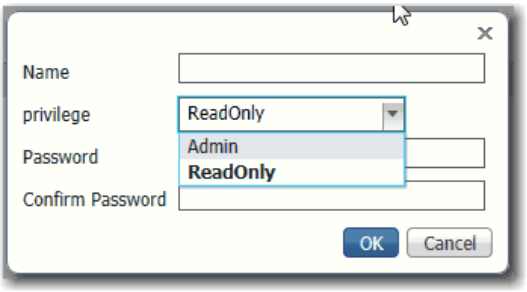


Table 20 - Add User Fields

Field	Description
Name	A unique user name. The user name cannot contain spaces.
Privilege	The level of access for the user: • Admin—Users can view and change all switch parameters. • ReadOnly—Users can only view switch status and monitoring information. Users cannot view configuration information, view administration information, or make any changes to the switch.
Password	The password that is required for access with this user name.
Confirm Password	

Configuration Files

The switch configuration files (config.text and vlan.dat) are in ASCII human-readable format. This configuration file is stored in nonvolatile memory and is read into the Random Access Memory (RAM) of the switch as the running configuration when the switch is powered up. When any changes are made to the configuration, the changes immediately take effect in the running configuration. Device Manager and the Logix Designer application automatically save changes to internal memory to be retained for the next power-up cycle. Any changes that are made via the CLI must be manually saved in internal memory to be retained for the next power-up cycle.

Manage Configuration Files via Device Manager

From the File Management menu, choose Load/Save and then do one of the following:

- To copy a configuration file from a file on another device to the internal memory, do the following:

  a. Enter the directory name of the folder on the switch.
  b. Browse to select the file.
  c. Click Upload.

- To download a configuration file from the internal memory to your computer, right-click the link and choose Save Link As.



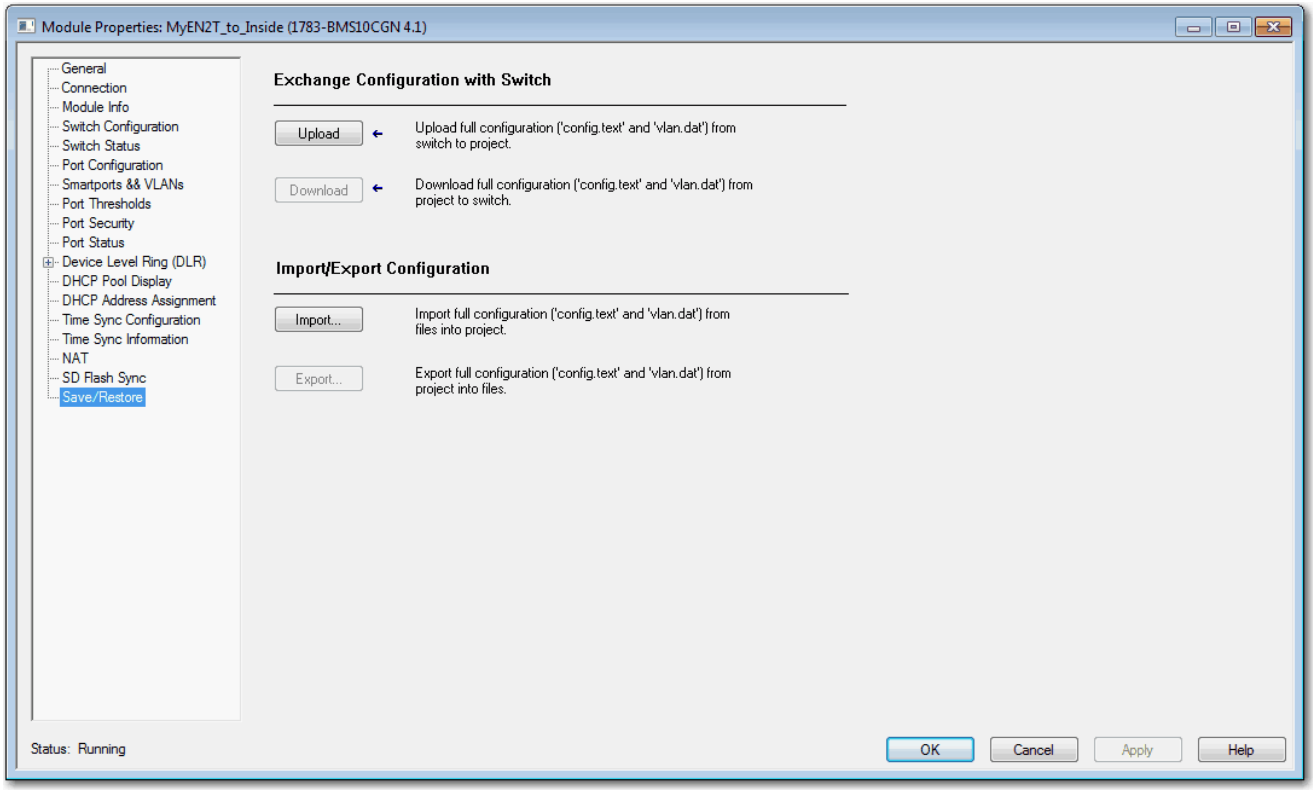
Manage Configuration Files via the Logix Designer Application

You can do the following:

- Save the switch configuration to a file for archiving
- Restore a switch configuration that is stored locally on the computer or within the Logix Designer application project.

To save and restore a switch configuration, be prepared to enter a valid switch password.

In the navigation pane, click Save/Restore.



The switch configuration consists of these two files:

- Text file with configuration parameters
- Binary file with VLAN information

Once the switch configuration is uploaded to the project file in the Logix Designer application, the switch configuration can be exported as computer files by using the Export button.

You can import a switch configuration from the appropriate files on your computer to the project by using the Import button on the Save/Restore view. You can then download the configuration to the switch by using the Download button.

Secure Digital (SD) Card

The following switches can store its configuration in an SD card or internal memory:

- Stratix 5700 and ArmorStratix 5700 switches have a slot for an optional SD card. You must use the 1784-SD1 card available from Rockwell Automation with the switches.
- Stratix 5400 and Stratix 5410 switches ship with an SD card, which stores the initial configuration and firmware for the switches.



ATTENTION: If a non-Rockwell SD card is used in Stratix switches, Rockwell Automation reserves the right to withhold support.

You can use the SD card instead of internal memory to do the following:

- Restore a switch configuration in case of failure.
- Duplicate configurations when you are deploying a new network.
- Synchronize the initial configuration and firmware of a Stratix 5400 switch to internal memory.

In general, the start method for the switch becomes the source for any changes you make to the configuration. For example, if you start from the SD card, any changes you make are saved to the SD card. If you start the switch from internal memory, even if you insert an SD card while starting the system, changes are saved to internal memory.

You can use Device Manager or the Logix Designer application to synchronize the SD card for configuration and IOS updates. The configuration synchronization process synchronizes config.text and vlan.dat from the source to the destination. If other files, such as back-up configurations, are present on the SD card, they are not synchronized.



ATTENTION: When synchronizing, be aware of your start-up source, so that you know which way to synchronize. Device Manager provides this information on the Manual Sync tab. If you synchronize in the wrong direction, you can overwrite your desired configuration.

If you start the switch from the SD card and then remove it while the switch is running, the following conditions apply:

- Device Manager is no longer be accessible.
- Changes that are made by using the CLI or the AOP take effect, but are not saved when the switch is restarted.
- If you reinsert the SD card into the slot, changes are not saved to the card unless new changes are made. Then the entire configuration is saved to the card.

ATTENTION: SD cards commonly have a physical read-only lock switch. If this switch is engaged, the switch starts from the SD card successfully. Changes that are made by using the CLI, AOP, or Device Manager take effect, but are not saved when the switch is restarted.

Synchronize the SD Card via Device Manager

To synchronize the SD card with the internal memory, use the Sync window. On the Manual Sync tab, you can view the following:

- Whether a card is present
- Card status
- If present, the source from which the switch was started

You can choose to synchronize the configuration or the software IOS from either the SD card to the internal memory or from the internal memory to the SD card.

The Auto Sync tab lets you configure default options for how Device Manager prompts you after a configuration change or IOS update.

To display the Manual Sync and Auto Sync tabs, from the File Management menu, choose Sync.

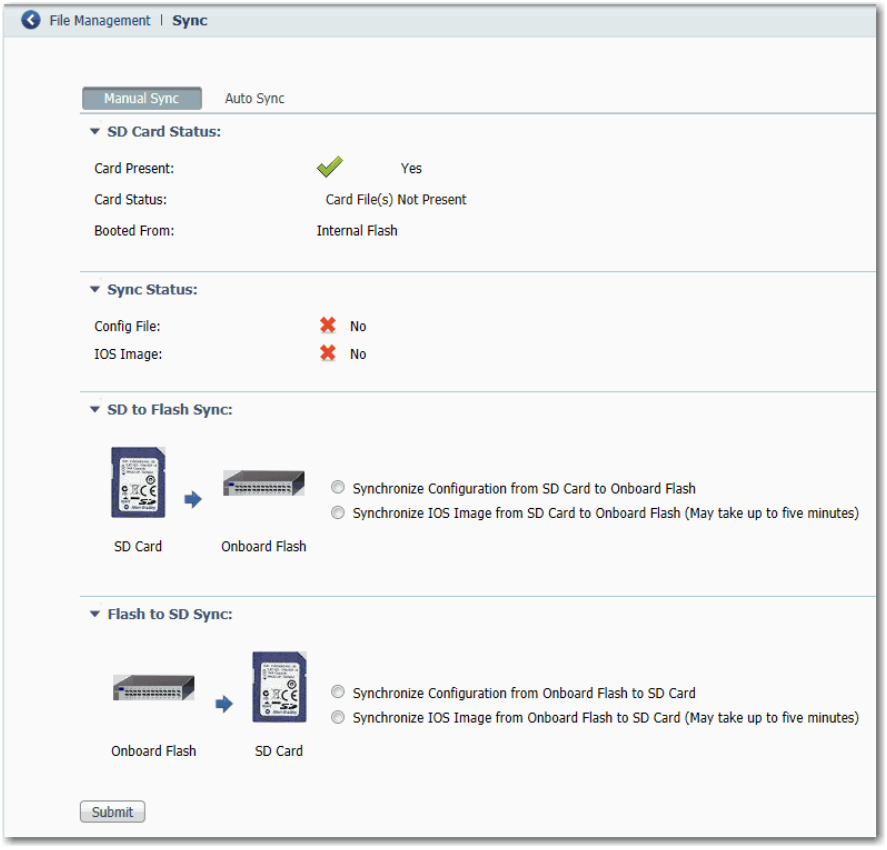


Table 21 - Manual Sync Tab Fields

Field	Description
SD Card Status	Indicates whether SD card is present, the status of the card, and from where its configuration was started.
SD to Flash Sync	Choose from these options: • Synchronize configuration from SD card to onboard flash • Synchronize IOS image from SD card to onboard flash
Flash to SD Sync	Choose from these options: • Synchronize configuration from onboard flash to SD card • Synchronize IOS image from onboard flash to SD card

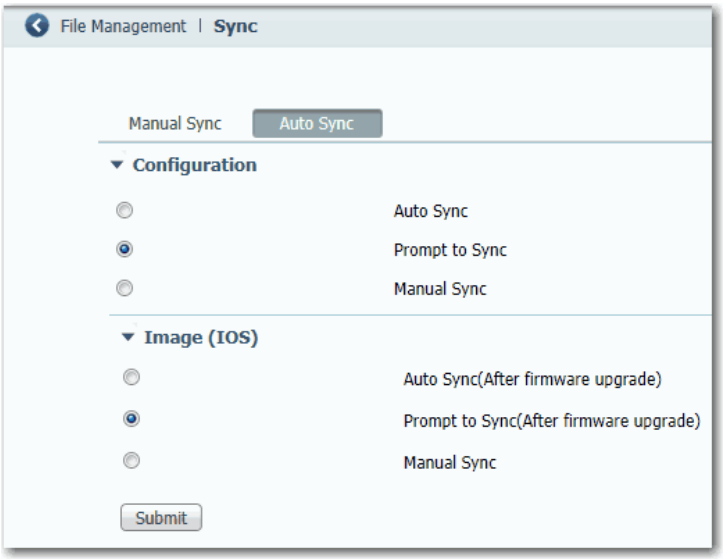


Table 22 - Auto Sync Tab Fields

Field	Description
Configuration	Auto Sync—Automatically synchronize the configuration when a configuration change is made in Device Manager. Auto Sync is the default configuration.
	Prompt to Sync—After a configuration change, a message prompts you to confirm the synchronization.
	Manual Sync—No synchronization occurs on a configuration change unless it is done manually.
Image (IOS)	Auto Sync (After firmware upgrade)—Automatically sync the changed configuration when firmware is upgraded.
	Prompt to Sync (After firmwareupgrade)—After firmware is upgraded, a message prompts you to confirm the configuration. Prompt to Sync is the default configuration.
	Manual Sync—No synchronization occurs after firmware is upgraded unless it is done manually.

Synchronize the SD Card via the Logix Designer Application

You can synchronize the SD card to either the configuration file or the entire image.

In the navigation pane, click SD Flash Sync.

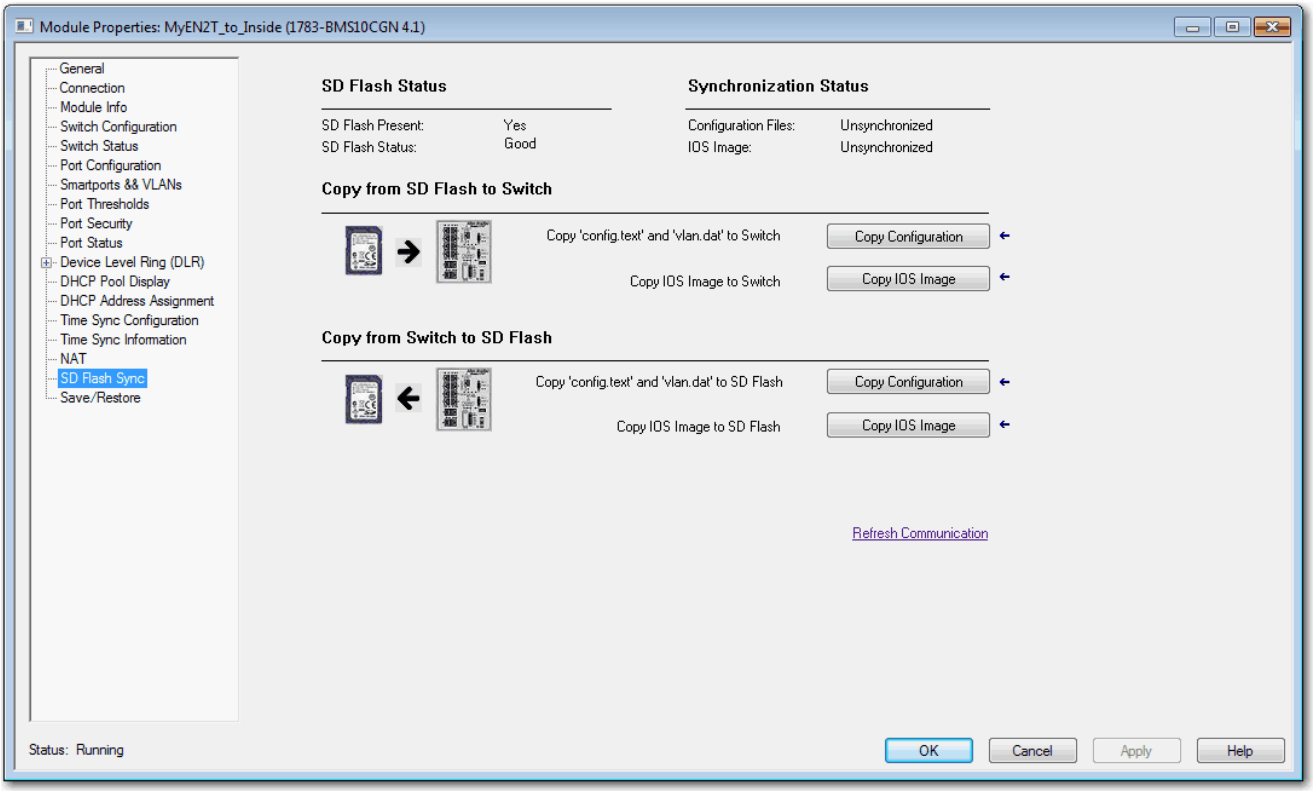


Table 23 - SD Flash Sync Fields

Field	Description
SD Flash Status	Indicates whether the SD card is present and the status. of the card
Synchronization Status	Indicates whether the configuration files and the IOS are synchronized or unsynchronized.
Copy from SD Flash to Switch	Choose from these options: • Copy Configuration • Copy IOS Image
Copy from Switch to SD Flash	Choose from these options: • Copy Configuration • Copy IOS Image

CompactFlash Memory Card (Stratix 8000/8300 Switches)

The CompactFlash card for Stratix 8000/8300 switches contains the switch IOS operating system, Device Manager firmware, and user-defined configuration settings. Without the CompactFlash card, the switch cannot power up or restart.

If you remove the card with the switch running, the switch continues to function. However, Device Manager is no longer available.

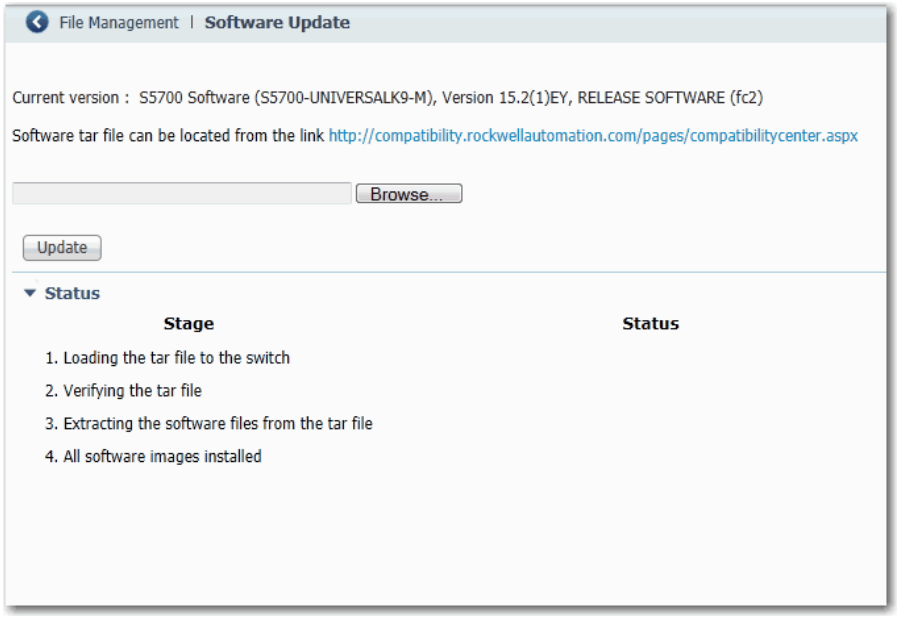
If you change the switch configuration after the card is removed, they are applied and used by the switch. However, the changes are not saved. If you insert the CompactFlash card later, the previous changes are still not saved to the card. Only changes that are made while the card is inserted are saved.

Each time a change is made with the card installed, both the AOP and Device Manager save the entire running configuration to the card.

Firmware Updates

You can download firmware for all switches from http://www.rockwellautomation.com.

From Device Manager, you can apply firmware updates to switches one at a time. From the Admin menu, choose Software Update.



With firmware revision 2.001 or later, the firmware is installed to the running nonvolatile memory location:

- If you start the switch with the SD card inserted, the firmware is installed on the SD card.
- If you start the switch from internal memory without the SD card inserted, the firmware is installed in the internal memory.

IMPORTANT Wait for the update process to complete. Do not use or close the browser session with Device Manager active. Do not access Device Manager from another browser session.

When the update process completes, a success message appears, and the switch automatically restarts. It can take a few minutes for the switch to restart with the new firmware.

Verify that the latest firmware revision on the switch appears in the Software field in the Switch Information area of the dashboard.

For more information, see the online help for Device Manager.

Cisco Network Assistant

Cisco Network Assistant is a web interface that you download from Cisco's website and run on your computer. It offers advanced options for configuring and monitoring multiple devices, including switches, switch clusters, switch stacks, routers, and access points.

Follow these steps to use the software.

1. Go to http://www.cisco.com/go/NetworkAssistant.

   You must be a registered user, but you need no other access privileges.
2. Find the Network Assistant installer.
3. Download the Network Assistant installer, and run it.

   You can run it directly from the web if your browser offers this choice.
4. When you run the installer, follow the displayed instructions.
5. In the final panel, click Finish to complete the Network Assistant installation.

   For more information, see the online help for Network Assistant.

Command-line Interface

You can manage the switch from the Command-line interface (CLI) by using these two methods:

- Connect your computer directly to the switch console port
- Enable Secure Shell (SSH) on the Express Setup window (IOS version 15.2(5)EA.fc4 and later)

IMPORTANT For secure network access, we recommend that you do not use Telnet. For new switch configurations with IOS version 15.2(5)EA.fc4 and later, Telnet is disabled by default. For more information about default settings after an upgrade, see page 212.

Follow these steps to access the CLI through the console port.

1. Connect to the console port in one of these ways:
   - To connect to the standard 9-pin serial port on a computer, use a RJ45-to-DB-9 adapter cable (not supplied with the switch).
   - (Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 switches). Use a standard mini-USB cable to connect to the mini-USB port on a computer. If you use the USB cable, download the drivers for Microsoft Windows from http://www.rockwellautomation.com. The USB cable is not provided with the switch.
2. Connect the other end of the cable to the console port on the switch.



WARNING: The console port is intended only for temporary local programming purposes and not intended for permanent connection. If you connect or disconnect the console cable with power applied to this module or the programming device on the other end of the cable, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

3. Start a terminal-emulation program on the computer.
4. Configure the computer terminal emulation software for 9600 bps, eight data bits, no parity, one stop bit, and no flow control.

Install Stratix 5400 Switches

Topic	Page
Specifications	75
Overview	75
Parts List and Required Tools	76
Install or Remove the SD Card	78
Verify Switch Operation	79
Mount the Switch on a DIN Rail	80
Remove the Switch from the DIN Rail	81
Ground the Switch	81
Wire the Switch DC Power Source	83
Attach the Switch Power Connectors	85
Install an SFP Module	87
Remove an SFP Module from an SFP Slot	89
Attach the Alarm Relay Connector to the Switch	90
Connect to 10/100 and 10/100/1000 Ports	93
Connect to 10BASE-T, 100BASE-TX, or 1000BASE-T Ports	94
Connect to PoE Ports	95
Connect to SFP Module Ports	95
Connect to a Dual-purpose Port	96

ATTENTION: Environment and Enclosure

This equipment is intended for use in a Pollution Degree 2 industrial environment, in overvoltage Category II applications (as defined in IEC 60664-1), at altitudes up to 2000 m (6562 ft) without derating.

This equipment is not intended for use in residential environments and may not provide adequate protection to radio communication services in such environments.

This equipment is supplied as open-type equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if nonmetallic. The interior of the enclosure must be accessible only by the use of a tool. Subsequent sections of this publication may contain additional information regarding specific enclosure type ratings that are required to comply with certain product safety certifications.

In addition to this publication, see the following:

- Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1, for additional installation requirements
- NEMA Standard 250 and IEC 60529, as applicable, for explanations of the degrees of protection provided by enclosures

North American Hazardous Location Approval

The following information applies when operating this equipment in hazardous locations.	**Informations sur l'utilisation de cet équipement en environnements dangereux.**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Les produits marqués "CL I, DIV 2, GP A, B, C, D" ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**WARNING: RISQUE D'EXPLOSION** • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

North American Zones:

UL 60079-0, 5th Ed, 2009-10-21l; UL 60079-15, 3rd Ed, 2009-7-17;
CAN/CSA C22.2 No. 60079-15-12 Ed. 1; CAN/CSA C22.2 No. 60079-0-11 Ed. 2

WARNING: When you connect or disconnect the Power or Alarm Removable Terminal Blocks (RTBs) with field side power applied, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

WARNING: If you connect or disconnect communication cables with power applied to this module or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

WARNING: Use supply wires suitable for 30 °C (86 °F) above surrounding ambient.

WARNING: If you connect or disconnect wiring while the field-side power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

WARNING: Do not use the USB-mini console port in hazardous locations.

European Hazardous Location Approval

The following applies to products marked CE Ex II 3 G: Such modules:

- Are Equipment Group II, Equipment Category 3, and comply with the Essential Health and Safety Requirements relating to the design and construction of such equipment given in Annex II to Directive 94/9/EC. See the EC Declaration of Conformity at http://www.rockwellautomation.com/products/certification for details.
- The type of protection is "Ex nA nC IIC T3 Gc" according to EN 60079-15.
- Comply to Standards: EN 60079-0:2012+A11:2013, EN 60079-15:2010, reference certificate number DEMKO14ATEX1423X.
- Are intended for use in areas in which explosive atmospheres caused by gases, vapors, mists, or air are unlikely to occur, or are likely to occur only infrequently and for short periods. Such locations correspond to Zone 2 classification according to ATEX directive 1999/92/EC.

WARNING: Special Conditions for Safe Use

- This equipment shall be mounted in an ATEX Zone 2 certified enclosure with a minimum ingress protection rating of at least IP54 (as defined in EN 60529) and used in an environment of not more than Pollution Degree 2 (as defined in EN 60664-1) when applied in Zone 2 environments. The enclosure must be accessible only by the use of a tool.
- This equipment shall be used within its specified ratings defined by Rockwell Automation.
- Provision shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 140% of the rated voltage when applied in Zone 2 environments.
- Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.
- Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.



ATTENTION: Prevent Electrostatic Discharge

This equipment is sensitive to electrostatic discharge, which can cause internal damage and affect normal operation. Follow these guidelines when you handle this equipment:

- Touch a grounded object to discharge potential static.
- Wear an approved grounding wriststrap.
- Do not touch connectors or pins on component boards.
- Do not touch circuit components inside the equipment.
- Use a static-safe workstation, if available.
- Store the equipment in appropriate static-safe packaging when not in use.



ATTENTION: The console ports are intended for temporary local programming purposes only and not intended for permanent connection.

The console port cables are not to exceed 3.0 m (9.84 ft) and must not contain hubs.



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



ATTENTION: Before installing, configuring, operating, or maintaining this product, read this document and the documents listed in the additional resources section for installing, configuring, or operating equipment. Users should familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.



ATTENTION: Installation, adjustments, putting into service, use, assembly, disassembly, and maintenance shall be carried out by suitably trained personnel in accordance with applicable code of practice. In case of malfunction or damage, no attempts at repair should be made. The module should be returned to the manufacturer for repair. Do not dismantle the module.



ATTENTION: This equipment is certified for use only within the surrounding air temperature range.



ATTENTION: Use only a soft dry anti-static cloth to wipe down equipment. Do not use any cleaning agents.



ATTENTION: Electrical Safety Considerations

To comply with the CE Low Voltage Directive (LVD), all connections to this equipment must be powered from a source compliant with the following:

- Safety Extra Low Voltage (SELV) Supply
- Protected Extra Low Voltage (PELV) Supply

Specifications

For additional specifications and certifications, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Attribute	1783-HMS8T4CGN, 1783-HMS16T4CGN, 1783-HMS8TG4CGN, 1783-HMS8TG4CGR, 1783-HMS4T4E4CGN	1783-HMS4C4CGN, 1783-HMS4S8E4CGN, 1783-HMS8TG8EG4CGN, 1783-HMS4SG8EG4CGN, 1783-HMS4EG8CGN, 1783-HMS4EG8CGR, 1783-HMS8TG8EG4CGR, 1783-HMS4SG8EG4CGR, 1783-HMS16TG4CGN, 1783-HMS16TG4CGR	1783-HMS8S4CGN, 1783-HMS8SG4CGN, 1783-HMS8SG4CGR
Power supply	12…54V DC, 3.7 A max	12…54V DC, 4.3 A max	12…54V DC, 5.0 A max
Alarm relay	30V DC, 1 A or 48V DC, 0.5 A		
Temp code	T3		
Screw torque, ground terminal	0.51 N•m (4.5 lb•in)		
Screw torque, power terminal	0.56 N•m (5.0 lb•in)		
Screw torque, alarm terminal	0.23 N•m (2.0 lb•in)		

Overview

When determining where to place the switch, observe these guidelines:

- For 10/100 ports and 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 100 m (328 ft).
- The fiber-optic cable length from a switch to an attached device cannot exceed the distance that is specified in Appendix D.
- Temperature surrounding the unit does not exceed 70 °C (158 °F).

IMPORTANT When the switch is installed in an industrial enclosure, the temperature within the enclosure is greater than normal room temperature outside the enclosure.

The temperature inside the enclosure cannot exceed 158 °F (70 °C), the maximum ambient enclosure temperature of the switch.

- Clearance to front and rear panels meets these conditions:
  - Front-panel status indicators can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Front-panel direct current (DC) power connectors and the alarm relay connector are within reach of the connection to the DC power source.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.



ATTENTION: Do not wire more than 1 conductor on any single terminal.

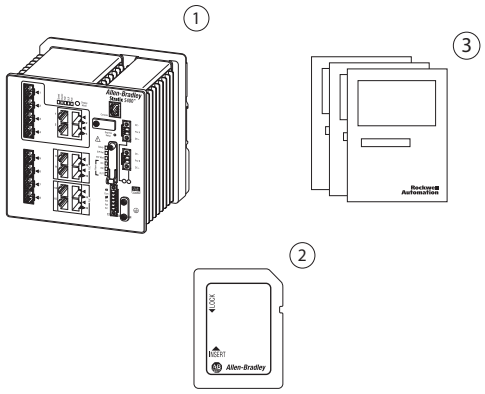
Follow these steps to install the switch.

1. (Optional) Install or remove the SD card.
2. Verify switch operation.
3. Mount the switch on a DIN rail.
4. Ground the switch.
5. Wire the DC power source for the switch and attach the switch power connectors.

   For switches with Power over Ethernet (PoE) capability, there is no separate power input for PoE, so no additional wiring or power connectors are required.
6. (Optional) Install an SFP module.
7. Wire external alarms and attach the alarm relay connector to the switch.
8. Connect to the switch ports:
   - 10/100 copper ports and 10/100/1000 ports
   - 10BASE-T, 100BASE-TX, and 10000BASE-T ports
   - PoE ports
   - SFP module ports
   - Dual-purpose ports

Parts List and Required Tools

Verify that you have these items. The secure digital (SD) card comes installed in the SD slot on the front panel of the switch.



1 Stratix® 5400 switch

2 SD card

3 Documentation



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

Obtain these tools:

- Ratcheting torque screwdriver that exerts up to 1.69 N•m (15 in•lbs) of pressure
- Small, flat-blade screwdriver
- #6 ring terminal lug for 5.3 mm^2 (10 AWG) wire, such as Thomas & Bett part number 10RC6 or equivalent
- Crimping tool, such as Thomas & Bett part number WT2000, ERG-2001, or equivalent
- 5.3 mm^2 (10 AWG) copper ground wire, such as Belden part number 9912 or equivalent
- Wire-stripping tool
- For panel-mounting without a DIN rail, M5 or #10-24 or #10-32 bolts or screws with 1.27 cm (0.5 in.) O.D. flat washers

For simplified cabling, the automatic medium-dependent interface crossover (auto-MDIX) feature is enabled by default on the switch. With auto-MDIX enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a 10/100 or 10/100/1000 Ethernet switch port, regardless of the type of device on the other end of the connection.

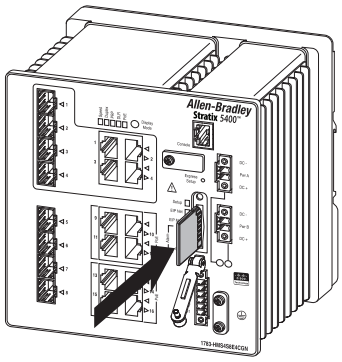
Install or Remove the SD Card

A secure digital (SD) card ships with the Stratix 5400 switch. The SD card contains the switch firmware and initial configuration. You can order a replacement SD card from Rockwell Automation, catalog number 1784-SD1, if needed. The replacement card ships without firmware and must be synced with the internal memory of the switch. See page 64.

To install or replace the SD card, follow these steps.

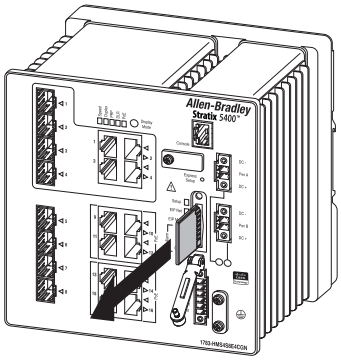
1. On the front of the switch, locate the door that protects the SD card slot.
2. Loosen the captive thumb screw at the top of the door by using a screwdriver to open the door.
3. Install or remove the card.

   To install the card, slide it into the slot, and press it firmly in place until it latches in the spring loaded mechanism. The card is keyed so that you cannot fully insert it the wrong way.



32555-M

   To remove the card, push it in and let it pop out via the spring-loaded mechanism. Grasp the card top and pull it out. Place it in an antistatic bag to protect it from static discharge.



32556-M

4. Close the guard door and fasten the captive screw by using a screwdriver to keep the door in place.

Verify Switch Operation

Before installing the switch in its final location, power on the switch, and verify that the switch powers up.

The time that is required for the switch to start up is directly related to your switch configuration. Start time is negatively affected by such things as the following:

- Spanning Tree Learning mode
- Number of files or images in onboard memory

To test the switch, follow these steps.

1. Apply power to the switch.

   If the switch is directly connected to a DC power source, locate the circuit breaker on the panel board that services the DC circuit, and switch the circuit breaker to the ON position.

2. Verify the start-up process.

   When you power on the switch, it begins a start-up process. The Setup status indicator blinks green as the IOS software image loads. If the routine fails, the Setup status indicator turns red.

   IMPORTANT Start-up failures are usually fatal to the switch. Contact your Rockwell Automation representative immediately if your switch does not complete the start sequence successfully.

   IMPORTANT You can disable Boot Fast and run the Power-on self-test (POST) by using the CLI. For more information, see the documentation at http://www.Cisco.com.

3. After successfully running this test, do the following:
   a. Turn off power to the switch.
   b. Disconnect the cables.
   c. Decide where you want to install the switch

Mount the Switch on a DIN Rail

The switch ships with a spring-loaded latch on the rear panel for mounting on a DIN rail.

ATTENTION: To prevent the switch from overheating, observe these minimum clearances:

- Top and bottom: 50.8 mm (2.0 in.)
- Exposed side (not connected to the module): 50.8 mm (2.0 in.)
- Front: 50.8 mm (2.0 in.)

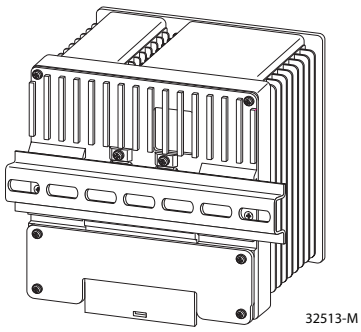
IMPORTANT The switch must be mounted in an upright orientation, as shown in these instructions. Alternative mounting orientations are not supported.

To attach the switch to a DIN rail, follow these steps.

1. Position the rear panel of the switch directly in front of the DIN rail.

   Make sure that the DIN rail fits in the space between the two hooks near the top of the switch and the spring-loaded latch near the bottom.

2. Hold the bottom of the switch away from the DIN rail, and place the two hooks on the back of the switch over the top of the DIN rail.

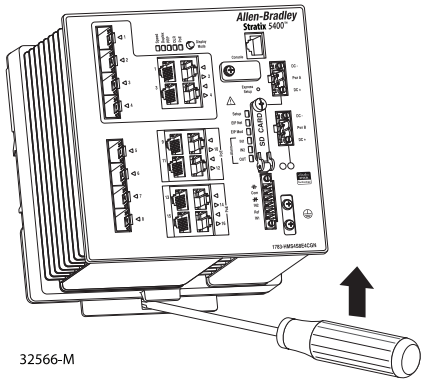


3. Push the switch toward the DIN rail to cause the spring loaded latch at the bottom rear of the switch to move down and snap into place.

Remove the Switch from the DIN Rail

To remove the switch from a DIN rail or a rack, follow these steps.

1. Remove power from the switch, and disconnect all cables and connectors from the front panel of the switch.
2. Insert a tool, such as a flat-head screwdriver, in the slot at the bottom of the spring-loaded latch and use it to release the latch from the DIN rail.



32566-M

Ground the Switch

For DC power connections, use UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

ATTENTION: To make sure that the equipment is reliably connected to earth ground, follow the grounding procedure instructions and use a suitable ring terminal lug, such as Thomas & Betts part number 10RCR or equivalent.

ATTENTION: For proper grounding, you must always connect the power supply functional-ground screw when connecting the power supply. You must provide an acceptable grounding path for each device in your application. For more information on proper grounding guidelines, refer to publication 1770-4.1, Industrial Automation Wiring and Grounding Guidelines.

When using DIN rail mounting, additional grounding can also be accomplished through the DIN rail. Use zinc-plated, yellow-chromate steel DIN rail to assure proper grounding to an Earth Grounding path. Secure DIN rail to mounting surface approximately every 200 mm (7.8 in.) using end-anchors appropriately and using a washer plate along the entire length of the DIN rail.

Use at least 4 mm^2 (12 AWG) wire to connect to the external grounding screw.

The ground lug is not supplied with the switch. You can use one of the these options:

- Single ring terminal
- Two single ring terminals

To ground the switch to earth ground, follow these steps. Be sure to follow any grounding requirements at your site.

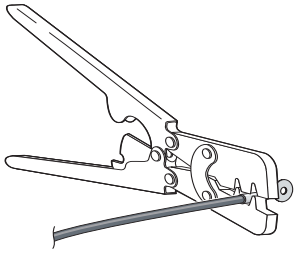
1. Use a Phillips screwdriver or a ratcheting torque screwdriver with a Phillips head to remove the ground screw from the front panel of the switch.

   Store the ground screw for later use.

2. Use the guidelines from the manufacturer to determine the wire length to be stripped.

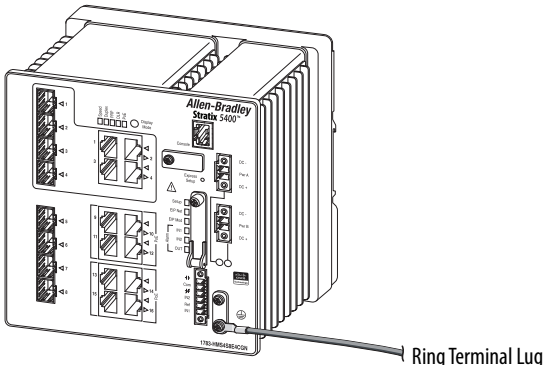
3. Insert the ground wire into the ring terminal lug and use a crimping tool to crimp the terminal to the wire.

   If you are using two ring terminals, repeat this action for the second ring terminal.



4. Slide the ground screw through the terminal.

5. Insert the ground screw into the functional ground screw opening on the front panel.



6. Use a ratcheting torque screwdriver to tighten the ground screws and ring terminal lugs to the switch front panel to 0.51 N•m (4.5 lb•in).

   Do not exceed the recommended torque.

7. Attach the other end of the ground wire to a grounded bare metal surface, such as a ground bus, a grounded DIN rail, or a grounded bare rack.

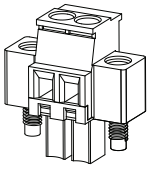
Wire the Switch DC Power Source

For switches with Power over Ethernet (PoE) capability, PoE power is drawn from the single power connection. There is no separate power input for PoE.

Switch Configuration	Required Voltage Input	Power Supplied per Port	Allen-Bradley Products
PoE	44-54V	15.4 W, max	Switched-mode power supplies: • 1606-XL Standard • 1606-XLE Essential • 1606-XLP Compact • 1606-XLS Performance
PoE+	50-54V	30 W, max	
Non-PoE	12…54V	Not applicable	

To wire the DC power source for the switch, follow these steps.

1. Locate the power connector.

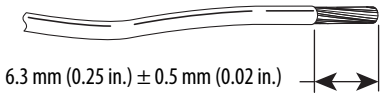


2. Identify the positive and return DC power connections.

   The positive DC power connection is labeled DC+, and the negative DC power connection is the adjacent connection labeled DC-.

3. Measure a length of 0.82...0.52 mm^2 (18...20 AWG) copper wire long enough to connect to the DC power source.
4. Use an 18-gauge wire-stripping tool to strip each of the two wires to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

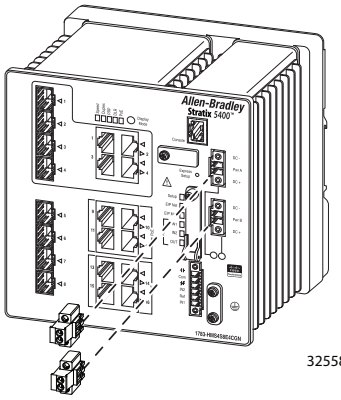
   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wire. Stripping more than the recommended amount of wire can leave wire exposed after installation.



31789-M

5. Loosen the two captive screws that attach the power connector to the switch, and remove the power connector.

   Remove both connectors if you are connecting to two power sources.

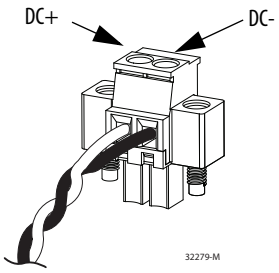


32558-M

6. Insert the exposed part of the positive wire into the connection labeled DC+ and the exposed part of the return wire into the connection labeled DC-.

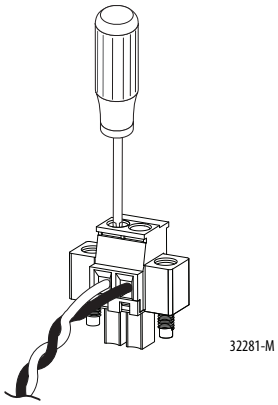
   Be sure that you cannot see any wire lead. Only wire with insulation can extend from the connector.

> **ATTENTION:** An exposed wire lead from a DC input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC input power source wire extends from the connectors or terminal blocks.



7. Use a ratcheting-torque screwdriver to torque the captive screws of the power connector to 0.56 N•m (5.0 lb•in).

   Do not exceed the recommended torque.

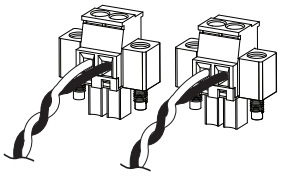


8. Connect the other end of the positive wire to the positive terminal on the DC power source.

9. Connect the other end of the return wire to the return terminal on the DC power source.

   When you are testing the switch, one power connection is sufficient. If you are installing the switch and are using a second power source, repeat this procedure with the second power connector.

   The following figure shows the completed DC input wiring on a power connector for a primary power source and an optional secondary power source.

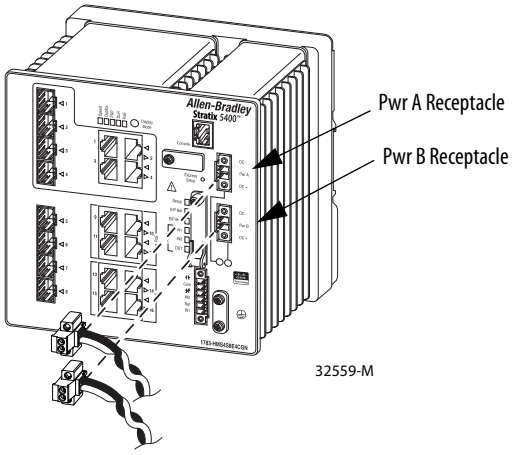


32282-M

Attach the Switch Power Connectors

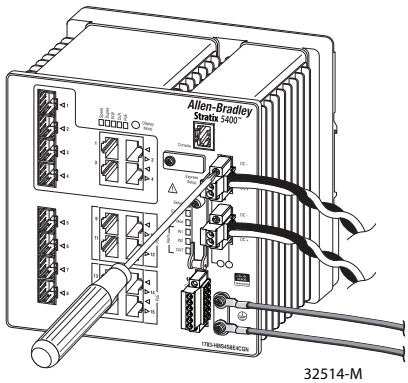
To attach the switch power connectors to the front panel of the switch, follow these steps. There is no separate power connector for PoE.

1. Insert one power connector into the Pwr A receptacle on the switch front panel, and the other into the Pwr B receptacle.



32559-M

2. Use a ratcheting torque flathead screwdriver to tighten the captive screws on the sides of the power connectors.

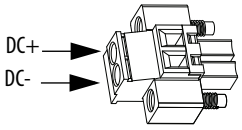


32514-M

When you test the switch, one power source is sufficient. If you install the switch and use a second power source, repeat this procedure for the second power connector (Pwr B), which installs just below the primary power connector (Pwr A).

3. When you install the switch, secure the wires from the power connectors to the rack by using tie wraps.
4. Insert the exposed part of the positive wire into the DC+ connection and the exposed part of the return wire into the DC- connection.

   Make sure that you cannot see any wire lead. Only wire with insulation can extend from the connector.



5. Use a ratcheting-torque screwdriver to torque the captive screws of the power connector to 0.56 N•m (5.0 lb•in).
6. Connect the other end of the positive wire (the one connected to DC+) to the positive terminal on the DC power source.
7. Connect the other end of the return wire (the one connected to DC-) to the return terminal on the DC power source.



ATTENTION: If multiple power sources are used, do not exceed the specified isolation voltage.

Install an SFP Module

WARNING: When you insert or remove the small form-factor pluggable (SFP) optical transceiver while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: Under certain conditions, viewing the small form-factor pluggable (SFP) optical transceiver may expose the eye to hazard. When viewed under some conditions, the optical port may expose the eye beyond the maximum permissible exposure recommendations.

ATTENTION: Use SFP modules from only Rockwell Automation. For details about supported modules, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

ATTENTION: We strongly recommend that you do not install or remove the SFP module with fiber-optic cables attached. If you leave the cables attached, damage to the cables, the cable connector, or the optical interfaces in the SFP module can occur. Disconnect all cables before removing or installing an SFP module.

IMPORTANT Installing and removing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is necessary.

On switch catalog numbers that support communication over fiber-optic cable, SFP modules are inserted into SFP module slots on the front of the switch. These field-replaceable modules provide the uplink optical interfaces, send (TX) and receive (RX).

You can use any combination of compatible SFP modules:

- Each SFP module must be of the same type as the SFP module on the other end of the cable. The cable must not exceed the stipulated cable length for reliable communications.
- Once you install SFP modules in the switch, be aware that the overall temperature rating of the combined modules (switch and SFP modules) is limited to the lowest maximum temperature rating and the highest minimum temperature rating.

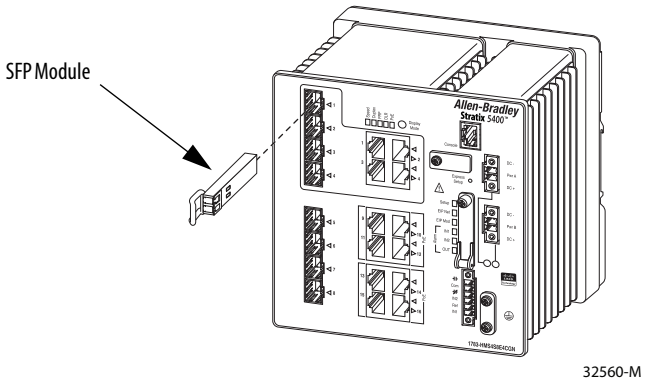
For cable length and temperature specifications, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

To insert an SFP module into the SFP slot, follow these steps.

1. Attach an ESD-preventive wriststrap to your wrist and to a grounded bare metal surface.
2. Grasp both sides of the SFP module and align the module sideways in front of the slot opening.

> **ATTENTION:** If the SFP module cannot be fully inserted, stop! Do not force the module into the slot. Rotate the SFP module 180° and try again.

3. Insert the SFP module into the slot as shown in the following figure until you feel the connector on the module snap into place in the rear of the slot.



4. Remove the dust plugs from the SFP module optical ports, store them for later use.

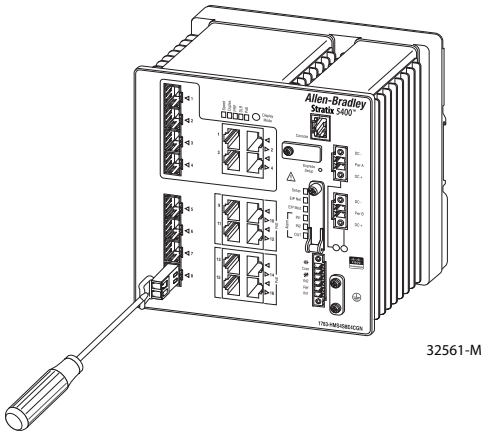
> **IMPORTANT** Do not remove the dust plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable.
>
> The plugs and caps help protect the SFP module ports and cables from contamination and ambient light.

Remove an SFP Module from an SFP Slot

To remove an SFP module from an SFP slot, follow these steps.

1. Attach an ESD-preventive wriststrap to your wrist and to a grounded bare metal surface.
2. Disconnect the fiber LC connector from the SFP module.
3. Insert a dust plug into the optical ports of the SFP module to keep the optical interfaces clean.
4. Unlock and remove the SFP module.

   If the module has a bale-clasp latch, swing the bale toward you and pull it gently to eject the module. If the bale-clasp latch is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the latch.



32561-M

5. Grasp the SFP module between your thumb and index finger, and carefully remove it from the module slot.
6. Place the removed SFP module in an antistatic bag or other protective environment.

Wire the External Alarms

The switch has two alarm inputs and one Form C (single-pole, double-throw) alarm output relay circuits for external alarms. The input alarm relay circuits are designed to sense if the alarm input is open or closed relative to the alarm input reference pin. The output alarm relay circuit has one Form C relay, with one normally open (NO) and one normally closed (NC) contact. You can configure the output alarm relay as either normally energized or normally de-energized by using the CLI.

See Appendix D for an alarm wiring example.

Alarm signals are connected to the switch through the 6-way alarm relay connector. Three connections are dedicated to the two alarm input circuits:

- Alarm input 1 (IN1)
- Alarm input 2 (IN2)
- Isolated reference ground

An alarm input and the reference ground wiring connection are required to complete one input alarm circuit. You must provide either an NO or an NC dry contact to complete the alarm circuit between reference ground and IN1 or IN2.



ATTENTION: Do not apply an external voltage source to either the IN1 or IN2 alarm inputs. Limit alarm output wiring to 48 V DC, 0.5 A.

The three remaining connections for the Form C output alarm circuit are as follows:

- NO output
- NC output
- common

An alarm output and the common wiring connection are required to complete one output alarm circuit. The Form C output alarm relay provides one NO and one NC dry contact.



ATTENTION: Wire connections to the power and relay connector, must be UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

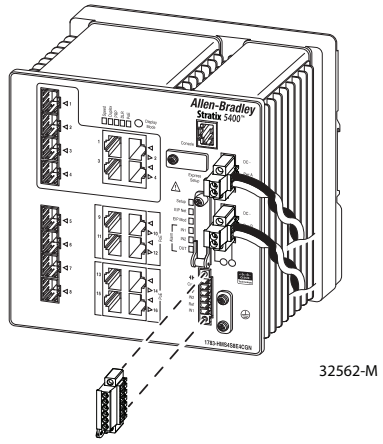
The labels for the alarm relay connector are on the switch panel.

Table 24 - Alarm Relay Connector Labels

Label	Connection
NO	Alarm Output Normally Open (NO) connection
COM	Alarm Output Common connection
NC	Alarm Output Normally Closed (NC) connection
IN2	Alarm Input 2
REF	Alarm Input Reference Ground connection
IN1	Alarm Input 1

To wire the switch to an external alarm device, follow these steps.

1. Loosen the captive screws that hold the alarm relay connector on the switch, and remove the connector from the switch chassis.



2. Measure two strands of twisted-pair wire (18...20 AWG) long enough to connect to the external alarm device.

   Choose between creating an external alarm input or output circuit.

3. Use a wire stripper to remove the casing from both ends of each wire to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

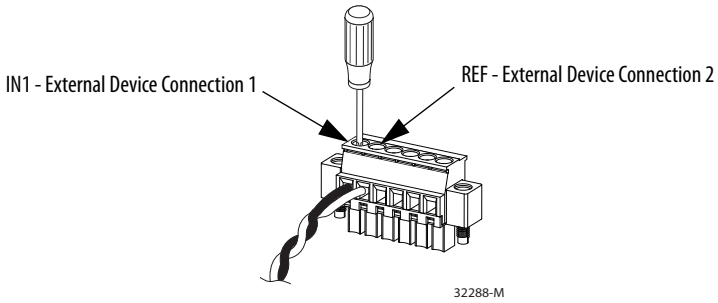
   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wires. Stripping more than the recommended amount of wire can leave exposed wire from the alarm relay connector after installation.

4. Insert the exposed wires for the external alarm device into the connections that are based on an alarm input or output circuit setup.

   See Table 24 on page 91.

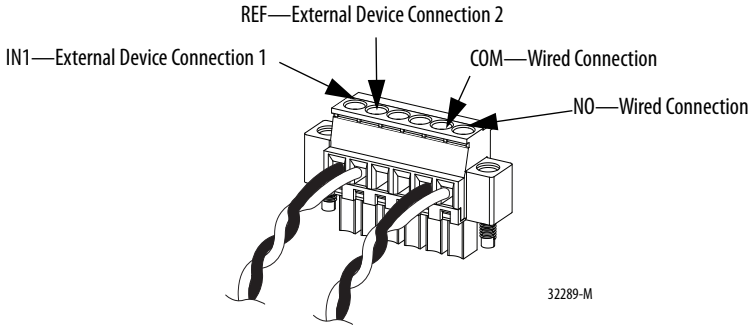
5. Use a ratcheting torque flathead screwdriver to torque the captive screw of the alarm relay connector to 0.23 N•m (2.0 lb•in).

   Do not exceed the recommended torque.



6. Repeat the preceding procedure to insert the input and output wires of one more external alarm device into the alarm relay connector.

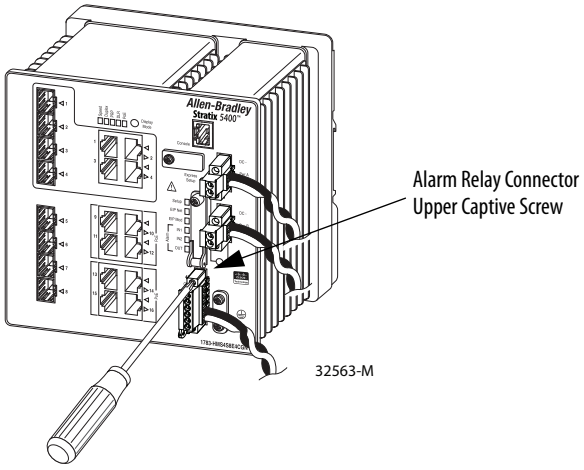
   The following figure shows the completed wiring for two external alarm devices. The first alarm device circuit is wired as an alarm relay input circuit—the IN1 and REF connections complete the circuit. The second alarm device circuit is wired as an alarm relay output circuit by using the normally open side of the form C relay contacts. The NO and COM connections complete the circuit.



Attach the Alarm Relay Connector to the Switch

To attach the alarm relay connector to the front panel of the switch, follow these steps.

1. Insert the alarm relay connector into the receptacle on the switch front panel.
2. Use a ratcheting torque flathead screwdriver to tighten the captive screws on the sides of the alarm relay connector.



Connect to 10/100 and 10/100/1000 Ports

The switch 10/100/1000 ports automatically configure themselves to operate at the speed of attached devices. If the attached ports do not support autonegotiation, you can explicitly set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have their speed and duplex parameters that are manually set can reduce performance or result in no linkage.

The Auto-MDIX feature is enabled by default. Unless this feature is disabled, you can use either straight-through or crossover cables to connect to other devices on the network.

To maximize performance, choose one of these methods for configuring the Ethernet ports:

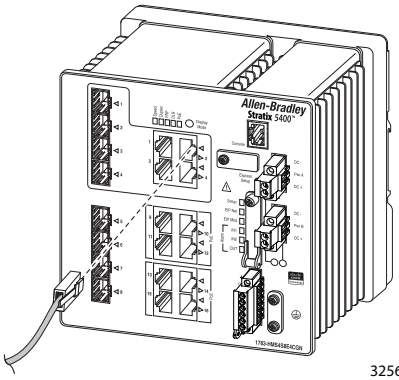
- Let the ports autonegotiate both speed and duplex
- Set the port speed and duplex parameters on both ends of the connection

Connect to 10BASE-T, 100BASE-TX, or 1000BASE-T Ports

To connect to 10BASE-T, 100BASE-TX, or 1000BASE-T ports, follow these steps.

ATTENTION: To prevent electrostatic-discharge (ESD) damage, follow recommended board and component handling procedures.

1. Choose one of these options to connect a device:
   - When connecting to workstations, servers, and routers, connect a straight-through cable to an RJ45 connector on the front panel.
   - When connecting to 1000BASE-T-compatible devices, use a twisted four-pair, Category 5e or higher cable.



32564-M

2. Connect the other end of the cable to an RJ45 connector on the other device.

   The Port status indicator turns on when both the switch and the connected device have an established link.

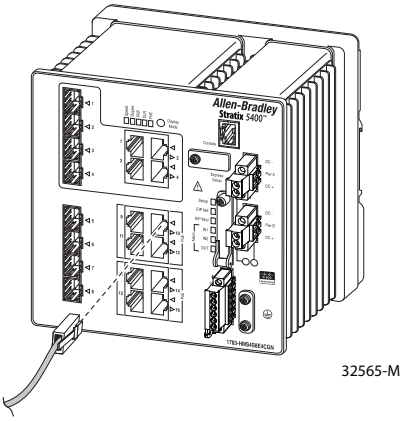
   The Port status indicator is amber while Spanning Tree Protocol (STP) discovers the topology and searches for loops. This can take up to 30 seconds, and then the Port status indicator turns green.

   The following conditions can prevent the Port status indicator from turning On:
   - The device at the other end is not turned On.
   - A problem exists with a cable or the adapter that is installed in the attached device.
3. Reconfigure and restart the connected device if necessary.
4. Repeat this procedure to connect each device.

Connect to PoE Ports

Switches with PoE ports require a separate power supply. For power supply requirements based on your application, refer to page 83.

1. Insert a straight-through, twisted four-pair, Category 5e or better cable with an RJ45 connector into the PoE port.



2. Insert the other cable end into an RJ45 connector on the other PoE powered device.

Connect to SFP Module Ports

To connect a fiber-optic cable to an SFP module, follow these steps.

ATTENTION: Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

1. Remove the rubber plugs from the module port and fiber-optic cable, and store them for future use.
2. Insert one end of the fiber-optic cable into the SFP module port.
3. Insert the other cable end into a fiber-optic receptacle on a target device.
4. Observe the port status indicator:
   - The status indicator turns amber while the SFP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port status indicator turns green.
   - The status indicator turns green when the switch and the target device have an established link.
   - The status indicator turns off if the target device is not turned on or there is a problem with the cable or the adapter that is installed in the target device.

   If necessary, reconfigure and restart the switch or the target device.

Connect to a Dual-purpose Port

A dual-purpose port is one port with two interfaces, one for an RJ45 cable and another for an approved SFP module. Only one interface can be active at a time. If both interfaces are connected, the SFP module has priority.



ATTENTION: Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

To connect to a dual-purpose port, follow these steps.

1. Connect an RJ45 connector to the 10/100/1000 port, or install an SFP module into the SFP module slot, and connect a cable to the SFP module port.
2. Connect the other end of the cable to the other device.

   By default, the switch detects whether an RJ45 connector or SFP module is connected to a dual-purpose port and configures the port accordingly. You can change this setting and configure the port to recognize only an RJ45 connector or only an SFP module by using the media type interface configuration command.

Install Stratix 5410 Switches

Topic	Page
Switch Specifications	101
Power Supply Specifications	101
Overview	102
Parts List and Required Tools	103
Install or Remove the SD Card	105
Verify Switch Operation	107
Mount the Switch on a Rack	107
Mount the Switch on a Wall	111
Ground the Switch	114
Install a Power Supply Module in the Switch	115
Wire the Power Source	116
Remove a Power Supply Module from the Switch	120
Install an SFP Module	120
Remove an SFP Module from an SFP Slot	122
Wire the External Alarms	123
Attach the Alarm Relay Connector to the Switch	124
Connect to 10/100/1000 Ethernet, PoE/PoE+ Ports	124
Connect to SFP/SFP+ Ports	126



ATTENTION: Environment and Enclosure

This equipment is intended for use in a Pollution Degree 2 industrial environment, in overvoltage Category II applications (as defined in IEC 60664-1), at altitudes up to 2000 m (6562 ft) without derating.

This equipment is not intended for use in residential environments and may not provide adequate protection to radio communication services in such environments.

This equipment is supplied as open-type equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if nonmetallic. The interior of the enclosure must be accessible only by the use of a tool. Subsequent sections of this publication may contain additional information regarding specific enclosure type ratings that are required to comply with certain product safety certifications.

In addition to this publication, see the following:

- Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1, for additional installation requirements
- NEMA Standard 250 and IEC 60529, as applicable, for explanations of the degrees of protection provided by enclosures

North American Hazardous Location Approval

The following information applies when operating this equipment in hazardous locations.	**Informations sur l'utilisation de cet équipement en environnements dangereux.**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Les produits marqués "CL I, DIV 2, GP A, B, C, D" ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**WARNING: RISQUE D'EXPLOSION** • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

North American Zones:

UL 60079-0, 5th Ed, 2009-10-21l; UL 60079-15, 3rd Ed, 2009-7-17;
CAN/CSA C22.2 No. 60079-15-12 Ed. 1; CAN/CSA C22.2 No. 60079-0-11 Ed. 2

European Hazardous Location Approval

The following applies to products marked CE Ex II 3 G: Such modules:

- Are Equipment Group II, Equipment Category 3, and comply with the Essential Health and Safety Requirements relating to the design and construction of such equipment given in Annex II to Directive 94/9/EC. See the EC Declaration of Conformity at http://www.rockwellautomation.com/products/certification for details.
- The type of protection is "Ex nA nC IIC T4 Gc" according to EN 60079-15.
- Comply to Standards EN 60079-0:2012+A11:2013, EN 60079-15:2010, reference certificate number DEMKO15ATEX1492X.
- Are intended for use in areas in which explosive atmospheres caused by gases, vapors, mists, or air are unlikely to occur, or are likely to occur only infrequently and for short periods. Such locations correspond to Zone 2 classification according to ATEX directive 1999/92/EC.

WARNING: Special Conditions for Safe Use

- This equipment shall be mounted in an ATEX Zone 2 certified enclosure with a minimum ingress protection rating of at least IP54 (as defined in EN 60529) and used in an environment of not more than Pollution Degree 2 (as defined in EN 60664-1) when applied in Zone 2 environments. The enclosure must be accessible only by the use of a tool.
- This equipment shall be used within its specified ratings defined by Rockwell Automation.
- Provision shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 140% of the rated voltage when applied in Zone 2 environments.
- Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.
- Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.
- The USB port is intended for temporary local programming purposes only and not intended for permanent connection. Do not use the USB port in hazardous locations.

WARNING: If you connect or disconnect the communication cable with power applied to this module or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

WARNING: Use supply wires suitable for 30 °C (86 °F) above surrounding ambient.

WARNING: When used in a Class I, Division 2, hazardous location, this equipment must be mounted in a suitable enclosure with proper wiring method that complies with the governing electrical codes.

WARNING: If you connect or disconnect wiring while the field-side power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

WARNING: When you insert or remove the CompactFlash/SD memory Card while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

WARNING: When you insert or remove the small form-factor pluggable (SFP) optical transceiver while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

WARNING: Do not use the USB port in hazardous locations.



ATTENTION: Prevent Electrostatic Discharge

This equipment is sensitive to electrostatic discharge, which can cause internal damage and affect normal operation. Follow these guidelines when you handle this equipment:

- Touch a grounded object to discharge potential static.
- Wear an approved grounding wriststrap.
- Do not touch connectors or pins on component boards.
- Do not touch circuit components inside the equipment.
- Use a static-safe workstation, if available.
- Store the equipment in appropriate static-safe packaging when not in use.



ATTENTION: The USB port is intended for temporary local programming purposes only and not intended for permanent connection. The USB cable is not to exceed 3.0 m (9.84 ft) and must not contain hubs.



ATTENTION: This product is grounded through the DIN rail to chassis ground. Use zinc-plated yellow-chromate steel DIN rail to assure proper grounding. The use of other DIN rail materials (for example, aluminum or plastic) that can corrode, oxidize, or are poor conductors, can result in improper or intermittent grounding. Secure DIN rail to mounting surface approximately every 200 mm (7.8 in.) and use end-anchors appropriately.



ATTENTION: Under certain conditions, viewing the optical port may expose the eye to hazard. When viewed under some conditions, the optical port may expose the eye beyond the maximum permissible exposure recommendations.



ATTENTION: Class 1 laser product. Laser radiation is present when the system is open and interlocks bypassed. Only trained and qualified personnel should be allowed to install, replace, or service this equipment.



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



ATTENTION: 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.



ATTENTION: 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.

In case of malfunction or damage, no attempts at repair should be made. The module should be returned to the manufacturer for repair. Do not dismantle the module.



ATTENTION: This equipment is certified for use only within the surrounding air temperature range of -40…60 °C (-40…140 °F). The equipment must not be used outside of this range.

ATTENTION: Use only a soft dry anti-static cloth to wipe down equipment. Do not use any cleaning agents.

ATTENTION: Electrical Safety Considerations

(Switches with DC power supply modules) To comply with the CE Low Voltage Directive (LVD), all connections to this equipment must be powered from a source compliant with the following:

- Safety Extra Low Voltage (SELV) Supply
- Protected Extra Low Voltage (PELV) Supply

Switch Specifications

For additional specifications and certifications, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Attribute	1783-IMS28NDC, 1783-IMS28RDC, 1783-IMS28GNDC, 1783-IMS28GRDC	1783-IMS28NAC, 1783-IMS28RAC, 1783-IMS28GNAC, 1783-IMS28GRAC
Power input	24…60V DC, 10 A	100…240V AC, 50…60 Hz, 2 A (per slot) or 100…250V DC, 2 A (per slot)
PoE output	54V DC, 15.4 W, max	
PoE+ output	54V DC, 30 W, max	
Alarm relay	30V DC, 1 A or 48V DC, 0.5 A	
Torque, power supply mount screw	0.904…1.13 N•m (8…10 lb•in)	
Torque, power terminal screw	0.96 N•m (± 0.06 N•m) or 8.5 lb•in (± 0.5 lb•in)	
Torque, functional ground lug screw	3.39 N•m (± 0.23 N•m) or 30 lb•in (± 2 lb•in)	
Operating temperature	-40 °C<Ta<+60 °C (-40…140 °F)	

Power Supply Specifications

Attribute	1783-IMXDC	1783-IMXAC
Input	24…60V DC, 10 A	100 …240V AC, 2.0 A 100 …250V DC, 2.0 A
Output	-54V DC…2.9 A 4.5V DC, 0.5 A	-54V DC, 2.9 A 4.5V DC, 0.5A

Overview

When determining where to place the switch, observe these guidelines:

- Airflow around the switch is unrestricted. To prevent the switch from overheating, observe these minimum clearances:
  - Top and bottom: 44.45 mm (1.75 in.)
  - Sides: 50.8 mm (2.0 in.)
  - Front: 50.8 mm (2.0 in.)
- For 10/100/1000 Ethernet, PoE/PoE+ ports, the cable length from a switch to an attached device cannot exceed 100 m (328 ft).
- The fiber-optic cable length from a switch to an attached device cannot exceed the distance that is specified in Appendix D.
- Temperature surrounding the unit must be in a range of -40...60 °C (-40...140 °F).
- Clearance to front and rear panels meets these conditions:
  - Front- or back-panel status indicators can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Power and alarm relay connectors are within reach of the connection to the AC or DC power source.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.



ATTENTION: Do not wire more than 1 conductor on any single terminal.

Follow these steps to install the switch.

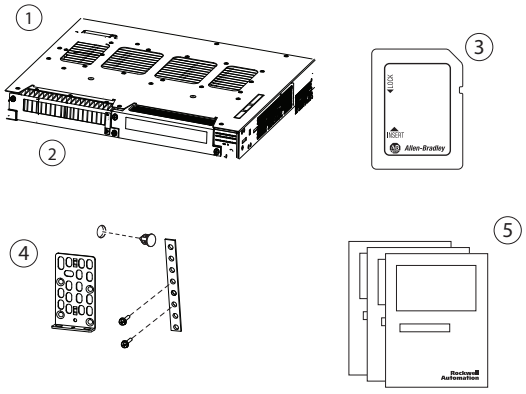
1. (Optional) Install or remove the SD card.
2. Verify switch operation.
3. Mount the switch on a rack.

   or

   Mount the switch on a wall.
4. Ground the switch.
5. (Optional) Install a second power supply module in the switch.
6. Wire the power source.
7. (Optional) Install an SFP module.
8. Wire external alarms and attach the alarm relay connector to the switch.
9. Connect to switch ports:
   - Ethernet, PoE/PoE+ ports
   - SFP/SFP+ ports

Parts List and Required Tools

Verify that you have these items. The Secure Digital (SD) card and power supply comes pre-installed in the switch.



1 Stratix® 5410 switch

2 Power supply module

3 SD card

4 Mounting kit(1)

5 Documentation

(1) Replacement kits can be ordered by requesting part number 53-100573-01.



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

Obtain these tools:

- Ring, spade, or flanged spade terminal (terminals should be insulated)
  - Ring terminal (such as Tyco part number 2-34158-1 for 16...14 AWG or 2-34852-1 for 12...10 AWG wire)
  - Spade terminal (such as Tyco part number 54367-2 for 16...14 AWG wire)
  - Flanged spade terminal (such as Tyco part number 2-324165-1 for 16...14 AWG wire or 1-324581-1 for 12...10 AWG wire)
- Crimping tool, such as Thomas & Bett part number WT2000, ERG-2001, or equivalent
- 6-gauge copper ground wire, such as Belden part number 9906 or equivalent
- 12-AWG wire (minimum) for the low-voltage power-supply module and 16-AWG (minimum) wire for the high-voltage power-supply module
- For power source connections, use wires that are rated for at least 194°F (90°C).
- UL- and CSA-rated style 1007 or 1569 twisted-pair copper wire, such as Belden part number 9318
- Wire-stripping tools for stripping 6-, 10-, 12-, 14-, and 16-gauge wires.
- Number-2 Phillips screwdriver
- Flat-blade screwdriver

For simplified cabling, the automatic medium-dependent interface crossover (auto-MDIX) feature is enabled by default on the switch. With auto-MDIX enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a 10/100/1000 Ethernet, PoE/PoE+ switch port, regardless of the type of device on the other end of the connection.

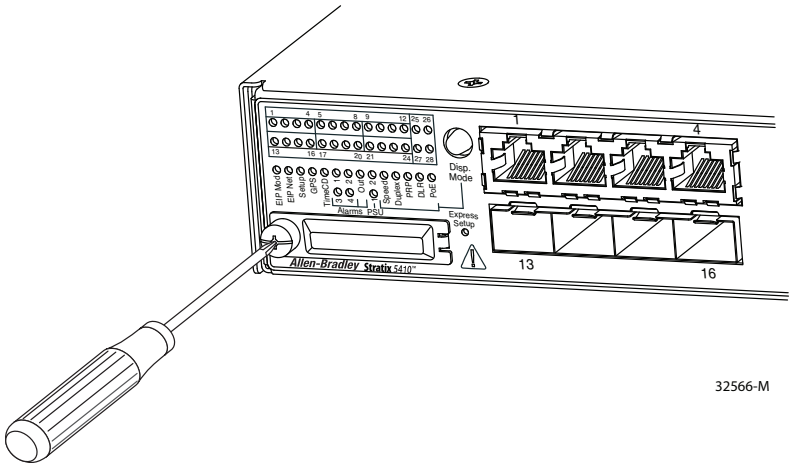
Install or Remove the SD Card

A Secure Digital (SD) card ships with the Stratix 5410 switch. The SD card contains the switch firmware and initial configuration. You can order a replacement SD card from Rockwell Automation, catalog number 1784-SD1, if needed. The replacement card ships without firmware and must be synced with the internal memory of the switch. See page 64.

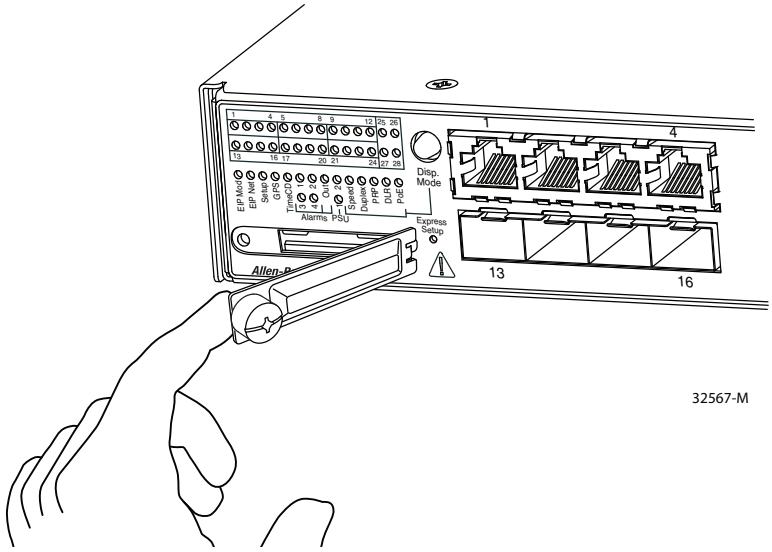
To install or replace the SD card, follow these steps.

1. On the front of the switch, locate the door that protects the SD card slot.
2. Loosen the captive thumb screw on the door by using a screwdriver and open the door.

   Use caution when removing the non-captive door.



32566-M

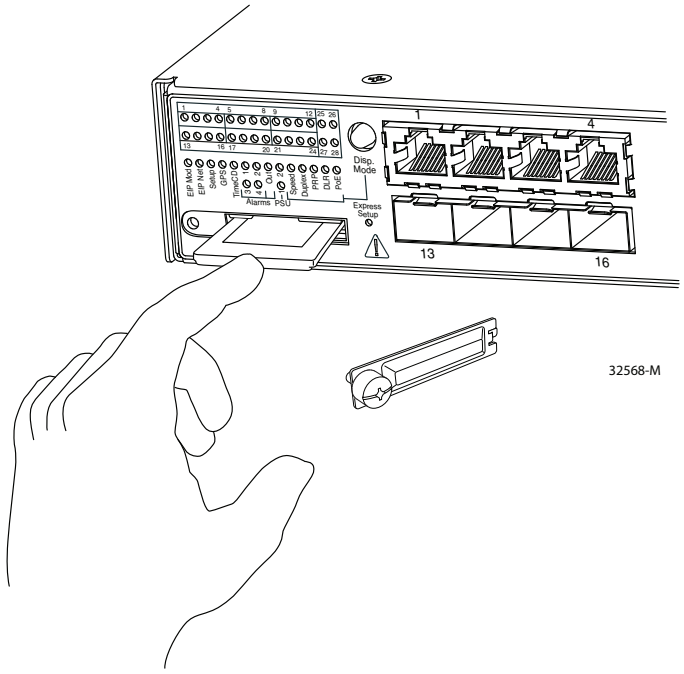


32567-M

3. Install or remove the card.

   To install the card, slide it into the slot, and press it firmly in place until it latches in the spring loaded mechanism. The card is keyed so that you cannot fully insert it the wrong way.

   To remove the card, push it in and let it pop out via the spring-loaded mechanism. Grasp the card top and pull it out. Place it in an antistatic bag to protect it from static discharge.



4. Close the guard door and fasten the captive screw by using a screwdriver to keep the door in place.

Verify Switch Operation

Before installing the switch in its final location, power on the switch, and verify that the switch powers up.

The time that is required for the switch to start up is directly related to your switch configuration. Start time is negatively affected by such things as the following:

- Spanning Tree Learning mode
- Number of files or images in onboard memory

To test the switch, follow these steps.

1. Apply power to the switch.

   If the switch is directly connected to a power source, locate the circuit breaker on the panel board that services the circuit. Switch the circuit breaker to the On position.

2. Verify the start-up process.

   When you power on the switch, it begins a start-up process. The Setup status indicator blinks green as the IOS software image loads. If the process fails, the Setup status indicator turns red.

   IMPORTANT Start-up failures can be fatal to the switch. Contact your Rockwell Automation representative immediately if your switch does not complete the start-up process successfully.

   IMPORTANT You can disable Boot Fast and run the Power-on self-test (POST) by using the CLI. For more information, see the documentation at http://www.Cisco.com.

3. After successfully running this test, do the following:
   a. Turn off power to the switch.
   b. Disconnect the cables.
   c. Decide where you want to install the switch.

Mount the Switch on a Rack

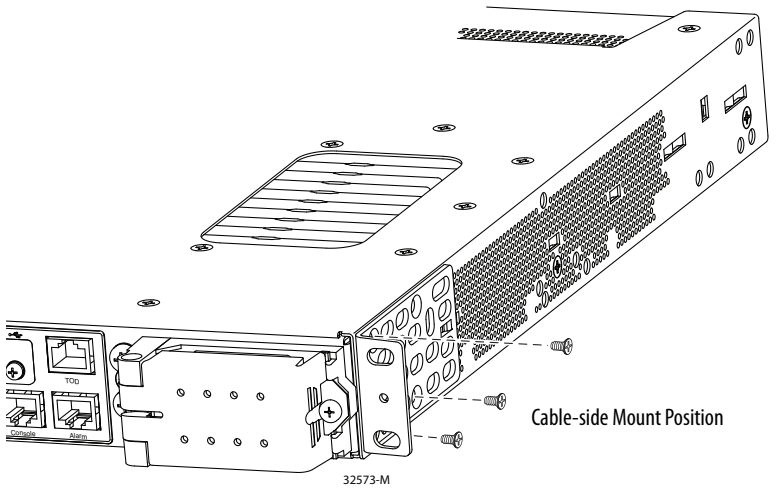
To mount the switch on a rack, see the following:

- Attach Brackets on page 108
- Mount the Switch on page 110

Attach Brackets

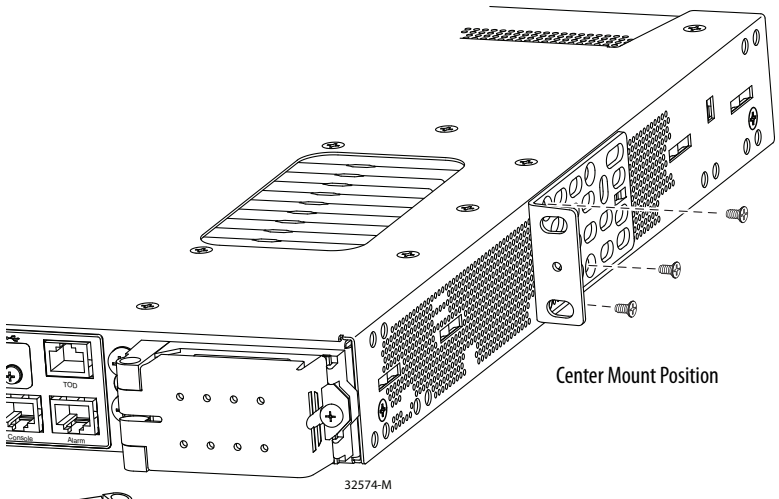
To attach brackets on the switch, follow this procedure.

1. Identify a mount position and attach brackets to both sides of the switch.



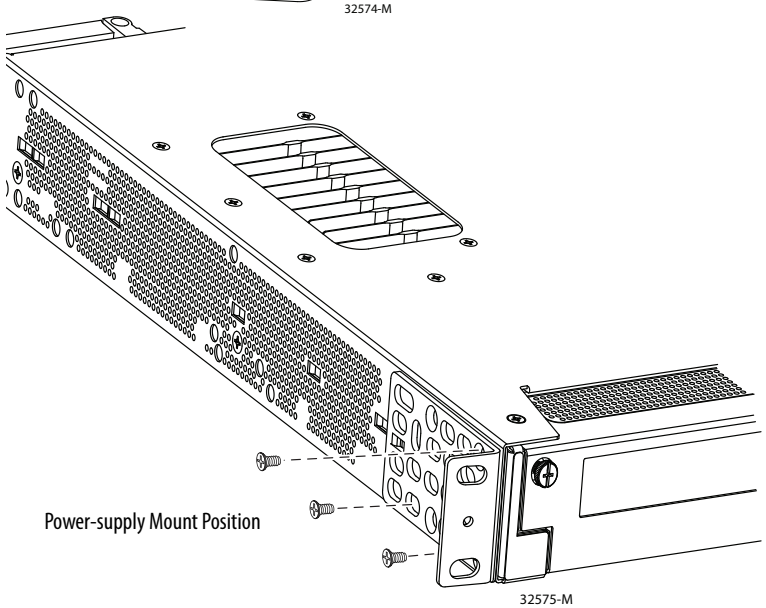
Cable-side Mount Position

32573-M



Center Mount Position

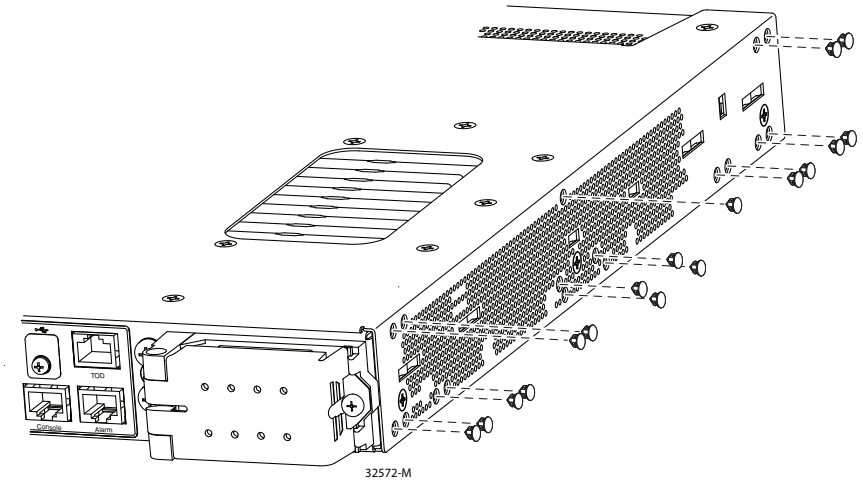
32574-M



Power-supply Mount Position

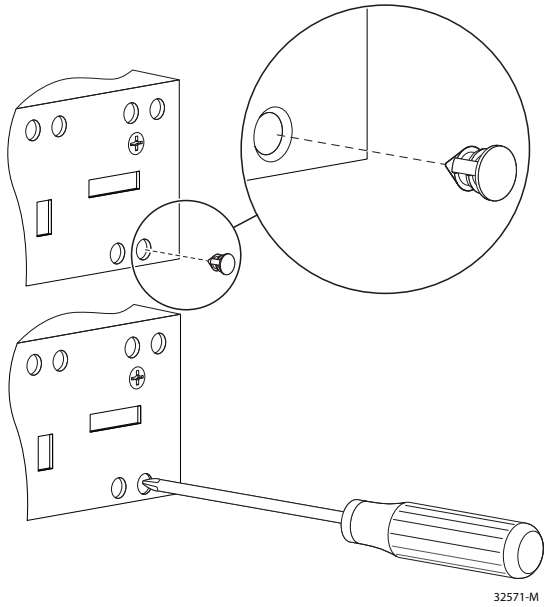
32575-M

2. Insert the rubber plugs in the unused holes on both sides of the switch.



32572-M

3. Use a screwdriver or pen to push in the rubber plugs completely.

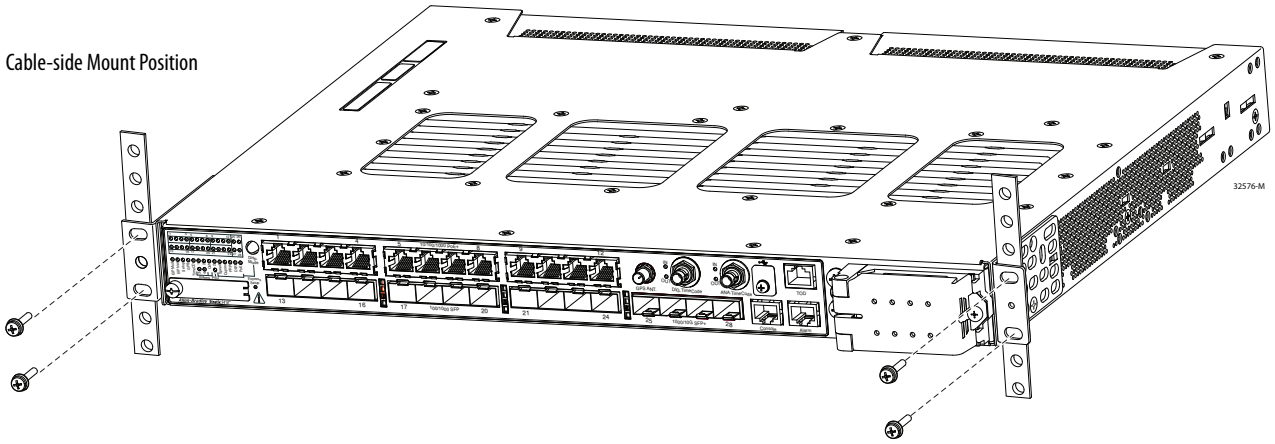


32571-M

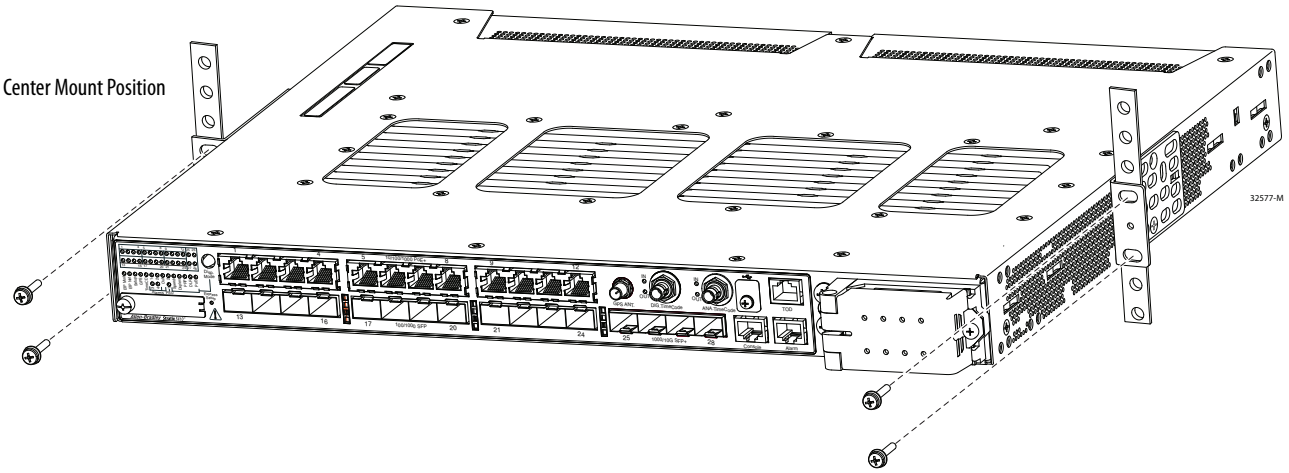
Mount the Switch

After you attach the brackets on the switch, use the four supplied number-12 Phillips machine screws to attach the brackets to the rack.

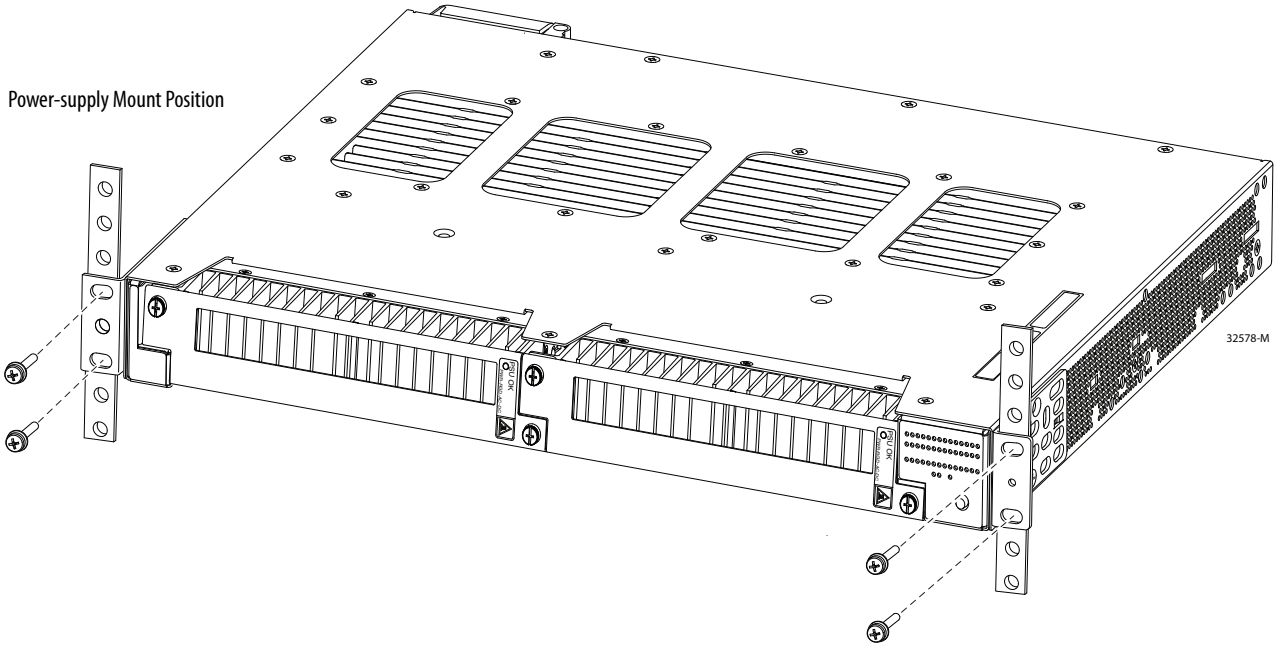
Cable-side Mount Position



Center Mount Position



Power-supply Mount Position



Mount the Switch on a Wall

To mount the switch on a wall, see the following:

- Attach the Brackets on page 111
- Mount the Switch on page 113

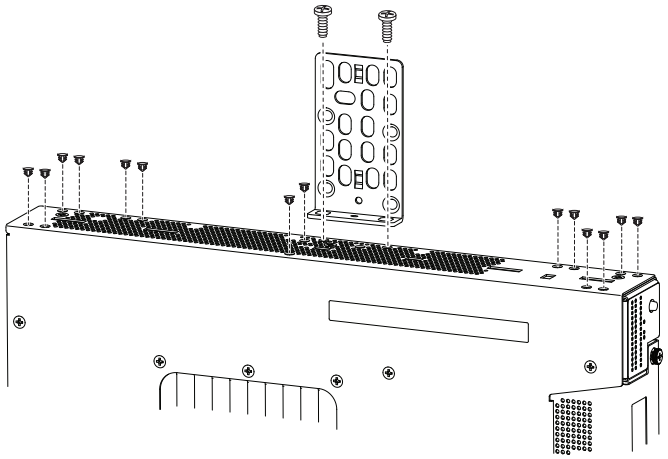
IMPORTANT To mount the switch on a wall in an enclosure, follow these minimum clearances:

- Sides of switch facing up and facing down: 9.52 cm (3.75 in.)
- Port side: 7.62 cm (3.0 in.)
- Power supply side: 13.33 cm (5.25 in.)
- Cover side not facing wall: 4.44 cm (1.75 in.)
- Base side facing wall: 0 cm (0 in.)

Attach the Brackets

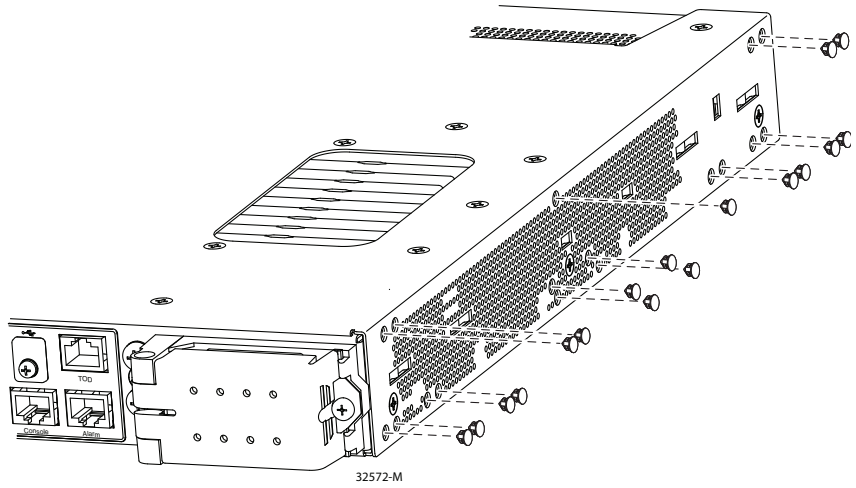
To attach brackets to the switch, follow this procedure.

1. Attach the brackets on both sides of the switch.



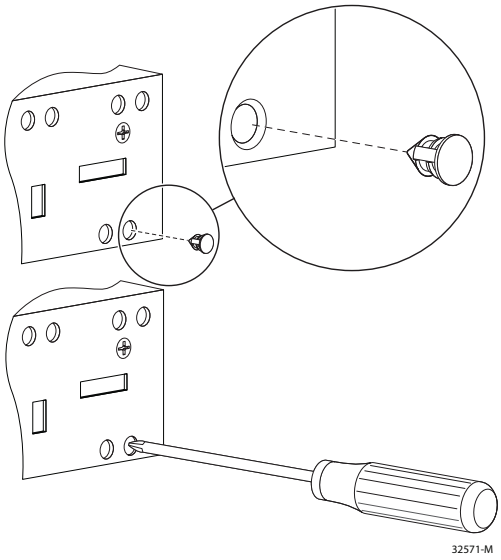
32579-M

2. Insert the rubber plugs in the unused holes on both sides of the switch.



32572-M

3. Use a screwdriver or pen to push in the rubber plugs completely.

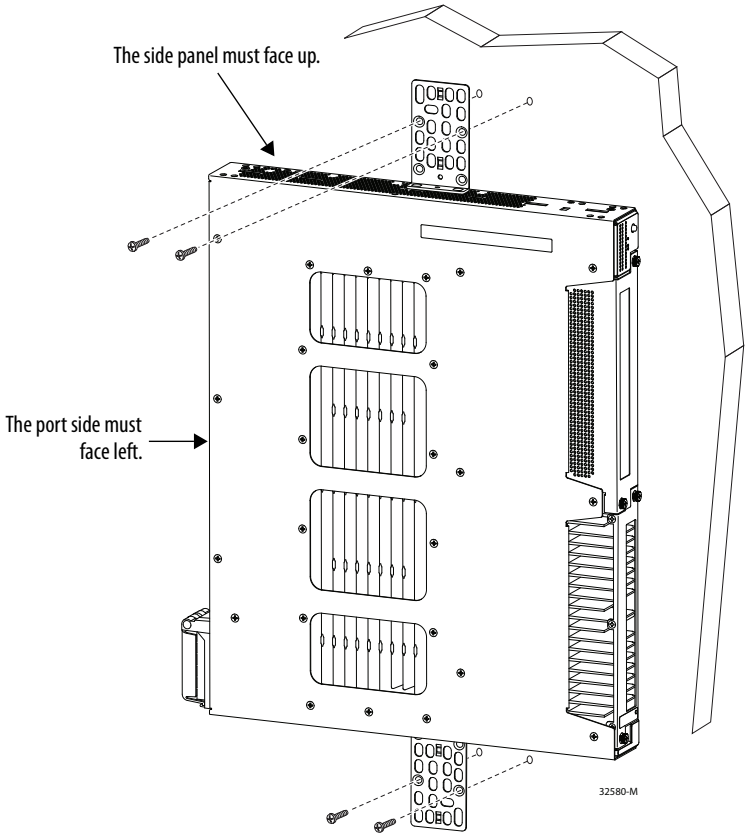


32571-M

Mount the Switch

The switch can be mounted on a wall in only one position: the side panel must face up, and the port side must face left.

For the best support of the switch and cables, make sure that the switch is attached securely to wall studs or to a firmly attached plywood backboard.



Ground the Switch

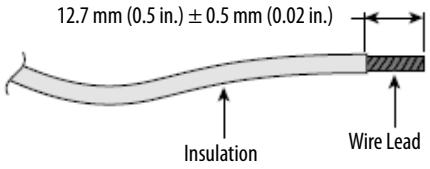
To ground the switch, follow these steps. Be sure to follow any grounding requirements at your site.

1. To remove the ground screw from the cable side of the switch, use a Phillips screwdriver or a ratcheting torque screwdriver with a Phillips head.

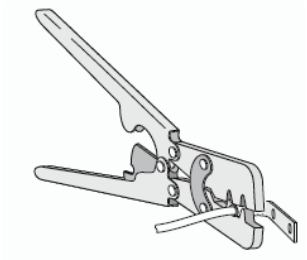
   Store the ground screw for later use.

2. Strip the 13.3 mm^2 (6 AWG) ground wire to 12.7 mm (0.5 in.) ± 0.5 mm (0.02 in.).

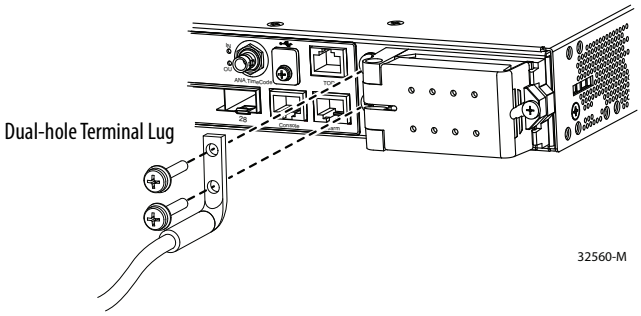
   Stripping more than the recommended amount of wire can leave exposed wire from the connector.



3. Insert the ground wire into the terminal lug, and crimp the terminal to the wire.



4. Slide the ground screw from Step 1 through the terminal lug, and insert the ground screws into the opening on the cable side.



5. Use a ratcheting-torque screwdriver to tighten the ground screws to 3.39 N•m (± 0.23 N•m) or 30 lb•in (± 2 lb•in).
6. Attach the other end of the ground wire to a grounded bare metal surface, such as a ground bus or a grounded bare rack.

Install a Power Supply Module in the Switch

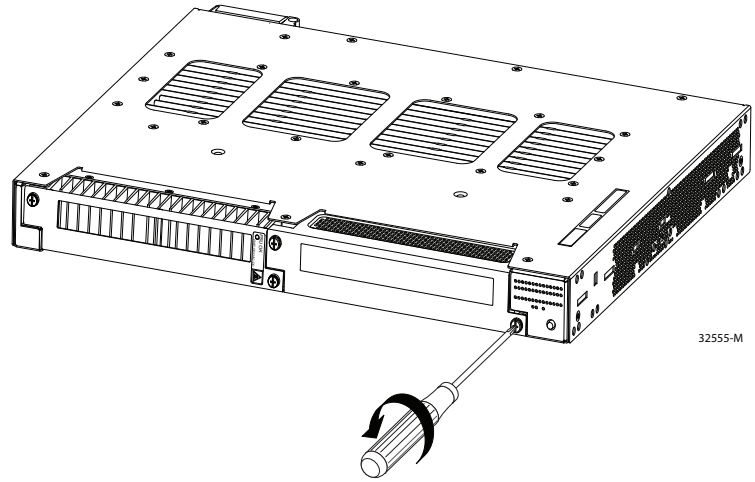
The switch ships with one pre-installed power supply. To install a second power supply, follow these steps.

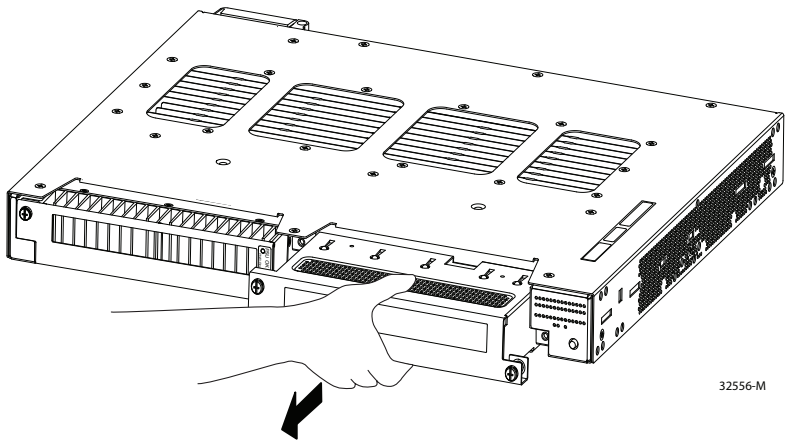
WARNING: If you connect or disconnect wiring while the field-side power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

1. Turn power off at the AC and DC circuits.

   IMPORTANT If the power is not off at the AC or DC circuit breaker, do not touch the power-input terminal.

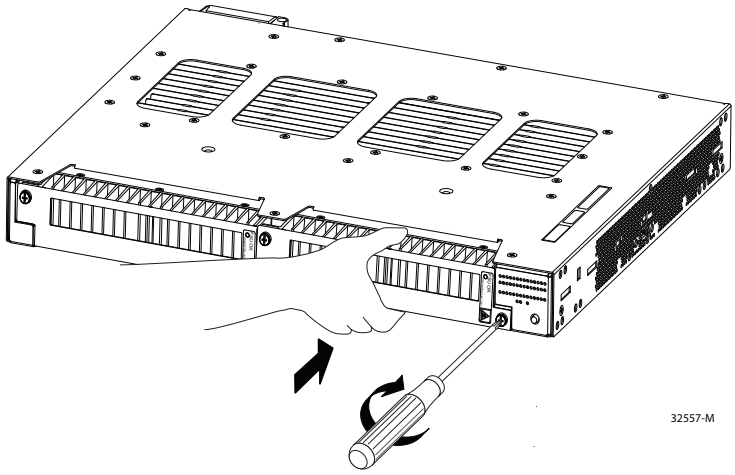
2. To loosen the two captive screws of the blank power-supply module and gently pull it out, use a Phillips screwdriver.





3. Insert the power supply module into the slot, and gently push it in.

   When inserted correctly, the power-supply module is flush with the switch.



4. Use a ratcheting torque screwdriver to torque each screw to 0.904...1.13 N•m (8...10 lb•in).

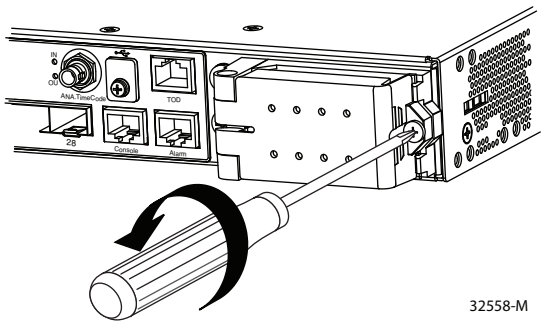
Wire the Power Source

To wire the power source, follow these steps.

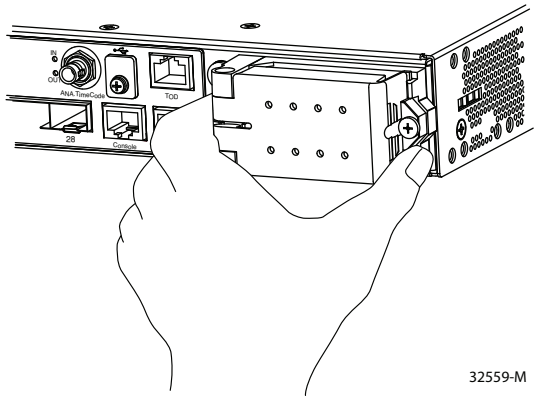
1. Turn power off at the AC and DC circuits.

IMPORTANT	If the power is not off at the AC or DC circuit breaker, do not touch the power-input terminal.

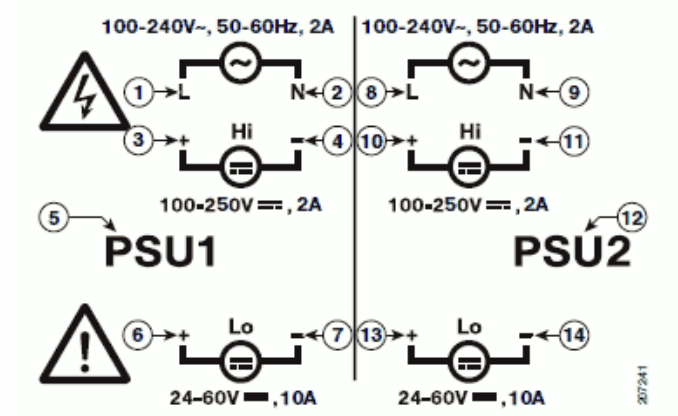
2. To loosen the captive screw on the power input terminal, use a Phillips screwdriver.



3. Open the cover.



The terminal screws labels are on the power-input terminal cover.



1	Line connection for high-voltage AC (PSU1)	8	Line connection for high-voltage AC (for PSU2)
2	Neutral connection for high-voltage AC (PSU1)	9	Neutral connection for high-voltage AC (PSU2)
3	Positive connection for high-voltage DC (PSU1)	10	Positive connection for high-voltage DC (PSU2)
4	Negative connection for high-voltage DC (PSU1)	11	Negative connection for high-voltage DC (PSU2)
5	PSU1 (power-supply module 1)	12	PSU2 (power-supply module 2)
6	Positive connection for low-voltage DC (PSU1)	13	Positive connection for low-voltage DC (PSU2)
7	Negative connection for low-voltage DC (PSU1)	14	Negative connection for low-voltage DC (PSU2)

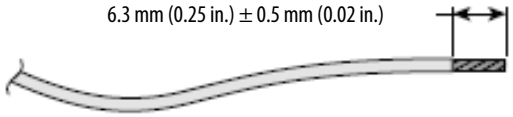
IMPORTANT The power supply module 1 connection is labeled PSU1, and the power supply module 2 connection is labeled PSU2. Make sure that you connect the wires to the correct terminal screws.

4. To connect from the power-input terminal to the power source, use twisted-pair copper wire (12-AWG to 18-AWG).

IMPORTANT Use 12 AWG (minimum) for the low-voltage DC power supply module. Use 16 AWG (minimum) for the high-voltage AC or DC power supply module.

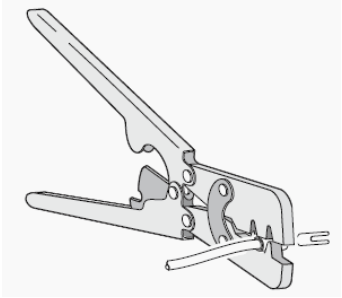
5. Strip each of the two wires to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wire. Stripping more than the recommended amount of wire can leave exposed wire from the connector after installation.



6. Insert the wire into a spade terminal, and crimp it to the wire.

   You can also use a ring or flanged spade terminal.



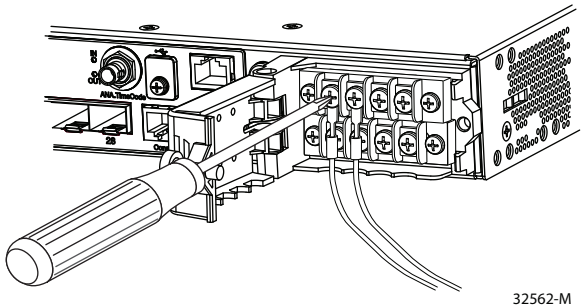
7. Loosen the terminal screw, and slide the terminal under the screw and washer.

IMPORTANT	Use the appropriate terminal screws that are based on power supply type: high-voltage (AC or DC) or a low-voltage (DC).

8. Make the power connection:

IMPORTANT	Make sure that you cannot see any wire lead. Only wire with insulation should extend from the terminal screw.

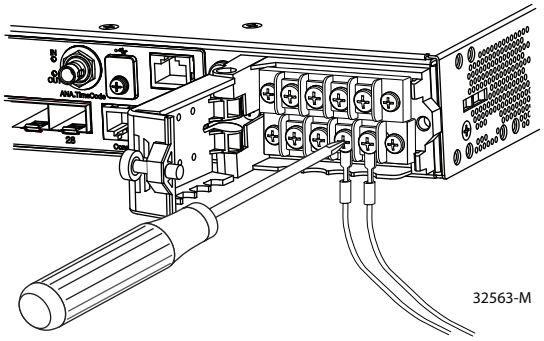
   - For AC power, connect the line wire into the terminal screw that is labeled L and the neutral wire into the terminal screw labeled N.



- For DC power, connect the positive wire into the terminal screw that is labeled +, and the negative wire into the terminal screw labeled -.

  For low-voltage DC power, connect the wires to the terminals labeled Lo.

  For high-voltage DC power, connect the wires to the terminals labeled Hi.



9. Torque the captive screws above the wires to 0.79 N•m (7 lb•in).
10. Complete the power connection:

IMPORTANT Make sure that you cannot see any wire lead. Only wire with insulation should extend from the terminal screw.

- For AC power, connect the other end of the line wire (the one connected to L) to the line terminal on the AC power source. Connect the other end of the neutral wire (the one connected to N) to the neutral terminal on the AC power source.
- For DC power, connect the other end of the positive wire (the one connected to +) to the positive terminal on the DC power source. Connect the other end of the negative wire (the one connected to –) to the negative terminal on the DC power source.

11. Close the power input terminal cover.
12. Use a ratcheting torque screwdriver to torque the screw to 0.79 N•m (7 lb•in).
13. Turn on the power at the AC or DC circuit.
14. Verify that the PSU 1 or 2 status indicator on the switch and PSU OK status indicator on the power supply module are green.

Remove a Power Supply Module from the Switch

By removing the power-supply modules, you can power off the switch without disconnecting the wiring from the power-input terminal.

To remove a power supply module from the switch, follow these steps.

1. Turn power off at the AC and DC circuits.

   IMPORTANT If the power is not off at the AC or DC circuit breaker, do not touch the power-input terminal.

2. Verify that the PSU 1 or 2 and PSU OK status indicators are blinking red or are off.
3. Use a Phillips screwdriver to loosen the captive screws that secure the power-supply module to the switch.
4. Remove the power-supply module from the power slot. The power-supply module might be hot.
5. Install a new power-supply module or a blank cover.

Install an SFP Module



WARNING: When you insert or remove the small form-factor pluggable (SFP) optical transceiver while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.
Be sure that power is removed or the area is nonhazardous before proceeding.



ATTENTION: Under certain conditions, viewing the small form-factor pluggable (SFP) optical transceiver may expose the eye to hazard. When viewed under some conditions, the optical port may expose the eye beyond the maximum permissible exposure recommendations.



ATTENTION: Use SFP modules from only Rockwell Automation. For details about supported modules, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.



ATTENTION: We strongly recommend that you do not install or remove the SFP module with fiber-optic cables attached. If you leave the cables attached, damage to the cables, the cable connector, or the optical interfaces in the SFP module can occur. Disconnect all cables before removing or installing an SFP module.

IMPORTANT Installing and removing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is necessary.

SFP modules are inserted into SFP module slots on the front of the switch. These field-replaceable modules provide the uplink optical interfaces, send (TX) and receive (RX).

You can use any combination of compatible SFP modules:

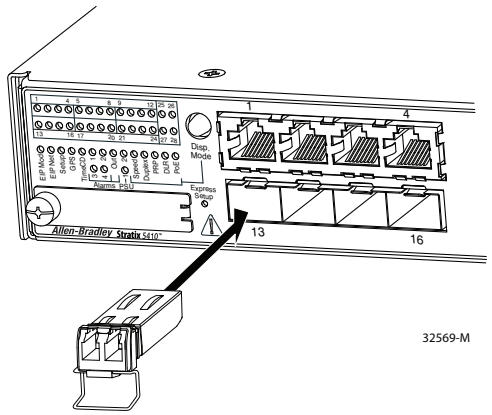
- Each SFP module must be of the same type as the SFP module on the other end of the cable. The cable must not exceed the stipulated cable length for reliable communications.
- Once you install SFP modules in the switch, be aware that the overall temperature rating of the combined modules (switch and SFP modules) is limited to the lowest maximum temperature rating and the highest minimum temperature rating.

For cable length and temperature specifications, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

To insert an SFP module into an SFP slot, follow these steps.

1. Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface.
2. Find the send (TX) and receive (RX) markings on the top of the module.

   On some SFP modules, the send and receive (TX and RX) markings are replaced by arrows that show the direction of the connection.
3. If the module has a bale-clasp latch, move it to the open, unlocked position.
4. Align the module in front of the slot opening and push until you feel the connector snap into place.



5. If the module has a bale-clasp latch, close it.

6. For fiber-optic SFP modules, remove the dust plugs and save.

ATTENTION: Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

7. Connect the SFP cables.

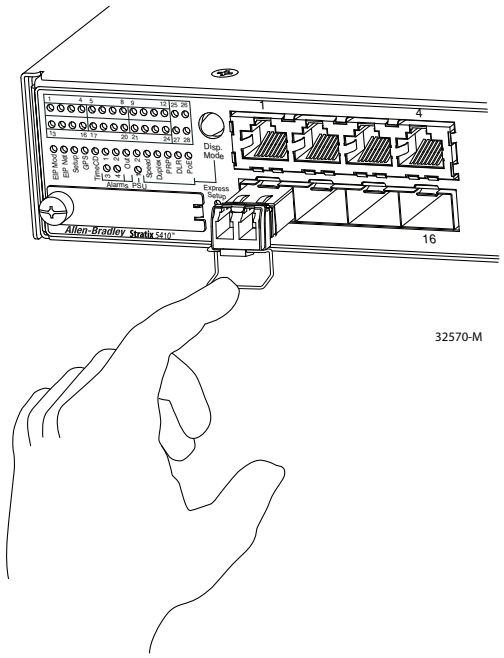
Remove an SFP Module from an SFP Slot

To remove an SFP module from an SFP slot, follow these steps.

1. Attach an ESD-preventive wriststrap to your wrist and to a bare metal surface.
2. Disconnect the cable from the SFP module.

   For reattachment, note which cable connector plug is send (TX) and which is receive (RX).
3. Insert a dust plug into the optical ports of the SFP module.
4. If the module has a bale-clasp latch, pull the bale out and down to eject it.

   If the latch is obstructed and you cannot use your finger, use a small, flat-blade screwdriver or other long, narrow instrument.



5. Grasp the SFP module, and carefully remove it from the slot.
6. Place the module in an antistatic bag or other protective environment.

Wire the External Alarms

The switch has four alarm inputs and one Form C (single-pole, double-throw) alarm output relay circuits for external alarms. The input alarm relay circuits are designed to sense if the alarm input is open or closed relative to the alarm input reference pin. The output alarm relay circuit has one Form C relay, with one normally open (NO) and one normally closed (NC) contact. You can configure the output alarm relay as either normally energized or normally de-energized by using the CLI.

See Appendix D for an alarm wiring example.

Alarm signals are connected to the switch through the 8-way alarm relay RJ45 connector. Five connections are dedicated to the four alarm input circuits:

- Alarm input 1
- Alarm input 2
- Alarm input 3
- Alarm input 4
- Common

An alarm input and the common wiring connection are required to complete one input alarm circuit. You must provide either an NO or an NC dry contact to complete the alarm circuit between common and one of the four alarm inputs.



ATTENTION: Do not apply an external voltage source to the alarm inputs. Limit alarm output wiring to 48 V DC, 0.5 A.

The three remaining connections for the Form C output alarm circuit are as follows:

- NO output
- NC output
- Common

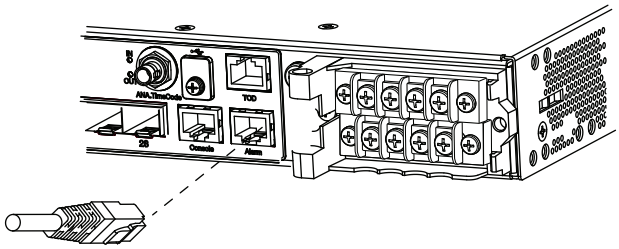
An alarm output and the common wiring connection are required to complete one output alarm circuit. The Form C output alarm relay provides one NO and one NC dry contact.



ATTENTION: Wire connections to the power and relay connector, must be UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

Attach the Alarm Relay Connector to the Switch

Insert the alarm relay RJ45 connector into the receptacle on the switch front panel.



Connect to 10/100/1000 Ethernet, PoE/PoE+ Ports

The 10/100/1000 ports on the switch automatically configure themselves to operate at the speed of attached devices. If the attached ports do not support autonegotiation, you can explicitly set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have their speed and duplex parameters that are manually set can reduce performance or result in no linkage.

The Auto-MDIX feature is enabled by default. Unless this feature is disabled, you can use either straight-through or crossover cables to connect to other devices on the network.

To maximize performance, choose one of these methods for configuring the Ethernet ports:

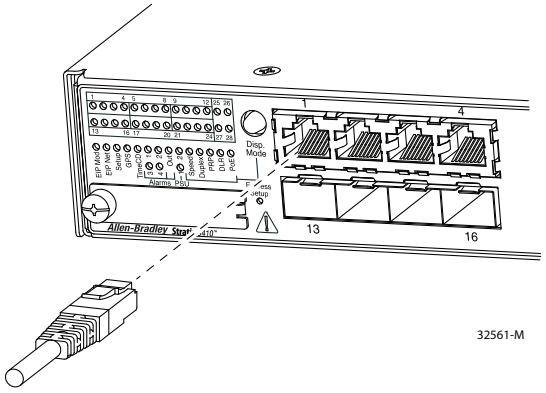
- Let the ports autonegotiate both speed and duplex
- Set the port speed and duplex parameters on both ends of the connection

To connect a device to a 10/100/1000 Ethernet, PoE/PoE+ port, follow these steps.

1. Choose one of these options:
   - If the auto-MDIX feature is enabled, connect either a crossover or straight-through cable to an RJ45 connector on the front panel. The default setting for auto-MDIX is enabled.
   - If auto-MDIX is disabled, use the following guidelines to choose the cable for connecting the 10/100/1000Ethernet ports to other devices.

Device	Crossover Cable(1)	Straight-through Cable(1)
Switch to switch	Yes	No
Switch to hub	Yes	No
Switch to computer or server	No	Yes
Switch to router	No	Yes

(1) 100BASE-TX and 1000BASE-T traffic requires twisted four-pair, Category 5, Category 5e, or Category 6 cable. 10BASE-T traffic uses Category 3 or Category 4 cable.



2. Connect the other end of the cable to an RJ45 connector on the other device.

   The port status indicator turns on when both the switch and the connected device have an established link.

   The port status indicator is amber while Spanning Tree Protocol (STP) discovers the topology and searches for loops. This process can take as long as 30 seconds, and then the Port status indicator turns green.

   The following conditions can prevent the Port status indicator from turning On:
   - The device at the other end is not turned On.
   - A problem exists with a cable or the adapter that is installed in the attached device.
3. Reconfigure and restart the connected device if necessary.
4. To connect another device, repeat this procedure.

Connect to SFP/SFP+ Ports

To connect a fiber-optic cable to an SFP or SFP+ module, follow these steps.

1. Remove the rubber plugs from the module port and fiber-optic cable, and store them for future use.
2. Insert one end of the fiber-optic cable into the SFP module port.
3. Insert the other cable end into a fiber-optic receptacle on a target device.
4. Observe the port status indicator:
   - The status indicator turns amber while the SFP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port status indicator turns green.
   - The status indicator turns green when the switch and the target device have an established link.
   - The status indicator turns off if the target device is not turned on or there is a problem with the cable or the adapter in the target device.
5. If necessary, reconfigure and restart the switch or the target device.

Install Stratix 5700 Switches

Topic	Page
Specifications	130
Overview	130
Parts List and Required Tools	132
Install or Remove the SD Card	133
Verify Switch Operation	134
Mount the Switch on a DIN Rail	135
Remove the Switch from the DIN Rail	137
Ground the Switch	137
Wire the Switch DC Power Source	139
Attach the Switch Power Connectors	143
Wire the Power over Ethernet DC Power Source	144
Attach the PoE Power Connector	145
Install an SFP Module	146
Remove an SFP Module from an SFP Slot	148
Wire the External Alarms	149
Attach the Alarm Relay Connector to the Switch	152
Connect to 10/100 and 10/100/1000 Ports	152
Connect to 10BASE-T, 100BASE-TX, or 1000BASE-T Ports	153
Connect to PoE Ports	154
Connect to SFP Module Ports	154
Connect to a Dual-purpose Port	155

ATTENTION: Environment and Enclosure

This equipment is intended for use in a Pollution Degree 2 industrial environment, in overvoltage Category II applications (as defined in IEC 60664-1), at altitudes up to 2000 m (6562 ft) without derating.

This equipment is not intended for use in residential environments and may not provide adequate protection to radio communication services in such environments.

This equipment is supplied as open-type equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if nonmetallic. The interior of the enclosure must be accessible only by the use of a tool. Subsequent sections of this publication may contain additional information regarding specific enclosure type ratings that are required to comply with certain product safety certifications.

In addition to this publication, see the following:

- Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1, for additional installation requirements
- NEMA Standard 250 and IEC 60529, as applicable, for explanations of the degrees of protection provided by enclosures

North American Hazardous Location Approval

The following information applies when operating this equipment in hazardous locations.	**Informations sur l'utilisation de cet équipement en environnements dangereux.**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Les produits marqués "CL I, DIV 2, GP A, B, C, D" ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**WARNING: RISQUE D'EXPLOSION** • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

European Hazardous Location Approval

The following applies to products marked CE Ex II 3 G: Such modules:

- Are Equipment Group II, Equipment Category 3, and comply with the Essential Health and Safety Requirements relating to the design and construction of such equipment given in Annex II to Directive 94/9/EC. See the EC Declaration of Conformity at http://www.rockwellautomation.com/products/certification for details.
- The type of protection is "Ex nA nC IIC T3 Gc" according to EN 60079-15.
- Are intended for use in areas in which explosive atmospheres caused by gases, vapors, mists, air or dust mixtures are unlikely to occur, or are likely to occur only infrequently and for short periods. Such locations correspond to Zone 2 classification according to ATEX directive 1999/92/EC.
- Comply to Standards: EN 60079-0:2012, EN 60079-15:2010, reference certificate number DEMKO 12 ATEX8694536X.

ATTENTION: This equipment is not resistant to sunlight or other sources of UV radiation.

WARNING: Special Conditions for Safe Use

- This equipment shall be mounted in an ATEX certified enclosure with a minimum ingress protection rating of at least IP54 (as defined in IEC60529) and used in an environment of not more than Pollution Degree 2 (as defined in IEC 60664-1) when applied in Zone 2 environments. The enclosure must utilize a tool removable cover or door.
- This equipment shall be used within its specified ratings defined by Rockwell Automation.
- Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.
- Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.
- The USB port is intended for temporary local programming purposes only and not intended for permanent connection and do not use the USB port in hazardous locations.
- Provision shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 140% of the rated voltage when applied in Zone 2 environments.

WARNING: If you connect or disconnect Ethernet cables with power applied to this module or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: The alarm port cables are not to exceed 10.0 m (32.81 ft).

Specifications

For additional specifications and certifications, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Table 25 - Stratix 5700 Switches

Attribute	1783-BMS4S2SGL, 1783-BMS4S2SGA, 1783-BMS06SL, 1783-BMS06SA, 1783-BMS06TL, 1783-BMS06TA, 1783-BMS06SGL, 1783-BMS06SGA, 1783-BMS06TGL, 1783-BMS06TGA, 1783-BMS10CL, 1783-BMS10CA, 1783-BMS10CGL, 1783-BMS10CGA,1783-BMS10CGP, 1783-BMS10CGN	1783-BMS20CL, 1783-BMS20CA, 1783-BMS20CGL, 1783-BMS20CGP, 1783-BMS20CGPK, 1783-BMS20CGN
Wire size, power connectors	0.5…0.8 mm^2 (18…20 AWG) twisted-pair copper wire suitable for 30 °C (86 °F) above surrounding ambient temperature outside of the enclosure	
Screw torque, ground terminals	0.4 N•m (3.5 lb•in)	
Screw torque, power terminals	0.23 N•m (2.0 lb•in)	
Alarm relay ratings	30V DC, 1.0 A or 48V DC, 0.5 A	
Power supply	12…48V DC, 0.5 … 2.0 A max	12…48V DC, 0.5 …3.0 A max

Table 26 - Stratix 5700 Power over Ethernet Switches

Attribute	1783-BMS12T4E2CGL, 1783-BMS12T4E2CGP, 1783-BMS12T4E2CGNK		
Wire size, power connectors	0.5…0.8 mm^2 (18…20 AWG) twisted-pair copper wire suitable for 30 °C (86 °F) above surrounding ambient temperature outside of the enclosure		
Screw torque, ground terminals	0.4 N•m (3.5 lb•in)		
Screw torque, power terminals	0.23 N•m (2.0 lb•in)		
Alarm relay ratings	30V DC, 1.0 A or 48V DC, 0.5 A		
Switch power input	12…48V DC, 0.5…3.0 A max		
PoE power input	**Application**	**Power Consumption**	**Power Supply per Port**
	PoE only (IEEE 802.3af)	44…57V DC (48V DC nom)	15.4 W, max for PoE
	PoE and PoE+ (IEEE 802.3at Type 2)	50…57V DC (54V DC nom)	30 W, max for PoE+

Overview

When determining where to place the switch, observe these guidelines:

- For 10/100 ports and 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 100 m (328 ft).
- The fiber-optic cable length from a switch to an attached device cannot exceed the distance that is specified in Appendix D.
- For maximum noise immunity, shielded cables must be used on the RJ45 uplink ports (Gi1/1 and Gi1/2) on these switches:
  - 1783-BMS06TGL
  - 1783-BMS06TGA
  - 1783-BMS10CGL
  - 1783-BMS10CGA
  - 1783-BMS10CGN
  - 1783-BMS10CGP
  - 1783-BMS12T4E2CGNK
  - 1783-BMS12T4E2CGP
  - 1783-BMS12T4E2CGL
  - 1783-BMS20CGL
  - 1783-BMS20CGN
  - 1783-BMS20CGP
  - 1783-BMS20CGPK

- Temperature surrounding the unit does not exceed 60 °C (140 °F).

IMPORTANT	When the switch is installed in an industrial enclosure, the temperature within the enclosure is greater than normal room temperature outside the enclosure. The temperature inside the enclosure cannot exceed 140 °F (60 °C), the maximum ambient enclosure temperature of the switch.

- Clearance to front and rear panels meets these conditions:
  - Front-panel status indicators can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Front-panel direct current (DC) power connectors and the alarm relay connector are within reach of the connection to the DC power source.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.
- Connect the unit to only a Class 2 DC power source.



ATTENTION: Do not wire more than 1 conductor on any single terminal.

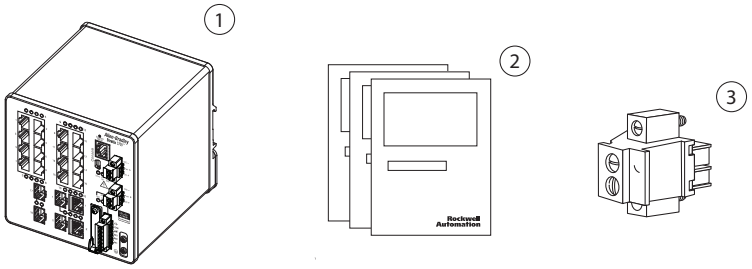
Follow these steps to install the switch.

1. (Optional) Install or remove the SD card.
2. Verify switch operation.
3. Mount the switch on a DIN rail.
4. Ground the switch.
5. Wire the DC power source for the switch and attach the switch power connectors.
6. (Optional) Wire the Power over Ethernet (PoE) DC power source and attach the PoE power connector.
7. (Optional) Install an SFP module.
8. Wire external alarms and attach the alarm relay connector to the switch.
9. Connect to the switch ports:
   - 10/100 copper ports and 10/100/1000 ports
   - 10BASE-T, 100BASE-TX, and 10000BASE-T ports
   - PoE ports
   - SFP module ports
   - Dual-purpose ports

Parts List and Required Tools

Verify that you have these items.

The PoE connector ships only with switch models with PoE ports. The connector is required only if you plan to use PoE.

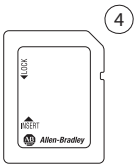


1 Stratix® 5700 switch

2 Documentation

3 PoE connector

If needed, an SD card can be ordered separately from the switch.



4 SD card



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

Obtain these tools:

- Ratcheting torque screwdriver that exerts up to 1.69 N•m (15 in•lbs) of pressure
- Small, flat-blade screwdriver
- #6 ring terminal lug for 5.3 mm^2 (10 AWG) wire, such as Thomas & Bett part number 10RC6 or equivalent
- Crimping tool, such as Thomas & Bett part number WT2000, ERG-2001, or equivalent
- 5.3 mm^2 (10 AWG) copper ground wire, such as Belden part number 9912 or equivalent
- Wire-stripping tool
- For panel-mounting without a DIN rail, M5 or #10-24 or #10-32 bolts or screws with 1.27 cm (0.5 in.) O.D. flat washers

For simplified cabling, the automatic medium-dependent interface crossover (auto-MDIX) feature is enabled by default on the switch. With auto-MDIX enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a 10/100 or 10/100/1000 Ethernet switch port, regardless of the type of device on the other end of the connection.

Install or Remove the SD Card

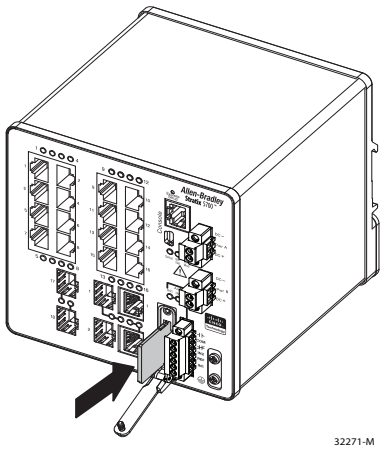
WARNING: When you insert or remove the CompactFlash/SD memory card while power is on, an electrical arc can occur. This can cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

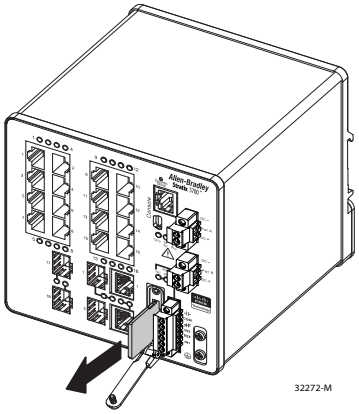
To install or replace the optional SD card, follow these steps.

1. On the front of the switch, locate the door that protects the SD card slot.
2. Loosen the captive thumb screw at the top of the door by using a screwdriver to open the door.
3. Install or remove the card.

   To install the card, slide it into the slot, and press it firmly in place until it latches in the spring loaded mechanism. The card is keyed so that you cannot fully insert it the wrong way.



To remove the card, push it in and let it pop out via the spring-loaded mechanism. Grasp the card top and pull it out. Place it in an antistatic bag to protect it from static discharge.



4. Close the guard door and fasten the captive screw by using a screwdriver to keep the door in place.

Verify Switch Operation

Before installing the switch in its final location, power on the switch, and verify that the switch powers up.

The time that is required for the switch to start up is directly related to your switch configuration. Start time is negatively affected by such things as the following:

- Spanning Tree Learning mode
- Number of files or images in onboard memory

To test the switch, follow these steps.

1. Apply power to the switch.

   If the switch is directly connected to a DC power source, locate the circuit breaker on the panel board that services the DC circuit, and switch the circuit breaker to the ON position.

2. Verify the start-up sequence.

   When you power on the switch, it begins a start-up routine. The Setup status indicator blinks green as the IOS software image loads. If the routine fails, the Setup status indicator turns red.

IMPORTANT	Start-up failures are usually fatal to the switch. Contact your Rockwell Automation representative immediately if your switch does not complete the start sequence successfully.

IMPORTANT	You can disable Boot Fast and run the Power-on self-test (POST) by using the CLI. For more information, see the documentation at http://www.Cisco.com.

3. After successfully running this test, do the following:
   a. Turn off power to the switch.
   b. Disconnect the cables.
   c. Decide where you want to install the switch

Mount the Switch on a DIN Rail

The switch ships with a spring-loaded latch on the rear panel for mounting on a DIN rail.

WARNING: If you connect or disconnect console port cables with power applied to this module or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

WARNING: Do not use the USB-mini console port in hazardous locations.

ATTENTION: Prevent Electrostatic Discharge

This equipment is sensitive to electrostatic discharge, which can cause internal damage and affect normal operation. Follow these guidelines when you handle this equipment:

- Touch a grounded object to discharge potential static.
- Wear an approved grounding wriststrap.
- Do not touch connectors or pins on component boards.
- Do not touch circuit components inside the equipment.
- Use a static-safe workstation, if available.
- Store the equipment in appropriate static-safe packaging when not in use.

ATTENTION: This equipment is supplied as open type equipment. It must be mounted within an enclosure suitably designed for those specific environmental conditions and appropriately designed to prevent personal injury resulting from accessibility to live parts. The interior of the enclosure must be accessible only by using a tool.

The enclosure must meet IP 54 or NEMA type 4 minimum enclosure rating standards.

ATTENTION: To prevent the switch from overheating, observe these minimum clearances:

- Top and bottom: 50.8 mm (2.0 in.)
- Exposed side (not connected to the module): 50.8 mm (2.0 in.)
- Front: 50.8 mm (2.0 in.)

ATTENTION: The console ports are intended for temporary local programming purposes only and not intended for permanent connection.

The console port cables are not to exceed 3.0 m (9.84 ft) and must not contain hubs.

ATTENTION: Under certain conditions, viewing the optical port may expose the eye to hazard. When viewed under some conditions, the optical port may expose the eye beyond the maximum permissible exposure recommendations.

ATTENTION: Class 1 laser product. Laser radiation is present when the system is open and interlocks bypassed. Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

ATTENTION: This product is grounded through the DIN rail to chassis ground. Use zinc plated yellow-chromate steel DIN rail to assure proper grounding. The use of other DIN rail materials (for example, aluminum or plastic) that can corrode, oxidize, or are poor conductors, can result in improper or intermittent grounding. Secure DIN rail to mounting surface approximately every 200 mm (7.8 in.) and use end-anchors appropriately.

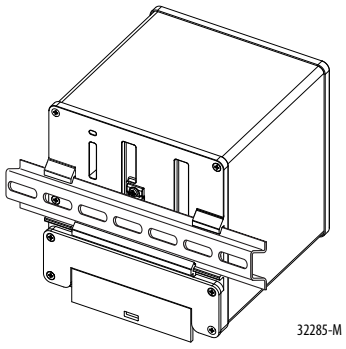
IMPORTANT The switch must be mounted in an upright orientation, as shown in these instructions. Alternative mounting orientations are not supported.

To attach the switch to a DIN rail, follow these steps.

1. Position the rear panel of the switch directly in front of the DIN rail.

   Make sure that the DIN rail fits in the space between the two hooks near the top of the switch and the spring-loaded latch near the bottom.

2. Hold the bottom of the switch away from the DIN rail, and place the two hooks on the back of the switch over the top of the DIN rail.

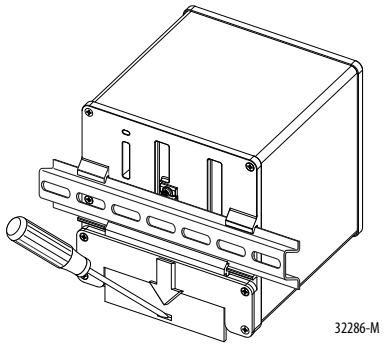


3. Push the switch toward the DIN rail to cause the spring loaded latch at the bottom rear of the switch to move down and snap into place.

Remove the Switch from the DIN Rail

To remove the switch from a DIN rail or a rack, follow these steps.

1. Remove power from the switch, and disconnect all cables and connectors from the front panel of the switch.
2. Insert a tool, such as a flat-head screwdriver, in the slot at the bottom of the spring-loaded latch and use it to release the latch from the DIN rail.



Ground the Switch

For DC power connections, use UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

WARNING: If you connect or disconnect power or alarm wiring while the field-side power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

This equipment is intended to be grounded to comply with emission and immunity requirements. Make sure that the switch functional ground lug is connected to earth ground during normal use.

ATTENTION: To make sure that the equipment is reliably connected to earth ground, follow the grounding procedure instructions and use a suitable ring terminal lug, such as Thomas & Betts part number 10RCR or equivalent.

ATTENTION: For proper grounding, you must always connect the power supply functional-ground screw when connecting the power supply. You must provide an acceptable grounding path for each device in your application. For more information on proper grounding guidelines, refer to publication 1770-4.1, Industrial Automation Wiring and Grounding Guidelines.

Use at least 4 mm^2 (12 AWG) wire to connect to the external grounding screw.

The ground lug is not supplied with the switch. You can use one of the these options:

- Single ring terminal
- Two single ring terminals

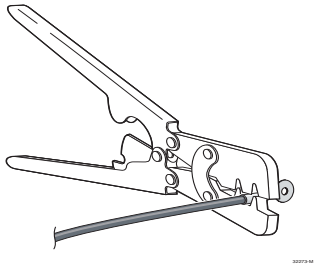
To ground the switch to earth ground, follow these steps. Be sure to follow any grounding requirements at your site.

1. Use a Phillips screwdriver or a ratcheting torque screwdriver with a Phillips head to remove the ground screw from the front panel of the switch.

   Store the ground screw for later use.

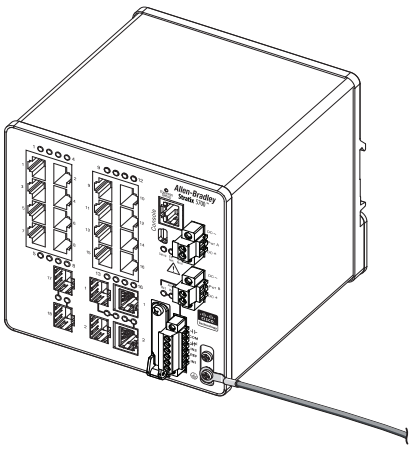
2. Use the guidelines from the manufacturer to determine the wire length to be stripped.
3. Insert the ground wire into the ring terminal lug and use a crimping tool to crimp the terminal to the wire.

   If you are using two ring terminals, repeat this action for the second ring terminal.



4. Slide the ground screw through the terminal.

5. Insert the ground screw into the functional ground screw opening on the front panel.



6. Use a ratcheting torque screwdriver to tighten the ground screws and ring terminal lugs to the switch front panel to 0.4 N•m (3.5 lb•in).

   Do not exceed the recommended torque.

7. Attach the other end of the ground wire to a grounded bare metal surface, such as a ground bus, a grounded DIN rail, or a grounded bare rack.

Wire the Switch DC Power Source

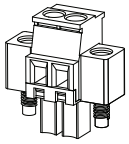
To wire the DC power source for the switch, follow these steps.

ATTENTION: Before performing any of the following procedures, make sure that power is removed from the DC circuit or the area is nonhazardous before proceeding:

- This product is intended to be supplied by a Class 2 power source marked with 'Class 2' and rated from 12, 24, or 48V DC, 2.5 A.
- To comply with the CE Low Voltage Directive (LVD), this equipment must be powered from a source compliant with the safety extra low voltage (SELV) or protected extra low voltage (PELV).
- A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.
- This product relies on the building's installation for short-circuit (overcurrent) protection. Make sure that the protective device is rated not greater than 3 A.
- Installation of the equipment must comply with local and national electrical codes.
- Allow only trained and qualified personnel to install, replace, or service this equipment.

ATTENTION: For wire connections to the power and relay connector, you must use UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

1. Locate the power connector.



32280-M

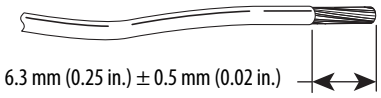
2. Identify the positive and return DC power connections.

   The positive DC power connection is labeled DC+, and the negative DC power connection is the adjacent connection labeled DC-.

3. Measure a length of 0.82...0.52 mm^2 (18...20 AWG) copper wire long enough to connect to the DC power source.

4. Use an 18-gauge wire-stripping tool to strip each of the two wires to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

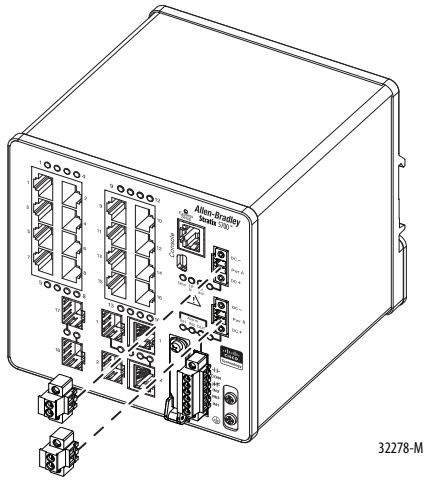
   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wire. Stripping more than the recommended amount of wire can leave wire exposed after installation.



31789-M

5. Loosen the two captive screws that attach the power connector to the switch, and remove the power connector.

   Remove both connectors if you are connecting to two power sources.

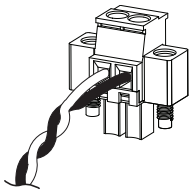


32278-M

6. Insert the exposed part of the positive wire into the connection labeled DC+ and the exposed part of the return wire into the connection labeled DC-.

Be sure that you cannot see any wire lead. Only wire with insulation can extend from the connector.

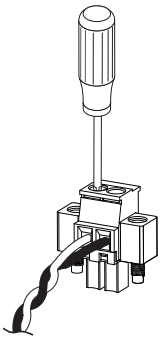
ATTENTION: An exposed wire lead from a DC input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC input power source wire extends from the connectors or terminal blocks.



32279-M

7. Use a ratcheting-torque screwdriver to torque the captive screws of the power connector to 0.23 N•m (2.0 lb•in).

   Do not exceed the recommended torque.

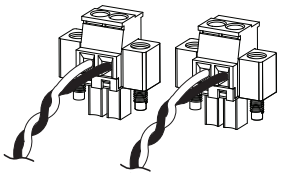


32281-M

8. Connect the other end of the positive wire to the positive terminal on the DC power source.
9. Connect the other end of the return wire to the return terminal on the DC power source.

   When you are testing the switch, one power connection is sufficient. If you are installing the switch and are using a second power source, repeat this procedure with the second power connector.

   The following figure shows the completed DC input wiring on a power connector for a primary power source and an optional secondary power source.

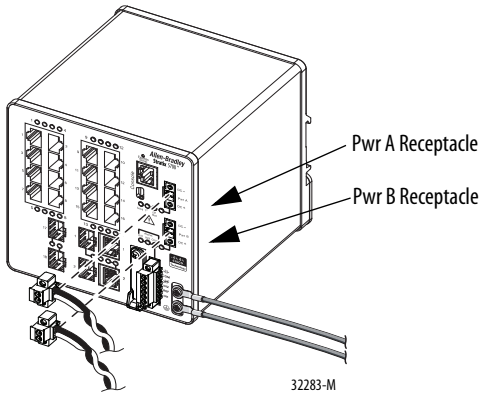


32282-M

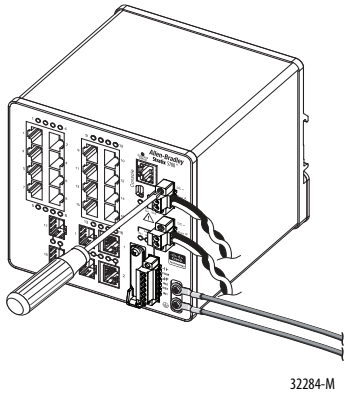
Attach the Switch Power Connectors

To attach the switch power connectors to the front panel of the switch, follow these steps.

1. Insert one power connector into the Pwr A receptacle on the switch front panel, and the other into the Pwr B receptacle.



2. Use a ratcheting torque flathead screwdriver to tighten the captive screws on the sides of the power connectors.



When you test the switch, one power source is sufficient. If you install the switch and use a second power source, repeat this procedure for the second power connector (Pwr B), which installs just below the primary power connector (Pwr A).

3. When you install the switch, secure the wires from the power connectors to the rack by using tie wraps.

Wire the Power over Ethernet DC Power Source

This procedure applies only to switches with PoE ports.

WARNING: The console port is intended only for temporary local programming purposes and not intended for permanent connection. If you connect or disconnect the console cable with power applied to this module or the programming device on the other end of the cable, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: To comply with the CE Low Voltage Directive (LVD), this equipment must be powered from a source compliant with the safety extra low voltage (SELV) or protected extra low voltage (PELV).

To comply with UL restrictions, this equipment must be powered from a source compliant with Class 2 or Limited Voltage/Current.

The switch must be wired and grounded.

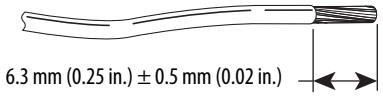
Power input requirements depend on your application.

Application	Power Supply per Port	Power Consumption	Allen-Bradley Products
PoE only IEEE 802.3af	44…57V DC (48V DC nom)	15.4 W, max	Switched mode power supplies: • 1606-XL Standard • 1606-XLE Essential • 1606-XLP Compact • 1606-XLS Performance
PoE and PoE + IEEE 802.3at Type 2	50…57V DC (54V DC nom)	15.4 W, max for PoE 30 W, max for PoE+	

WARNING: Before performing any of the following procedures, make sure that power is removed from the DC circuit or the area is nonhazardous before proceeding.

1. Measure a length of 0.82...0.52 mm^2 (18...20 AWG) copper wire long enough to connect to the DC power source.
2. Using an 18-gauge wire-stripping tool, strip each of the two wires to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wire. Stripping more than the recommended amount of wire can leave wire exposed after installation.

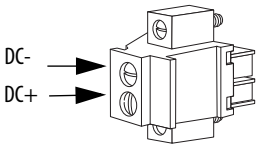


31789-M

3. Locate the power connector.

4. Insert the exposed part of the positive wire into the DC+ connection and the exposed part of the return wire into the DC- connection.

   Make sure that you cannot see any wire lead. Only wire with insulation can extend from the connector.



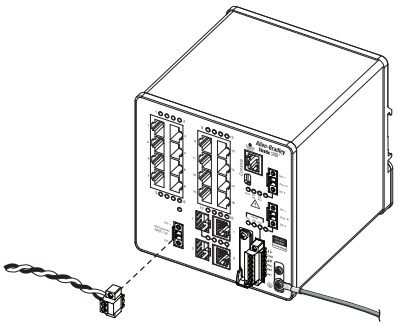
5. Use a ratcheting-torque screwdriver to torque the captive screws of the power connector to 0.23 N•m (2.0 lb•in).
6. Connect the other end of the positive wire (the one connected to DC+) to the positive terminal on the DC power source.
7. Connect the other end of the return wire (the one connected to DC-) to the return terminal on the DC power source.

ATTENTION: If multiple power sources are used, do not exceed the specified isolation voltage.

Attach the PoE Power Connector

This procedure applies only to switches with PoE ports.

1. Insert the power connector into the DC input terminal block on the switch front panel.
2. Use a screwdriver to tighten the captive screws on the sides of the power connector.



ATTENTION: Exposure to some chemicals can degrade the sealing properties of materials used in the relay. Periodically inspect the relay and check for any degradation.

Install an SFP Module

WARNING: When you insert or remove the small form-factor pluggable (SFP) optical transceiver while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: Under certain conditions, viewing the small form-factor pluggable (SFP) optical transceiver may expose the eye to hazard. When viewed under some conditions, the optical port may expose the eye beyond the maximum permissible exposure recommendations.

ATTENTION: Use SFP modules from only Rockwell Automation. For details about supported modules, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

ATTENTION: We strongly recommend that you do not install or remove the SFP module with fiber-optic cables attached. If you leave the cables attached, damage to the cables, the cable connector, or the optical interfaces in the SFP module can occur. Disconnect all cables before removing or installing an SFP module.

IMPORTANT Installing and removing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is necessary.

On switch catalog numbers that support communication over fiber-optic cable, sfp modules are inserted into SFP module slots on the front of the switch. These field-replaceable modules provide the uplink optical interfaces, send (TX) and receive (RX).

You can use any combination of compatible SFP modules:

- Each SFP module must be of the same type as the SFP module on the other end of the cable. The cable must not exceed the stipulated cable length for reliable communications.
- Once you install SFP modules in the switch, be aware that the overall temperature rating of the combined modules (switch and SFP modules) is limited to the lowest maximum temperature rating and the highest minimum temperature rating.

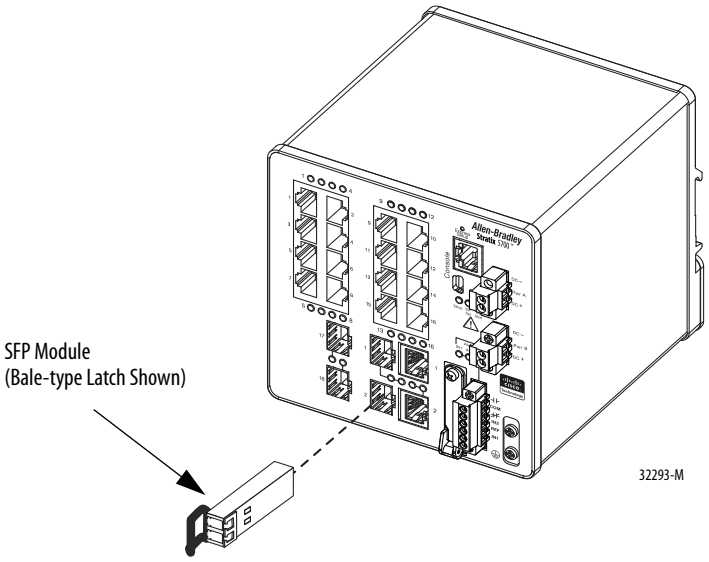
For cable length and temperature specifications, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

To insert an SFP module into an SFP slot, follow these steps.

1. Attach an ESD-preventive wriststrap to your wrist and to a grounded bare metal surface.
2. Grasp both sides of the SFP module and align the module sideways in front of the slot opening.

> **ATTENTION:** If the SFP module cannot be fully inserted, stop! Do not force the module into the slot. Rotate the SFP module 180° and try again.

3. Insert the SFP module into the slot as shown in the following figure until you feel the connector on the module snap into place in the rear of the slot.



4. Remove the dust plugs from the SFP module optical ports, store them for later use.

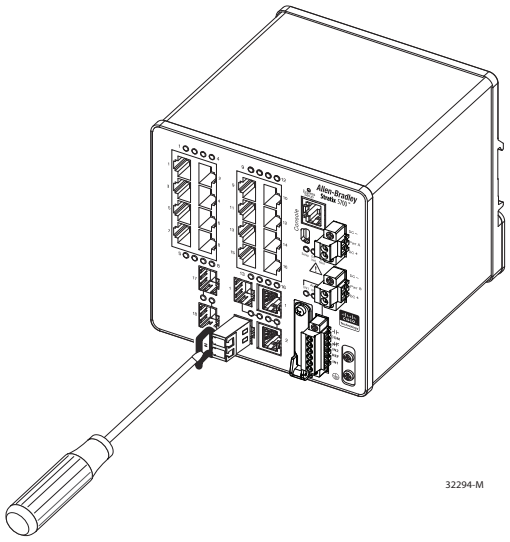
IMPORTANT	Do not remove the dust plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps help protect the SFP module ports and cables from contamination and ambient light.

Remove an SFP Module from an SFP Slot

To remove an SFP module from an SFP slot, follow these steps.

1. Attach an ESD-preventive wriststrap to your wrist and to a grounded bare metal surface.
2. Disconnect the fiber LC connector from the SFP module.
3. Insert a dust plug into the optical ports of the SFP module to keep the optical interfaces clean.
4. Unlock and remove the SFP module.

   If the module has a bale-clasp latch, swing the bale toward you and pull it gently to eject the module. If the bale-clasp latch is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the latch.



5. Grasp the SFP module between your thumb and index finger, and carefully remove it from the module slot.
6. Place the removed SFP module in an antistatic bag or other protective environment.

Wire the External Alarms

The switch has two alarm inputs and one Form C (single-pole, double-throw) alarm output relay circuits for external alarms. The input alarm relay circuits are designed to sense if the alarm input is open or closed relative to the alarm input reference pin. The output alarm relay circuit has one Form C relay, with one normally open (NO) and one normally closed (NC) contact. You can configure the output alarm relay as either normally energized or normally de-energized by using the CLI.

See Appendix D for an alarm wiring example.

Alarm signals are connected to the switch through the 6-way alarm relay connector. Three connections are dedicated to the two alarm input circuits:

- Alarm input 1 (IN1)
- Alarm input 2 (IN2)
- Isolated reference ground

An alarm input and the reference ground wiring connection are required to complete one input alarm circuit. You must provide either an NO or an NC dry contact to complete the alarm circuit between reference ground and IN1 or IN2.



ATTENTION: Do not apply an external voltage source to either the IN1 or IN2 alarm inputs. Limit alarm output wiring to 48 V DC, 0.5 A.

The three remaining connections for the Form C output alarm circuit are as follows:

- NO output
- NC output
- common

An alarm output and the common wiring connection are required to complete one output alarm circuit. The Form C output alarm relay provides one NO and one NC dry contact.



ATTENTION: Wire connections to the power and relay connector, must be UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

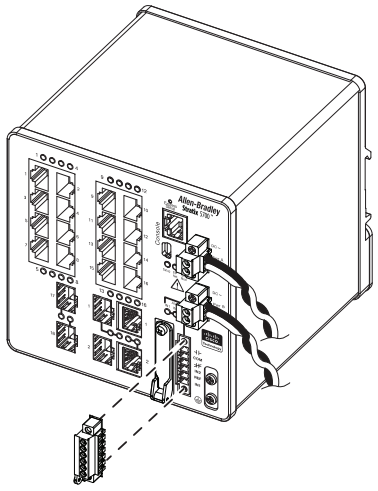
The labels for the alarm relay connector are on the switch panel.

Table 27 - Alarm Relay Connector Labels

Label	Connection
NO	Alarm Output Normally Open (NO) connection
COM	Alarm Output Common connection
NC	Alarm Output Normally Closed (NC) connection
IN2	Alarm Input 2
REF	Alarm Input Reference Ground connection
IN1	Alarm Input 1

To wire the switch to an external alarm device, follow these steps.

1. Loosen the captive screws that hold the alarm relay connector on the switch, and remove the connector from the switch chassis.



32287-M

2. Measure two strands of twisted-pair wire (18...20 AWG) long enough to connect to the external alarm device.

   Choose between creating an external alarm input or output circuit.

3. Use a wire stripper to remove the casing from both ends of each wire to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

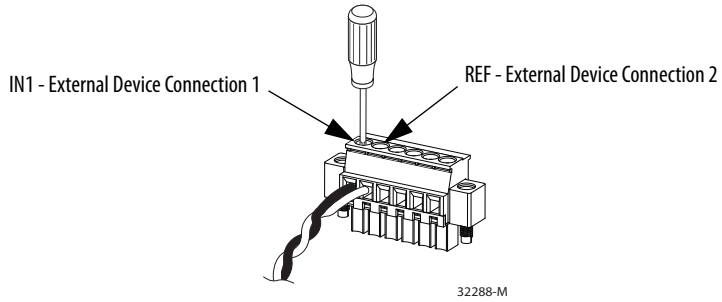
   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wires. Stripping more than the recommended amount of wire can leave exposed wire from the alarm relay connector after installation.

4. Insert the exposed wires for the external alarm device into the connections that are based on an alarm input or output circuit setup.

   See Table 27 on page 150.

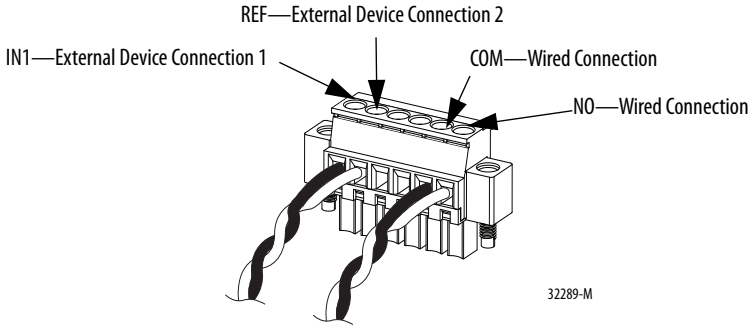
5. Use a ratcheting torque flathead screwdriver to torque the captive screw of the alarm relay connector to 0.23 N•m (2.0 lb•in).

   Do not exceed the recommended torque.



6. Repeat the preceding procedure to insert the input and output wires of one more external alarm device into the alarm relay connector.

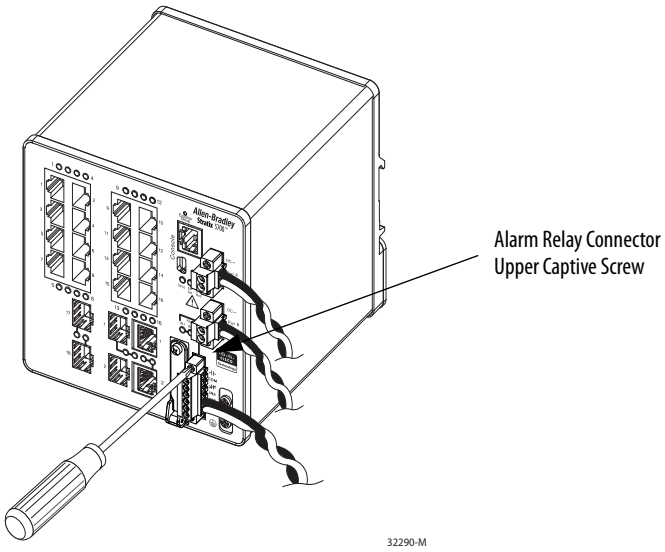
   The following figure shows the completed wiring for two external alarm devices. The first alarm device circuit is wired as an alarm relay input circuit—the IN1 and REF connections complete the circuit. The second alarm device circuit is wired as an alarm relay output circuit by using the normally open side of the form C relay contacts. The NO and COM connections complete the circuit.



Attach the Alarm Relay Connector to the Switch

To attach the alarm relay connector to the front panel of the switch, follow these steps.

1. Insert the alarm relay connector into the receptacle on the switch front panel.
2. Use a ratcheting torque flathead screwdriver to tighten the captive screws on the sides of the alarm relay connector.



Connect to 10/100 and 10/100/1000 Ports

The switch 10/100/1000 ports automatically configure themselves to operate at the speed of attached devices. If the attached ports do not support autonegotiation, you can explicitly set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have their speed and duplex parameters that are manually set can reduce performance or result in no linkage.

The Auto-MDIX feature is enabled by default. Unless this feature is disabled, you can use either straight-through or crossover cables to connect to other devices on the network.

To maximize performance, choose one of these methods for configuring the Ethernet ports:

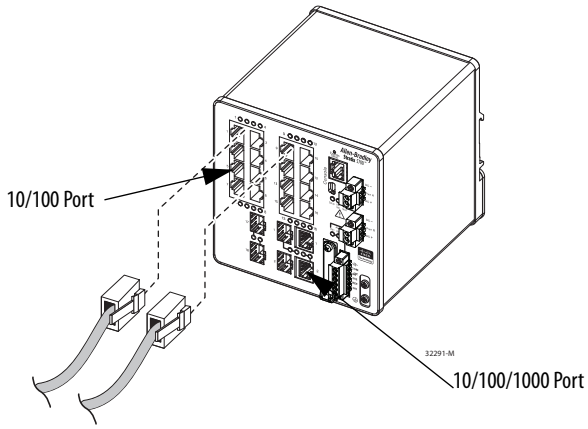
- Let the ports autonegotiate both speed and duplex
- Set the port speed and duplex parameters on both ends of the connection

Connect to 10BASE-T, 100BASE-TX, or 1000BASE-T Ports

To connect to 10BASE-T, 100BASE-TX, or 1000BASE-T ports, follow these steps.

ATTENTION: To prevent electrostatic-discharge (ESD) damage, follow recommended board and component handling procedures.

1. Choose one of these options to connect a device:
   - When connecting to workstations, servers, and routers, connect a straight-through cable to an RJ45 connector on the front panel.
   - When connecting to 1000BASE-T-compatible devices, use a twisted four-pair, Category 5e or higher cable.



2. Connect the other end of the cable to an RJ45 connector on the other device.

   The Port status indicator turns on when both the switch and the connected device have an established link.

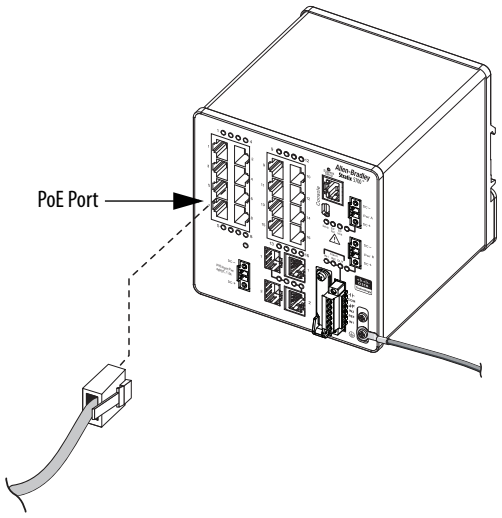
   The Port status indicator is amber while Spanning Tree Protocol (STP) discovers the topology and searches for loops. This can take up to 30 seconds, and then the Port status indicator turns green.

   The following conditions can prevent the Port status indicator from turning On:
   - The device at the other end is not turned On.
   - A problem exists with a cable or the adapter that is installed in the attached device.
3. Reconfigure and restart the connected device if necessary.
4. Repeat this procedure to connect each device.

Connect to PoE Ports

Switches with PoE ports require a separate power supply. For power supply requirements based on your application, refer to page 144.

1. Insert a straight-through, twisted four-pair, Category 5e or better cable with an RJ45 connector into the PoE port.



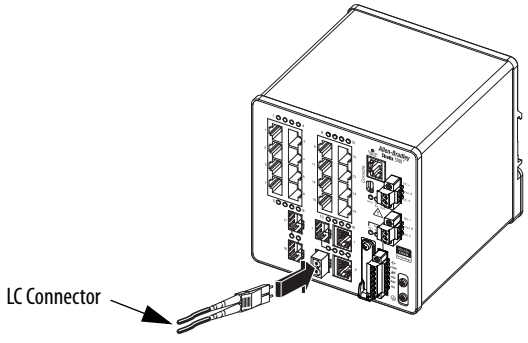
2. Insert the other cable end into an RJ45 connector on the other PoE powered device.

Connect to SFP Module Ports

To connect a fiber-optic cable to an SFP module, follow these steps.

ATTENTION: Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

1. Remove the rubber plugs from the module port and fiber-optic cable, and store them for future use.
2. Insert one end of the fiber-optic cable into the SFP module port.



3. Insert the other cable end into a fiber-optic receptacle on a target device.

4. Observe the port status indicator:
   - The status indicator turns amber while the SFP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port status indicator turns green.
   - The status indicator turns green when the switch and the target device have an established link.
   - The status indicator turns off if the target device is not turned on or there is a problem with the cable or the adapter that is installed in the target device.

   If necessary, reconfigure and restart the switch or the target device.

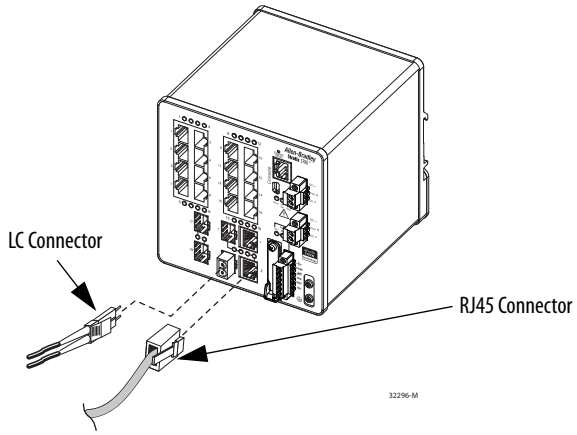
Connect to a Dual-purpose Port

A dual-purpose port is one port with two interfaces, one for an RJ45 cable and another for an approved SFP module. Only one interface can be active at a time. If both interfaces are connected, the SFP module has priority.

ATTENTION: Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

To connect to a dual-purpose port, follow these steps.

1. Connect an RJ45 connector to the 10/100/1000 port, or install an SFP module into the SFP module slot, and connect a cable to the SFP module port.



2. Connect the other end of the cable to the other device.

   By default, the switch detects whether an RJ45 connector or SFP module is connected to a dual-purpose port and configures the port accordingly. You can change this setting and configure the port to recognize only an RJ45 connector or only an SFP module by using the media type interface configuration command.

Notes:

Install Stratix 8000 and 8300 Switches

Topic	Page
Specifications	159
Overview	160
Parts List and Required Tools	162
Attach Expansion Modules	164
Mount the Switch	166
Install an SFP Module	169
Ground the Switch	171
Wire the DC Power Source for the Switch	172
Wire the DC Power Source for the PoE Expansion Module	174
Attach the Power and Relay Connector to the Switch to the Switch	176
Attach the Power Connector to the PoE Expansion Module	178
Wire External Alarms	178
Connect to 10/100 Copper Ports	180
Connect to a PoE Expansion Module Port	180
Connect to Dual-purpose Uplink Ports	181
Connect to 100BaseFX Ports	182
Install or Remove the CompactFlash Card	182

ATTENTION: Environment and Enclosure

This equipment is intended for use in a Pollution Degree 2 industrial environment, in overvoltage Category II applications (as defined in IEC 60664-1), at altitudes up to 2000 m (6562 ft) without derating.

This equipment is not intended for use in residential environments and may not provide adequate protection to radio communication services in such environments.

This equipment is supplied as open-type equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if nonmetallic. The interior of the enclosure must be accessible only by the use of a tool. Subsequent sections of this publication may contain additional information regarding specific enclosure type ratings that are required to comply with certain product safety certifications.

In addition to this publication, see the following:

- Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1, for additional installation requirements
- NEMA Standard 250 and IEC 60529, as applicable, for explanations of the degrees of protection provided by enclosures

North American Hazardous Location Approval

The following information applies when operating this equipment in hazardous locations.	**Informations sur l'utilisation de cet équipement en environnements dangereux.**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Les produits marqués "CL I, DIV 2, GP A, B, C, D" ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**WARNING: RISQUE D'EXPLOSION** • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

European Hazardous Location Approval

The following applies when the product bears the Ex Marking.

This equipment is intended for use in potentially explosive atmospheres as defined by European Union Directive 94/9/EC and has been found to comply with the Essential Health and Safety Requirements relating to the design and construction of Category 3 equipment intended for use in Zone 2 potentially explosive atmospheres, given in Annex II to this Directive.

ATTENTION: This equipment is not resistant to sunlight or other sources of UV radiation.

WARNING:

- This equipment shall be mounted in an ATEX-certified enclosure with a minimum ingress protection rating of at least IP54 (as defined in IEC60529) and used in an environment of not more than Pollution Degree 2 (as defined in IEC 60664-1) when applied in Zone 2 environments. The enclosure must have a tool-removable cover or door.
- This equipment shall be used within its specified ratings defined by Rockwell Automation.
- Provision shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 140% of the rated voltage when applied in Zone 2 environments.
- Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.
- Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.

ATTENTION: To comply with the CE Low Voltage Directive (LVD), all connections to this equipment must be powered from a source compliant with safety extra low voltage (SELV) or protected extra low voltage (PELV).

To comply with UL restrictions, all connections to this equipment must be powered from a source compliant with Class 2 or Limited Voltage/Current.

Specifications

For additional specifications and certifications, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Table 28 - Stratix 8000 and 8300 Switches

Attribute	1783-MS06T, 1783-MS10T, 1783-RMS06T, 1783-RMS10T	1783-MX08T	1783-MX08F	1783-MX04S	1783-MX08S
Wire size, power connectors	0.5…0.8 mm^2 (18…20 AWG) twisted-pair copper wire suitable for 86 °F (30 °C) above surrounding ambient temperature outside of the enclosure	NA			
Screw torque, ground terminals	0.96 N•m (8.5 lb•in)				
Screw torque, relay terminals	0.23 N•m (2.0 lb•in)				
Screw torque, power terminals					
Alarm relay ratings	30V DC, 1.0 A max				
Power supply, user supplied	18…60V DC, 2.0 A max	NA			
Power consumption, expansion modules	NA	3.3V DC, 1.7 A max	3.3V DC, 3.6A max	3.3V DC, 2.5 A max	3.3V DC, 4.0 A max

Table 29 - Stratix 8000 and 8300 Power over Ethernet Expansion Modules

Attribute	1783-MX04E	1783-MX04T04E
Wire size, power connectors	0.5…0.8 mm^2 (18…20 AWG) twisted-pair copper wire suitable for 30 °C (86 °F) above surrounding ambient temperature outside the enclosure	
Screw torque, ground terminals	0.96 N•m (8.5 lb•in)	
Screw torque, power terminals	0.23 N•m (2.0 lb•in)	
DC input voltage, PoE	48/54V DC	
DC input current, PoE	2.5 A	2.5 A
Power consumption, module	7.3 W	7.9 W
Backplane power, module	3.3V DC @ 0.94 A	3.3V DC @ 1.08 A

Overview

When determining where to place the switch, observe these guidelines:

- Operating environment is within the range specified in the technical specifications. See the Stratix Ethernet Managed Switches Technical Data, publication 1783-TD001.
- Clearance to front and rear panels meets these conditions:
  - Front-panel status indicators can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Front-panel direct current (DC) power and relay connector is within reach of the connection to the DC power source.
- Airflow around the switch and through the vents is unrestricted.

  To prevent the switch from overheating, observe these minimum clearances:
  - Top and bottom: 105 mm (4.13 in.)
  - Left and right: 90 mm (3.54 in.)
  - Front: 65 mm (2.56 in.)
- Temperature surrounding the unit does not exceed 60 °C (140 °F).

IMPORTANT	When the switch is installed in an industrial enclosure, the temperature within the enclosure is greater than normal room temperature outside the enclosure. The temperature inside the enclosure cannot exceed 60 °C (140 °F), the maximum ambient enclosure temperature of the switch.

- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.
- Switch is grounded to a bare metal surface, such as a ground bus or a grounded DIN rail.

Follow these steps to install the switch.

1. (Optional) Attach expansion modules.
2. Mount the switch on one of the following:
   - DIN rail
   - Wall or panel
3. (Optional) Install an SFP module.
4. Ground the switch.
5. Wire the DC power source for the switch.
6. (Optional) Wire the DC power source for the PoE expansion module.
7. Attach the power and alarm connector.

8. Wire external alarms.
9. Connect to the switch ports:
   - 10/100 copper ports
   - PoE ports
   - Dual-purpose uplink (10/100/1000 and SFP fiber) ports
   - 100BaseFX
10. Install or remove the CompactFlash card.



WARNING: If you connect or disconnect the communication cable with power applied to this module or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.



WARNING: If you connect or disconnect wiring while the field-side power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.



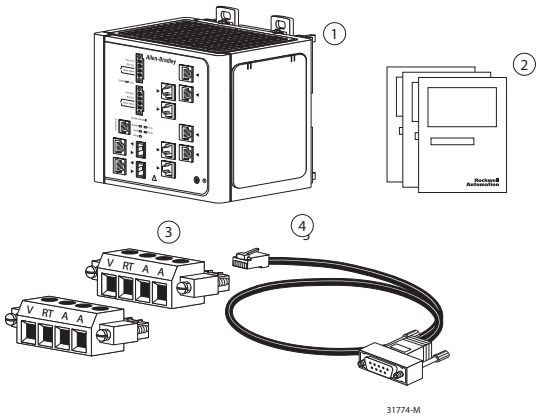
ATTENTION: Prevent Electrostatic Discharge

This equipment is sensitive to electrostatic discharge, which can cause internal damage and affect normal operation. Follow these guidelines when you handle this equipment:

- Touch a grounded object to discharge potential static.
- Wear an approved grounding wriststrap.
- Do not touch connectors or pins on component boards.
- Do not touch circuit components inside the equipment.
- Use a static-safe workstation, if available.
- Store the equipment in appropriate static-safe packaging when not in use.

Parts List and Required Tools

Verify that you have these items.



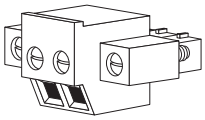
1 Stratix® 8000/8300 switch

2 Documentation

3 Power and alarm relay connectors (qty. 2)

4 Console cable

If you plan to install a PoE expansion module, verify that you have a PoE power connector.



32437-M



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

Obtain these tools:

- Ratcheting torque screwdriver that exerts up to 1.69 N•m (15 in•lbs) of pressure
- #6 ring terminal lug for 5.3 mm^2 (10 AWG) wire, such as Thomas & Bett part number 10RC6 or equivalent
- Crimping tool, such as Thomas & Bett part number WT2000, ERG-2001, or equivalent
- 5.3 mm^2 (10 AWG) copper ground wire, such as Belden part number 9912 or equivalent
- Wire-stripping tool
- For panel-mounting without a DIN rail, M5 or #10-24 or #10-32 bolts or screws with 1.27 cm (0.5 in.) O.D. flat washers

For simplified cabling, the automatic medium-dependent interface crossover (auto-MDIX) feature is enabled by default on the switch. With auto-MDIX enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a 10/100 or 1 0/100/1000 Ethernet switch port, regardless of the type of device on the other end of the connection.

Attach Expansion Modules

IMPORTANT If you are adding expansion modules, attach the expansion modules to the switch before mounting the switch.

The switch can operate as a standalone device with two uplink ports and four or eight Fast Ethernet ports, or you can increase the number of Fast Ethernet ports by 8 or 16 by connecting expansion modules.

You can install as many as two expansion modules per base unit. However, only one of the two modules can be a 1783-MX08F or 1783-MX08S fiber expansion module.

If you install a 1783-MX08F or 1783-MX08S fiber expansion module, the module must be in the right-most position.

Base Unit	Expansion Module	1783-MX08F or 1783-MX08S Expansion Module

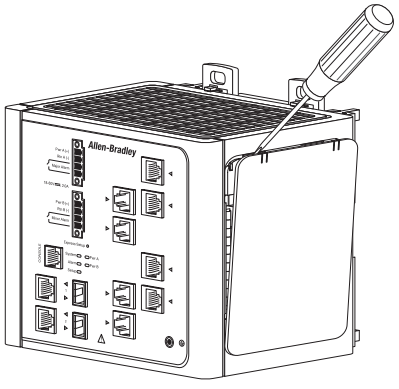
Depending on the mix of switches and expansion modules, you can have as many 24 Fast Ethernet ports.

To connect the expansion modules to the switch, follow these steps.

IMPORTANT You must add expansion modules to the base unit before you apply power to the switch. Remove power from the switch when reconfiguring it.

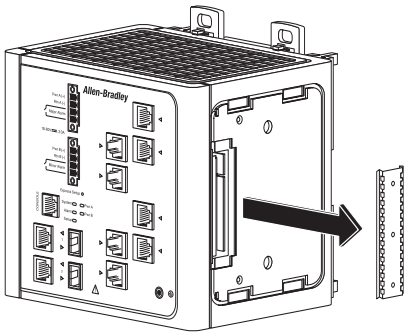
1. Remove the right side panel by firmly grasping both sides of it in the middle and pulling it outward.

   If necessary, use a screwdriver to pry open the side panel.



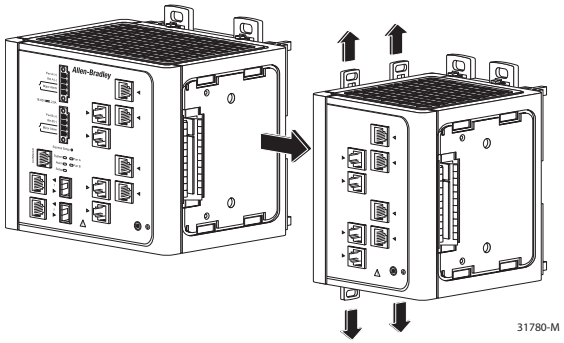
31779-M

2. Remove the protective EMI-connector cover from the side panel.

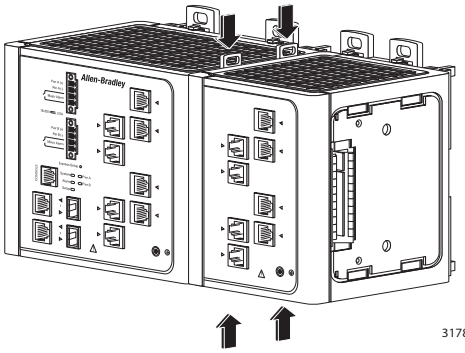


3. Push the upper module latches up and the lower module latches down. Then slide the switch and module together.

   The expansion module is shown with the side panel removed. Do not remove this panel unless you plan to install another module.



4. Push the upper and lower module latches in to secure the module to the switch.



5. If you are installing a second module, repeat steps 1...4, but secure the second module to the right side of the first module.

IMPORTANT You cannot install an expansion module to the right of the 1783-MX08F or 1783-MX08S fiber expansion module.

Mount the Switch

You can mount the switch on one of the following:

- DIN rail, as described on page 166
- Wall or panel, as described on page 168

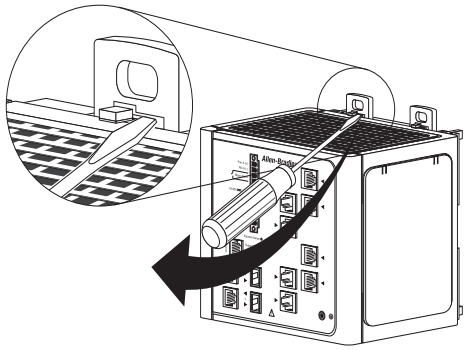
IMPORTANT The switch must be mounted in an upright orientation, as shown in these instructions. Alternative mounting orientations are not supported.

Mount the Switch on a DIN Rail

WARNING: When using DIN rail mounting, additional grounding is also accomplished through the DIN rail to chassis ground. Use zinc-plated yellow-chromate steel DIN rail to assist in proper grounding. The use of other DIN rail materials (for example, aluminum or plastic)) that can corrode, oxidize, or are poor conductors, can impede proper grounding. Secure DIN rail to mounting surface approximately every 200 mm (7.8 in.) using end-anchors appropriately and using a washer plate along the entire length of the DIN rail.

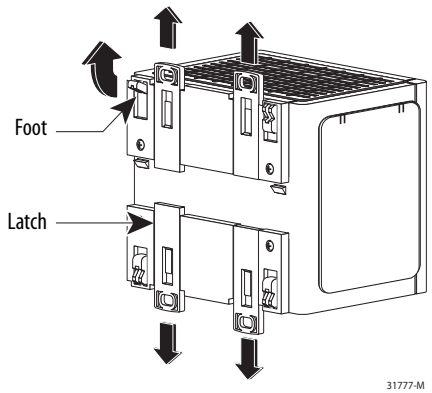
Follow these steps to mount the switch on a DIN rail.

1. Insert a sharp tool, such as a screwdriver, in the space next to the tab, push gently to release the catch, then turn the screwdriver to push the tab out.

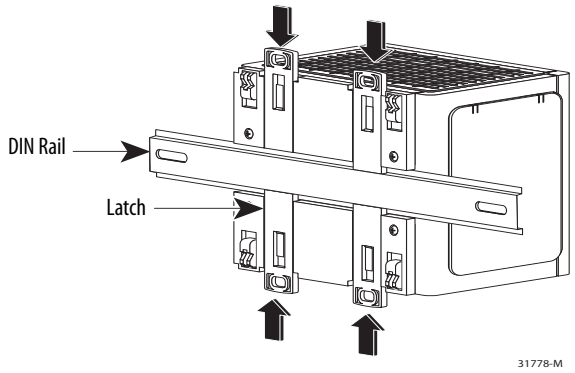


2. If you are using a heavy-duty 35 mm x 15 mm (1.38 in. x 0.59 in.) DIN rail, rotate all feet to the extended positions.

   Otherwise, if you are using 35 mm x 7.5 mm (1.38 in. x 0.30 in.) DIN rail, rotate the feet to the recessed positions.



3. Position the rear panel of the switch directly in front of the DIN rail, making sure that the DIN rail fits in the space between the two latches.



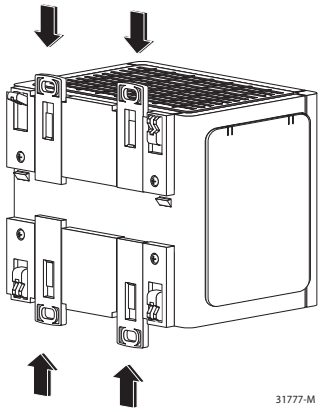
4. Push the DIN rail latches in after the switch is over the DIN rail to secure the switch to the rail.

Mount the Switch on a Wall or Panel

To mount the switch on a wall or a panel, you need M5 or #10-24 or #10-32 bolts or screws with 1.27 cm (0.5 in.) O.D. flat washers. This hardware is not provided with the switch.

Follow these steps to mount the switch to a wall or a panel.

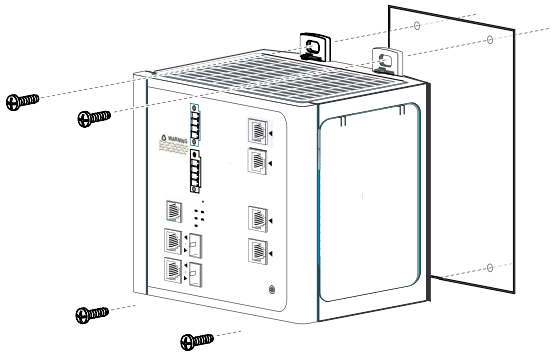
1. If the DIN rail latches are pushed out, push them in so they are fully locked in place.



2. Rotate all feet to their recessed positions so that the switch can mount flat on the wall or pane.

   If greater air circulation around the switch is required, rotate the feet to their extended positions before mounting the switch on the wall.

3. Position the rear panel of the switch against the wall or a panel in the desired location, as shown in this figure.



4. Place M5 or #10-24 or #10-32 bolts or screws with 1.27 cm (0.5 in.) O.D. flat washers through each DIN rail latch, and screw them into the wall.

Install an SFP Module

WARNING: When you insert or remove the small form-factor pluggable (SFP) optical transceiver while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: Under certain conditions, viewing the small form-factor pluggable (SFP) optical transceiver may expose the eye to hazard. When viewed under some conditions, the optical port may expose the eye beyond the maximum permissible exposure recommendations.

ATTENTION: Use SFP modules from only Rockwell Automation. For details about supported modules, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

ATTENTION: We strongly recommend that you do not install or remove the SFP module with fiber-optic cables attached. If you leave the cables attached, damage to the cables, the cable connector, or the optical interfaces in the SFP module can occur. Disconnect all cables before removing or installing an SFP module.

IMPORTANT Installing and removing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is necessary.

You can use any combination of compatible SFP modules:

- Each SFP module must be of the same type as the SFP module on the other end of the cable. The cable must not exceed the stipulated cable length for reliable communications.
- Once you install SFP modules in the switch, be aware that the overall temperature rating of the combined modules (switch and SFP modules) is limited to the lowest maximum temperature rating and the highest minimum temperature rating.

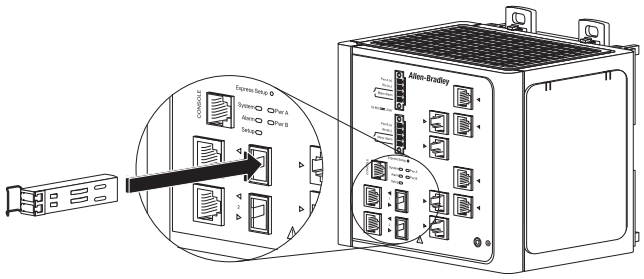
For cable length and temperature specifications, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

To insert an SFP module into an SFP slot, follow these steps.

1. Attach an ESD-preventive wriststrap to your wrist and to a grounded bare metal surface.
2. Grasp both sides of the SFP module and align the module sideways in front of the slot opening.

> **ATTENTION:** If the SFP module cannot be fully inserted, stop! Do not force the module into the slot. Rotate the SFP module 180° and try again.

3. Insert the SFP module into the slot as shown in the following figure until you feel the connector on the module snap into place in the rear of the slot.



31782-M

Ground the Switch

ATTENTION: For proper grounding, you must always connect the power supply functional-ground screw when connecting the power supply. You must provide an acceptable grounding path for each device in your application. For more information on proper grounding guidelines, refer to publication 1770-4.1, Industrial Automation Wiring and Grounding Guidelines.

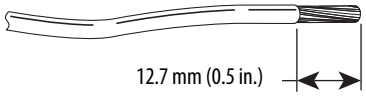
ATTENTION: You must use the external grounding screw on the front of the switch to ground the switch. Use a 5.3 mm^2 (10 AWG) ground wire.

Follow these steps to connect the switch to a protective ground.

1. Use a screwdriver to remove the ground screw from the front panel of the switch.

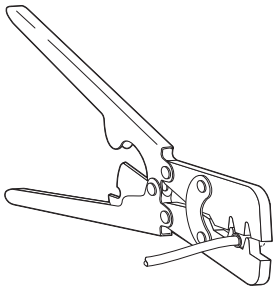
   Store the ground screw for later use.

2. If your ground wire is insulated, use a wire stripping tool to strip the 5.3 mm^2 (10 AWG) ground wire to 12.7 mm (0.5 in.) ± 0.5 mm (0.02 in.).



31789-M

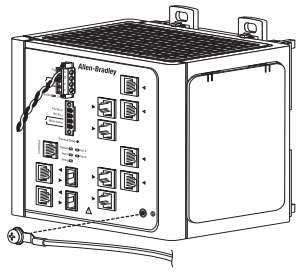
3. Insert the ground wire into the ring terminal lug.
4. Use a crimping tool to crimp the ring terminal to the wire.



31790-M

5. Slide the ground screw through the ring terminal.

6. Insert the ground screw into the ground-screw opening on the front panel.



31791-M

7. Use a ratcheting torque screwdriver to tighten the ground screw and ring terminal lug to the switch front panel to 0.96 N•m (8.5 lb•in).
8. Attach the other end of the ground wire to a grounded bare-metal surface, such as a ground bus, or a grounded DIN rail.

Wire the DC Power Source for the Switch

WARNING: Before performing any of the following procedures, make sure that power is removed from the DC circuit or the area is nonhazardous before proceeding.

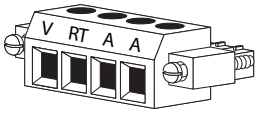
WARNING: To comply with the CE Low Voltage Directive (LVD), this equipment must be powered from a source compliant with the safety extra low voltage (SELV) or protected extra low voltage (PELV).

To comply with UL restrictions, this equipment must be powered from a source compliant with Class 2 or Limited Voltage/Current.

Follow these steps to wire DC power to the switch.

1. Locate the power and alarm relay connector and identify the positive and return DC power connections.

   The positive DC power connection is labeled V, and the negative DC power connection is the adjacent connection labeled RT. Connections labeled A are used for the alarm relay connectors.

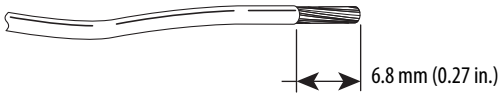


31783-M

2. Measure a length of 0.82...0.52 mm^2 (18...20 AWG) copper wire long enough to connect to the DC power source.

3. Using an 18-gauge wire-stripping tool, strip each of the two wires to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

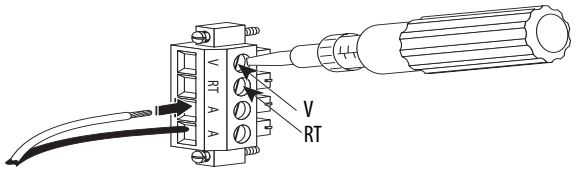
   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wire. Stripping more than the recommended amount of wire can leave exposed wire from the connector after installation.



31784-M

4. Insert the exposed part of the positive wire into the connection labeled V and the exposed part of the return wire into the connection labeled RT.

   Make sure that you cannot see any wire lead. Only wire with insulation can extend from the connector.



31785-M

5. Use a ratcheting-torque screwdriver to torque the power and relay connector captive screws above the installed wire leads to 0.23 N•m (2.0 lb•in).
6. Connect the other end of the positive wire (the one connected to V) to the positive terminal on the DC power source, and connect the other end of the return wire (the one connected to RT) to the return terminal on the DC power source.

   You can use a second power source to provide redundant power. The alarm relays on the switch can be used to warn you if one of the power supplies fails. The switch operates properly with only one power source connected at either Pwr A or Pwr B.
7. If you are installing the switch and are using a second power source, repeat these with a second power and relay connector.



ATTENTION: If multiple power sources are used, do not exceed the specified isolation voltage.

Wire the DC Power Source for the PoE Expansion Module

Follow these instructions if you have a PoE expansion module.

WARNING: Before performing any of the following procedures, make sure that power is removed from the DC circuit or the area is nonhazardous before proceeding.

WARNING: To comply with the CE Low Voltage Directive (LVD), this equipment must be powered from a source compliant with the safety extra low voltage (SELV) or protected extra low voltage (PELV).

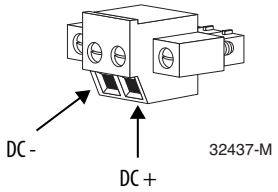
To comply with UL restrictions, this equipment must be powered from a source compliant with Class 2 or Limited Voltage/Current.

Power supply requirements for a PoE expansion module depend on your application.

Application	Power Consumption	Power Supply per Port	Allen-Bradley Products
PoE only IEEE 802.3af	44…57V DC (48V DC nom)	15.4 W, max	Switched mode power supplies: • 1606-XL Standard • 1606-XLE Essential • 1606-XLP Compact • 1606-XLS Performance
PoE and PoE + IEEE 802.3at Type 2	50…57V DC (54V DC nom)	15.4 W, max for PoE 30 W, max for PoE+	

Follow these steps to wire DC power to the PoE expansion module.

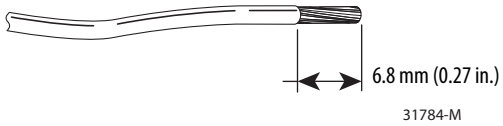
1. Locate the power connector and identify the positive and return DC power connections.



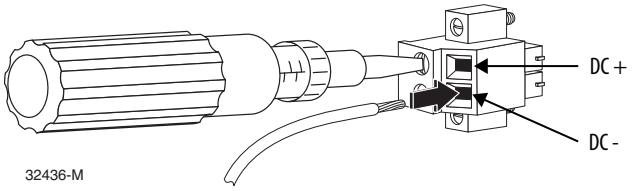
2. Measure a length of 0.82...0.52 mm^2 (18...20 AWG) copper wire long enough to connect to the DC power source.

3. Use an 18-gauge wire-stripping tool to strip each of the two wires to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wire. Stripping more than the recommended amount of wire can leave exposed wire from the connector after installation.



4. Insert the exposed part of the positive wire into the DC + connection and the exposed part of the return wire into the DC - connection.
5. Make sure that you cannot see any wire lead; only wire with insulation can extend from the connector.



6. Use a ratcheting-torque screwdriver to torque the power connector captive screws above the installed wire leads to 0.23 N•m (2.0 lb•in).
7. Connect the other end of the positive wire (the one connected to DC +) to the positive terminal on the DC power source, and connect the other end of the return wire (the one connected to DC -) to the return terminal on the DC power source.

Attach the Power and Relay Connector to the Switch

ATTENTION: The input voltage source of the alarm circuits must be an isolated source and limited to less than or equal to 24V DC, 1 A.

ATTENTION: Exposure to some chemicals can degrade the sealing properties of materials used in the relay. Periodically inspect the relay and check for any degradation. If the relay appears damaged in any way, replace the switch.

Sealed Device: Relay Model AGN200A03, manufactured by Matsushita Electric Works

Relay Cover: Manufacture of Plastic Material—Nippon Oil Corp.
Designation of Plastic Material—Type FC-100
Generic Name of Plastic Material —Liquid crystal polymer

Relay Body: Manufacture of Plastic Material—Ueno Fine Chemicals Industry Ltd.
Designation of Plastic Material— Type 2125G
Generic Name of Plastic Materialv—Liquid crystal polymer

Relay Epoxy: Manufacture of Material—Resinous Kasei Co. Ltd.
Designation of Material – Type A-2500BK
Generic Name of Plastic Material—Epoxy Resin

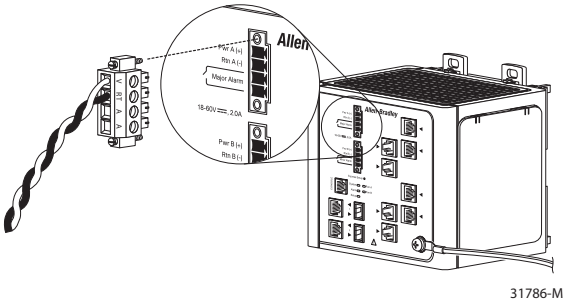
Sealed Device: Relay Model B4GA003Z, manufactured by Fujitsu Takamisawa Electric Co. Ltd.
Relay Cover: Manufacture of Plastic Material —Sumitomo Chemical Co. Ltd.
Designation of Plastic Material—Type E4009
Generic Name of Plastic Material—Liquid crystal polymer

Relay Body: Manufacture of Plastic Material—Sumitomo Chemical Co. Ltd.
Designation of Plastic Material—Type E6807LHF
Generic Name of Plastic Material—Liquid crystal polymer

Relay Epoxy: Manufacture of Material—Sumitomo Bakelite Co. Ltd.
Designation of Material—Type 'SUMIMAC' ECR-9750K2
Generic Name of Plastic Material—Epoxy Resin

Follow these steps to connect the DC power source and relay connector to the switch.

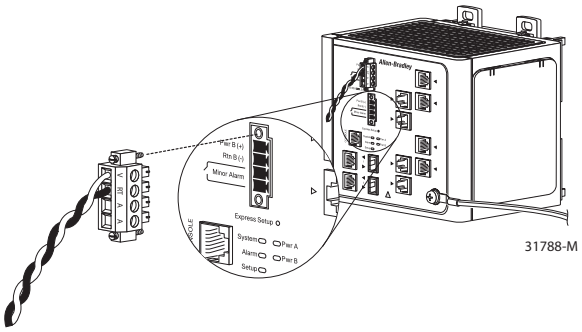
1. Insert the power and relay connector into the Pwr A receptacle on the switch front panel.



31786-M

2. Use a screwdriver to tighten the captive screws on the sides of the power and relay connector.
3. If a second power source is required, insert a second power and relay connector into the Pwr B receptacle on the switch front panel.

ATTENTION: If multiple power sources are used, do not exceed the specified isolation voltage



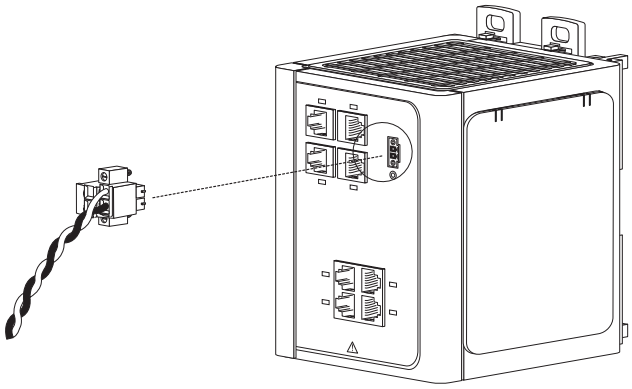
31788-M

4. Use a screwdriver to tighten the captive screws on the sides of the second power and relay connector.

Attach the Power Connector to the PoE Expansion Module

If you have a PoE expansion module, follow these steps to connect the DC power source to the PoE expansion module.

1. Insert the power connector into the DC input terminal block on the PoE expansion module.



2. Use a screwdriver to tighten the captive screws on the sides of the power connector.

Wire External Alarms

The alarm relays on the switch are normally open. To connect an external alarm device to the relays, you must connect two relay contact wires to complete an electrical circuit. Because each external alarm device requires two connections to a relay, the switch supports a maximum of two external alarm devices.

ATTENTION: The input voltage source of the alarm circuits must be an isolated source and limited to less than or equal to 24 V DC, 1 A.

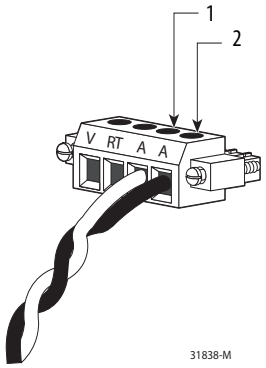
For wire connections to the power and relay connector, you must use UL and CSA rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire (such as Belden part number 9318).

Follow these steps to wire alarms.

1. Measure two strands of twisted-pair wire (18...20 AWG) long enough to connect to the external alarm device.
2. Use a wire stripper to remove the casing from both ends of each wire to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

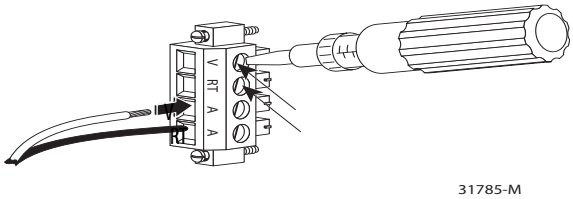
IMPORTANT Do not strip more than 6.8 mm (0.27 in.) of insulation from the wires. Stripping more than the recommended amount of wire can leave exposed wire from the power and relay connector after installation.

3. Insert the exposed wires for the external alarm device into the two connections labeled A, as shown in the following figure.



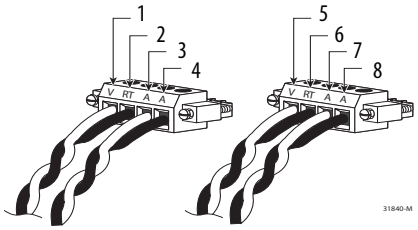
1	External device, relay wire A connection 1	**2**	External device, relay wire A connection 2

4. Use a screwdriver to torque the power and relay connector captive screw (above the installed wire leads) to 0.23 N•m (2.0 lb•in).



5. Repeat these steps to insert the input and output wires of an additional external alarm device into the second power and relay connector.

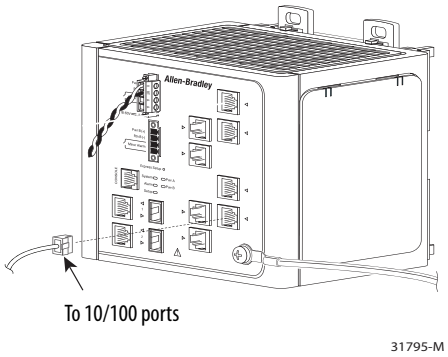
   The following figure shows the completed wiring for two power supplies and two external alarm devices.



1	Power source A positive connection	**5**	Power source B positive connection
2	Power source A return connection	**6**	Power source B return connection
3	External device 1, relay wire major alarm connection	**7**	External device 2, relay wire minor alarm connection
4	External device 1, relay wire major alarm connection	**8**	External device 2, relay wire minor alarm connection

Connect to 10/100 Copper Ports

1. Insert a straight-through, twisted four-pair, Category 5e or better cable with an RJ45 connector into the port.



2. Insert the other cable end into an RJ45 connector on the other device.

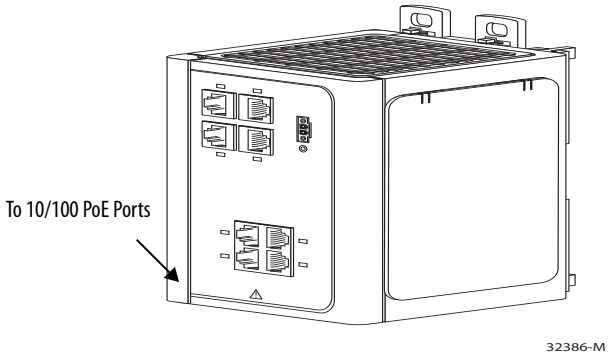
Connect to a PoE Expansion Module Port

Two expansion modules provide PoE capability:

- The 1783-MX04E PoE expansion module provides four PoE ports. You can configure as many as four ports in any combination of PoE and PoE+.
- The 1783-MX04T04E PoE expansion module provides four PoE ports and four non-PoE ports. You can configure as many as four ports in any combination of PoE and PoE+.

The PoE expansion modules each require a separate power supply. For power supply requirements based on your application, refer to page 174.

1. Insert a straight-through, twisted four-pair, Category 5e or better cable with an RJ45 connector into the port.



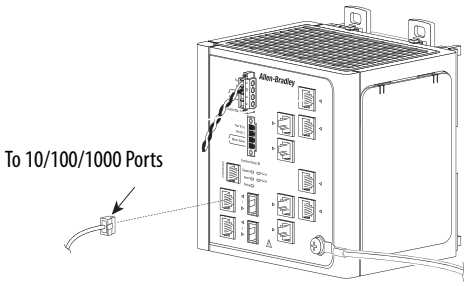
2. Insert the other cable end into an RJ45 connector on the other PoE powered device.

Connect to Dual-purpose Uplink Ports

The switches have two dual-purpose uplink ports. Each dual-purpose uplink port has a 10/100/1000 RJ45 connector for a copper interface and a slot for an SFP module. Only one port of the dual-purpose port can be active at a time. If an SFP module port is connected, the SFP module port has priority.

Connect to 10/100/1000 Uplink Ports

1. Insert a straight-through, twisted four-pair, Category 5e or better cable with an RJ45 connector into the port.



31795-M

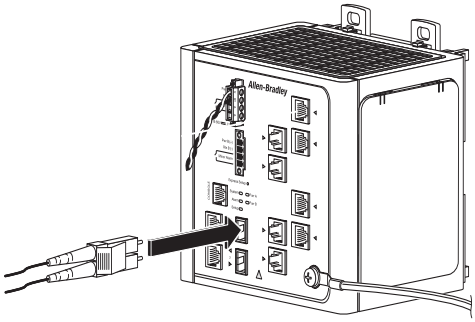
2. Insert the other cable end into an RJ45 connector on the other device.

Connect to SFP Fiber Ports

ATTENTION: Class 1 laser product. Laser radiation is present when the small form-factor pluggable (SFP) optical transceiver is open and interlocks bypassed. Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Follow these steps if you installed an SFP module. For instructions on installing, removing, and connecting to SFP modules, see the documentation that shipped with the SFP module.

1. Insert a fiber-optic cable with an LC connector into the SFP fiber port.



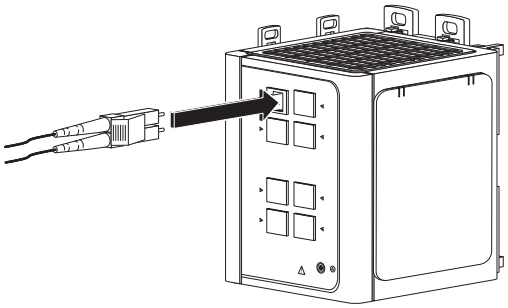
31796-M

2. Insert the other cable end into the other device.

Connect to 100BaseFX Ports

ATTENTION: Class 1 laser product. Laser radiation is present when the system is open and interlocks bypassed. Only trained and qualified personnel are allowed to install, replace, or service this equipment.

1. Insert a fiber-optic cable with an LC connector into the 100BASE-FX port of the 1783-MX08F expansion module.



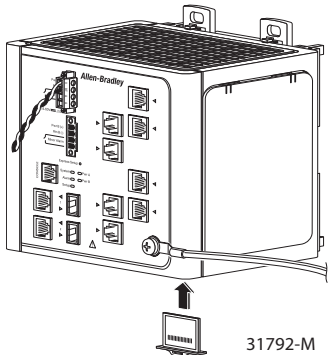
2. Insert the other cable end into the other device.

Install or Remove the CompactFlash Card

The switches ship with the CompactFlash card installed. Follow this procedure when you need to install or remove it from the switch.

WARNING: When you insert or remove the CompactFlash Card while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

Install or remove the CompactFlash card by grasping the tab on the card and either inserting it or removing it from the slot at the bottom of the switch.



IMPORTANT You can install and remove the CompactFlash card while the switch is powered. However, if you do not have a CompactFlash card installed in the switch, you are unable to do the following:

- Start the Device Manager web interface when you apply power to the switch.
- Save configuration changes you made with the AOP via software.
- Start up the switch.

Configure Switch Features

Topic	Page
Access Control Lists (ACLs)	184
Alarms	189
CIP Sync Time Synchronization (Precision Time Protocol)	194
Cryptographic IOS	212
Device-level Ring (DLR)	212
Dynamic Host Configuration Protocol (DHCP) Persistence	238
EtherChannels	244
Motion Prioritized QoS Macros	248
Horizontal Stacking	250
Internet Group Management Protocol (IGMP) Snooping with Querier	252
Network Address Translation (NAT)	254
Network Time Protocol (NTP)	295
Parallel Redundancy Protocol (PRP)	297
Port Mirroring	301
Port Security	303
Port Thresholds	309
Power over Ethernet (PoE)	314
Resilient Ethernet Protocol (REP)	325
Layer 3 Routing	330
Enhanced Interior Gateway Routing Protocol (EIGRP)	332
Open Shortest Path First (OSPF)	337
Simple Network Management Protocol (SNMP)	347
Smartports	350
Spanning Tree Protocol (STP)	361
Virtual Local Area Networks (VLANs)	365

This chapter describes software features that you can configure via Device Manager, the Studio 5000 Logix Designer® application, or both. More software features are available. You can configure some features with the global macro or Smartports feature.

For information about how to configure features not available in Device Manager or the Logix Designer application, see the documentation available at http://www.Cisco.com.

Some features are available only on select switch models and firmware types. See Lite Versus Full Firmware Features (Stratix 5700 Switches) on page 20 and Software Features on page 21.

Access Control Lists (ACLs)

ACLs, also called access lists, filter traffic as it passes through the switch. ACLs permit or deny packets as they cross specified interfaces or VLANs. You configure ACLs on switches with Layer 2 or Layer 3 firmware to provide basic security for your network. If you do not configure ACLs, all packets that pass through the switch can be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces.

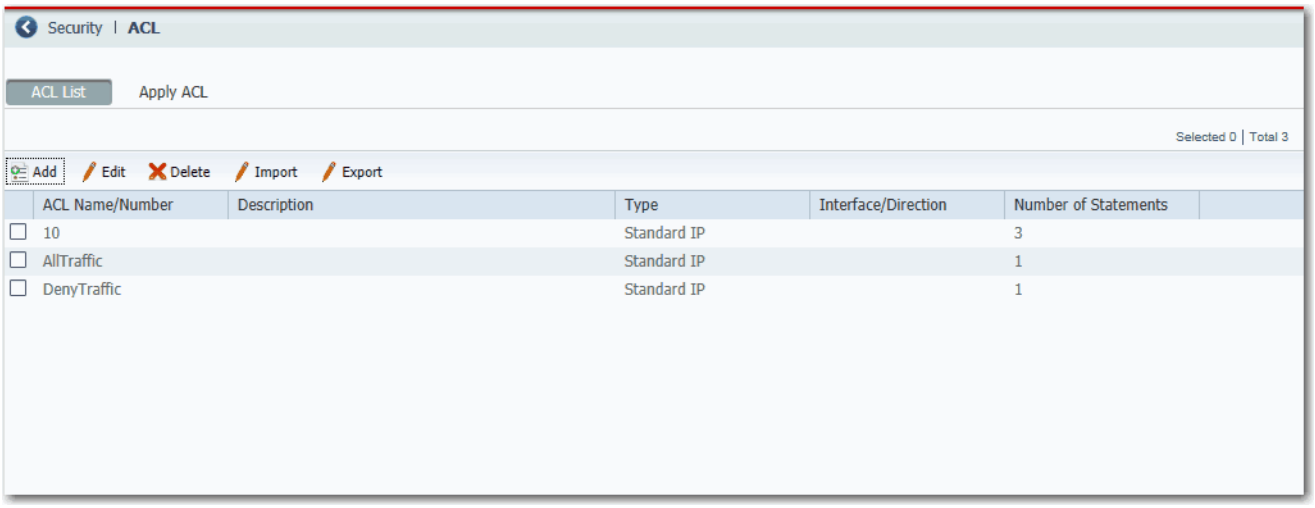
An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies whether to permit or deny packets. An ACE also specifies a set of conditions a packet must satisfy to match the ACE. The meaning of permit or deny depends on the context in which the ACL is used.

When a packet is received on a port, the switch compares the fields in the packet against any ACLs applied to the port. Based on the criteria in the ACL, the switch determines whether the packet has the required conditions to be forwarded. One by one, it tests packets against the conditions in an ACL. The first match decides whether the switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet. Otherwise, the switch drops the packet.

Configure ACLs via Device Manager

The ACL window shows all existing standard and extended ACLs defined on the switch. Once you add an ACL to the ACL List tab, you can apply it to a port and specify a direction on the Apply ACL tab.

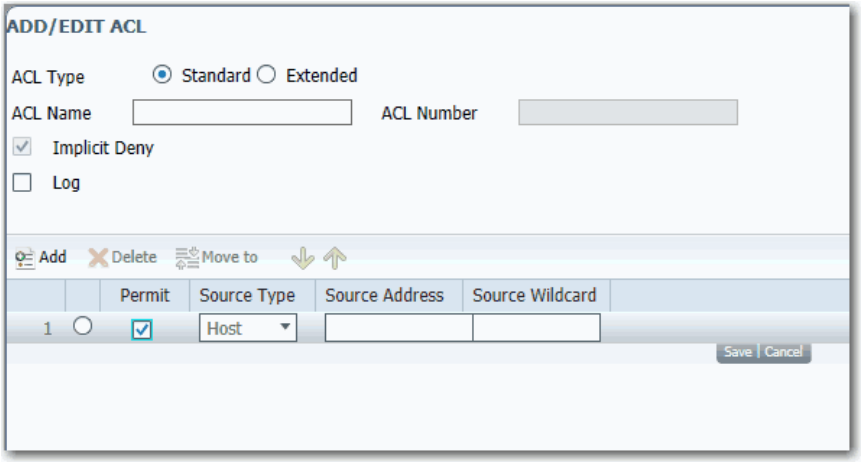
To configure an ACL, from the Configure menu, choose ACL.



Create an ACL

To create an ACL, follow these steps.

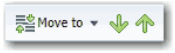
1. From the ACL window, click the ACL List tab.
2. Click Add, and then complete the fields in the header area.



Field	Description
ACL Type	Click Standard or Extended: • Standard (default)—Uses source addresses. • Extended—Uses source and destination addresses and optional protocol type information.
ACL Name	Type an alphanumeric name to identify the ACL. Named access lists are more convenient than numbered access lists because you can specify a meaningful name that is easier to remember and associate with a task. You can reorder statements in or add statements to a named access list.
ACL Number	The number of the ACL, which shows the type of access list: • 1…99—IP standard access list. • 100…199—IP extended access list. • 1300…1999—IP standard access list (expanded range). • 2000…2699—IP extended access list (expanded range).
Implicit Deny	(Not editable). By default, all ACLs have an implicit deny statement at the end. If a packet does not match any of the criteria that are specified in the ACL, it is denied.
Log	Check the checkbox to enable informational logging messages about packets that are permitted or denied by an ACL to be sent to the system log. To view the system log, from the Monitor menu, choose Syslog.

3. To define the ACL entry, click Add in the table area, and then complete the fields.

Field	Description
Permit	To permit traffic, check the checkbox. To deny traffic, clear the checkbox. An access list must contain at least one permit statement or all packets are denied entry into the network.
Protocol	(Extended ACL only). Type the following: • The name or number of an IP protocol (AHP, EIGRP, ESP, GRE, ICMP, IGMP, IGRP, IP, IPINIP, NOS, OSPF, PCP, PIM, TCP, or UDP) or • An integer in the range of 0…255 representing an IP protocol number To match any internet protocol, including ICMP, TCP, and UDP, type IP.
Source Type	Choose the source from which the packet is sent: • Host • Any • Network
Source Address	Type the address of the network or host from which the packet is sent.
Source Wildcard	Type an ACL mask for the source.
Source Operator	(Extended ACL only). To compare the source, choose an operator from the pull-down menu.
Source Port	(Extended ACL only). Type the source port number to compare. Valid values: 0…65535
Destination Type	(Extended ACL only). Choose the type of the destination to which the packet is sent: • Host • Any • Network
Dest Address	(Extended ACL only). Type the network or host number to which the packet is sent.
Dest Wildcard	(Extended ACL only). Type an ACL mask for the destination.
Dest Operator	(Extended ACL only). To compare the destination, choose an operator from the pull-down menu.
Dest Port	(Extended ACL only). Type the destination port number to compare. Valid values: 0…65535

4. Click Save.
5. Repeat Steps 3 and 4 to create as many conditions as needed.
6. To order the conditions in the list, use the Move buttons 

.

IMPORTANT The order of the conditions is critical to whether a packet is forwarded. The first condition in the list that matches a packet allows the packet to be forwarded. After the first match, the switch stops testing.

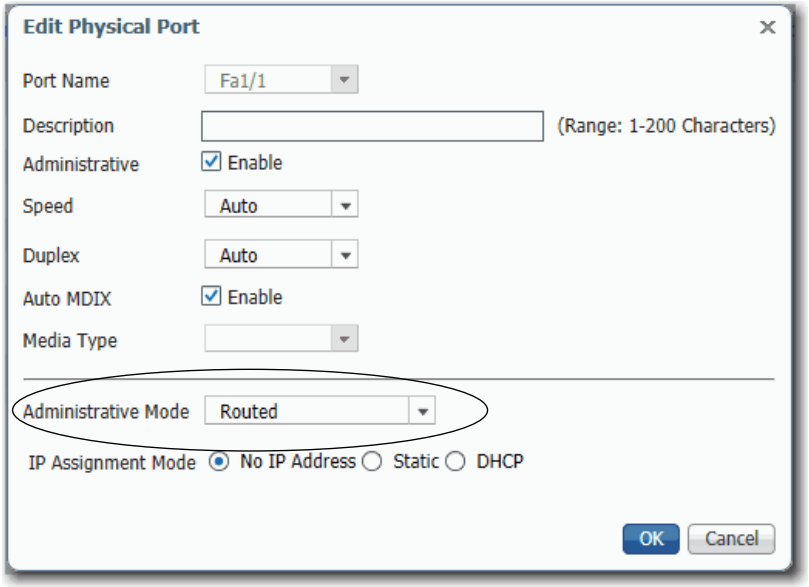
7. Click Submit.

Apply an ACL

You can apply inbound and outbound ACLs to ports:

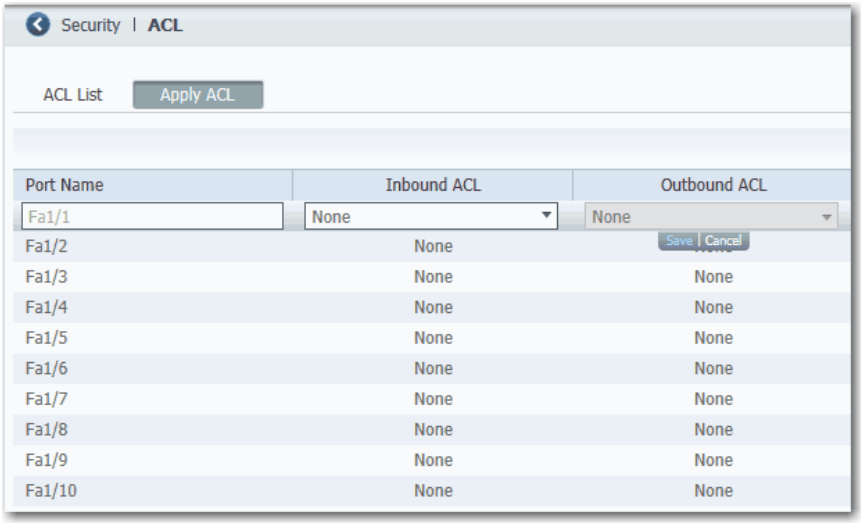
- Inbound ACLs can be applied to any port.
- Outbound ACLs can be applied to only routed ports or ports assigned to an Access VLAN. You can configure these port settings in the Administrative Mode field on the Edit Physical Port window (Figure 2). For more information about configuring port settings, see Port Configuration on page 59.

Figure 2 - Edit Physical Port Window



To apply an ACL to a port, follow these steps.

1. From the ACL window, click the Apply ACL tab.



2. Click the row for a port name.
3. In the Inbound ACL column, choose the ACL from the list of configured ACLs.
4. In the Outbound ACL column, choose ACL from the list of configured ACLs.
5. Click Save.

Alarms

Alarms vary by switch model.

Table 30 - Alarm Descriptions

Switch	Alarm Description
Stratix® 5400 switch	The switch lets you connect two alarm inputs from external devices, such as a door or temperature gauge, to the alarm input port on the front panel of the switch. An over- or under-temperature alarm or a port not forwarding condition automatically triggers the default output. You can configure the output alarm relay as either normally energized or de-energized.
Stratix 5410 switch	The switch provides the following external alarms: • Four alarm inputs to sense whether the alarm setting is open or closed. The alarm input is a dry-contact alarm port. You can connect up to four alarm inputs from devices, such as a door, a temperature gauge, or a fire alarm to the alarm port. An alarm generates a system message and turns on an alarm status indicator. • One alarm output that you can configure as a minor or major alarm. Output alarms often control an external alarm, such as a bell or a light. To connect an external alarm device to the relay, you connect two relay contact wires to complete the electrical circuit. The front panel alarm port uses an RJ45 connector.
Stratix 5700 switch	The switch lets you connect two alarm inputs from external devices, such as a door or temperature gauge, to the alarm input port on the front panel of the switch. An over- or under-temperature alarm or a port not forwarding condition automatically triggers the default output. You can configure the output alarm relay as either normally energized or de-energized.
ArmorStratix™ 5700 switch	The switch provides the following external alarms: • One input alarm relay circuit to sense whether the alarm input is open or closed relative to the alarm input reference pin. • One output alarm relay circuit with one Form C (single-pole, double-throw) relay with one normally open (NO) and one normally closed (NC) contact. You can configure the output alarm as either normally energized or normally de-energized.
Stratix 8000/8300 switch	The switches provide the following on the front panel: • Major alarm relay—When closed, the major alarm relay indicates a dual-mode power supply or primary temperature alarm. • Minor alarm relay—When closed, the minor alarm relay indicates these alarm states: – Link fault – Port not forwarding – Port not operating – Frame Check Sequence (FCS) bit error rate

Configure Alarms via Device Manager

The switch software monitors conditions on a per port or a global basis. If the conditions do not match the set parameters, an alarm or a system message is triggered. By default, the switch sends the system messages to a logging facility. You can configure the switch to send SNMP traps to an SNMP server. You can also configure the switch to trigger an external alarm device by using the two independent alarm relays.

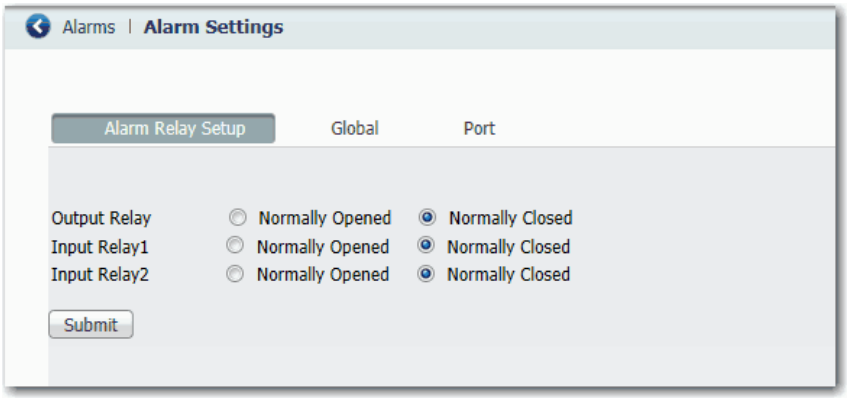
Alarm Relay Settings

You can configure the switch to trigger an external alarm device. The switch software is configured to detect faults that are used to energize the relay coil and change the state on both of the relay contacts. Normally open contacts close and normally closed contacts open.

To configure alarm relay settings, from the Configure menu, choose Alarm Settings.

On the Alarm Relay Setup tab, click one of these options for each type of alarm relay:

- Normally Opened—The normal condition is that no current flows through the contact. The alarm is generated when current flows.
- Normally Closed—The normal condition has current that flows through the contact. The alarm is generated when the current stops flowing.



Global Alarms

From the Configure menu, choose Alarm Settings and click the Global tab.

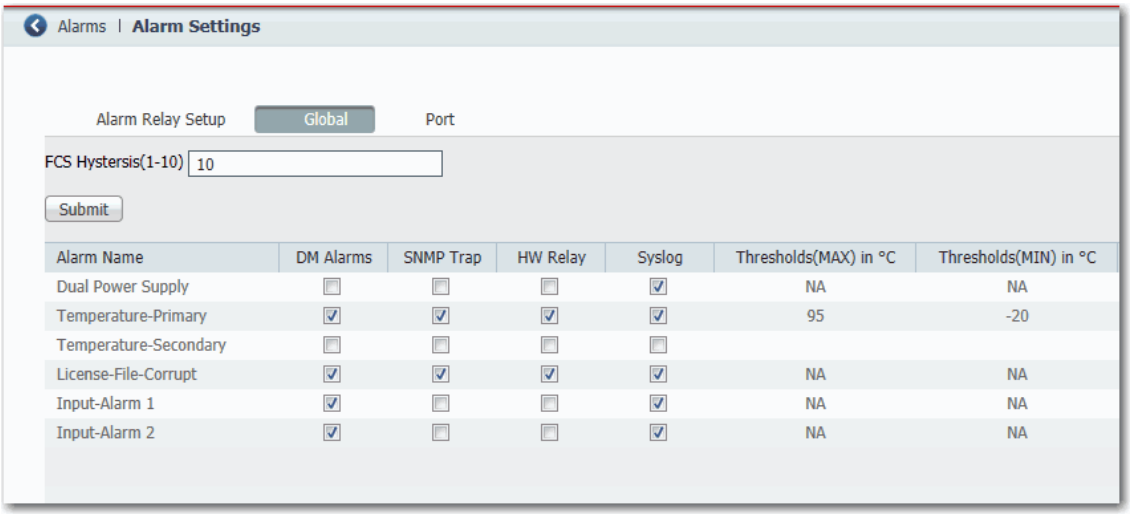
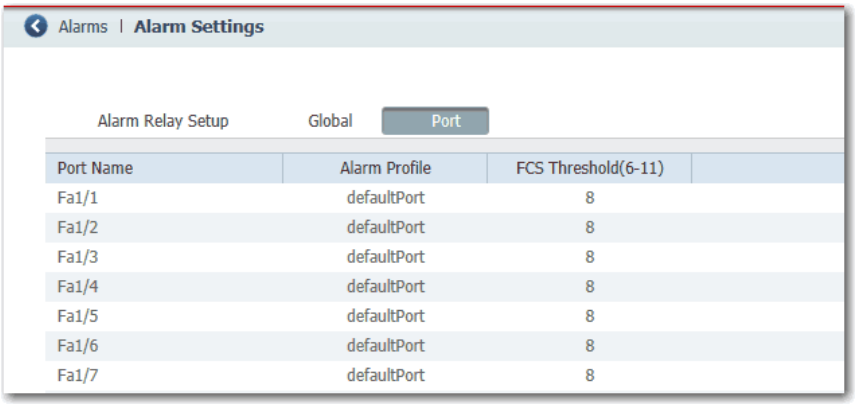


Table 31 - Global Tab Fields

Field	Description
FCS Hysteresis (1-10)	The frame check sequence (FCS) error hysteresis threshold is used to determine when an alarm condition is cleared. This value is expressed as a percentage of fluctuation from the FCS bit error rate. The default setting is 8 percent. You can adjust the percentage to prevent toggling the alarm condition when the FCS bit error rate fluctuates near the configured bit error rate. Valid percentages for global settings are 1 . . . 10. This setting can also be configured on an individual port by clicking the Port tab.
Alarm Name	These types of alarms can be enabled or disabled: • Dual Power Supply—The switch monitors DC power supply levels. If the system is configured to operate in a dual power mode, an alarm is triggered if a power supply fails or is missing. The alarm is automatically cleared when the power supplies are present or working. You can configure the power supply alarm to be connected to the hardware relays. • Temperature-Primary—These alarms are triggered when the system temperature is higher or lower than the configured thresholds. By default, the primary temperature alarm is associated with the major relay. • Temperature-Secondary—These alarms are triggered when the system temperature is higher or lower than the configured thresholds. • License-File-Corrupt—An alarm is triggered when the license file is corrupt. • Input-Alarm 1—An alarm is triggered based on an external input alarm. • Input-Alarm 2—An alarm is triggered based on an external input alarm.
DM Alarms	Alarm information appears on the dashboard of Device Manager.
SNMP Trap	Alarm traps are sent to an SNMP server, if SNMP is enabled on the Configure > Security > SNMP window.
HW Relay	If the alarm relay is triggered, the switch sends a fault signal to a connected external alarm device, such as a bell, light, or other signaling device.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Monitor > Syslog window.
Thresholds (MAX) in °C	The maximum temperature threshold for the corresponding Temperature-Primary or Temperature-Secondary alarm, if enabled.
Thresholds (MIN) in °C	The minimum temperature threshold for the corresponding Temperature-Primary or Temperature-Secondary alarm, if enabled.

Port Alarms

From the Configure menu, choose Alarm Settings and click the Port tab.



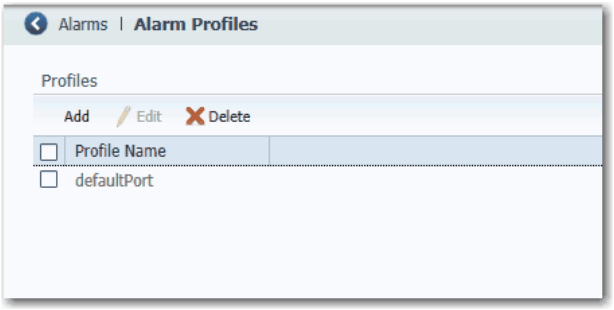
For each port, choose an Alarm Profile and set the FCS threshold. The frame check sequence (FCS) error hysteresis threshold is expressed as a percentage of fluctuation from the FCS bit error rate. The default setting is 8 percent. You can adjust the percentage to prevent toggling the alarm condition when the FCS bit error rate fluctuates near the configured bit error rate. Valid percentages for port settings are 6...11.

Alarm Profiles

You can use alarm profiles to apply a group of alarm settings to multiple interfaces. These alarm profiles are created for you:

- defaultPort
- ab-alarm (created during Express Setup)

From the Configure menu, choose Alarm Profiles.



On the Add/Edit Profile Instance window, you can configure the alarms and actions for an alarm profile.

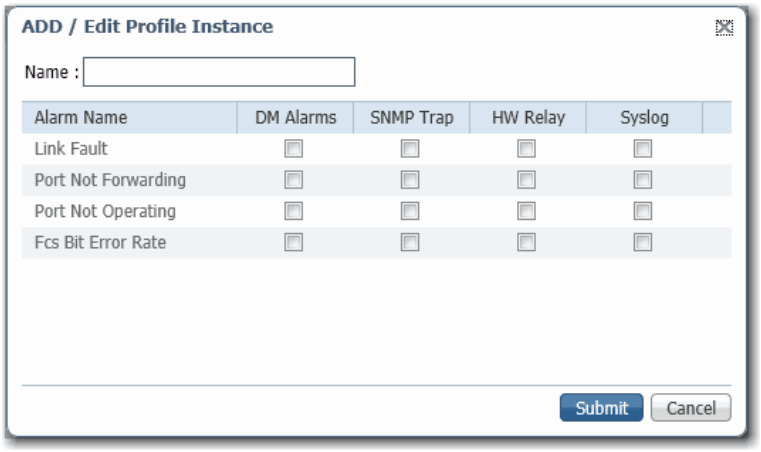


Table 32 - Add/Edit Profile Instance Fields

Field	Description
Name	A unique name for the alarm profile.
Alarm Name	These types of alarms can trigger an action.
DM Alarms	Alarm information appears on the dashboard of Device Manager.
SNMP Trap	Alarm traps are sent to an SNMP server, if SNMP is enabled on the Configure > Security > SNMP window.
HW Relay	If the alarm relay is triggered, the switch sends a fault signal to a connected external alarm device, such as a bell, light, or other signaling device.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Monitor > Syslog window.

CIP Sync Time Synchronization (Precision Time Protocol)

CIP Sync time synchronization refers to the IEEE 1588 standard for Precision Time Protocol (PTP). The protocol enables precise synchronization of clocks in measurement and control systems. Clocks are synchronized with nanosecond accuracy over the EtherNet/IP communication network. PTP enables systems that include clocks of various precisions, resolution, and stability to synchronize. PTP generates a master-slave relationship among the clocks in the system. All clocks ultimately derive their time from a clock that is selected as the grandmaster clock.

By default, PTP is disabled on all Fast Ethernet and Gigabit Ethernet ports. You can enable or disable PTP on a per-port basis. For a list of switches that support PTP, see page 21.

To configure PTP, you choose one of these clock modes:

- Boundary mode
- End to End Transparent mode
- Forward mode (default)
- NTP-PTP Clock mode

For more information about these modes, refer to the Converged Plantwide Ethernet Design and Implementation Guide, publication ENET-TD001.

Boundary Mode

In Boundary mode, the switch participates in selecting the best master clock. If the switch does not detect a better clock, the switch becomes the grandmaster clock on the network and the parent clock to all connected devices. If the best master is determined to be a clock connected to the switch, the switch synchronizes to that clock as a child to the clock, and then acts as a parent clock to devices connected to other ports.

After initial synchronization, the switch and the connected devices exchange timing messages to correct time skew caused by clock offsets and network delays. This mode can eliminate the effects of latency fluctuations. Because jitter and errors can accumulate in cascaded topologies, choose this mode only for networks with fewer than four layers of cascaded devices.

The clock selection process is determined in part by the relative priority of the switches in the network. You can define the priorities of switches in the Priority 1 and Priority 2 fields in either Device Manager or the Logix Designer application.

In Boundary mode, one or more switch ports can be PTP-enabled.

End to End Transparent Mode

IMPORTANT End to End Transparent mode does not work with redundant gateways in a device-level ring (DLR). For more information about redundant gateways, see page 217.

In End to End Transparent mode, the switch transparently synchronizes all clocks with the master clock connected to it. All ports are enabled by default. This device corrects the delay incurred by every packet passing through it (referred to as residence time). This mode causes less jitter and error accumulation than Boundary mode.

In End to End Transparent mode, all switch ports are PTP-enabled by default.

Forward Mode

In Forward mode, the switch passes PTP packets as normal multicast traffic. All switch ports are PTP-enabled by default. Forward mode is the default mode.

NTP-PTP Clock Mode (Stratix 5400 and 5410 Switches)

In NTP-PTP Clock mode, the switch functions as the grandmaster clock and boundary clock:

- As grandmaster, it uses PTP while deriving the time source from Network Time Protocol (NTP).
- If configured as a secondary grandmaster, the switch functions as a boundary clock to forward time, making sure that all devices on the PTP network remain synchronized in a failover scenario.

IMPORTANT When changing PTP timing message settings, remember that the system does not operate properly unless all devices in the system have the same values.

NTP-PTP Clock mode enables tightly-controlled PTP zones, such as motion applications, to maintain time relative to other devices outside the PTP zone that use NTP. In this scenario, NTP-PTP clock time is beneficial for logging and event tracking.

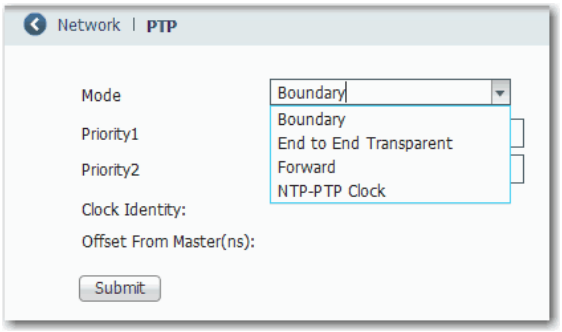
Before you configure a switch to use NTP-PTP clock mode, do the following:

- Configure NTP, as described on page 295. While NTP-PTP Clock mode requires only one NTP time source, as a best practice, we recommend you configure two or more NTP time sources.
- Make sure the NTP clock is stable.
- Know the priority settings assigned to other PTP devices, so that you can set up the switch as the grandmaster.

Configure Time Synchronization via Device Manager

1. From the Configure menu, choose PTP.
2. From the Mode pull-down menu, choose a mode.

   The modes and fields shown in the following figure vary based on the switch model and mode setting.



3. Complete the following fields, and then click Submit.

Field	Description
Priority 1	(Boundary or NTP-PTP Clock mode). Type a value to override the default criteria (clock quality, clock class, and so on) for the best master clock selection. A lower value takes precedence. Valid values: 0…255 Default: 128
Priority 2	(Boundary or NTP-PTP Clock mode). Type a value to use as a tie-breaker between two devices that are otherwise equally matched in the default criteria. For example, you can give a specific switch priority over other identical switches. A lower value takes precedence. Valid values: 0…255 Default: 128
Clock Identity	Displays a unique identifier for the clock.
Offset From Master (ns)	Displays the time offset in nanoseconds between the slave and master clocks.
Passthrough (Stratix 8000/8300 switches)	(Boundary or End to End Transparent mode). Check the checkbox to enable PTP pass-through processing. After PTP pass-through is enabled, all PTP messages are passed to and from the expansion module ports in the VLAN on which the packets are received. The PTP pass-through feature is not compatible with the Virtual Routing and Forwarding (VRF), PolicyBased Routing (PBR), and PVLAN (Private Virtual Local Area Network) features.

4. To complete the remaining fields, refer to the figure and table that corresponds to your mode.

Mode	Page
Boundary	197
End to End	199
Forward	201
NTP-PTP Clock	202

Figure 3 - Boundary Mode

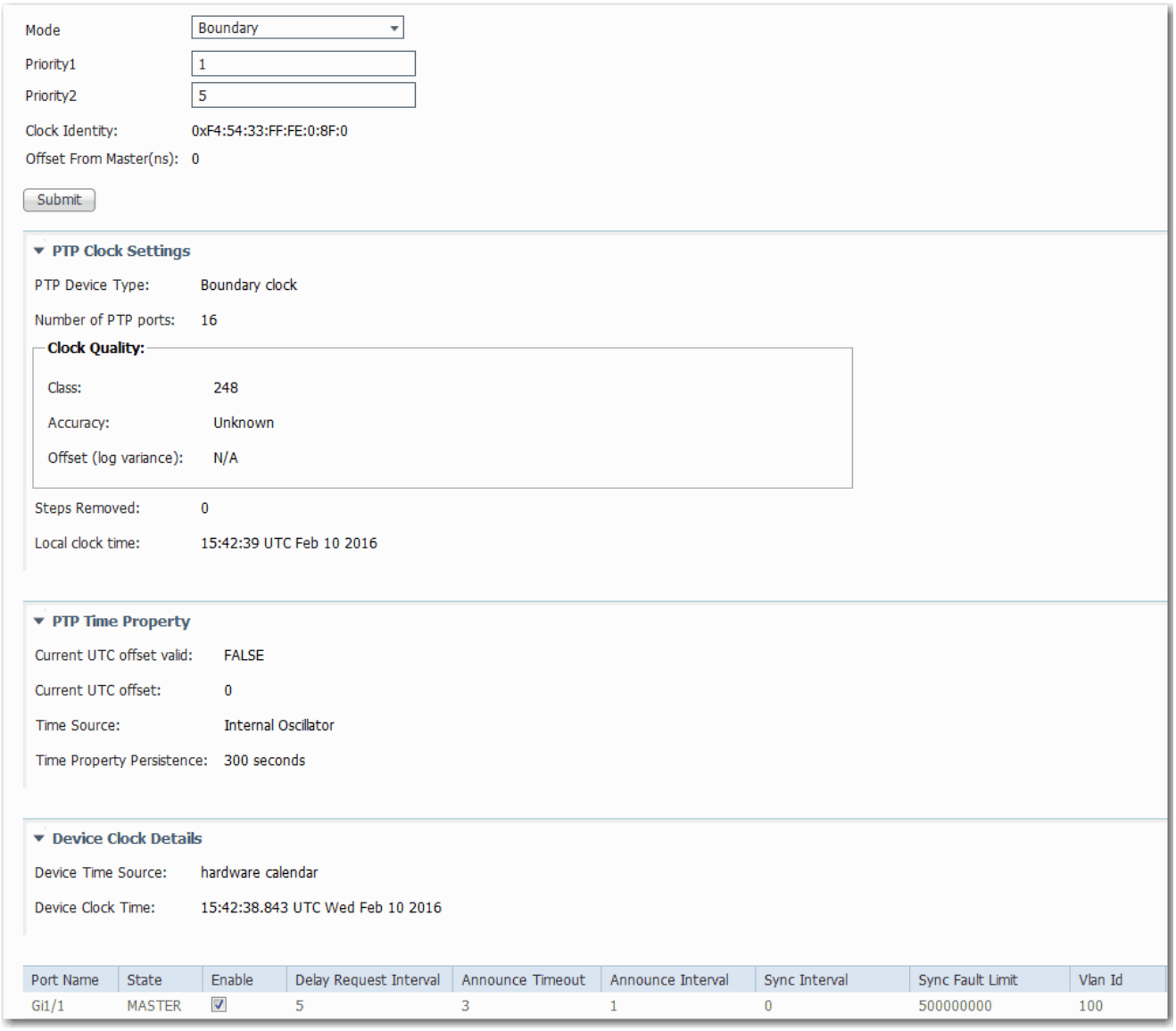


Table 33 - Boundary Mode Fields

Field	Description
PTP Clock Settings	
PTP Device Type	Displays the PTP clock type of the switch, as determined by the Mode setting.
Number of PTP ports	Displays the number of ports assigned to the PTP clock.

Table 33 - Boundary Mode Fields (Continued)

Field	Description
Clock Quality	Displays a summary of the quality of the grandmaster clock: • Class—Time and frequency traceability of the grandmaster clock. • Accuracy—Expected accuracy of the grandmaster clock when the Best Master Clock algorithm is in use. • Offset (log variance)— Offset between the local clock and an ideal reference clock.
Steps Removed	Displays the number of hops from the local clock to the grandmaster clock.
Local clock time	Displays the time stamp of the local clock.
PTP Time Property	
Current UTC offset valid	Indicates whether the current Coordinated Universal Time (UTC) offset is valid.
Current UTC offset	Displays the offset between the International Atomic Time (TAI) and UTC in seconds.
Time Source	Displays the time source used by the grandmaster clock.
Time Property Persistence	Displays the number of seconds that time properties are preserved after a primary grandmaster clock fails and a secondary grandmaster clock takes over.
Device Clock Details	
Device Time Source	Displays the time source used by the switch.
Device Clock Time	Displays the time on the switch, obtained from the time source.
Per Port Settings	
Port Name	Displays the port type and port number: • Fa—Fast Ethernet • Gi—Gigabit Ethernet • Te—TenGigabit Ethernet
State	Displays the synchronization state of the switch port with the parent or grandmaster clock: • Initializing—The switch port is waiting while a parent or grandmaster clock is selected. • Listening—The switch port is waiting while a parent or grandmaster clock is selected. • Pre-master—The switch port is transitioning to change to Master state. • Master—The switch is acting as a parent clock to the devices connected to that switch port. • Passive—The switch has detected a redundant path to a parent or grandmaster clock. For example, two different switch ports claim the same parent or grandmaster clock. To prevent a loop in the network, one of the ports changes to Passive state. • Uncalibrated—The switch port cannot synchronize with the parent or grandmaster clock. • Slave—The switch port is connected to and synchronizing with the parent or grandmaster clock. • Faulty—Either PTP is not operating properly on the switch port or nothing is connected to the port. • Disabled—PTP is not enabled on the switch port.
Enable	Check the checkbox for each port on which to enable PTP. You can enable one or more switch ports. By default, PTP is enabled on all the Fast Ethernet and Gigabit Ethernet ports. For Stratix 8000/8300 switches, only the ports on the base switch module are PTP-capable. The switch expansion modules do not support PTP. When at least one switch port is PTP-enabled, the End to End Transparent mode is selected by default.
Delay Request Interval	The logarithmic mean interval in seconds Type the recommended to connected devices to send delay request messages when the switch port is in the master state. Valid values: • -1—half second • 0—1 second • 1—2 seconds • 2—4 seconds • 3—8 seconds • 4—16 seconds • 5—32 seconds • 6—64 seconds Default: 5 (32 seconds)
Announce Timeout	Type the number of announce intervals, specified as the logarithmic mean in seconds, that must pass without receipt of an announce message from the parent or grand master clock before the switch selects a new parent or grand master clock. Valid values: 2…10 Default: 3 (8 seconds)

Table 33 - Boundary Mode Fields (Continued)

Field	Description
Announce Interval	Type the time interval, specified as the logarithmic mean in seconds, for sending announce messages. Valid values: • 0—1 second • 1—2 seconds • 2— 4 seconds • 3— 8 seconds • 4—16 seconds Default: 1 (2 seconds)
Sync Interval	Type the time interval, specified as the logarithmic mean in seconds, for sending synchronization messages. Valid values: • -1—half second • 0—1 second • 1— 2 seconds Default: 0 (1 second)
Sync Fault Limit	Type the maximum clock offset before PTP attempts to reacquire synchronization. Valid values: 50…500000000 nanoseconds Default: 50000 nanoseconds **IMPORTANT:** We recommend against setting the sync limit below the default (50000 nanoseconds). Use values below 50000 nanoseconds only in networks with a very high-precision grandmaster clock. These networks have a critical need to keep very sensitive devices synchronized.
Vlan Id (Not available on Stratix 8000/8300 switches)	To configure PTP on a VLAN of a trunk port, type the VLAN ID. Only PTP packets in the VLAN you specify are processed. PTP packets from other VLANs are dropped. You can only enable PTP on one VLAN on a trunk port. Valid values: 1…4094 The default is the native VLAN of the trunk port.

Figure 4 - End to End Transparent Mode

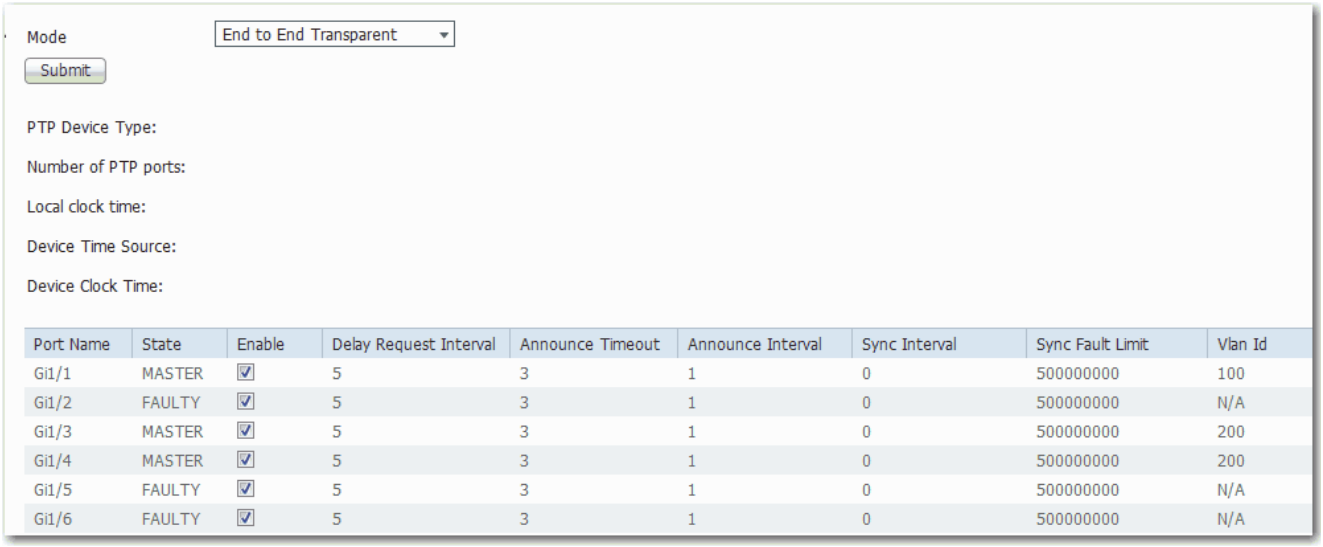


Table 34 - End to End Transparent Mode Fields

Field	Description
PTP Device Type	Displays the PTP clock type of the switch, as determined by the Mode setting.
Number of PTP ports	Displays the number of ports assigned to the PTP clock.
Local clock time	Displays the time stamp of the local clock.
Device Time Source	Displays the time source used by the switch.
Device Clock Time	Displays the time on the switch, obtained from the time source.

Table 34 - End to End Transparent Mode Fields (Continued)

Field	Description
Per Port Settings	
Port Name	Displays the port type and port number: • Fa—Fast Ethernet • Gi—Gigabit Ethernet • Te—TenGigabit Ethernet
State (Not available on Stratix 8000/8300 switches)	Displays the synchronization state of the switch port with the parent or grandmaster clock: • Initializing—The switch port is waiting while a parent or grandmaster clock is selected. • Listening—The switch port is waiting while a parent or grandmaster clock is selected. • Pre-master—The switch port is transitioning to change to Master state. • Master—The switch is acting as a parent clock to the devices connected to that switch port. • Passive—The switch has detected a redundant path to a parent or grandmaster clock. For example, two different switch ports claim the same parent or grandmaster clock. To prevent a loop in the network, one of the ports changes to Passive state. • Uncalibrated—The switch port cannot synchronize with the parent or grandmaster clock. • Slave—The switch port is connected to and synchronizing with the parent or grandmaster clock. • Faulty—Either PTP is not operating properly on the switch port or nothing is connected to the port. • Disabled—PTP is not enabled on the switch port.
Enable	Check the checkbox for each port on which to enable PTP. You can enable one or more switch ports. By default, PTP is enabled on all the Fast Ethernet and Gigabit Ethernet ports. For Stratix 8000/8300 switches, only the ports on the base switch module are PTP-capable. The switch expansion modules do not support PTP. When at least one switch port is PTP-enabled, the End to End Transparent mode is selected by default.
Delay Request Interval (Not available on Stratix 8000/8300 switches)	The logarithmic mean interval in seconds Type the recommended to connected devices to send delay request messages when the switch port is in the master state. Valid values: • -1—half second • 0—1 second • 1—2 seconds • 2—4 seconds • 3—8 seconds • 4—16 seconds • 5—32 seconds • 6—64 seconds Default: 5 (32 seconds)
Announce Timeout (Not available on Stratix 8000/8300 switches)	Type the number of announce intervals, specified as the logarithmic mean in seconds, that must pass without receipt of an announce message from the parent or grand master clock before the switch selects a new parent or grand master clock. Valid values: 2…10 Default: 3 (8 seconds)
Announce Interval (Not available on Stratix 8000/8300 switches)	Type the time interval, specified as the logarithmic mean in seconds, for sending announce messages. Valid values: • 0—1 second • 1—2 seconds • 2— 4 seconds • 3— 8 seconds • 4—16 seconds Default: 1 (2 seconds)

Table 34 - End to End Transparent Mode Fields (Continued)

Field	Description
Sync Interval (Not available on Stratix 8000/8300 switches)	Type the time interval, specified as the logarithmic mean in seconds, for sending synchronization messages. Valid values: • -1—half second • 0—1 second • 1— 2 seconds Default: 0 (1 second)
Sync Fault Limit (Not available on Stratix 8000/8300 switches)	Type the maximum clock offset before PTP attempts to reacquire synchronization. Valid values: 50…500000000 nanoseconds Default: 50000 nanoseconds **IMPORTANT:** We recommend against setting the sync limit below the default (50000 nanoseconds). Use values below 50000 nanoseconds only in networks with a very high-precision grandmaster clock. These networks have a critical need to keep very sensitive devices synchronized.
Vlan Id (Not available on Stratix 8000/8300 switches)	Stratix To configure PTP on a VLAN of a trunk port, type the VLAN ID. Only PTP packets in the VLAN you specify are processed. PTP packets from other VLANs are dropped. You can only enable PTP on one VLAN on a trunk port. Valid values: 1…4094 The default is the native VLAN of the trunk port.

Figure 5 - Forward Mode

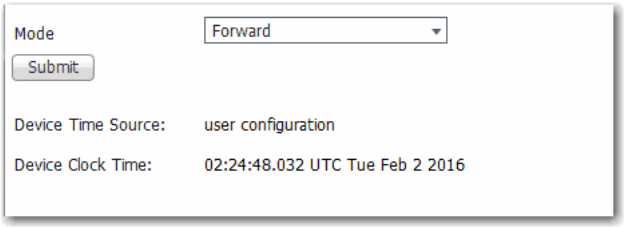


Table 35 - Forward Mode Fields

Field	Description
Device Time Source	Displays the time source used by the switch.
Device Clock Time	Displays the time on the switch, obtained from the time source.

Figure 6 - NTP-PTP Clock Mode

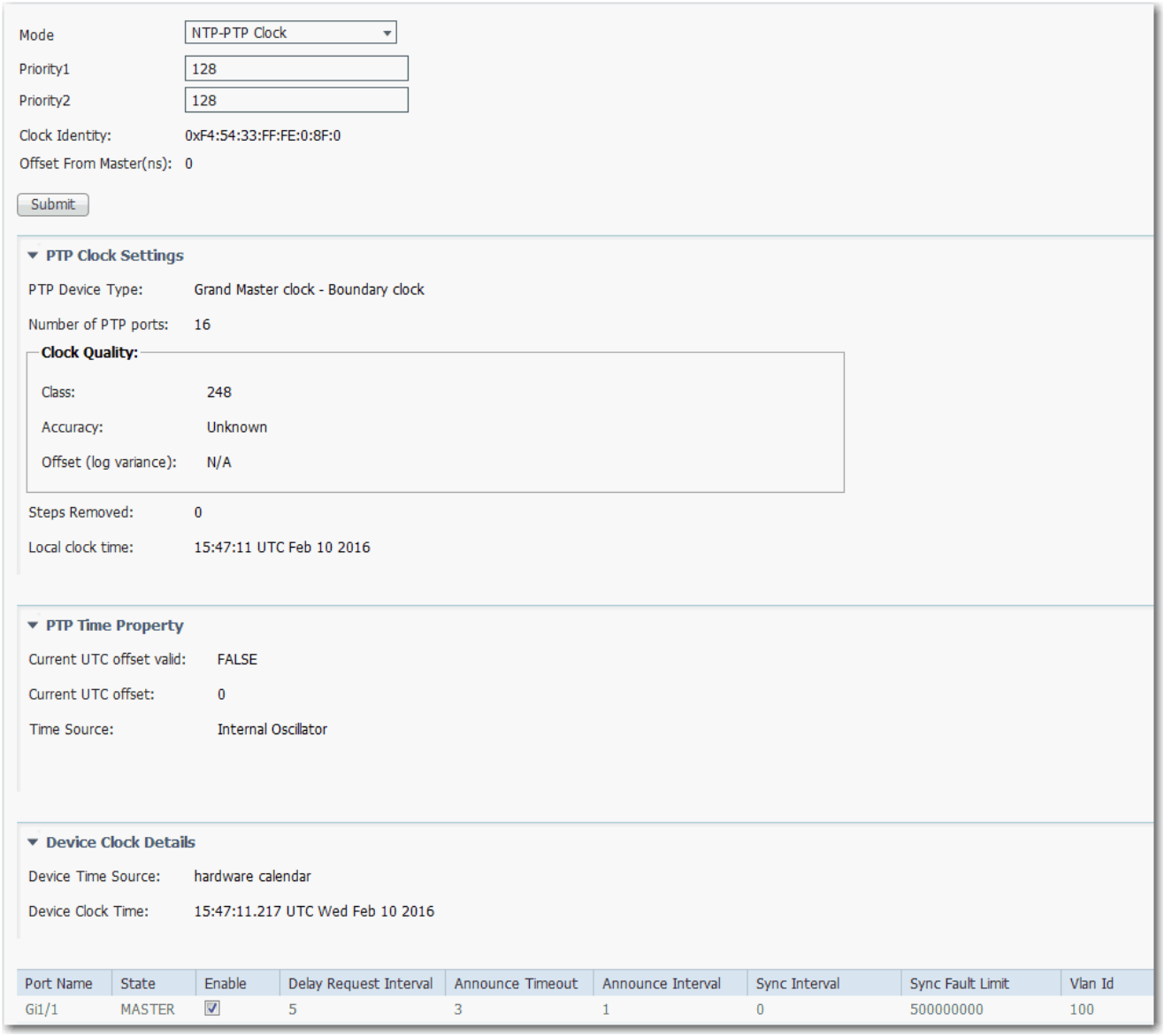


Table 36 - NTP-PTP Clock Mode Fields

Field	Description
PTP Clock Settings	
PTP Device Type	Displays the PTP clock type of the switch, as determined by the Mode setting.
Number of PTP ports	Displays the number of ports assigned to the PTP clock.
Clock Quality	Displays a summary of the quality of the grandmaster clock: • Class—Time and frequency traceability of the grandmaster clock. • Accuracy—Expected accuracy of the grandmaster clock when the Best Master Clock algorithm is in use. • Offset (log variance)— Offset between the local clock and an ideal reference clock.
Steps Removed	Displays the number of hops from the local clock to the grandmaster clock.
Local clock time	Displays the time stamp of the local clock.
PTP Time Property	
Current UTC offset valid	Indicates whether the current Coordinated Universal Time (UTC) offset is valid.
Current UTC offset	Displays the offset between the International Atomic Time (TAI) and UTC in seconds.

Table 36 - NTP-PTP Clock Mode Fields (Continued)

Field	Description
Time Source	Displays the time source used by the grandmaster clock.
Device Clock Details	
Device Time Source	Displays the time source used by the switch.
Device Clock Time	Displays the time on the switch, obtained from the time source.
Per Port Settings	
Port Name	Displays the port type and port number: • Fa—Fast Ethernet • Gi—Gigabit Ethernet • Te—TenGigabit Ethernet
State	Displays the synchronization state on the switch port with the parent or grandmaster clock: • Initializing—The switch port is waiting while a parent or grandmaster clock is selected. • Listening—The switch port is waiting while a parent or grandmaster clock is selected. • Pre-master—The switch port is transitioning to change to Master state. • Master—The switch is acting as a parent clock to the devices connected to that switch port. • Passive—The switch has detected a redundant path to a parent or grandmaster clock. For example, two different switch ports claim the same parent or grandmaster clock. To prevent a loop in the network, one of the ports changes to Passive state. • Uncalibrated—The switch port cannot synchronize with the parent or grandmaster clock. • Slave—The switch port is connected to and synchronizing with the parent or grandmaster clock. • Faulty—Either PTP is not operating properly on that switch port or nothing is connected to the port. • Disabled—PTP is not enabled on the switch port.
Enable	Check the checkbox for each port on which to enable PTP. You can enable one or more switch ports. By default, PTP is enabled on all the Fast Ethernet and Gigabit Ethernet ports. For Stratix 8000/8300 switches, only the ports on the base switch module are PTP-capable. The switch expansion modules do not support PTP. When at least one switch port is PTP-enabled, the End to End Transparent mode is selected by default.
Delay Request Interval	Type the recommended to connected devices to send delay request messages when the switch port is in the master state. Valid values: • -1—half second • 0—1 second • 1—2 seconds • 2—4 seconds • 3—8 seconds • 4—16 seconds • 5—32 seconds • 6—64 seconds Default: 5 (32 seconds)
Announce Timeout	Type the number of announce intervals, specified as the logarithmic mean in seconds, that must pass without receipt of an announce message from the parent or grand master clock before the switch selects a new parent or grand master clock. Valid values: 2…10 Default: 3 (8 seconds)
Announce Interval	Type the time interval, specified as the logarithmic mean in seconds, for sending announce messages. Valid values: • 0—1 second • 1—2 seconds • 2— 4 seconds • 3— 8 seconds • 4—16 seconds Default: 1 (2 seconds)

Table 36 - NTP-PTP Clock Mode Fields (Continued)

Field	Description
Sync Interval	Type the time interval, specified as the logarithmic mean in seconds, for sending synchronization messages. Valid values: • -1—half second • 0—1 second • 1— 2 seconds Default: 0 (1 second)
Sync Fault Limit	Type the maximum clock offset before PTP attempts to reacquire synchronization. Valid values: 50…500000000 nanoseconds Default: 50000 nanoseconds **IMPORTANT:** We recommend against setting the sync limit below the default (50000 nanoseconds). Use values below 50000 nanoseconds only in networks with a very high-precision grandmaster clock. These networks have a critical need to keep very sensitive devices synchronized.
Vlan Id	To configure PTP on a VLAN of a trunk port, type the VLAN ID. Only PTP packets in the VLAN you specify are processed. PTP packets from other VLANs are dropped. You can only enable PTP on one VLAN on a trunk port. Valid values: 1…4094 The default is the native VLAN of the trunk port.

Configure Time Synchronization via the Logix Designer Application

To configure time synchronization, follow these steps.

1. In the navigation pane, click Time Sync Configuration.
2. From the Clock Type pull-down menu, choose a mode.

   The available modes vary based on the switch model.
3. To complete the remaining fields, refer to the figure and table that corresponds to your mode.

Mode	Page
Boundary	205
End to End	207
Forward	207
NTP-PTP Clock	208

Figure 7 - Boundary Mode

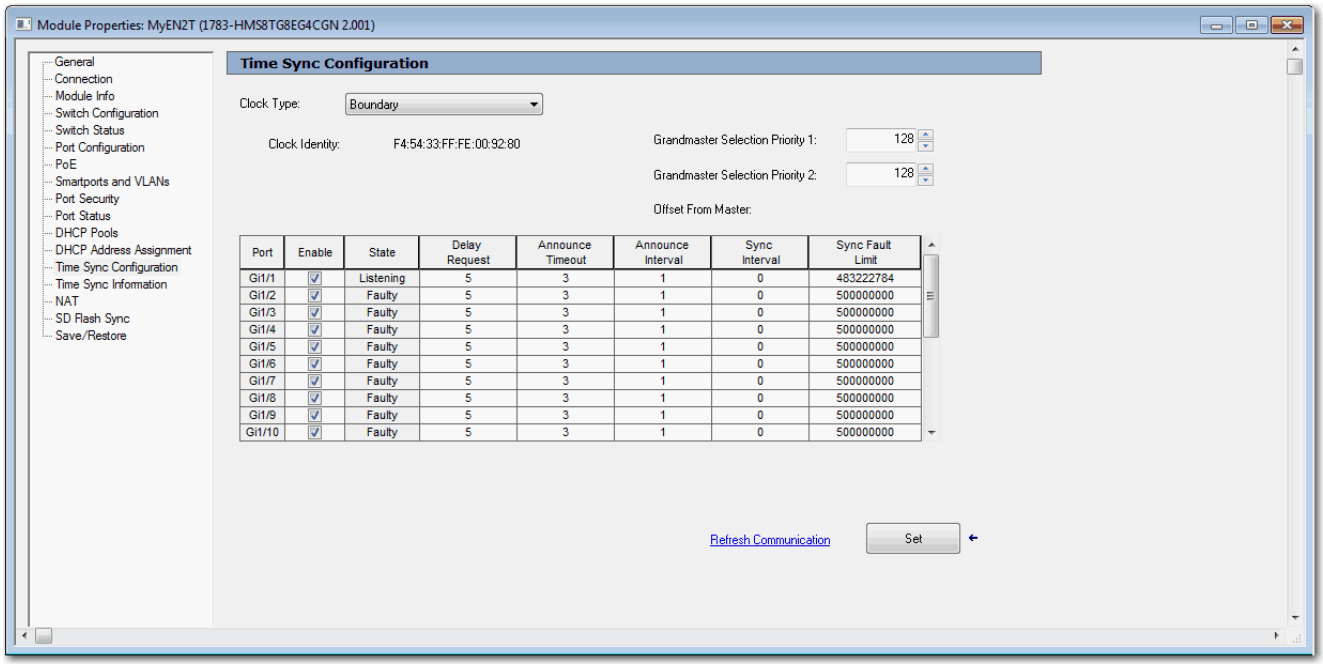


Table 37 - Boundary Mode

Field	Description
Clock Identity	Displays a unique identifier for the clock.
Grandmaster Selection Priority1	Type a value to override the default criteria (clock quality, clock class, and so on) for the best master clock selection. A lower value takes precedence. Valid values: 0…255 Default: 128
Grandmaster Selection Priority 2	Type a value to use as a tie-breaker between two devices that are otherwise equally matched in the default criteria. For example, you can give a specific switch priority over other identical switches. A lower value takes precedence. Valid values: 0…255 Default: 128
Offset from Master	Displays the time offset in nanoseconds between the slave and master clocks.
Port	Displays the port type and port number: • Fa—Fast Ethernet • Gi—Gigabit Ethernet • Te—TenGigabit Ethernet
Enable	Check the checkbox for each port on which to enable PTP. You can enable one or more switch ports. By default, PTP is enabled on all the Fast Ethernet and Gigabit Ethernet ports. For Stratix 8000/8300 switches, only the ports on the base switch module are PTP-capable. The switch expansion modules do not support PTP.
State	Displays the synchronization state of the switch port with the parent or grandmaster clock: • Initializing—The switch port is waiting while a parent or grandmaster clock is selected. • Listening—The switch port is waiting while a parent or grandmaster clock is selected. • Pre-master—The switch port is transitioning to change to Master state. • Master—The switch is acting as a parent clock to the devices connected to that switch port. • Passive—The switch has detected a redundant path to a parent or grandmaster clock. For example, two different switch ports claim the same parent or grandmaster clock. To prevent a loop in the network, one of the ports changes to Passive state. • Uncalibrated—The switch port cannot synchronize with the parent or grandmaster clock. • Slave—The switch port is connected to and synchronizing with the parent or grandmaster clock. • Faulty—Either PTP is not operating properly on the switch port or nothing is connected to the port. • Disabled—PTP is not enabled on the switch port.

Table 37 - Boundary Mode (Continued)

Field	Description
Delay Request	The logarithmic mean interval in seconds. Type the recommended to connected devices to send delay request messages when the switch port is in the master state. Valid values: • -1—half second • 0—1 second • 1—2 seconds • 2—4 seconds • 3—8 seconds • 4—16 seconds • 5—32 seconds • 6—64 seconds Default: 5 (32 seconds)
Announce Timeout	Type the number of announce intervals, specified as the logarithmic mean in seconds, that must pass without receipt of an announce message from the parent or grand master clock before the switch selects a new parent or grand master clock. Valid values: 2…10 Default: 3 (8 seconds)
Announce Interval	Type the time interval, specified as the logarithmic mean in seconds, for sending announce messages. Valid values: • 0—1 second • 1—2 seconds • 2— 4 seconds • 3— 8 seconds • 4—16 seconds Default: 1 (2 seconds)
Sync Interval	Type the time interval, specified as the logarithmic mean in seconds, for sending synchronization messages. Valid values: • -1—half second • 0—1 second • 1— 2 seconds Default: 0 (1 second)
Sync Fault Limit	Type the maximum clock offset before PTP attempts to reacquire synchronization. Valid values: 50…500000000 nanoseconds Default: 50000 nanoseconds **IMPORTANT:** We recommend against setting the sync limit below the default (50000 nanoseconds). Use values below 50000 nanoseconds only in networks with a very high-precision grandmaster clock. These networks have a critical need to keep very sensitive devices synchronized.

Figure 8 - End-to-End Transparent Mode

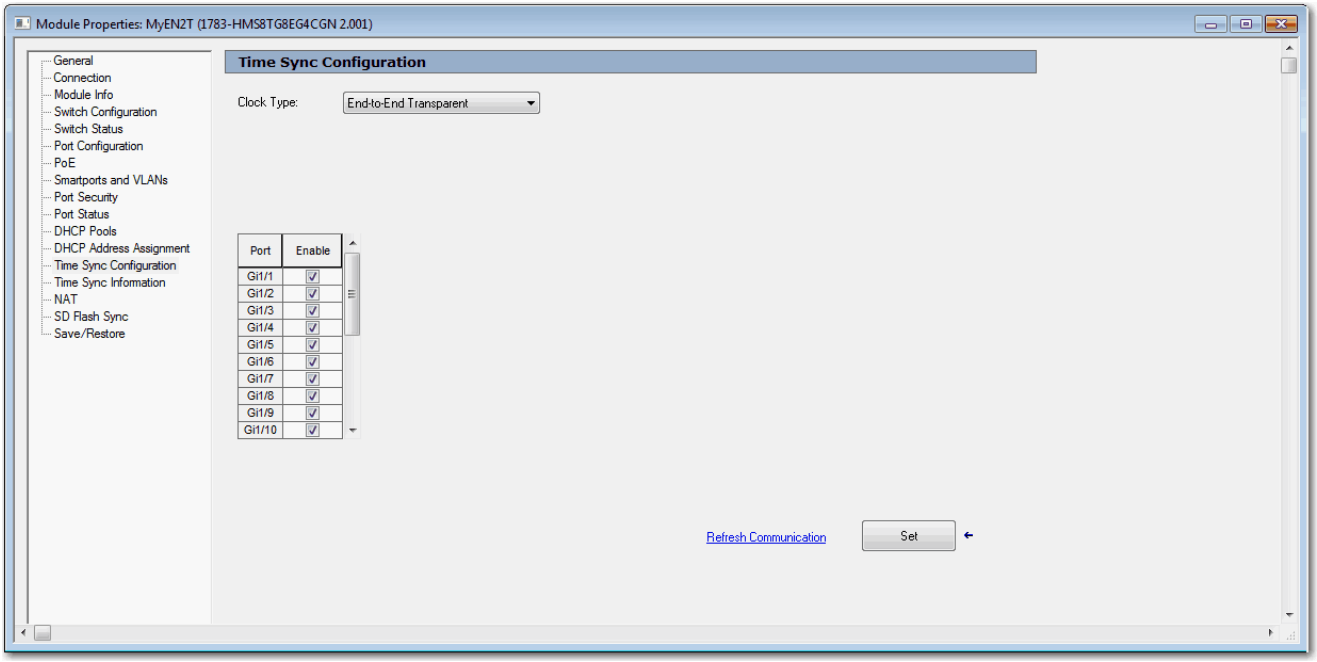


Table 38 - End to End Transparent Mode Fields

Field	Description
Port	Displays the port type and port number: • Fa—Fast Ethernet • Gi—Gigabit Ethernet • Te—TenGigabit Ethernet
Enable	Check the checkbox for each port on which to enable PTP. You can enable one or more switch ports. By default, PTP is enabled on all the Fast Ethernet and Gigabit Ethernet ports. For Stratix 8000/8300 switches, only the ports on the base switch module are PTP-capable. The switch expansion modules do not support PTP. When at least one switch port is PTP-enabled, the End to End Transparent mode is selected by default.

Figure 9 - Forward Mode

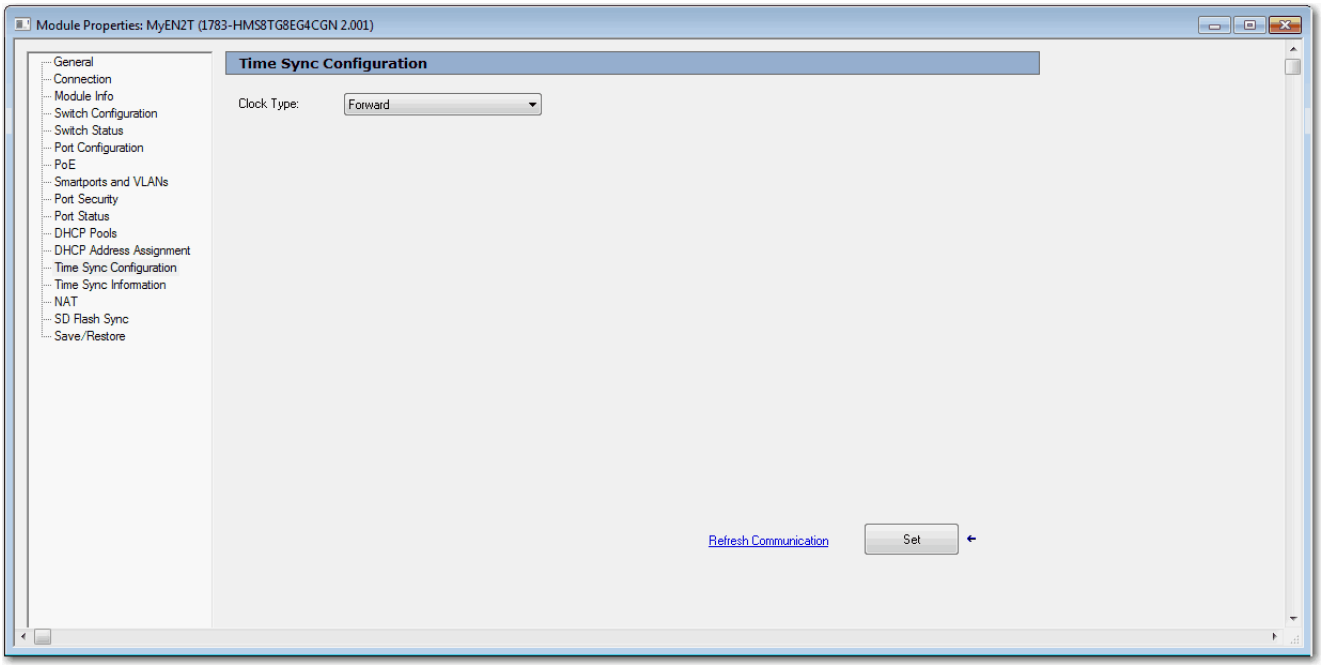


Figure 10 - NTP-PTP Mode

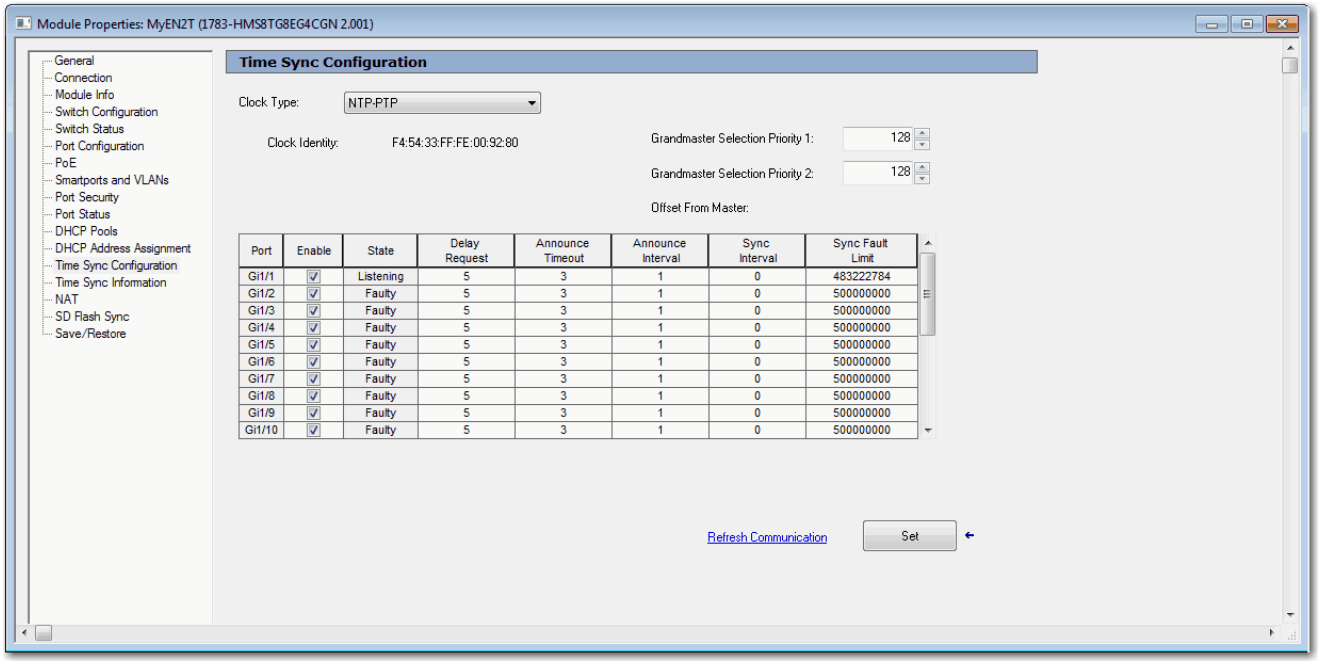


Table 39 - NTP-PTP Mode Fields

Field	Description
Clock Identity	Displays a unique identifier for the clock.
Grandmaster Selection Priority1	Type a value to override the default criteria (clock quality, clock class, and so on) for the best master clock selection. A lower value takes precedence. Valid values: 0…255 Default: 128
Grandmaster Selection Priority 2	Type a value to use as a tie-breaker between two devices that are otherwise equally matched in the default criteria. For example, you can give a specific switch priority over other identical switches. A lower value takes precedence. Valid values: 0…255 Default: 128
Offset from Master	Displays the time offset in nanoseconds between the slave and master clocks.
Port	Displays the port type and port number: • Fa—Fast Ethernet • Gi—Gigabit Ethernet • Te—TenGigabit Ethernet
Enable	Check the checkbox for each port on which to enable PTP. You can enable one or more switch ports. By default, PTP is enabled on all the Fast Ethernet and Gigabit Ethernet ports. For Stratix 8000/8300 switches, only the ports on the base switch module are PTP-capable. The switch expansion modules do not support PTP.
State	Displays the synchronization state on the switch port with the parent or grandmaster clock: • Initializing—The switch port is waiting while a parent or grandmaster clock is selected. • Listening—The switch port is waiting while a parent or grandmaster clock is selected. • Pre-master—The switch port is transitioning to change to Master state. • Master—The switch is acting as a parent clock to the devices connected to that switch port. • Passive—The switch has detected a redundant path to a parent or grandmaster clock. For example, two different switch ports claim the same parent or grandmaster clock. To prevent a loop in the network, one of the ports changes to Passive state. • Uncalibrated—The switch port cannot synchronize with the parent or grandmaster clock. • Slave—The switch port is connected to and synchronizing with the parent or grandmaster clock. • Faulty—Either PTP is not operating properly on that switch port or nothing is connected to the port. • Disabled—PTP is not enabled on the switch port.

Table 39 - NTP-PTP Mode Fields (Continued)

Field	Description
Delay Request Interval	Type the recommended to connected devices to send delay request messages when the switch port is in the master state. Valid values: • -1—half second • 0—1 second • 1—2 seconds • 2—4 seconds • 3—8 seconds • 4—16 seconds • 5—32 seconds • 6—64 seconds Default: 5 (32 seconds)
Announce Timeout	Type the number of announce intervals, specified as the logarithmic mean in seconds, that must pass without receipt of an announce message from the parent or grand master clock before the switch selects a new parent or grand master clock. Valid values: 2…10 Default: 3 (8 seconds)
Announce Interval	Type the time interval, specified as the logarithmic mean in seconds, for sending announce messages. Valid values: • 0—1 second • 1—2 seconds • 2— 4 seconds • 3— 8 seconds • 4—16 seconds Default: 1 (2 seconds)
Sync Interval	Type the time interval, specified as the logarithmic mean in seconds, for sending synchronization messages. Valid values: • -1—half second • 0—1 second • 1— 2 seconds Default: 0 (1 second)
Sync Fault Limit	Type the maximum clock offset before PTP attempts to reacquire synchronization. Valid values: 50…500000000 nanoseconds Default: 50000 nanoseconds **IMPORTANT:** We recommend against setting the sync limit below the default (50000 nanoseconds). Use values below 50000 nanoseconds only in networks with a very high-precision grandmaster clock. These networks have a critical need to keep very sensitive devices synchronized.

View Time Sync Information in the Logix Designer Application

In the navigation pane, click Time Sync Information.

The Time Sync Information view shows current information about the real-time clocks in the network. The CIP Time Synchronization protocol provides a standard mechanism to synchronize clocks across a network of distributed devices.

The CIP Sync Time Synchronization feature supports both Boundary and End-to-End Transparent mode. End to End Transparent mode synchronizes all switch ports with the grandmaster clock using the IEEE 1588 V 2 End to End Transparent clock mechanism, and is the preferred mode.

Figure 11 - Time Sync Information

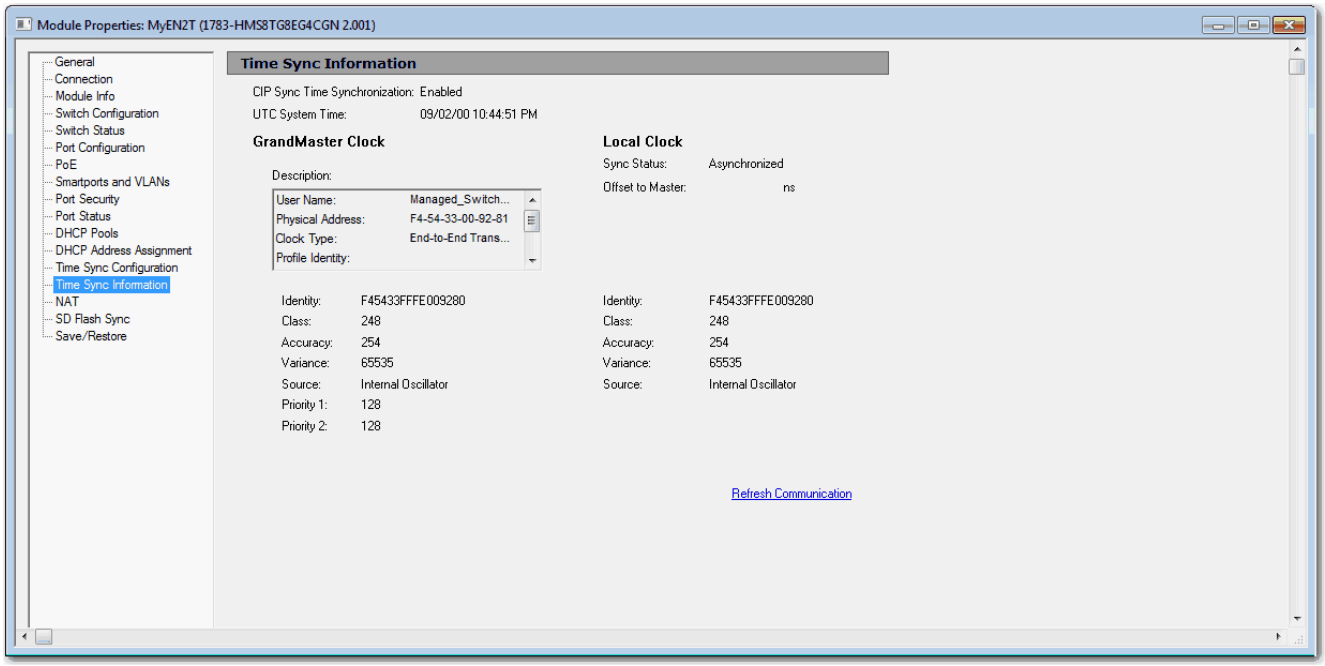


Table 40 - Time Sync Information Fields

Field	Description
CIP Sync Time Synchronization	Displays whether the Precision Time Protocol is enabled or disabled on the device.
UTC System Time	Displays the current system time in units of microseconds.
Grandmaster Clock	
Description	Displays information to identify the grandmaster clock, including the configured the clock type.
Identity	Displays the unique identifier for the grandmaster clock. The format depends on the network protocol.
Class	Displays a measure of the quality of the grandmaster clock. Values are defined from 0…255 with 0 as the best clock.
Accuracy	Indicates the expected absolute accuracy of the Grandmaster clock relative to CIP Sync time synchronization epoch (31 December, 1969 23:59:51.99918 UTC). The accuracy is specified as a graduated scale starting at 25 ns and ending at greater than 10 seconds or unknown. For example, a GPS time source has an accuracy of approximately 250 ns. A hand-set clock typically has an accuracy less than 10 seconds. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the grandmaster clock. The value is in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the clock time source: • Atomic Clock • GPS • Terrestrial Radio • CIP Time Synchronization • NTP • HAND Set • Other • Internal Oscillator
Priority 1 Priority 2	Displays the relative priority of the grandmaster clock to other clocks in the system. The value is between 0…255. The highest priority is 0.
Local Clock	
Sync Status	Displays whether the local clock is synchronized or asynchronized with the grandmaster clock.
Offset to Master	Displays the offset value between the local clock and the master clock.
Identity	Displays the unique identifier for the local clock. The format depends on the network protocol. • The Ethernet protocol encodes the MAC address into the identifier. • The DeviceNet and ControlNet protocols encode the Vendor ID and serial number into the identifier.

Table 40 - Time Sync Information Fields (Continued)

Field	Description
Class	Displays a measure of the quality of the local clock. Values are defined from 0 . . . 255 with 0 as the best clock.
Accuracy	Indicates the expected absolute accuracy of the local clock relative to CIP Sync time synchronization epoch (31 December, 1969 23:59:51.99918 UTC). The accuracy is specified as a graduated scale starting at 25 ns and ending at greater than 10 seconds or unknown. For example, a GPS time source has an accuracy of approximately 250 ns. A hand-set clock typically has an accuracy less than 10 seconds. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the local clock. The value is in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the clock time source: • Atomic Clock • GPS • Terrestrial Radio • CIP Time Synchronization • NTP • HAND Set • Other • Internal Oscillator

Cryptographic IOS

With IOS version 15.2(5)EA.fc4 and later, the default firmware that ships from manufacturing is the cryptographic IOS. The cryptographic IOS provides increased network security by encrypting administrator traffic during SNMP sessions. The cryptographic IOS supports all features of the standard IOS and these protocols:

- Secure Shell (SSH) Protocol v2
- SNMPv3
- HTTPS

With the cryptographic IOS, HTTPS is the default protocol for accessing Device Manager. For instructions on accessing Device Manager via secure connection, see Access Device Manager on page 48.

Non-cryptographic IOS software is available to download from the Product Compatibility and Download Center on http://www.ab.com.

If you upgrade an existing configuration from IOS 15.2(4)EA3 or earlier to IOS 15.2(5)EA.fc4 or later, the default switch settings are as follows:

- If you upgrade the switch to the cryptographic IOS, Telnet remains enabled, SSH remains disabled, but HTTPS becomes the default protocol for Device Manager.
- If you upgrade the switch to the non-cryptographic IOS, Telnet remains enabled, SSH remains disabled, and HTTP remains the default protocol for Device Manager.

Device-level Ring (DLR)

DLR is available on Stratix 5400 switches and some models of Stratix 5700 and ArmorStratix 5700 switches. For a list of switches that support DLR, see page 21.

This section covers the following topics:

- Overview
- DLR Port Choices
- DLR Considerations
- Redundant Gateways
- DHCP for Ring Devices
- Multiple Rings
- Configure DLR via Device Manager
- Configure DLR via the Logix Designer Application

Overview

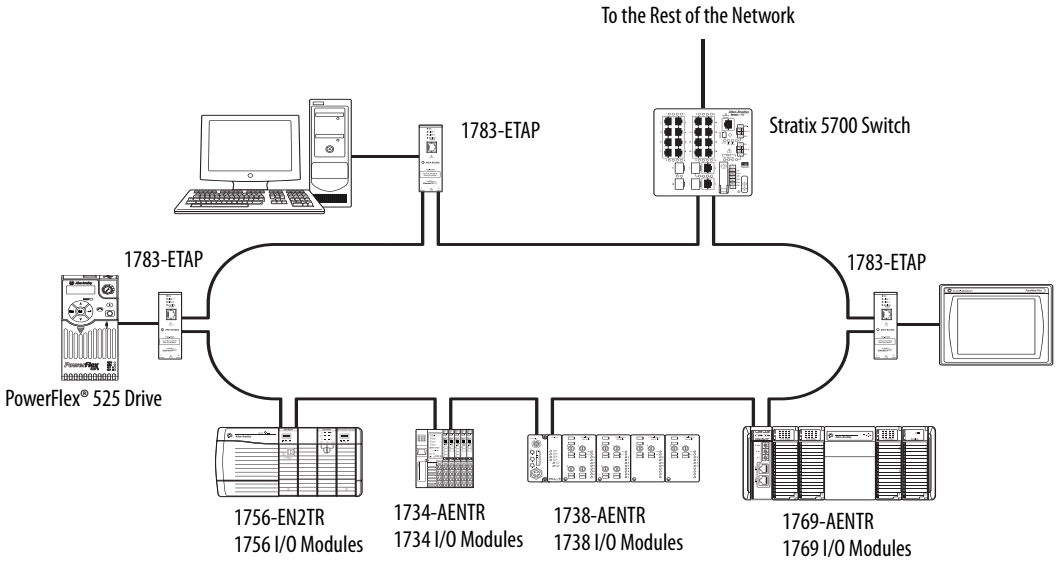
A DLR network is a single-fault-tolerant ring network that is intended for the interconnection of automation devices without the need for more switches. The ring topology offers these advantages:

- Media redundancy
- Fast-network fault detection and reconfiguration
- Resiliency of a single-fault-tolerant network
- Easy implementation without more hardware requirements

IMPORTANT This section summarizes a DLR network. To plan, configure, and monitor DLR networks, see EtherNet/IP Embedded Switch Technology Application Guide, publication ENET-AP005.

One DLR network can support as many as 50 nodes. A DLR network supports copper connections (maximum of 100 m), fiber-optic connections (maximum of 2 km), or a mix of copper and fiber.

Figure 12 - Example Device-level Ring Topology



IMPORTANT Stratix 5700 and ArmorStratix 5700 switches support only one ring per switch.

Stratix 5400 switches support as many as three rings per switch.

Figure 13 - A DLR network includes the following nodes.

Node	Description
Supervisor node	A DLR network requires at least one node to be configured as ring supervisor. **IMPORTANT:** By default, the supervisor function is disabled on supervisor-capable devices, so they are ready to participate in a linear network or as a ring node on a DLR network. In a DLR network, you must configure at least one of the supervisor-capable devices as the ring supervisor before physically connecting the ring. If you do not, the DLR network does not work. The ring supervisor provides these main functions: • Manages traffic on the DLR network • Collects diagnostic information for the network We recommend that you do the following: • Configure at least one back-up supervisor. • Configure the desired active ring supervisor with a numerically higher precedence value as compared to the back-up supervisors. • Track the supervisor-precedence values for all supervisor-enabled nodes in the DLR network.
Ring node	A ring node is any node that operates on the network to process data that is transmitted over the network. A ring node can also pass on the data to the next node on the network. When a fault occurs on the DLR network, the ring nodes reconfigure themselves and relearn the network topology. Additionally, ring nodes can report fault locations to the active ring supervisor.

DLR Port Choices

Table 41 and Table 42 show which ports you can configure for DLR:

- Stratix 5700 and ArmorStratix 5700 switches support one ring and two DLR-enabled ports per switch.
- Stratix 5400 switches support as many as three rings and six DLR-enabled ports per switch.

We recommend that you use the Multiport Automation Device Smartport role on ports you configure for DLR.

Table 41 - DLR Port Choices for Stratix 5400 Switches

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

Table 42 - DLR Port Choices for Stratix 5700 and ArmorStratix 5700 Switches

Switch	Port							
1783-BMS10CGP	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2				
1783-BMS10CGN	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2				
1783-BMS12T4E2CGL	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2				
1783-BMS12T4E2CGP	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2				
1783-BMS12T4E2CGNK	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2				
1783-BMS20CL	Fa 1/15	Fa 1/16			Fa 1/17	Fa 1/18	Fa 1/19	Fa 1/20
1783-BMS20CA	Fa 1/15	Fa 1/16			Fa 1/17	Fa 1/18	Fa 1/19	Fa 1/20
1783-BMS20CGL	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2	Fa 1/17	Fa 1/18		
1783-BMS20CGP	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2	Fa 1/17	Fa 1/18		
1783-BMS20CGN	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2	Fa 1/17	Fa 1/18		
1783-BMS20CGPK	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2	Fa 1/17	Fa 1/18		
1783-ZMS4T4E2TGP	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2				
1783-ZMS8T8E2TGP	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2				
1783-ZMS4T4E2TGN	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2				
1783-ZMS8E82TGN	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2				

DLR Considerations

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

Some switch capabilities are not supported on DLR-enabled ports. Unsupported capabilities include, but are not limited to, the following:

- EtherChannels
- NAT
- REP
- MST/PVST/RPVST
- FlexLinks
- 802.1x Security
- Multiple VLANs
- Smartport roles, except for Multiport Automation Device or None

DLR ports function only as access ports and not trunk ports.

Redundant Gateways

IMPORTANT Redundant gateways do not work with End to End Transparent mode for Precision Time Protocol. For more information about End to End Transparent mode, see page 195.

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

Typically, the redundant gateway feature is configured on trunk ports independent of the DLR configuration of the access ports.

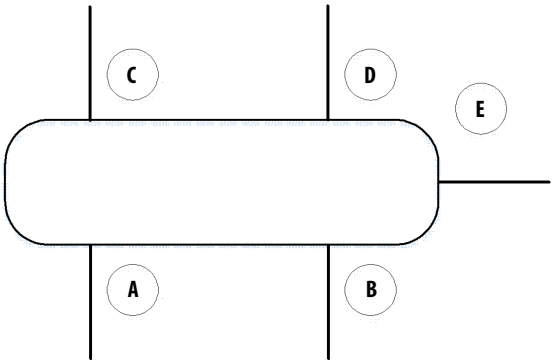
IMPORTANT The redundant gateway feature requires all devices on the ring to be compatible with redundant gateway. Connections to devices wired to or through a DLR network can be lost upon a gateway changeover if all DLR network devices are not compatible with redundant gateway.

For more information about redundant gateway compatibility, see answer ID 731689 in the Technical Support Center:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/731689

Figure 14 shows an example of a switch configured for redundant gateway. All ports are assigned to VLAN 1.

Figure 14 - Redundant Gateway Switch Ports



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

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

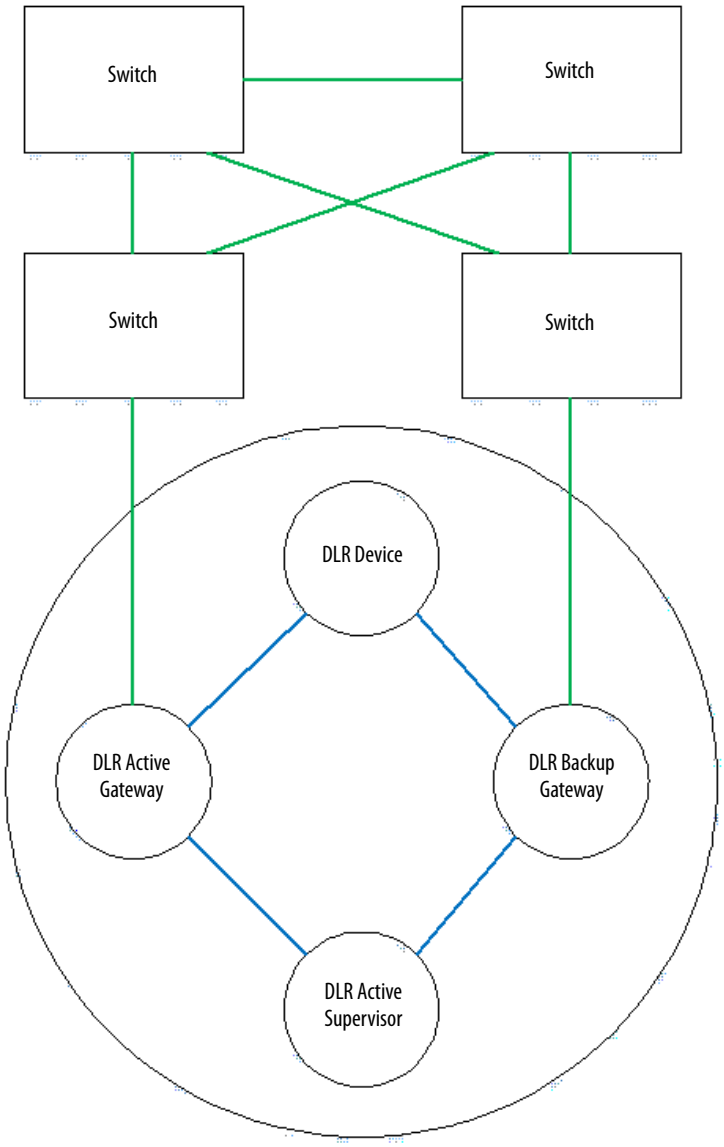
When the switch acts a **backup** redundant gateway, traffic on the switch that is assigned to VLAN 1 can flow as follows:

- Between only Ports A and B
- Between only Ports C, D, and E
- To join the ring, traffic on Ports C, D, and E must flow through the non-DLR port, through devices connected to the backup redundant gateway, and then through the active redundant gateway (see Figure 15).

  IMPORTANT Traffic flow restrictions from the backup gateway to the ring include CIP and Device Manager traffic. As a result, all traffic flowing from a ring device to the backup gateway must use this path:
  - Exit the ring through the active gateway
  - Flow through the outside network above the ring
  - Enter the backup gateway through the uplink port.

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

Figure 15 - Traffic from Backup Gateway to Ring



You can configure redundant gateways on switches that are either ring supervisors or ring nodes.

Figure 16 shows two Stratix 5700 switches that are configured as ring supervisors with redundant gateway:

- One switch is configured as the active ring supervisor and also the active redundant gateway.
- The other switch is configured as a backup ring supervisor and the backup redundant gateway.

In this example, the switch acts as a ring supervisor. The switch also manages redundant gateway switchovers.

Figure 16 - Ring Supervisor with Redundant Gateway

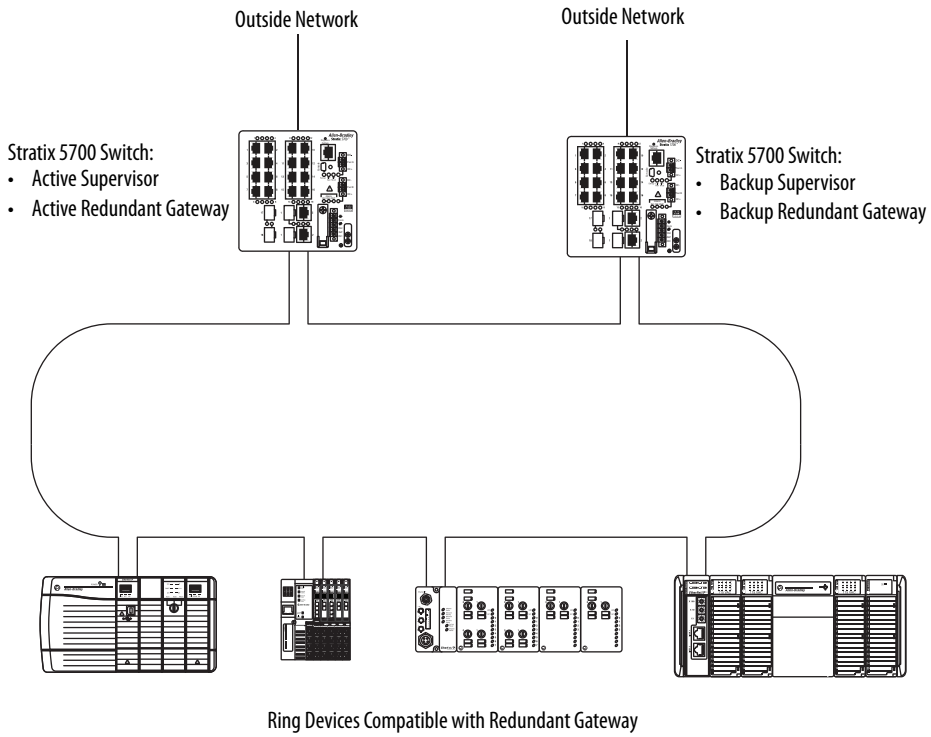
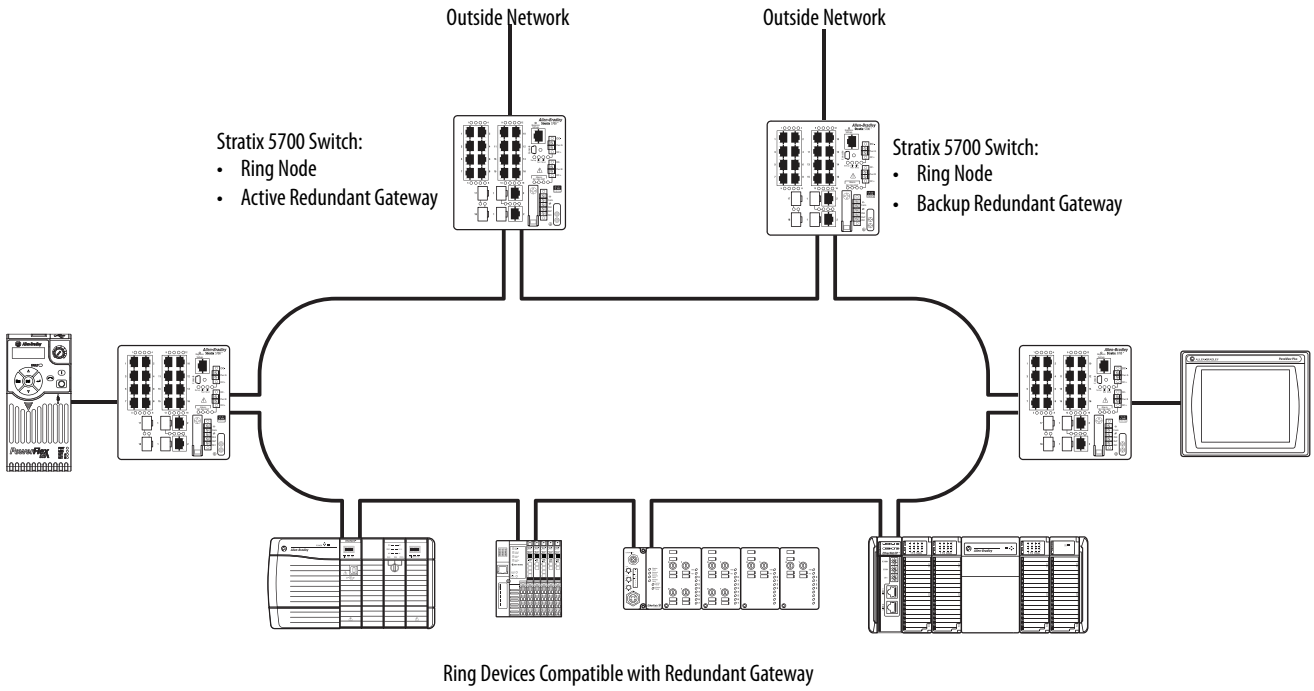


Figure 17 shows two Stratix 5700 switches that are configured as ring nodes with redundant gateway:

- One switch is a ring node and the active redundant gateway.
- The other switch is a ring node and the backup redundant gateway.

In this example, the switch provides redundant gateway functionality, so that all ring nodes have access to the outside network.

Figure 17 - Ring Node with Redundant Gateway



DHCP for Ring Devices

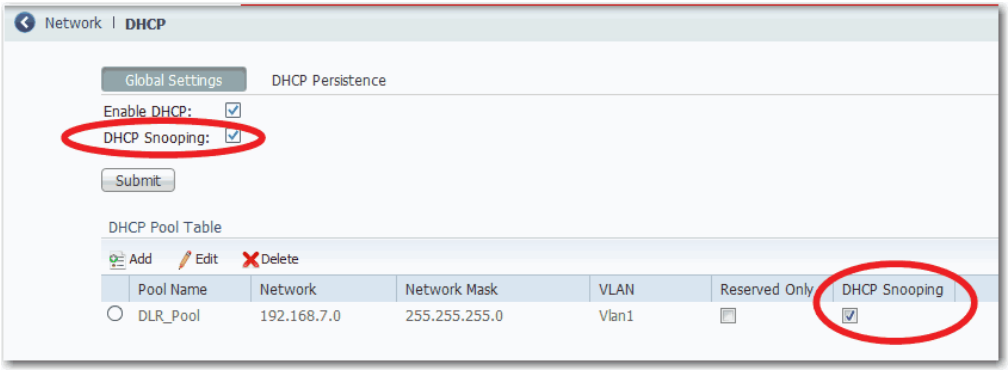
IMPORTANT DHCP for ring devices does not work with DHCP peristence, as described on page 241. Configure only one of these features on your switch.

You can configure DHCP to assign IP addresses to devices connected to a ring based on their positions in the ring. This feature makes sure that a replaced device receives the expected IP address:

- A ring supervisor functions as the active ring DHCP server to assign IP addresses to the participating nodes through two DLR ports.
- If enabled, a backup ring DHCP server runs on the backup ring supervisor and obtains its reference table automatically from the active ring DHCP server on the active ring supervisor. There can be multiple backup ring DHCP servers in the ring.
- If the active ring DHCP server in the ring fails, the backup ring supervisor becomes the active supervisor. The backup ring DHCP server on the backup ring supervisor becomes the active ring DHCP server and takes over IP assignment and renewal for the ring until one of the following happens:
  - The original active ring DHCP server is restored.
  - A new active ring DHCP server is manually configured.

IMPORTANT To enable a ring to assign correct addresses by using DHCP, you must check both DHCP Snooping checkboxes on the DHCP page, as shown in Figure 18.

Figure 18 - DHCP Snooping Checkboxes



DHCP snooping for a ring can be enabled or disabled. By default, DHCP snooping for a ring is enabled:

- When enabled, DHCP snooping prevents DHCP address assignments from going beyond an active ring DCHP server and the devices within the ring. DHCP requests from another server cannot enter the ring, and DHCP requests from the active ring DCHP server cannot leave the ring.
- When disabled, DHCP snooping lets the active ring DHCP server forward DHCP requests outside of the ring. However, DHCP requests passed around the ring from a ring device are never passed to devices connected to the backup DHCP server. The requests are treated as ring traffic and stay in the ring.

Figure 19 on page 224 shows two Stratix 5700 switches that are configured for DHCP in a ring:

- Ring device 1 is the active ring supervisor and ring DHCP server.
- Ring device 2 is the backup ring supervisor and ring DHCP server.
- Ring devices 2 and 5 have statically-assigned IP addresses and appear as blank entries in DHCP table (Table 43).
- Ring devices 3 and 6 are configured to receive IP addresses from BOOTP.
- Ring device 4 is configured to receive IP addresses from DHCP.

In this example, the active ring DHCP server recognizes IP address requests from ring devices 3, 4, and 6 and responds with the position-based IP address specified in the DHCP table (Table 43). The ring device index numbers in the DCHP table begin incrementing in order from the device connected to the lowest DLR port. For example, in Figure 19, the DLR ports are Gi1/1 and Gi1/2. The lowest DLR port is Gi1/1, so the device connected to Gi1/1 has an index number of 2.

Figure 19 - DHCP for Ring Devices

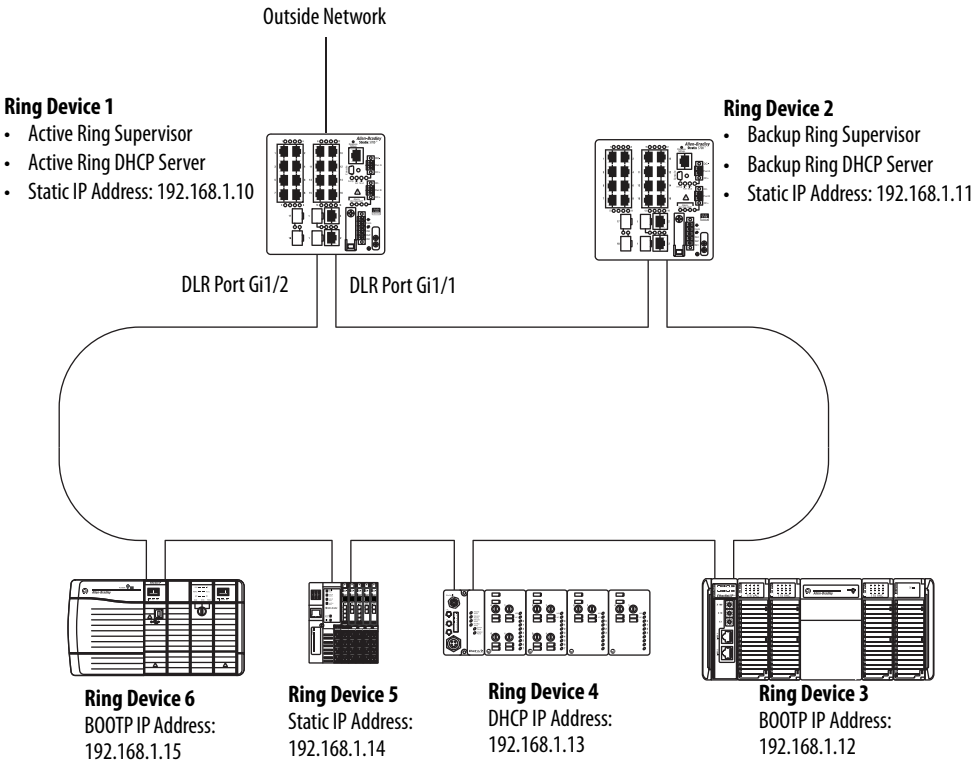


Table 43 - Example DHCP Table for Ring Devices

Ring Device Index(1)	IP Address	Host Name	DHCP Pool
2			
3	192.168.1.12	Rack 2	Pool 1
4	192.168.1.13	Rack 3	Pool 1
5			
6	192.168.1.15	Rack 5	Pool 1

(1) Index 1 represents the active ring DHCP server and is not configurable.

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

You can configure DHCP for ring devices on the Config DHCP tab in Device Manager, as shown on page 228. Before you configure DHCP for ring devices, you must enable DHCP and configure an IP address pool to use for the ring devices, as described on page 238.

Once you configure DHCP for ring devices, the changes take effect when the ring converges after the loss of a network connection. However, if you assign a new IP address to a device currently in use, the new IP address does not take effect until the device's current address lease expires or until the device restarts.

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

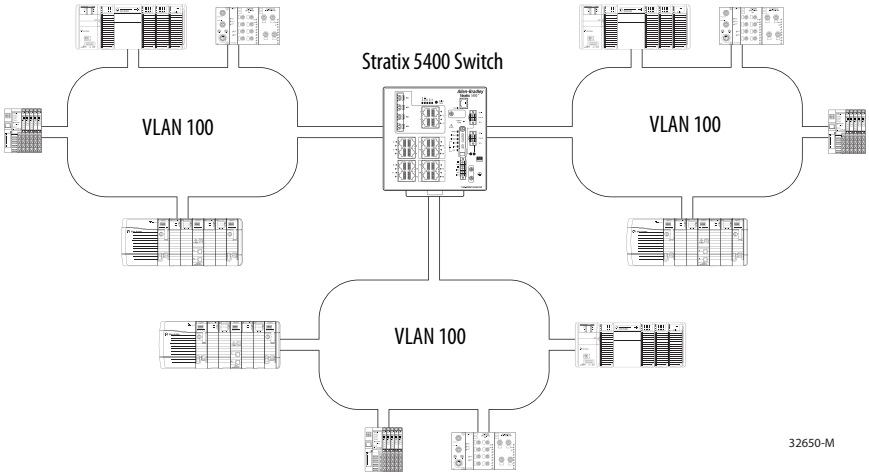
Multiple Rings

Stratix 5400 switches support as many as three device-level rings with these configuration rules:

- Ring ports function only as access ports.
- Multiple rings cannot share the same ring ports. Valid ring ports are defined in Table 41 on page 215.
- All ring ports within the same ring or belonging to different rings must be assigned to the same access VLAN.
- The same Stratix 5400 switch must serve as the active gateway for all rings.
- The same Stratix 5400 switch must serve as the backup gateway for all rings.

Figure 20 shows an example of a Stratix 5400 switch configured for three rings.

Figure 20 - Stratix 5400 Switch with Multiple Rings



Configure DLR via Device Manager

IMPORTANT Be sure to configure DLR on the switch prior to connecting ring ports. Connecting both ring ports on a switch that has not yet been configured for DLR can result in undesired behavior and limit the ability to configure the switch.

From the Configure menu, choose DLR:

- To configure the switch as a ring node or a ring supervisor, complete the fields on the Config DLR tab, as described in Table 44 on page 227.
- To configure DHCP for ring devices, complete the fields on the Configure DHCP tab, as described in Table 45 on page 228.

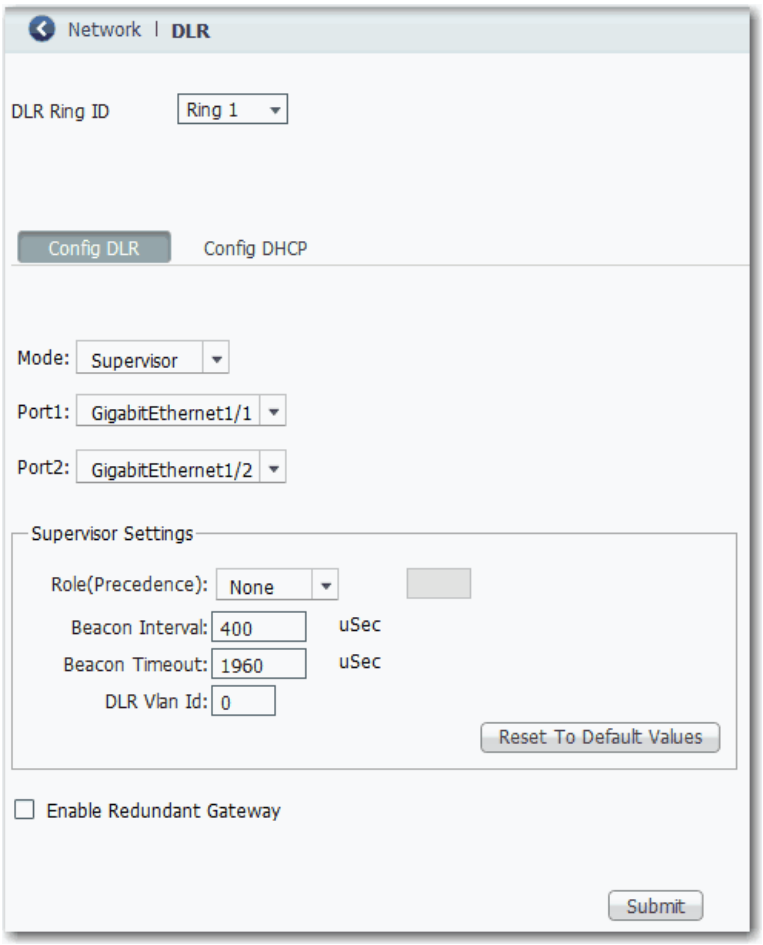


Table 44 - Config DLR Fields

Field	Description
DLR Ring ID	(Stratix 5400 switches). Choose the ring number to configure: • Ring 1 • Ring 2 • Ring 3
Mode	Choose one of these modes: • Disabled—The DLR feature is disabled on the switch. • Node—The switch is a ring node. • Supervisor—The switch is a ring supervisor. Default: Disabled
Port1	Choose a ring port. By default, if the switch is the ring supervisor, port 1 is node 1 on the ring, and port 2 is blocked.
Port2	Choose a ring port.
Supervisor Settings	
Role (Precedence)	Choose a role to assign to the ring supervisor that corresponds to a predefined precedence value. The switch transmits the precedence value in beacon frames and uses it to determine the active ring supervisor when multiple supervisors are configured. A higher value means higher precedence. When two DLR supervisors have the same precedence, the device with the numerically highest MAC address becomes the active supervisor. Valid values: • None—0 • Primary—255 • Backup 1—100 • Backup 2—90 • Backup 3—80 • Custom—Type a value from 0…255
Beacon Interval	Type an interval for the supervisor to transmit beacon frames. Valid values: 200…100,000 µs Default: 400 µs.
Beacon Timeout	Type the amount of time ring nodes wait before timing out in the absence of received beacon messages. Valid values: 200…500,000 µs Default: 1960 µs
DLR Vlan Id	Type the VLAN ID for sending DLR protocol management frames. Valid values: 0…4095 Default: 0 (no VLAN ID is used) **IMPORTANT:** DLR ports function only as access ports and not trunk ports.
Redundant Gateway Settings	
Enable Redundant Gateway	Check the checkbox to enable the configuration of redundant gateways. The configuration fields are available only after you enable the feature. Default: Disabled
Role (Precedence)	Choose a role to assign to the redundant gateway that corresponds to a predefined precedence value. The switch transmits the precedence value is advertise messages and is used to select the redundant gateway when multiple redundant gateways are configured. A higher value means higher precedence. When two DLR redundant gateways have the same precedence, the device with the numerically highest MAC address will become the redundant gateway. Valid values: • None—0 • Primary—255 • Backup 1—100 • Backup 2—90 • Backup 3—80 • Custom—Type a value from 0…255
Advertise Interval	Type the time interval for the gateway to transmit advertise messages. Valid values: 200…100,000 µs Default: 2000 µs

Table 44 - Config DLR Fields (Continued)

Field	Description
Advertise Timeout	Type the duration of time for nodes to wait before timing out in the absence of received advertise messages. Valid values: 200…500,000 µs Default: 5000 µs
Learning Update	Check the checkbox to enable learning update messages. Default: Enabled
Uplink Ports	Check the checkbox for each uplink port on which to enable redundant gateway.

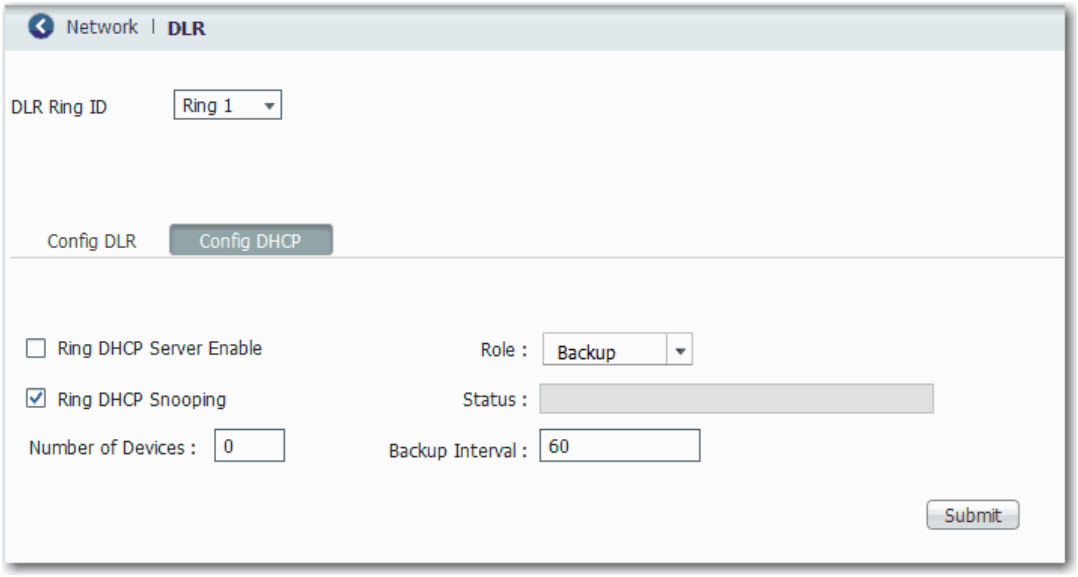


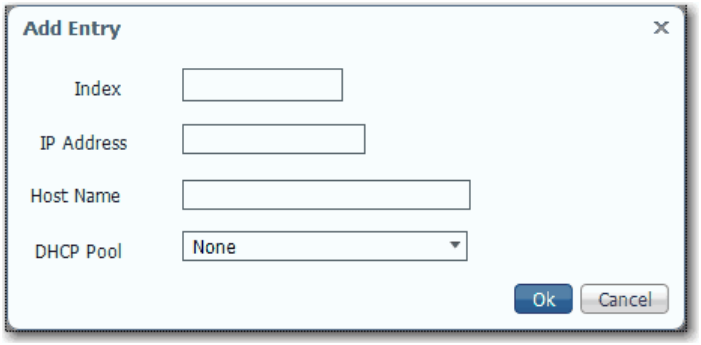
Table 45 - Config DHCP Fields

Field	Description
Ring DHCP Server Enable	Check the checkbox to enable the ring DHCP server on the DLR supervisor device.
Role	Choose a role to assign to the ring DHCP server. Valid values: • None—The server is inactive. • Primary—The DLR supervisor functions as the active ring DHCP server. • Backup—The DLR supervisor functions as the backup ring DHCP server.
Ring DHCP Snooping	Check the checkbox to restrict the broadcast of DHCP requests from going beyond the ring. Only devices in the ring receive address assignments from the DHCP server. DHCP snooping is enabled by default. If you are not using DLR DHCP, you must disable Ring DHCP Snooping to use DHCP server functionality outside of the ring.
Status	Displays the status of the ring. Valid values: • Normal • Ring Fault • Unexpected Loop Detected • Partial Network Fault • Rapid Fault/Restore Cycle
Number of Devices	Type the number of devices in the ring, including switches.
Backup Interval	Type the interval in seconds at which the backup ring DHCP server reads the reference table of the active ring DHCP server. Valid values: 1…65535 seconds Default: 60

Assign IP Addresses to Ring Devices

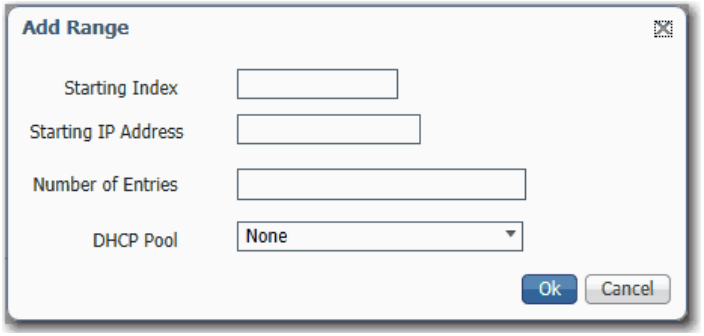
Use the table on the Config DHCP tab to assign IP addresses to devices based on their position in the ring.

To add IP addresses individually, click Add Entry.



Field	Description
Index	Type a value that indicates the location of the ring device. Valid values: 2 . . .255
IP Address	Type the IP address for the entry.
Host Name	Type a host name to associate with the IP address for the entry.
DHCP Pool	Choose the name of the IP address pool to use for ring devices. This pool must be previously configured, as described on page 238. DHCP persistance and DHCP for ring devices can coexist, but cannot share the same pool.

To specify a range of IP addresses, click Add Range.



Field	Description
Starting Index	Type a value that indicates the starting location of the ring devices in the range. Valid values: 2 . . .255
Starting IP Address	Type the starting IP address for the range of entries.
Number of Entries	Type the number of entries in the range.
DHCP Pool	Choose the name of the IP address pool to use for ring devices. This pool must be previously configured, as described on page 238. DHCP persistance and DHCP for ring devices can coexist, but cannot share the same pool.

Configure DLR via the Logix Designer Application

Configuration parameters appear for the number of available rings:

- Stratix 5700 and ArmorStratix 5700 switches show one ring.
- Stratix 5400 switches show three rings.

Configure each ring:

- To enable DLR on specified ring ports and to view information about the DLR network, click Device Level Ring (DLR), and then complete the fields as described in Table 46 on page 231.
- To configure a ring network, expand Device Level Ring (DLR), click Ring 1, Ring 2, or Ring 3, and then complete the fields, as described in Table 47 on page 232.
- To configure redundant gateways, expand Device Level Ring (DLR), expand Ring 1, Ring 2, or Ring 3, click Redundant Gateway Configuration, and then complete the fields, as described in Table 49 on page 234.
- To configure DHCP for ring devices, expand Device Level Ring (DLR), expand Ring 1, Ring 2, or Ring 3, click DHCP, and then complete the fields, as described in Table 50 on page 235.

To view the status and parameters that are configured for a ring, or to view the MAC and IP addresses of each device in the ring, see Monitor DLR Status via the Logix Designer Application on page 408.

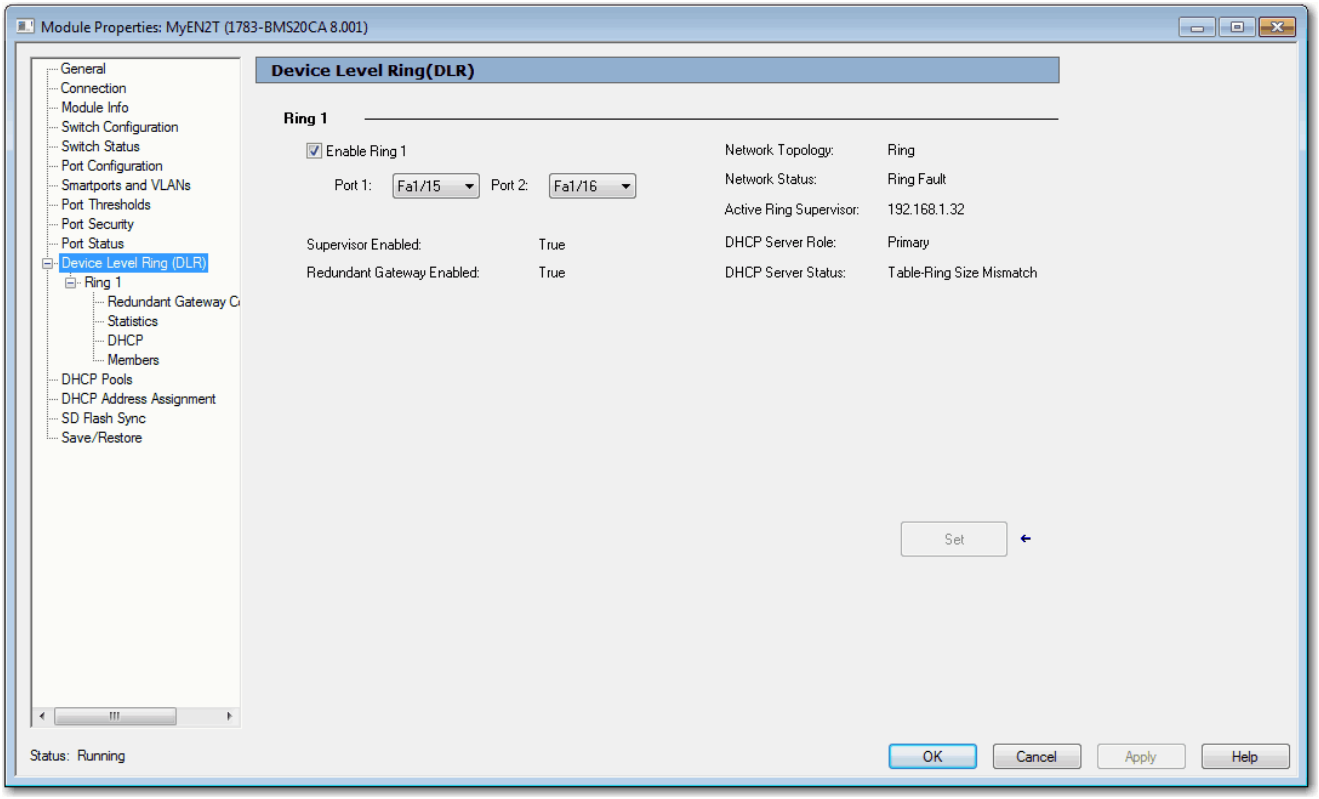


Table 46 - Device Level Ring (DLR) Fields

Field	Description
Enable Ring 1/Enable Ring 2/Enable Ring 3	Check to enable DLR on the ports that are specified in the associated Port 1 and Port 2 fields for the ring.
Port 1	Choose a ring port. The default value is None. This field is unavailable if the Enable Ring 1 checkbox is cleared.
Port 2	Choose a ring port. Port 1 and Port 2 cannot be the same port. The default value is None. This field is unavailable if the Enable Ring 1 checkbox is cleared.
Supervisor Enabled	Displays whether the switch is a ring supervisor. Valid values: • True— The switch is a ring supervisor. • False—The switch is a ring node.
Redundant Gateway Enabled	Displays whether redundant gateways are enabled for the ring.
Network Topology	Displays whether the switch is operating in a DLR or linear network. Valid values: • Ring • Linear
Network Status	Displays the status of the network. Valid values: • Normal • Ring Fault • Unexpected Loop Detected • Partial Network Fault • Rapid Fault/Restore Cycle

Table 46 - Device Level Ring (DLR) Fields (Continued)

Field	Description
Active Ring Supervisor	Displays the IP address of the active ring supervisor.
DCHP Server Role	Displays the role of the ring DHCP server. Valid values: • Disabled • Primary • Secondary • Backup
DHCP Server Status	Displays the status of the DHCP server. Valid values: • Normal operation • Table-ring size mismatch • Table-ring order mismatch • IP address conflict

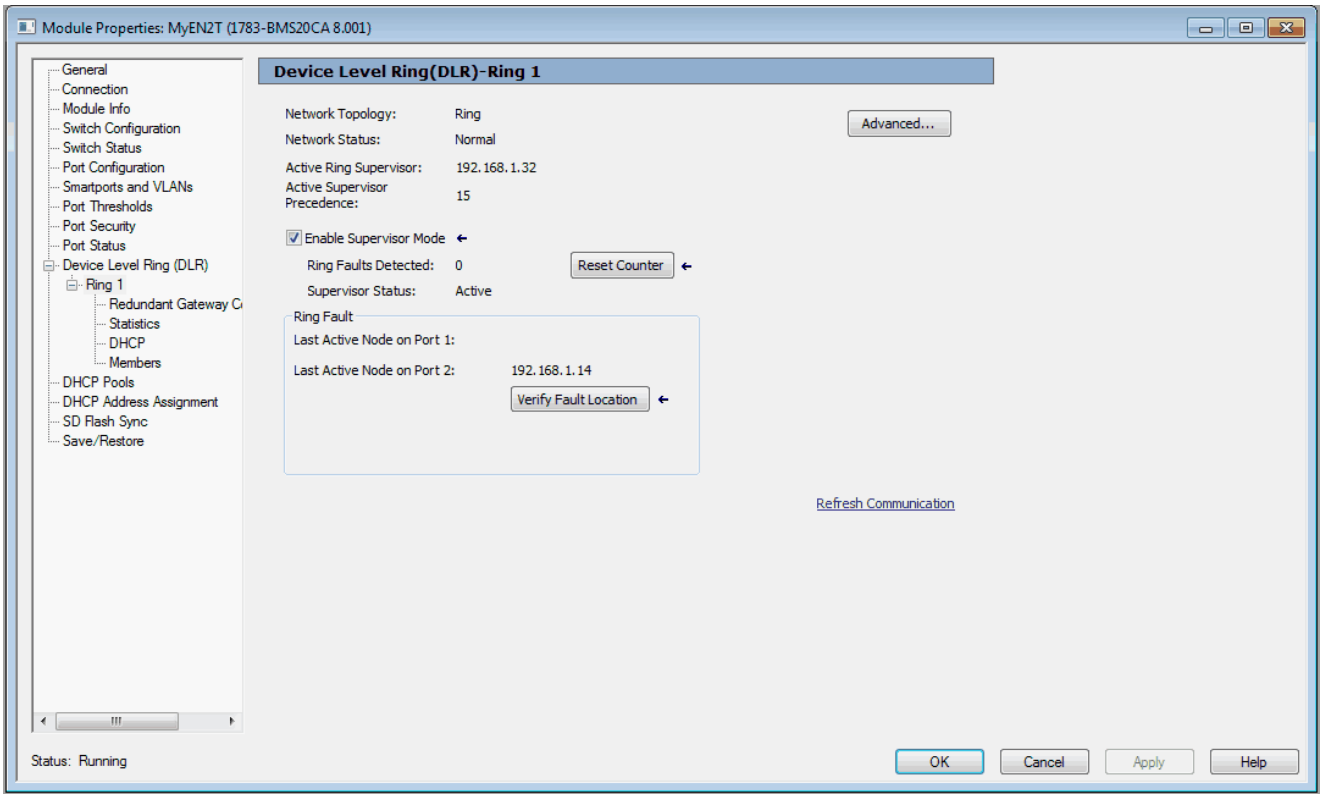


Table 47 - Ring 1/Ring 2/Ring 3 Fields

Field	Description
Network Topology	Displays whether the switch is operating in a DLR or linear network. Valid values: • Ring • Linear
Network Status	Displays the status of the network. Valid values: • Normal • Ring Fault • Unexpected Loop Detected • Partial Network Fault • Rapid Fault/Restore Cycle
Active Ring Supervisor	Displays the IP address of the active ring supervisor.

Table 47 - Ring 1/Ring 2/Ring 3 Fields (Continued)

Field	Description
Active Supervisor Precedence	Displays the precedence that is assigned to the ring supervisor. You assign the precedence value on the Advanced Network Configuration dialog box. See Table 48.
Enable Supervisor Mode	Check to make the switch a ring supervisor. The configuration takes effect immediately.
Ring Faults Detected	Displays the number of faults that are currently detected in the ring. When a DLR network is powered-up, the supervisor can detect ring faults as a result of powering up before other devices on the network. You can use an MSG instruction to clear the faults.
Supervisor Status	Displays whether the switch is operating as the active ring supervisor or back-up ring supervisor. Valid values: • Active • Backup
Last Active Node on Port 1	Displays the IP address of the last active node on DLR port 1.
Last Active Node on Port 2	Displays the IP address of the last active node on DLR port 2.

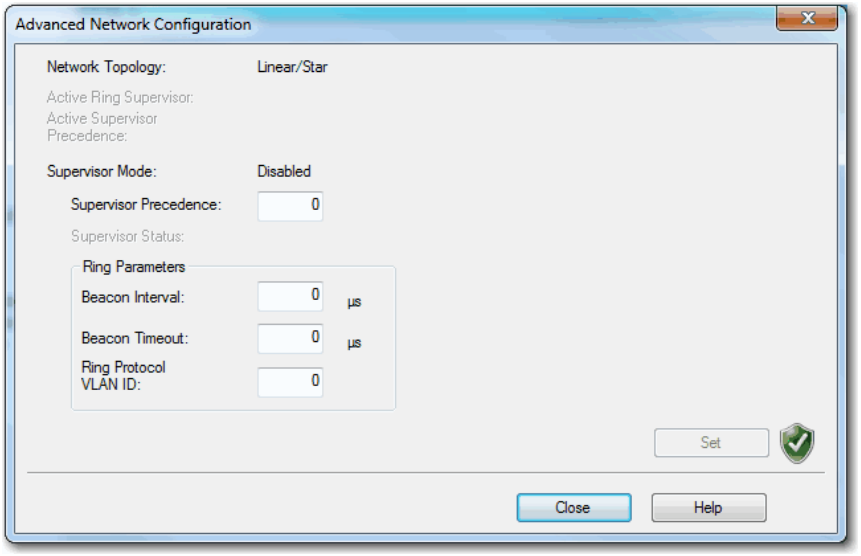


Table 48 - Advanced Network Configuration Fields

Field	Description
Network Topology	Displays whether the switch is operating in a DLR or linear network. Valid values: • Ring • Linear
Active Ring Supervisor	Displays the IP address of the active ring supervisor.
Active Supervisor Precedence	Displays the precedence that is currently assigned to the active ring supervisor.
Supervisor Mode	Displays the status of Supervisor mode. You can enable Supervisor mode on the Ring 1, Ring 2, or Ring 2 view. See Table 47. Valid values: • Enabled • Disabled (default)
Supervisor Precedence	Type a precedence value to assign to the ring supervisor. When multiple supervisors are configured, the precedence value determines the active ring supervisor. Only one supervisor can be active at one time. The precedence is transmitted in beacon frames. When two supervisors have the same precedence, the device with the numerically highest MAC address becomes the active supervisor. Valid values: 0…255. The default precedence is 0. The highest precedence is 255.

Table 48 - Advanced Network Configuration Fields

Field	Description
Beacon Interval	Type an interval for the supervisor to transmit beacon frames. Valid values: 200…100,000 µs The default interval i s 400 µs.
Beacon Timeout	Type the amount of time ring nodes wait before timing out in the absence of received beacon messages. Valid values: 400…500,000 µs The default timeout is 1960 µs.
Ring Protocol VLAN ID	Reserved for future use.

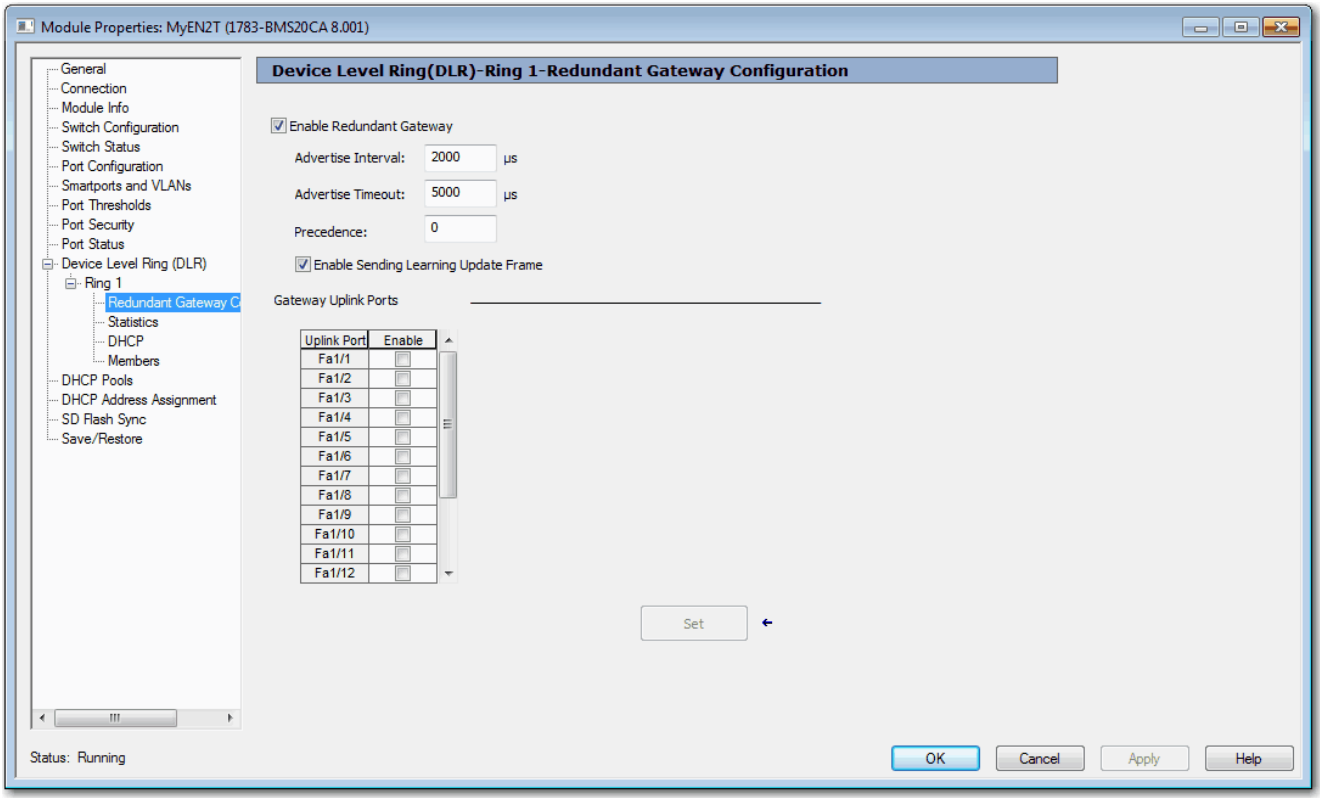


Table 49 - Redundant Gateway Configuration Fields

Field	Description
Enable Redundant Gateway	Check the checkbox to enable the configuration of redundant gateways. The configuration fields are available only after you enable the feature. Default: Disabled
Advertise Interval	Type the time interval for the gateway to transmit advertise messages. Valid values: 200…100,000 µs Default: 2000 µs
Advertise Timeout	Type the duration of time for nodes to wait before timing out in the absence of received advertise messages. Valid values: 200…500,000 µs Default: 5000 µs

Table 49 - Redundant Gateway Configuration Fields (Continued)

Field	Description
Precedence	Choose a role to assign to the redundant gateway that corresponds to a predefined precedence value. The switch transmits the precedence value is advertise messages and is used to select the redundant gateway when multiple redundant gateways are configured. A higher value means higher precedence. When two DLR redundant gateways have the same precedence, the device with the numerically highest MAC address will become the redundant gateway. Valid values: • None—0 • Primary—255 • Backup 1—100 • Backup 2—90 • Backup 3—80 • Custom—Type a value from 0…255
Enable Sending Learning Update Frame	Check the checkbox to enable learning update messages. Default: Enabled
Gateway Uplink Ports	Check the Enable checkbox for each uplink port on which to enable redundant gateway.

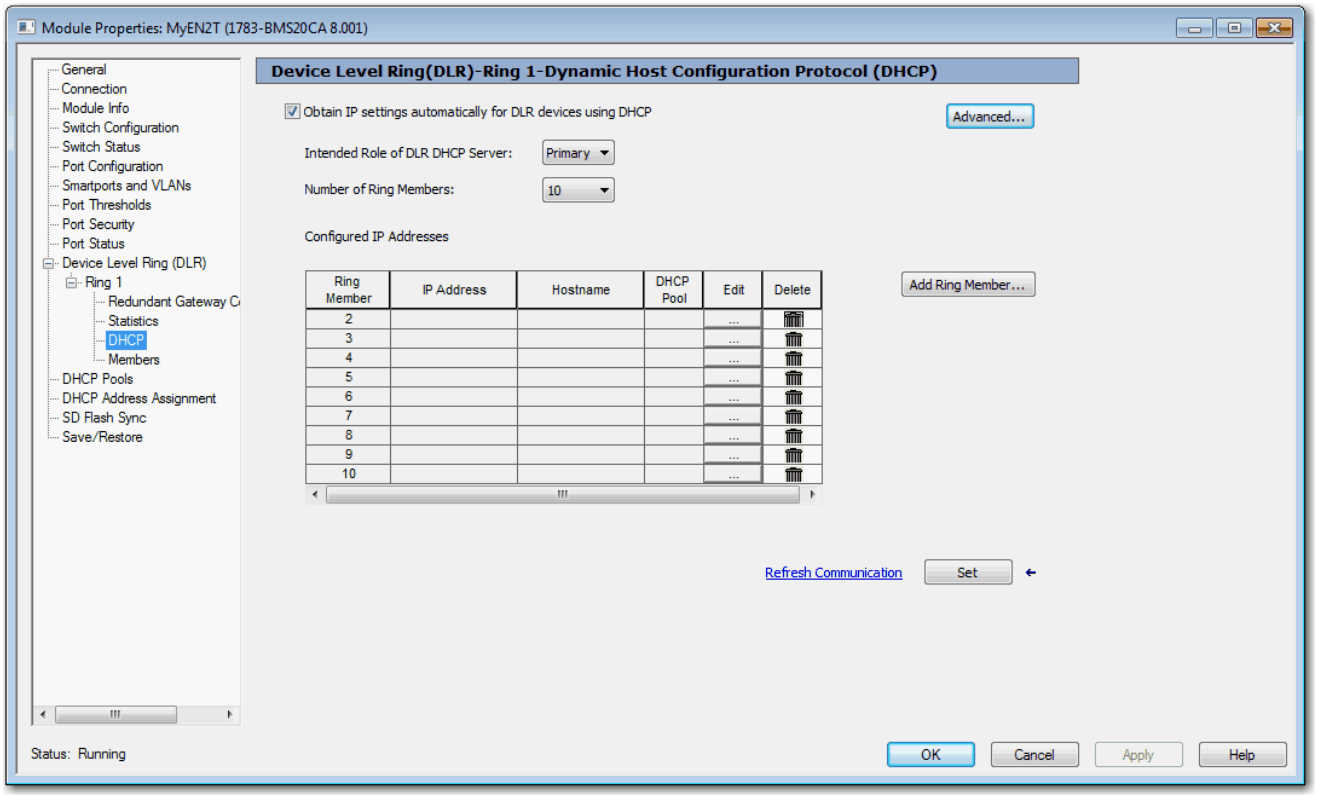


Table 50 - DHCP Fields

Field	Description
Obtain IP settings automatically for DLR devices using DHCP	Check the checkbox to enable the ring DHCP server on the DLR supervisor device.
Intended Role of DHCP Server	Choose the role to assign to the DHCP server: • Primary—The DLR supervisor functions as the active ring DHCP server. • Backup—The DLR supervisor functions as the backup ring DHCP server.
Number of Ring Members	Choose the number of devices in the ring, including switches.
Ring Member	Displays the order of devices in the ring when the switch is the ring supervisor. The switch is always ring member 1.

Table 50 - DHCP Fields

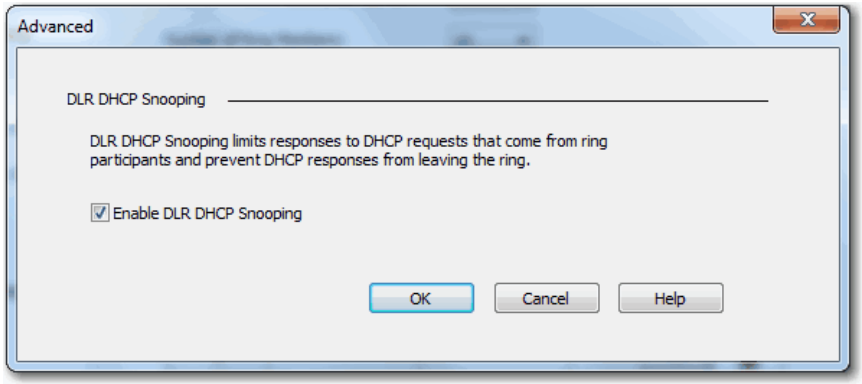
Field	Description
IP Address	Displays the IP address of the ring member. The IP address is reserved for the selected port and is not available for normal DHCP assignment. The IP address must be an address from the pool specified in DHCP IP address pool. To assign IP addresses to ring members, see Refer to Assign IP Addresses to Ring Members on page 236.
Hostname	Displays the name for the host associated with the ring member.
DHCP Pool	Displays the name of the DHCP IP address pool configured on the switch.

Enable Ring DHCP Snooping

To enable DHCP snooping within the ring, click Advanced and check the Enable DLR DCHP Snooping checkbox.

Ring DHCP snooping restricts the broadcast of DHCP requests from going beyond the ring. Only devices in the ring receive address assignments from the DHCP server.

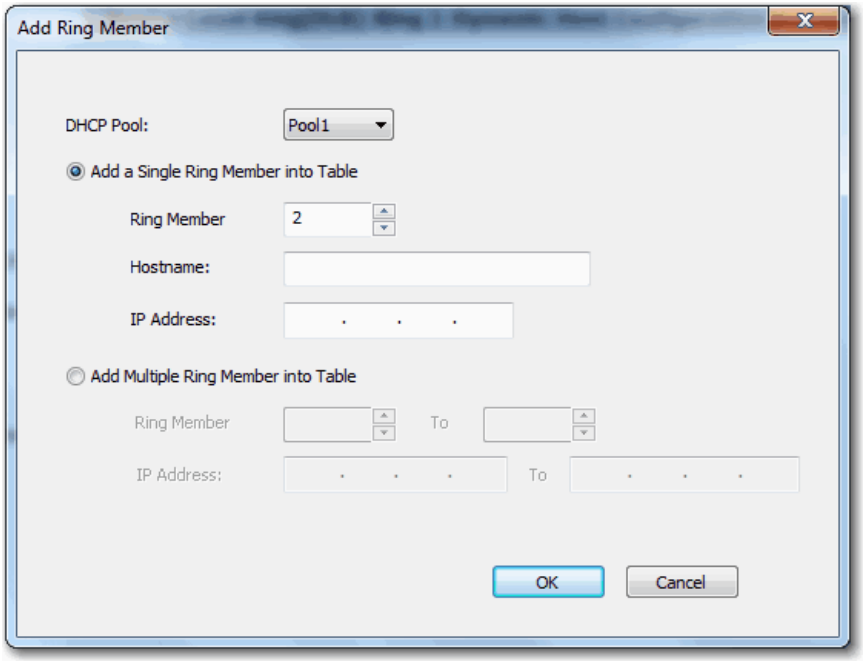
DHCP snooping is enabled by default. If you are not using DLR DHCP, you must disable Ring DHCP Snooping to use DHCP server functionality outside of the ring.



Assign IP Addresses to Ring Members

To assign IP addresses to ring members, follow these steps.

1. Click Add Ring Member to display the Add Ring Member dialog box.



2. From the DHCP Pool field, choose the name of the IP address pool to use for ring devices.

   This pool must be previously configured, as described on page 243.

   DHCP persistance and DHCP for ring devices can coexist, but cannot share the same pool.

3. To assign an IP address to a single ring member, click Add a Single Ring Member into Table, and then compete these fields:
   - Ring Member—Type a value between 2 ...255 to indicate the location of the ring device. The switch is always ring member 1.
   - Hostname—Type a host name to associate with the IP address for the ring member.
   - IP Address—Type the IP address for the ring member.
4. To assign IP addresses to multiple ring members, click Add Multiple Ring Members into Table, and then complete these fields:
   - Ring Member...To—Type values between 2 ...255 to indicate the starting and ending locations of the ring members.
   - IP Address...To—Type the starting and ending IP addresses for the ring members.
5. Click OK.

Dynamic Host Configuration Protocol (DHCP) Persistence

Every device in an IP-based network must have a unique IP address. DHCP assigns IP address information from a pool of available addresses to newly connected devices (DHCP clients) in the network. If a device leaves and then rejoins the network, the device receives the next available IP address, which is not necessarily the same address that it had before.

The switch can be set to operate as a DHCP server to provide DHCP persistence. With DHCP persistence, you can assign a specific IP address to each port to make sure that a device that is attached to a specific port receives the same IP address. This feature works with only one device that is connected to each port configured for DHCP persistence. The DHCP server also serves addresses to BOOTP clients.

IMPORTANT To make sure DHCP persistence works correctly, follow the application rules.

Configure DHCP via Device Manager

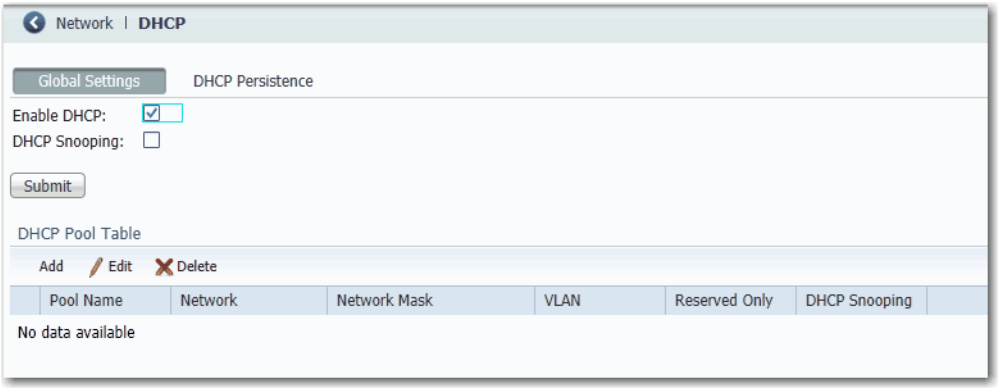
To use DHCP persistence, complete this process:

1. Enable DHCP.
2. Configure the IP address pool.
3. Assign a specific IP address to each port.

Configure the DHCP Server

To enable the DHCP Server mode on the switch, do the following.

1. From the Configure menu, choose DHCP.



2. Check the Enable DHCP checkbox.

3. To enable DHCP snooping, check the DHCP Snooping checkbox.

   DHCP snooping restricts the broadcast of DHCP requests beyond the connected switch. As a result, devices receive address assignments from only the connected switch. This option is available only on ports assigned to a VLAN. To enable DHCP Snooping on a specific VLAN, check the DHCP Snooping checkbox for the specific VLAN in the DHCP pool table.

4. To reserve an address pool for only the devices that are specified in the DHCP persistence table, check the Reserved Only checkbox in the DHCP pool table.

   DHCP requests from ports not in the persistence table or from another switch are ignored. By default, this option is disabled and the Reserved Only checkbox is cleared.

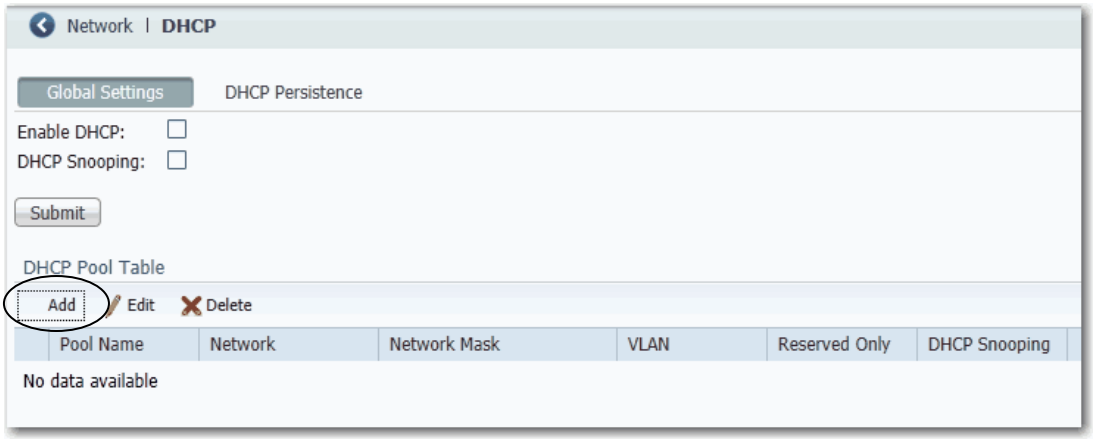
5. Click Submit.

Configure a DHCP IP Address Pool

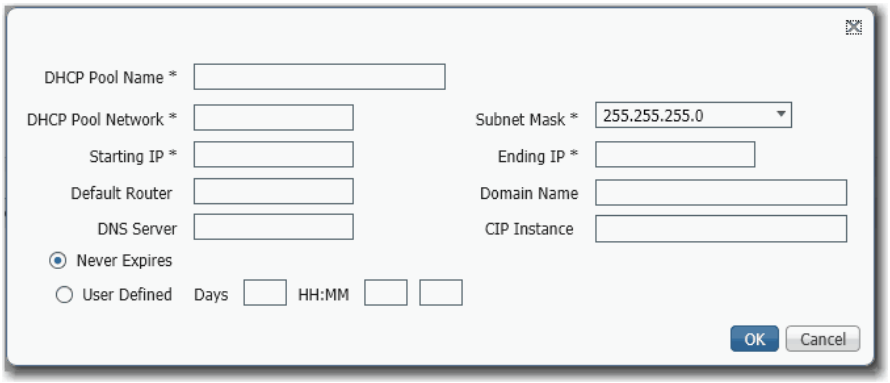
Once DHCP is enabled, you can create the DHCP address pool.

To configure a DHCP IP address pool, follow these steps.

1. From the Configure menu, choose DHCP.
2. Click Add.



3. Complete the fields and click OK.



Field	Description
DHCP Pool Name	The name of the DHCP IP address pool that is configured on the switch. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab. This field is required. A DHCP IP address pool is a range (or pool) of available IP addresses that the switch can assign to connected devices.
DHCP Pool Network	The subnetwork IP address of the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers that are separated by periods. Each number can be from 0…255. This field is required.
Subnet Mask	The network address that identifies the subnetwork (subnet) of the DHCP IP address pool. Subnets segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is required.
Starting IP	The starting IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers that are separated by periods. Each number can be from 0…255. Be sure that none of the IP addresses that you assign are being used by another device in your network. This field is required.
Ending IP	The ending IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers that are separated by periods. Each number can be from 0…255. Make sure that none of the IP address you assign are being used by other devices in your network. This field is required.
Default Router	The default router IP address for the DHCP client that uses this server. The format is a 32-bit numeric address that is written as four numbers that are separated by periods. Each number can be from 0… 255.
Domain Name	The domain name for the DHCP client. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab.
DNS Server	The IP addresses of the domain name system (DNS) IP servers available to a DHCP client. The format is a 32-bit numeric address that is written as four numbers that are separated by periods. Each number can be from 0…255.
CIP Instance	A number from 1…15 to identify the address pool.
[Lease Length]	The duration of the lease for an IP address that is assigned to a DHCP client. Click one of the following: • Never Expires • User Defined If you click User Defined, enter the duration of the lease in the numbers of days, hours, and minutes. This lease length is used for all assignments.

Reserve IP Addresses through DHCP Persistence

IMPORTANT DHCP persistence does not work with DHCP for ring devices, as described on page 222. Configure only one of these features on your switch.

You can reserve and preassign an IP address from the IP address pool to a specific switch port. As a result, a device that is connected to that switch port always receives the same IP address regardless of its MAC address.

DHCP persistence is useful in networks that you configure in advance, where dependencies on the exact IP addresses of some devices exist. Use DHCP persistence when the attached device has a specific role to play and when other devices know its IP address. If the device is replaced, the replacement device is assigned the same IP address, and the other devices in the network require no reconfiguration.

When the DHCP persistence feature is enabled, the switch acts as a DHCP server for other devices on the same subnet, including devices that are connected to other switches. If the switch receives a DHCP request, it responds with any unassigned IP addresses in its pool. To prevent the switch from responding when it receives a request, check the Reserve Only box on the DHCP window.

When DHCP persistence is enabled and a DHCP request is made from a connected device on that port, the switch assigns the IP address for that port. It also broadcasts the DHCP request to the remainder of the network. If another DHCP server with available addresses is on the network and receives this request, it can try to respond. The response can override the initial IP address the switch assigns depending on how the end device behaves (takes first IP address response or the last). To prevent the IP address from being overridden, enable DHCP snooping on the appropriate VLAN. Enabling DHCP snooping blocks the broadcast of this DHCP request, so that no other server, including another Stratix switch with DHCP persistence enabled, responds.

If you are using DHCP persistence, we recommend that you initially assign static IP addresses to end devices. If an end device fails and is replaced, the DHCP persistence feature assigns an IP address from the DHCP persistence table. The device functions properly with this IP address, but we recommend that you reassign a static IP address to the replaced devices.

The following figure and table illustrate DHCP persistence behavior.

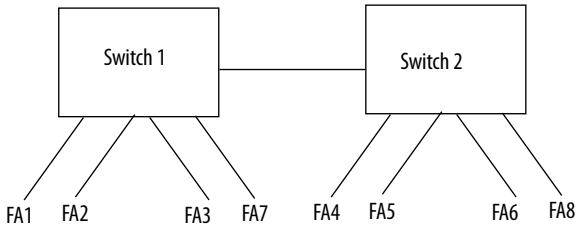


Table 51 - DHCP Persistence Behavior

If	Then
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6, and FA8 in its persistence table • Reserve Only is not selected and DHCP snooping is off	A new device that is connected to switch 1 FA1 receives an IP address from the switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 responds if there is an unassigned address in its pool. The response can override the assignment that is made by switch 1.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6, and FA8 in its persistence table • Reserve Only is selected in both switches and DHCP snooping is off	A new device that is connected to switch 1 FA1 receives an IP address from the switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 does not respond to the request. If the device is connected to FA7 of switch 1, it does not receive an IP address from the switch pool because it is not defined in the persistence table. Also, unused addresses in the pool are blocked.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6, and FA8 in its persistence table • Reserve Only is selected in switch 1 and DHCP snooping is off, but not switch 2 when DHCP snooping is off	A new device is connected to FA1 receives an IP address from the persistence table. A broadcast request is also sent across the network. Switch 2 does not respond to the request. In addition, a device that is connected to FA4 receives an IP address from the switch 2 persistence table. A broadcast request is sent out, and switch 1 responds with an unused IP address from its pool. The response can override the assigned port.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6, and FA8 in its persistence table • DHCP Snooping is selected • Reserved Only is checked	A new device that is connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is not sent across the network, so Switch 2 does not respond. If a device is connected to FA7 of Switch 1, it does not receive an IP address from the switch pool because it is not defined in the persistence table. Also, unused addresses in the pool are blocked.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6, and FA8 in its persistence table • DHCP Snooping is selected • Reserved Only is not checked	A new device that is connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is not sent across the network, therefore Switch 2 does not respond. If a device is connected to FA7 (not defined in the DHCP persistence table) of Switch 1, it receives an unassigned IP address from the switch 1 pool.

To manage switch port IP addresses, click the DHCP Persistence tab.

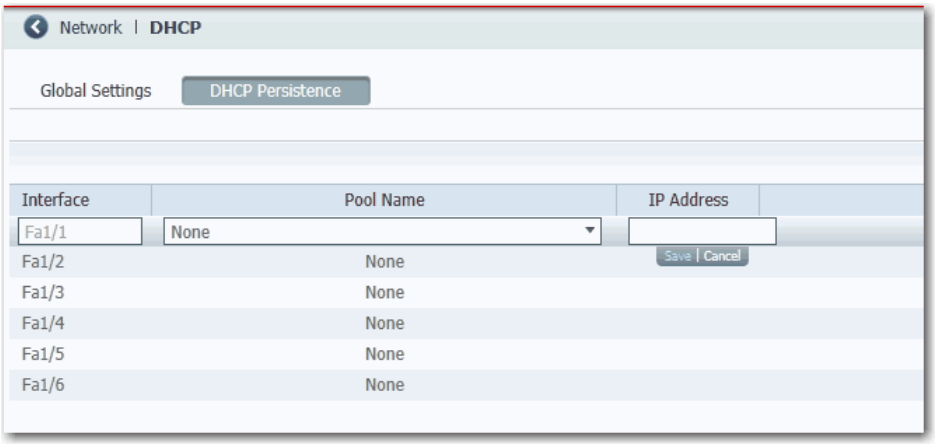


Table 52 - DHCP Persistence Fields

Field	Description
Interface	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), and the specific port number. For example, Fa1/1 is Fast Ethernet port 1 on the switch.
Pool Name	The name of the DHCP IP address pool that is configured on the switch.
IP Address	The IP address that is assigned to the switch port. The IP address that you assign is reserved for the selected port and is not available for normal DHCP dynamic assignment. The IP address must be an address from the pool that is specified in the DHCP Pool Name field.

Configure DHCP via the Logix Designer Application

In the navigation pane, click DHCP Address Assignment.

You can assign a specific IP address to each port, so that the device attached to a given port receives the same IP address.

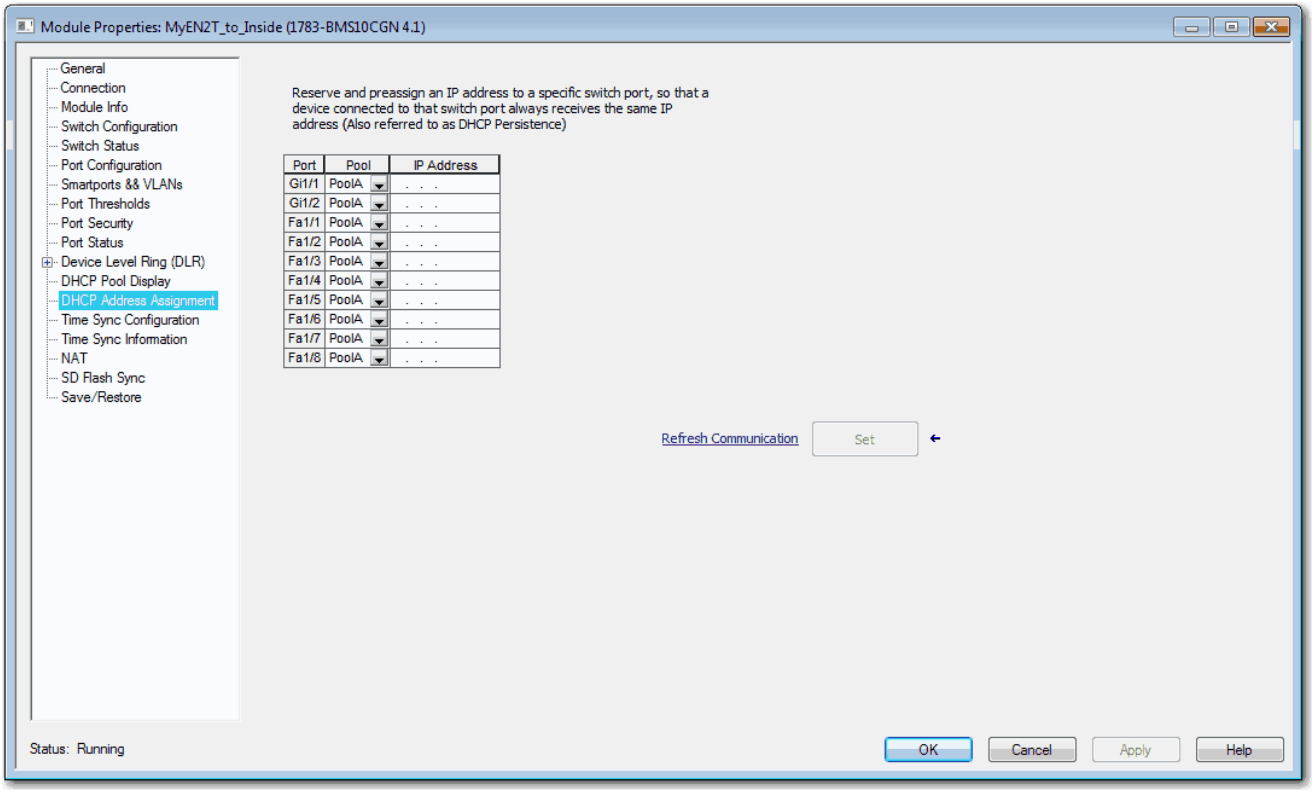


Table 53 - DHCP Address Assignment Fields

Field	Description
Unit (Stratix 8000/8300 switches)	Displays the unit on which the selected port resides: • 6 Port Base • 10 Port Base • Expansion 1 • Expansion 2
Port	Displays the ports available for the configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the port number: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa1/1 is Fast Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module. • Fa3/1 is Fast Ethernet port 1 on the second expansion module.
Pool	Displays the pool names from the DHCP IP address pool that corresponds to the instances available in the switch. If you delete all rows that contain pools on the DHCP Pool Display tab and click Refresh, the Pool field is blank.
IP Address	Displays the IP address that is assigned to the switch port. The format is a 32-bit numeric address that is written as four numbers that are separated by periods (for example, 255.255.255.255). Each number can be from 0…255. The IP address that you assign is reserved for the selected port and is not available for normal DHCP dynamic assignment. The IP address must be an address from the pool that is specified in the DHCP Pool Name field.

EtherChannels

An EtherChannel, or port group, is a group of two or more Fast Ethernet or Gigabit Ethernet switch ports that are bundled into a logical link. The group creates a higher bandwidth link between two switches. For example, four 10/100 switch ports can be assigned to an EtherChannel to provide Full-duplex bandwidth of up to 800 Mb/s. If one of the ports in the EtherChannel becomes unavailable, traffic is carried over the remaining ports within the EtherChannel.

All ports in an EtherChannel must have the same characteristics:

- All are applied with the Smartports IE Switch port role and belong to the same VLAN.
- All are either 10/100 ports, or all are 10/100/1000 ports. You cannot group a mix of 10/100 and 10/100/1000 ports in an EtherChannel.
- All are enabled. A disabled port in an EtherChannel is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel.

IMPORTANT Do not enable Layer 3 addresses on the physical EtherChannel interfaces.

Table 54 shows the maximum number of EtherChannels available per switch. Each EtherChannel can consist of up to eight compatible, configured Ethernet ports.

Table 54 - EtherChannels by Switch

Switch	EtherChannels, max
Stratix 5400	10
Stratix 5410	10
Stratix 5700(1)	6
ArmorStratix 5700	6
Stratix 8000/8300	6

(1) EtherChannels are available only on swithes with Full firmware.

Figure 21 shows two EtherChannels. Two Full-duplex 10/100/1000-Mbps ports on Switches A and C create an EtherChannel with a bandwidth of up to 4 Gbps between both switches. Similarly, two Full-duplex 10/100 ports on Switches B and D create an EtherChannel with a bandwidth of up to 400 Mbps between both switches.

If one of the ports in the EtherChannel becomes unavailable, traffic is sent through the remaining ports within the EtherChannel.

Figure 21 - EtherChannel Example

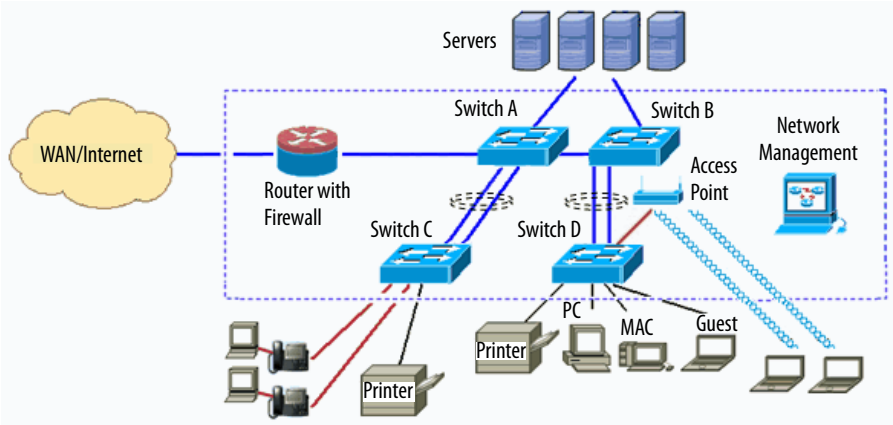


Table 55 describes the modes you can assign to an EtherChannel:

Table 55 - EtherChannel Modes

Mode	Description
Static	All ports join the EtherChannel, without negotiations. This mode can be useful if the remote device does not support the protocols that other modes require. The switches at both ends of the link must be configured in Static mode.
Port Aggregation Control Protocol (PAgP)	A Cisco-proprietary protocol. The port responds to requests to create EtherChannels but does not initiate such negotiations. This silent mode is recommended when a port is connected to a device, such as a file server or a packet analyzer that is unlikely to send PAgP packets. A port in the PAgP mode can form an EtherChannel with another port in the PAgP Desirable mode.
Port Aggregation Control Protocol (PAgP) (non-silent)	This mode is the same as PAgP mode but is recommended when the port is connected to a device that is expected to be active in initiating EtherChannels. A port in PAgP mode can form an EtherChannel with another port in the PAgP Desirable mode.
Port Aggregation Control Protocol (PAgP) Desirable	This mode enables PAgP. The port initiates negotiations to form EtherChannels by sending PAgP packets to other ports. This silent mode is recommended when a port is connected to a device, such as a file server or a packet analyzer that is unlikely to send PAgP packets. A port in the Desirable mode can form an EtherChannel with another port that is in PAgP or PAgP Desirable mode.
Port Aggregation Control Protocol (PAgP) Desirable (non-silent)	This mode is the same as PAgP Desirable mode but is recommended when the port is connected to a device that initiates EtherChannels.
Link Aggregation Control Protocol (LACP) (active)	This mode enables LACP unconditionally. The port sends LACP packets to other ports to initiate negotiations to create EtherChannels. A port in active LACP mode can form an EtherChannel with another port that is in active or passive LACP mode. The ports must be configured for Full-duplex.
Link Aggregation Control Protocol (LACP) (passive)	This mode enables LACP only if an LACP device is detected at the other end of the link. The port responds to requests to create EtherChannels but does not initiate such negotiations. The ports must be configured for Full-duplex.

Configure both ends of the EtherChannel in the same mode:

- When you configure one end of an EtherChannel in PAgP or LACP mode, the system negotiates with the other end of the channel to determine the ports to become active. Incompatible ports are suspended. Instead of a suspended state, the local port is put into an independent state and continues to carry data traffic as any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

- When you configure an EtherChannel in Static mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the Static mode; otherwise, packet loss can occur.

If a link within an EtherChannel fails, traffic previously carried over that failed link moves to the remaining links within the EtherChannel. If traps are enabled on the switch, a trap is sent for a failure that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

Configure EtherChannels via Device Manager

From the Configure menu, choose EtherChannels.

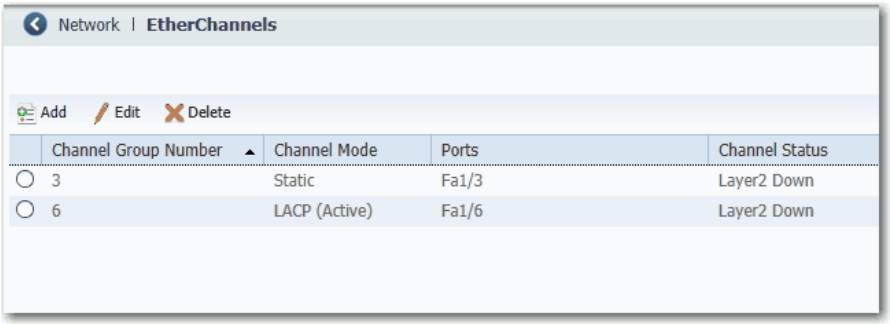


Table 56 - EtherChannel Fields

Field	Description
Channel Group Number	A number to identify the EtherChannel. See Table 54 for the maximum number of EtherChannels available per switch.
Channel Mode	Determines how ports become active. With all modes except Static, negotiations occur to determine which ports become active. Incompatible ports are put into an independent state and continue to carry data traffic, but do not participate in the EtherChannel. **IMPORTANT:** Make sure that all ports in an EtherChannel are configured with the same speed and duplex mode. See Table 55 for a description of EtherChannel modes.
Ports	The ports that can participate in the EtherChannel.
Channel Status	The status of the group.

Configure EtherChannels via the Logix Designer Application

In the navigation pane, click EtherChannels.

You can add, edit, and delete EtherChannel members.

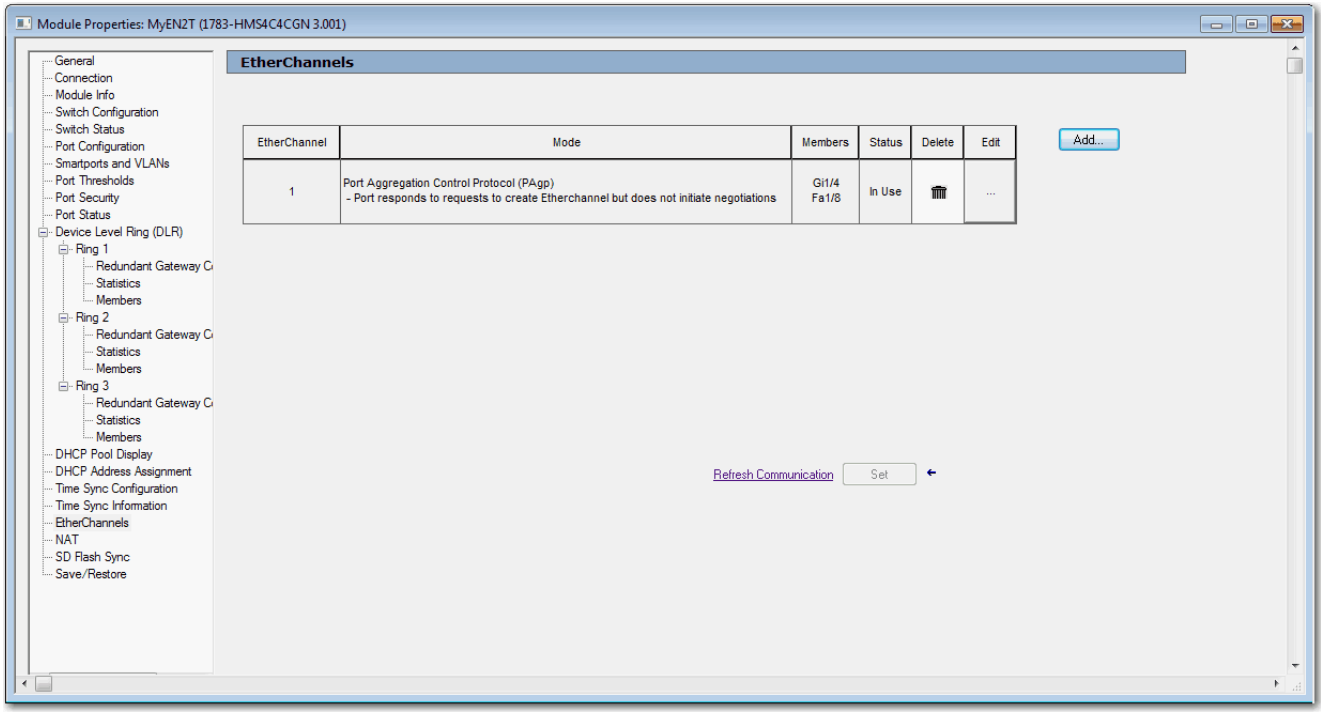


Table 57 - EtherChannels Fields

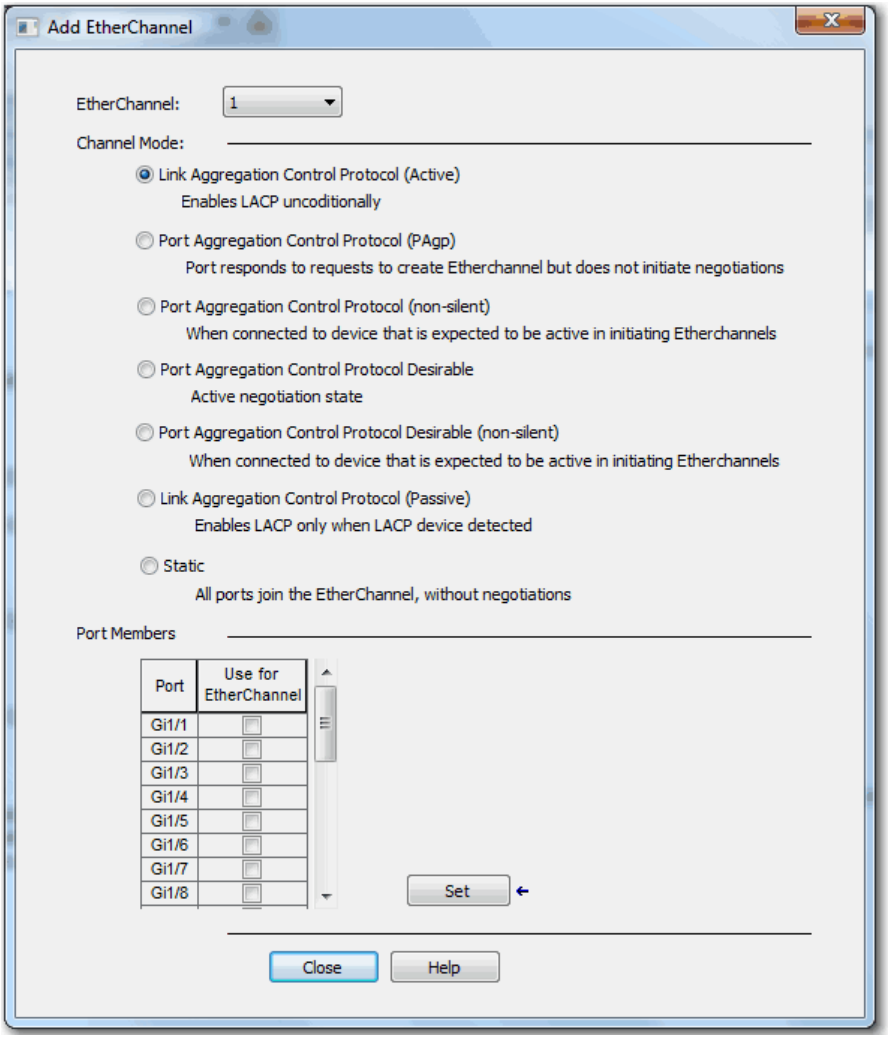
Field	Description
EtherChannel	A number to identify the EtherChannel. See Table 54 for the maximum number of EtherChannels available per switch.
Mode	Determines how ports become active. With all modes except Static, negotiations occur to determine which ports become active. Incompatible ports are put into an independent state and continue to carry data traffic, but do not participate in the EtherChannel. **IMPORTANT:** Make sure that all ports in an EtherChannel are configured with the same speed and duplex mode. See Table 55 for a description of EtherChannel modes.
Members	The ports that can participate in the EtherChannel.
Status	The status of the group.

Add an EtherChannel

To add an EtherChannel, follow these steps.

1. On the EtherChannels view, click Add.
2. Choose a number to assign to the EtherChannel.
3. Click a mode to assign to the EtherChannel.

   See Table 55 for a description of each mode.
4. In the use for EtherChannel column, check the checkbox next to each port to participate in the EtherChannel.
5. Click Close.



Motion Prioritized QoS Macros

During Express Setup, the switch applies QoS settings optimized for most applications. The default QoS settings assign equal priority to traffic for CIP and traffic for Integrated Motion on the EtherNet/IP network. However, you can assign the highest priority to traffic for Integrated Motion on the EtherNet/IP network by applying the following QoS macros in Device Manager.

Table 58 - Motion Prioritized QoS Macros

Switch	Macro
Stratix 5400	Motion Prioritized QoS
Stratix 5410	
Stratix 5700	Motion Prioritized QoS Step 1 Motion Prioritized QoS Step 2
ArmorStratix 5700	
Stratix 8000	

These macros move motion traffic to the highest level queue with time sync. After you apply the macros, motion traffic takes priority over CIP traffic.

Configure Motion Prioritized QoS Macros via Device Manager

From the Configure menu, choose Global Macros:

- To apply a macro, check the checkbox for the macro and click Save.
- To remove a macro, clear the checkbox for the macro and click Save.

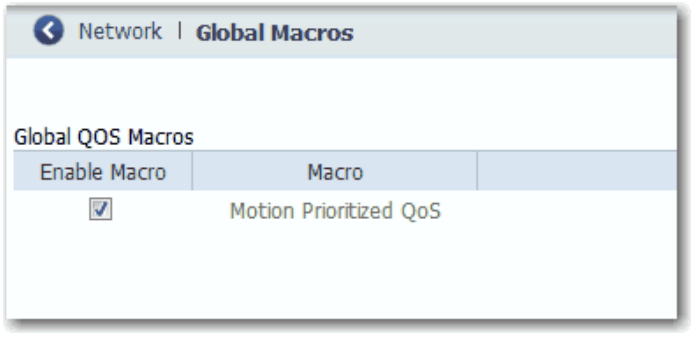
Once you click Save, the changes take effect immediately.

IMPORTANT For Stratix 5700 and 8000 switches, you must apply both Motion Prioritized QoS Step 1 and Motion Prioritized QoS Step 2 macros. If you enable only one macro, the QoS settings applied during Express Setup remain active.

Figure 22 - QoS Macros for Stratix 5700, ArmorStratix 5700, and Stratix 8000 Switches



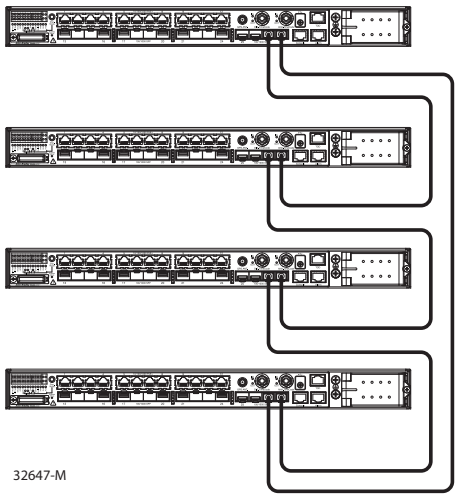
Figure 23 - QoS Macro for Stratix 5400 and 5410 Switches



Horizontal Stacking

Horizontal stacking lets you manage as many as four Stratix 5410 switches as one logical device. To stack multiple switches, you connect the switches via as many as two uplink Ethernet ports per switch. You use the CLI to configure network ports as designated stack ports. Once you configure a network port as a stack port, you cannot apply any network configuration to that port.

Figure 24 - Switch Stack



Within a horizontal stack, one switch acts as the master switch and the others as slaves. For instructions on how to configure and monitor a switch stack via the CLI, refer to documentation available at http://www.Cisco.com.

If communication fails between devices in a stack, the convergence time is more than one second.

The following table lists the switch catalog numbers and ports that support horizontal stacking.

Stratix 5410 Switch (four switches per stack, max)	Stack Ports (two ports per switch, max)
1783-IMS28NAC	Te1/25
1783-IMS28RAC	Te1/26
1783-IMS28NDC	Te1/27
1783-IMS28RDC	Te1/28

IMPORTANT A stack of switches must meet these minimum requirements:

- All switches must use the same firmware model
- All switches must use the same SDM template

If the SDM template of a switch is different than that of the master switch, apply the matching SDM template separately before you connect the switch to the stack.

You can configure a stack in either a ring topology (Figure 25) or a linear topology (Figure 26).

Figure 25 - Switch Stack in a Ring Topology

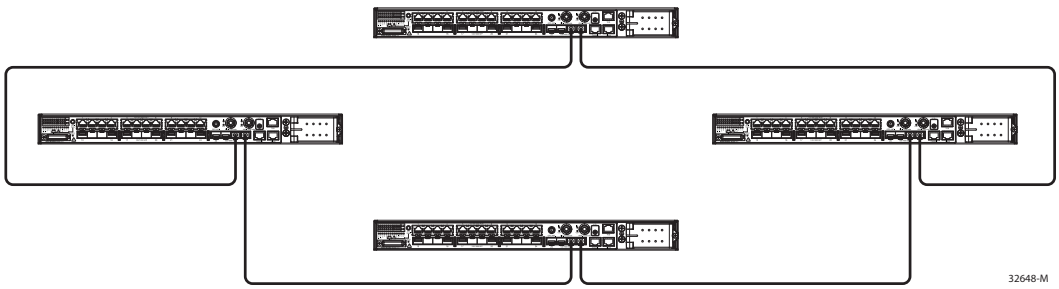


Figure 26 - Switch Stack in a Linear Topology

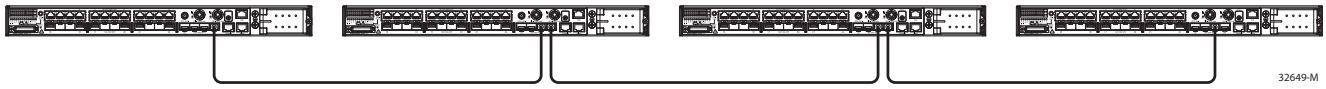


Table 59 lists the supported features for horizontal stacking.

Table 59 - Supported Features

Feature Type	Support
Layer 2 features	• Link status detection, speed, duplex • Layer 2 learning and forwarding • STP, MSTP, RSTP, BPDU Guard • VLAN, VTP, DTP, VLAN Table • CDP, LLDP • UDLD • EtherChannel (LACP and PAgP) • Flex links • IGMP Snooping • ARP • REP ring convergence
Layer 3 features	• ARP • Static routes • Layer 3 host configuration
Power over Ethernet (PoE)	PoE is supported in Stack mode.
Traffic types	• Layer 2 unicast • Layer 2 multicast and broadcast • Layer 3 unicast traffic • Layer 3 multicast and broadcast

Any feature not listed in Table 59...includes features, such as...

The following features are not supported:

- Device Manager
- CIP
- Layers 2 NAT
- PRP
- PTP

Internet Group Management Protocol (IGMP) Snooping with Querier

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic. IGMP snooping dynamically configures Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces that are associated with IP multicast devices. IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and track multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, it adds the host port number to the forwarding table entry. When the switch receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts that are interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The switch supports IP multicast group-based bridging, rather than MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address alias issues.

Table 60 defines the default number of supported multicast groups. You can modify the number of multicast groups that are supported by using the Command-line interface.

Table 60 - Default Supported Multicast Groups

Switch	Default Multicast Groups
Stratix 5400 and Stratix 5410 switches	1024
Stratix 5700 and ArmorStratix 5700 switches	256 If you exceed 180 multicast groups, we recommend that you switch to the routing SDM template via Device Manager.
Stratix 8000 switches	256 If you exceed180 multicast groups, we recommend that you modify the number of multicast groups by changing the SDM template to the Lanbase Routing template via Device Manager.
Stratix 8300 switches	1024

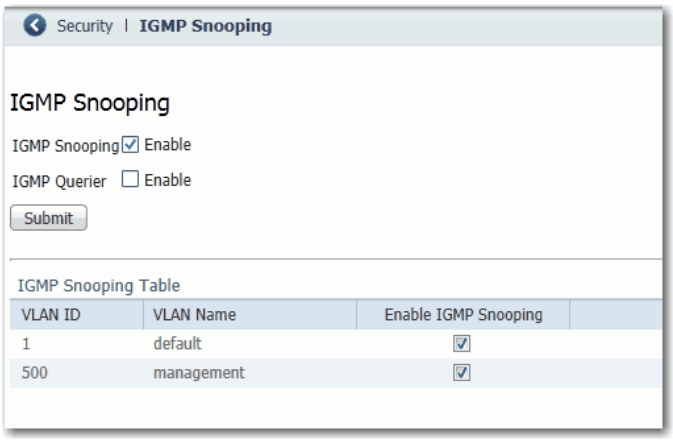
The IP multicast groups that are learned through IGMP snooping are dynamic. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings. The switch learns multicast IP addresses that are used by the EtherNet/IP network for I/O traffic.

IGMP implementation in the switch is IGMP V2. This version is backward-compatible with switches running IGMP V1. The switch has a built-in querier function, and the global macro enables on IGMP Snooping and the querier.

Configure IGMP Snooping via Device Manager

From the Configure menu, choose IGMP Snooping:

- To enable IGMP Snooping for all VLAN IDs, check Enable next to IGMP Snooping.
- To enable IGMP Querier for all VLAN IDs, check Enable next to IGMP Querier.
- To enable or disable IGMP snooping on a VLAN, select the VLAN and check or clear the Enable IGMP Snooping checkbox.



Network Address Translation (NAT)

For a list of switches that support NAT, see page 21.

NAT is a service that translates one IP address to another IP address via a NAT-configured switch. The switch translates the source and destination addresses within data packets as traffic passes between subnets.

This service is useful if you reuse IP addresses throughout a network. NAT enables devices that share one IP address on a private subnet to be segmented into multiple identical private subnets while maintaining unique identities on the public subnet.(1)

The implementation of NAT in Stratix switches is distinct in these ways:

- One-to-one NAT—The switch uses one-to-one NAT, rather than one-to-many NAT. One-to-one NAT requires that each source address translates to one unique destination address. Unlike one-to-many NAT, multiple source addresses cannot share a destination address.
- Layer 2 implementation—The implementation of NAT operates at the Layer 2 level. At this level, the switch can replace only IP addresses and does not act as a router.

See also the Stratix 5700 NAT Whitepaper, publication ENET-WP032.

Configuration Overview

To configure NAT, you create one or more unique NAT instances. A NAT instance contains entries that define each address translation and other configuration parameters.

IMPORTANT Before you create NAT instances, configure all Smartport roles and VLANs.

The translations that you define depend on whether traffic is routed through a Layer 3 switch or router or a Layer 2 switch.

IMPORTANT As a best practice, we recommend you route traffic through a Layer 3 switch or router.

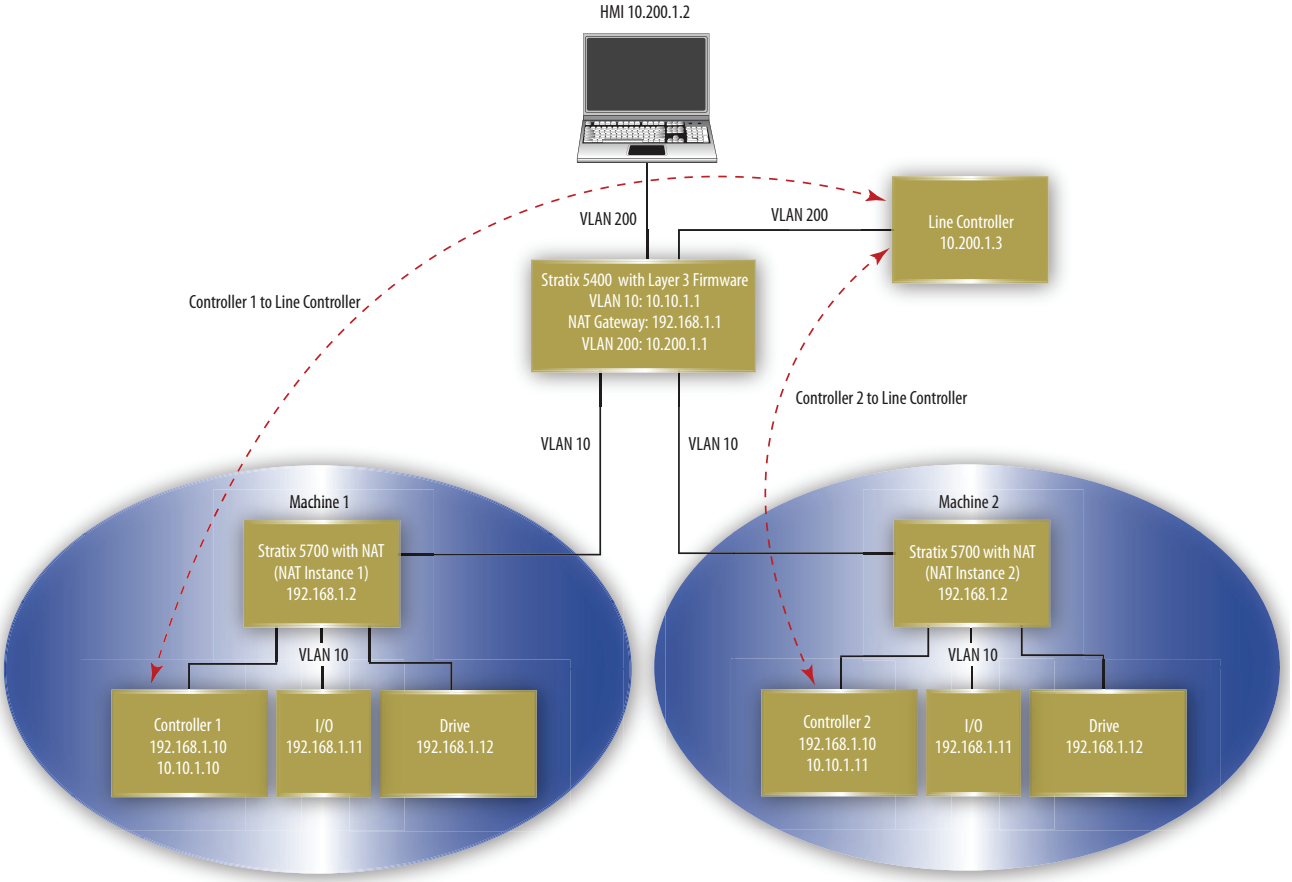
(1) The terms private and public differentiate the two networks on either side of the NAT device. The terms do not mean that the public network must be Internet routable.

If traffic is routed through a Layer 3 switch or router (Figure 27 and Figure 28), you define the following:

- A private-to-public translation for each device on the private subnet that communicates on the public subnet.(1)
- A gateway translation for the Layer 3 switch or router.

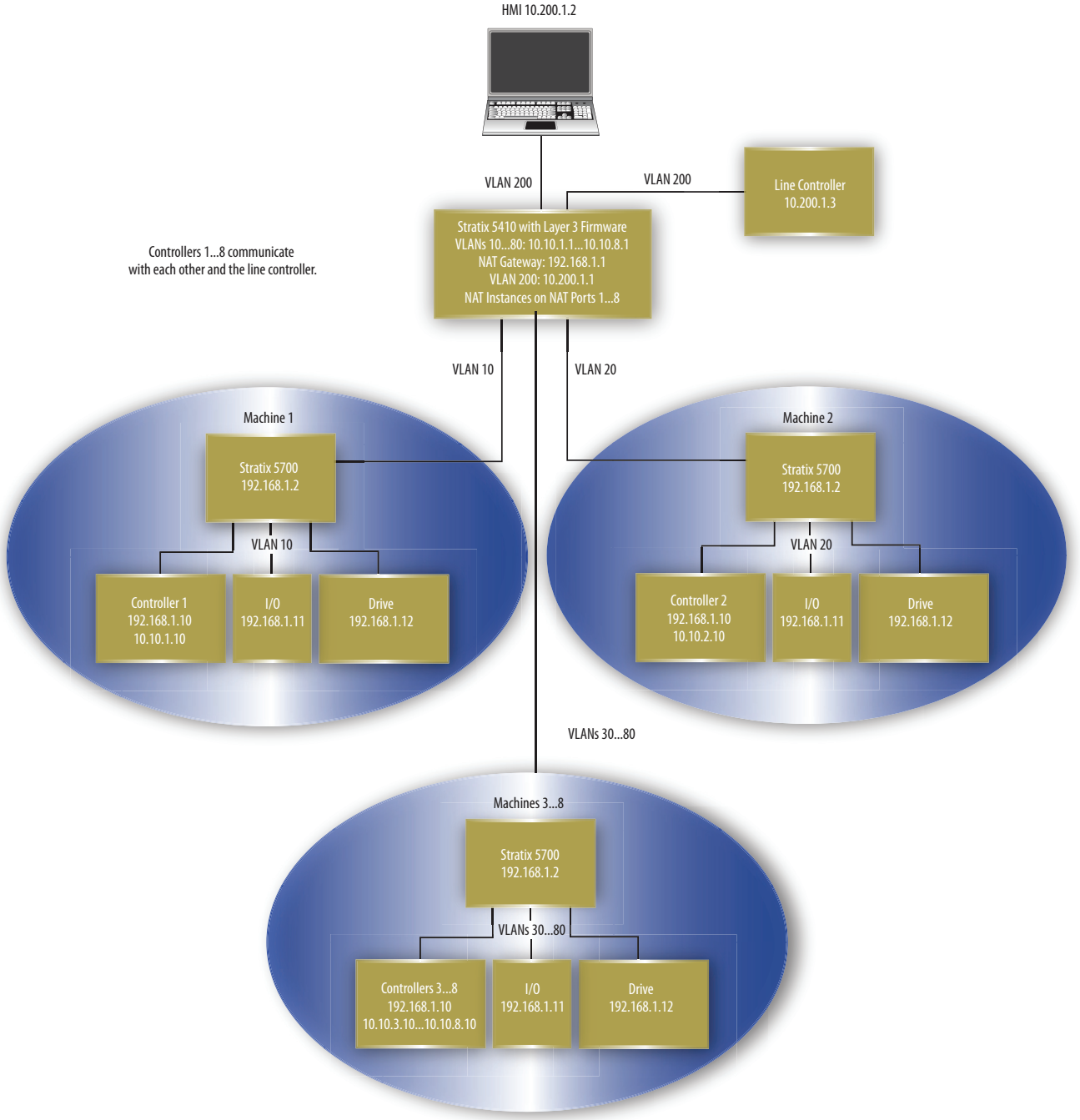
  You do not need to configure NAT for all devices on the private subnet. For example, you can choose to omit some devices from NAT to increase security, decrease traffic, or conserve public address space. By default, untranslated packets are dropped at the NAT boundary.

Figure 27 - Layer 3 Example with NAT in Stratix 5700 Switch



(1) Machines that communicate with each other within the same VLAN and subnet across a NAT boundary also require public-to-private translations.

Figure 28 - Layer 3 Example with NAT in Stratix 5410 Layer 3 Firmware Model



If traffic is routed through a Layer 2 switch (Figure 29 and Figure 30), you define the following.

- A private-to-public translation for each device on the private subnet that communicates on the public subnet.
- A public-to-private translation for each device on the public subnet that communicates on the private subnet.

Figure 29 - Layer 2 Example with NAT in Stratix 5700 Switch

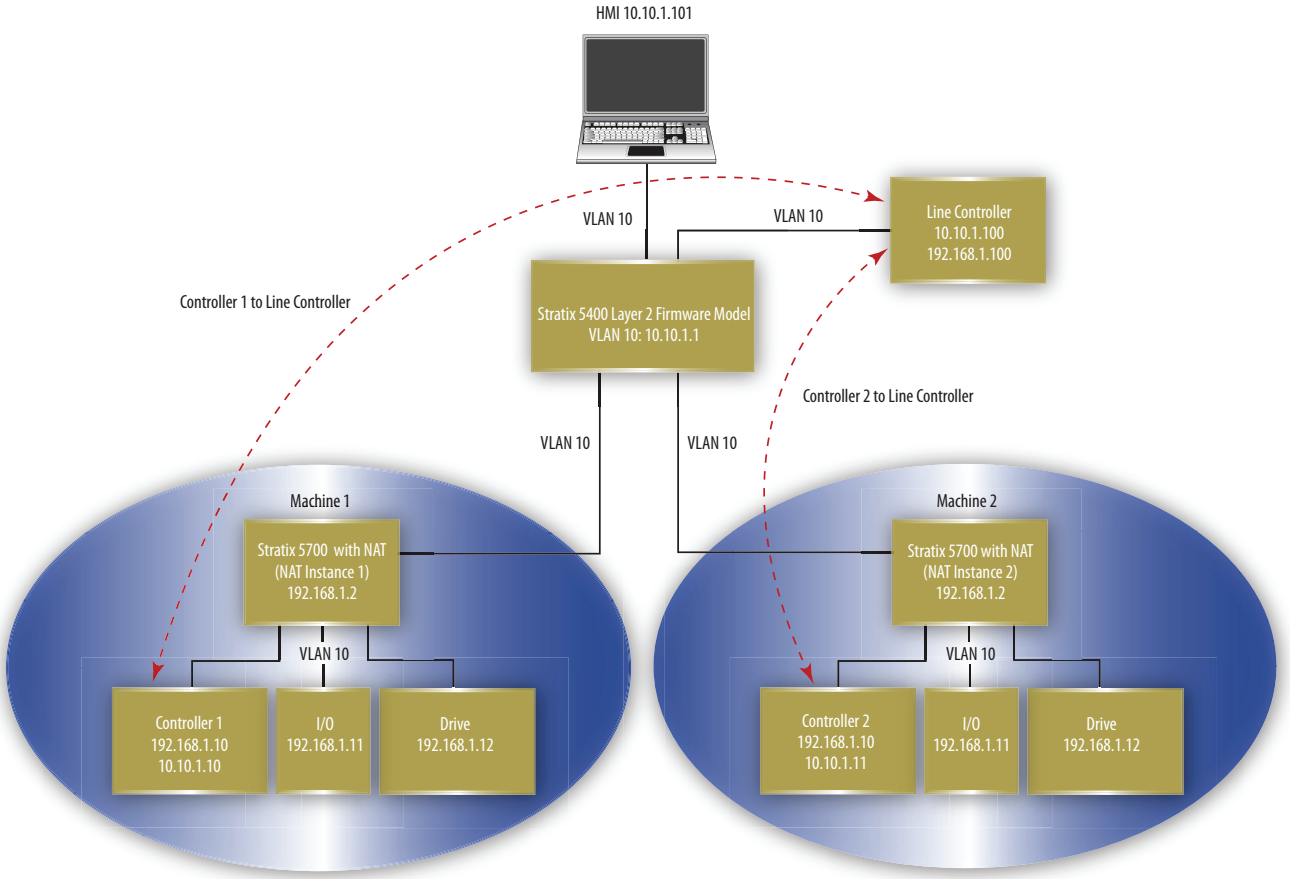
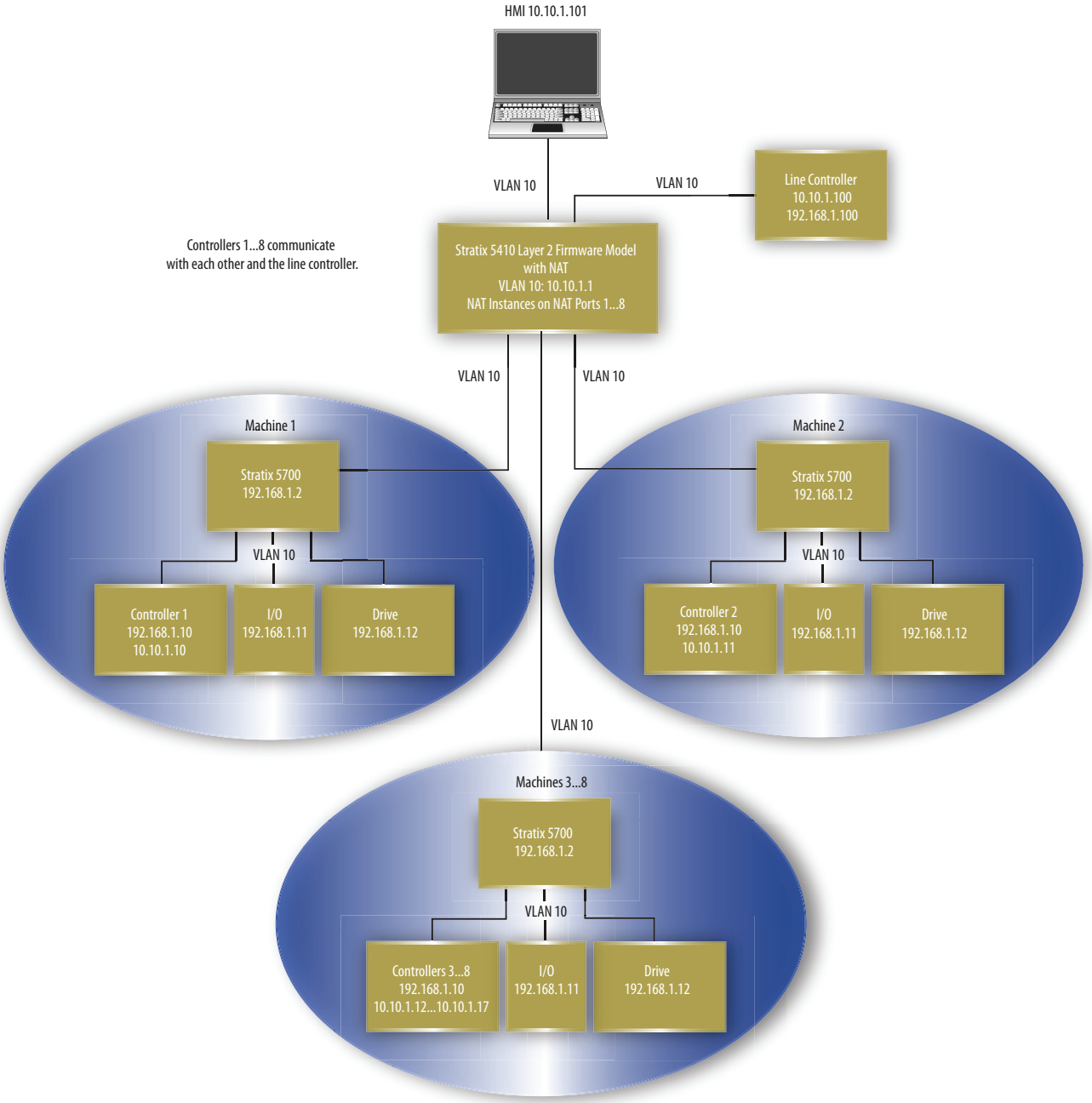


Figure 30 - Layer 2 Example with NAT in Stratix 5410 Layer 2 Firmware Model



An address translation can be one of three types. The type of translation determines the number of translation entries as shown in Table 61.

Table 61 - Number of Translation Entries by Translation Type

Translation Type	Translation Entries	Description
Single	1	Translates one IP address. Consists of the following: • One private IP address • One public IP address
Range	Multiple	Translates a range of IP addresses. Consists of the following: • One starting private IP address • One starting public IP address • Multiple entries that are based on the range you specify
Subnet	1	Translates all IP addresses within a subnet or portion of a subnet. Consists of the following: • One starting private IP address • One starting public IP address that is aligned on valid subnet boundaries • Subnet mask

EXAMPLE The following translation types count as 10 translation entries:

- Single translation for one device
- Range translation for eight devices
- Subnet translation for all devices on the subnet

Singe and range translation types have a one-to-one relationship between translations entries and addresses to be translated. However, subnet translations have a one-to-many relationship allowing one translation entry for many addresses.

Table 62 defines the maximum number of translation entries that are allowed per switch.

Table 62 - Maximum Translation Entries

Switch	Maximum Translation Entries
Stratix 5400 and Stratix 5700	128 across all NAT ports.
Stratix 5410	128 across NAT ports 1…6 and 13…18. and 128 across NAT ports 7…12, 19…24, and 25…28.

VLAN Assignments

When configuring NAT, you can assign one or more VLANs to a NAT instance. When you assign a VLAN to a NAT instance, the traffic that is associated with that VLAN is subject to the configuration parameters of the NAT instance. Configuration parameters include whether traffic is translated, fixed up, blocked, or passed through.

IMPORTANT Changes to the native VLAN on a port assigned to a NAT instance can break existing NAT configurations. If you change the VLAN assigned to a port associated with a NAT instance, you must reassign VLANs to that NAT instance.

Make sure all VLANs and Smartport roles are configured prior to NAT configuration.

When assigning VLANs to a NAT instance, consider the following:

- NAT supports both trunk ports and access ports.
- NAT does not change VLAN tags.
- You can assign a maximum of 128 VLANs to one or more instances.
- You can assign the same VLAN to multiple instances as long as the VLAN is associated with different ports. For example, you can assign VLAN 1 to both instance A and instance B. However, VLAN 1 must be associated with port Gi1/1 on instance A and port Gi1/2 on instance B.
- By default, each instance is assigned to all VLANs on port Gi1/1 and no instances on port Gi1/2.

VLANs associated with a trunk port can or cannot be assigned to a NAT instance:

- If a VLAN is assigned to a NAT instance, its traffic is subject to the configuration parameters of the NAT instance.
- If a VLAN is unassigned to a NAT instance, its traffic remains untranslated and is always permitted to pass through the trunk port.

Management Interface and VLANs

The management interface can be associated with a VLAN that is or is not assigned to a NAT instance:

- If its associated VLAN is assigned to a NAT instance, the management interface resides on the private subnet by default. To manage the switch from the private subnet, no additional configuration is required. To manage the switch from the public subnet, you must configure a private-to-public translation.

- If its associated VLAN is not assigned to a NAT instance, the traffic of the management interface remains untranslated and is always permitted to pass through the port.

Configuration Considerations

Consider these guidelines and limitations when configuring NAT:

- All switches can translate only IPv4 addresses.
- All switches can have a maximum of 128 NAT instances.
- Switch-specific features are shown in the following table.

Feature	Stratix 5700 Switch	Stratix 5400 Switch	Stratix 5410 Switch
Uplink Ports	2	4	4(2)
Downlink Ports	0	0	8(2)
Translation Entries(1)	128	128	256(3)

(1) A subnet translation counts as only one translation entry, but includes translations for many devices
(2) Both uplink and downlink ports can be configured for as many as 8 NAT ports.
(3) 128 entries across ports 1…6 and 13…18, plus 128 entries across ports 7…12, 19…24, and 25…28 for a total of 256 entries.

IMPORTANT Some NAT configurations can result in greater-than-expected traffic loads on both private and public subnets. Also, unintended traffic can be visible.

NAT is not a substitute for a firewall. Make sure that your configuration is performance qualified before use in a production environment.

Ports that are configured for NAT do **not** support the following across the NAT boundary due to embedded IP addresses that are not fixed up, encrypted IP addresses, or reliance on multicast traffic:

- Traffic encryption and integrity checking protocols incompatible with NAT, including IPsec Transport mode (1756-EN2TSC module)
- Applications that use dynamic session initiations, such as NetMeeting
- File transfer protocol (FTP)
- Microsoft Distributed Component Object Model (DCOM), which is used in Open Platform Communications (OPC)
- Multicast traffic, including applications that use multicast, such as CIP Sync (IEEE1588) and ControlLogix redundancy

Traffic Permits and Fixups

While a NAT-configured port can translate many types of traffic, only unicast and broadcast traffic are supported. You can choose to block or pass through the following unsupported traffic types:

- Untranslated unicast traffic
- Multicast traffic
- IGMP traffic

By default, all preceding traffic types are blocked.

Some traffic types must be fixed up to work properly with NAT because their packets contain embedded IP addresses. The switch supports fixups for these traffic types:

- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)

By default, fixups are enabled for both ARP and ICMP.

Configure NAT via Device Manager

To configure NAT, follow one of these procedures that are based on your application:

- Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router

  For an example of this application, see Figure 27 and Figure 30.
- Create NAT Instances for Traffic Routed through a Layer 2 Switch

  For an example of this application, see Figure 29 and Figure 30.

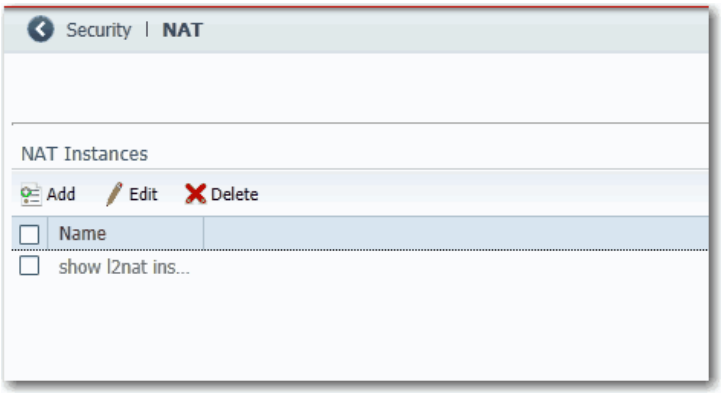
IMPORTANT	Configure all Smartport roles and VLANs before creating NAT instances. If you change a Smartport role or the native VLAN for a port that is associated with a NAT instance, you must reassign VLANs to the NAT instance.

IMPORTANT	As a result of Layer 2 forwarding, current traffic sessions remain established until manually disconnected. If you change an existing translation, you must manually disconnect all associated traffic sessions before the new translation can take effect.

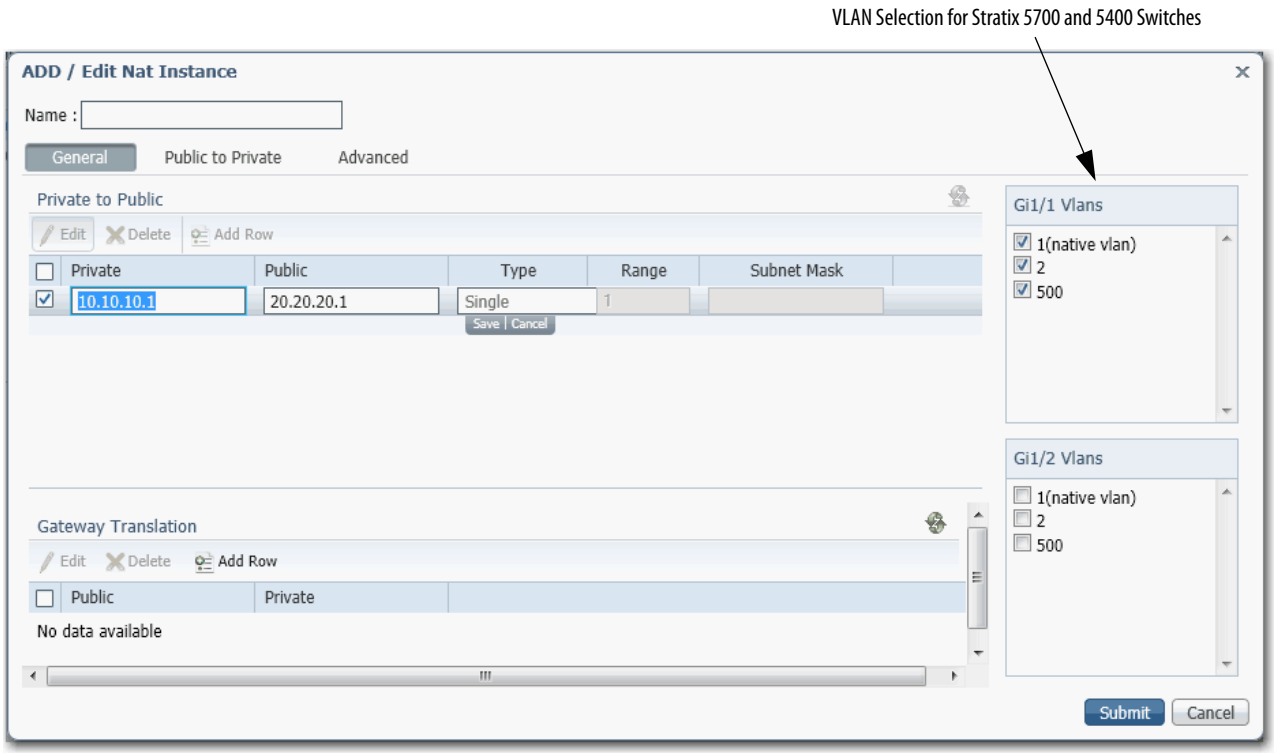
Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router

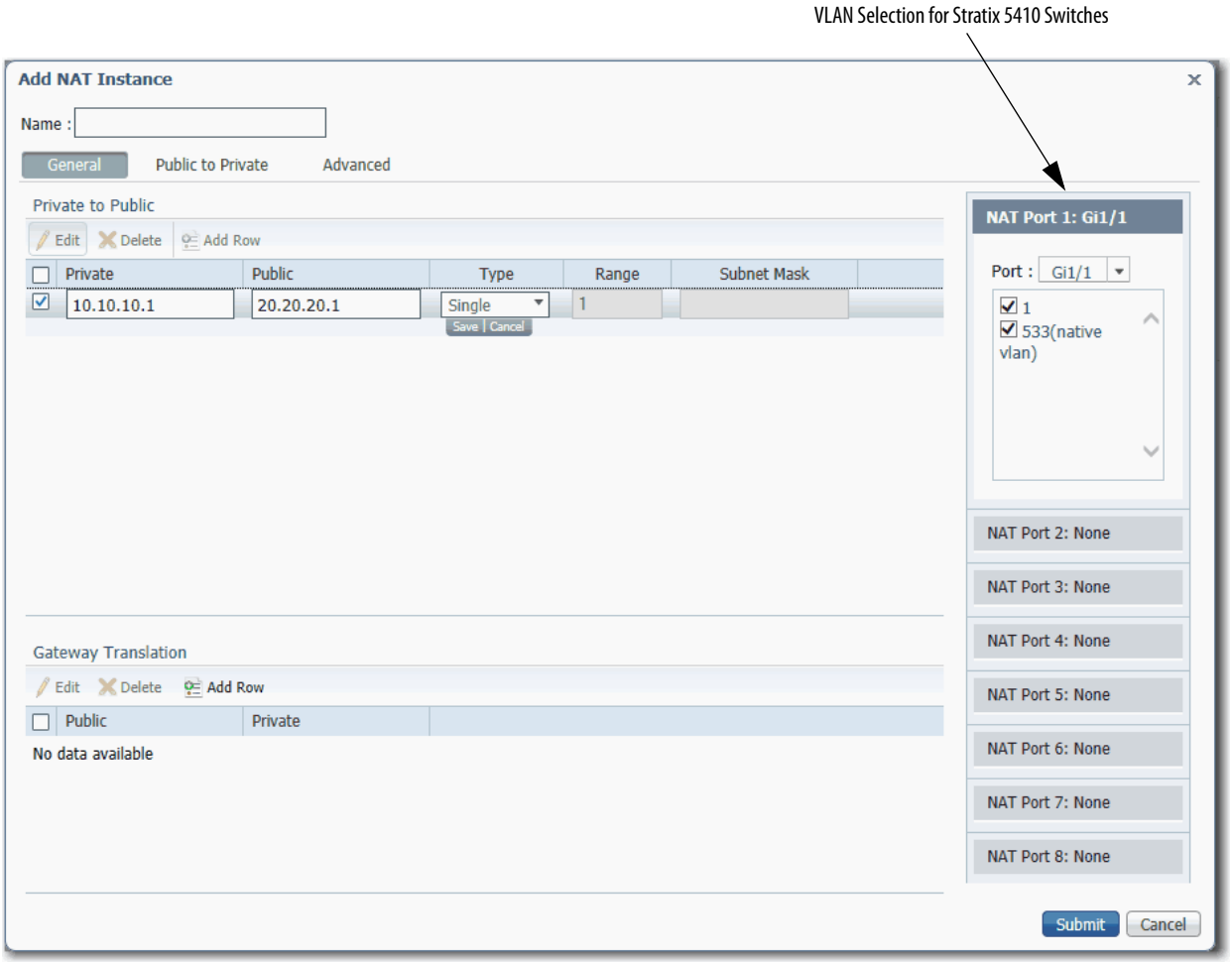
To create a NAT instance for traffic that is routed through a Layer 3 switch or router, follow these steps.

1. From the Configure menu, choose NAT to display the NAT window.



2. Click Add to display the General tab of the Add/Edit NAT Instance window.


VLAN Selection for Stratix 5700 and 5400 Switches
ADD / Edit Nat Instance
Name :
General
Public to Private
Advanced
Private to Public
Edit
Delete
Add Row
Private
Public
Type
Range
Subnet Mask
10.10.10.1
20.20.20.1
Single
1
Save | Cancel
Gi1/1 Vlans
1(native vlan)
2
500
Gi1/2 Vlans
1(native vlan)
2
500
Gateway Translation
Edit
Delete
Add Row
Public
Private
No data available
Submit
Cancel


VLAN Selection for Stratix 5410 Switches
Add NAT Instance
Name :
General
Public to Private
Advanced
Private to Public
Edit
Delete
Add Row
Private
Public
Type
Range
Subnet Mask
10.10.10.1
20.20.20.1
Single
1
Save | Cancel
NAT Port 1: Gi1/1
Port : Gi1/1
1
533(native vlan)
NAT Port 2: None
NAT Port 3: None
NAT Port 4: None
NAT Port 5: None
NAT Port 6: None
NAT Port 7: None
NAT Port 8: None
Gateway Translation
Edit
Delete
Add Row
Public
Private
No data available
Submit
Cancel

3. In the Name field, type a unique name to identify the instance.

   The instance name cannot include spaces or exceed 32 characters.

4. Complete VLAN assignments:
   - (Stratix 5700 and 5400 switches) For each uplink port on the right, select each VLAN to assign to the instance.
   - (Stratix 5410 switches) For each NAT port, choose an uplink or downlink port, and then select each VLAN to assign to the instance.

     The pull-down menu includes all ports (Gi1/1...Gi1/24 and Te1/25 ...Te1/28) and the default option None. When choosing ports, these rules apply:

     – You can configure as many as four NAT ports from Gi1/1...Gi1/6 and Gi1/13...Gi1/18.

     – You can configure as many as four NAT ports from Gi1/7...Gi1/12, Gi1/19...Gi1/24, and Te1/25...Te1/28.

     – If four ports from Gi 1/1...Gi 1/6 and Gi 1/13...Gi 1/18 are already in use, all other ports in that range are unavailable in subsequent port selection lists.

     – If you choose a downlink port, all uplink ports become unavailable, and if you choose an uplink port, all downlink ports become unavailable.

   For more information about VLAN assignments, see page 260.

5. In the Private to Public area, click Add Row, complete the fields, and click Save.

Field	Description	
Private IP Address	Type a private IP address: • To translate one address, type the existing address for the device on the private subnet. • To translate a range of addresses, type the first address in the range of sequential addresses. • To translate addresses in a subnet, type the existing starting address for a device on the private subnet. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	**Starting Private Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 192.168.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 192.168.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 192.168.1.0 or 192.168.1.128
	255.255.255.192	The last octet must end in one of the following: 0, 64, 128, 192. **EXAMPLE:** 192.168.1.64
	255.255.255.224	The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 192.168.1.32
	255.255.255.240	The last octet must end in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 192.168.1.16

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Public IP Address</td><td>Type a public IP address:
• To translate one address, type a unique public address to represent the device.
• To translate a range of addresses, type the first address in the range of sequential addresses.
• To translate addresses in a subnet, type a unique, starting public address to represent the devices. This address must correspond to the size of the subnet mask to translate.
<table>
<tr><th>Subnet Mask</th><th>Starting Public Subnet Address</th></tr>
<tr><td>255.255.0.0</td><td>The last two octets must end in 0.
EXAMPLE: 10.200.0.0</td></tr>
<tr><td>255.255.255.0</td><td>The last octet must end in 0.
EXAMPLE: 10.200.1.0.</td></tr>
<tr><td>255.255.255.128</td><td>The last octet must end in 0 or 128.
EXAMPLE: 10.200.1.0 or 10.200.1.128</td></tr>
<tr><td>255.255.255.192</td><td>The last octet must end in one of the following: 0, 64, 128, 192.
EXAMPLE: 10.200.1.64</td></tr>
<tr><td>255.255.255.224</td><td>The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224.
EXAMPLE: 10.200.1.32</td></tr>
<tr><td>255.255.255.240</td><td>The last octet must end in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXAMPLE: 10.200.1.16</td></tr>
</table></td></tr>
<tr><td>Type</td><td>Choose one of these values:
• Single—Translate one address.
• Range—Translate a range of addresses.
• Subnet—Translate all addresses in the private subnet or a portion of the private subnet.</td></tr>
<tr><td>Range</td><td>Type the number of addresses to translate. This field is available only if you choose Range in the Type field.
Valid values: 2…128
Default value = 1
IMPORTANT: Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.</td></tr>
<tr><td>Subnet Mask</td><td>Type the subnet mask for the addresses to translate.
Valid values:
• Class B: 255.255.0.0
• Class C: 255.255.255.0
• Portion of Class C:
– 255.255.255.128 (provides 128 addresses per translation entry)
– 255.255.255.192 (provides 64 addresses per translation entry)
– 255.255.255.224 (provides 32 addresses per translation entry)
– 255.255.255.240 (provides 16 addresses per translation entry)</td></tr>
</table>

6. In the Gateway Translation area, click Add Row, complete the fields, and click Save.

   The gateway translation enables devices on the public subnet to communicate with devices on the private subnet.

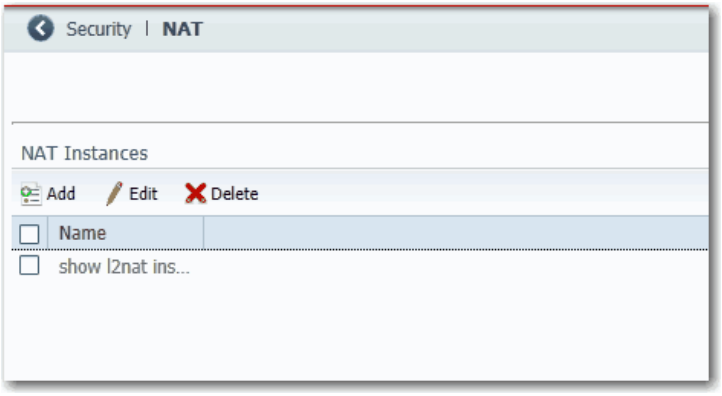
Field	Description
Public	Type the default gateway address of the Layer 3 switch or router that is connected to the uplink port of the switch.
Private	Type a unique IP address to represent the Layer 3 switch or router on the private network.

7. (Optional). To configure traffic permits and packet fixups, see Configure Traffic Permits and Fixups on page 273.
8. Click Submit.

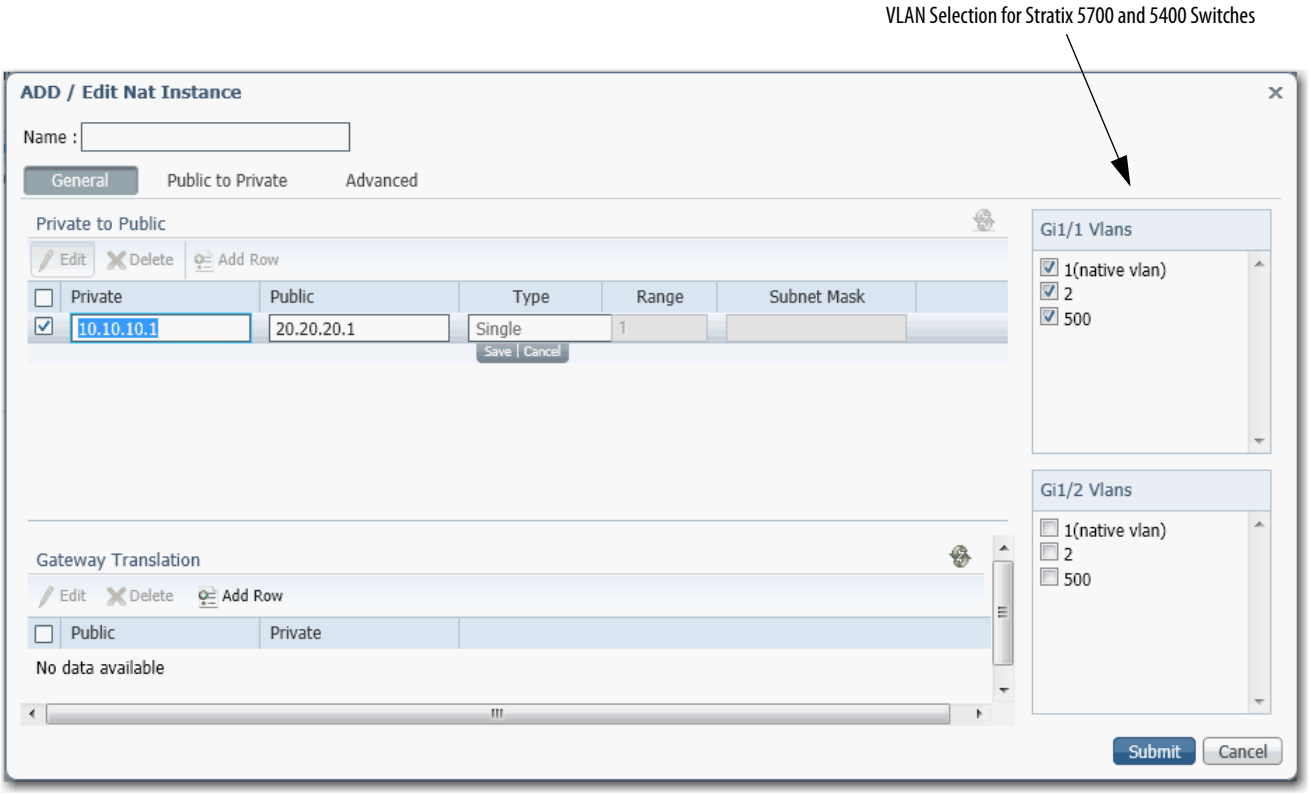
Create NAT Instances for Traffic Routed through a Layer 2 Switch

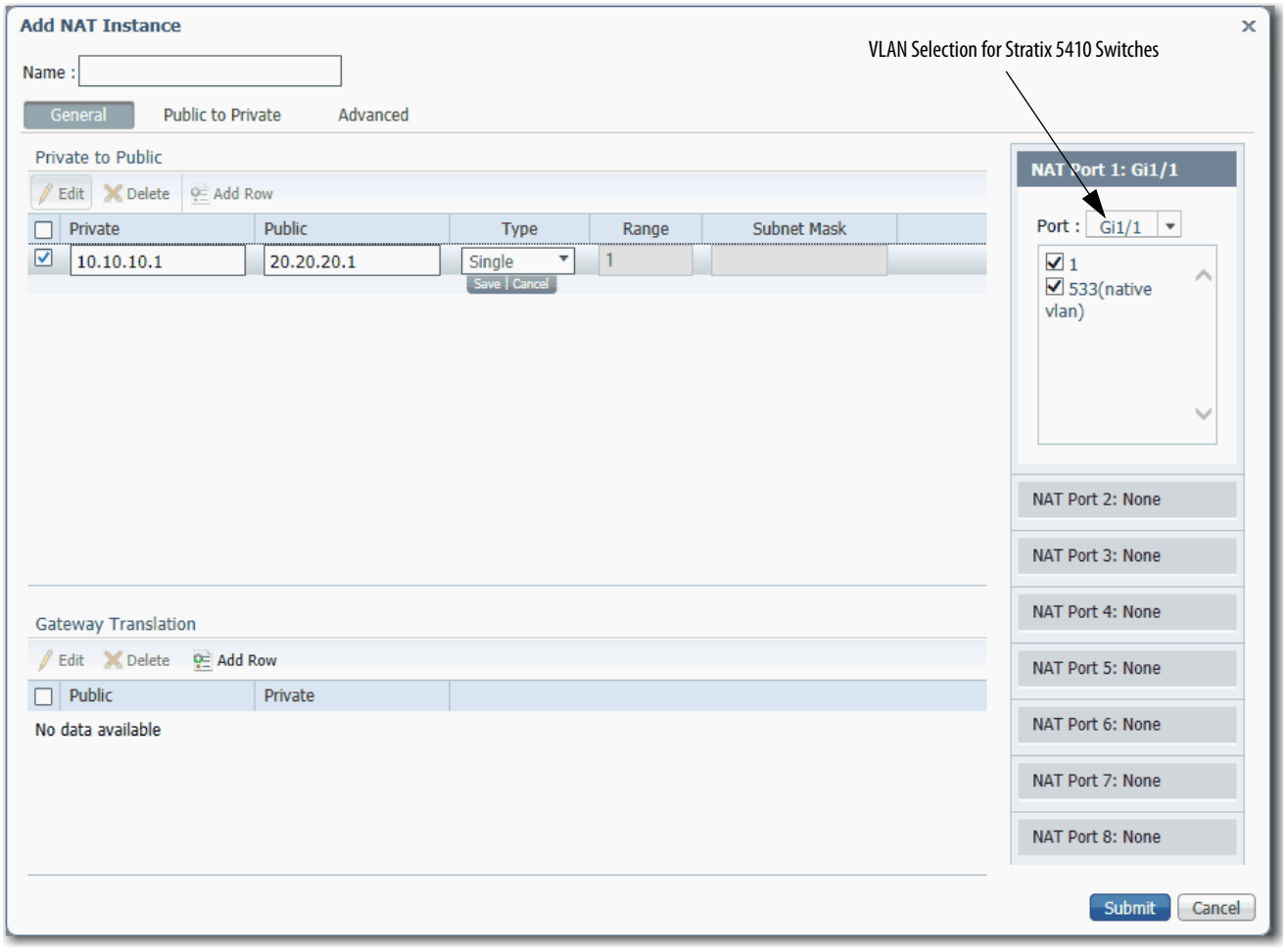
To create a NAT instance for traffic that is routed through a Layer 2 switch, follow these steps.

1. From the Configure menu, choose NAT to display the NAT window.



2. Click Add to display the General tab of the Add/Edit NAT Instance window.


VLAN Selection for Stratix 5700 and 5400 Switches
ADD / Edit Nat Instance
Name :
General
Public to Private
Advanced
Private to Public
Edit
Delete
Add Row
Private
Public
Type
Range
Subnet Mask
10.10.10.1
20.20.20.1
Single
1
Save | Cancel
Gi1/1 Vlans
1(native vlan)
2
500
Gi1/2 Vlans
1(native vlan)
2
500
Gateway Translation
Edit
Delete
Add Row
Public
Private
No data available
Submit
Cancel


Add NAT Instance
VLAN Selection for Stratix 5410 Switches
Name :
General
Public to Private
Advanced
Private to Public
Edit
Delete
Add Row
Private
Public
Type
Range
Subnet Mask
10.10.10.1
20.20.20.1
Single
1
Save | Cancel
NAT Port 1: Gi1/1
Port : Gi1/1
1
533(native vlan)
NAT Port 2: None
NAT Port 3: None
NAT Port 4: None
NAT Port 5: None
NAT Port 6: None
NAT Port 7: None
NAT Port 8: None
Gateway Translation
Edit
Delete
Add Row
Public
Private
No data available
Submit
Cancel

3. In the Name field, type a unique name to identify the instance.

   The instance name cannot include spaces or exceed 32 characters.

4. Complete VLAN assignments:
   - (Stratix 5700 and 5400 switches) For each uplink port on the right, select each VLAN to assign to the instance.
   - (Stratix 5410 switches) For each NAT port, choose an uplink or downlink port, and then select each VLAN to assign to the instance.

     The pull-down menu list includes all ports (Gi1/1...Gi1/24 and Te1/25 ...Te1/28) and the default option None. When choosing ports, these rules apply:

     – You can configure up to four NAT ports from Gi1/1...Gi1/6 and Gi1/13...Gi1/18.

     – You can configure up to four NAT ports from Gi1/7...Gi1/12, Gi1/19...Gi1/24, and Te1/25...Te1/28.

     – If four ports from Gi 1/1...Gi 1/6 and Gi 1/13...Gi 1/18 are already in use, all other ports in that range are unavailable in subsequent port selection lists.

     – If you choose a downlink port, all uplink ports become unavailable, and if you choose an uplink port, all downlink ports become unavailable.

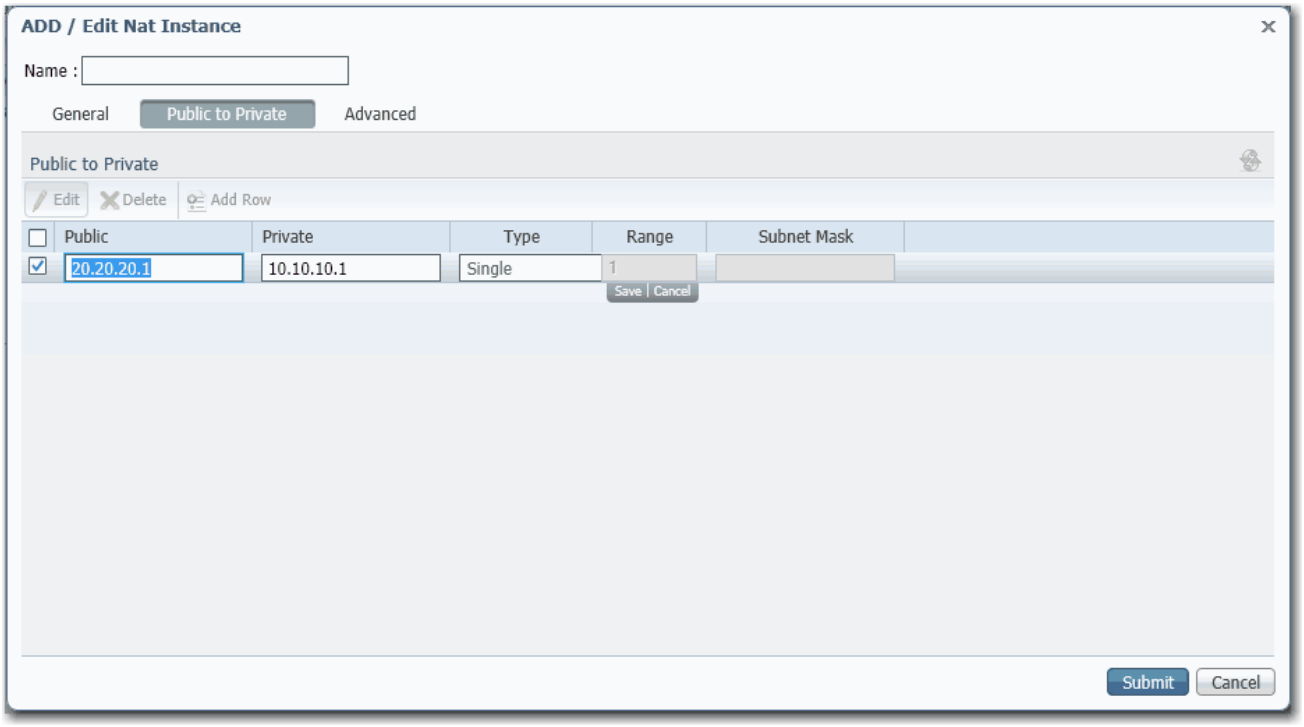
   For more information about VLAN assignments, see page 260.

5. In the Private to Public area, click Add Row, complete the fields, and click Save.

Field	Description	
Private IP Address	Type a private IP address: • To translate one address, type the existing address for the device on the private subnet. • To translate a range of addresses, type the first address in the range of sequential addresses. • To translate addresses in a subnet, type the existing starting address for a device on the private subnet. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	**Starting Private Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 192.168.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 192.168.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 192.168.1.0 or 192.168.1.128
	255.255.255.192	The last octet must end in one of the following: 0, 64, 128, 192. **EXAMPLE:** 192.168.1.64
	255.255.255.224	The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 192.168.1.32
	255.255.255.240	The last octet must end in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 192.168.1.16

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Public IP Address</td><td>Type a public IP address:
• To translate one address, type a unique public address to represent the device.
• To translate a range of addresses, type the first address in the range of sequential addresses.
• To translate addresses in a subnet, type a unique, starting public address to represent the devices. This address must correspond to the size of the subnet mask to translate.
<table><tr><th>Subnet Mask</th><th>Starting Public Subnet Address</th></tr><tr><td>255.255.0.0</td><td>The last two octets must end in 0.
EXAMPLE: 10.200.0.0</td></tr><tr><td>255.255.255.0</td><td>The last octet must end in 0.
EXAMPLE: 10.200.1.0.</td></tr><tr><td>255.255.255.128</td><td>The last octet must end in 0 or 128.
EXAMPLE: 10.200.1.0 or 10.200.1.128</td></tr><tr><td>255.255.255.192</td><td>The last octet must in one of the following: 0, 64, 128, 192.
EXAMPLE: 10.200.1.64</td></tr><tr><td>255.255.255.224</td><td>The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224.
EXAMPLE: 10.200.1.32</td></tr><tr><td>255.255.255.240</td><td>The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXAMPLE: 10.200.1.16</td></tr></table></td></tr>
<tr><td>Type</td><td>Choose one of these values:
• Single—Translate one address.
• Range—Translate a range of addresses.
• Subnet—Translate all addresses in the private subnet or a portion of the private subnet.</td></tr>
<tr><td>Range</td><td>Type the number of addresses to translate. This field is available only if you choose Range in the Type field.
Valid values: 2…128
Default value = 1
IMPORTANT: Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.</td></tr>
<tr><td>Subnet Mask</td><td>Type the subnet mask for the addresses to translate.
Valid values:
• Class B: 255.255.0.0
• Class C: 255.255.255.0
• Portion of Class C:
– 255.255.255.128 (provides 128 addresses per translation entry
– 255.255.255.192 (provides 64 addresses per translation entry
– 255.255.255.224 (provides 32 addresses per translation entry
– 255.255.255.240 (provides 16 addresses per translation entry)</td></tr>
</table>

6. Click the Public to Private tab.



7. Click Add Row, complete the fields, and click Save.

Field	Description	
Public IP Address	Type a public IP address: • To translate one address, type the existing address for the device on the public subnet. • To translate a range of addresses, type the first address in the range of sequential addresses. • To translate addresses in a subnet, type the existing starting address for the range of devices on the public subnet. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	**Starting Public Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 10.200.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 10.200.1.0.
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 10.200.1.0 or 10.200.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 10.200.1.16

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Private IP Address</td><td>Type a private IP address:
• To translate one address, type a unique private address to represent the device.
• To translate a range of addresses, type the first address in the range of sequential addresses.
• To translate addresses in a subnet, type a unique, starting private address to represent the devices. This address must correspond to the size of the subnet mask to translate.
<table><tr><th>Subnet Mask</th><th>Starting Private Subnet Address</th></tr><tr><td>255.255.0.0</td><td>The last two octets must end in 0.
EXAMPLE: 192.168.0.0</td></tr><tr><td>255.255.255.0</td><td>The last octet must end in 0.
EXAMPLE: 192.168.1.0</td></tr><tr><td>255.255.255.128</td><td>The last octet must end in 0 or 128.
EXAMPLE: 192.168.1.0 or 192.168.1.128</td></tr><tr><td>255.255.255.192</td><td>The last octet must in one of the following: 0, 64, 128, 192.
EXAMPLE: 192.168.1.64</td></tr><tr><td>255.255.255.224</td><td>The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224.
EXAMPLE: 192.168.1.32</td></tr><tr><td>255.255.255.240</td><td>The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXAMPLE: 10.200.1.16</td></tr></table></td></tr>
<tr><td>Type</td><td>Choose one of these values:
• Single—Translate one address.
• Range—Translate a range of addresses.
• Subnet—Translate all addresses in the public subnet or a portion of the public subnet.</td></tr>
<tr><td>Range</td><td>Type the number of addresses to translate. This field is available only if you choose Range in the Type field.
Valid values: 2…128
Default value = 1
IMPORTANT: Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.</td></tr>
<tr><td>Subnet Mask</td><td>Type the subnet mask for the addresses to translate.
Valid values:
• Class B: 255.255.0.0
• Class C: 255.255.255.0
• Portion of Class C:
– 255.255.255.128 (provides 128 addresses per translation entry
– 255.255.255.192 (provides 64 addresses per translation entry
– 255.255.255.224 (provides 32 addresses per translation entry
– 255.255.255.240 (provides 16 addresses per translation entry)</td></tr>
</table>

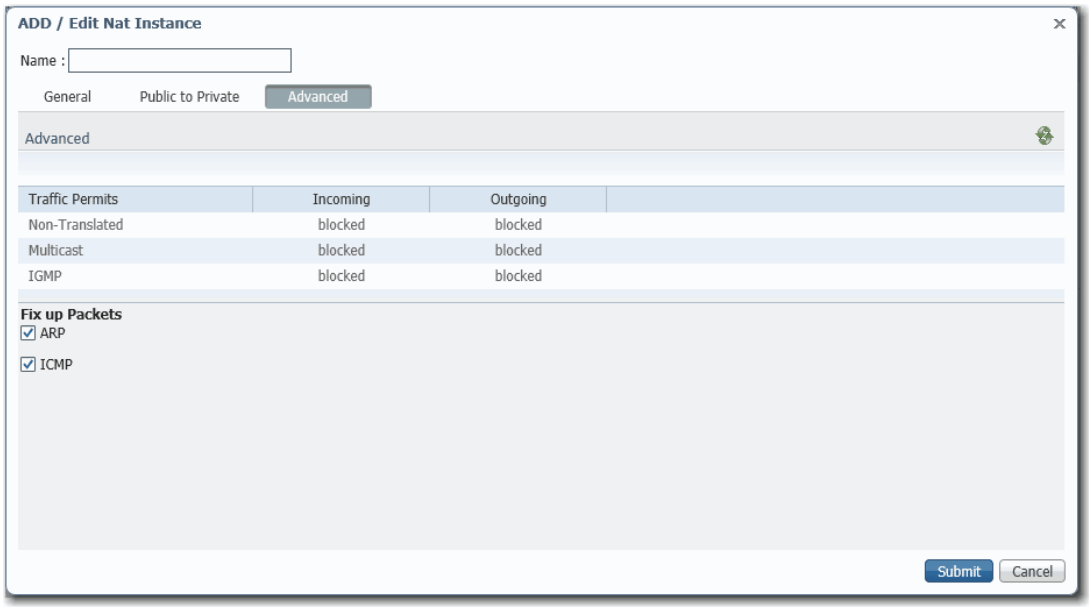
8. (Optional). To configure traffic permits and packet fixups, see Configure Traffic Permits and Fixups.
9. On the NAT window, click Submit.

Configure Traffic Permits and Fixups

Use caution when you configure traffic permits and fixups. We recommend that you use the default values.

To configure traffic permits or fixups, follow these steps.

1. Click the Advanced tab.



2. Choose one of these options for incoming and outgoing packets that are not handled by NAT:
   - Pass-through—Permit the packets to pass across the NAT boundary.
   - Blocked—Drop the packets.
3. In the Fix up Packets area, check or clear the checkboxes to enable or disable fixups for ARP and ICMP.

   By default, fixups are enabled for both ARP and ICMP.
4. Click Submit.

Configure NAT via the Logix Designer Application

For Stratix 5410 switches, see page 286.

In the navigation pane, click NAT.

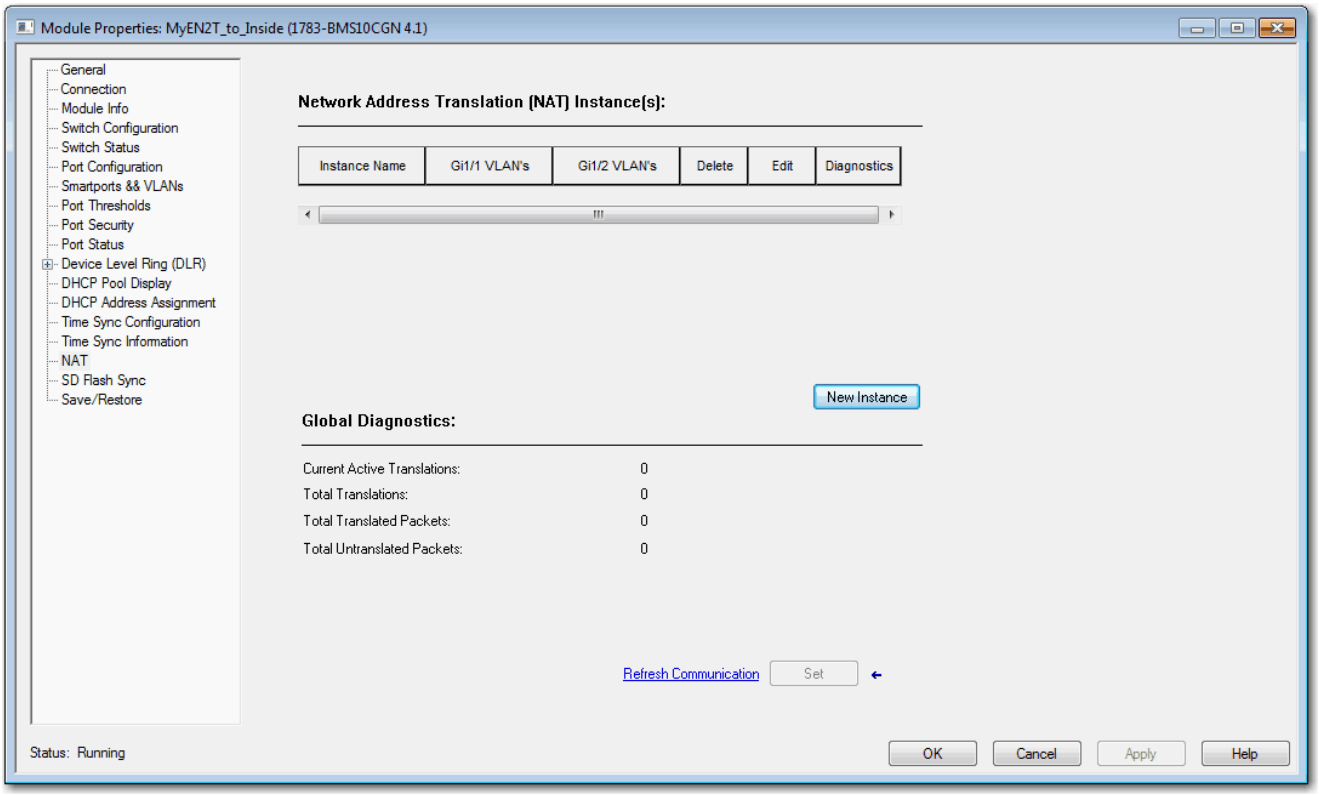


Table 63 - NAT Fields

Field	Description
Instance Name	Displays the unique name of the NAT instance.
Gi1/1 VLANs	Displays the VLANs assigned to each NAT instance on port Gi1/1.
Gi1/2 VLANs	Displays the VLANs assigned to each NAT instance on port Gi1/2.
Delete	Click to delete a NAT instance permanently. The switch deletes the instance when you click Set.
Edit	Click to modify the configuration of a NAT instance.
Diagnostics	Click to view translation diagnostics for an instance. See Monitor NAT Statistics via the Logix Designer Application on page 399.
Global Diagnostics	
Current Active Translations	Displays the total number of translations that occurred within the last 90 seconds across all NAT instances.
Total Translations	Displays the total number of translations across all NAT instances.
Total Translated Packets	Displays the total number of translated packets across all NAT instances.
Total Untranslated Packets	Displays the total number of packets that have been bypassed across all NAT instances.

To configure NAT, follow one of these procedures that are based on your application:

- Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router

  For an example of this application, see Figure 28 on page 256.
- Create NAT Instances for Traffic Routed through a Layer 2 Switch

  For an example of this application, see Figure 29 on page 257.

IMPORTANT Configure all Smartport roles and VLANs before creating NAT instances.

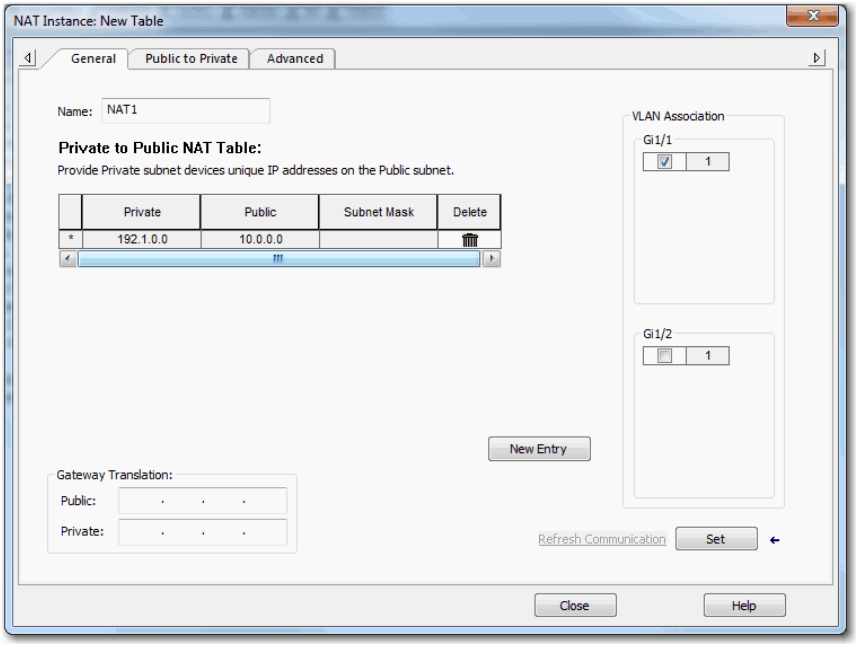
If you change a Smartport role or the native VLAN for a port that is associated with a NAT instance, you must reassign VLANs to the NAT instance.

IMPORTANT As a result of Layer 2 forwarding, current traffic sessions remain established until manually disconnected. If you change an existing translation, you must manually disconnect all associated traffic sessions before the new translation can take effect.

Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router

To create a NAT instance for traffic that is routed through a Layer 3 switch or router, follow these steps.

1. From the NAT view, click New Instance to display the General tab.



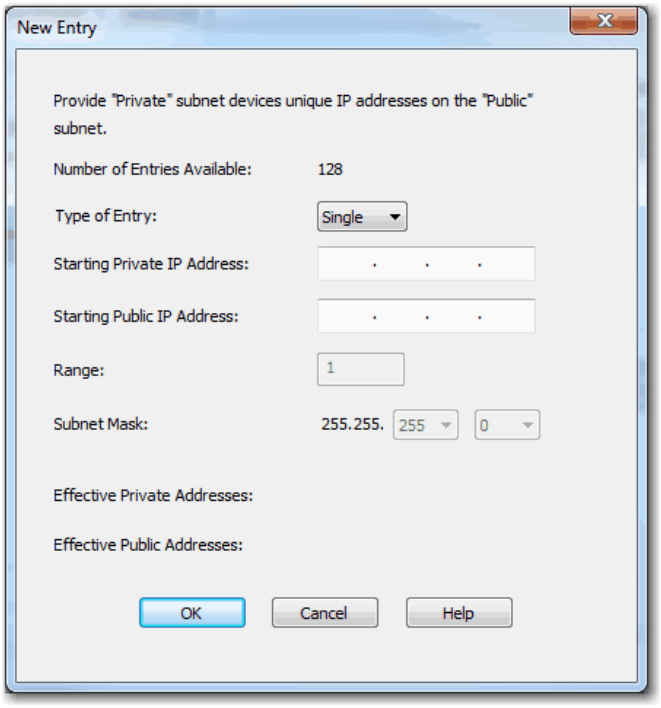
2. In the Name field, type a unique name to identify the instance.

   The instance name cannot include spaces or exceed 32 characters.

3. In the VLAN Association area, check the checkbox next to each VLAN to assign to the instance.

   For more information about VLAN assignments, see page 260.

4. Click New Entry to display the New Entry dialog box.



5. Do one of the following:
   - To translate one address for a device on the private subnet that communicates on the public subnet, see Table 64.
   - To translate a range of addresses for devices on the private subnet that communicates on the public subnet, see Table 65.
   - To translate all addresses in the private subnet or a portion of the private subnet, see Table 66.

Table 64 - Single Translation

Field	Description
Type of Entry	Choose Single. Single is the default value.
Starting Private IP Address	Type the existing address for the device on the private subnet.
Starting Public IP Address	Type a unique public address to represent the device.
Effective Private Addresses	Displays the existing address for the device on the private subnet that is configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Public Addresses	Displays the unique public address to represent the device. If blank, verify that the values in the preceding fields are valid.

Table 65 - Range Translation

Field	Description
Type of Entry	Choose Range.
Starting Private IP Address	Type the existing starting address for the device on the private subnet.
Starting Public IP Address	Type a unique, starting public address to represent the device.
Range	Type the number of addresses to include in the range. Valid values: 2…128 Default value = 1 **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.

Table 66 - Subnet Translation

Field	Description	
Type of Entry	Choose Subnet.	
Starting Private IP Address	Type the existing starting address for a device on the private subnet. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	**Starting Private Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 192.168.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 192.168.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 192.168.1.0 or 192.168.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 192.168.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 192.168.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 192.168.1.16
Starting Public IP Address	Type a unique, starting public address to represent the devices. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	**Starting Public Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 10.200.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 10.200.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 10.200.1.0 or 10.200.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 10.200.1.16

Table 66 - Subnet Translation (Continued)

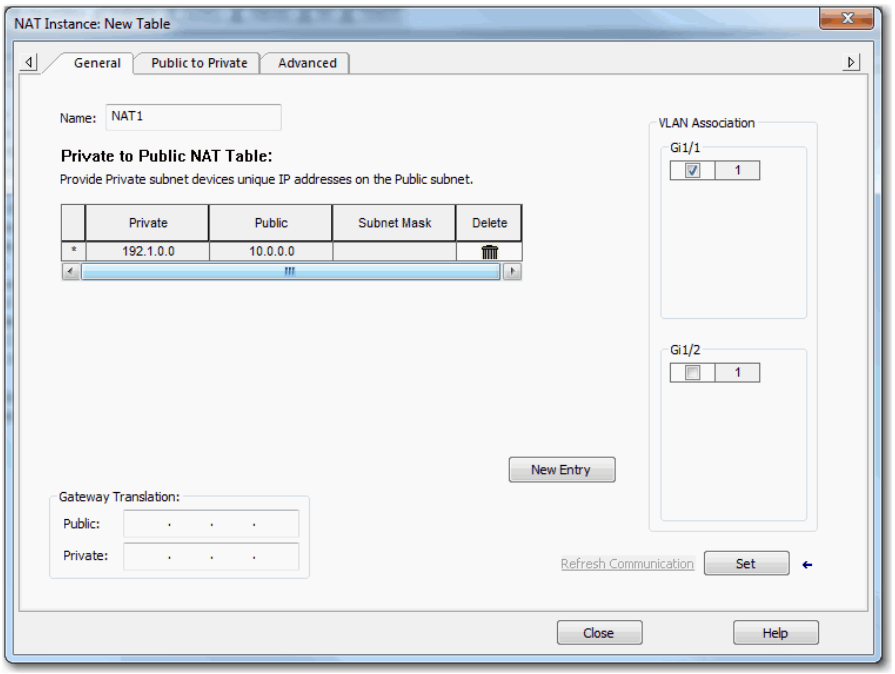
Field	Description
Subnet Mask	Choose the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry – 255.255.255.192 (provides 64 addresses per translation entry – 255.255.255.224 (provides 32 addresses per translation entry – 255.255.255.240 (provides 16 addresses per translation entry)
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.

6. Click OK.
7. Complete the Gateway Translation fields to enable devices on the public subnet to communicate with devices on the private subnet:
   - Public—Type the default gateway address of the Layer 3 switch or router that is connected to the uplink port of the switch.
   - Private—Type a unique IP address to represent the Layer 3 switch or router on the private network.
8. To configure traffic permits and packet fixups, see Configure Traffic Permits and Fixups on page 273.
9. Click Set.

Create NAT Instances for Traffic Routed through a Layer 2 Switch

To create a NAT instance for traffic that is routed through a Layer 2 switch, follow these steps.

1. From the NAT view, click New Instance to display the General tab.



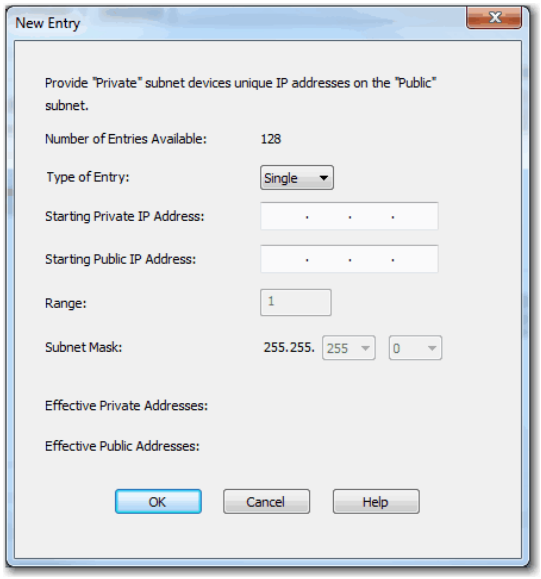
2. In the Name field, type a unique name to identify the instance.

   The instance name cannot include spaces or exceed 32 characters.

3. In the VLAN Association area, check the checkbox next to each VLAN to assign to the instance.

   For more information about VLAN assignments, see page 260.

4. Click New Entry to display the New Entry dialog box.



5. Do one of the following:
   - To translate one address for a device on the private subnet that communicates on the public subnet, see Table 67.
   - To translate a range of addresses for devices on the private subnet that communicates on the public subnet, see Table 68
   - To translate all addresses in the private subnet or a portion of the private subnet, see Table 69.

Table 67 - Single Translation

Field	Description
Type of Entry	Choose Single. Single is the default value.
Starting Private IP Address	Type the existing address for the device on the private subnet.
Starting Public IP Address	Type a unique public address to represent the device.
Effective Private Addresses	Displays the existing address for the device on the private subnet that is configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Public Addresses	Displays the unique public address to represent the device. If blank, verify that the values in the preceding fields are valid.

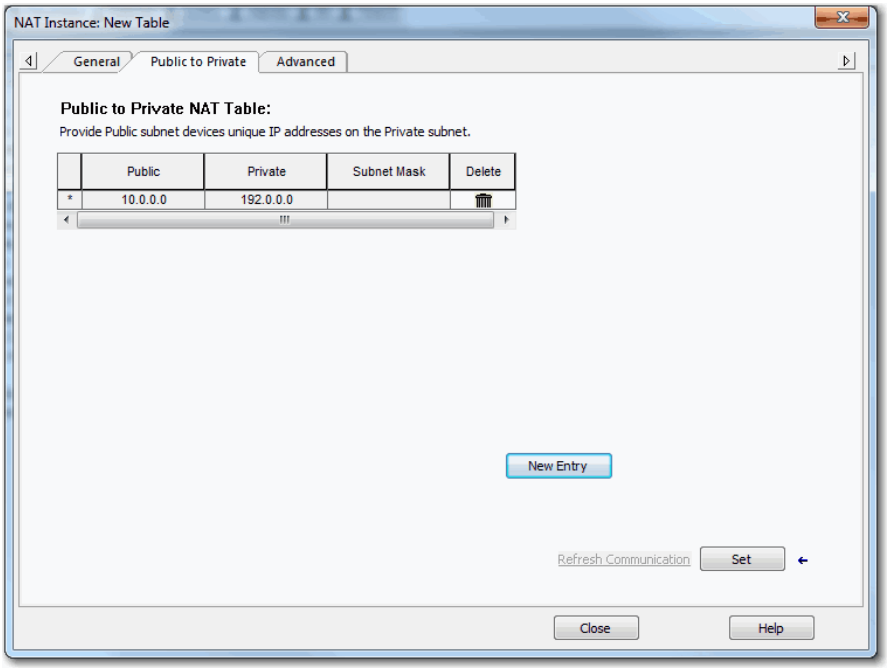
Table 68 - Range Translation

Field	Description
Type of Entry	Choose Range.
Starting Private IP Address	Type the existing starting address for the device on the private subnet.
Starting Public IP Address	Type a unique, starting public address to represent the devices.
Range	Type the number of addresses to include in the range. Valid values: 2…128 Default value = 1 **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.

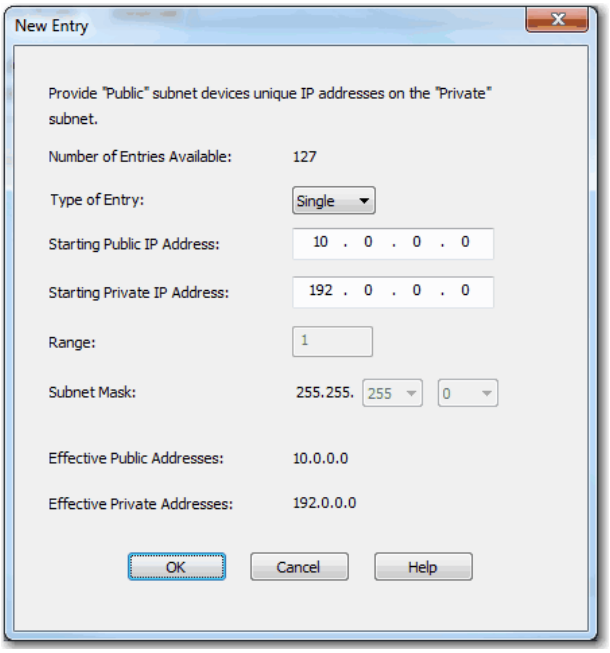
Table 69 - Subnet Translation

Field	Description	
Type of Entry	Choose Subnet.	
Starting Private IP Address	Type the existing starting address for a device on the private subnet. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	**Starting Private Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 192.168.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 192.168.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 192.168.1.0 or 192.168.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 192.168.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 192.168.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 192.168.1.16
Starting Public IP Address	Type a unique, starting public address to represent the devices. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	**Starting Public Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 10.200.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 10.200.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 10.200.1.0 or 10.200.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 10.200.1.16
Subnet Mask	Choose the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry – 255.255.255.192 (provides 64 addresses per translation entry – 255.255.255.224 (provides 32 addresses per translation entry – 255.255.255.240 (provides 16 addresses per translation entry)	
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.	
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.	

6. Click OK.
7. Click the Public to Private tab.



8. Click New Entry to display the New Entry dialog box.



9. Do one of the following:
   - To translate one address for a device on the public subnet that communicates on the private subnet, see Table 70.
   - To translate a range of addresses for devices on the public subnet that communicates on the private subnet, see Table 71.
   - To translate a range of addresses for devices on the public subnet that communicates on the private subnet, seeTable 72.

Table 70 - Single Translation

Field	Description
Type of Entry	Choose Single. Single is the default value.
Starting Public IP Address	Type the existing address for the device on the public subnet.
Starting Private IP Address	Type a unique private address to represent the device.
Effective Public Addresses	Displays the existing address for the device on the public subnet that is configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Private Addresses	Displays the unique private address to represent the device. If blank, verify that the values in the preceding fields are valid.

Table 71 - Range Translation

Field	Description
Type of Entry	Choose Range.
Starting Public IP Address	Type the existing starting address for the device on the public subnet.
Starting Private IP Address	Type a unique, starting private address to represent the devices.
Range	Type the number of addresses to include in the range. Valid values: 2…128 Default value = 1 **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Effective Public Addresses	Displays the range of existing addresses for devices on the public subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Private Addresses	Displays the range of unique private addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.

Table 72 - Subnet Translation

Field	Description	
Type of Entry	Choose Subnet.	
Starting Public IP Address	Type the existing starting address for a device on the public subnet. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	**Starting Public Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 10.200.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 10.200.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 10.200.1.0 or 10.200.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 10.200.1.16

Table 72 - Subnet Translation (Continued)

Field	Description	
Starting Private IP Address	Type a unique, starting private address to represent the devices. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	**Starting Private Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 192.168.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 192.168.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 192.168.1.0 or 192.168.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 192.168.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 192.168.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 192.168.1.16
Subnet Mask	Choose the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry – 255.255.255.192 (provides 64 addresses per translation entry – 255.255.255.224 (provides 32 addresses per translation entry – 255.255.255.240 (provides 16 addresses per translation entry)	
Effective Public Addresses	Displays the range of existing addresses for devices on the public subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.	
Effective Private Addresses	Displays the range of unique private addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.	

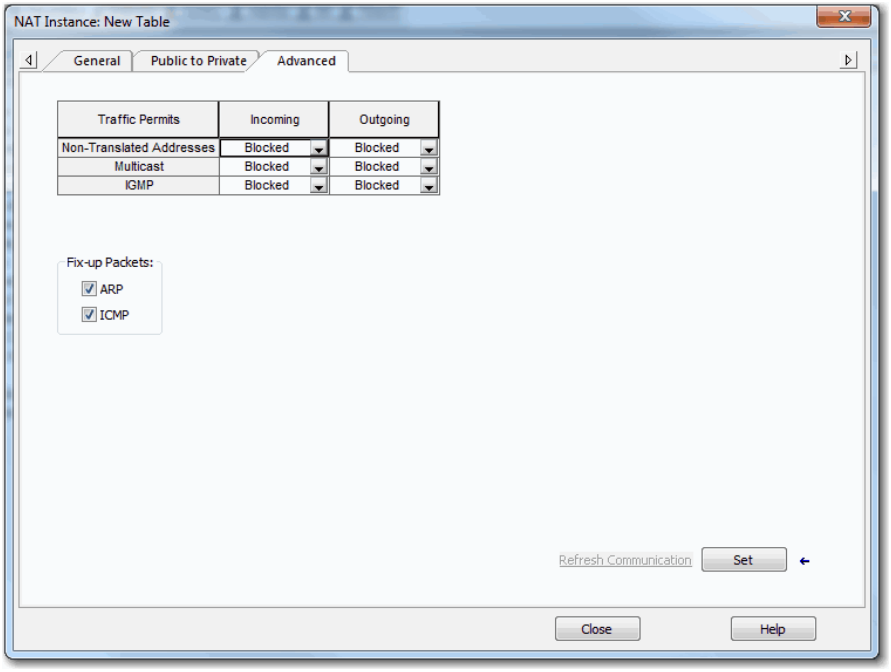
10. Click OK.
11. (Optional). To configure traffic permits and packet fixups, see Configure Traffic Permits and Fixups on page 273.
12. Click Set.

Configure Traffic Permits and Fixups

Use caution when you configure traffic permits and fixups. We recommend that you use the default values.

To configure traffic permits or packet fixups, follow these steps.

1. Click the Advanced tab.



2. In the Traffic Permits table, choose one of these options for unsupported incoming and outgoing packets:
   - Pass-Through—Permit the packets to pass across the NAT boundary.
   - Blocked—Drop the packets.
3. In the Fix-up Packets area, check or clear the checkboxes to enable or disable protocol fixups for ARP and ICMP.

   By default, fixups are enabled for both ARP and ICMP.

Configure NAT via the Logix Designer Application (Stratix 5410 Switches)

In the navigation pane, click NAT.

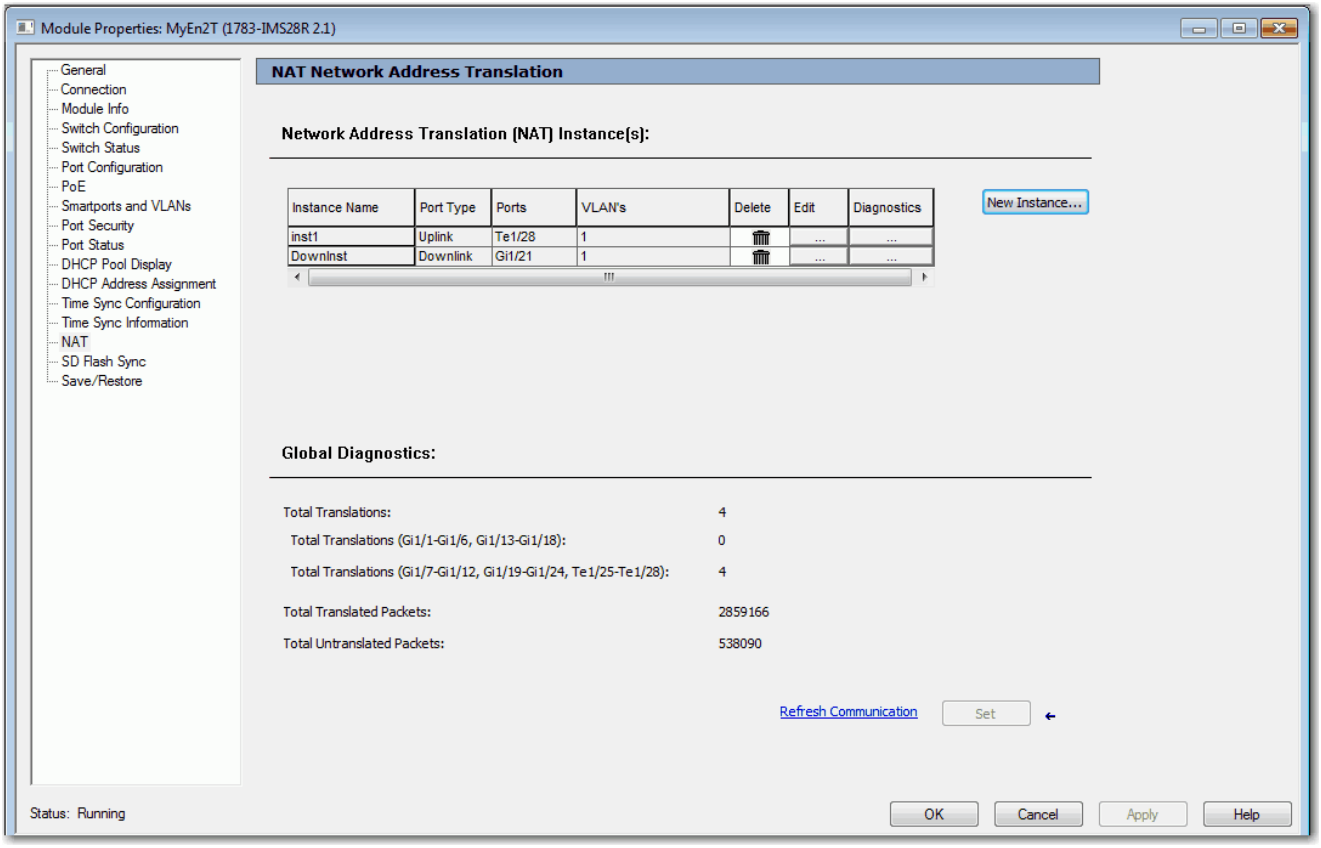


Table 73 - NAT Fields

Field	Description
Instance Name	Displays the unique name of the NAT instance.
Port Type	Identifies the port type as either uplink or downlink: • Ports 1…24 are downlink ports. • Ports 25…28 are uplink ports.
Ports	Identifies the port numbers that are assigned to each NAT instance.
VLANs	Displays the VLANs assigned to each NAT instance on port listed in the Port column.
Delete	Click to delete a NAT instance permanently. The switch deletes the instance when you click Set.
Edit	Click to modify the configuration of a NAT instance.
Diagnostics	Click to view translation diagnostics for an instance. See Monitor NAT Statistics via the Logix Designer Application on page 399.
Global Diagnostics	
Total Translations	Displays the total number of translations across all NAT instances.
Total Translations (Gi1/1-Gi1/6, Gi1/13-Gi1/18)	Displays the total number of translations across port ranges Gi1/1…Gi1/6 and Gi1/13…Gi1/18. These ranges can include a combined maximum of 128 translations.
Total Translations (Gi1/7-Gi1/12, Gi1/19-Gi1/24, Te1/25-Te1/28)	Displays the total number of translations across port ranges Gi1/7…Gi1/12, Gi1/19…Gi1/24 and Te1/25…Te1/28. These ranges can include a combined maximum of 128 translations.
Total Translated Packets	Displays the total number of translated packets across all NAT instances.
Total Untranslated Packets	Displays the total number of packets that have passed throughl all NAT instances without being translated.

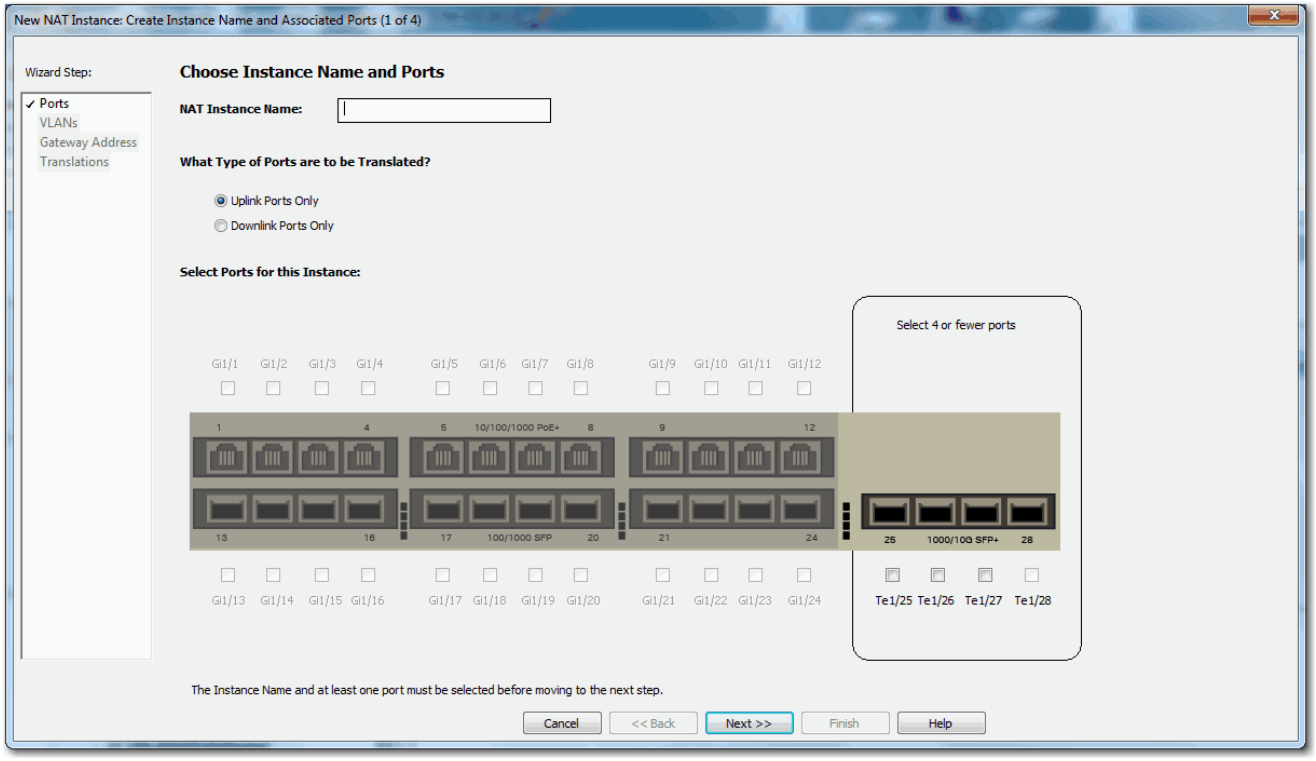
To create a NAT instance, follow these steps.

IMPORTANT Configure all Smartport roles and VLANs before creating NAT instances.

If you change a Smartport role or the native VLAN for a port that is associated with a NAT instance, you must reassign VLANs to the NAT instance.

IMPORTANT As a result of Layer 2 forwarding, current traffic sessions remain established until manually disconnected. If you change an existing translation, you must manually disconnect all associated traffic sessions before the new translation can take effect.

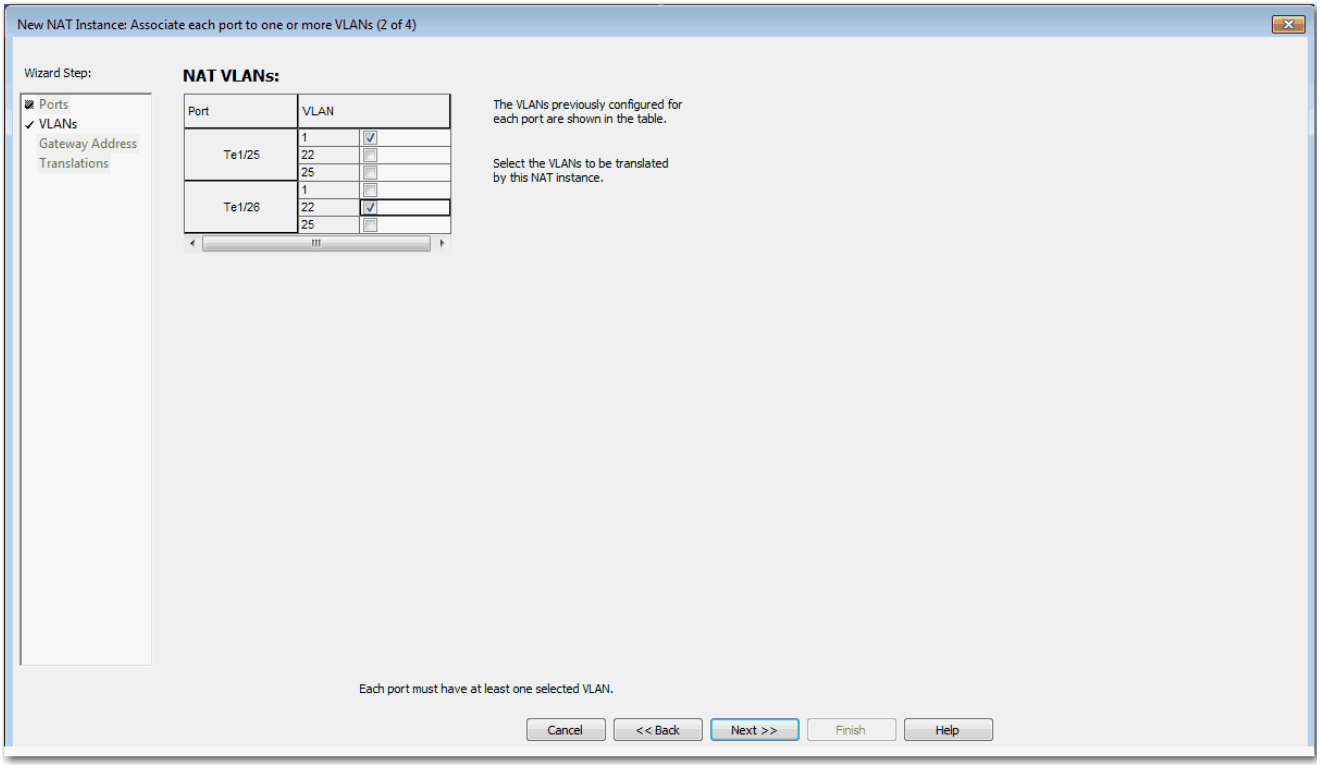
1. From the NAT view, click New Instance to display the Ports view.



2. Configure the ports to assign to the instance.
   a. In the NAT Instance Name field, type a unique name to identify the instance.
   b. Click the type of ports to assign to the NAT instance:
      •Uplink Ports Only (Te1/25...Te1/28)
      •(Default) Downlink Ports Only (Gi1/1...Gi1/24)
   c. Select the ports to assign to the NAT instance.

Port Type	Valid Port Ranges
Downlink	Select as many as eight downlink ports. Select four or fewer ports from these ranges: • Gi1/1…Gi1/6 • Gi1/13…Gi1/18 Select four or fewer ports from these ranges: • Gi1/7…Gi1/12 • Gi1/19…Gi1/24
or	
Uplink	Select four or fewer ports from this range: Te1/25…Te1/28

3. Click Next to display the VLANs view.



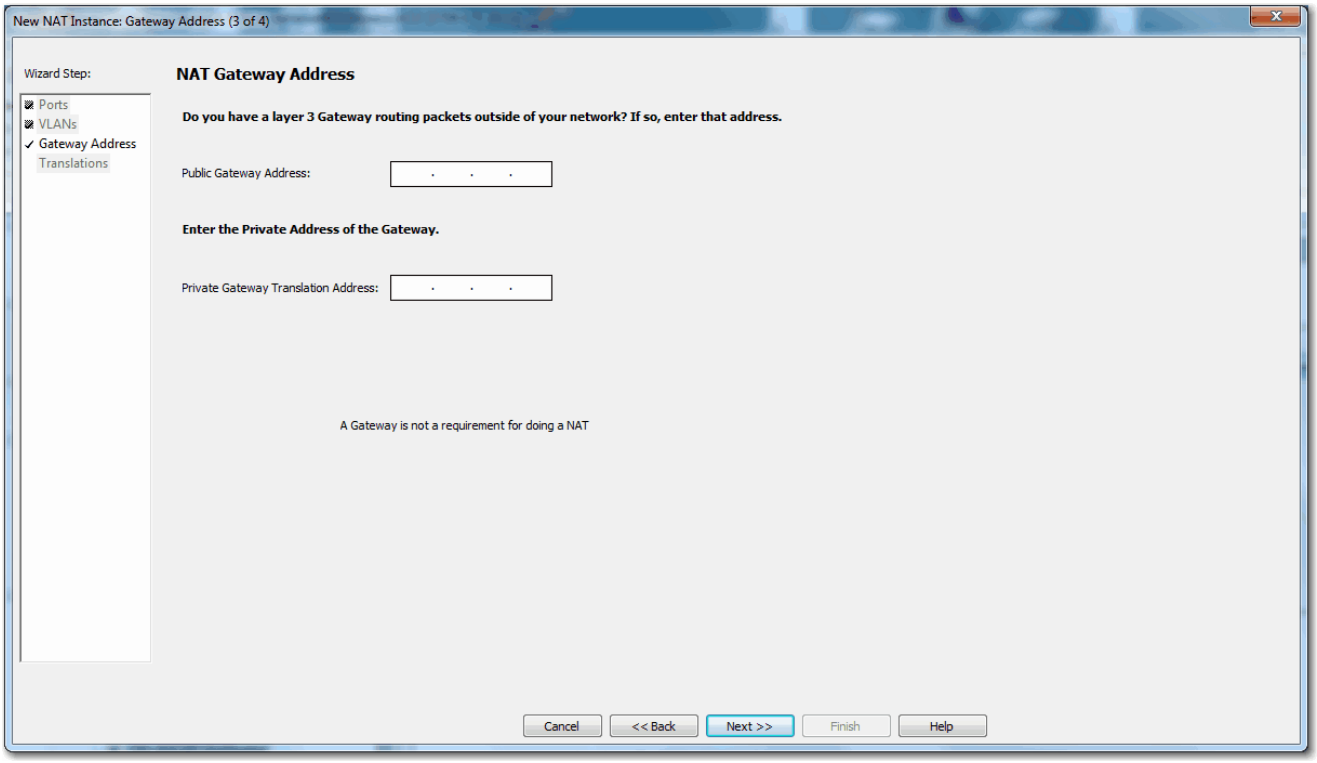
4. For each port, select one or more VLANs to assign to the NAT instance.

   The VLANs available for selection are VLANs previously assigned to the port. You can select the same VLAN for multiple ports. VLANs assigned to another NAT instance are unavailable for selection.

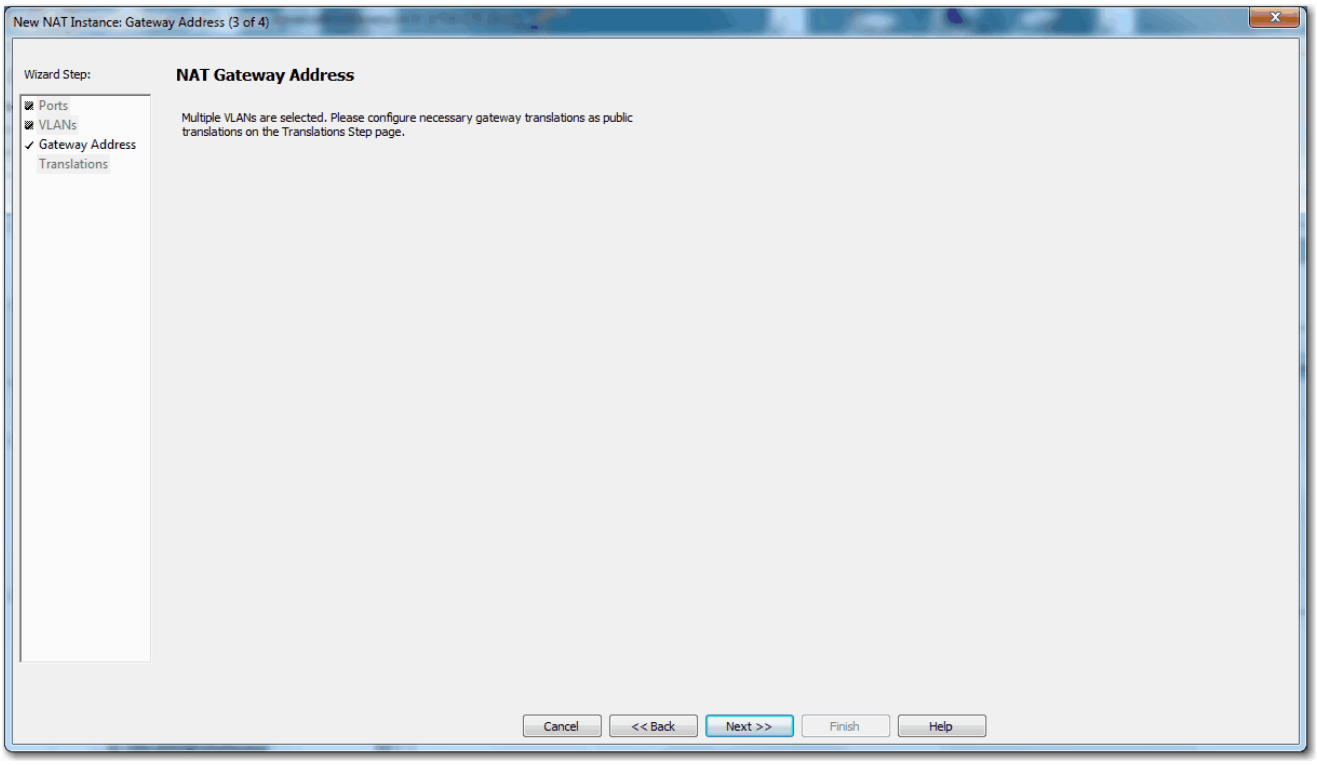
5. Click Next to display the Gateway Address view.

   If you assigned only one VLAN to the NAT instance and use a Layer 3 gateway, specify the following addresses:

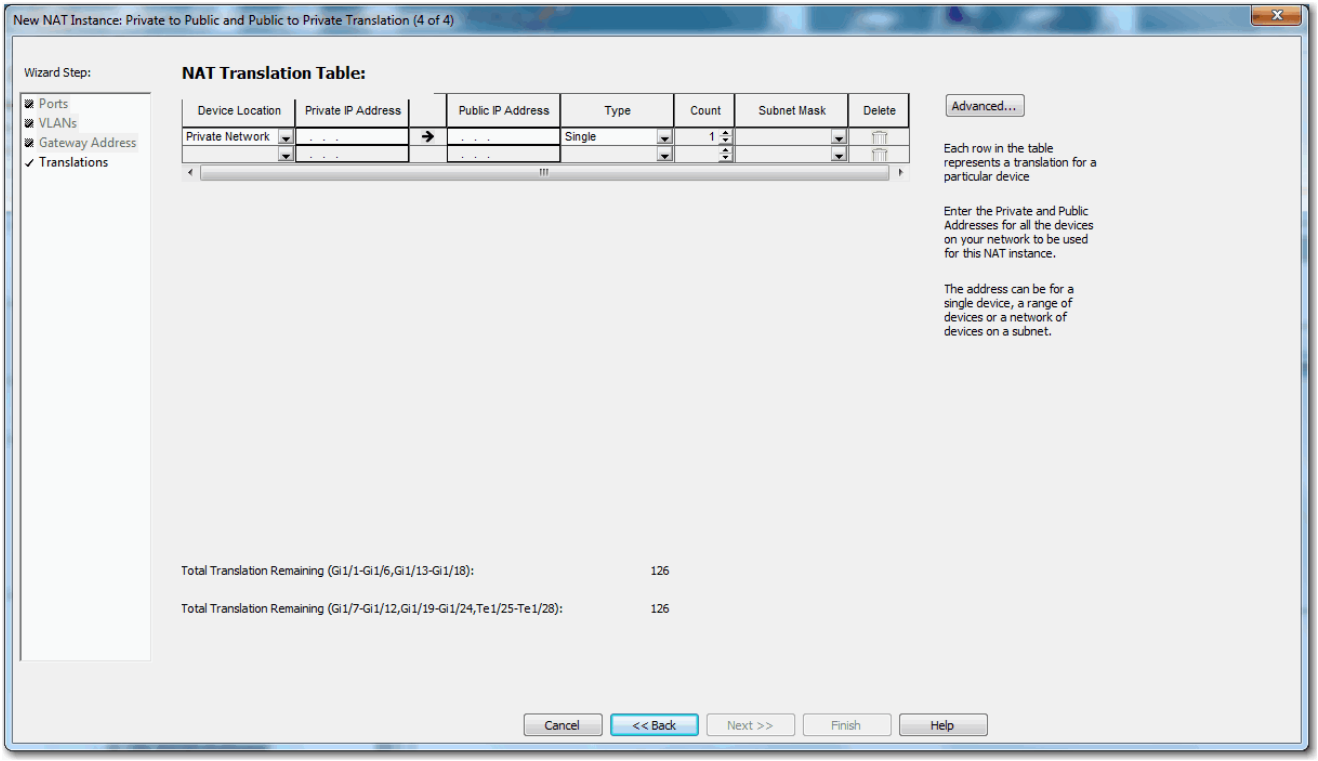
   - Public Gateway Address—Type the default gateway address of the Layer 3 switch or router for this subnet.
   - Private Gateway Translation Address—Type a unique IP address to represent the Layer 3 switch or router on the private network.



If you assigned multiple VLANs to the NAT instance, no gateway configuration is necessary.



6. Click Next to display the Translations view.



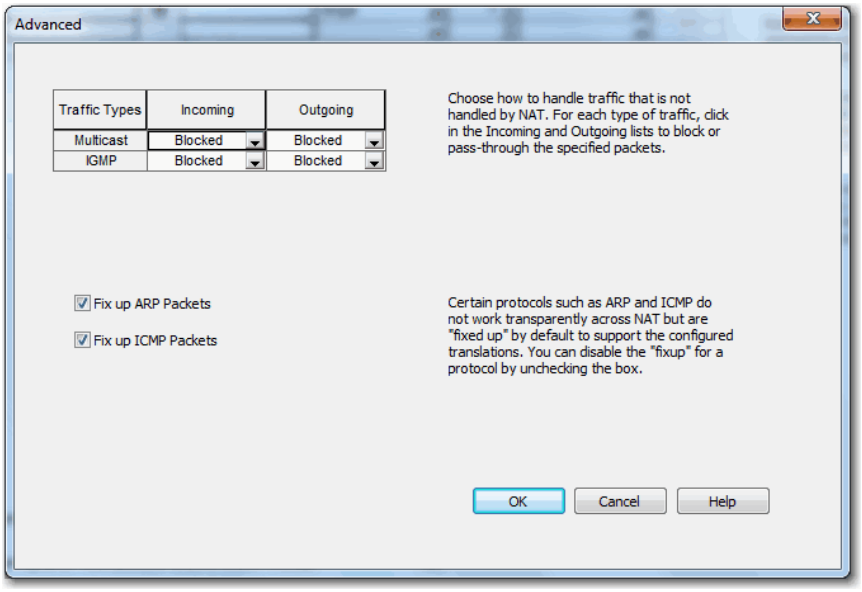
7. Configure translations for one device, a range of devices, or all devices on a subnet.

Field	Description
Device Location	Choose the type of network on which the device resides: • Private Network • Public Network
Private IP Address	Specify a private IP address. Single translations: • If the device is on a private network, type the existing address for the device. • If the device is on a public network, type a unique address to represent the device on the private network. Range translations: • If the devices are on a private network, type the existing starting address for the devices. • If the devices are on a public network, type a unique starting address to represent the devices on the private network. Subnet translations: • If the devices are on a private subnet, type the existing starting address for the devices. • If the devices are on a public subnet, type a unique starting address to represent the devices on the private subnet. Subnet addresses must correspond to the size of the subnet mask to translate. See Table 74 on page 293.
Public IP Address	Specify a public IP address. Single translations: • If the device is on a private network, type a unique address to represent the device on the public network. • If the device is on a public network, type the existing address for the device. Range translations: • If the devices are on a private network, type a unique starting address to represent the devices on the public subnet. • If the devices are on a public network, type the existing starting address for the devices on the public subnet. Subnet translations: • If the devices are on a private subnet, type a unique starting address to represent the devices on the private network. • If the devices are on a public subnet, type the existing starting address for the devices. Subnet addresses must correspond to the size of the subnet mask to translate. See Table 74 on page 293.
Type	Choose a translation type: • Single—Translates one address. • Range—Translates a range of addresses. • Subnet—Translates all or a portion of addresses on a subnet.
Count	(Range translation types only). Choose the number of addresses to include in the range. Valid values: 2…128 **IMPORTANT:** Each address in a range counts as one translation entry: • Port ranges Gi1/1…Gi1/6 and Gi1/13…Gi1/18 can include a combined maximum of 128 translation entries. • Port ranges Gi1/7…Gi1/12, Gi1/19…Gi1/24, and Te1/25…Te1/28 can include a combined maximum of 128 translation entries.
Subnet Mask	(Subnet translation types only). Choose the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry) – 255.255.255.192 (provides 64 addresses per translation entry) – 255.255.255.224 (provides 32 addresses per translation entry) – 255.255.255.240 (provides 16 addresses per translation entry) **IMPORTANT:** Each subnet mask counts as one translation entry: • Port ranges Gi1/1…Gi1/6 and Gi1/13…Gi1/18 can include a combined maximum of 128 translation entries. • Port ranges Gi1/7…Gi1/12, Gi1/19…Gi1/24, and Te1/25…Te1/28 can include a combined maximum of 128 translation entries.
Delete	Click to delete the translation entry.

Table 74 - Valid Subnet Addresses

Subnet Mask	Subnet Address
255.255.0.0	The last two octets of the address must end in 0. **EXAMPLE:** Private address: 192.168.0.0 Public address: 10.200.0.0
255.255.255.0	The last octet of the address must end in 0. **EXAMPLE:** Private address: 192.168.1.0 Public address: 10.200.1.0
255.255.255.128	The last octet of the address must end in 0 or 128. **EXAMPLE:** Private address: 192.168.1.0 or 192.168.1.128 Public address: 10.200.1.0 or 10.200.1.128
255.255.255.192	The last octet of the address must end in one of the following: 0, 64, 128, 192. **EXAMPLE:** Private address: 192.168.1.64 Public address: 10.200.1.64
255.255.255.224	The last octet of the address must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** Private address: 192.168.1.32 Public address: 10.200.1.32
255.255.255.240	The last octet of the address must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** Private address: 192.168.1.16 Public address: 10.200.1.16

8. To configure traffic permits and fixups, click Advanced to display the Advanced view.



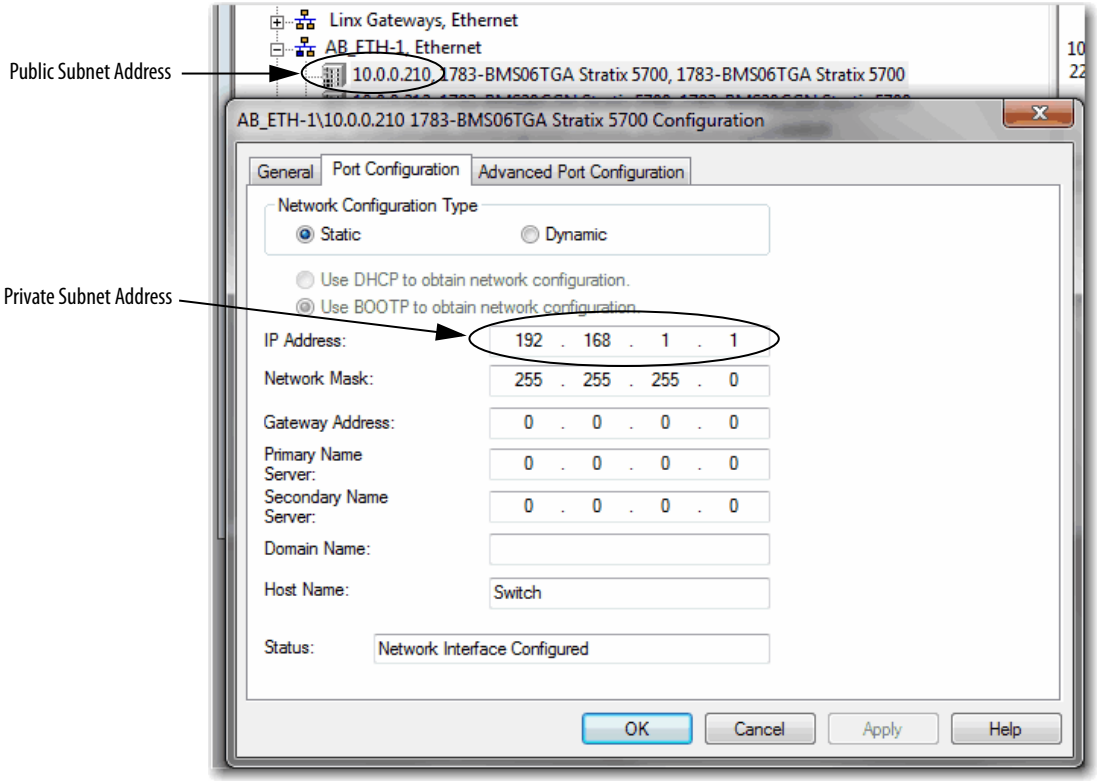
9. In the Incoming and Outgoing fields for each type of traffic, choose one of these options:
   - Pass-Through—Permit unsupported packets to pass across the NAT boundary.
   - Blocked—Drop unsupported packets.
10. To disable protocol fixups for ARP, clear the Fix up ARP checkbox.
11. To disable protocol fixups for ICMP, clear the Fix up ARP checkbox.

    By default, fixups are enabled for both ARP and ICMP.
12. Click OK to return to the Translations view.
13. On the Translations view, click Finish.

View Address Translations in RSLinx Software

The Ethernet driver in RSLinx software supports devices with address translations. If an address of a device is configured for translation, the public subnet address appears on the main dialog box of RSLinx software. However, its private subnet address appears in the configuration properties of the device.

Figure 31 - Public and Private Subnet Addresses in RSLinx Software



Network Time Protocol (NTP)

Network Time Protocol (NTP), documented in RFC 1305, is the traditional method of synchronizing clocks across packet-based networks. NTP uses a two-way time transfer mechanism between a master and a slave.

NTP is capable of synchronizing devices in a tightly-controlled network. The switch can use NTP as a time source for PTP, which lets you correlate data generated in the PTP network with data in the enterprise data center running NTP. For information about configuring NTP to PTP time conversion, see page 195.

Use the configuration software for the switch to view NTP status and to configure the NTP associations. An NTP association can be one of these types:

- Peer association—The switch can either synchronize to another device or allow the other device to synchronize to the switch.
- Server association—Only the switch synchronizes to another device. The other device cannot synchronize to the switch.

Configure NTP in Device Manager

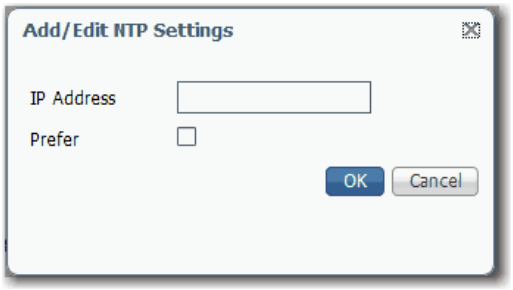
From the Configure menu, choose NTP.



You can add, edit, and delete NTP associations in the table area on the NTP page. You can add multiple NTP servers.

To add an association, follow these steps.

1. Click Add.



2. In the IP Address field, specify one of the following:
   - For a peer association, type the IP address of the peer providing, or being provided, the clock synchronization.
   - For a server association, type the IP address of the time server providing the clock synchronization.
3. To make the peer or server the preferred one that provides synchronization, check the Prefer checkbox.
4. Click OK.

Table 75 - NTP Fields

Field	Description
Clock Status	Displays the current status of NTP clock synchronization: • Synchronized • Unsynchronized
Stratum	Displays the NTP stratum of this system. The stratum indicates how many NTP hops away a device is from an authoritative time source.
Reference	Displays the address of the peer that the system is synchronized with.
NTP Up Time	Displays the uptime of the NTP entity.
Resolution	Displays the time resolution of the underlying operating system in milliseconds.
Reference Time	Displays the reference time stamp.
Clock Offset	Displays the offset of the system clock to the synchronized peer in milliseconds.
Root Delay	Displays the total delay along the path to the root clock in milliseconds.
Root Dispersion	Displays the number that indicates the maximum error relative to the primary reference source at the root of the synchronization subnet in milliseconds.
Peer Dispersion	Displays the number that indicates the maximum error relative to the synchronized peer (in milliseconds).
System Poll Interval	Displays the poll interval of the peer.
Last Update	Displays the time the system last updated its NTP information.

Table 75 - NTP Fields (Continued)

Field	Description
NTP Association Settings	
Status	Displays a symbol to indicate the status of the NTP peer association. * sys.peer # selected + candidate - outlyer
Configured	Displays the status of the NTP peer association.
IP Address	Displays the specified IP address for the association: • For a peer association, the IP address identifies the peer providing, or being provided, the clock synchronization. • For a server association, the IP address identifies the time server providing the clock synchronization.
Prefer	If checked, the peer or server is the preferred one that provides synchronization.
Ref Clock	Displays a 32-bit code or Internet address that identifies the reference clock of the peer.
Stratum	Displays the stratum of the peer.
When	Displays the time in seconds since the last NTP packet was received from the peer.
Poll	Displays the polling interval in seconds.
Delay	Displays the round-trip delay to the peer in milliseconds.
Offset	Displays the relative time of the peer clock to the local clock in milliseconds.

Parallel Redundancy Protocol (PRP)

Stratix 5400 and 5410 switches support PRP as a redundancy box (RedBox). As a RedBox, PRP sends duplicate packets from two different ports on independent network paths. The redudant paths provide high availability for data transmission if one of the paths enounters a failure. For more informatoin about PRP, see the IEC 62439-3 standard.

Table 76 describes terms to know before you configure PRP.

Table 76 - PRP Terms

Term	Description
Dual Attached Node implementing PRP (DANP)	End-device with PRP functionality connected to each of the two independent LANs.
Single Attached Node (SAN)	Device with a single network interface connected directly to one of the two LANs.
Redundancy Box (RedBox)	Device that connects one or more SANs to both LANs. The switch implements RedBox functionality.
Virtual DAN (VDAN)	A SAN connected to both LANs through a RedBox. A node behind a RedBox appears to other nodes as a DAN.
PRP channel	A logical interface that aggregates PRP groups (access, trunk, or routed) into a single link. The PRP channel remains up as long as one of its member ports remain up and send traffic. When both member ports are down, the channel is down. Only the up and down states of the ports can trigger different redundancy behavior or SAN traffic routing decisions. Each channel contains two Layer 2 or Layer 3 Gigabit Ethernet interfaces. Within each channel group, the lowest numbered Gigabit Ethernet interfaces (Gi1/1 and Gi1/3 or Gi1/17 and Gi1/19, depending on the switch) are always the primary port. The highest numbered Gigabit Ethernet interfaces (Gi1/2 and Gi1/4 or Gi1/18 and Gi1/20, depending on the switch) are the secondary port.
PRP channel group	A group is composed of two ports, one of which represents LAN A and the other LAN B: • PRP channel group 1 always contains the Gi1/1 and Gi1/2 or Gi1/17 and Gi1/18 interfaces. • PRP channel group 2 always contains Gi1/3 and Gi1/4 or Gi1/19 and Gi1/20 interfaces.

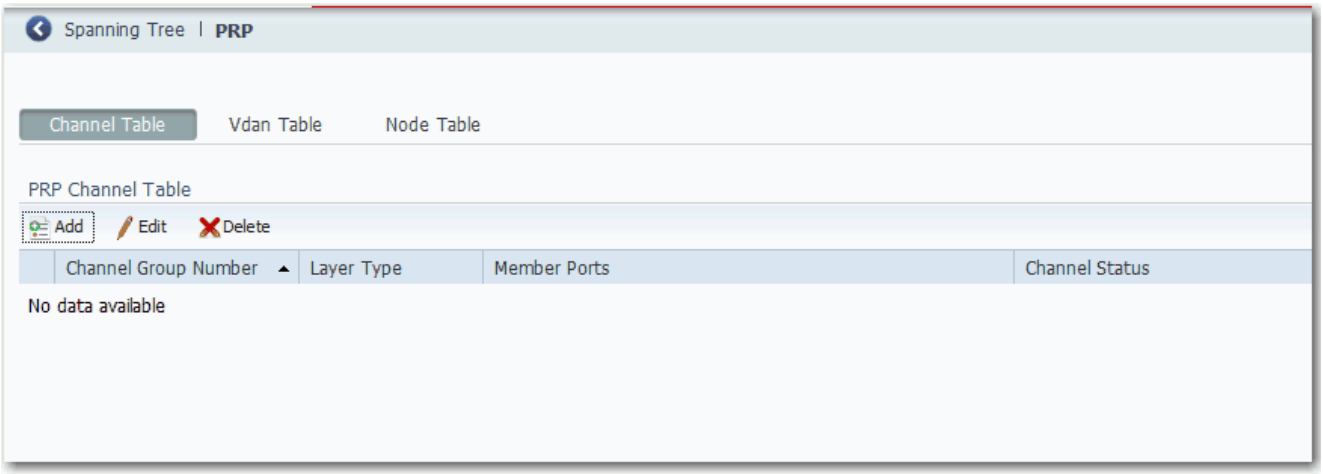
Traffic egressing the RedBox PRP channel group can be mixed, that is, destined to either SANs (connected only on either LAN-A or LAN-B) or DANs. To avoid duplication of packets for SANs, the switch learns source MAC addresses from received supervision frames for DAN entries and source MAC addresses from non-PRP (regular traffic) frames for SAN entries. The switch maintains these addresses in the Node table. When forwarding packets out of the PRP channel to SAN MAC addresses, the switch looks up the entry and determines which LAN to send to rather than duplicating the packet.

A RedBox with VDANs needs to send supervisory frames on behalf of those VDANs. For traffic coming in on all other ports and going out PRP channel ports, the switch learns source MAC addresses, adds them to the VDAN table, and starts sending Supervisory frames for these addresses.

You can add static entries to the VDAN and Node tables.

Configure PRP via Device Manager

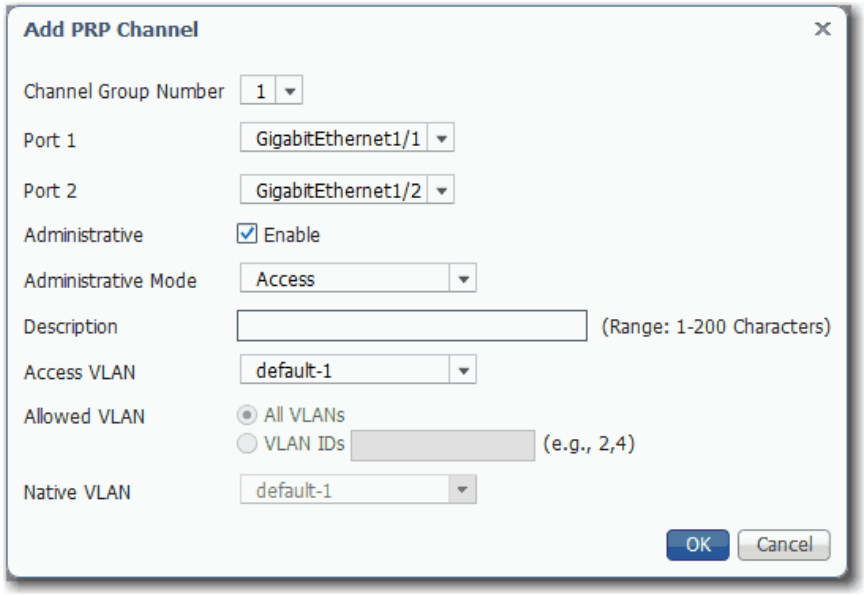
From the Configure menu, choose PRP.



PRP Channel Table

To add a PRP channel, follow these steps.

1. From the PRP window, click the Channel Table tab.
2. Click Add, and then complete the fields, and then click OK.

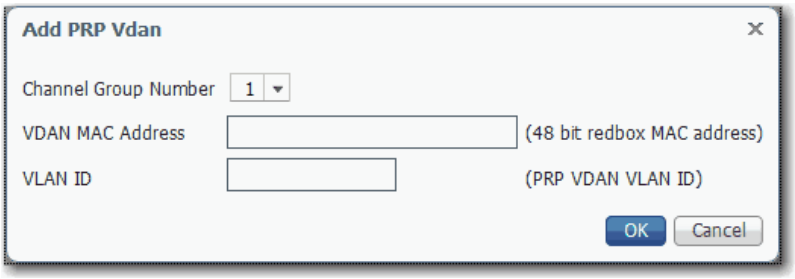


Field	Description
Channel Group Number	Choose a channel group number: • 1 (default) • 2
Port 1	Choose a port to be a member of the channel group: • Valid ports on Stratix 5400 switches: Gi1/1 and Gi1/2 • Valid ports on Stratix 5410 switches: Gi1/17 and Gi1/18
Port 2	Choose a port to be a member of the channel group: • Valid ports on Stratix 5400 switches: Gi1/3 and Gi1/4 • Valid ports on Stratix 5410 switches: Gi1/19 and Gi1/20
Administrative	Check the Enable checkbox to enable the switch ports. By default, the ports are enabled. Clear the Enable checkbox to disable the switch ports.
Administrative Mode	Choose a mode to assign to the PRP channel group: • Access (default)—Layer 2 • Trunk—Trunk mode • Routed—Layer 3
Description	Type a description for the PRP channel. The description can contain a maximum of 200 characters.
Access VLAN	(Access mode only). Choose the VLAN associated with the PRP channel group. The default value is **default-1**.
Allowed VLAN	(Trunk mode only). Click one of these options to specify the VLANs to transmit traffic from this channel group in tagged format: • All VLANS (default)—Click to allow all VLANs to transmit traffic from this channel group. • VLAN IDs—Click to allow only the VLANs you specify to transmit traffic from this channel group. Type each VLAN ID separated by a comma.
Native VLAN	(Trunk mode only). Choose the VLAN to send and receive untagged traffic on the trunk port. The default value is **default-1**.
IP Assignment Mode	(Routed mode only). Click one of these options to specify the IP address of this PRP channel group: • No IP Address—Do not assign an IP address. • Static—Assign a static IP address. Type the IP address and the subnet mask. • DHCP—Allow an IP address to be assigned via DHCP.

VDAN Table

To add an entry to the PRP VDAN table, follow these steps.

1. From the PRP window, click the VDAN Table tab.
2. Click Add, and then complete the fields, and then click OK.

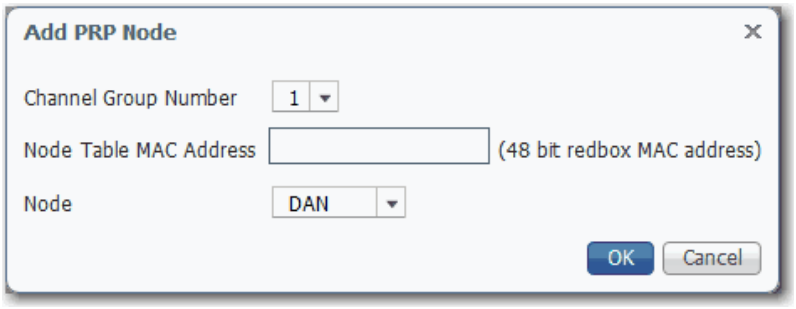


Field	Description
Channel Group Number	Choose a channel group number: • 1 (default) • 2
VDAN MAC Addres	Type the MAC address of the VDAN.
VLAN ID	(Access mode only). Choose the VLAN associated with the PRP channel group. The default value is **default-1**.

Node Table

To add an entry to the PRP Node table, follow these steps.

1. From the PRP window, click the Node Table tab.
2. Click Add, and then complete the fields, and then click OK.



Field	Description
Channel Group Number	Choose a channel group number: • 1 (default) • 2
Node Table MAC Addres	Type the MAC address of the DAN or SAN.
Node	Choose the type of PRP node: • DAN (default)—Dual attached node • SAN-A—Single attached node on LAN A • SAN-B—Single attached nnode on LAN B

Port Mirroring

Port mirroring is for advanced users with experience in troubleshooting traffic and protocol issues on networks. Port mirroring copies, or mirrors, traffic on one port to a monitoring port where a network protocol analyzer tool can capture the packet. Use port mirroring as a diagnostic tool or debugging feature.

Port mirroring does not affect the switching of network traffic on the monitored port. You must dedicate a monitoring port for port mirroring use. Except for traffic that is being copied for the port mirroring session, the monitoring port does not receive or forward traffic.

You can configure port mirroring by assigning the Port Mirroring Smartport role on a switch port via Device Manager.

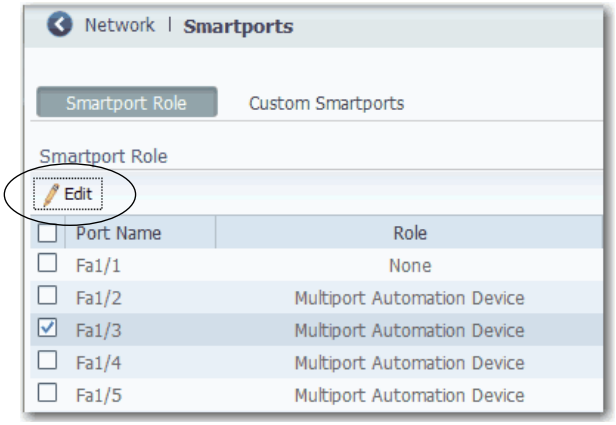
IMPORTANT You can configure port mirroring on only one port via Device Manager. However, you can configure multiple ports via the CLI.

IMPORTANT Port mirroring is a tool for analyzing end node traffic. Because the switch can filter certain network control traffic, we recommend that you do not use port mirroring when you require an exact copy of all network traffic.

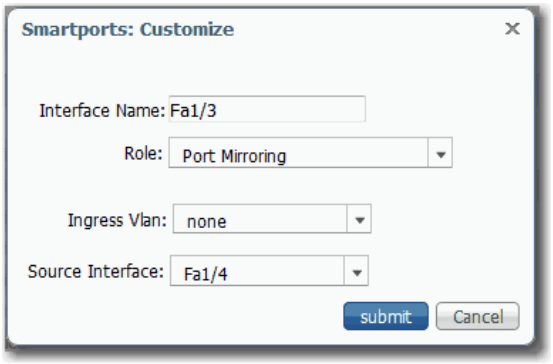
Configure Port Mirroring in Device Manager

To configure port mirroring, follow these steps.

1. From the Configure menu, choose Smartports.
2. Select the checkbox next to the port to do the monitoring, and then click Edit.

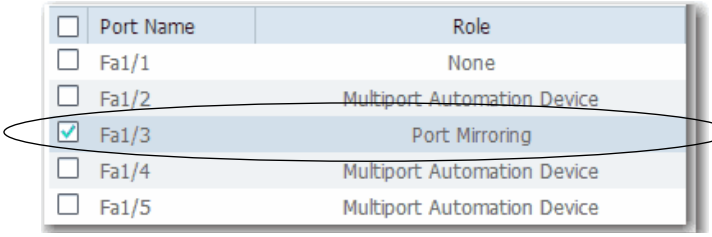


3. Complete the fields, and then click Submit.



Field	Description
Interface Name	Displays the port you selected to do the monitoring.
Role	Choose Port Mirroring.
Ingress Vlan	(Optional). Choose a VLAN to monitor.
Source Interface	Choose the port to monitor. The port you assigned to the Port Mirroring role monitors traffic that passes through this port.

4. Verify that the Port Mirroring role is assigned to the port.



Port Security

Stratix managed switches implement MAC address-based port security. A MAC address is a unique address that is assigned to each Ethernet-capable device. Switches can enforce communication either dynamically or statically per MAC address.

With dynamic port security, a switch port communicates with some number of devices. The port tracks only the number of devices rather than the MAC addresses of those devices. Static port security adds devices to the port security table on a per MAC address basis. With static dynamic port security, only devices with the MAC addresses in the security table are able to communicate on that port.

Port Security is not available on Stratix 5700 switches with lite firmware.

Dynamic Secure MAC Address (MAC ID)

Many Smartport roles have a maximum number of MAC IDs that can use that port. For example, the Smartport role 'Automation Device' configures the port for a maximum of one MAC ID. The MAC ID is dynamic, meaning the switch learns the first source MAC ID to use the port. Attempts by any other MAC ID to access the port are denied.

If the link becomes inactive, the switch dynamically relearns the MAC ID to be secured.

The default number of MAC IDs can be changed on the Port Security tab within Device Manager or the Logix Designer application.

The following table shows the Smartport role and the maximum number of supported MAC IDs.

Table 77 - Maximum Number of MAC IDs per Smartport Role

Smartport Role	Number of MAC IDs (max)
Automation Device	1
Desktop for Automation	1
Switch for Automation	Not restricted
Router for Automation	Not restricted
Phone for Automation	3
Wireless for Automation	Not restricted
Multiport Automation Devices	Not restricted
Virtual Desktop for Automation	2
Port Mirroring	Not restricted
None	Not restricted

Static Secure MAC Address (MAC ID)

The other method of limiting MAC IDs is to configure statically one or more MAC IDs for a port by defining them via port security with Device Manager. These addresses become part of the saved configuration of the switch. This method provides strong security. However, if you replace any devices that are connected to the port, you must reconfigure the MAC IDs because the new devices have different MAC IDs than the previous devices.

For Stratix 8000/8300 switches, you can configure the static secure method only with the Logix Designer application. Configuration for this method is not available with Device Manager.

Security Violations

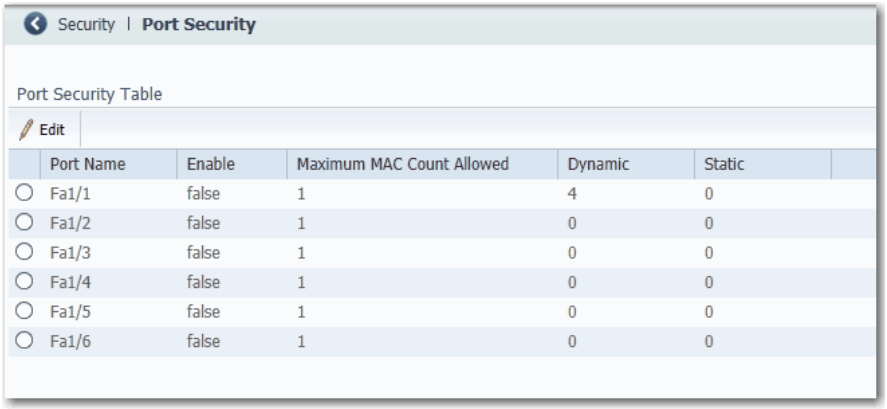
It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses that have been configured for a port are in the address table. A station whose MAC address is not in the address table attempts to access the interface.
- An address that is learned or configured on one secure interface is seen on another secure interface in the same VLAN.

When a violation occurs, the port goes into the Restrict mode. In this mode, packets with unknown source addresses are dropped and you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

Configure Port Security via Device Manager

From the Configure menu, choose Port Security.



Port security limits and identifies the MAC addresses of devices that can send traffic through the switch port. The switch port does not forward traffic from devices outside the defined group of devices. A security violation occurs when any of the following conditions occur:

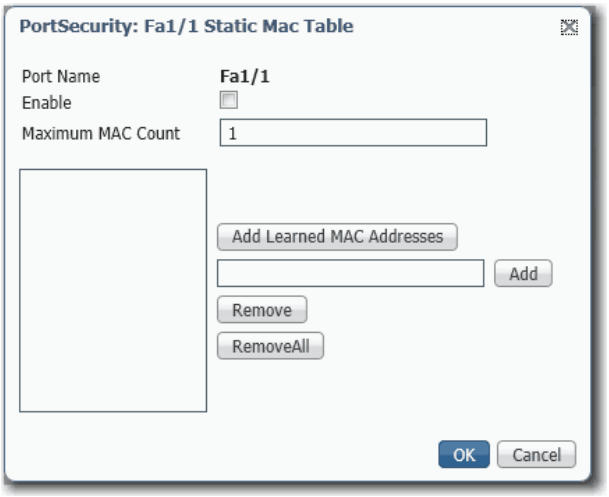
- A device, which has a MAC address different from any identified secure MAC addresses, attempts to access the switch port.
- The number of MAC addresses on the port exceeds the maximum number that is supported on the port.

Port security supports multiple security levels:

- The ability to define the number of devices that are connected to a given port. Devices are assigned on a first-come, first-served basis and time out after a certain period of inactivity.
- The ability to store the existing MAC Address configuration by selecting Add Learned MAC Addresses on the Static MAC Address Table.
- The ability to add and remove manually MAC Addresses on a per port basis.

To change the Static MAC Addresses table for a port, follow these steps.

1. Click the radio button next to the port to configure.
2. Click Edit.
3. Clear or check the Enable checkbox.
4. Configure MAC addresses as follows:
   - To add the existing MAC addresses of devices that are currently connected to a port, click Add Learned MAC Addresses.
   - To add a specific MAC address to the table, type a MAC address in the format fields and click Add.
   - To remove a MAC address from the table, select the MAC address and click Remove.
   - To clear the MAC address table, click Remove All.



5. Click OK.

Configure Port Security via the Logix Designer Application

In the navigation pane, click Port Security.

For Stratix 8000/8300 switches, use Advanced Port Configuration, as described on page 308.

Figure 32 - Port Security

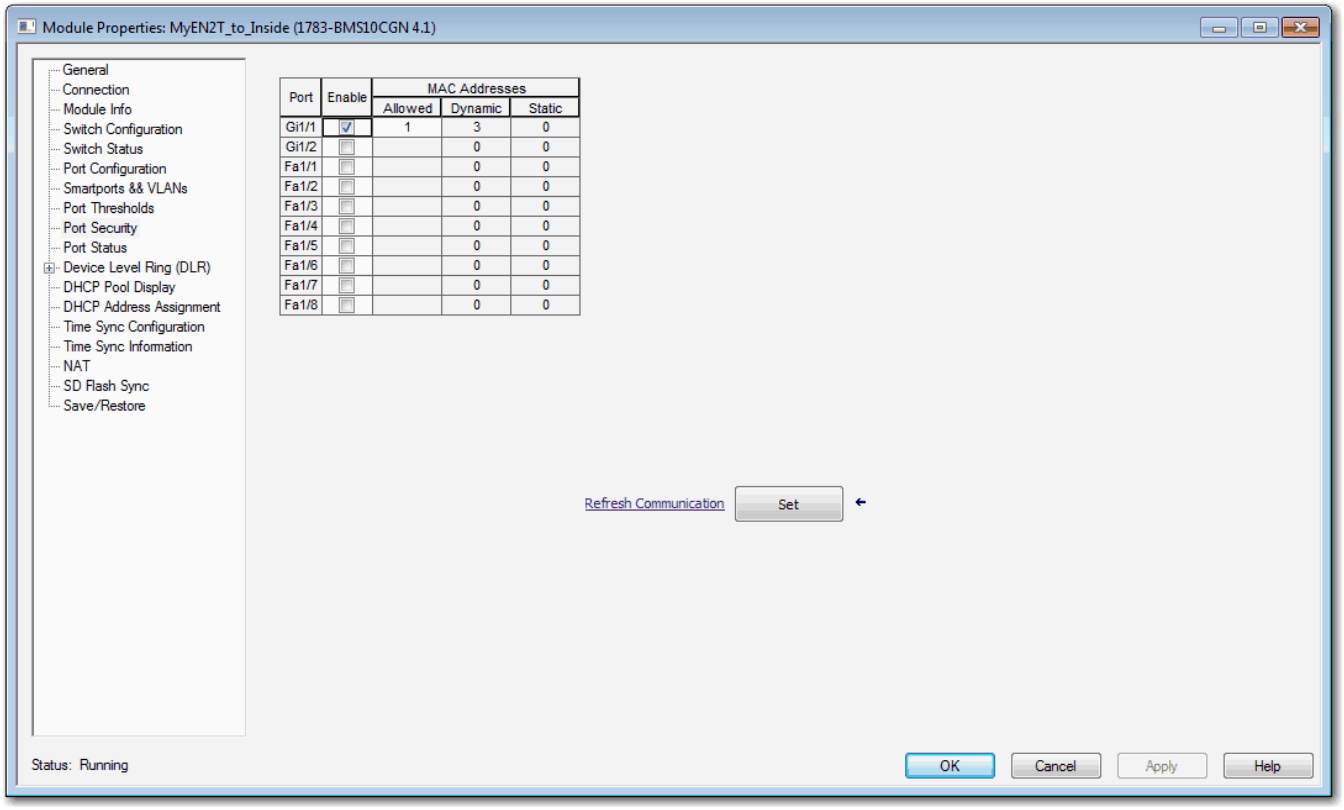


Table 78 - Port Security Fields

Field	Description
Port	The port on which you want to enable or disable security.
Enable	Check the checkbox to enable port security.
MAC Addresses	The number of supported dynamic or static MAC addresses. • Allowed—1…80. • Dynamic—The number of MAC addresses (devices) currently connected to the port that is not manually (statically) defined. • Static—The number of MAC addresses (devices) statically defined by using Device Manager. This number must be greater than the sum of the static + dynamic for a given port. If you wish to set the number to less, disconnect the appropriate devices and let their entries in the port security table time out.

For Stratix 8000/8300 switches, in the navigation pane, click Advanced Port Configuration.

Figure 33 - Advanced Port Configuration for Stratix 8000/8300 Switches

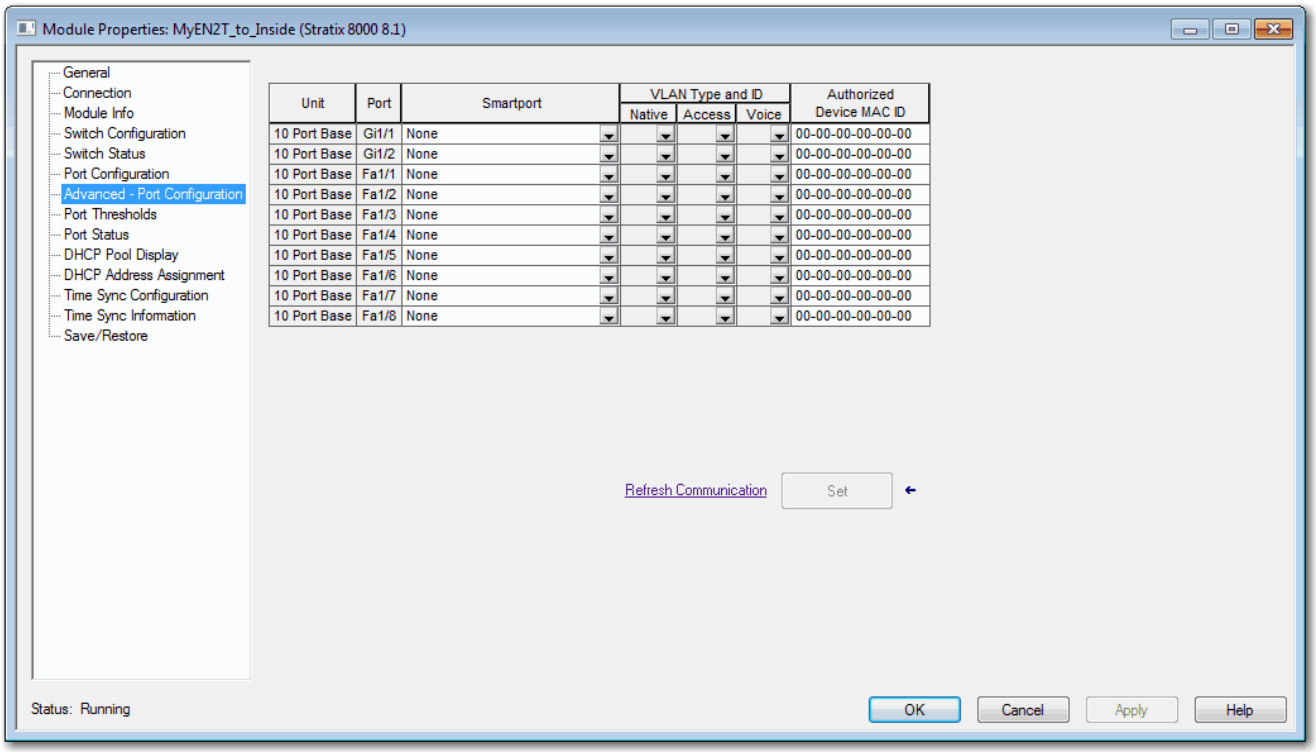


Table 79 - Advanced Port Configuration Fields for Stratix 8000/8300 Switches

Field	Description
Unit	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	Indicates the port that is selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number, such as in the following examples: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Smartport	See Assign Smartports and VLANs via the Logix Designer Application on page 358.
VLAN Type and ID	
Authorized Device MAC ID	To authorize a specific MAC address to communicate on the port, type the MAC address of the device that is connected to the port. You can authorize only one MAC address to communicate on the port. If other MAC addresses communicate on the port, they are blocked. This feature must not be set for ports that are connected to other switches or routers. The MAC address is also known as Ethernet address, physical address, or hardware address. Each node on the network has a unique MAC address. The MAC ID is six hexadecimal numbers, such as 00-00-BC-22-A0-D8.

Port Thresholds

Port thresholds prevent traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. Port thresholds do not apply to switches with lite firmware.

A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing denial-of-service attacks can cause a storm.

Incoming (storm control)

Incoming port thresholds (or traffic suppression) monitor packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type that is received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold.

Port thresholds use one of these methods to measure traffic activity:

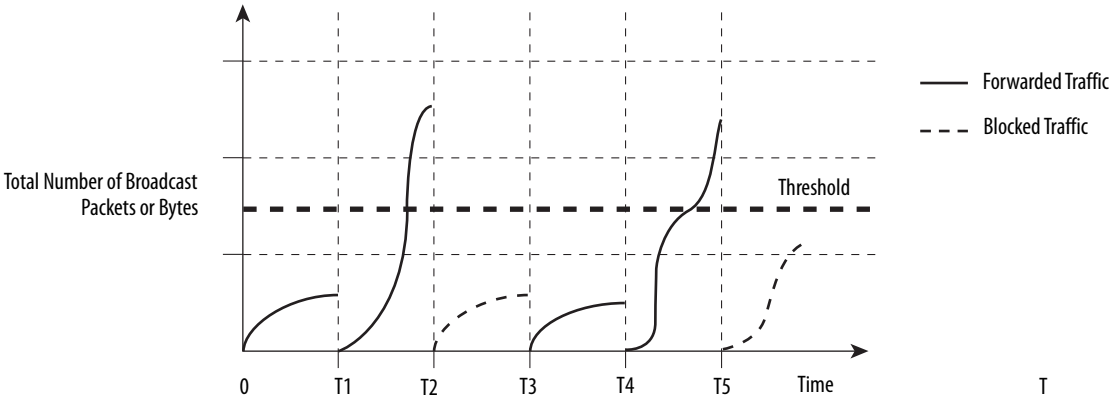
- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic.
- Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received.
- Traffic rate in bits per second at which broadcast, multicast, or unicast packets are received.

With each method, the port blocks traffic when the rising threshold is reached. The port remains blocked until the traffic rate drops below the falling threshold and then resumes normal forwarding. In general, the higher the level, the less effective the protection against broadcast storms.

IMPORTANT When the port threshold for multicast traffic is reached, all multicast traffic is blocked. An exception is management traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames.

The graph shows broadcast traffic patterns on an interface over a given time. The example can also be applied to multicast and unicast traffic. In this example, the broadcast traffic being forwarded exceeded the configured threshold between time intervals T1 and T2 and between T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped for the next time period. Therefore, broadcast traffic is blocked during the intervals following T2 and T5. At the next time interval (for example, T3), if broadcast traffic does not exceed the threshold, it is again forwarded.

Figure 34 - Port Thresholds Example



The combination of the storm-control suppression level and the 1-second time interval controls the way the port thresholds algorithm works. A higher threshold enables more packets to pass through. A threshold value of 100% means that no limit is placed on the traffic. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.

IMPORTANT Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of port thresholds.

Outgoing (rate limiting)

Outgoing port thresholds limit the rate at which the switch communicates with a client device as a percentage of wire speed. Limiting bandwidth to specific users and ports helps control network congestion, enable high performance, create efficient networks, and prevent a few devices from monopolizing network bandwidth. It can also improve reliability by limiting maximum bandwidth to end devices that are not capable of handling large amounts of traffic. From Device Manager or the Logix Designer application AOP, you can enable or disable rate limiting on a per port basis.

Default Port Thresholds Configuration

By default, incoming unicast, broadcast, and multicast port thresholds are disabled. Outgoing port thresholds are also disabled.

Configure Port Thresholds via Device Manager

From the Configure menu, choose Port Thresholds.

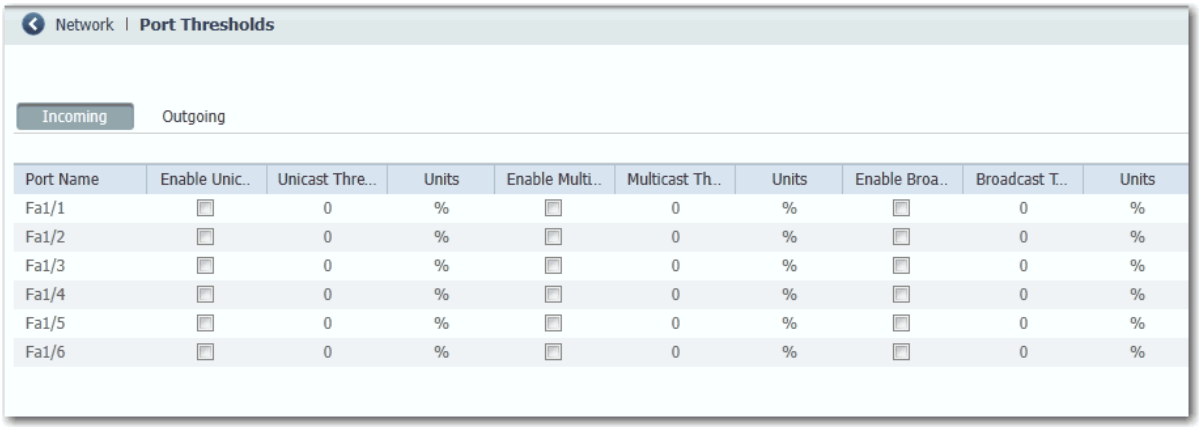


Table 80 - Port Threshold Fields

Field	Description
Incoming	
Unicast Multicast Broadcast	For each port, do the following: 1. Check or clear the Enable checkbox. 2. Type the threshold value. 3. Choose one of these units: – PPS (0…10 billion) – BPS (0…10 billion) – % (0…100)
Outgoing	
All Traffic	For each port, do the following: 1. Check or clear the Enable checkbox. 2. Type the threshold value. 3. Click Save.

Configure Port Thresholds via the Logix Designer Application

You can configure threshold limits for broadcast, unicast, and multicast traffic for each active port. This feature is available only with Full firmware. The number of packets being sent is compared against the threshold value. These limits help to prevent a single device from sending too much traffic.

Figure 35 - Port Thresholds for Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 Switches

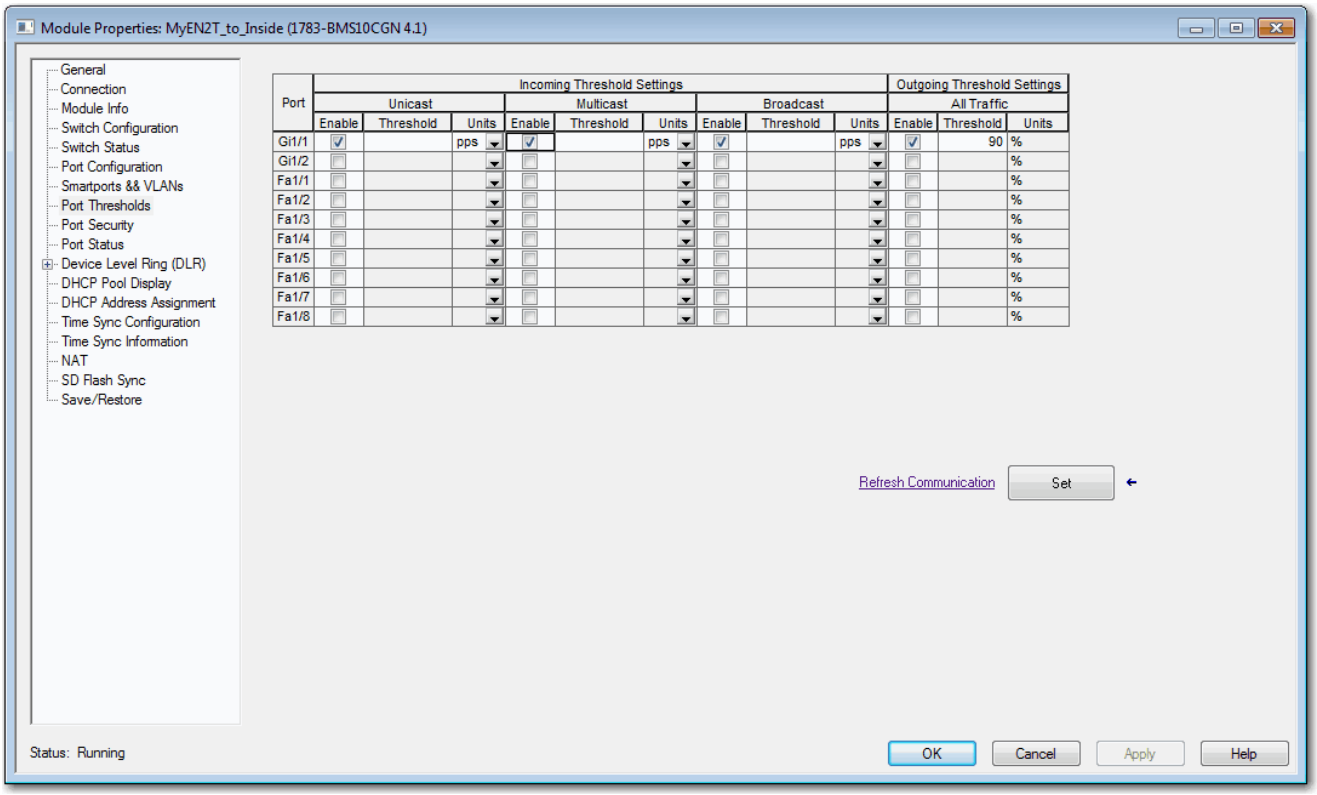


Table 81 - Port Threshold Fields for Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 Switches

Field	Description
Port	The port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Incoming Threshold Settings	Enable incoming thresholds and set the threshold values for the unicast, multicast, and broadcast traffic for each port. Valid values for units: • Packets per second (pps) • Percentage of total bandwidth (%) • Bits per second (bps)
Outgoing Threshold Settings	Enable outgoing thresholds and set the threshold values for the traffic for each port. Units % = Percentage of total bandwidth

Figure 36 - Port Thresholds for Stratix 8000/8300 Switches

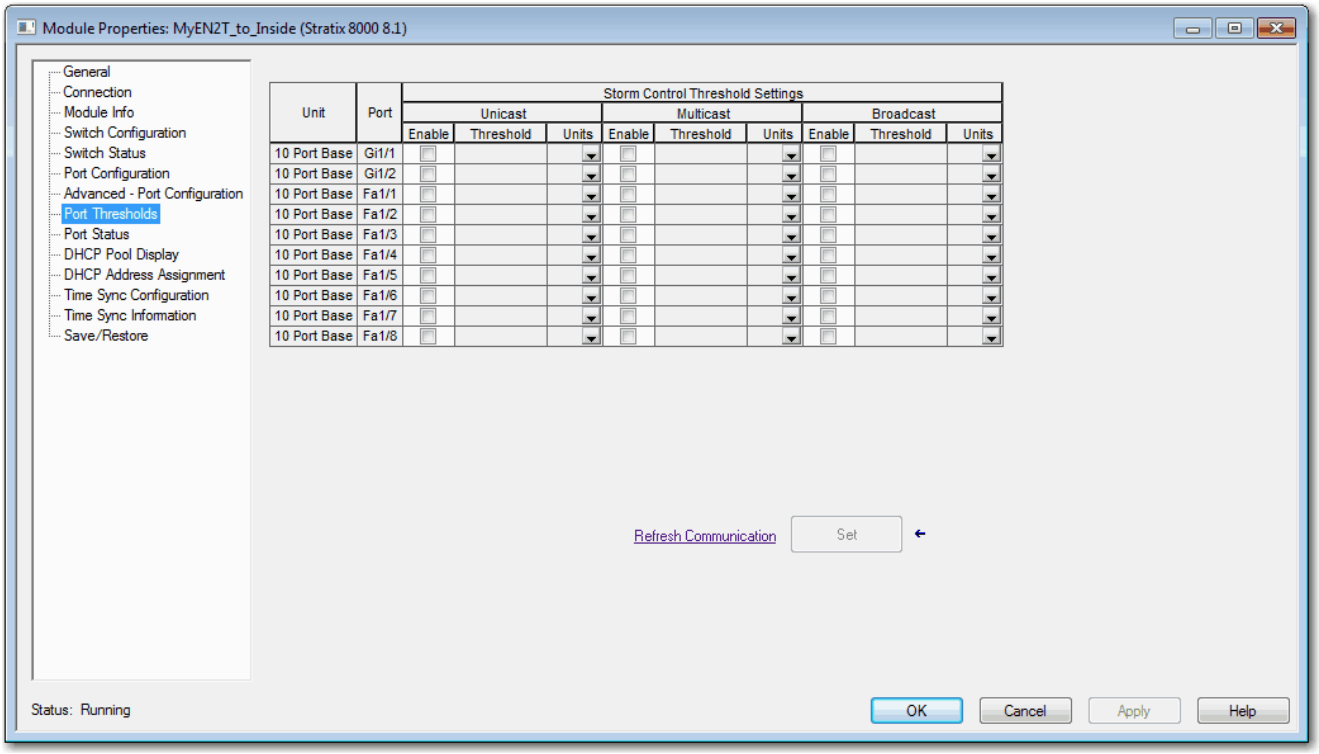


Table 82 - Port Threshold Fields for Stratix 8000/8300 Switches

Field	Description
Unit	Indicates where the port resides: • Base (for example, 1783-MS10T) • Expansion module (for example, 1783-MX08T)
Port	Indicates the port that is selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number. For example: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Storm Control Threshold Settings	Set the threshold values for the broadcast, unicast, and multicast traffic for each port. The number of packets being sent is compared against the threshold value. If an undesirable network event occurs and the threshold value has been exceeded, a Yes value appears on the Port Status view and in the Traffic Threshold Exceeded on Any Port field on the Switch Status view. Network traffic of the type that exceeded threshold (broadcast, unicast, or multicast) is dropped until it falls below the falling threshold. The falling threshold is automatically set to 5% less than the entered threshold value.
Broadcast, Unicast and Multicast	Complete these fields for each traffic type: • Enable—Check to enable the storm control on the selected port. The respective threshold value and units are applied to the selected port when you click Set. Clear the checkbox to disable the storm control for the selected port. Zero is applied to the threshold value and units attributes when you click Set. • Threshold—Type the value for the threshold after you choose the unit of measurement: – If Units is set to pps or bps, type a value between 0…10000000000. – If Units is set to %, type a value between 0…100. • Units—Choose the unit of measurement for the threshold: – pps (packets per second) – bps (bits per second) – %

Power over Ethernet (PoE)

Switches and expansion modules with PoE ports are software-configurable and provide these features:

- Support for IEEE 802.3af (PoE)-compliant devices.
- Support for IEEE 802.3at Type 2 (PoE+), which increases the available power that can be drawn by powered devices from 15.4...30 W per port.
- Automatic detection and power budgeting. The switch maintains a power budget, monitors and tracks requests for power, and grants power only when it is available.
- Power to connected Cisco pre-standard and IEEE 802.3af-compliant powered devices if the switch detects that there is no power on the circuit.
- Support for Cisco Discovery Protocol (CDP) with power consumption. CDP applies only when using switches with Cisco end devices. The powered Cisco end device notifies the switch of the amount of power it is consuming. The switch can supply or remove power from the PoE port.
- Support for Cisco intelligent power management. A powered Cisco end device and the switch negotiate through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-powered device consuming more than 7 W to operate at its highest power mode. The powered device first starts up in Low-power mode, consumes less than 7 W, and negotiates to obtain enough power to operate in High-power mode. The device changes to High-power mode only when it receives confirmation from the switch.

  Cisco intelligent power management is backward-compatible with CDP with power consumption. The module responds according to the CDP message that it receives. CDP is not supported on third-party powered devices, so the module uses the IEEE classification to determine the power usage of the device.
- (Stratix 5410 switches) Support for high and low priority PoE/PoE+ ports. When two power-supply modules are installed, the system has enough power to support all ports as PoE/PoE+ ports. If one power-supply module fails, the system drops power to the low priority ports. Power to the high priority ports remains uninterrupted. If there is not enough power for one supply to support all high priority ports, ports are dropped by port number from highest to lowest port number.

PoE and PoE+ features are supported on switches and expansion modules with PoE ports when a correct power supply is connected to the switch. For power supply requirements, see page 144.

Configuration options include the following:

- Limit the total power supported.
- Configure mode and power settings for individual ports.

For most applications, the default configuration (Auto mode) is sufficient and no further configuration is required. However, you can customize the settings to meet your needs. For example, to make sure that power is pre-allocated to a specific port, set the port mode to Static. As another example, to disallow high-power devices on a port, set the mode to Auto and specify a maximum power limit.

IMPORTANT When you make PoE configuration changes to a port, the port drops power. Whether the port powers up again depends on the new configuration, the state of the other PoE ports, and the state of the power budget.

For example, if port 1 is in Auto mode and the On state, and you configure it for Static mode, the switch removes power from port 1, detects the powered device, and repowers the port.

If port 1 is in Auto mode and the On state and you configure it with a maximum wattage of 10 W, the switch removes power from the port and then redetects the powered device. The switch repowers the port only if the powered device is a Class 1, Class 2, or a Cisco-only powered device.

Powered Device Detection and Initial Power Allocation

A switch or expansion module detects a powered device when a port with PoE capability is active, PoE is enabled (the default), and the connected device is not powered by another power source.

After device detection, the switch determines the device power requirements that are based on its type:

- The switch classifies the detected 802.3 af/at compliant IEEE device within a power consumption class. Based on the available power in the power budget, the switch determines if a PoE port can be powered. Table 83 lists these levels.

Table 83 - IEEE Power Classifications

Class	Power Supplied per Port, Max
0 (class status unknown)	15.4 W
1	4 W
2	7 W
3	15.4 W
4	30 W PoE+ devices only

- A Cisco pre-standard powered device does not provide its power requirement when the switch detects it. A port that is not configured for PoE+ allocates 15.4 W as the initial allocation for power budgeting. A port that is configured for a PoE+ switch allocates 30 W.

  The initial power allocation is the maximum amount of power that a powered device requires. The switch initially allocates this amount of power when it detects and powers the powered device. As the powered device negotiates power levels with the module through CDP power-negotiation messages, the initial power allocation can be adjusted.

The switch monitors and tracks requests for power and grants power only when it is available. The switch tracks its power budget, which is the amount of power available on each PoE port. The switch performs power-accounting calculations when a port is granted or denied power to keep the power budget up to date.

After power is applied to a PoE port, the switch uses CDP (if CDP is supported by the powered Cisco end device) to determine the actual power consumption requirement of the connected powered devices. The switch adjusts the power budget accordingly. The switch processes a request and either grants or denies power. If the request is granted, the switch updates the power budget. If the request is denied, the switch verifies that power to the port is turned off, generates a syslog message, and updates the status indicators. Powered devices can also negotiate with the module for more power.

If the switch detects a fault that is caused by an undervoltage, overvoltage, overtemperature, oscillator-fault, or short-circuit condition, it does the following:

- Turns off power to the port
- Generates a syslog message
- Updates the power budget and status indicators

Power Management Modes

PoE ports support these modes:

- Auto (default)—The port automatically detects if the connected device requires power. If the port discovers a connected powered device and the module has enough power, the port does the following:

  – Grants power
  – Updates the power budget
  – Turns on power to the port on a first-come, first-served basis
  – Updates the status indicators

If enough power is available for all powered devices that are connected to the switch, power is turned on to all devices. If there is not enough power to accommodate all connected devices and if a device is reconnected while other devices are waiting for power, it cannot be determined which devices are granted or are denied power.

If granting power exceeds the system power budget, the switch denies power, verifies that power to the port is turned off, generates a syslog message, and updates the status indicators. After power has been denied, the switch periodically rechecks the power budget and continues to attempt to grant the request for power.

If a device being powered by the switch is then connected to wall power, the switch can continue to power the device. The switch can continue to report that it is still powering the device whether the device is being powered by the switch or receiving power from an AC power source.

If a powered device is removed, the switch automatically detects the disconnect and removes power from the port. You can connect a nonpowered device without damaging it.

You can specify the maximum wattage that is allowed on the port. If the IEEE-class maximum wattage of the powered device is greater than the configured maximum value, the switch does not provide power to the port. If the switch powers a Cisco end device, but the device later requests through CDP messages more than the configured maximum value, the switch removes power to the port. The power that was allocated to the powered device is reclaimed into the global power budget. If you do not specify a wattage, the switch delivers the maximum value.

- Static—The switch pre-allocates power to the port even when no powered device is connected and makes sure that power is available for the port. The switch allocates the port-configured maximum wattage, and the amount is never adjusted through the IEEE class or by CDP messages from a powered Cisco end device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed to be powered when it is connected to the static port. The port no longer participates in the first-come, first-served model.

  However, if the powered-device IEEE class is greater than the maximum wattage, the switch does not supply power to it. If the switch learns through CDP messages that a powered Cisco end device needs more than the maximum wattage, the powered device is shut down.

  If you do not specify a wattage, the switch pre-allocates the maximum value. The switch powers the port only if it discovers a powered device. Use the static setting on a high-priority interface.

- Off—The switch disables powered-device detection and never powers the PoE port, even if an unpowered device is connected. Use this mode only when you want to make sure that power is never applied to a PoE port, making the port a data-only port.

Maximum Power Allocation (cutoff power) on a PoE Port

The switch determines the cutoff power on a PoE port in this order.

1. Manually when you configure the power level to budge for the port
2. Manually when you configure the power level that limits the power that is allocated to the port
3. Automatically when the switch sets the power usage of the device by using the IEEE classification and LLDP power negotiation or CDP power negotiation

If you do not manually configure the cutoff-power value, the switch can automatically determine the value by using CDP power negotiation when connected to a Cisco end device. If the switch cannot determine the value by using one of these methods, it uses the default value of 15.4 W.

With PoE+, if you do not manually configure the cutoff-power value, the switch determines it by using one of the following:

- The device IEEE classification and LLDP power negotiation
- CDP power negotiation with a Cisco end device

If CDP or LLDP is not enabled, the default value of 30 W is applied. However, without CDP or LLDP, the switch does not allow devices to consume more than 15.4 W of power. Values from 15,400...30,000 mW are allocated based on only CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP negotiation, the device can be in violation of the maximum current limitation. The device can experience a fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.

Power Consumption Values

You can configure the initial power allocation and the maximum power allocation on a port. However, these values are only the configured values that determine when the switch turns on or turns off power on the PoE port. The maximum power allocation is not the same as the actual power consumption of the powered device. When you manually set the maximum power allocation, you must consider the power loss over the cable from the port to the powered device. The cutoff power is the sum of the rated power consumption of the powered device and the worst-case power loss over the cable.

The actual amount of power that is consumed by a powered device on a PoE port is the cutoff-power value plus a calibration factor of 500 mW (0.5 W). The actual cutoff value is approximate and varies from the configured value by a percentage of the configured value. For example, if the configured cutoff power is 12 W, the actual cutoff-value is 11.4 W, which is 0.05% less than the configured value.

Because the switch supports external removable power supplies for PoE/PoE+ and can configure the budget per the power supply that is used, the total amount of power available varies depending on the power supply configuration:

- If a power supply is removed and replaced by a new power supply with less power and there is insufficient power for the powered devices, power is denied to PoE ports that are in Auto mode. If there is still insufficient power, power is denied to PoE ports in Static mode. In both cases, power is denied in descending order of the port numbers.
- If the new power supply supports more power than the previous one, and more power is available, power is granted to the PoE ports in Static mode. If power is still available, the power is granted to PoE ports in Auto mode. In both cases, power is granted in ascending order of the port numbers.

IMPORTANT For power to be assigned accurately, the total wattage of the power supply must be manually configured via Device Manager or CIP.

Configure PoE Ports via Device Manager

From the Configure menu, choose Power Management.

Figure 37 - PoE Configuration for Stratix 5410 Switches

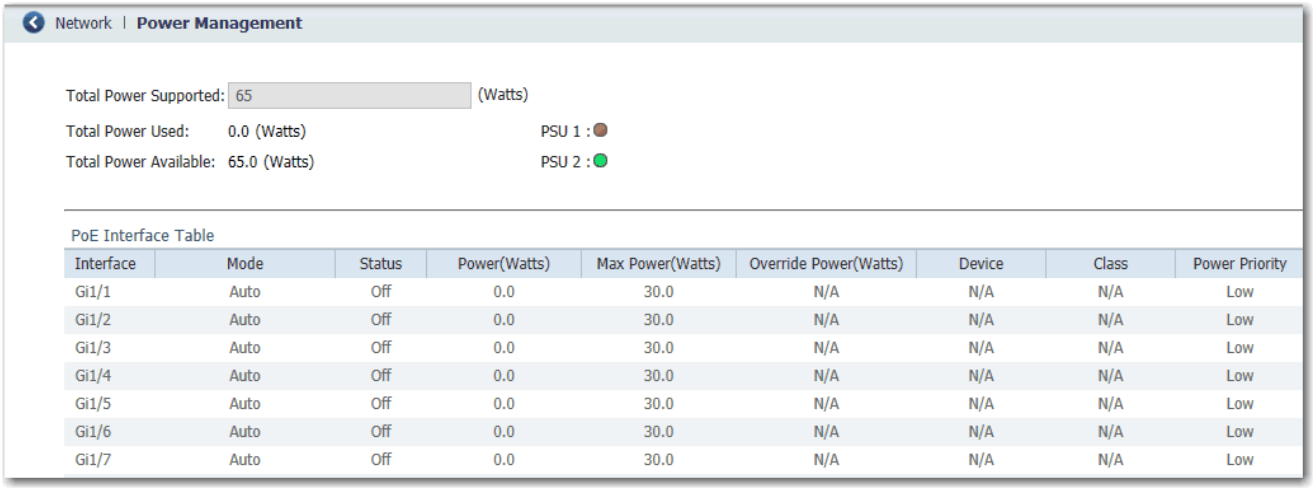


Figure 38 - PoE Configuration for Stratix 5400, Stratix 5700, and ArmorStratix 5700 Switches

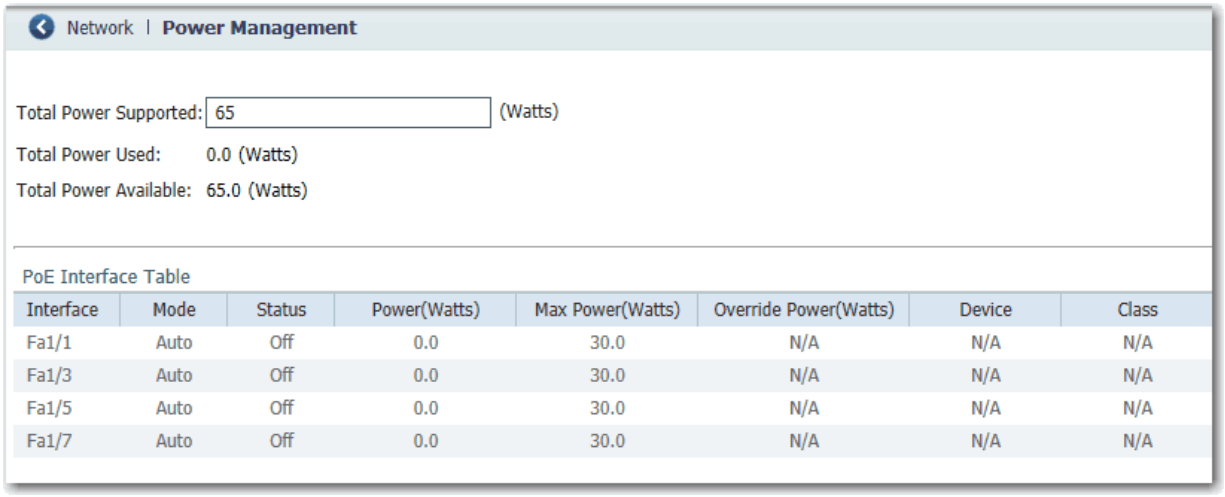


Figure 39 - PoE Configuration for Stratix 8000/8300 Switches

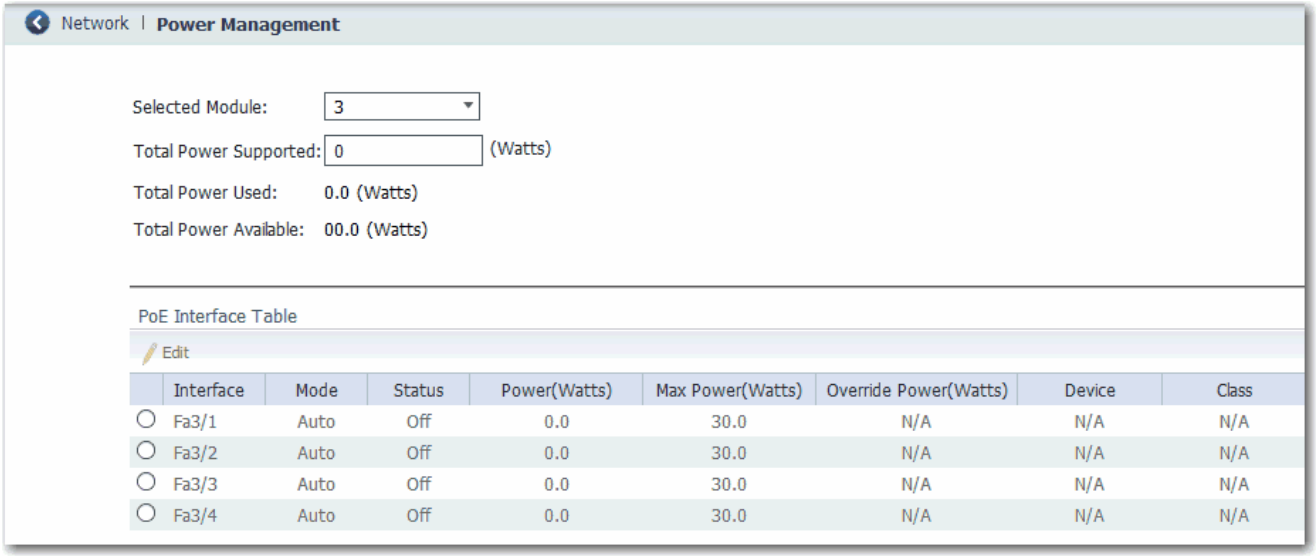


Table 84 - Power Management Fields

Field	Description
Selected Module (Stratix 8000/8300 switches)	Choose a connected PoE module for which to view status information: • 2—Module in the left position • 3—Module in the right position
Total Power Supported	To limit the total PoE power budget, type an appropriate value that is based on the power source: • A 48V power source supports a maximum of 65 W. • A 54V power source supports a maximum of 130 W. When you save this setting, it changes the total PoE power budget and resets the powered devices to meet the new budget. **IMPORTANT:** A mismatch between the total power that is supported and the power supply can cause damage to the switch. Take care not to oversubscribe the power supply: • If you intend to connect to a power supply that allows more wattage than configured, change the power supply and then specify the total power supported. • If you intend to connect to a power supply that allows less wattage than configured, change the total power that is supported to an appropriate value and then change the power supply.
Total Power Used	Displays the amount of power the module is using.
Total Power Available	Displays the amount of unused power available to the module.
Interface	Displays the port number.

Table 84 - Power Management Fields (Continued)

Field	Description
Mode	Displays the Power Management mode of the port: • Auto—(Default) Enables the detection of powered devices and automatically allocates power to the PoE port if a device is connected. To limit the power that is used by this port, adjust the Max Power setting. • Static—Reserves power for this port even when no device is connected to make sure that power is provided upon device detection. You can also choose Static mode to pre-allocate power to a specific port. The switch allocates power to Static mode ports before it allocates power to Auto mode ports. • Off—PoE is disabled. For more information, see Power Management Modes on page 316.
Status	Displays whether PoE is enabled (on) or disabled (off) on the port.
Power (Watts)	Displays the amount of power that is allocated to the port.
Max Power (Watts)	Displays the maximum amount of power available to the port: PoE ports: 4…15.4 W PoE+ ports: 4…30 W
Override Power (Watts)	Indicates the power override configured for the port. This configuration overrides both the IEEE classification that is shown in the Class column and power negotiation. If no override is configured, the field displays N/A. You can configure a power override only by using the Command-line interface (CLI). For more information, see the Cisco IE-3000 Software Configuration Guide. **EXAMPLE:** An administrator can choose to configure an override when the power requirement of a connected device is known and is less than the maximum value for the class. For instance, if a device requires only 5 W but is in Class 0, which allows a maximum of 15.4 W, configuring an override allows more power to other devices.
Device	Displays the device that is connected to the port. If no device is connected to the port, the field displays N/A.
Class	Displays the power classification of the powered device (PD). For power classification descriptions, see Table 83 on page 315.
Power Priority (Stratix 5410 switches)	Choose a power priority to assign to the port if there is a reduced power budget, such as a power supply failure. The system selectively removes PoE power and shuts down lower priority ports to keep higher priority ports active. When multiple ports have the same priority level, ports are shut down from highest port number to lowest port number. The system removes power from only the number of ports necessary to maintain system operation without power cycling or other such disruptive results. • Low (default) • High

Configure PoE via the Logix Designer Application

In the navigation pane, click PoE.

Figure 40 - PoE Configuration for Stratix 5410 Switches

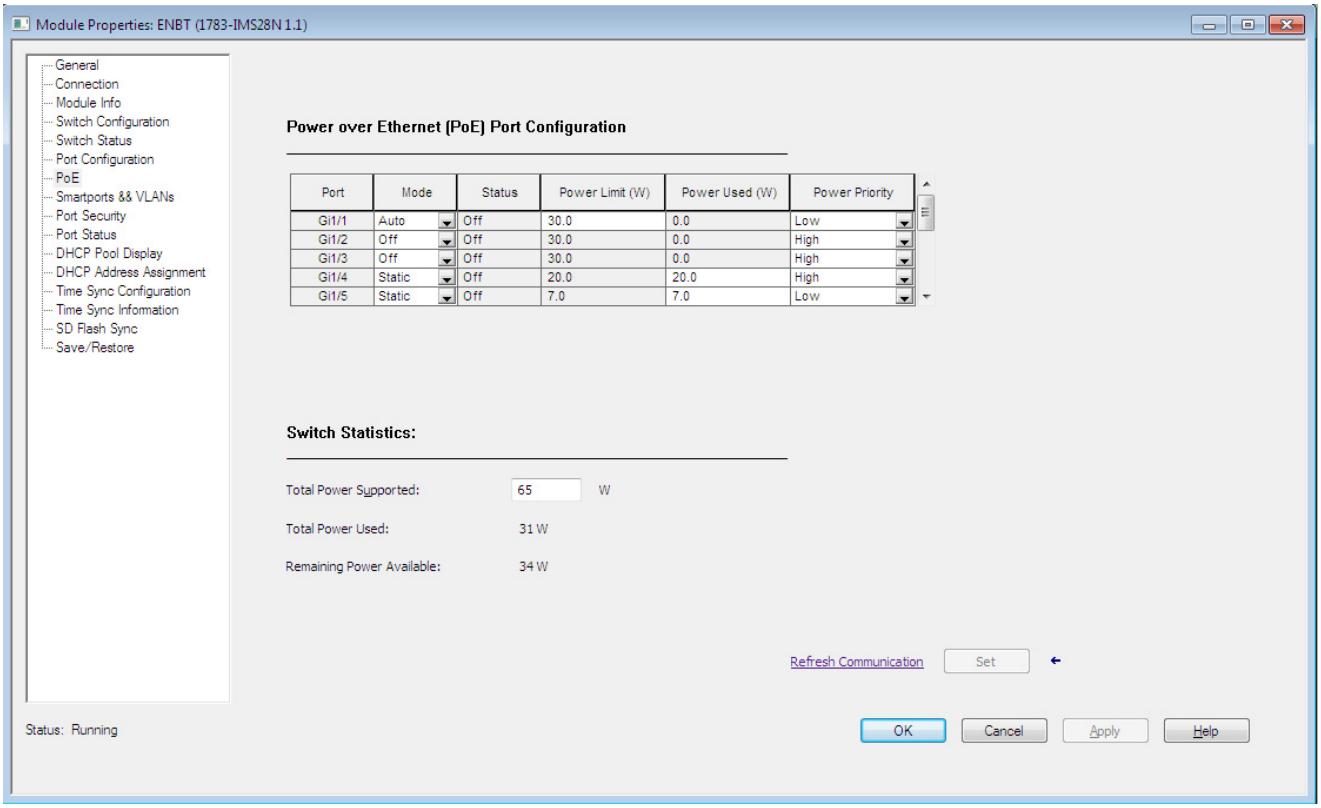


Figure 41 - PoE Configuration for Stratix 5400, Stratix 5700, and ArmorStratix 5700 Switches

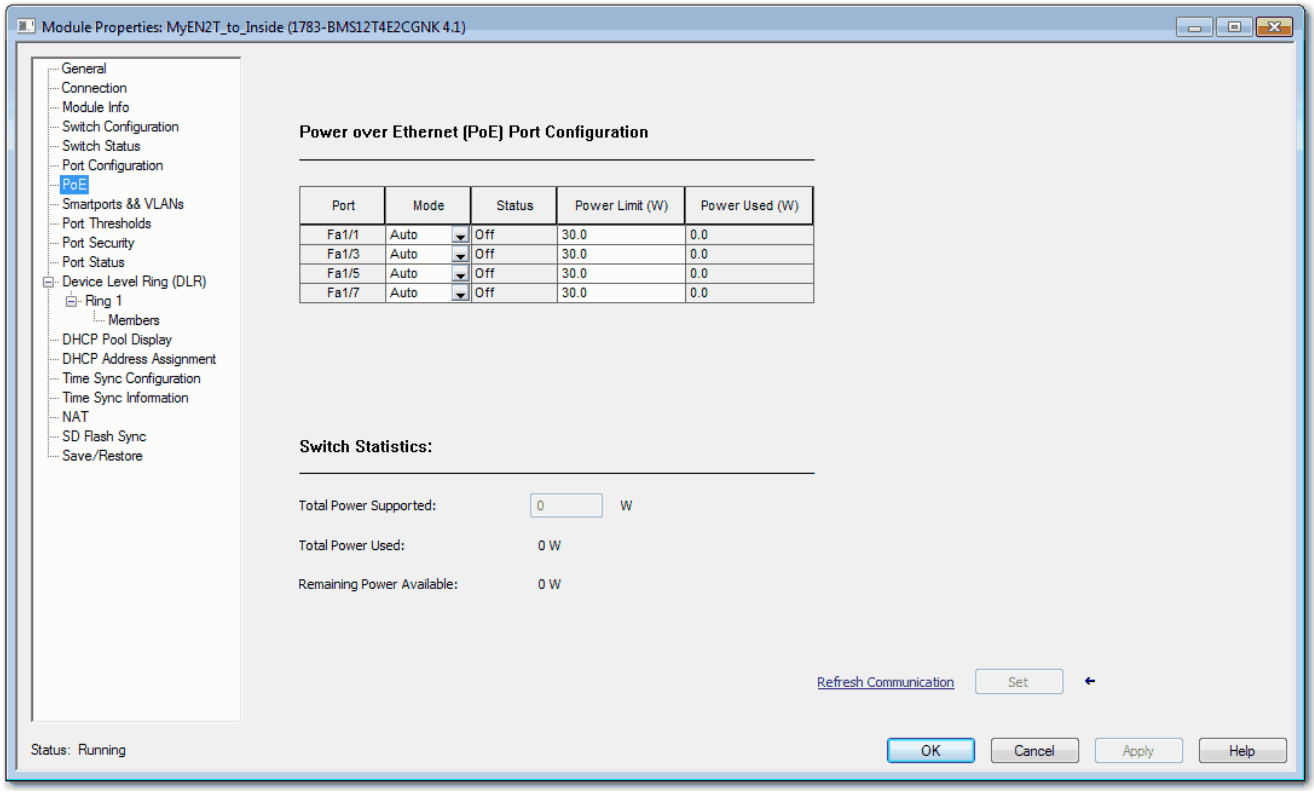


Figure 42 - PoE Configuration for Stratix 8000/8300 Switches

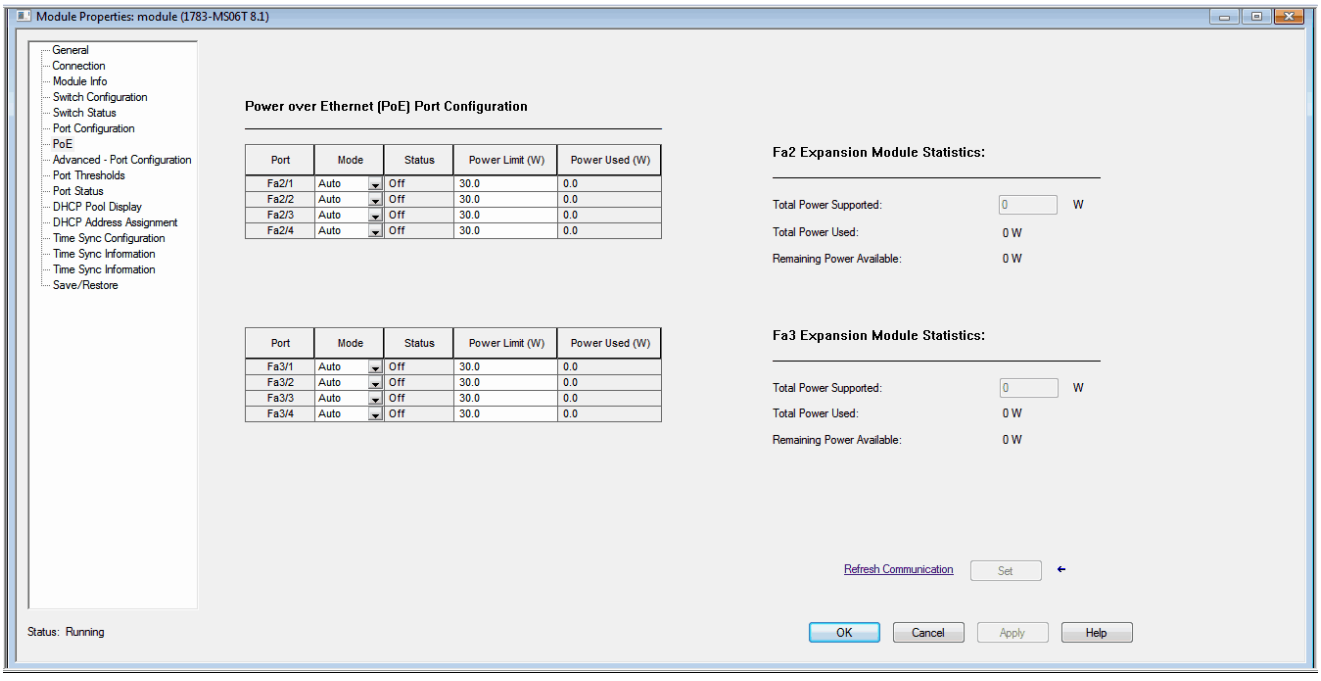


Table 85 - PoE Fields

Field	Description
Power over Ethernet (PoE) Port Configuration	
Port	Displays the port number.
Mode	Displays the Power Management mode of the port: • Auto—Enables the detection of powered devices and automatically allocates power to the PoE port if a device is connected. This setting is selected by default. To limit the power that is used by this port, adjust the value Power Limit field. • Static—Reserves power for this port even when no device is connected to make sure that power is provided upon device detection. You can also choose Static mode to pre-allocate power to a specific port. The device allocates power to Static mode ports before it allocates power to Auto mode ports. • Off—PoE is disabled. For more information, see Power Management Modes on page 316.
Status	Displays the status of the port: • 0—The status is unknown. • 1—PoE is enabled. Power is supplied to the port with no errors. • 2—PoE is not enabled. Power is not supplied to the port. • 3—PoE is enabled, but the device denied power to the port. • 4—PoE is enabled, but a system fault occurred while power was supplied to the port. • 5—PoE is enabled, but the port overdrew power.
Power Limit (W)	Displays the maximum amount of power available to the port: PoE ports: 4…15.4 W PoE+ ports: 4…30 W If the port is in Auto mode, you can enter a value. The default value is 15.4 W.
Power Used (W)	Displays the amount of power currently in use by the port. If the port is in Auto mode, the default value is 15.4 W. If the port is in Static mode, you can enter a value to reserve power for the port.
Power Priority (Stratix 5410 switches)	Choose a power priority to assign to the port if there is a reduced power budget, such as a power supply failure. The system selectively removes PoE power and shuts down lower priority ports to keep higher priority ports active. When multiple ports have the same priority level, ports are shut down from highest port number to lowest port number. The system removes power from only the number of ports necessary to maintain system operation without power cycling or other such disruptive results. • Low (default) • High
Switch/Expansion Module Statistics	
Total Power Supported	To limit the total PoE power budget, type an appropriate value that is based on the power source: • A 48V power source supports a maximum of 65 W. • A 54V power source supports a maximum of 130 W. For Stratix 5410 switches use the following values: • One power supply supports a maximum of 65 W. • Two power supplies support a maximum of 185 W. When you save this setting, it changes the total PoE power budget and resets the powered devices to meet the new budget. **IMPORTANT:** A mismatch between the total power that is supported and the power supply can cause damage to the device. Take care not to oversubscribe the power supply: • If you intend to connect to a power supply that allows more wattage than configured, change the power supply and then specify the total power supported. • If you intend to connect to a power supply that allows less wattage than configured, change the total power that is supported to an appropriate value. Then change the power supply.
Total Power Used	Displays the amount of power in watts the device is using.
Remaining Power Available	Displays the amount of unused power in watts available to the device.

Resilient Ethernet Protocol (REP)

REP provides an alternative to Spanning Tree Protocol (STP) to control network rings and loops, handle link failures, and improve convergence time. REP controls a group of ports that are connected in a segment, makes sure that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

REP is a segment protocol. One REP segment is a chain of ports that are connected to each other and configured with a segment ID. Each segment consists of standard (transit) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium; however, on any link, only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interfaces. Selecting the Switch for Automation Smartport enables Layer 2 trunking. REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

You can construct almost any type of network that is based on REP segments. REP also supports VLAN load-balancing, controlled by the primary edge port but occurring at any port in the segment.

These types of REP ports are selectable in Device Manager:

- Primary—This port is a primary edge port. This port always participates in VLAN load balancing in the REP segment.
- Edge—This port is a secondary edge port. It also participates in VLAN load balancing in the REP segment.

  Edge ports are termination points of an REP segment. You must configure two edge ports, including one primary edge port, for each REP segment. Entering edge without primary configures the port as a secondary edge port. Primary and secondary edge ports must be configured even if support of VLAN balancing is not required.
- Transit—This port is a non-edge port in the REP segment.
- No-Neighbor Primary—This port is a primary edge port connected a non-REP switch.
- No-Neighbor—This port is a secondary edge port that is connected to a non-REP switch.

  The no-neighbor edge ports contain all properties of regular edge ports. These ports enable the construction of a REP ring containing a switch that does not support REP protocol.
- None—This port is not part of the REP segment.

REP and STP can coexist on the same switch, but not on the same port. REP does not interact with STP. For example, if a port is configured as an REP port, STP is disabled on that port. STP bridge protocol data units (BPDUs) are not accepted on or sent from REP ports. However, adjacent REP and STP rings or domains can share a common link. This common link can be used for passing REP and STP date plane traffic, or for the STP control plane traffic.

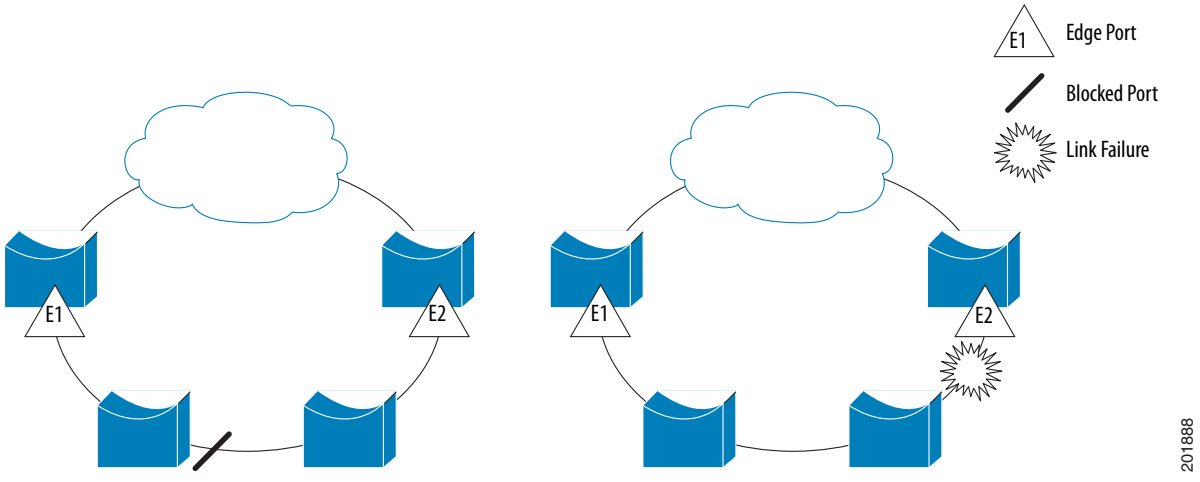
Figure 43 shows an example of a segment consisting of six ports that are spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), one port is blocked, shown by the diagonal line. When there is a failure in the network, as shown in the diagram on the right, the blocked port returns to the forwarding state to minimize network disruption.

REP Open Segment

The segment that is shown in Figure 43 is an open segment. There is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop and you can connect the segment edges to any network. All hosts that are connected to switches inside the segment have two possible connections to the rest of the network through the edge ports. However, only one connection is accessible at any time. If a failure causes a host to be unable to access its usual gateway, REP unblocks all ports to make sure that connectivity is available through the other gateway.

In the following example, E1 or E2 can be configured as the primary edge port.

Figure 43 - Open Segment Example

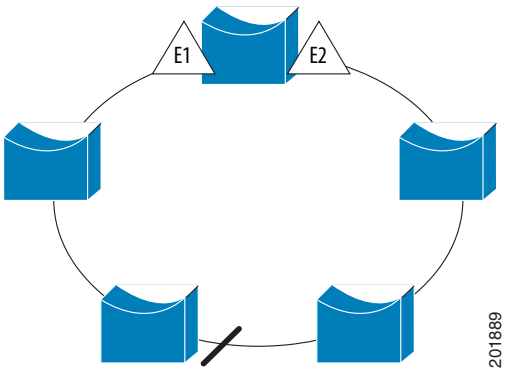


REP Ring Segment

The segment that is shown in Figure 44, with both edge ports on the same switch, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two switches in the segment.

In the following figure, E1 or E2 can be configured as the primary edge port.

Figure 44 - Ring Segment Example



REP segments have these characteristics:

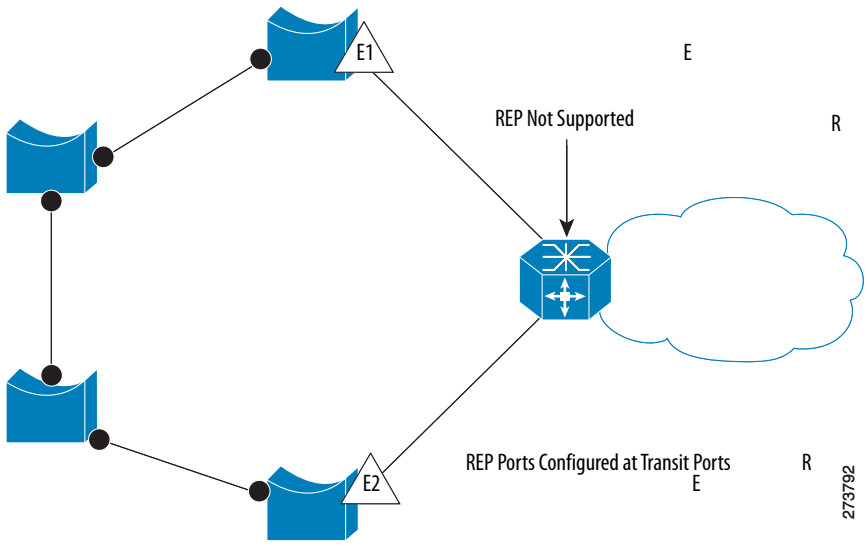
- If all ports in the segment are operational, one port (referred to as the alternate port) is in the blocked state for each VLAN.
- If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to support ongoing connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.

Access Ring Topologies

In access ring topologies, the neighboring switch cannot support REP, as shown in Figure 45. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all properties of edge ports. You can configure them the same as any edge port, including configuring them to send STP or REP topology change notices to the aggregation switch. In this case, the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

In the example that is shown in Figure 45, E1 or E2 can be configured as the primary no-neighbor port.

Figure 45 - Ring Topology Example



REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only one failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.

Configure REP in networks only with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Link Integrity

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines the neighbor port to become the alternate port and which ports forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to the format used by the spanning tree algorithm: a port number (unique on the bridge), associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared as operational after it performs a three-way handshake with a neighbor in the same segment.

Configure REP via Device Manager

From the Configure menu, choose REP.

To create a REP segment, set a segment ID and port type for a switch port.

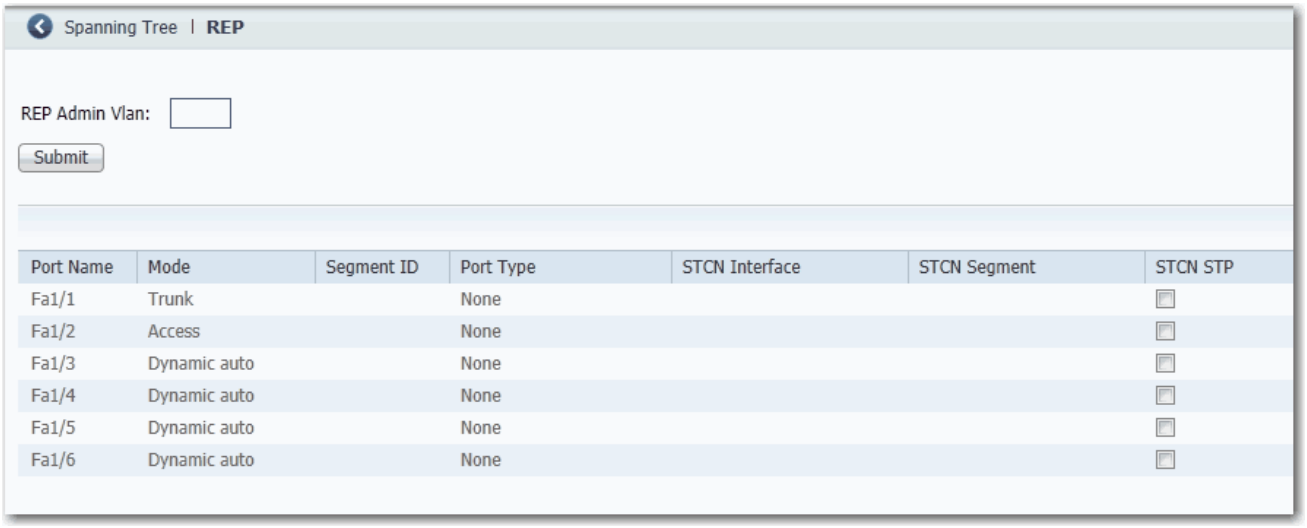


Table 86 - REP Fields

Field	Description
REP Admin VLAN	The administrative VLAN. The range is 2…4094. The default is VLAN 1. REP ports are assigned to the same REP Admin VLAN. If the REP Admin VLAN changes, all REP ports are automatically assigned to the new REP Admin VLAN.
Port Name	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet).
Mode	The administrative mode. To set this mode, from the Configure menu, choose Port Settings.
Segment ID	The ID of the segment. The segment ID range is from 1…1024. If no segment ID is set, REP is disabled.
Port Type	Each REP segment must have exactly two primary edge ports and can have secondary ports to use when a primary port fails. You can specify preferred primary and secondary ports. Configuring a port as preferred does not mean that it becomes the alternate port but gives it a slight edge among equal contenders. You can indicate that a port connects to switches that do not support REP. Choose one of these port types: • Edge—A secondary edge port that participates in VLAN load balancing. • Edge no-neighbor—A secondary edge port that is connected to a non-REP switch. • Edge no-neighbor preferred—A secondary edge port that is connected to a non-REP switch and is the preferred alternate port for VLAN load balancing. • Edge no-neighbor primary—A secondary edge port that always participates in VLAN load balancing in this REP segment and is connected to a non-REP switch. • Edge no-neighbor primary preferred—An edge port that always participates in VLAN load balancing in this REP segment, is connected to a non-REP switch, and is the preferred port for VLAN load balancing. • Edge preferred—A secondary edge port that is the preferred alternate port for VLAN load balancing. • Edge primary—An edge port that always participates in VLAN load balancing in this REP segment. • Edge primary preferred—An edge port that always participates in VLAN load balancing in this REP segment and is the preferred port for VLAN load balancing. • None—This port is not part of the REP segment. The default is None. • Preferred—A secondary edge port that is the preferred alternate port for VLAN load balancing.

Table 86 - REP Fields (Continued)

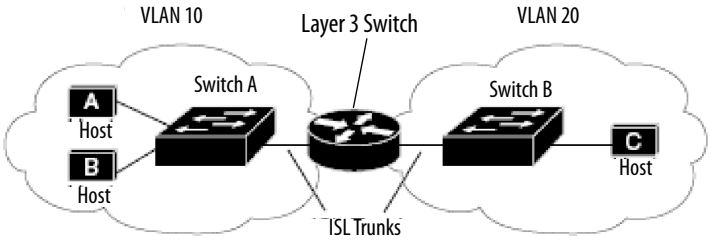
Field	Description
STCN Interface	Configure segment topology change notices (STCNs) for a port. The default is None. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.
STCN Segment	Configure STCNs to a segment ID. The default is a blank field. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.
STCN STP	Configure STCNs to an STP network. The default is cleared checkbox. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.

Layer 3 Routing

Stratix 8300 and Stratix 5400 and Stratix 5410 Layer 3 firmware models use IP address routing to map subnetworks (subnets) to an individual VLAN. In some network environments, VLANs are associated with individual networks or subnets. In an IP network, each subnetis mapped to an individual VLAN. Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, network devices in different VLANs cannot communicate with one another without a Layer 3 device to route traffic between the VLAN, referred to as inter-VLAN routing. You configure one or more Layer 3 capable switches to route traffic to the appropriate destination VLAN.

Figure 46 shows a basic routing topology.

Figure 46 - Example of Routing Topology



Switch A is in VLAN 10, and Switch B is in VLAN 20. The Layer 3 switch has an interface in each VLAN.

When Host A in VLAN 10 communicates with Host B in VLAN 10, it sends a packet that is addressed to that host. Switch A forwards the packet directly to Host B, without sending it to the Layer 3 switch.

When Host A sends a packet to Host C in VLAN 20, Switch A forwards the packet to the Layer 3 switch, which receives the traffic on the VLAN 10 interface. The Layer 3 switch checks the routing table, finds the correct outgoing interface, and forwards the packet on the VLAN 20 interface to Switch B. Switch B receives the packet and forwards it to Host C.

Types of Routing

Stratix 8300 and Stratix 5400 and Stratix 5410 Layer 3 firmware models can route packets by using these methods.

Table 87 - Layer 3 Routing

Feature	Description
Enhanced Interior Gateway Routing Protocol (Stratix 8300 switches)	See Enhanced Interior Gateway Routing Protocol (EIGRP) on page 332.
Open Shortest Path First (Stratix 8300 switches)	See Open Shortest Path First (OSPF) on page 337.
Static and connected routing	See Static and Connected Routing on page 344.
Dynamic routing	Dynamic routing protocols are used by Layer 3 switches to calculate dynamically the best route for forwarding traffic. There are two types of dynamic routing protocols: • Distance-vector protocols • Link-state protocols Layer 3 switches using distance-vector protocols maintain routing tables with distance values of networked resources, and periodically pass these tables to their neighbors. Distance-vector protocols use one or a series of metrics for calculating the best routes. These protocols are easy to configure and use. The switch supports these distance-vector protocols: • Routing Information Protocol (RIP), which uses a distance metric (cost) to determine the best path • Border Gateway Protocol (BGP), which adds a path vector mechanism The switch also supports the Open Shortest Path First (OSPF) link-state protocol and Enhanced IGRP (EIGRP). The features add link-state routing features to traditional Interior Gateway Routing Protocol (IGRP) to improve efficiency. Routers that use link-state protocols maintain a complex database of network topology, which is based on the exchange of link-state advertisements (LSAs) between routers. An event in the network triggers LSAs, which speeds up the convergence time or time that is required to respond to these changes. Link-state protocols respond quickly to topology changes, but require greater bandwidth and more resources than distance-vector protocols
Unicast routing	Unicast routing is used for all network processes where a private or unique resource is requested.
Multicast routing	In multicast routing, routers create optimal distribution paths for data that is sent to a multicast destination address spanning tree in real time. Multicast routing protocols that are supported are PIM (SM, SM, SDM), DVMRP tunneling.
Redundant routing	Redundant routing localizes the effects of route failures, and reduces control traffic overhead and route reconfiguration time by providing a redundant network path. Redundant routing protocols that are supported are HSRP (Hot Standby Router Protocol) and CEF (Cisco Express Forwarding).
IPv6 routing	IPv6 network segments, also known as links or subnets, are connected by IPv6 routers, which are devices that pass IPv6 packets from one network segment to another. EIGRP is the supported protocol.
VRF Lite	Virtual Routing and Forwarding (VRF) lets multiple instances of a routing table to coexist within the same router simultaneously. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. The simplest form of VRF implementation is VRF Lite. In this implementation, each router within the network participates in the virtual routing environment in a peer-based fashion.

See the following manuals:

- For more information about routing features and how to modify them, see the Cisco IE3000 Switch Software Configuration Manual, available from http://www.Cisco.com.
- For information about using the CLI to configure routing, see the Cisco IE3000 Switch Command-Line Interface Manual, available from http://www.Cisco.com.

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is available on Stratix 8300switches and Stratix 5400 and 5410 switches with Layer 3 firmware.

EIGRP is a Cisco proprietary, distance-vector-routing protocol. Key capabilities that distinguish EIGRP from other routing protocols include fast convergence, support for variable-length subnet mask, support for partial updates, and support for multiple network layer protocols.

A router that runs EIGRP stores all neighbor routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries propagate until an alternate route is found. Its support for variable-length subnet masks permits routes to be automatically summarized on a network number boundary. In addition, EIGRP can be configured to summarize on any bit boundary at any interface. EIGRP does not make periodic updates. Instead, it sends partial updates only when the metric for a route changes. Propagation of partial updates is automatically bounded so that only those routers that need the information are updated.

Neighbor discovery is the process that the EIGRP router uses to learn dynamically of other routers on directly attached networks. EIGRP routers send out multicast hello packets to announce their presence on the network. You can also define static neighbors, which receive unicast packets. When the router receives a hello packet from a new neighbor, it sends its topology table to the neighbor with an initialization bit set. When the neighbor receives the topology update with the initialization bit set, the neighbor sends its topology table back to the EIGRP router. Once this neighbor relationship is established, routing updates are not exchanged unless there is a change in the network topology.

EIGRP uses the Diffusing Update Algorithm (DUAL), which provides loop-free operation at every instance throughout a route computation. DUAL allows all devices that are involved in a topology change to synchronize simultaneously. Routers that are not affected by topology changes are not involved in recomputations.

To configure EIGRP, create an EIGRP instance and associate networks. EIGRP sends updates to the interfaces in the specified networks. If you do not specify an interface network, it is not advertised in any EIGRP update.

Configure EIGRP via Device Manager

From the Configure menu, choose EIGRP.

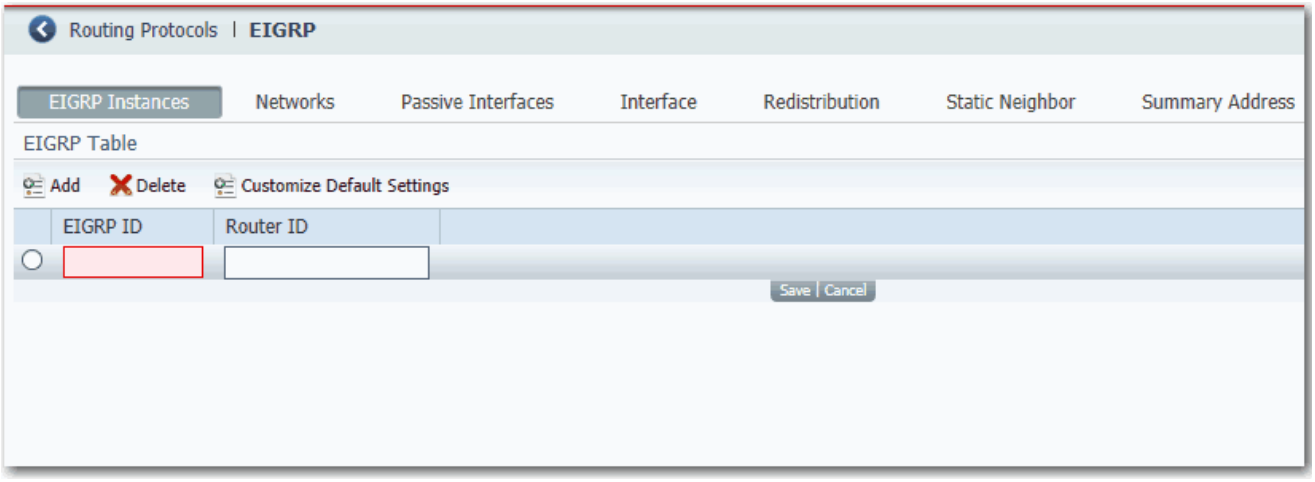


Table 88 - EIGRP Fields

Field	Description
EIRGP Instances—Add EIGRP instances to the EIGRP table. To customize the default settings for an instance, see page 336.	
EIGRP ID	Type the Autonomous System (AS) number of the EIGRP routing process. Valid values: 1…65535.
Router ID	Type the IP address of the router that is associated with the EIGRP instance.
Networks—Add EIGRP networks to the Network table.	
EIGRP ID	Choose the Autonomous System (AS) number of the EIGRP routing process.
Network Address	Type the address of the network that is associated with an EIGRP routing process. EIGRP sends updates to the interfaces in the specified networks.
Wildcard Mask	Choose a wildcard mask. A wildcard mask indicates a subnetwork, bitwise complement of the subnet mask.
Passive Interfaces—Add passive interfaces to prevent other routers on a local network from dynamically learning about routes.	
EIGRP ID	Choose an EIGRP ID.
Suppress routing updating on all interfaces	Check the checkbox to suppress routing update messages from being sent through all interfaces.
Interface	Choose a Layer 3 interface to suppress sending routing updates through.
Passive	Check the checkbox to suppress routing update messages from being sent through the corresponding interface.
Interface—Add EIGRAP interface instances.	
EIGRP ID	Choose the Autonomous System (AS) number of the EIGRP routing process.
Interface	Choose a Layer 3 interface that is associated with the EIGRP ID.
Hello Interval	Type the hello interval for the EIGRP interface instance. Valid values: 1…65535 Default: 60 seconds for low-speed nonbroadcast multiaccess (NBMA) networks and 5 seconds for all other networks
Hold Time	Type the hold time interval for an EIGRP routing process. The hello packet advertises the hold time. The hold time indicates to EIGRP neighbors the length of time for the neighbor to consider the router reachable. Valid values: 1…65535 seconds Default: 180 seconds for low-speed NBMA networks and 15 seconds for all other networks

Table 88 - EIGRP Fields (Continued)

Field	Description
Enable Split Horizon	Check the checkbox to enable split horizon on the interface. Split horizon controls the sending of EIGRP update and query packets. When split horizon is enabled on an interface, update and query packets are not sent to destinations for which this interface is the next hop. Controlling update and query packets in this manner reduces the possibility of routing loops. By default, split horizon is enabled on all interfaces. In general, we recommend that you not change the default state of split horizon unless you are certain that your application requires the change to properly advertise routes.
Delay	Type the delay value in tens of microseconds for the interface. The interface delay value to use in EIGRP distance calculations. Type the value in tens of microseconds for the interface.
Authentication	
Enable MD5 Authentication	Check the checkbox to enable message digest algorithm 5 (MD5) authentication in EIGRP packets. EIGRP route authentication provides MD5 authentication of routing updates from the EIGRP routing protocol. The MD5 keyed digest in each EIGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources. All EIGRP neighbors on interfaces that are configured for EIGRP message authentication must be configured with the same authentication mode and key for adjacencies to be established.
Key Chain Name	Choose an authentication key chain for EIGRP.
MD5 Keys and IDs	
Key Chain Name	Type a name for the authentication key chain for EIGRP authentication.
MD5 Key ID	Type an identification number for an authentication key on the key chain. The range of keys is from 0…2147483647. The key identification numbers do not need to be consecutive.
MD5 Key	Type an authentication string that must be sent and received in the EIGRP packets being authenticated. The string can contain from 1…80 uppercase and lowercase alphanumeric characters.
Redistribution—Redistribute routes that are discovered by RIP and OSPF into the EIGRP routing process. You can also redistribute static and connected routes into the EIGRP routing process. If connected routes fall within the range of a network statement in the EIGRP configuration, you do not need to redistribute the routes.	
EIGRP ID	Choose the Autonomous System (AS) number of the EIGRP routing process.
Protocol	Click the route type for redistribution into the EIGRP routing process: • Static—-Redistributes static routes into the EIGRP routing process. • Connected—Redistributes connected routes into the EIGRP routing process. • OSPF—Redistributes routes from an OSPF routing process into the EIGRP routing process. • RIP—Redistributes routes from an RIP routing process into the EIGRP routing process.
Match	(Optional). Match and set properties of routes that are imported from OSPF: • Internal—Matches internal OSPF routes. • External 1—Matches Type 1 external routes. • External 2—Matches Type 2 external routes. • NSSA External 1—Matches Type 1 NSSA routes. • NSSA External 2—Matches Type 2 NSSA routes.
Bandwidth	Type the minimum bandwidth of the route in kilobits per second. Valid values: 1…4294967295
Delay	Type the route delay in tens of microseconds. Valid values: 1 or any positive number that is a multiple of 39.1 nanoseconds
Reliability	Type a number from 0 through 255 that represents likelihood of successful packet transmission. Valid values: 0…255 where 255 means 100 percent reliability; 0 means no reliability
Loading	Type a number that represents the effective bandwidth of the route. Valid values: 1…255 where 255 is 100 percent loading
MTU	Type the smallest allowed value for the maximum transmission unit (MTU) in bytes. Valid values: 1…65535

Table 88 - EIGRP Fields (Continued)

Field	Description
Static Neighbor—EIGRP hello packets are sent as multicast packets. If an EIGRP neighbor is located across a nonbroadcast network, such as a tunnel, you must manually define that neighbor. When you manually define an EIGRP neighbor, hello packets are sent to that neighbor as unicast messages.	
EIGRP ID	Choose the Autonomous System (AS) number of the EIGRP routing process.
Neighbor	Type the IP address of the neighbor.
Interface	Choose the interface through which the neighbor is available.
Summary Address—Define summary addresses in either of these scenarios: • If you want to create summary addresses that do not occur at a network number boundary • If you want to use summary addresses on a router with automatic route summarization disabled. If any more specific routes are in the routing table, EIGRP advertises the summary address out the interface with a metric equal to the minimum of all more specific routes.	
EIGRP ID	Choose the Autonomous System (AS) number of the EIGRP routing process.
Network Address	Type the IP address of the summary address.
Net Mask	Choose the network mask of the summary address.
Administrative Distance	Type the distance value of the summary address. Default: 5

To change the default settings after adding an EIGRP instance, on the EIGRP Instances tab, click the button in the row to customize, and then click Customize Default Settings.

IMPORTANT Setting metrics is complex and is not recommended without guidance from an experienced network designer.

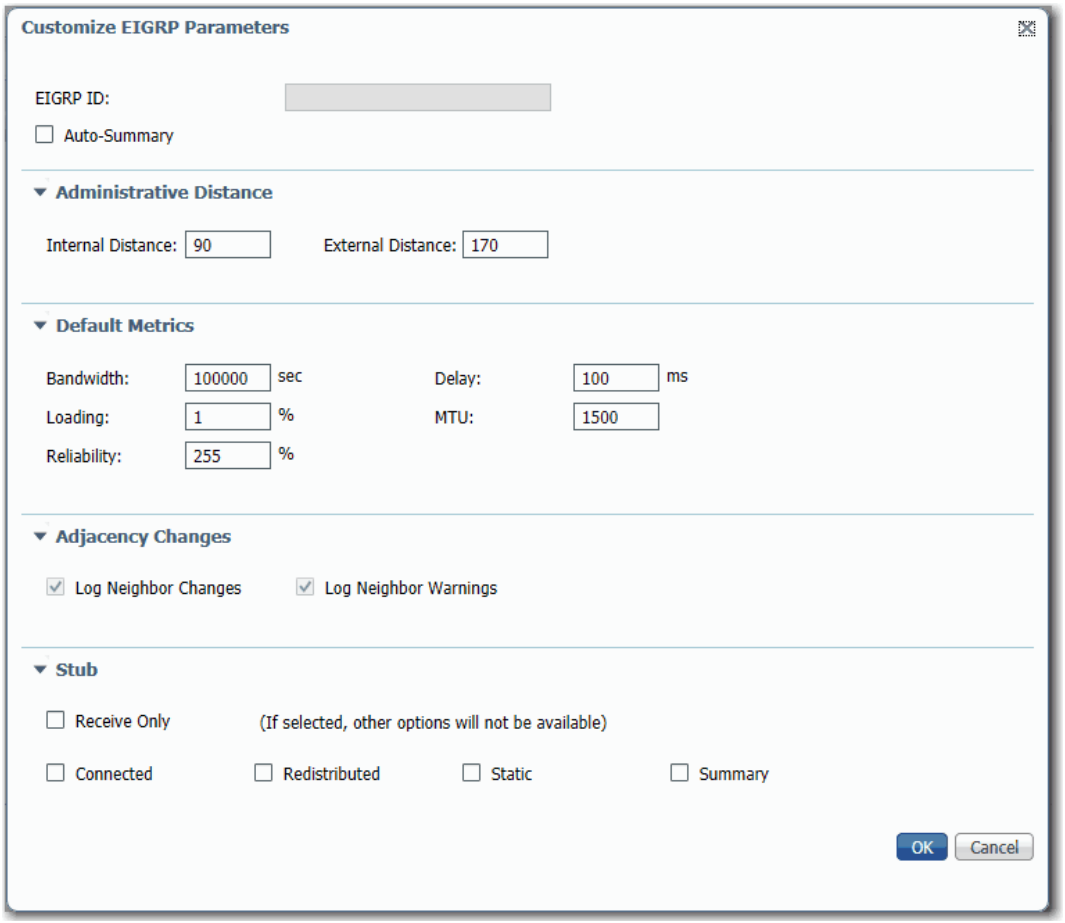


Table 89 - Customize EIGRP Parameters

Field	Description
EIGRP ID	(Not editable). Displays the Autonomous System (AS) number of the EIGRP routing process.
Auto-Summary	Check the checkbox to allow the automatic summarization of subnet routes into network-level routes. This feature is disabled by default (the software sends subprefix routing information across classful network boundaries). EIGRP summary routes are given an administrative distance value of 5. You cannot configure this value.
Administrative Distance	
Internal Distance	Type an administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system. Valid values: 1…255 Default: 90
External Distance	Type an administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Valid values: 1…255 Default: 170
Metrics	
Bandwidth	Type the minimum bandwidth of the route in kilobits per second. Valid values: 1…4294967295
Loading	Type a number that represents the effective bandwidth of the route. Valid values: 1…255 where 255 is 100 percent loading
Reliability	Type a number that represents likelihood of successful packet transmission. Valid values: 0…255 where 255 means100 percent reliability; 0 means no reliability

Table 89 - Customize EIGRP Parameters

Field	Description
Delay	Type a route delay in tens of microseconds. Valid values: 1 or any positive number that is a multiple of 39.1 nanoseconds
MTU	Type the smallest allowed value for the maximum transmission unit (MTU), in bytes. Valid values: 1…65535
Adjacency Changes	
Log Neighbor Changes	Enables the logging of syslog messages when a neighbor state changes. Default: Disabled (no adjacency changes are logged)
Log Neighbor Warnings	Enables the logging of neighbor warning messages. Default: Disabled (no adjacency changes are logged)
Stub	
Receive Only	Check the checkbox to restrict the router from sharing any of its routes with any other router in the EIGRP autonomous system. When you enable this parameter, you cannot specify any other Stub parameters because it prevents any type of route from being advertised. Default: Disabled
Connected	Check the checkbox to permit EIGRP stub routing to send connected routes. If the connected routes are not covered by a network statement, they can be redistributed using the Redistributed parameter. Default: Disabled
Redistributed	Check the checkbox to permit EIGRP stub routing to advertise other routing protocols and autonomous systems. If this parameter is not enabled, EIGRP does not advertise redistributed routes. Default: Disabled
Static	Check the checkbox to permit EIGRP stub routing to advertise static routes. If you do not select this option, EIGRP does not send any static routes, including internal static routes that normally would be automatically redistributed. It is still necessary to redistribute static routes with the Redistributed parameter. Default: Disabled
Summary	Check the checkbox to permit EIGRP stub routing to advertise summary routes. You can manually create summary routes on the Summary Address page or automatically at a major network border router by enabling the Auto-Summary feature. Default: Disabled

Open Shortest Path First (OSPF)

OSPF is available on Stratix 8300switches and Stratix 5400 and 5410 switches with Layer 3 firmware.

OSPF is an interior gateway routing protocol that uses link states rather than distance vectors for path selection. OSPF propagates link-state advertisements (LSAs) rather than routing table updates. Because only LSAs are exchanged instead of the entire routing tables, OSPF networks converge more quickly than Routing Information Protocol (RIP) networks.

OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area contains an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors. Routing decisions are based on cost, which is an indication of the overhead that is required to send packets across a certain interface. The router calculates the cost of an interface that is based on link bandwidth rather than the number of hops to the destination. The cost can be configured to specify preferred paths.

The OSPF implementation on the switch conforms to the OSPF Version 2 specifications with support for these key features:

- Definition of stub areas.
- Routes that are learned through any IP routing protocol can be redistributed into another IP routing protocol. At the intradomain level, OSPF can import routes that are learned through EIGRP and RIP. OSPF routes can also be exported into RIP.
- Plain text and message digest algorithm 5 (MD5) authentication among neighboring routers within an area.
- Virtual links.
- Not-so-stubby-areas (NSSAs) per RFC 1587.

To enable OSPF, complete these steps.

1. Create an OSPF routing process.
2. Specify the range of IP addresses to be associated with the routing process.
3. Assign area IDs to be associated with that range.

OSPF typically requires coordination among many internal routers, area border routers (ABRs) connected to multiple areas, and autonomous system boundary routers (ASBRs). The minimum configuration uses all default parameter values, no authentication, and interfaces assigned to areas. If you customize your environment, make sure all routers have a coordinated configuration.

Configure OSPF via Device Manager

From the Configure menu, choose OSPF.

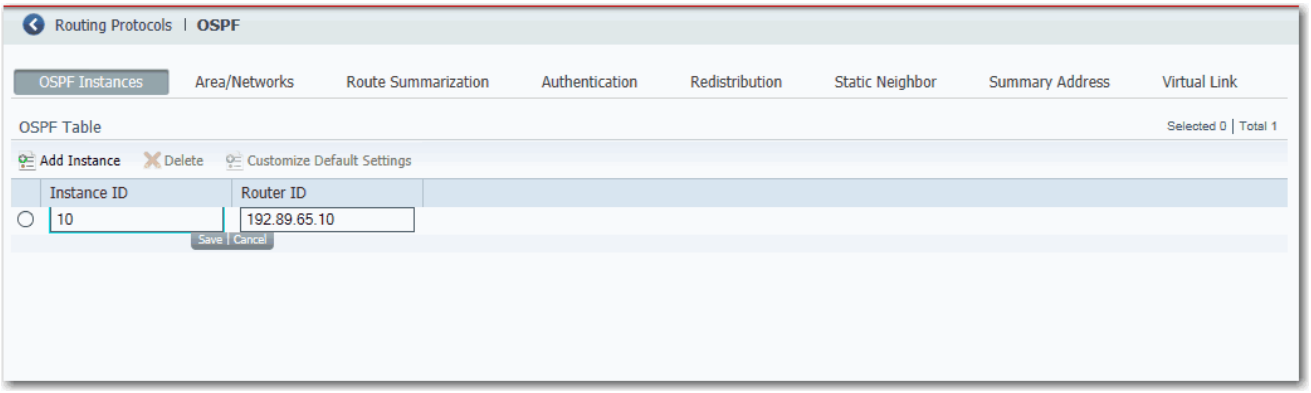


Table 90 - OSPF Fields

Field	Description
OSPF Instances—Add OSPF instances to the OSPF table. To customize the default settings for an instance, see page 342.	
Instance ID	Type a unique value to identify internally the OSPF routing process. Valid values: 1…65535
Router ID	Type the IP address of the router that is associated with the OSPF instance.
Area/Networks—Configure the area properties and networks for the OSPF instance.	
OSPF ID	Choose the OSPF routing process ID.
Area ID	Type an identifier of the area to associate with the OSPF address range. You can use either a decimal value or an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value.
Area Type	Click an area type and specify related parameters: • Normal—Normal areas can be either standard areas or transit (backbone) areas. Standard areas can accept intra-area, inter-area, and external routes. The backbone area is the central area to which all other areas in OSPF connect. • Stub—Stub areas do not receive information about external routes. – Summary—Allows sending link-state advertisements (LSAs) into the stub network. • NSSA—Not-so-stubby-areas are an extension of OSPF stub areas. However, an NSSA can import external routes into the OSPF routing domain. Every router within the same area must agree that the area is an NSSA. – Redistribution—Allows routes redistribution. – Summary—Allows sending LSAs into an NSSA network. – Default Information Originate—Enable on an area border router (ABR) to allow the importing of type 7 LSAs into an NSSA network.
Network Address	Type one or multiple interfaces to be associated with a specific OSPF area. **IMPORTANT:** Any individual interface can be attached to only one area. If the address ranges specified for different areas overlap, the system adopts the first area in the network list and ignore the subsequent overlapping portions. In general, we recommend that you configure address ranges that do not overlap to avoid inadvertent conflicts.
Network Mask	Choose an IP-address-type mask.
Authentication	Click the authentication type for the area: • No Authentication • Password • MD5 The authentication type must be the same for all routers and access servers in an area.
Default Cost	Type a value to specify the cost of sending a packet on an interface. Valid values: 1…65535 Default: 1

Table 90 - OSPF Fields (Continued)

Field	Description
Route Summarization—Route summarization consolidates and summarizes addresses for an area and is used only with area border routers (ABRs). In OSPF, an ABR advertises networks in one area into another area. If the network numbers in an area are contiguous, you can configure the ABR to advertise a summary route that covers all individual networks within the area that are in the specified range. Routing information is condensed at area boundaries. External to the area, one route is advertised for each address range.	
OSPF ID	Choose an OSPF routing process ID.
Area ID	Type the area ID for the routes to be summarized.
IP Address	Type the IP address of the summary route.
Netmask	Choose a netmask for the summary route.
Advertise Routes	Check the checkbox to set the address range status to advertise and generate a Type 3 summary link-state advertisement (LSA).
Authentication—OSPF supports MD5 and clear text neighbor authentication. Use authentication with all routing protocols when possible because route redistribution between OSPF and other protocols (like RIP) can potentially be used by attackers to subvert routing information.	
Interface Name	Indicates the name of the OSPF interface.
Authentication	Click the authentication type for an interface: • No Authentication • Password • MD5 The authentication type must be the same for all routers and access servers in an area.
Authentication Password	Type a shared password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication. The password can be any string of keyboard-entered characters up to 8 bytes in length. All neighboring routers on the same network must have the same password to exchange OSPF information.
MD5 Key ID	Type an identifier. Valid values: 1…255.
MD5 Key	Type an alphanumeric password of up to 16 bytes.
Redistribution—Redistributing routes into OSPF from other routing protocols or from static routes causes these routes to become OSPF external routes.	
OSPF ID	Choose an OSPF routing process ID.
Protocol	Click the route type for redistribution into the OSPF routing process: • Static—-Redistributes static routes into the OSPF routing process. • Connected—Redistributes connected routes into the OSPF routing process. • OSPF—Redistributes routes from an OSPF routing process into another OSPF routing process. • RIP—Redistributes routes from an RIP routing process into the OSPF routing process. • EIGRP—Redistributes routes from an EIGRP routing process into the OSPF routing process.
Match	(Optional). Match and set properties of routes that are imported from OSPF: • Internal—Matches internal OSPF routes. • External 1—Matches Type 1 external routes. • External 2—Matches Type 2 external routes. • NSSA External 1—Matches Type 1 NSSA routes. • NSSA External 2—Matches Type 2 NSSA routes.
Metric Value	Matches routes with the specified OSPF metric cost value.
Metric Type	Matches External Type 1 or 2 routes.
Tag Value	Matches routes with the specified name.
Subnets	Check the checkbox to include subnetted routes in the redistribution.
Static Neighbor—Define static OSPF neighbors to advertise OSPF routes over a point-to-point, non-broadcast network.	
OSPF ID	Choose an OSPF routing process ID.
Neighbor	Type the IP address of the OSPF neighbor.

Table 90 - OSPF Fields (Continued)

Field	Description
Summary Address—An OSPF ASBR uses a summary address to advertise one external route as an aggregate for all redistributed routes that are covered by the address.	
OSPF ID	Choose an OSPF routing process ID.
IP Address	Type the summary address that is designated for a range of addresses.
Net Mask	Choose the IP subnet mask to use for the summary route.
Virtual Link—In OSPF, all areas must be connected to a backbone area. You can establish a virtual link if there is a backbone-continuity break by configuring two Area Border Routers as endpoints of a virtual link. Configuration information includes the identity of the other virtual endpoint (the other ABR) and the nonbackbone link that the two routers have in common (the transit area). Virtual links cannot be configured through a stub area.	
OSPF ID	Choose an OSPF routing process ID.
Area ID	Choose the area ID for the area that is assigned to the OSPF virtual link.
Peer Router ID	Type the router ID associated with the virtual link neighbor.
Authentication	Choose the authentication type for the virtual link: • No Authentication • Password • MD5 The authentication type must be the same for all routers and access servers in an area.
Authentication Password	Type a shared password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication. The password can be any string of keyboard-entered characters up to 8 bytes in length. All neighboring routers on the same network must have the same password to exchange OSPF information.
MD5 Key ID	Type an identifier. Valid values: 1c255.
MD5 Key	Type an alphanumeric password of up to 16 bytes.
Hello	Type the time (in seconds) between the hello packets that the software sends on an interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers that are attached to a common network. Valid values: 1…8192 Default: 10
Transmit Delay	Type the estimated time (in seconds) required to send a link-state update packet on the interface. The integer value that must be greater than zero. LSAs in the update packet have their age that is incremented by this amount before transmission. Valid values: 1…8192 Default: 1
Retransmit	Type the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. Valid values: 1…8192 Default: 5
Dead Interval	Type the time (in seconds) that hello packets are not seen before a neighbor declares the router down. The dead interval is an unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers that are attached to a common network.

To change the default settings after adding an EIGRP instance, on the EIGRP Instances tab, click the button in the row to customize, and then click Customize Default Settings.

IMPORTANT Setting metrics is complex and is not recommended without guidance from an experienced network designer.

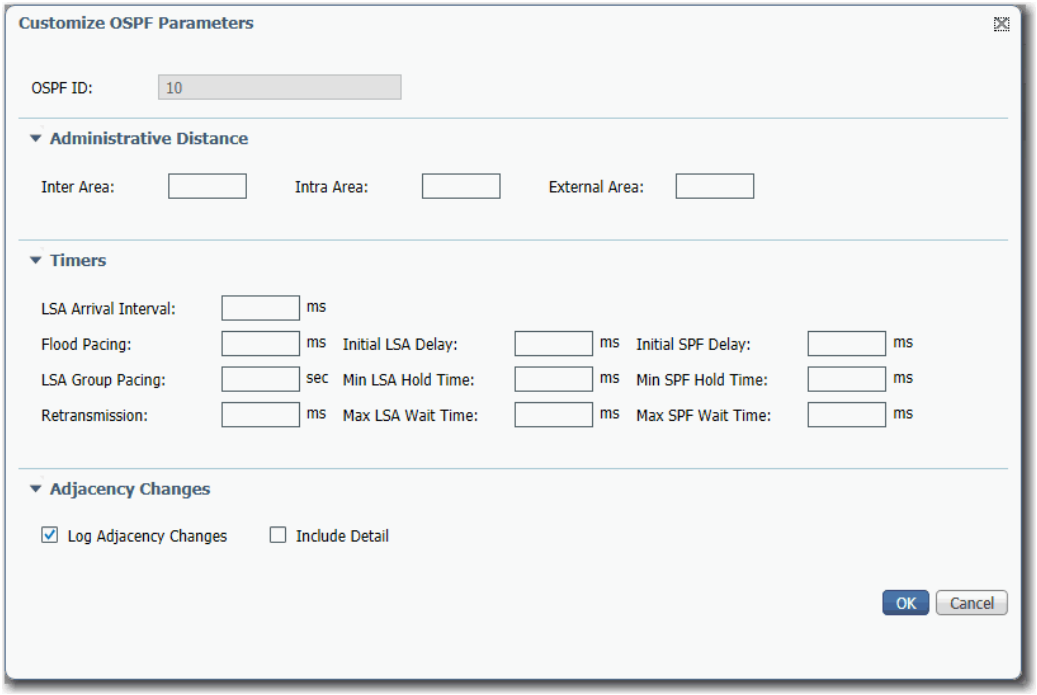


Table 91 - Customize OSPF Parameters

Field	Description
OSPF ID	(Not editable). Displays the OSPF routing process ID.
Administrative Distance	
Inter Area	Type an administrative distance for routes within an area. Valid values: 1…255 Default: 200
Intra Area	Type an administrative distance for routes to another area. Valid values: 1…255 Default: 200
External Area	Type an administrative distance for routes from another routing domain that is learned through redistribution. Valid values: 1…255 Default: 20
Timers	
LSA Arrival Interval	Type the minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped. Valid values: 0…600,000 ms Default: 1000 ms

Table 91 - Customize OSPF Parameters (Continued)

Field	Description
Flood Pacing	Type the time at which LSAs in the flooding queue are paced between updates. Valid values: 5…100 ms Default: 33 ms The default settings for OSPF packet pacing timers are suitable for most OSPF deployments. Do not change the packet pacing timers unless all other options to meet OSPF packet flooding requirements have been exhausted. Specifically, we recommend that network operators use summarization, stub area usage, queue tuning, and buffer tuning before changing the default flood timers. There are no guidelines for changing timer values; each OSPF deployment is unique and must be considered on a case-by-case basis.
LSA Group Pacing	Type the number of seconds in the interval at which LSAs are grouped and refreshed, checksummed, or aged. OSPF LSA group pacing allows the router to group OSPF LSAs and pace the refreshing, check-summing, and aging functions for more efficient router use. The optimum group pacing interval is inversely proportional to the number of LSAs the router is refreshing, check-summing, and aging. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing interval is beneficial. If you have a small database (40…100 LSAs), increasing the pacing interval to 10…20 minutes can benefit you slightly. Valid values: 10…1800 s Default: 240 s
Retransmission	Type the time in milliseconds at which LSAs in the retransmission queue are paced. Valid values: 5…200 ms Default: 66 ms.
Initial LSA Delay	Type the delay in milliseconds to generate the first occurrence of the LSA. Default: 0 ms
Min LSA Hold Time	Type the minimum delay in milliseconds to originate the same LSA. Default: 5000 ms
Max LSA Wait Time	Type the maximum delay in milliseconds to originate the same LSA. Default: 5000 ms
Initial SPF Delay	Type the time in milliseconds between when OSPF receives a topology change and when the SPF calculation starts. Valid values: 0…60,0000 ms
Min SPF Hold Time	Type the hold time in milliseconds between consecutive SPF calculations. Valid values: 0…60,0000 ms
Max SPF Wait Time	Type the maximum wait time between two consecutive SPF calculations. Valid values: 0…60,0000 ms
Adjacency Changes	
Log Neighbor Changes	Enables the logging of syslog messages when a neighbor state changes. Default: Disabled (no adjacency changes are logged)
Include Detail	Enables the logging of syslog messages whenever any state change occurs, not just when a neighbor goes up or down. Default: Disabled

Static and Connected Routing

The switch supports these forms of routing:

- Static routing—Defines explicit paths between two devices (routers and switches). You must manually define the route information, including the destination IP address, destination subnet mask, and next hop router IP address.

- Connected routing—Enables all devices on any VLAN that use the switch to communicate with each other if they use the switch as their default gateway. Connected routing is automatically enabled if you enable static routing. To disable connected routing and prevent inter-VLAN communication, you must configure access control lists (ACLs) by using the CLI.

To enable routing, follow these steps in Device Manager.

1. Reallocate switch memory for routing by changing the Switch Database Management (SDM) template from the default template to the Lanbase Routing template.

   IMPORTANT Step 1 is not required on Stratix 8300 switches.

2. Enable connected routing only.

   or

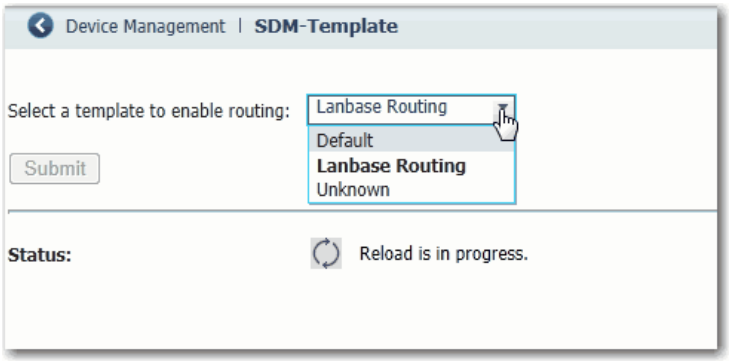
   Enable and configure static routing, which also enables connected routing by default.

Reallocate Switch Memory for Routing via Device Manager

Switch Management Database (SDM) templates optimize how switch memory is allocated for specific features, such as routing. To enable routing, you must change the default SDM template to the Lanbase Routing template.

To apply an SDM template, follow these steps.

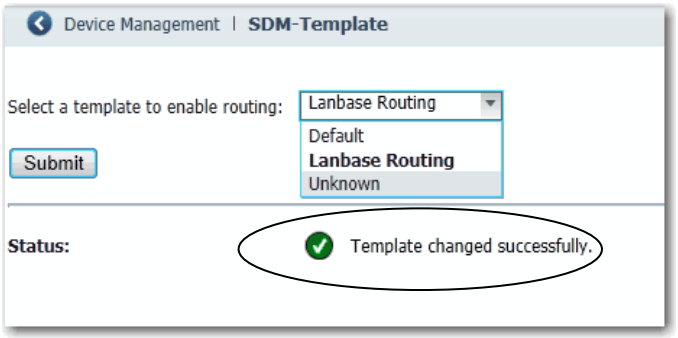
1. From the Admin menu, choose SDM-Template.
2. From the pull-down menu, choose a template:
   - Default—Gives balance to all Layer 2 functions
   - Lanbase Routing—Maximizes system resources for IPv4 unicast routing, which is required to enable routing
   - Unknown—User-configured from the CLI



3. Click Submit.
4. When a message appears prompting you to continue, click OK.

IMPORTANT The process of changing the template causes the switch to restart.

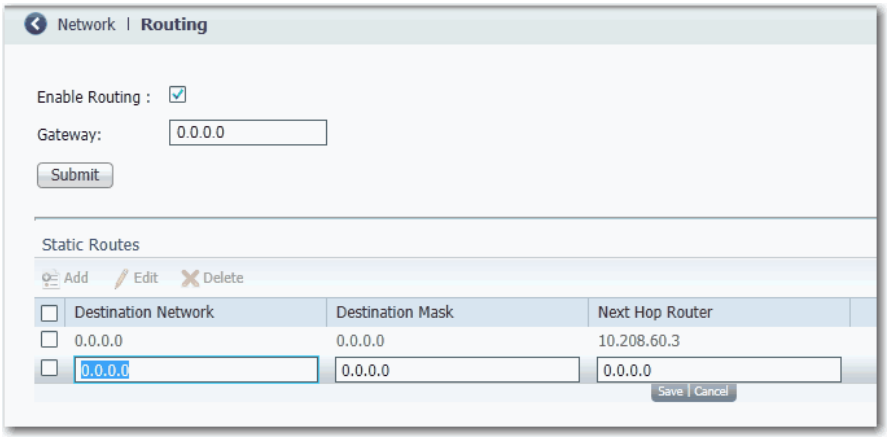
A message appears once the process is complete.



Enable and Configure Routing via Device Manager

Before you can enable routing, you must reallocate switch memory for routing, as described on page 345.

From the Configure menu, choose Routing.



From the Routing window, you can enable connected routing only or both static and connected routing. When static routing is enabled, connected routing is enabled by default. For more information about these routing types, refer to Layer 3 Routing on page 330.

Enable Connected Routing Only

To enable connected routing only, check Enable Routing and click Submit.

No further configuration is required for connected routing.

Enable Both Static and Connected Routing

To enable both static and connected routing, follow these steps.

1. Check Enable Routing and click Submit.
2. Configure static route information.

Field	Description
Destination Network	The IP address of the destination.
Destination Mask	The subnet mask of the destination.
Next Hop Router	The IP address of the router where this device sends the packets for the specified destination.

Simple Network Management Protocol (SNMP)

The switch supports SNMP versions 1, 2C, and 3. SNMP enables the switch to be remotely managed through other network management software. This feature is disabled by default.

SNMP is based on three concepts:

- SNMP managers (client software)
- SNMP agents (network devices)
- Management Information Base (MIB)

Refer to Supported MIBs on page 348 for the MIBs supported on the switch.

The SNMP manager runs SNMP management software. Network devices to be managed, such as bridges, routers, servers, and workstations, have an agent software module. The agent provides access to a local MIB of objects that reflects the resources and activity of the device. The agent also responds to manager commands to retrieve values from the MIB and to set values in the MIB. The agent and the MIB are on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

Both SNMPv1 and v2C use a community-based form of security. SNMP managers can access the agent MIB through passwords referred to as community strings. SNMPv1 and v2C are used for network monitoring without network control.

SNMPv3 provides network monitoring and control. It provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security model that is used by SNMPv3 is an authentication strategy that is set up for a user and user group. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used for an SNMP packet.

The following are guidelines for SNMPv3 objects:

IMPORTANT SNMPv.3 is available only in cryptographic switch firmware.

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy defines which SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications that its users can receive.
- A group also defines the security model and security level for its users.
- An SNMP view is a list of MIBs that a group can access.
- Data can be securely collected from SNMP devices without fear of the data being tampered with or corrupted.
- Confidential information, for example, SNMP Set command packets that change a router configuration, can be encrypted to prevent the contents from being exposed on the network.

Supported MIBs

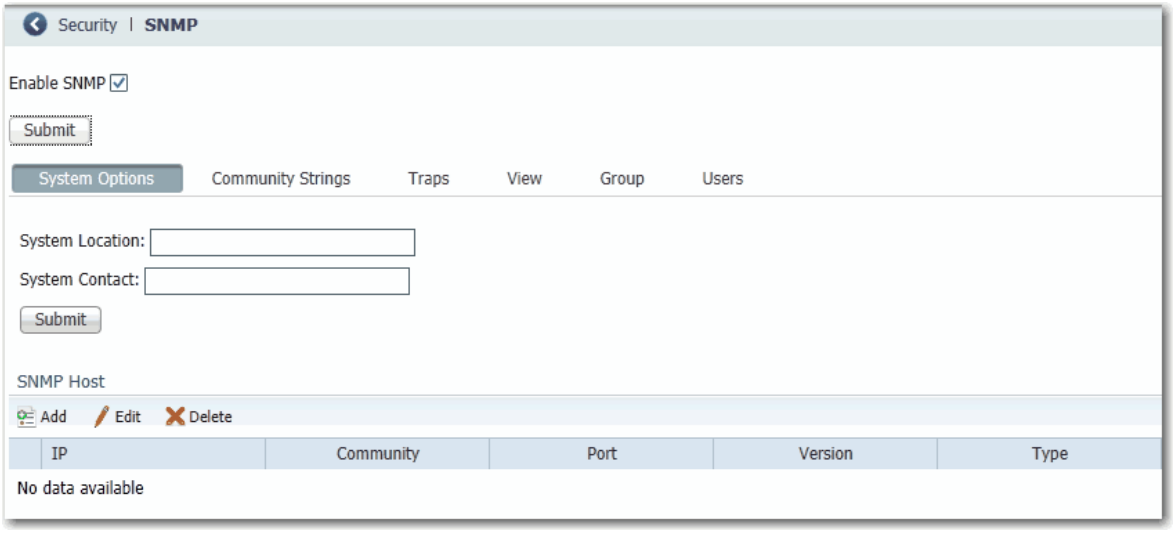
Stratix managed switches support the following MIBs.

Table 92 - Supported MIBs

MIB Name		
BRIDGE-MIB	CISCO-MEMORY-POOL-MIB	IP-MIB
CALISTA-DPA-MIB	CISCO-PAE-MIB	LLDP-EXT-MED-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-PAGP-MIB	LLDP-MIB
CISCO-ADMISSION-POLICY-MIB	CISCO-PING-MIB	NETRANGER
CISCO-AUTH-FRAMEWORK-MIB	CISCO-PORT-QOS-MIB	NOTIFICATION-LOG-MIB
CISCO-BRIDGE-EXT-MIB	CISCO-PORT-SECURITY-MIB	OLD-CISCO-CHASSIS-MIB
CISCO-BULK-FILE-MIB	CISCO-PORT-STORM-CONTROL-MIB	OLD-CISCO-CPU-MIB
CISCO-CABLE-DIAG-MIB	CISCO-PRIVATE-VLAN-MIB	OLD-CISCO-FLASH-MIB
CISCO-CALLHOME-MIB	CISCO-PROCESS-MIB	OLD-CISCO-INTERFACES-MIB
CISCO-CAR-MIB	CISCO-PRODUCTS-MIB	OLD-CISCO-IP-MIB
CISCO-CDP-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	OLD-CISCO-MEMORY-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-RTTMON-ICMP-MIB	OLD-CISCO-SYS-MIB
CISCO-CLUSTER-MIB	CISCO-RTTMON-IP-EXT-MIB	OLD-CISCO-SYSTEM-MIB
CISCO-CONFIG-COPY-MIB	CISCO-RTTMON-MIB	OLD-CISCO-TCP-MIB
CISCO-CONFIG-MAN-MIB	CISCO-RTTMON-RTP-MIB	OLD-CISCO-TS-MIB
CISCO-DATA-COLLECTION-MIB	CISCO-SNMP-TARGET-EXT-MIB	RMON-MIB
CISCO-DHCP-SNOOPING-MIB	CISCO-STACK-MIB	RMON2-MIB
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-STACKMAKER-MIB	SMON-MIB
CISCO-ENTITY-ALARM-MIB	CISCO-STP-EXTENSIONS-MIB	SNMP-COMMUNITY-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-SYSLOG-MIB	SNMP-FRAMEWORK-MIB
CISCO-ENVMON-MIB	CISCO-TCP-MIB	SNMP-MPD-MIB
CISCO-ERR-DISABLE-MIB	CISCO-UDLDP-MIB	SNMP-NOTIFICATION-MIB
CISCO-FLASH-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	SNMP-PROXY-MIB
CISCO-FTP-CLIENT-MIB	CISCO-VLAN-MEMBERSHIP-MIB	SNMP-TARGET-MIB
CISCO-IF-EXTENSION-MIB	CISCO-VTP-MIB	SNMP-USM-MIB
CISCO-IGMP-FILTER-MIB	ENTITY-MIB	SNMP-VIEW-BASED-ACM-MIB
CISCO-IMAGE-MIB	ETHERLIKE-MIB	SNMPv2-MIB
CISCO-IP-STAT-MIB	HC-RMON-MIB	TCP-MIB
CISCO-LAG-MIB	IEEE8021-PAE-MIB	UDP-MIB
CISCO-LICENSE-MGMT-MIB	IEEE8023-LAG-MIB	
CISCO-MAC-AUTH-BYPASS-MIB	IF-MIB	
CISCO-MAC-NOTIFICATION-MIB	IP-FORWARD-MIB	

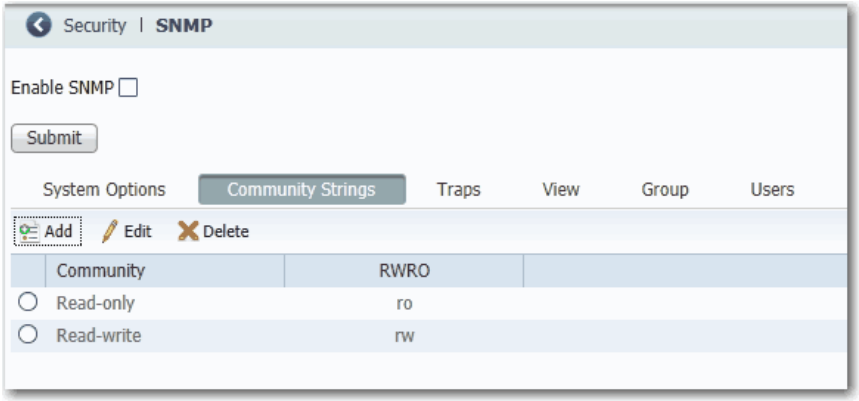
Configure SNMP via Device Manager

From the Configure menu, choose SNMP.



Community strings are passwords to the switch Management Information Base (MIB). You can create community strings that provide a remote manager read-only or read-write access to the switch.

To create, modify, and delete, click the Community Strings tab.



A read-only community string enables the switch to validate Get (read-only) requests from a network management station. If you set the SNMP read community, users can access MIB objects, but cannot change them.

A read-write community string enables the switch to validate Set (read-write) requests from a network management station.

Use SNMP Management Applications

You can use SNMP management applications such as IntraVue or HP OpenView to configure and manage the switch. Refer to Simple Network Management Protocol (SNMP) on page 347 for more information.

Smartports

Smartports are recommended configurations for the switch ports. These configurations, referred to as port roles, optimize the switch connections and provide security, transmission quality, and reliability for traffic from the switch ports. The port roles also help prevent port misconfigurations.

TIP Use Smartport roles immediately after the initial setup of the switch to configure the switch ports before they connect to devices.

The port roles that are described in Table 93 are based on the type of devices to be connected to the switch ports. For example, the Desktop for Automation port role is specifically for switch ports to be connected to desktop and laptop computers.

Table 93 - Smartport Roles

Port Role	Description
Automation Device	Apply this role to ports to be connected to EtherNet/IP (Ethernet Industrial Protocol) devices. It can be used for industrial automation devices, such as logic controllers and I/O: • Port is set to Access mode. • Port security supports only one MAC ID. • Optimize queue management for CIP traffic.
Multiport Automation Device	Apply this role to DLR-enabled ports and ports connected to multiport EtherNet/IP devices. Devices include multiport EtherNet/IP devices arranged in a linear or daisy chain topology, the 1783-ETAP module (for connection to only the device port), unmanaged switches, such as the Stratix 2000, and managed switches with Remote Spanning Tree Protocol (RSTP) disabled: • Port is set to Access mode. • No port security. • Optimized queue management for CIP traffic.
Desktop for Automation	Apply this role to ports to be connected to desktop devices, such as desktop computers, workstations, notebook computers, and other client-based hosts: • Port is set to Access mode. • Portfast enabled. • Port security supports only one MAC ID. Do not apply to ports to be connected to switches, routers, or access points.
Virtual Desktop for Automation	Apply this role to ports connected to computer running virtualization software. This can be used with devices running up to two MAC addresses: • Port is set to Access mode. • Portfast is enabled. • Port security supports two MAC IDs. **IMPORTANT:** Do not apply the Virtual Desktop for Automation role to ports that are connected to switches, routers, or access points.
Switch for Automation	Apply this role to ports to be connected to other switches with Spanning Tree enabled. Port is set to Trunk mode.
Router for Automation	Apply this role to ports to be connected to routers or Layer 3 switches with routing services enabled.
Phone for Automation	Apply this role to ports to be connected to IP phones. A desktop device, such as a computer, can be connected to the IP phone. Both the IP phone and the connected computer have network access through the port: • Port is set to Trunk mode. • Port security supports three MAC IDs to this port. This role prioritizes voice traffic over general data traffic to provide clear voice reception on the IP phones.
Wireless for Automation	Apply this role to ports to be connected to wireless access points. The access point can provide network access to as many as 30 wireless users.

Table 93 - Smartport Roles (Continued)

Port Role	Description
Port Mirroring	Apply this role to ports monitored by a network analyzer. For more information about port mirroring, see page 301.
None	Apply this role to ports if you do not want a specialized Smartport role on the port. This role can be used on connections to any device, including devices with other Smartport roles.
CS1…CS10	Custom Smartport roles. You can create a customized port role with a user-defined name. See page 351.

Custom Smartport Roles

You can create and modify as many as 10 custom Smartport roles for a variety of custom applications. By default, the switch ports are set to the None port role. This feature is not available on Stratix 8000/8300 switches.

Avoid Smartport Mismatches

A Smartport mismatch occurs when an attached device does not match the Smartport role that is applied to the switch port. Mismatches can have adverse effects on devices and your network.

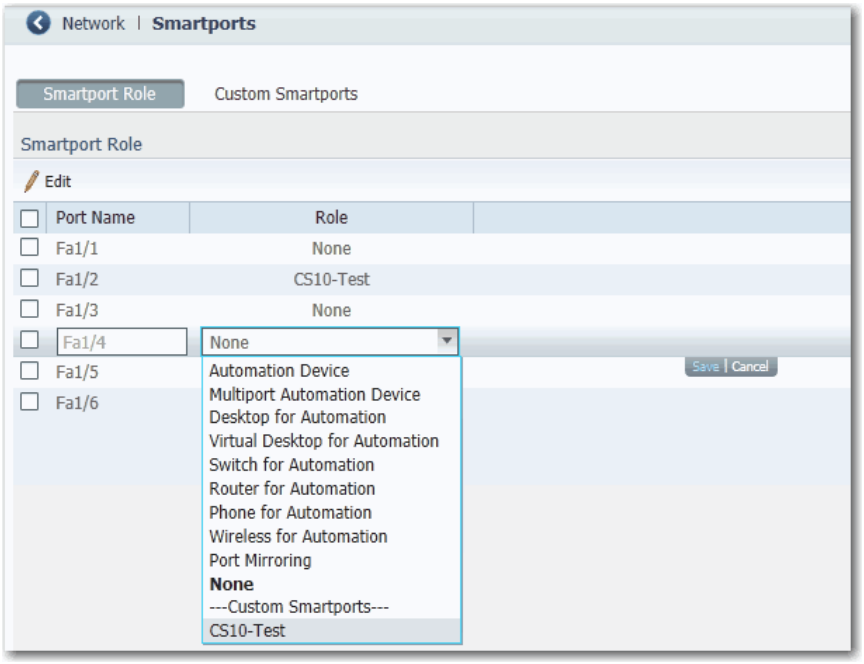
Mismatches can result in the following conditions:

- Affect the behavior of the attached device
- Lower network performance (reduce the level of quality of service [QoS]) on CIP, voice, wireless, switch, and router traffic
- Reduce restrictions on guest access to the network
- Reduce protection from denial of service (DoS) attacks on the network
- Disable or shut down the port

We recommend that you always verify which Smartport role is applied to a port before attaching a device to the port or reconnecting devices.

Configure Smartports via Device Manager

From the Configure menu, choose Smartports.



Follow these guidelines when using Smartport roles:

- Before using Smartport roles, decide which switch port is connected to which device type.
- Before attaching a device to the port or reconnecting devices that have been moved, verify which Smartport role is applied to a port.

  IMPORTANT We recommend that you do not change port settings after enabling a Smartport role on a port. Any port setting changes can alter the effectiveness of the Smartport role.

- If you attempt to apply a port role to a routed port in the Smartports window, this error message appears:

  A port role cannot be configured on a routed port.

To apply a Smartport role, follow this procedure.

1. From the Configure menu, choose Smartports.
2. Select a port.
3. From the pull-down menu in the Role column, choose a Smartport role.
4. Click Save.

Customize Port Role Attributes

Each switch port is a member of a VLAN. Devices that are attached to switch ports that belong to the same VLAN share data broadcasts and system resources.

Depending on your network requirements, it can be sufficient to assign all ports to the default VLAN, which is named default. One VLAN can be sufficient for a small network.

Before changing virtual local-area network (VLAN) memberships, understand what a VLAN is, its purpose, and how to create a VLAN. See page 365 for more information about VLANs.

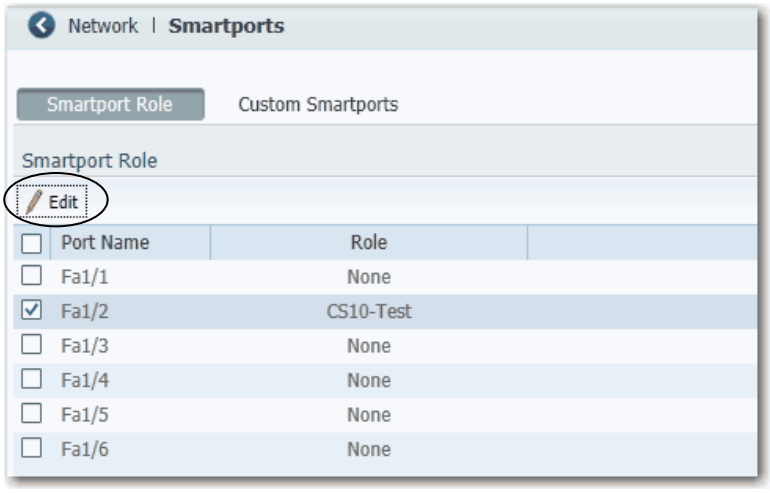
Assign a Port to a VLAN

Each switch port is a member of a VLAN. Devices that are attached to switch ports that belong to the same VLAN share data broadcasts and system resources. Communication between VLANs requires a Layer 3 device, such as a router or a Layer 3 switch.

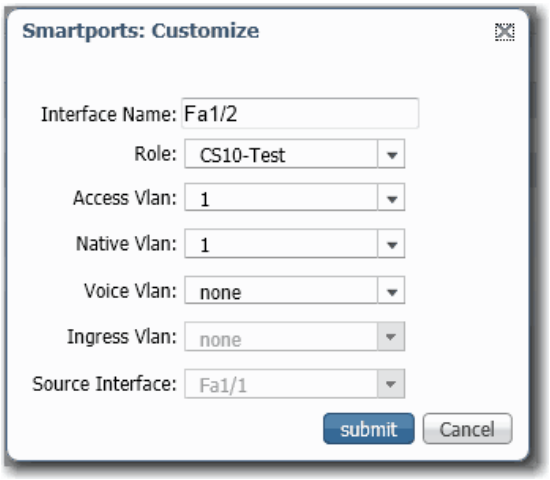
Depending on your network requirements, it can be sufficient to assign all ports to the default VLAN, which is named default. If additional VLANs have been created, you must decide which ports are best suited to which VLANs.

To change a VLAN assignment, follow these steps.

1. From the Configure menu, choose Smartports.
2. Check the checkbox next to the port for which to change the VLAN.
3. Click Edit.



4. Modify the VLAN assignments as needed:
   - For ports applied with the Automation Device with QoS, Switch For Automation, Router For Automation, or Wireless For Automation port role, choose a VLAN from the Native VLAN list.
   - For ports applied with the Automation Device, Desktop For Automation, Phone For Automation, or None port role, choose a VLAN from the Access VLAN list.
   - For ports applied with the Phone For Automation port role, choose a VLAN from the Voice VLAN list.
   - For ports applied with the Port Mirroring port role, choose a VLAN from the Ingress VLAN list and choose the port to be monitored from the Source Interface list.



5. Click Submit.

Manage Custom Smartport Macros

To create a custom Smartports macro follow these steps. This feature is not available on Stratix 8000/8300 switches.

1. Click the Custom Smartports tab.
2. Click Add.
3. Enter the name for the macro.

   Macro names are case-sensitive. The string can be up to 31 alphanumeric characters. The string cannot contain a ?, a space, or a tab.
4. Choose a macro icon (CS1 to CS10).

5. Enter a macro definition.

   The definition can contain up to 3000 characters. Enter the macro commands with one command per line. Use the # character at the beginning of a line to enter comment text within the macro.

   Available parameters for the macro are $native_vlan, $access_vlan, and $voice_vlan.

6. Enter an antimacro definition.

   The antimacro definition is the portion of the applied macro that removes the macro when you do the following:

   - Change it to another macro.
   - Remove it with the None Smartport role.

   Before the macro definition can be applied to the port, the antimacro must first be defined with the proper commands to set the port back to its original state.

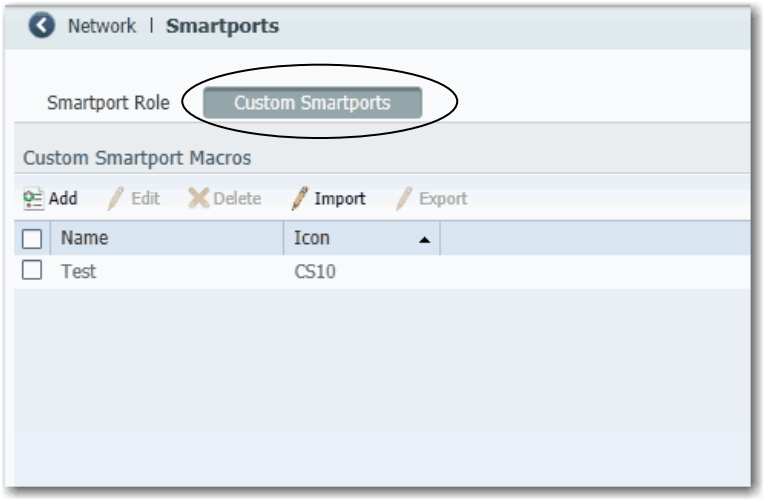
   The definition can contain up to 3000 characters. Enter the antimacro commands with one command per line. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro.

7. Click Submit.
8. To discard any unsaved changes, click Cancel.

Modify the Definition of a Custom Smartports Macro

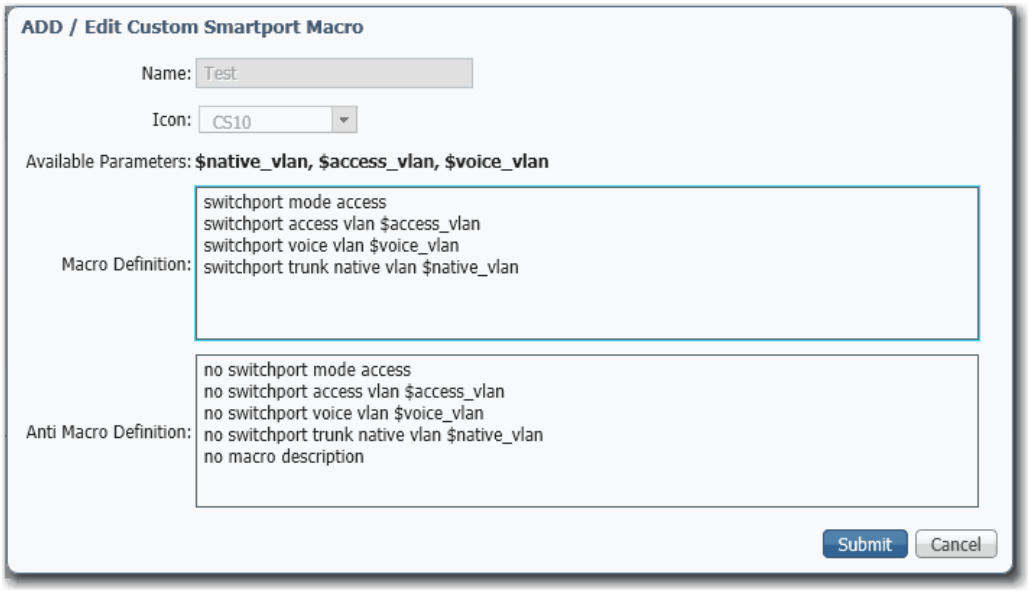
You cannot modify a custom Smartports macro that is currently in use.

1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.



3. Check the checkbox next to the macro to modify.

4. Click Edit.

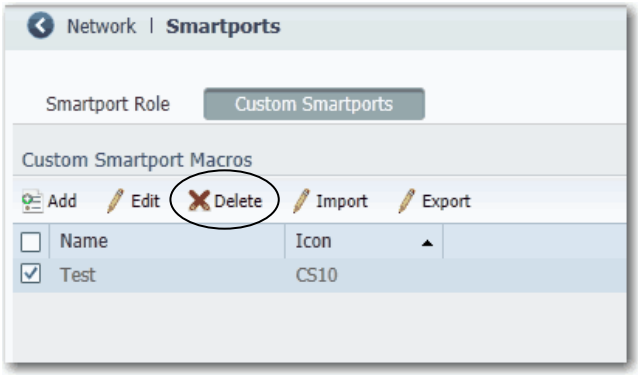


5. Change the definitions as needed.
6. Click Submit.

Delete a Custom Smartports Macro

You cannot delete a custom Smartports macro that is currently in use.

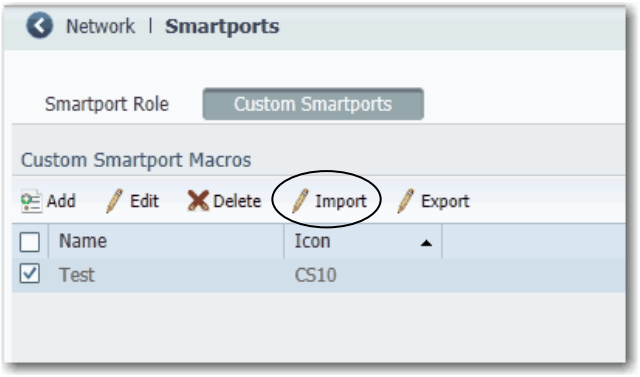
1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.
3. Check the checkbox next to the macro to delete.



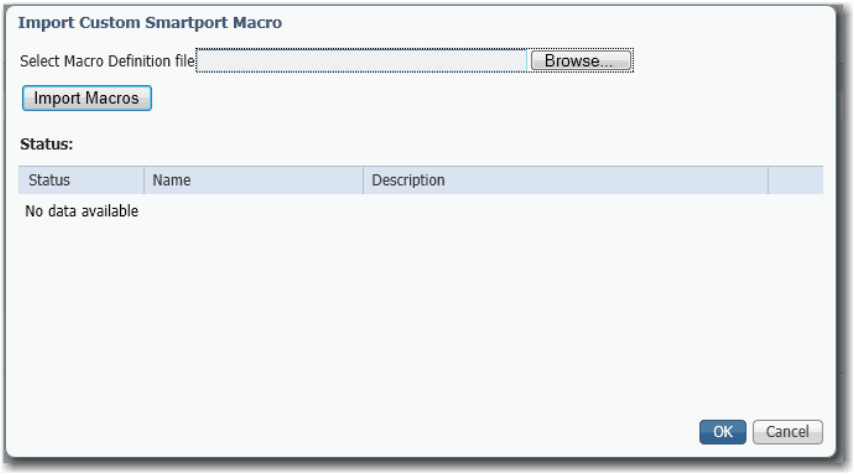
4. Click Delete.

Import a Custom Smartports Macro

1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.
3. Click Import.



4. Click Browse.

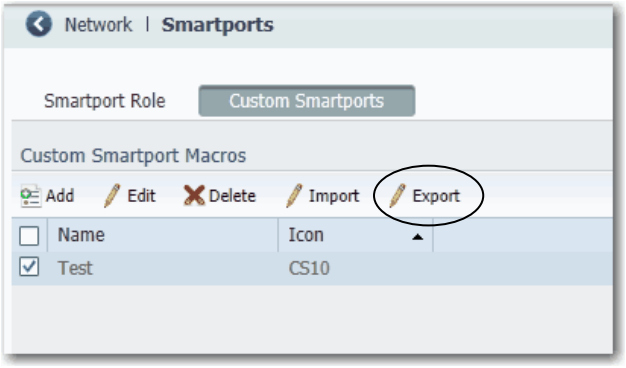


5. Select the macro file on your computer or network drive.

   The file must be an appropriately formatted .xml file.
6. Click Import Macros.
7. Click OK.

Export a Custom Smartports Macro

1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.
3. Check the checkbox next to the macro to export.
4. Click Export.



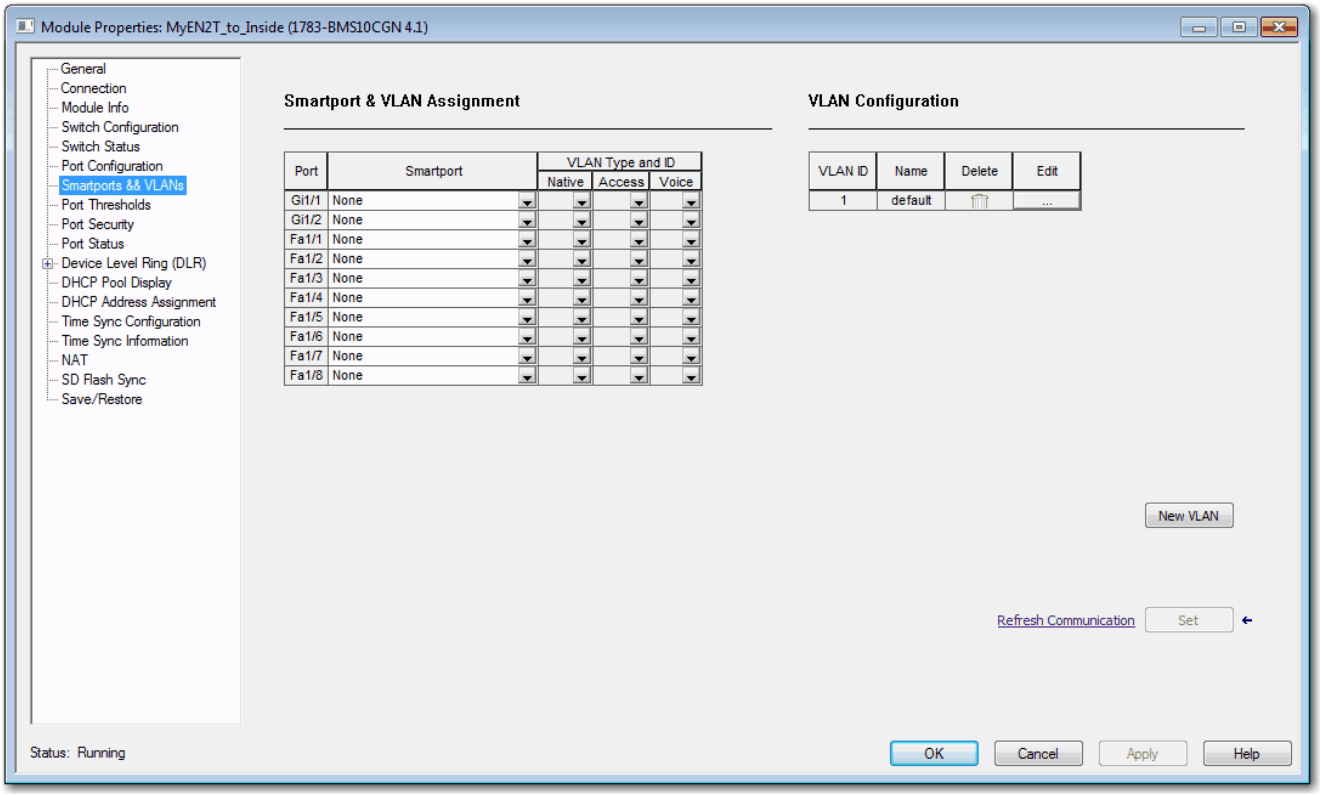
5. Save the resulting file.

Assign Smartports and VLANs via the Logix Designer Application

In the navigation pane, click Smartports & VLANs.

For Stratix 8000/8300 switches, use Advanced Port Configuration, as described on page 360.

Figure 47 - Smartport & VLAN Assignment



For Stratix 8000/8300 switches, in the navigation pane, click Advanced Port Configuration.

Figure 48 - Advanced Port Configuration for Stratix 8000/8300 Switches

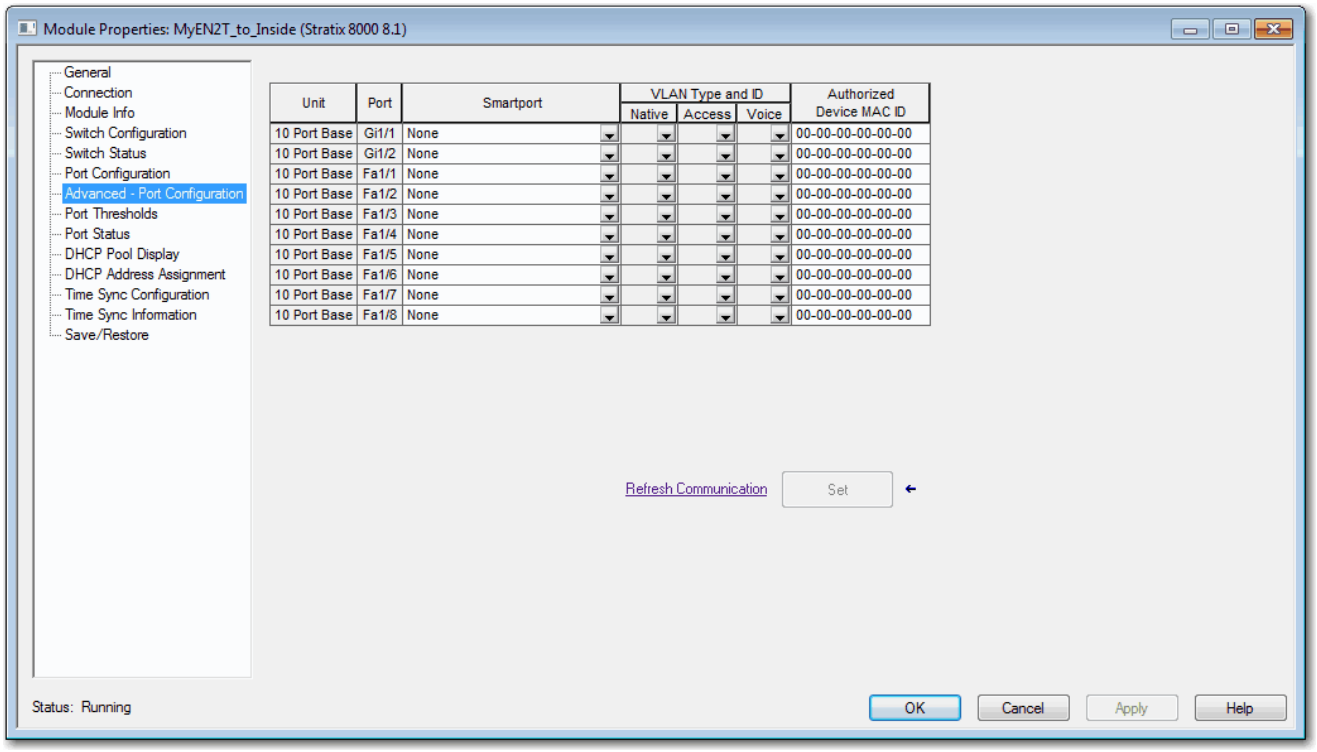


Table 94 - Smartport and VLAN Assignment Fields

Field	Description
Unit (Stratix 8000/8300 switches)	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	Indicates the port that is selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number, such as in the following examples: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Smartport	Choose the Smartport role to apply to the connected port. For descriptions of each role, see Table 93 on page 350. The Smartport roles are recommended configurations for the ports. These configurations are referred to as port roles. They optimize the switch connections and help ensure security, transmission quality, and reliability to traffic from the switch ports. These configurations also prevent problems that are caused by port misconfigurations. The port roles are based on the type of device that is connected to the switch port. Make sure that you decide which port to connect to which type of device before you choose a Smartport role.
VLAN Type and ID	Choose a VLAN to assign to the port. Only the first 128 VLANs are listed: • Native—Represents the valid Native VLAN ID for ports set to the Router for Automation and Switch for Automation role. A native VLAN is for ports that can belong to a VLAN trunk (a port belonging to more than one VLAN). The Native VLAN feature is blank when the Smartport role is set to any value other than Switch for Automation and Router for Automation. • Access—Represents the valid Access VLAN ID for ports set to Automation Device, Desktop for Automation, Phone for Automation, Wireless, and Automation Device with QoS role. An access VLAN is for ports that can belong to only one VLAN. The Access VLAN feature is blank when the Smartport role is set to Switch for Automation and Router for Automation. • Voice—Represents the valid Voice VLAN ID for ports set to the Phone for Automation role. The voice VLAN helps ensure that all voice traffic has better quality of service and is not mixed with data traffic. The Voice VLAN feature is blank when the Smartport role is set to any value other than Phone for Automation.
Authorized Device MAC ID	See Configure Port Security via the Logix Designer Application on page 307.

Spanning Tree Protocol (STP)

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations can receive duplicate messages. Switches can also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port that is elected for the spanning-tree topology.
- Designated—A forwarding port that is elected for every switched LAN segment.
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree.
- Backup—A blocked port in a loopback configuration.

The switch that has all of its ports assigned to the Designated role or the Backup role is the root switch. The switch that has at least one of its ports assigned to the Designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

Spanning Tree Protocol (STP) modes include the following:

- Multiple Spanning Tree (MST) prevents network loops by enabling only one active path for traffic. MST also provides a redundant path if the active path becomes unavailable. This is the default STP mode. If you connect the switch to a Cisco network switch, the typical default is PVST+, not MST. To provide compatibility, one or the other switch must be modified.
- Per VLAN Spanning Tree Plus (PVST+) runs on each VLAN on the switch up to the maximum supported to prevent network loops.
- Rapid Per VLAN Spanning Tree Plus (RPVST+) immediately deletes dynamically learned MAC address entries upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC addresses.

We recommend that you leave STP enabled to prevent network loops and provide a redundant path if the active path becomes unavailable.

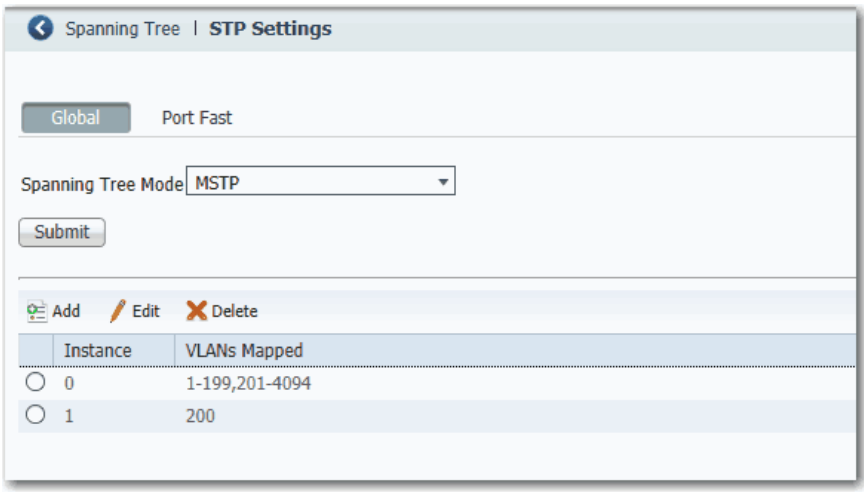
IMPORTANT Disabling STP can affect connectivity to the network.

Configure STP via Device Manager

From the Configure menu, choose STP Settings.

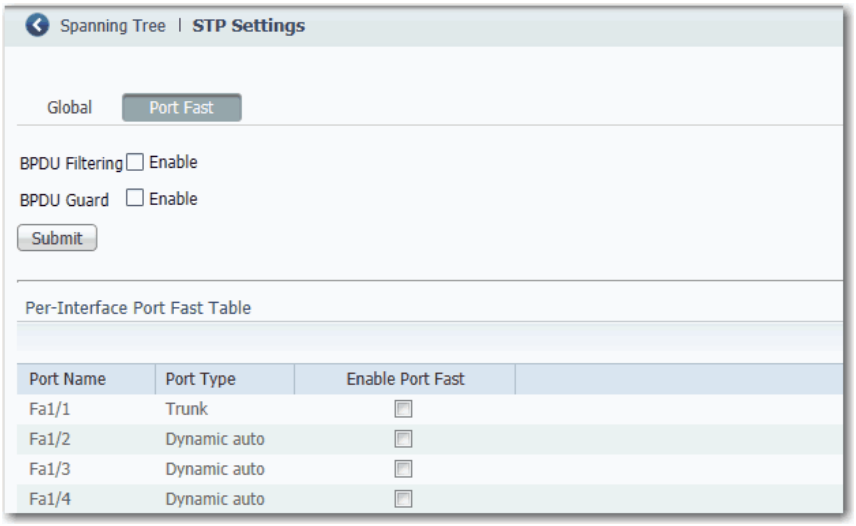
Global Settings

To choose the STP mode for the switch or to configure STP on individual VLANs, click the Global tab. On the Global tab, you can add, edit, or delete instances. If you choose PVST+ or Rapid PVST+ mode, you can enable or disable STP on each instance.



PortFast Settings

To enable PortFast and related features, click the PortFast tab. On the PortFast tab, you can change the way that STP is implemented on individual ports.



PortFast features are typically enabled only on access ports. Access ports connect to devices such as personal computers, access points, and servers that are not expected to send bridge protocol data units (BPDUs). These features are typically not enabled on ports that connect to switches because spanning tree loops can occur.

BPDU Features

Switches exchange special frames that are called BPDUs to communicate network information, to track changes, and to create the STP topology. Because transmitted BPDUs reveal network information and received BPDUs can influence your STP topology, consider enabling BPDU Filtering and BPDU Guard on your access ports. These features prevent a rogue device from interfering with your STP topology. However, we recommend you use these features with caution:

- BPDU Filtering—This PortFast feature blocks all sending and receiving of BPDUs through all PortFast-enabled ports. This feature effectively disables STP on these ports and loops can result. If a BPDU is received, PortFast is disabled on the port and the global STP settings apply. To enable BPDU Filtering on all PortFast-enabled ports, check Enable.

- BPDU Guard—This PortFast feature shuts down a port if it receives a BPDU. To enable BPDU Guard on all Port Fast-enabled ports, check Enable.

If you enable both of these features, BPDU Guard has no effect because BPDU Filtering prevents the port from receiving any BPDUs.

Per Interface PortFast Table

Spanning tree requires an interface to progress through the listening and learning states, to exchange information and establish a loop-free path before it can forward frames. On ports that connect to devices such as workstations and servers, you can allow an immediate connection. PortFast immediately transitions the port into STP forwarding mode upon linkup.

To enable PortFast on an interface and apply the selected BPDU features to the interface, select the interface, and then check Enable Port Fast.

Configure STP via the Logix Designer Application

STP configuration via the Logix Designer application is available for only Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 switches.

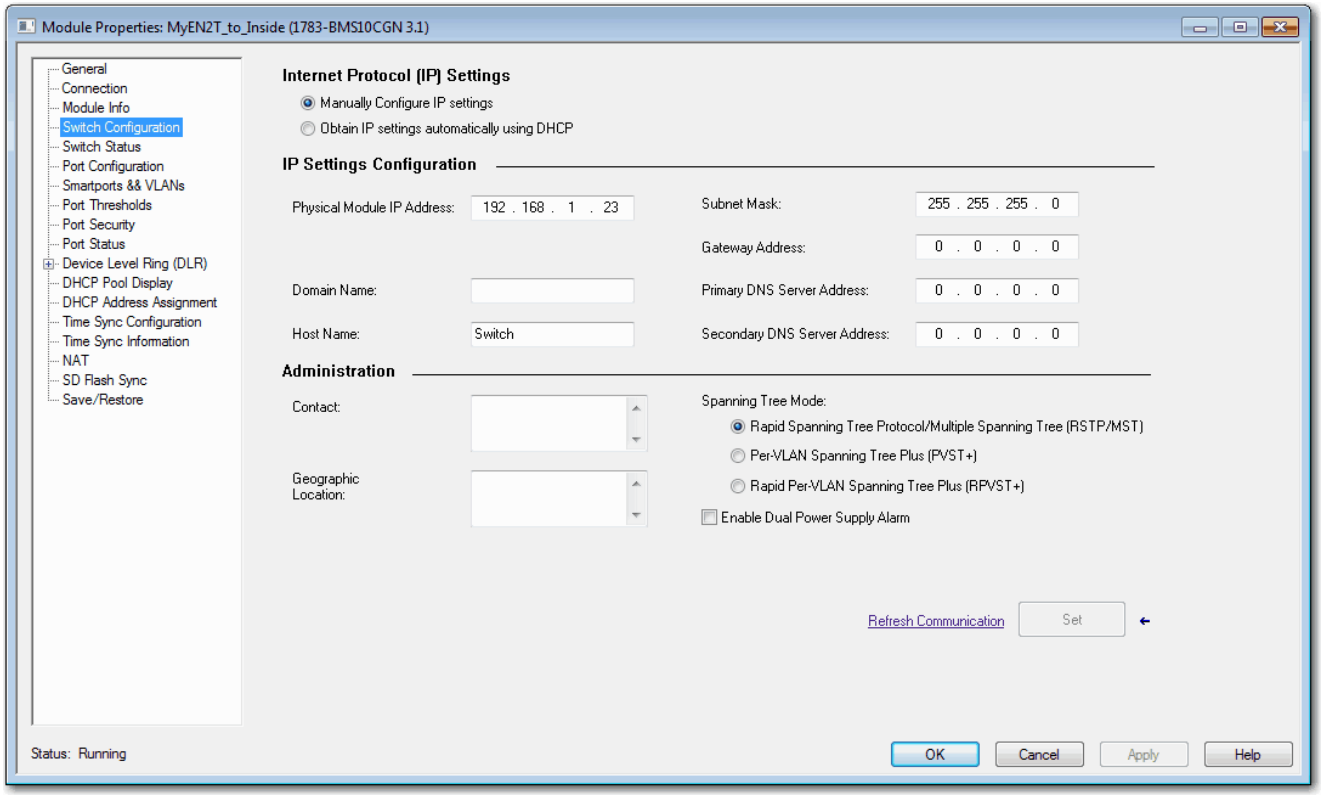
In the navigation pane, click Switch Configuration.

In the Administration area, you can assign a Spanning Tree mode:

- Rapid Spanning Tree Protocol/Multiple Spanning Tree (RSTP/MST)
- Per VLAN Spanning Tree Plus (PVST+)
- Rapid Per-VLAN Spanning Tree (RPVST+)

MST/RSTP is the default.

Figure 49 - Switch Configuration for Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 Switches



Virtual Local Area Networks (VLANs)

A VLAN is a logical segment of network users and resources grouped by function, team, or application. This segmentation is without regard to the physical location of the users and resources. For example, VLANs can be based on the departments in your company or by sets of users who communicate mostly with each other.

The switch ships with a default VLAN to which each switch port initially belongs. The switch supports a maximum of 255 VLANs, including the default VLAN.

Every VLAN has a name and ID number. The default VLAN is named default. The ID can be from 1...1001 and 1005...4094, where 1 is the default ID. To create a VLAN, you must give the VLAN a name and a unique ID number. You can modify the name of a VLAN but not its number. You cannot rename or delete the default VLAN.

You can assign switch ports to either the default VLAN or to VLANs that you have created.

IMPORTANT Changes to VLAN assignments on a port with Network Address Translation (NAT) can break existing NAT configurations. Review your NAT configurations to make sure VLAN assignments are correct.

The default VLAN alone can be sufficient based on the size and requirements of your network. We recommend that you first determine your VLAN needs before creating VLANs.

With custom Smartports, you can specify the type of VLAN you want to implement on that port. The custom Smartports feature is not available on Stratix 8000/8300 switches.

The default VLAN is also the management VLAN. After the initial setup, you can create VLANs and designate any VLAN on the switch as the management VLAN. The management VLAN provides administrative access to the switch. You must assign one of the switch ports to the management VLAN. Otherwise, you do not have administrative access to the switch. Initially, all ports are assigned to the management VLAN.

You can assign all ports, regardless of their Smartport role, to the default VLAN (default).

Isolate Traffic and Users

By using VLANs, you can isolate different types of traffic, such as voice and data. Isolating different types of traffic helps to preserve the quality of the transmission and to minimize excess traffic among the logical segments. You can also use VLANs to isolate different types of users. For example, you can restrict specific data broadcasts to specific logical workgroups for security purposes. For example, you can keep information about employee salaries only on devices in a VLAN created for payroll-related communication.

VLANs can also reduce the amount of administrative effort that is required to examine requests to network resources.

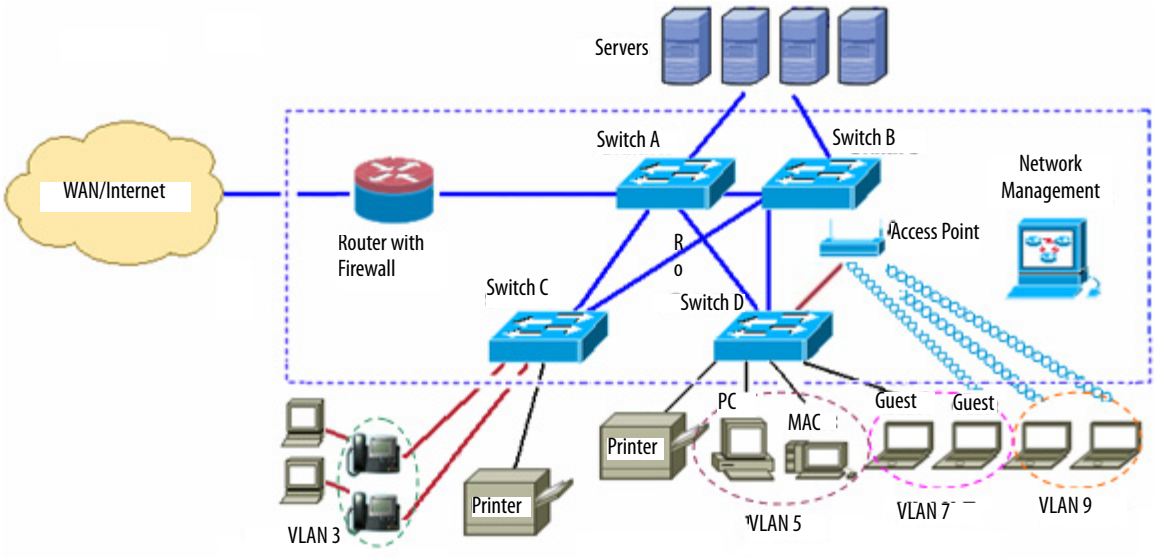
VLANs isolate parts of your network. Therefore, devices that are attached to the switch ports in the same VLAN can communicate only with each other and can share data.

Devices that are attached to switch ports in different VLANs cannot communicate with each other through the switch, unless the switch is configured for routing. A Stratix 5700 switch, a router, or a Layer 3 switch must be configured to enable routing across VLANs (inter-VLAN routing), and additional security policies must be set.

If your network is also using a DHCP server, make sure that the server is accessible to the devices in all the VLANs.

The following figure is an example network that uses VLANs based on different network traffic and network users. Organizing a network around these factors helps to define the size and membership of the VLANs in the network.

Figure 50 - VLAN Example



Isolate Different Traffic Types

Isolating data traffic from delay-sensitive traffic, such as voice traffic, increases the quality of the voice transmission. In Figure 50, switch ports that are connected to the IP phones belong to VLAN 3, a VLAN that is configured to provide Voice over IP (VoIP) services on these connections, meaning priority is given to voice traffic over regular IP data traffic. Voice traffic from the phone and IP-phone service requests to an IP PBX server have priority over traffic from the desktop devices that are attached to the IP phones.

To isolate data traffic further from voice traffic, the data traffic from the attached desktop devices can be assigned to a separate VLAN.

Group Users

The network that is shown in Figure 50 provides access to three types of network users:

- Wired employees
- Wireless employees
- Wired or wireless company visitors

Each user type requires different access levels to the company network. VLANs and security policies on a router or Layer 3 switch can enforce privileges and restrictions to different user types.

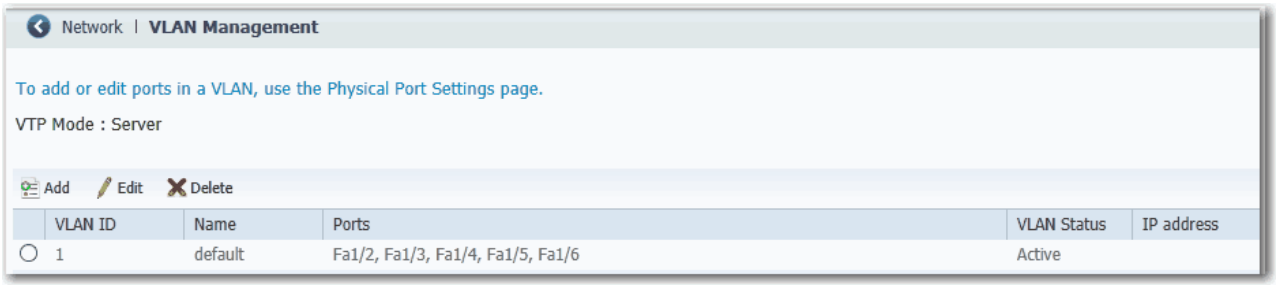
Refer to Figure 50 on page 366:

- VLAN 5 offers employee-level access to the company resources. This network access requires a direct connection to the specific switch ports.
- VLAN 7 offers Internet-only access to company visitors. Visitors with wired or wireless connections to switch ports are assigned to this VLAN, which automatically restricts guest access to only the Internet.
- VLAN 9, which has one or more switch ports that are connected to the wireless access point, enforces security policies:
  - Identifies the wireless user as an employee or a guest, for example.
  - Determines what the user can do on the network, such as access only the Internet or access other network resources.

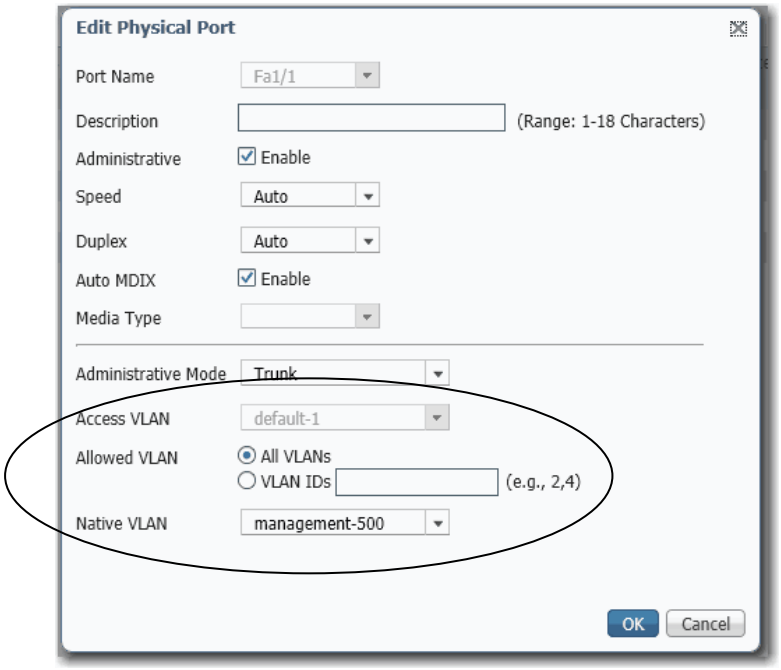
Configure VLANs via Device Manager

From the Configure menu, choose VLAN Management.

You can add, edit, and delete VLANs.



To assign ports to VLANs, use the Edit Physical Ports window, as described on page 51. Before you assign ports to VLANs, make sure that each port has the appropriate port role.



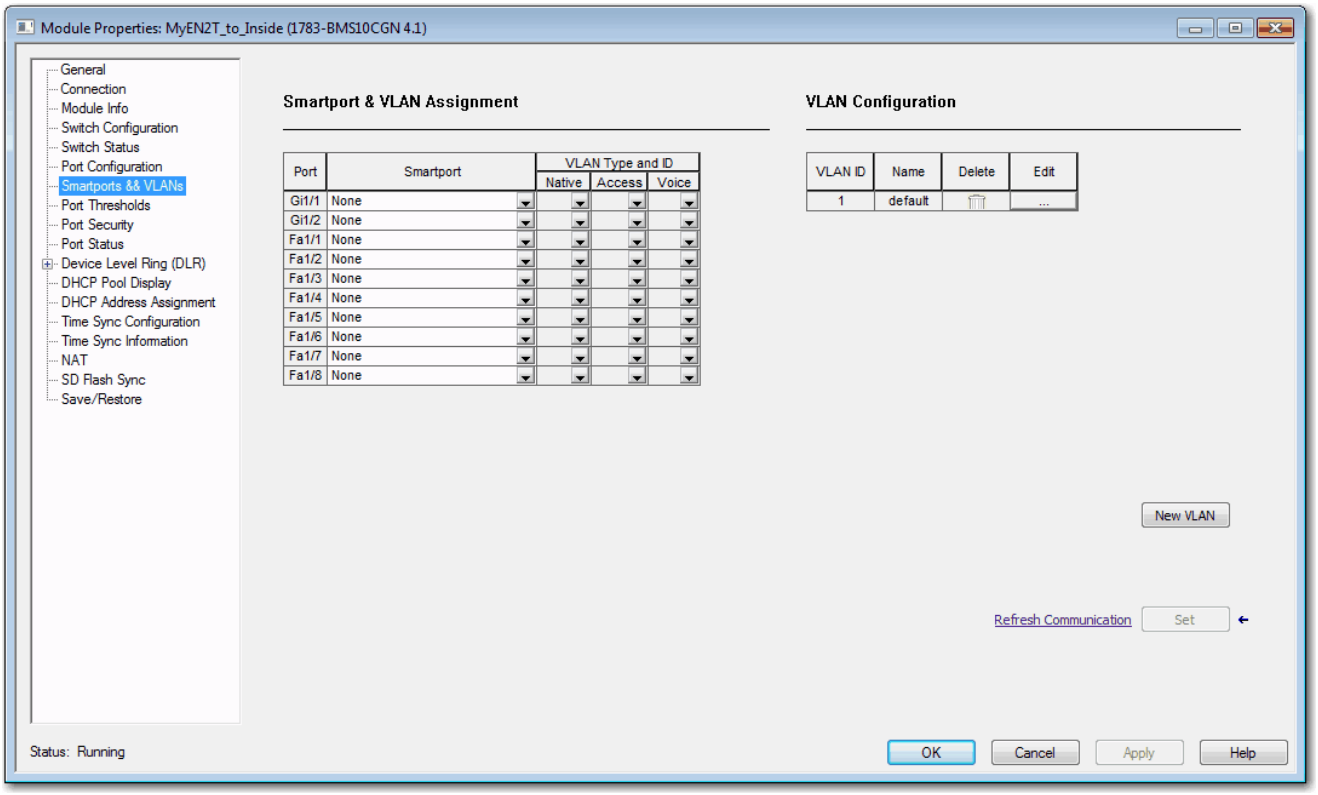
Configure VLANs via the Logix Designer Application

VLAN configuration via the Logix Designer application is available for only Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 switches.

In the navigation pane, click Smarports & VLANs.

In the VLAN Configuration area, you can add, edit, and delete VLANs.

Figure 51 - VLAN Configuration for Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 Switches



To assign ports to VLANs, see Assign Smartports and VLANs via the Logix Designer Application on page 358.

Monitor the Switch

Topic	Page
Switch Status via Device Manager	372
Switch Status via the Logix Designer Application	388
System Log Messages	392
Trends	394
Port Statistics	395
NAT Statistics	396
REP Status	403
CIP Status	403
DHCP Clients	405
DLR Status	406
PRP Status	410
Port Diagnostics	412
Cable Diagnostics	414
DHCP Pool Display	416

Switch Status via Device Manager

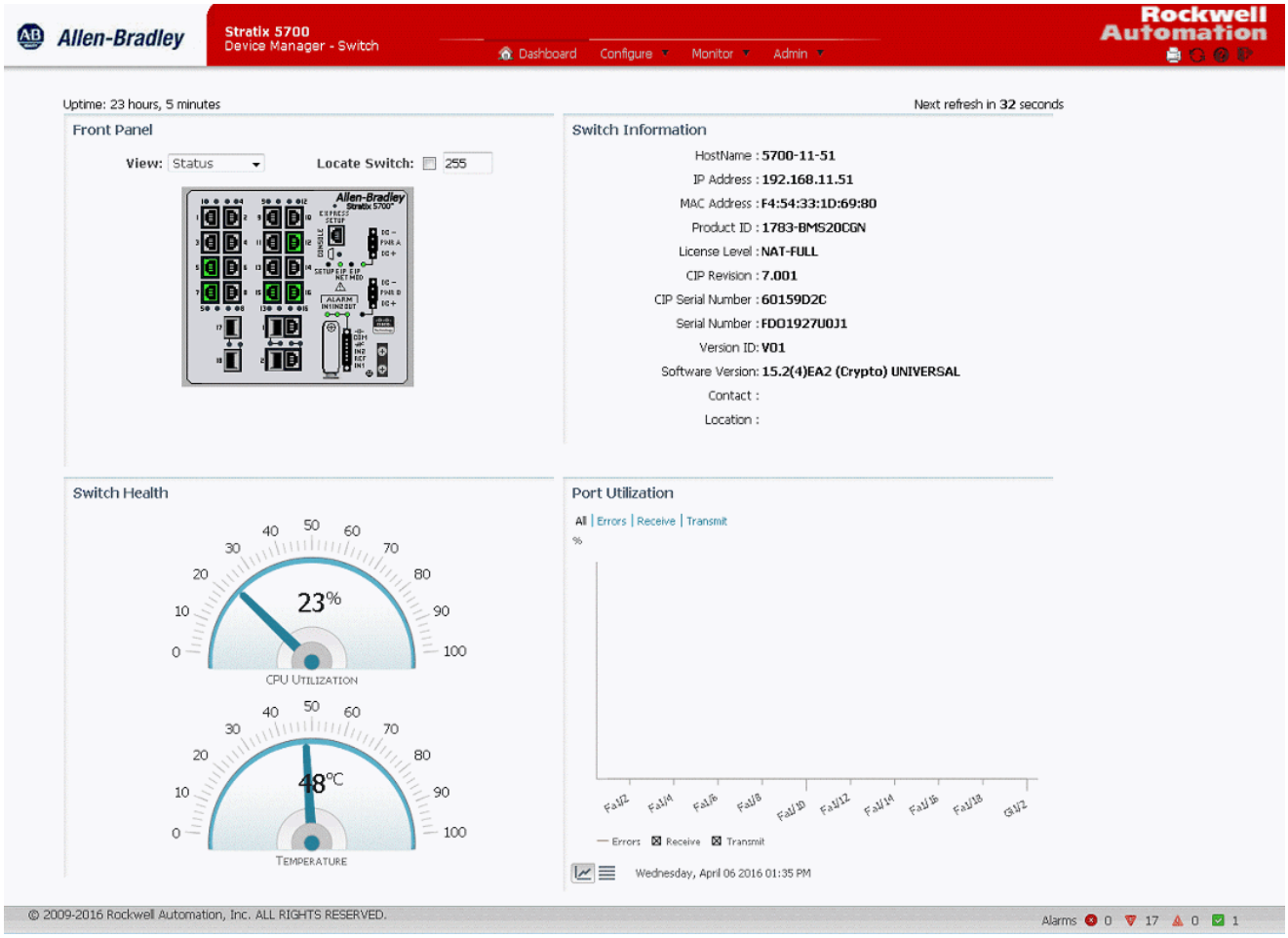
The Dashboard window in Device Manager lets you monitor switch status and performance.

The Dashboard window is similar to the Monitor > Trends window. The Dashboard window displays the instantaneous status while the Trends window displays the historical status. By using them together, you can gather the detailed conditions of the switch and its ports. For information about the Trends window, see page 394.

The Front Panel has four areas to monitor the status of the switch:

- Front Panel, as described on page 373
- Switch Information, as described on page 385
- Switch Health, as described on page 386
- Port Utilization, as described on page 387

Figure 52 - Dashboard Window

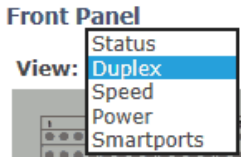


Front Panel

The Front Panel view on the dashboard is a graphical display of the switch front panel. The switch components on the front panel view are color-coded by status. The status indicators on the view in Device Manager match the status indicators on the physical switch:

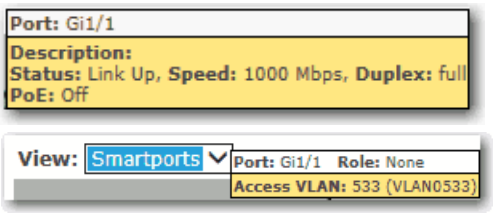
- System status indicators let you monitor the status of the switch, network status, power, and alarms.
- Port status indicators let you monitor the status of each port. Each combo port has two indicators: one for the SFP module and one for the RF45 connector. You can change the behavior of the port status indicators by choosing a view mode from the View pull-down on the front panel view. Stratix® 5400 and Stratix 5410 switches also have a Mode button on the physical switch that affects the behavior of the port status indicators.

Figure 53 - Front Panel View Menu



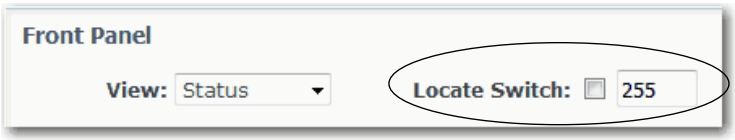
To display specific information about the port and its status, hover your mouse pointer over a port image. When you choose Smartports from the View pull-down menu, the hover text for a port image shows the Smartport role and VLAN assigned to the port.

Figure 54 - Port Hover Text



You can identify the physical switch in the group of similar devices by checking the Locate Switch checkbox on the Front Panel view.

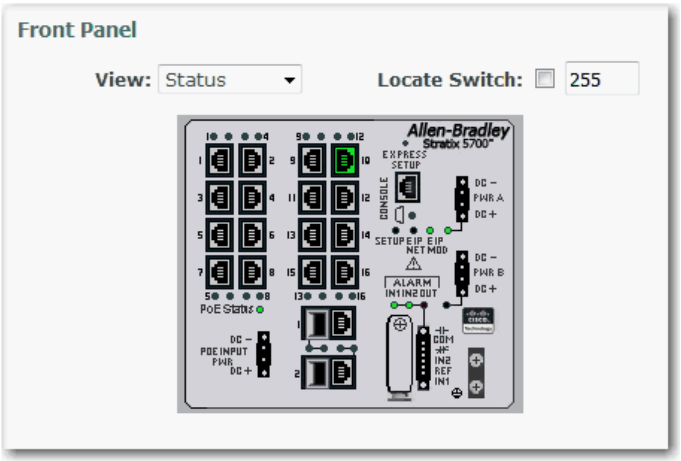
Figure 55 - Locate Switch Checkbox



When you check the Locate Switch checkbox, the system status indicators on the physical switch (Setup, EIP NET, EIP Mod, Alarm) flash green to visually notify you that the feature is enabled. The status indicators continue to flash green for the length of time you specify in the adjacent field. Valid values are 9...255 seconds.

Stratix 5700 and ArmorStratix Front Panels

Stratix 5700 View



ArmorStratix 5700 View

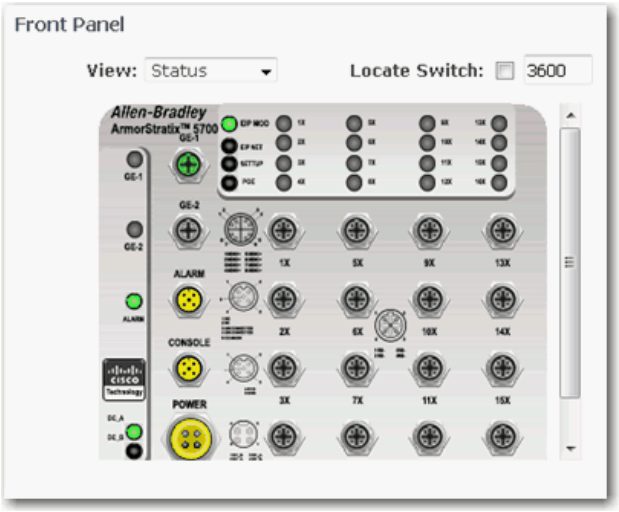


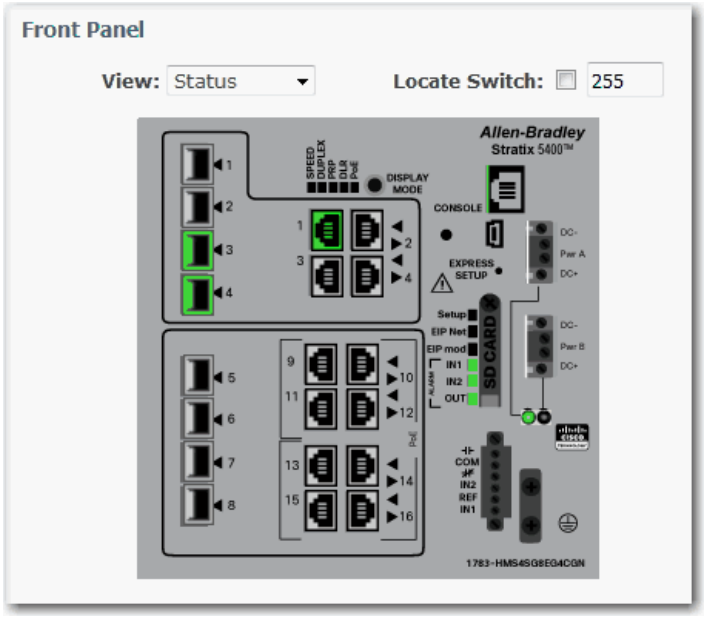
Table 95 - Stratix 5700 and ArmorStratix 5700 System Status Indicators

Indicator	Status	Description
Setup	The Setup status indicator shows the status of the initial setup of the switch.	
	Off	The switch is configured as a managed switch.
	Solid green	The switch is in initial setup.
	Flashing green	The switch is in initial setup, fault recovery, or initial setup is incomplete.
	Solid red	The switch failed to start initial setup or recovery because there is no available switch port to connect to the management station. Disconnect a device from a switch port, then press the Express Setup button on the switch.
EIP Net	The EIP Net status indicator shows the network status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch has an established CIP connection to one or more attached devices.
	Flashing green	The switch has an IP address but the switch does not have an established connection to one or more attached devices.
	Flashing red	One or more connections to attached devices have timed out.
	Solid Red	The switch has detected that its IP address is already in use by another device in the network.
	Flashing green and red	The switch is running its power-on self-test (POST).
EIP Mod	The EIP Mod status indicator shows the status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch is operating properly.
	Flashing green	The switch is not configured. For example, the switch does not have an IP address configured.
	Flashing red	The switch has detected a recoverable system fault.
	Solid red	The switch has detected a nonrecoverable system fault.
	Flashing green and red	The switch is running its power-on self-test (POST).
DC_A/PWR A DC_B/PWR B	The power status indicators show the status of power to the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	Power is present on the associated circuit.
	Solid red	Power is not present on the associated circuit, and the switch is configured for dual-input power.
Alarm IN1 Alarm IN2	The alarm input status indicators show the status of the alarm inputs.	
	Off	Alarm input is not configured.
	Solid green	Alarm input is configured; no alarm detected.
	Flashing red	Major alarm detected.
	Solid red	Minor alarm detected.
Alarm Out	The alarm out status indicators show the status of the alarm output.	
	Off	Alarm Out is not configured, or the switch is off.
	Solid green	Alarm Out is configured; no alarm is detected.
	Flashing red	The switch has detected a major alarm.

Table 96 - Stratix 5700 and ArmorStratix 5700 Port Status Indicators

Mode	Status	Description
Status	In Status mode, the port status indicators show the connection and activity status of the port. Status mode is the default mode.	
	Off	No link present on the port.
	Solid green	Port link; no activity.
	Flashing green and off	Link is active and healthy.
	Alternating green and amber	There is a fault or error on the link.
	Solid amber	The port is disabled.
Duplex	In Duplex mode, the port status indicators show the Duplex mode (Full-duplex or Half-duplex) of the ports. The 10/100/1000 ports operate only in Full-duplex mode.	
	Off	The port is not operating.
	Solid amber	The port is operating in Half-duplex mode.
	Solid green	The port is operating in Full duplex mode.
Speed	In Speed mode, the port status indicators show the operating speed of the ports.	
	Off	The port is not operating.
	Solid amber	The port is operating at 10 Mbps.
	Solid green	The port is operating at 100 Mbps.
	Flashing green	The port is operating at 1000 Mbps.
Power	In Power mode, the port status indicators show the status of PoE on switch models with PoE capability.	
	Off	PoE is disabled on the port.
	Solid green	PoE is enabled on the port. The switch port is providing power.
	Flashing green and amber	PoE is denied because it exceeds the power capacity of the switch.
	Flashing amber	PoE is denied because it exceeds the configured power limit for the switch port.

Stratix 5400 Front Panel



In addition to the View modes on the Dashboard window, the Stratix 5400 switch has a Display Mode button on the physical switch. The Display Mode button changes the behavior of the port status indicators based on the selected mode. Select a mode by pressing the Display Mode button on the physical switch. Each time that you press the switch, the active mode moves from the default Status mode to Speed, Duplex, PRP, and PoE respectively, and then back to Status mode. For a description of the modes, see Table 98.

When a mode is active, its mode status indicator turns on. When a mode is inactive, its mode status indicator turns off. When all status indicators for Speed, Duplex, PRP, DLR, and PoE are off, the switch is in the default Status mode.

Figure 56 - Stratix 5400 Display Modes

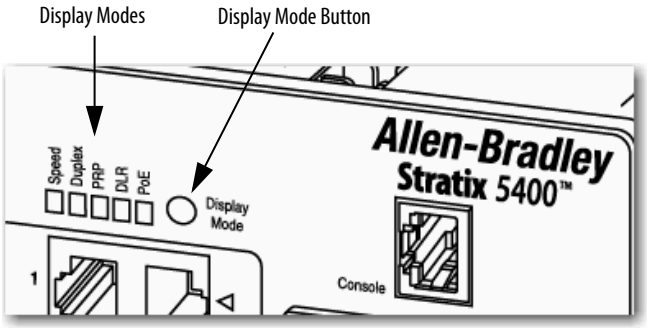


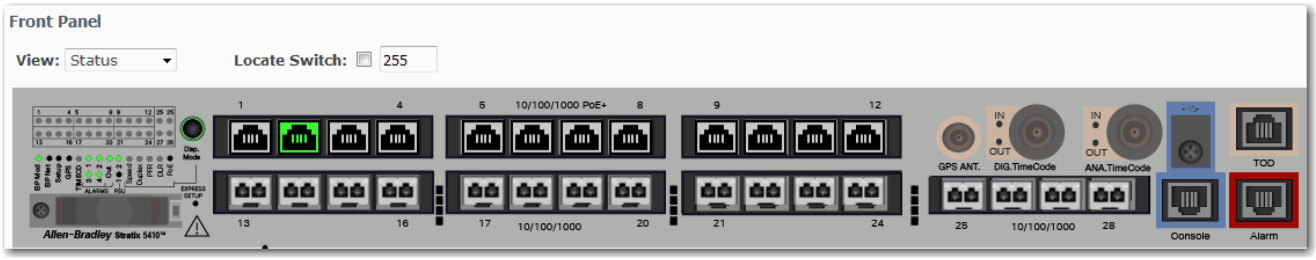
Table 97 - Stratix 5400 System Status Indicators

Indicator	Status	Description
Setup	The Setup status indicator shows the status of the initial setup of the switch.	
	Off	The switch is configured as a managed switch.
	Solid green	The switch is in initial setup.
	Flashing green	The switch is in initial setup, fault recovery, or initial setup is incomplete.
	Solid red	The switch failed to start initial setup or recovery because there is no available switch port to connect to the management station. Disconnect a device from a switch port, then press the Express Setup button on the switch.
EIP Net	The EIP Net status indicator shows the network status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch has an established CIP connection to one or more attached devices.
	Flashing green	The switch has an IP address but the switch does not have an established connection to one or more attached devices.
	Flashing red	One or more connections to attached devices have timed out.
	Solid Red	The switch has detected that its IP address is already in use by another device in the network.
	Flashing green and red	The switch is running its power-on self-test (POST).
EIP Mod	The EIP Mod status indicator shows the status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch is operating properly.
	Flashing green	The switch is not configured. For example, the switch does not have an IP address configured.
	Flashing red	The switch has detected a recoverable system fault.
	Solid red	The switch has detected a nonrecoverable system fault.
	Flashing green and red	The switch is running its power-on self-test (POST).
Pwr A Pwr B	The power status indicators show the status of power to the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	Power is present on the associated circuit.
	Solid red	Power is not present on the associated circuit, and the switch is configured for dual-input power.
Alarm IN1 Alarm IN2	The alarm input status indicators show the status of the alarm inputs.	
	Off	Alarm input is not configured.
	Solid green	Alarm input is configured; no alarm detected.
	Flashing red	Major alarm detected.
	Solid red	Minor alarm detected.
Alarm Out	The alarm out status indicator shows the status of the alarm output.	
	Off	Alarm Out is not configured, or the switch is off.
	Solid green	Alarm Out is configured; no alarm is detected.
	Flashing red	The switch has detected a major alarm.

Table 98 - Stratix 5400 Port Status Indicators

Mode	Status	Description
Status	In Status mode, the port status indicators show the connection and activity status of the port. Status mode is the default mode. You can choose Status mode via the View pull-down menu in Device Manager. You can also choose Status mode by pressing the Disp. Mode button on the physical switch until all mode status indicators on the switch turn off.	
	Off	No link present on the port.
	Solid green	Port link; no activity.
	Flashing green and off	Link is active and healthy.
	Alternating green and amber	There is a fault or error on the link.
	Solid amber	The port is disabled.
Duplex	In Duplex mode, the port status indicators show the Duplex mode (Full-duplex or Half-duplex) of the ports. The 10/100/1000 ports operate only in Full-duplex mode.	
	Off	The port is not operating.
	Solid amber	The port is operating in Half-duplex mode.
	Solid green	The port is operating in Full duplex mode.
Speed	In Speed mode, the port status indicators show the operating speed of the ports.	
	Off	The port is not operating.
	Solid amber	The port is operating at 10 Mbps.
	Solid green	The port is operating at 100 Mbps.
	Flashing green	The port is operating at 1000 Mbps.
PRP	In PRP mode, the port status indicators show the status of Parallel Redundancy Protocol (PRP). To configure PRP, see page 297.	
	Off	PRP is disabled or not in use on the port.
	Solid green	PRP is active on the port.
DLR—Not functional as of the current release.		
Power/PoE	In Power or PoE mode, the port status indicators show the status of PoE on switch models with PoE capability. The Power mode available via the View pull-down menu in Device Manager is the same as the PoE mode available via the Disp. Mode button on the physical switch.	
	Off	PoE is disabled on the port.
	Solid green	PoE is enabled on the port. The switch port is providing power.
	Flashing green and amber	PoE is denied because it exceeds the power capacity of the switch.
	Flashing amber	PoE is denied because it exceeds the configured power limit for the switch port.

Stratix 5410 Front Panel



In addition to the View modes on the Dashboard window, the Stratix 5410 switch has a Disp. Mode button on the physical switch that changes the behavior of the port status indicators based on the selected mode. Select a mode by pressing the Disp. Mode button on the physical switch. Each time that you press the switch, the active mode moves from the default Status mode to Speed, Duplex, PRP, and PoE respectively, and then back to Status mode. For a description of the modes, see Table 100.

When a mode is active, its mode status indicator turns on. When a mode is inactive, its mode status indicator turns off. When all status indicators for Speed, Duplex, PRP, DLR, and PoE are off, the switch is in the default Status mode.

Figure 57 - Stratix 5410 Display Modes

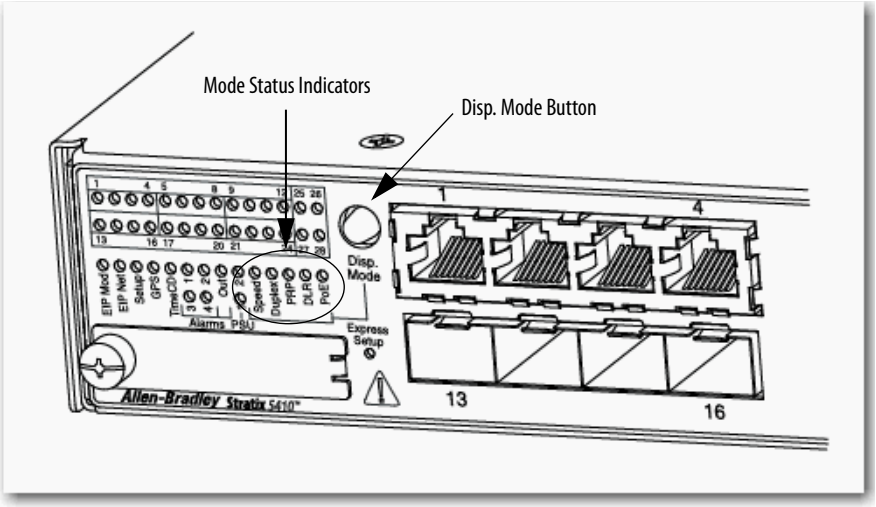


Table 99 - Stratix 5410 System Status Indicators

Indicator	Status	Description
EIP Mod	The EIP Mod status indicator shows the status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch is operating properly.
	Flashing green	The switch is not configured. For example, the switch does not have an IP address configured.
	Flashing red	The switch has detected a recoverable system fault.
	Solid red	The switch has detected a nonrecoverable system fault.
	Flashing green and red	The switch is running its power-on self-test (POST).
EIP Net	The EIP Net status indicator shows the network status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch has an established CIP connection to one or more attached devices.
	Flashing green	The switch has an IP address but the switch does not have an established connection to one or more attached devices.
	Flashing red	One or more connections to attached devices have timed out.
	Solid Red	The switch has detected that its IP address is already in use by another device in the network.
	Flashing green and red	The switch is running its power-on self-test (POST).
Setup	The Setup status indicator shows the status of the initial setup of the switch.	
	Off	The switch is configured as a managed switch.
	Solid green	The switch is in initial setup.
	Flashing green	The switch is in initial setup, fault recovery, or initial setup is incomplete.
	Solid amber	The switch failed to start initial setup or recovery because there is no available switch port to connect to the management station. Disconnect a device from a switch port, then press the Express Setup button on the switch.
GPS	Not available in the current release.	
TimeCD	Not available in the current release.	
Alarms 1…4	The alarm input status indicators show the status of the alarm inputs.	
	Off	Alarm input is not configured.
	Solid green	Alarm input is configured; no alarm detected.
	Solid red	Minor alarm detected.
	Flashing red	Major alarm detected.
	Alternating green and red	Critical alarm detected.
Alarm Out	The alarm input status indicator shows the status of the alarm output.	
	Off	Alarm Out is not configured.
	Solid green	Alarm Out is configured; no alarm detected.
	Solid red	Alarm detected.
PSU 1 PSU 2	The power status indicators show the status of power to the switch.	
	Off	Power is not present on the circuit, or the system is not powered up.
	Solid green	Power output is good.
	Flashing red	Power supply is installed, but power input is bad.
	Solid red	Power output is bad.

Table 100 - Stratix 5410 Port Status Indicators

Mode	Status	Description
Status	In Status mode, the port status indicators show the connection and activity status of the port. Status mode is the default mode. You can choose Status mode via the View pull-down menu in Device Manager. You can also choose Status mode by pressing the Disp. Mode button on the physical switch until all mode status indicators on the switch turn off.	
	Off	No link present on the port.
	Solid green	Port link; no activity.
	Flashing green and off	Link is active and healthy.
	Alternating green and amber	There is a fault or error on the link.
	Solid amber	The port is disabled.
Speed	In Speed mode, the port status indicators show the operating speed of the ports.	
Ports 1…24	Off	The port is not operating.
	Solid amber	The port is operating at 10 Mbps.
	Solid green	The port is operating at 100 Mbps.
	Flashing green	The port is operating at 1000 Mbps.
Ports 25…28	Off	The port is not operating.
	Solid green	The port is operating at 1000 Mbps
	Flashing green	The port is operating at 10 Gbps.
Duplex	In Duplex mode, the port status indicators show the Duplex mode (Full-duplex or Half-duplex) of the ports. The 10/100/1000 ports operate only in Full-duplex mode.	
	Off	The port is not operating.
	Solid amber	The port is operating in Half-duplex mode.
	Solid green	The port is operating in Full duplex mode.
PRP	In PRP mode, the port status indicators show the status of Parallel Redundancy Protocol (PRP). To configure PRP, see page 297.	
	Off	PRP is disabled or not in use on the port.
	Solid green	PRP is configured and active on the port.
	Solid amber	PRP is configured on the port and has a redundancy fault.
DLR—Not functional as of the current release.		
Power or PoE	In Power or PoE mode, the port status indicators show the status of PoE. The Power mode available via the View pull-down menu in Device Manager is the same as the PoE mode available via the Disp. Mode button on the physical switch.	
	Off	PoE is not enabled on the port.
	Solid green	PoE is enabled on the port and functioning properly.
	Alternating green and amber	PoE is enabled on the port, but power is disconnected or failing on this low priority port.
	Flashing amber	PoE is enabled on the port, but power is disconnected or failing on this high priority port.
	Solid amber	PoE is enabled on the port, but has failures.

Stratix 8000/8300 Front Panel

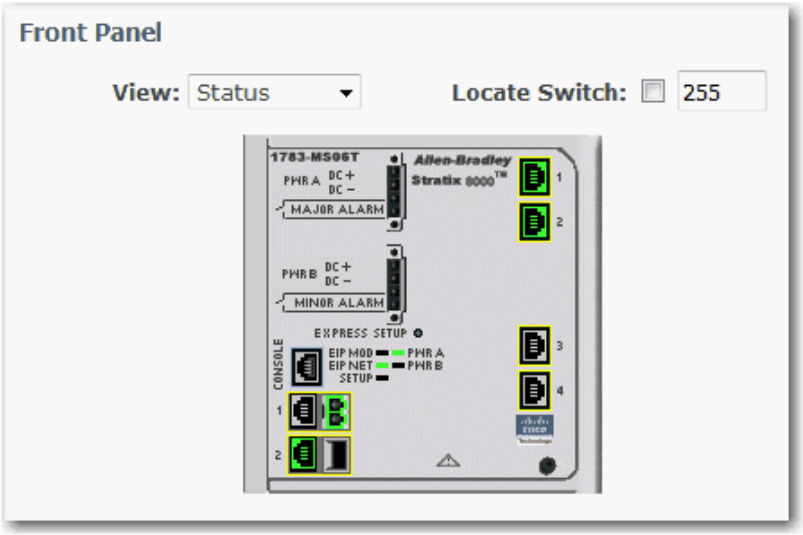


Table 101 - Stratix 8000/8300 System Status Indicators

Indicator	Status	Description
EIP Mod	The EIP Mod status indicator shows the status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch is operating properly.
	Flashing green	The switch is not configured. For example, the switch does not have an IP address configured.
	Flashing red	The switch has detected a recoverable system fault. Use the system log to see more details about the problem. See System Log Messages on page 392.
	Solid red	The switch has detected a nonrecoverable system. Use the system log to see more details about the problem. See System Log Messages on page 392.
	Flashing green and red	The switch is running its power-on self-test (POST).
EIP Net	The EIP Net status indicator shows the network status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch has an established CIP connection to one or more attached devices.
	Flashing green	The switch has an IP address but the switch does not have an established connection to one or more attached devices.
	Flashing red	One or more connections to attached devices have timed out.
	Solid red	The switch has detected that its IP address is already in use by another device in the network.
	Flashing green and red	The switch is running its power-on self-test (POST).
Setup	The configuration mode in which the switch is operating.	
	Off	The switch is configured as a managed switch or the switch is operating as an unmanaged switch.
	Flashing green	Switch is in the initial Setup mode or is in the Direct Managed mode, or the initial setup is incomplete.
Pwr A and Pwr B	The Pwr status indicators show the DC power status.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	Power is present.
	Solid red	Power to the switch is not present and the power alarm is on.

Table 102 - Stratix 8000/8300 Port Status Indicators

Mode	Status	Description
Status	In Status mode, the port status indicators show the status of the ports. Status is the default mode.	
	Off	No link
	Solid green	No activity on link.
	Flashing green	Link activity.
	Solid brown	Port has been disabled.
	Yellow	An error has disabled the port.
	Flashing green and amber	Faulty link.
	Flashing amber	Smartports configuration mismatch on port.
	Solid amber	Port is faulty, disabled due to an error, or is in an STP-blocked state.
Duplex	In Duplex mode, the port status indicators show the Duplex mode (Full-duplex or Half-duplex) of the ports. The 10/100/1000 ports operate only in Full-duplex mode.	
	Off	No link.
	Solid light blue	Port is in Half-duplex mode.
	Solid green	Port is in Full-duplex mode.
Speed	In Speed mode, the port status indicators show the operating speed of the ports.	
	Off	No link.
	Solid light blue	10 Mbps
	Solid green	100 Mbps
	Flashing green	1000 Mbps

Switch Information

The Switch Information area on the Dashboard displays information about the switch.

Table 103 - Switch Information Fields

Field	Description
Host Name	A descriptive name for this switch. The default name is Switch. You can set this parameter on the Admin > Express Setup window.
IP Address	The IP address of this switch. You can configure this setting on the Admin > Express Setup window.
MAC Address	The MAC address of this switch. This information cannot be changed.
Product ID	The model of this switch. This information cannot be changed.
License Level	The type of firmware on the switch: Full or Lite. This information cannot be changed.
CIP Revision	The version of Common Industrial Protocol (CIP) that is supported on this switch. This information cannot be changed.
CIP Serial Number	The CIP serial number. This information cannot be changed.
Serial Number	The serial number of this switch. This information cannot be changed.
Version ID	The hardware version. This information cannot be changed.
Software	The version of IOS that this switch is running. This information is updated when you upgrade the switch firmware.
Contact	The person who is the administrative contact for this switch. You can set this parameter on the Configure > SNMP window.
Location	The physical location of this switch. You can set this parameter on the Configure > SNMP window.

Switch Health

You can use the health gauges to monitor CPU utilization and temperature.

The CPU Utilization gauge shows the percentage of CPU processing power that is in use on the switch. Data is collected at each 60-second system refresh. The gauge changes as the switch experiences the network activity from devices sending data through the network. As network activity increases, so does contention between devices to send data through the network.

As you monitor utilization on the switch, note whether the percentage of usage is what you expect during that given time of network activity. If utilization is high when you expect it to be low, perhaps a problem exists. As you monitor the switch, note if the bandwidth utilization is consistently high, which can indicate congestion in the network. If the switch reaches its maximum bandwidth (above 90% utilization) and its buffers become full, it begins to discard the data packets that it receives. Some packet loss in the network is not considered unusual, and the switch is configured to help recover lost packets, such as by signaling to other devices to resend data. However, excessive packet loss can create packet errors, which can degrade overall network performance.

To reduce congestion, consider segmenting the network into subnetworks that are connected by other switches or routers. Look for other causes, such as faulty devices or connections, which can also increase bandwidth utilization on the switch.

The Temperature gauge shows the internal temperature of the switch. For information about the switch temperature range and the operating environment guidelines, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Port Utilization

You can choose which types of network traffic to display and in what format:

- Types of traffic—By default, all traffic is displayed for all interfaces. Click the links above the display area to display all traffic, errors, received traffic, or transmitted traffic.
- Formats—Click the buttons below the display area to view the data in Chart Mode or Grid Mode.
- Chart details—When displaying a chart, position your mouse pointer over a bar or a point on the chart to view the data.

As you monitor the usage on the ports, note whether the percentage is what you expect during that given time of network activity. If usage is high when you expect it to be low, a problem can exist. Bandwidth allocation can also be based on whether the connection is operating in Half-duplex or Full-duplex mode.

Reasons for errors that are received on or sent from the switch ports include the following:

- Bad cable connection
- Defective ports
- Software problems
- Driver problems

Data is collected at each 60-second system refresh.

See Trends on page 394 for a graph to view per-port patterns over incremental instances in time (by 60 seconds, 1 hour, 1 day, or 1 week).

See Port Statistics on page 395 for details on the specific port errors that are detected on each port.

Switch Status via the Logix Designer Application

The Switch Status view in the Studio 5000 Logix Designer® application lets you view status parameters for the switch.

In the navigation pane, click Switch Status.

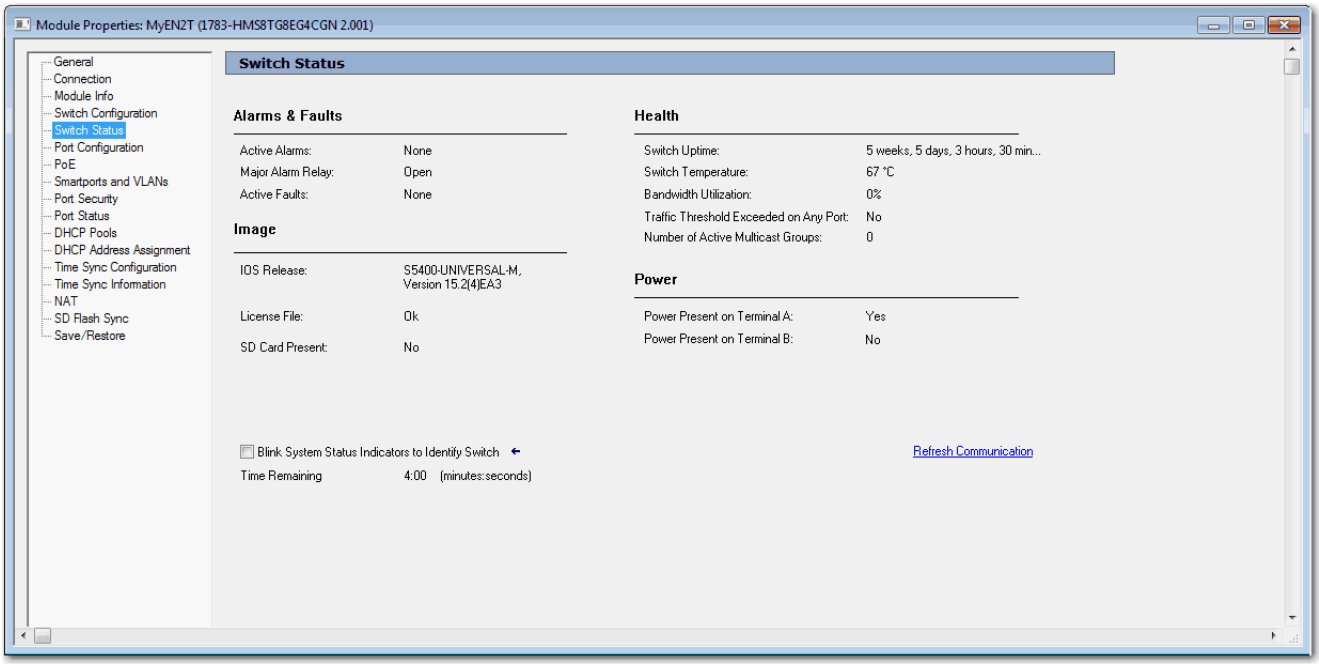


Table 104 - Switch Status Fields

Field	Description
Alarms & Faults	
Active Alarms	Displays one of these values: • None • Port alarm • Dual Mode Power Supply alarm • Primary Temperature alarm
Major Alarm Relay	Displays one of these values: • Open • Closed
Active Faults	Displays one of these values: • None • Port fault • Hardware fault If the port and hardware faults are active, the Hardware fault status appears.
Health	
Switch Uptime	Displays the days, hours, and minutes that the switch has been functioning since the last restart.
Switch Temperature	Displays the current internal temperature (in degree Celsius) of the switch.
Bandwidth Utilization	Displays the total percentage of the switch bandwidth being used.
Traffic Threshold Exceeded on Any Port	Displays a yes or no value to indicate whether the current unicast, multicast, and broadcast thresholds have been exceeded on any port.
Number of Active Multicast Groups	Displays the number of active multicast groups.
Image	
IOS Release	Displays the current version of the switch operating system.
License File	Displays whether the license file is valid.

Table 104 - Switch Status Fields (Continued)

Field	Description
SD Card Present	Displays whether the SD card is installed.
Power	
Power Present on Terminal A	Displays a yes or no value to indicate whether power is present on Terminal A.
Power Present on Terminal B	Displays a yes or no value to indicate whether power is present on Terminal B.
Power Supply Unit 1 (Stratix 5410 switches)	Displays the type of power supply installed in the PSU1 slot. If a fault exists with a power supply, the field displays either AC_Fault or DC_Fault. Valid values: • AC • AC_Fault • DC • DC_Fault • None
Power Supply Unit 2 (Stratix 5410 switches)	Displays the type of power supply installed in the PSU2 slot. If a fault exists with a power supply, the field displays either AC_Fault or DC_Fault. Valid values: • AC • AC_Fault • DC • DC_Fault • None
Locate Switch Feature	
Blink System Status Indicators to Identify Switch	If you need to physically connect or disconnect ports or move a switch in a group of similar devices, you can identify the switch in the group by checking this checkbox. When you check the checkbox, the system status indicators on the physical switch (Setup, EIP NET, EIP Mod, Alarm) flash green for 4 minutes or until you clear this checkbox.
Time Remaining	Displays the amount of time remaining for the system status indicators to continue flashing while the Blink EIP LED checkbox is checked.

You can also monitor the switch status on the Module Info view.

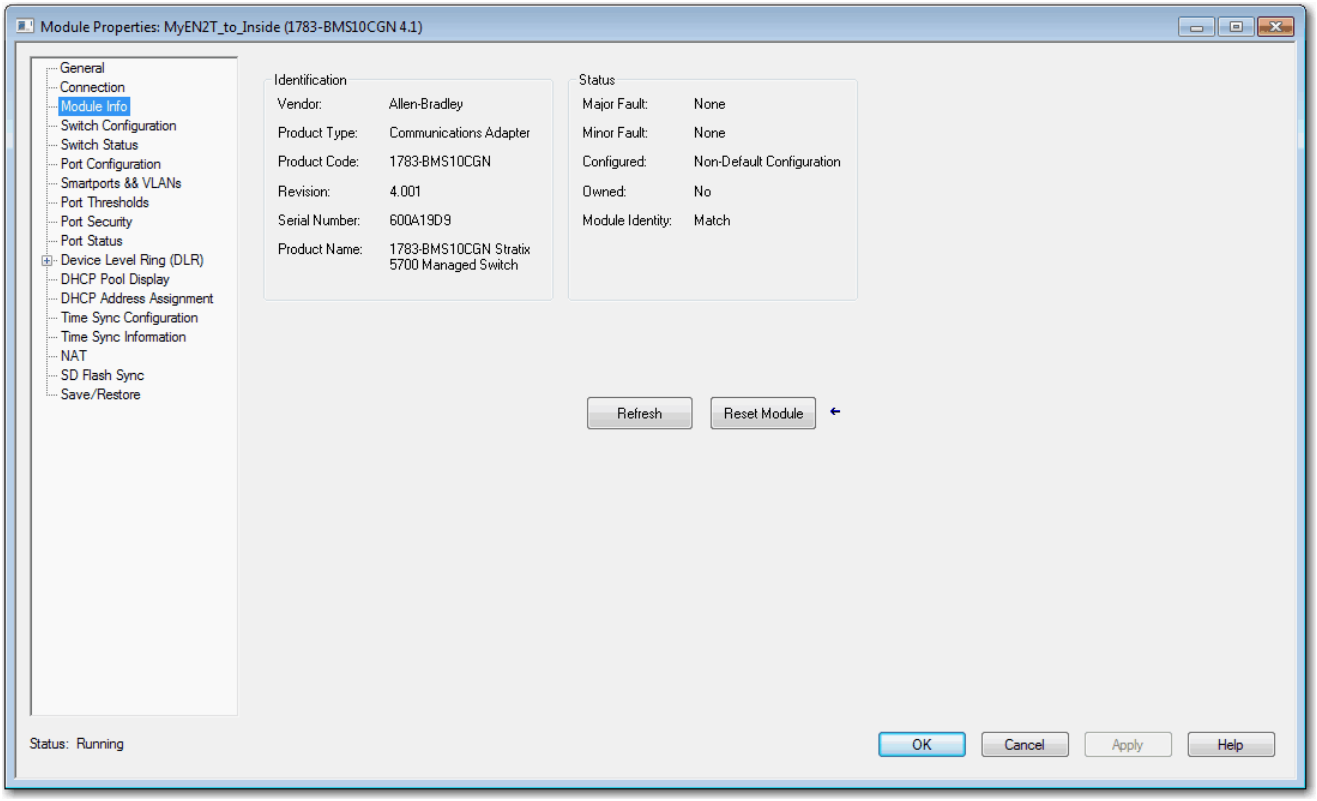


Table 105 - Module Info Fields

Field	Description
Identification	Displays the following switch information: • Vendor • Product type • Product code • Revision • Serial number • Product name
Status	Displays the following status information: • Major/minor fault status – None – Recoverable – Nonrecoverable • Configuration – Non-default configuration – Default configuration • Owned – Yes. There is an I/O connection. – No. There is not an I/O connection. • Module identity – Match. Agrees with what is specified on the General view. In order for the Match condition to exist, the vendor, product type, product code, and major revision must agree. – Mismatch. Does not agree with what is specified on the General view. The Module Identity field does not take into account the Electronic Keying or Minor Revision selections for the switch that were specified on the General view.

Port Status

In the navigation pane, click Port Status.

You can monitor alarms, statuses, thresholds, and bandwidth utilization for each switch port. You can also access port and cable diagnostics.

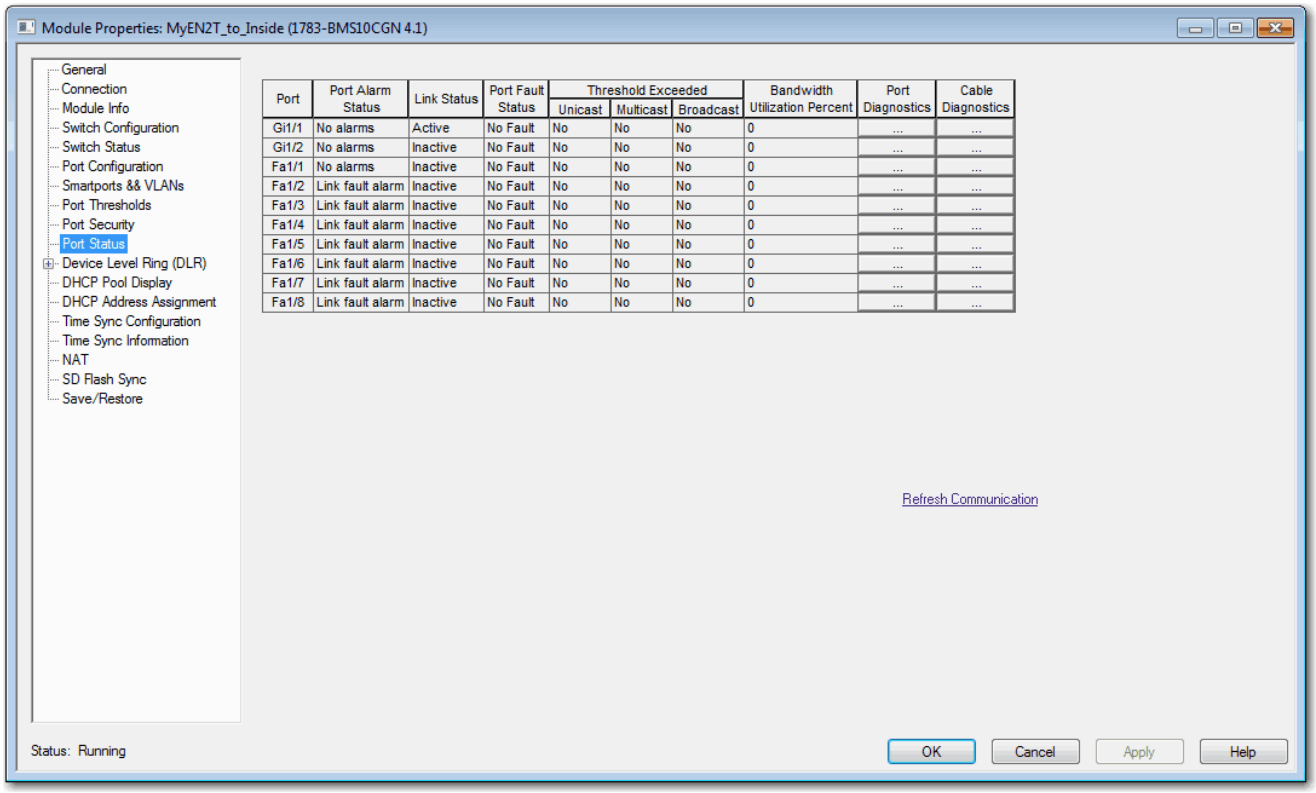


Table 106 - Port Status Fields

Field	Description
Unit (Stratix 8000/8300 switches)	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	Displays the selected port. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet) and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Port Alarm Status	Displays the status of the port alarm. Valid values: • Link fault alarm • Port not forwarding alarm • Port not operating alarm • High bit error rate alarm • No alarms
Link Status	Displays whether the link is active or inactive.
Port Fault Status	Displays the status of the port alarm. Valid values: • Error - Disable event • SFP error - Disabled • CDP native VLAN mismatch • MAC address flap • Port security violation • No fault

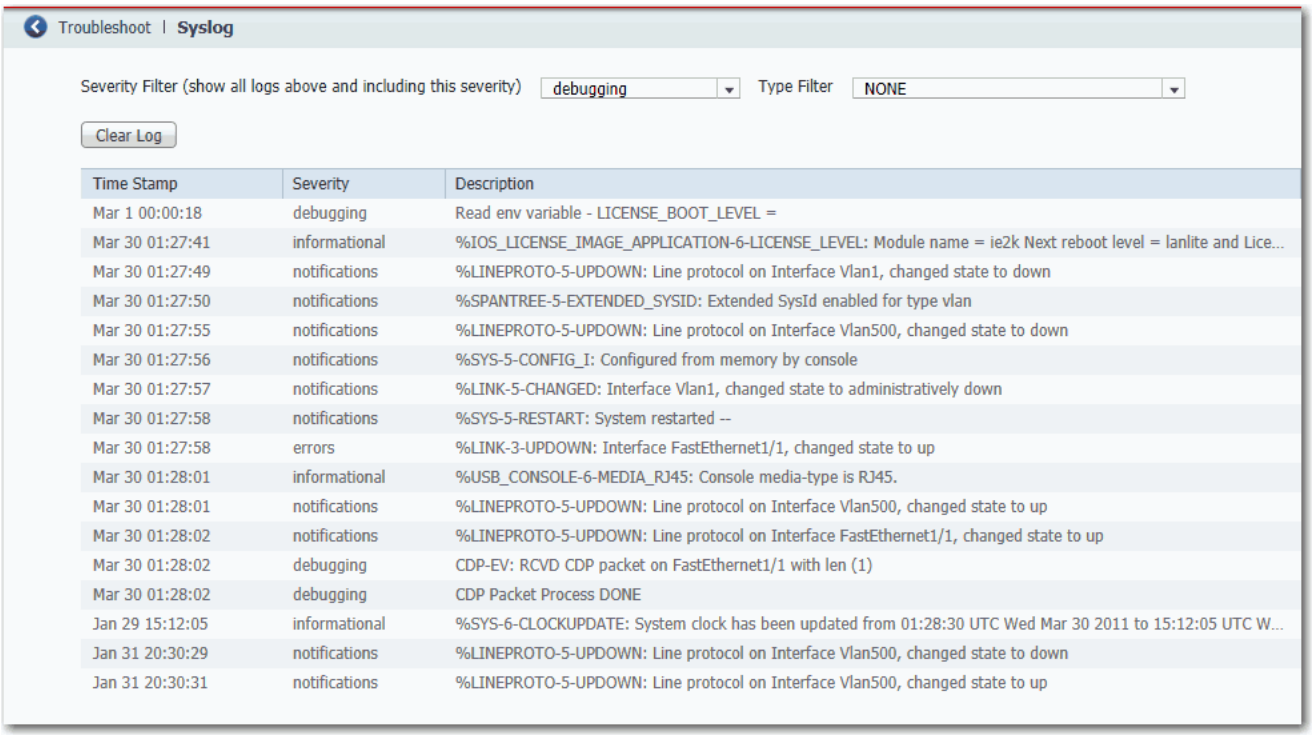
Table 106 - Port Status Fields (Continued)

Field	Description
Threshold Exceeded	Displays unusual changes for these types of network traffic: • Unicast—Displays a yes or no value to indicate whether the current unicast traffic has exceeded the threshold value. • Multicast—Displays a yes or no value to indicate whether the current multicast traffic has exceeded the threshold value. • Broadcast—Displays a yes or no value to indicate whether the current broadcast traffic has exceeded the threshold value.
Bandwidth Utilization Percent	Displays the percentage of the bandwidth being used. Note whether the percentage of usage is what you expect during the given time of network activity. If usage is higher than expected, an issue can exist.
Port Diagnostics	Click to display information to diagnose a network performance issue for the corresponding port. See page 412.
Cable Diagnostics	Click to display information to diagnose a cable issue for the corresponding port. See page 414.

System Log Messages

In Device Manager, the system log displays events that occur on the switch and its ports. The events are based on the Alarm Settings you configure on the Configure > Alarm Settings window.

From the Monitor menu, choose Syslog.



To filter historical events, choose a severity filter or type filter:

- Debugging—Debug messages.
- Informational—Informational messages.
- Notifications—The switch is operating normally but has a significant condition.
- Warnings—The switch has a warning condition.
- Errors—The switch has an error condition.
- Critical—The switch has a critical condition.
- Alerts—The switch requires immediate action.
- Emergencies—The switch is unusable.

Click Clear Log to acknowledge that you have read the alerts. The Clear Log button does not resolve the issue.

Table 107 - Syslog Fields

Field	Description
Time Stamp	The date and time the event occurred. Use the Express Setup window to connect the device to an NTP server. Time settings are lost if the switch loses power.
Severity Level	The type and severity of the event.
Description	The description of the problem, including the port on which the problem was detected.

Trends

In Device Manager, you can view historical data to help you to analyze traffic patterns and to identify problems. Data can be displayed in increments of seconds, minutes, hours, or days.

To view the data in a table, click the Grid Mode button below the area. To display a chart, click the Chart Mode button. Use the 60 s, 1 h, 1 d, and 1 w links to display the data in increments of 60 seconds, 1 hour, 1 day, or 1 week.

From the Monitor menu, choose Trends.

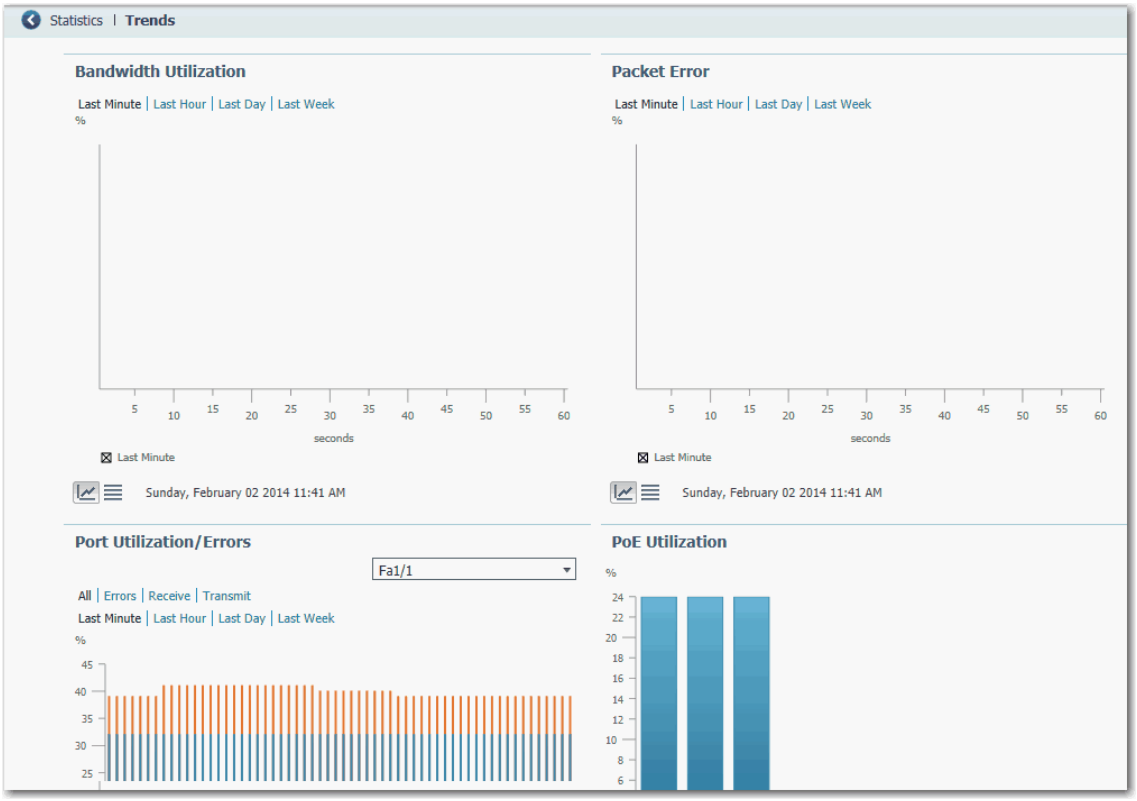


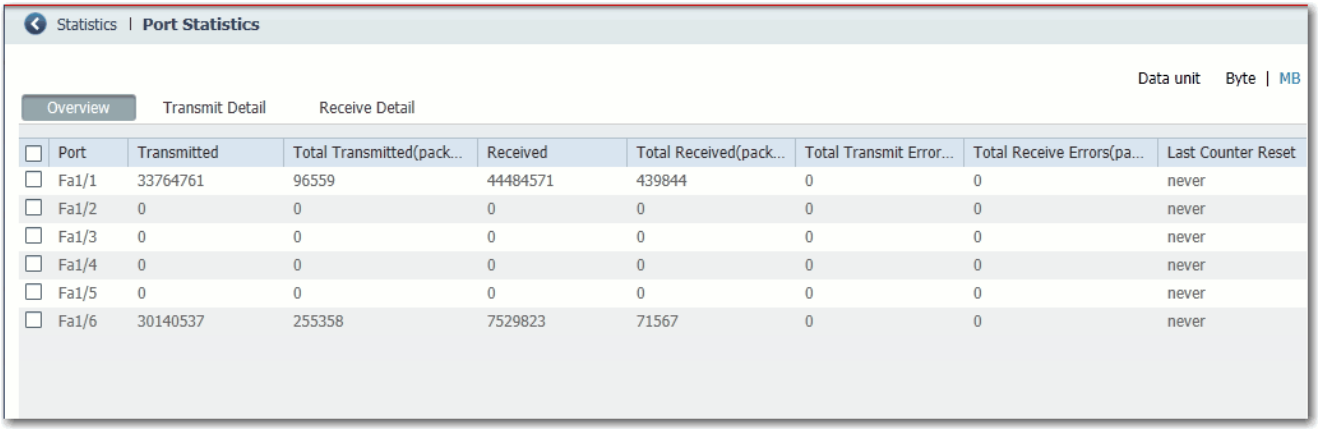
Table 108 - Trends Graphs

Graph	Description
Bandwidth Utilization	The Bandwidth Utilization graph indicates the percentage of the available bandwidth that was used. The graph can show the bandwidth usage patterns over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). This graph also marks the highest peak reached. The default is 60 seconds. You can use this data to determine when network usage is high or low.
Packet Error	The Packet Error graph shows the percentage of packet errors that are collected over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). The default is 60 seconds. Use this graph to audit the effect that connected devices have on the switch performance or the network. For example, if you suspect that a connected device is sending error packets, you can verify if the data on the graph changes when you disconnect and reconnect the device.
Port Utilization/Errors	The Port Utilization/Errors graph shows the usage patterns of a specific port over incremental instances in time by 60 seconds, 60 minutes, 24 hours, or 14 days. The default is 60 seconds. To display the trends for a specific port, choose a port from the Port list. Use these graphs to observe the performance of a specific port. For example, if a network user is having intermittent network connectivity, use the Port Utilization graph to observe the traffic patterns on the port to which the computer is connected. You can also use the Port Errors graph to see if the port is receiving or sending error packets.
PoE Utilization	For PoE switches, the PoE Utilization graph shows the power that is allocated to the connected devices.

Port Statistics

In Device Manager, you can view statistics for data that passes through the switch ports.

From the Monitor menu, choose Port Statistics. For more information, see the online help for Device Manager.



Port	Transmitted	Total Transmitted(pack...	Received	Total Received(pack...	Total Transmit Error...	Total Receive Errors(pa...	Last Counter Reset
Fa1/1	33764761	96559	44484571	439844	0	0	never
Fa1/2	0	0	0	0	0	0	never
Fa1/3	0	0	0	0	0	0	never
Fa1/4	0	0	0	0	0	0	never
Fa1/5	0	0	0	0	0	0	never
Fa1/6	30140537	255358	7529823	71567	0	0	never

The types of port statistics are grouped under these tabs on the Port Statistics window:

- Overview tab—Use this tab to display the number of error packets that is received and sent from the port. This level of detail is not available from the Dashboard graphs.

  The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity.

- Transmit Detail tab—Use this tab to troubleshoot unusual changes in network traffic. This tab displays these statistics:

  – Unicast, multicast, and broadcast packets that are sent from each port
  – Detailed statistics of errors that are sent to each port

  If a port is sending an unusually high amount of traffic, such as multicast or broadcast packets, monitor the connected device to see whether the traffic pattern is normal.

- Receive Detail tab—Use this tab to troubleshoot unusual changes in network traffic. This tab displays these statistics:

  – Unicast, multicast, and broadcast packets that are received on each port
  – Detailed statistics of errors that are received on each port

  If a port is receiving an unusually high amount of traffic, such as multicast or broadcast packets, monitor the connected device to see whether the traffic pattern is normal.

NAT Statistics

You can monitor NAT statistics in both Device Manager and the Logix Designer application.

Monitor NAT Statistics via Device Manager

You can monitor these types of NAT statistics:

- Global statistics for all instances
- Statistics per instance
- Detailed private translations per instance
- Detailed public translations per instance

From the Monitor menu, choose NAT Statistics.

Figure 58 - NAT Statistics for Stratix 5400 and 5700 Switches

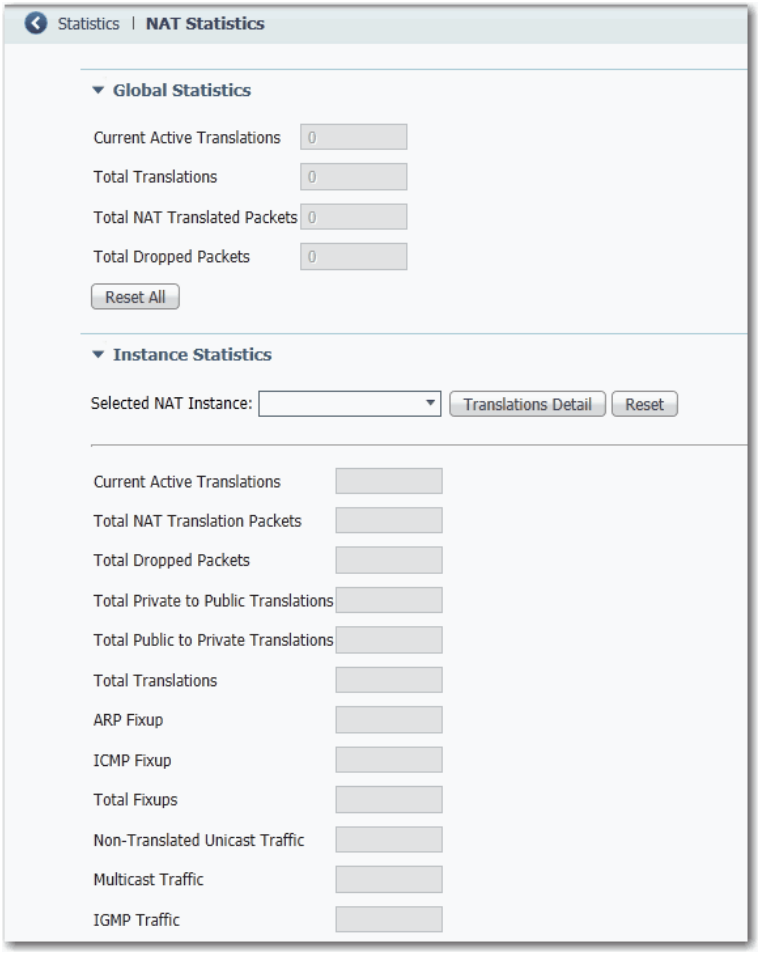


Figure 59 - NAT Statistics for Stratix 5410

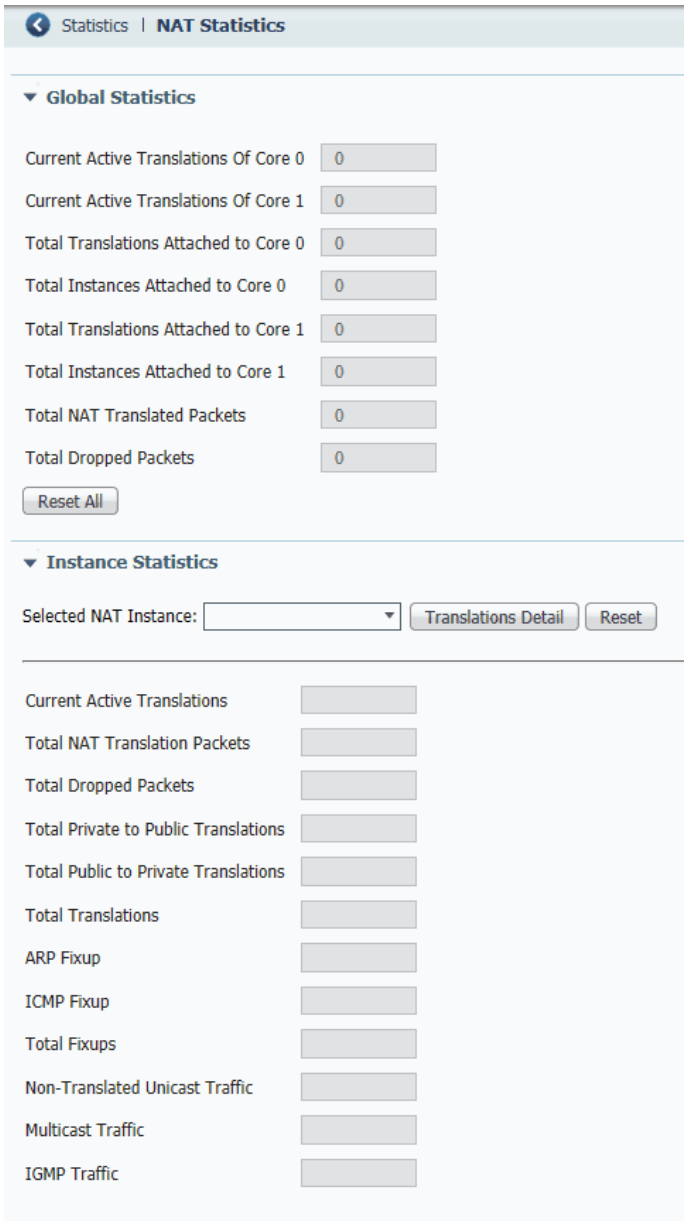


Table 109 - NAT Statistics

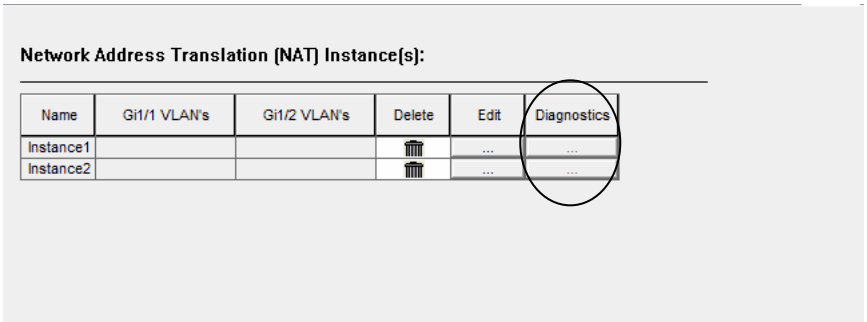
Field	Description
Global Statistic s for Stratix 5400 and 5700 Switches	
Current Active Translations	The number of IP addresses that have been translated within the last 90 seconds across all NAT instances.
Total Translations	The total number of translations across all NAT instances.
Total NAT Translated Packets	The total number of packets across all NAT instances.
Total Dropped Packets	The total number of packets that have been dropped across all NAT instances.
Global Statistic s for Stratix 5410 Switches	
Current Active Translations of Core 0	The number of IP addresses that have been translated within the last 90 seconds across all NAT instances for ports 1…6 and 13…18.
Current Active Translations of Core 1	The number of IP addresses that have been translated within the last 90 seconds across all NAT instances for ports 7…12, 19…24, and 25…28.
Total Translations Attached to Core 0	The total number of translations across all NAT instances for ports 1…6 and 13…18.
Total Instances Attached to Core 0	The total number of NAT instances across ports 1…6 and 13…18.
Total Translations Attached to Core 1	The total number translations across all NAT instances for ports 7…12, 19…24, and 25…28.
Total Instances Attached to Core 1	The total number of NAT instances across ports 7…12, 19…24, and 25…28.
Total NAT Translated Packets	The total number of packets across all NAT instances for all ports.
Total Dropped Packets	The total number of packets that have been dropped across all NAT instances for all ports.
Instance Statistics	
Selected Instance	From the pull-down menu, choose the instance for which to view statistics.
Current Active Translations	The number of translations that have occurred within the last 90 seconds for the instance.
Total NAT Translated Packets	The total number of packets that have been translated for the instance.
Total Dropped Packets	The total number of packets that have been dropped for the instance.
Total Private to Public Address Translations	The total number of translations that are configured for devices on the private subnet.
Total Public to Private Address Translations	The total number of translations that are configured for devices on the public subnet.
Total Translations	The total number of translations that are configured for the instance.
ARP Fixup	The number of ARP packets that have been fixed up for the instance.
ICMP Fixup	The number of ICMP packets that have been fixed up for the instance.
Total Fixups	The total number of ARP and ICMP packets that have been fixed up for the instance.
Non-Translated Unicast Traffic	The number of packets with untranslated unicast traffic for the instance.
Multicast Traffic	The number of packets with multicast traffic for the instance.
IGMP Traffic	The number of packets with IGMP traffic for the instance.

Monitor NAT Statistics via the Logix Designer Application

For each NAT instance, you can monitor these diagnostics:

- Diagnostics for both private and public translations
- Diagnostics for only private translations
- Diagnostics for only public translations

In the navigation pane, click NAT, and then click the ellipse in the Diagnostics column.



The NAT Diagnostics dialog box displays diagnostics for the selected instance.

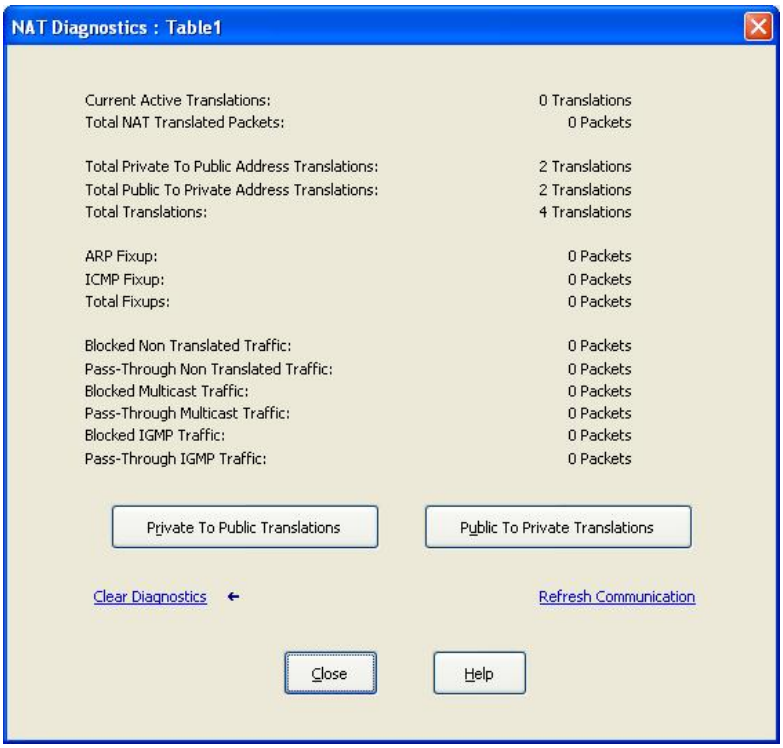


Table 110 - NAT Diagnostics per Instance

Field	Description
Current Active Translations	Displays the number of translations that have occurred within the last 90 seconds across all NAT instances.
Total NAT Translated Packets	Displays the total number of packets that have been translated for this instance.
Total Private to Public Address Translations	Displays the total number of private-to-public translations for this instance.
Total Public to Private Address Translations	Displays the total number of public-to-private translations for this instance.
ARP Fixup	Displays the number of ARP packets that have been fixed up for this instance.
ICMP Fixup	Displays the number of ICMP packets that have been fixed up for this instance.
Total Fixups	Displays the number of ARP and ICMP packets that have been fixed up for this instance.
Incoming Non Translated Traffic (Pass-Through)	Displays the number of incoming packets with untranslated traffic that NAT passed through for this instance.
Outgoing Non Translated Traffic (Blocked)	Displays the number of outgoing packets with untranslated traffic that NAT blocked for this instance.
Incoming Multicast Traffic (Blocked)	Displays the number of incoming packets with multicast traffic that NAT blocked for this instance.
Outgoing Multicast Traffic (Pass-Through)	Displays the number of outgoing packets of multicast traffic that NAT passed through for this instance.
Incoming IGMP Traffic (Blocked)	Displays the number of incoming packets with IGMP traffic that NAT blocked for this instance.
Outgoing IGMP Traffic (Blocked)	Displays the number of outgoing packets with IGMP traffic that NAT blocked for this instance.
Private to Public Translations	Click to view private-to-public translation diagnostics for the instance. page 401.
Public to Private Translations	Click to view private-to-public translation diagnostics for the instance. page 402.

Private-to-Public Translation Diagnostics

From the Private to Public Translations dialog box for an instance, you can view a list of IP addresses that have been changed by NAT within the last 90 seconds.

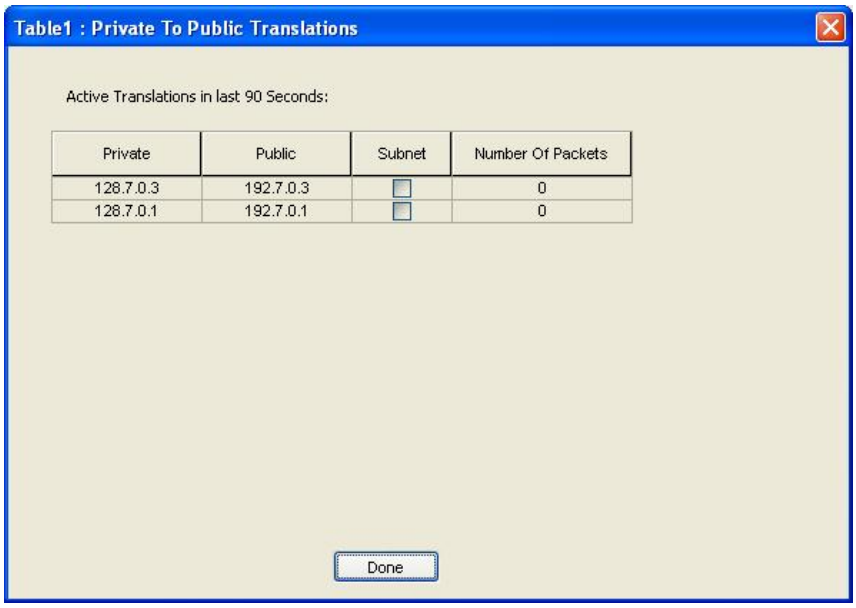


Table 111 - Private-to-Public Translation Diagnostics

Field	Description
Private	Displays the existing address for a device on the private subnet.
Public	Displays a unique public address that represents the corresponding device on the private subnet.
Subnet	Indicates whether the translation is part of a Subnet entry type.
Number of Packets	Displays the number of packets that contain the translation.

Public-to-Private Translation Diagnostics

From the Public to Private Translations dialog box for an instance, you can view a list of IP addresses that have been changed by NAT within the last 90 seconds.

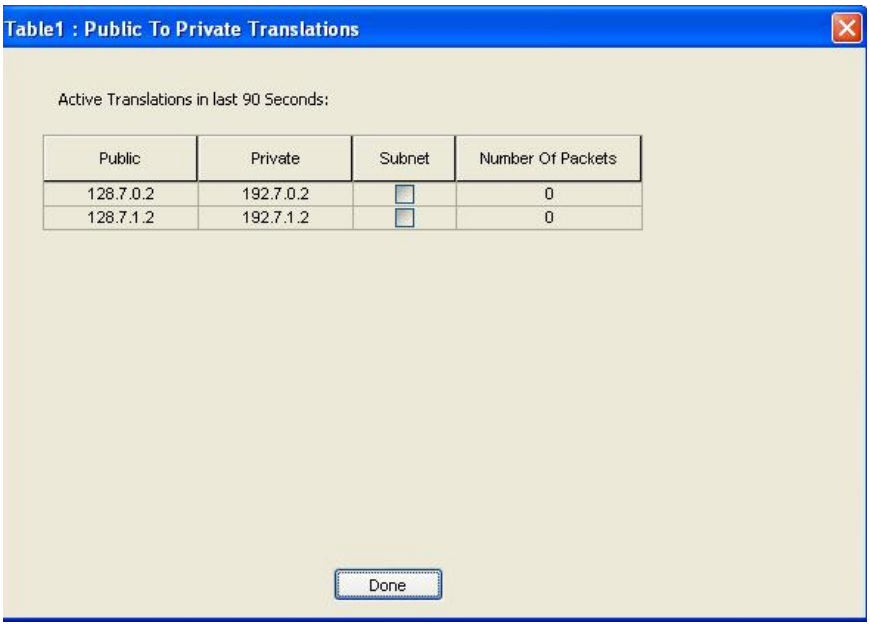


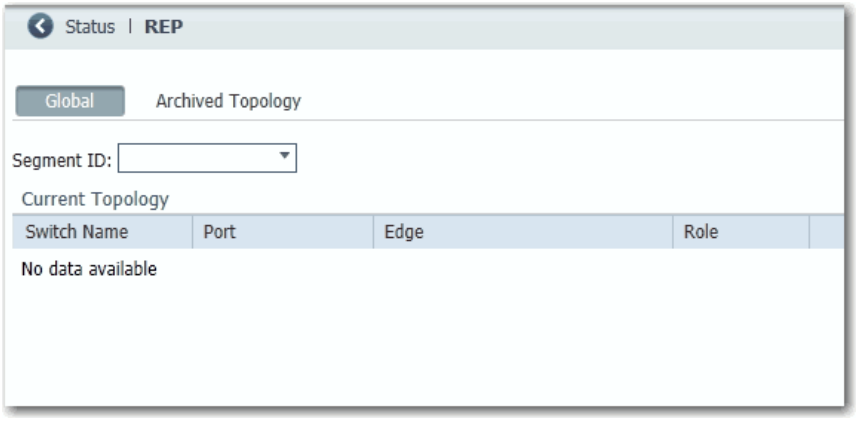
Table 112 - Public-to-Private Translation Diagnostics

Field	Description
Public	Displays the unique IP address on the public subnet that represents the corresponding IP address on the private subnet.
Private	Displays the IP address on the private subnet that was changed to a unique IP address on the public subnet.
Subnet	Indicates whether the translation is part of a Subnet entry type.
Number of Packets	Displays the number of packets that contain the translation.

REP Status

In Device Manager, you can review the status of the REP topology for one or all network segments.

From the Monitor menu, choose REP.



To display an archived REP topology, click the Archived Topology tab and then select the segment ID.

CIP Status

In Device Manager, you can monitor Common Industrial Protocol (CIP) status. CIP is an application layer messaging protocol that is used by various industrial automation and control devices to communicate as part of a control system. CIP is the application layer for the EtherNet/IP network. Stratix switches contain an EtherNet/IP server that enables the switch to be part of the industrial automation and control system for basic management and monitoring.

The CIP Status window displays information about CIP status (Overview field) and statistics (Request Details field) for the following:

- When the switch was last powered on or restarted
- When the counters were last reset

To troubleshoot an issue, reset the CIP counters, and see if the counters show that the issue still exists.

IMPORTANT Except for Active Multicast Groups, all other categories are related to the CIP server in the switch. The categories pertain to CIP traffic directed to the switch as a CIP target device. The categories do not refer to CIP (EtherNet/IP) traffic that flows through the switch among these devices:

- Various CIP controllers
- HMI devices
- Configuration tools
- Other CIP target devices, such as drives, I/O modules, motor starters, sensors, and valves

From the Monitor menu, choose CIP Status.

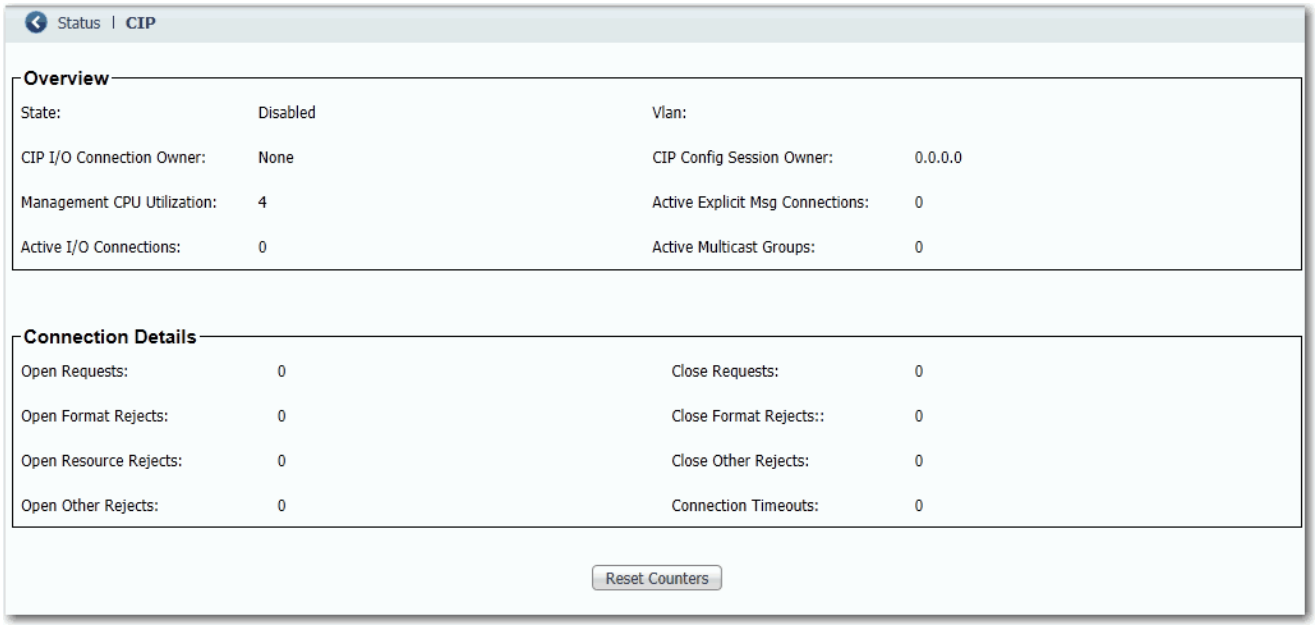


Table 113 - CIP Status Fields

Field	Description
Overview	
State	The state of the CIP connection (Enabled or Disabled).
Vlan	The VLAN ID.
CIP I/O Connection Owner	The IP address of the device to and from which application-specific I/O output data is sent and received.
CIP Config Session Owner	The IP address of the device controlling the CIP configuration session.
Management CPU Utilization (%)	Percentage of the Management CPU used for management functions. Switch functions have dedicated ASICs. Management functions do not impact the ASICs.
Active Explicit Msg Connections	The number of active, explicit messaging connections to the switch as a target.
Active I/O Connections	The number of active I/O connections with the switch as a target.
Active Multicast Groups	The number of multicast groups, including CIP multicast groups that flow through the switch.
Connection Details	
Open Requests	The number of Forward Open requests received by the switch to establish a connection with the switch.
Close Requests	The number of Forward Close requests received by the switch after a connection was successfully established with the switch.
Open Format Rejects	The number of Forward Open requests directed to the switch that failed because the request is not in the proper format.
Close Format Rejects	The number of Forward Close requests directed to the switch that failed because the request is not in the proper format.
Open Resource Rejects	The number of Forward Open requests that failed to establish a new connection for reasons such as insufficient memory.
Close Other Rejects	The number of Forward Close requests that failed for reasons such as incompatible electronic keying.
Open Other Rejects	The number of Forward Open requests that failed for reasons such as incompatible electronic keying.
Connection Timeouts	The number of CIP connections that timed out due to inactivity.

DHCP Clients

In Device Manager, you can view information about devices connected to a switch with DHCP snooping enabled. These devices are known as DHCP clients. The DHCP snooping feature dynamically builds and maintains entries in the DHCP Clients table shown below. For example, the feature removes an entry once its leased IP address expires.

IMPORTANT Information in the DHCP Clients table does not include DHCP devices in a device-level ring. For information about DHCP devices in a ring, see DLR Status on page 406.

The table contains an entry for each device that meets this criteria:

- The device received its IP address from the switch via DHCP, and the IP address lease is active.
- A VLAN is assigned to the DHCP client port that connects to the switch, and DHCP snooping is enabled for that VLAN.

From the Monitor menu, choose DHCP Clients.

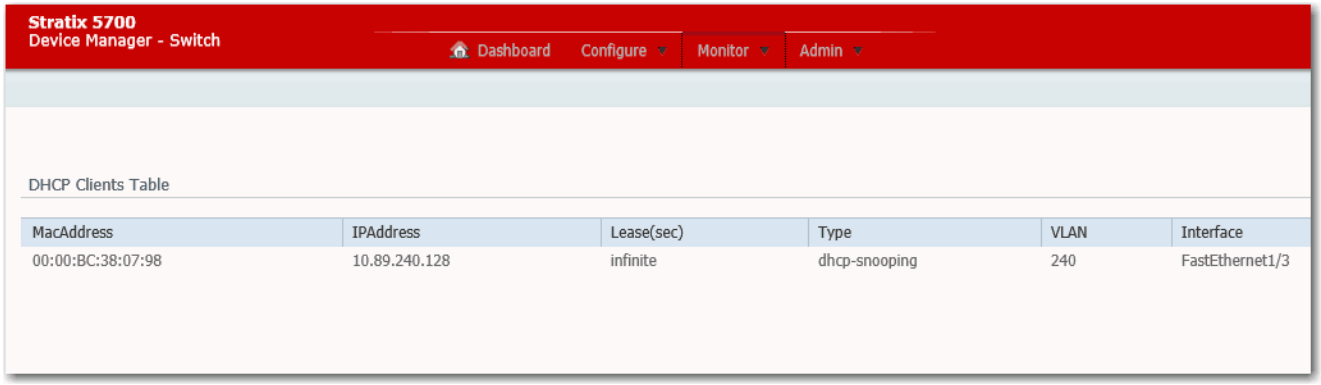


Table 114 - DHCP Clients Table Fields

Field	Description
MAC Address	The MAC address of the DHCP client.
IP Address	The IP address the switch has assigned to the DHCP client.
Lease (sec)	The IP address lease time in seconds.
Type	Whether the IP address of the DHCP client was dynamically assigned from a pool of IP addresses or a statically configured to one or more specific IP addresses.
VLAN	The VLAN on which the DHCP address was assigned.
Interface	The port that connects to the DHCP client.

DLR Status

You can monitor device-level ring (DLR) status in both Device Manager and the Logix Designer application.

Configuration parameters appear for the number of available rings:

- Stratix 5700 and ArmorStratix™ 5700 switches show one ring.
- Stratix 5400 switches show three rings.

For more information about DLR troubleshooting, see Troubleshoot EtherNet/IP Networks, publication ENET-AT003.

Monitor DLR Status via Device Manager

From the Monitor menu, choose DLR:

- The Overview tab shows the status and parameters that are configured for the switch, redundant gateway, ring DHCP server, and the active ring supervisor.

  You can also clear these faults:

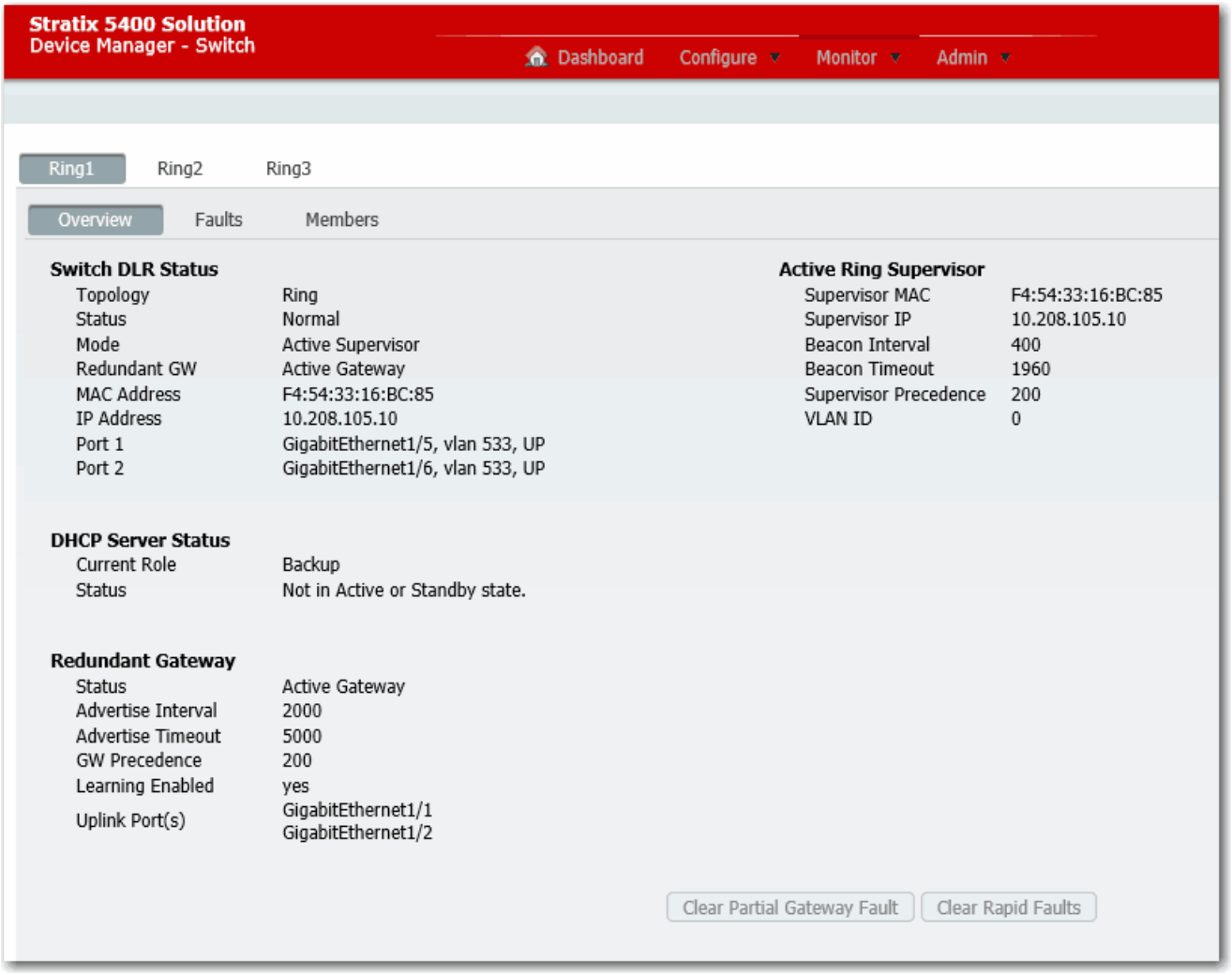
  – Partial gateway faults that can occur when traffic is lost in only one direction. The active ring supervisor detects a partial fault by monitoring the loss of beacon frames on a port.

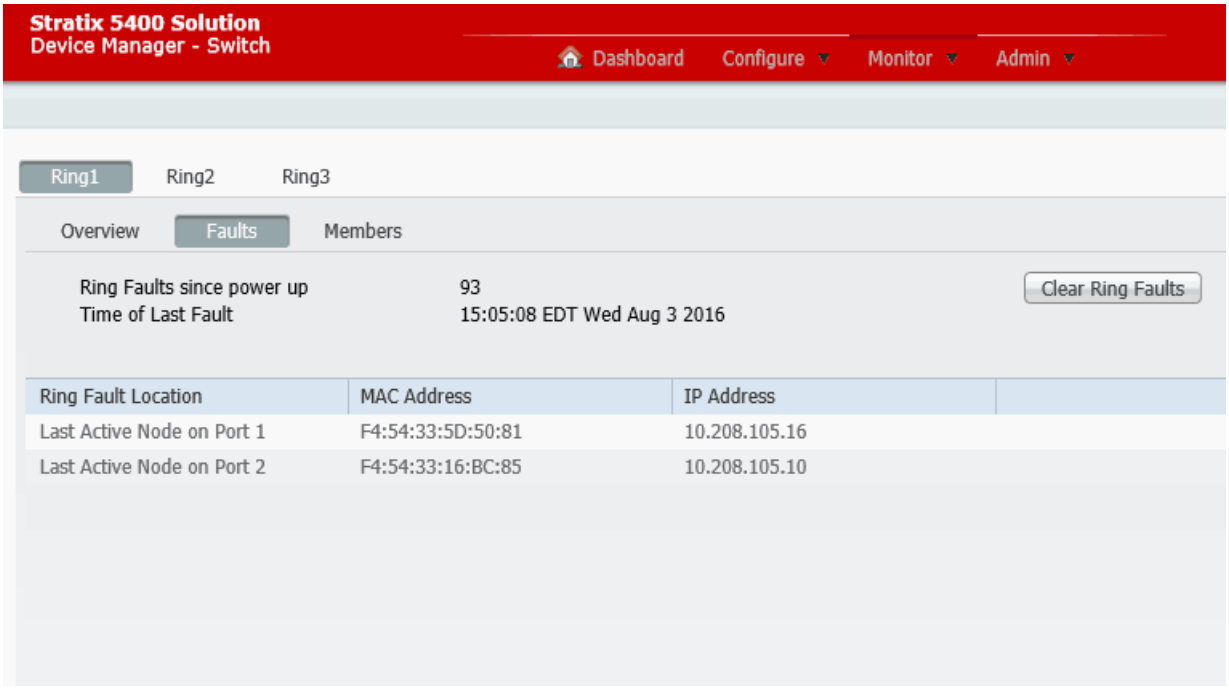
  – Rapid faults that can occur after five intentional disconnections and reconnections of a node from the network within 30 seconds.

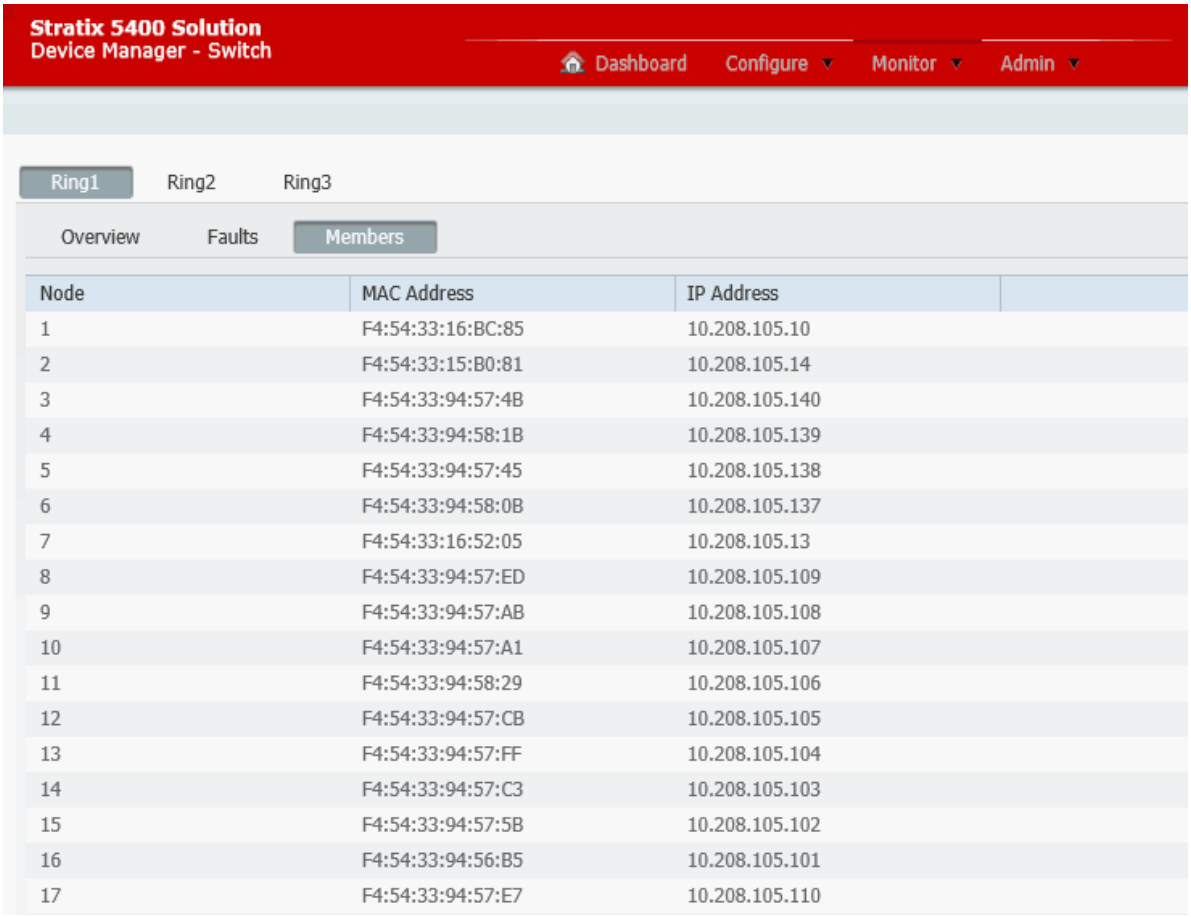
  When the active ring supervisor detects either type of fault, it blocks traffic on the port, which results in network segmentation. To resolve this condition, you must manually clear the faults.

- The Ring Faults tab shows the number, time, and location of faults in a ring.

- The Ring Members tab lists the MAC and IP addresses of each device in a ring.


Stratix 5400 Solution
Device Manager - Switch
Dashboard
Configure
Monitor
Admin
Ring1
Ring2
Ring3
Overview
Faults
Members
Switch DLR Status
Topology Ring
Status Normal
Mode Active Supervisor
Redundant GW Active Gateway
MAC Address F4:54:33:16:BC:85
IP Address 10.208.105.10
Port 1 GigabitEthernet1/5, vlan 533, UP
Port 2 GigabitEthernet1/6, vlan 533, UP
Active Ring Supervisor
Supervisor MAC F4:54:33:16:BC:85
Supervisor IP 10.208.105.10
Beacon Interval 400
Beacon Timeout 1960
Supervisor Precedence 200
VLAN ID 0
DHCP Server Status
Current Role Backup
Status Not in Active or Standby state.
Redundant Gateway
Status Active Gateway
Advertise Interval 2000
Advertise Timeout 5000
GW Precedence 200
Learning Enabled yes
Uplink Port(s) GigabitEthernet1/1 GigabitEthernet1/2
Clear Partial Gateway Fault
Clear Rapid Faults


Stratix 5400 Solution
Device Manager - Switch
Dashboard
Configure
Monitor
Admin
Ring1
Ring2
Ring3
Overview
Faults
Members
Ring Faults since power up 93
Time of Last Fault 15:05:08 EDT Wed Aug 3 2016
Clear Ring Faults
Ring Fault Location
MAC Address
IP Address
Last Active Node on Port 1 F4:54:33:5D:50:81 10.208.105.16
Last Active Node on Port 2 F4:54:33:16:BC:85 10.208.105.10



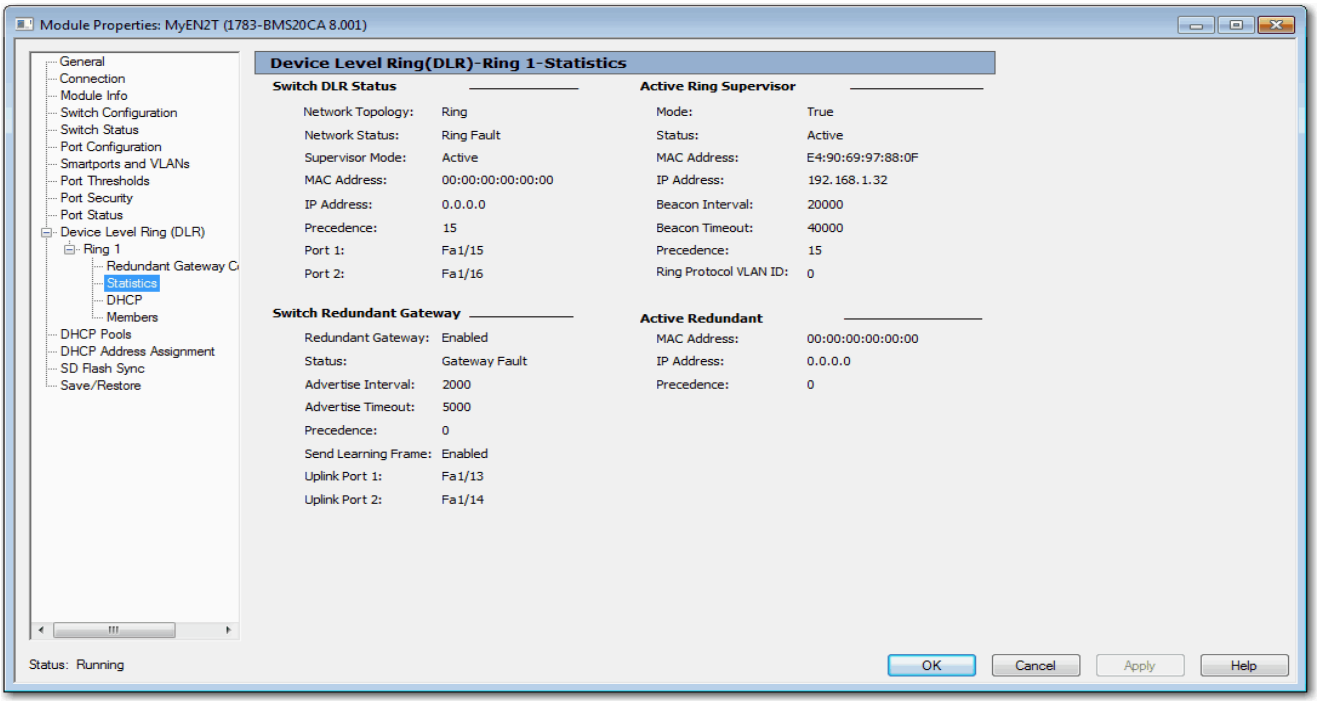
Node	MAC Address	IP Address
1	F4:54:33:16:BC:85	10.208.105.10
2	F4:54:33:15:B0:81	10.208.105.14
3	F4:54:33:94:57:4B	10.208.105.140
4	F4:54:33:94:58:1B	10.208.105.139
5	F4:54:33:94:57:45	10.208.105.138
6	F4:54:33:94:58:0B	10.208.105.137
7	F4:54:33:16:52:05	10.208.105.13
8	F4:54:33:94:57:ED	10.208.105.109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

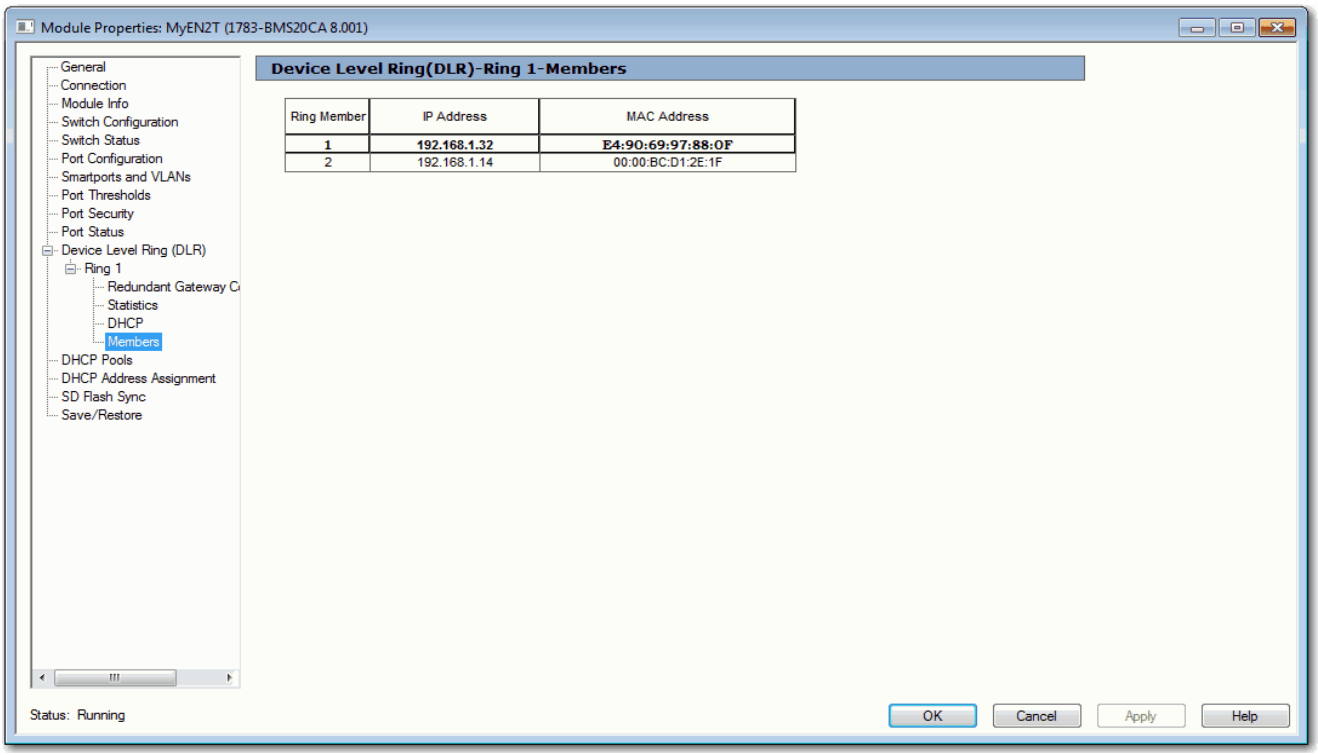
Monitor DLR Status via the Logix Designer Application

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

- To view the status and parameters that are configured for the switch, the redundant gateway, and the active ring supervisor, click Statistics.
- To view the MAC and IP addresses of each device in the ring, click Members.

To obtain network diagnostic information via MSG instructions, see the EtherNet/IP Embedded Switch Technology Application Guide, publication ENET-AP005.


Module Properties: MyEN2T (1783-BMS20CA 8.001)
General
Connection
Module Info
Switch Configuration
Switch Status
Port Configuration
Smartports and VLANs
Port Thresholds
Port Security
Port Status
Device Level Ring (DLR)
Ring 1
Redundant Gateway C
Statistics
DHCP
Members
DHCP Pools
DHCP Address Assignment
SD Flash Sync
Save/Restore
Device Level Ring(DLR)-Ring 1-Statistics
Switch DLR Status
Network Topology: Ring
Network Status: Ring Fault
Supervisor Mode: Active
MAC Address: 00:00:00:00:00:00
IP Address: 0.0.0.0
Precedence: 15
Port 1: Fa1/15
Port 2: Fa1/16
Active Ring Supervisor
Mode: True
Status: Active
MAC Address: E4:90:69:97:88:0F
IP Address: 192.168.1.32
Beacon Interval: 20000
Beacon Timeout: 40000
Precedence: 15
Ring Protocol VLAN ID: 0
Switch Redundant Gateway
Redundant Gateway: Enabled
Status: Gateway Fault
Advertise Interval: 2000
Advertise Timeout: 5000
Precedence: 0
Send Learning Frame: Enabled
Uplink Port 1: Fa1/13
Uplink Port 2: Fa1/14
Active Redundant
MAC Address: 00:00:00:00:00:00
IP Address: 0.0.0.0
Precedence: 0
Status: Running
OK
Cancel
Apply
Help


Module Properties: MyEN2T (1783-BMS20CA 8.001)
General
Connection
Module Info
Switch Configuration
Switch Status
Port Configuration
Smartports and VLANs
Port Thresholds
Port Security
Port Status
Device Level Ring (DLR)
Ring 1
Redundant Gateway C
Statistics
DHCP
Members
DHCP Pools
DHCP Address Assignment
SD Flash Sync
Save/Restore
Device Level Ring(DLR)-Ring 1-Members
Ring Member
IP Address
MAC Address
1
192.168.1.32
E4:90:69:97:88:0F
2
192.168.1.14
00:00:BC:D1:2E:1F
Status: Running
OK
Cancel
Apply
Help

PRP Status

In Device Manager, you can view statistics for configured and learned Virtual DAN (VDAN) and node entries. The VDAN table shows the number of MAC addresses and the number of static (user-configured) nodes for each PRP channel group, as well as table entries. The Node table shows the total number of MAC addresses and MAC addresses of each node type for each PRP channel group, as well as table entries.

For more information about PRP, see the following:

- Parallel Redundancy Protocol (PRP) on page 297.
- Stratix 5400 Display Modes on page 377
- Stratix 5410 Display Modes on page 380

From the Monitor menu, choose PRP.

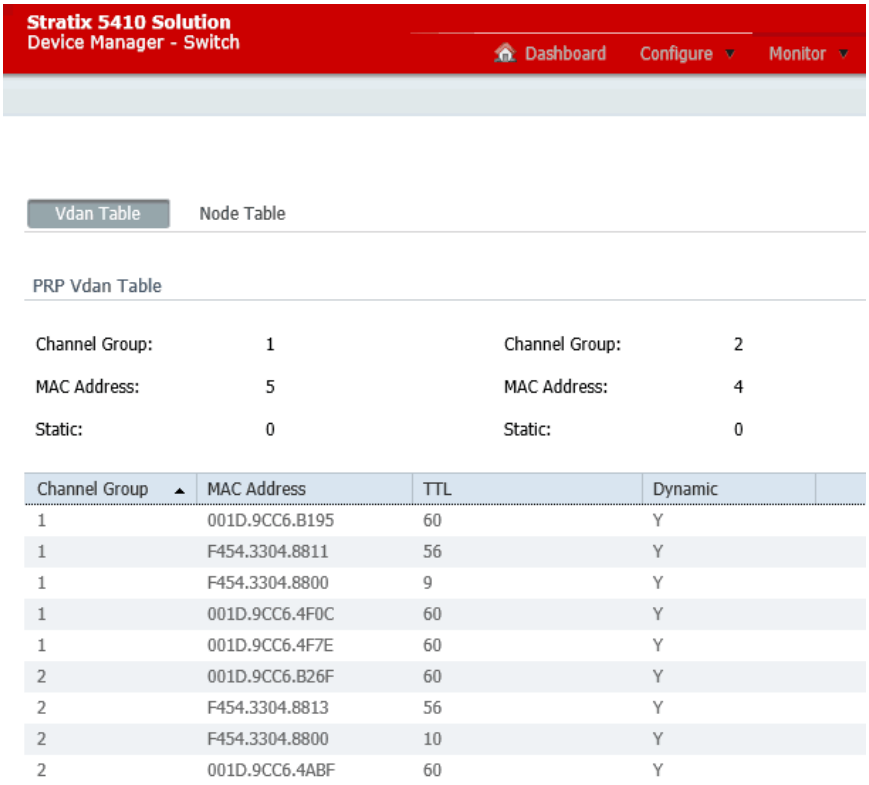


Table 115 - VDAN Table Fields

Field	Description
Channel Group 1, 2	The number of the PRP channel group.
MAC Address	The number of MAC addresses (static and dynamic) for the channel group.
Static	The number of static entries for the channel group.
Grid Fields	
Channel Group	The channel group of the associated entry.
MAC Address	The MAC address of the VDAN.
TTL	The amount of time before the learned MAC address expires.
Dynamic	Whether or not (Y or N) the entry was added as a learned MAC address.

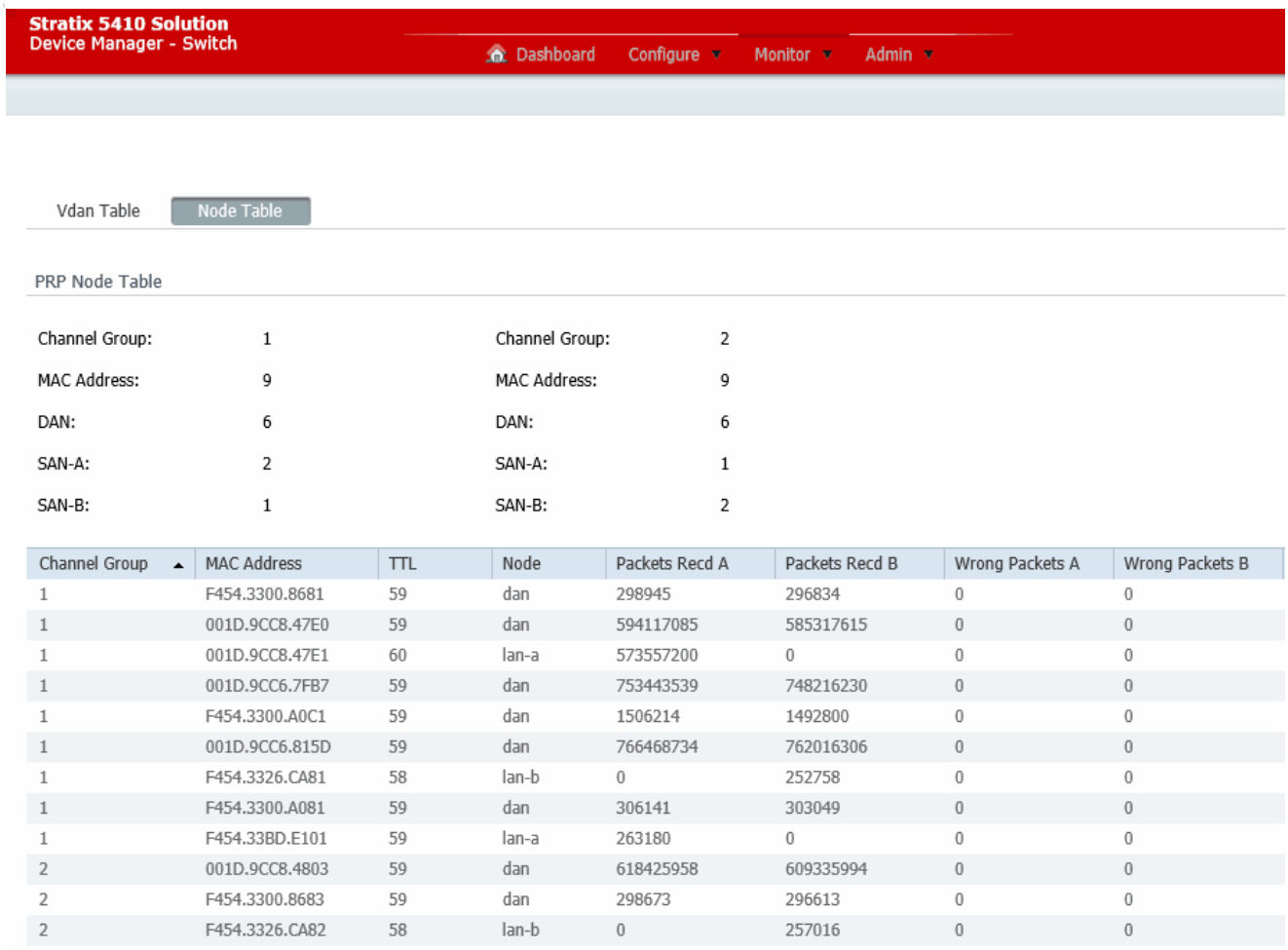


Table 116 - Node Table Fields

Field	Description
Channel Group 1, 2	The number of the PRP channel group.
MAC Address	The number of MAC addresses (static and dynamic) for the channel group.
DAN	The number of dual attached node (DAN) MAC addresses for the channel group.
SAN-A	The number of single attached nodes (SANs) on LAN A.
SAN-B	The number of single attached nodes (SANs) on LAN B.
Grid Fields	
Channel Group	The channel group of the associated entry.
MAC Address	The MAC address of the DAN or SAN.
TTL	The amount of time before the learned MAC address expires.
Node	The type of PRP node: • DAN—Dual attached node • SAN-A—Single attached node on LAN A • SAN-B—Single attached node on LAN B
Packets Recd A	The number of packets received on LAN A.
Packets Recd B	The number of packets received on LAN B.
Wrong Packets A	The number of packets received on LAN A having the wrong LAN A destination.
Wrong Packets B	The number of packets received on LAN B having the wrong LAN B destination.

Port Diagnostics

The Port Diagnostics feature in the Logix Designer application lets you view the status of the link performance:

- View octet and packet counters
- View collisions on the link
- View errors on the link

You can also reset and clear all status counters.

In the navigation pane, click Port Status, and then click the button in the Port Diagnostics column for the corresponding port.

Port	Port Alarm Status	Link Status	Port Fault Status	Threshold Exceeded			Bandwidth Utilization Percent	Port Diagnostics	Cable Diagnostics
				Unicast	Multicast	Broadcast			
Gi1/1	No alarms	Active	No Fault	No	No	No	0	...	...
Gi1/2	No alarms	Inactive	No Fault	No	No	No	0	...	...
Fa1/1	No alarms	Inactive	No Fault	No	No	No	0	...	...
Fa1/2	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/3	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/4	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/5	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/6	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/7	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/8	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...

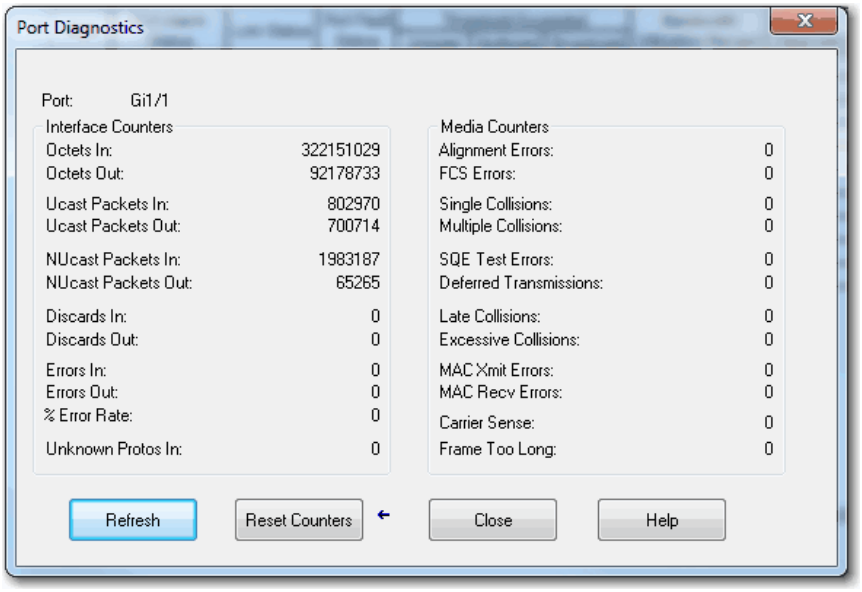


Table 117 - Port Diagnostics Fields

Field	Description
Unit (Stratix 8000/8300 switches)	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	The port that is selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module for Stratix 8000/8300 switches, and the specific port number. **EXAMPLE:** • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Interface Counters	These counters let you view status of octets received and sent, and packets received and sent: • Octets In—The number of octets that are received by the port. • Octets Out—The number of octets that are sent by the port. • Ucast Packets In—The number of unicast packets that are received by the port. • Ucast Packets Out—The number of unicast packets that are sent by the port. • NUcast packets In—The number of multicast packets that are received by the port. • NUcast packets Out—The number of multicast packets that are sent by the port. • Discards In—The number of inbound packets that have been discarded. • Discards Out—The number of outbound packets that have been discarded. • Errors In—The number of inbound packets that contain errors. • Errors Out—The number of outbound packets that contain errors. • Unknown Protos (Protocols) In —The number of inbound packets with unknown protocols.
Media Counters	These counters let you view the number of collisions on a link: Collision counters: • Single—The number of single collisions. • Multiple—The number of multiple collisions. • Late —The number of late collisions. • Excessive—The number of frames for which transmission fails due to excessive collisions. Error counters: • Alignment—The number of frames received that are not an integral number of octets in length. • FCS (Frame Check Sequence)—The number of frames received that do not pass the FCS check. • SQE Test Errors —The number of times that the SQE TEST ERROR message is generated. • Deferred Transmissions—The count of transmissions that are deferred by busy network. • MAC Xmit Errors—The number of frames that failed to transmit due to an internal MAC sublayer transmit error. • MAC Recv Errors—The number of frames that failed to be received due to an internal MAC sublayer receive error. • Carrier Sense—The number of times the carrier sense condition was lost or never asserted when attempting to transmit a frame. • Frame Too Long —The number of frames received that exceed the maximum permitted frame size.

Cable Diagnostics

The Cable Diagnostics feature lets you run a test on each switch port to determine the integrity of the cable that is connected to the RJ45 (copper) ports. The test determines the distance to the break from the switch for each cable with a plus or minus error value individually listed. This feature is not available for fiber ports.

Diagnose Cables via Device Manager

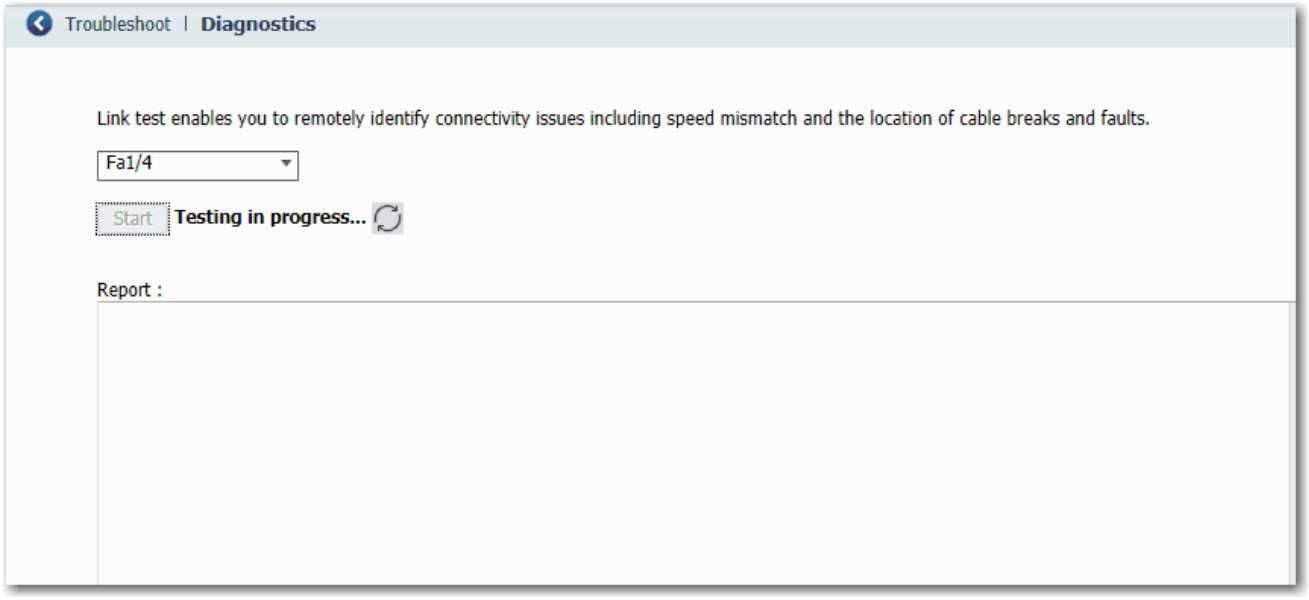
Use the Diagnostics window to run the Broken Wire Detection test, which uses Time Domain Reflectometry (TDR) detection to identify, diagnose, and resolve cable problems. TDR detection is supported on copper Ethernet 10/100 and 10/100/1000 ports. TDR is not supported on small form-factor pluggable (SFP) module ports.

The link test can interrupt traffic between the port and the connected device. Only run the test on a port that has a suspected problem. Before running the link test, use the Front Panel view, the Port Status, and the Port Statistics windows to gather information about a potential problem.

IMPORTANT To run a valid test on gigabit ports, you must first configure the gigabit port as an RJ45 media type, as described in Configure Port Settings on page 51.

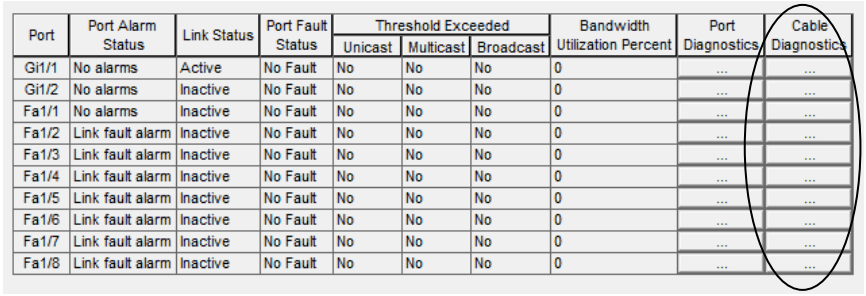
From the Monitor menu, choose Diagnostics.

To run a test, select a port and then click Start.



Diagnose Cables via the Logix Designer Application

In the navigation pane, click Port Status, and then click the button in the Cable Diagnostics column for the corresponding port.



Port	Port Alarm Status	Link Status	Port Fault Status	Threshold Exceeded			Bandwidth Utilization Percent	Port Diagnostics	Cable Diagnostics
				Unicast	Multicast	Broadcast			
Gi1/1	No alarms	Active	No Fault	No	No	No	0	...	...
Gi1/2	No alarms	Inactive	No Fault	No	No	No	0	...	...
Fa1/1	No alarms	Inactive	No Fault	No	No	No	0	...	...
Fa1/2	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/3	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/4	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/5	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/6	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/7	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Fa1/8	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...

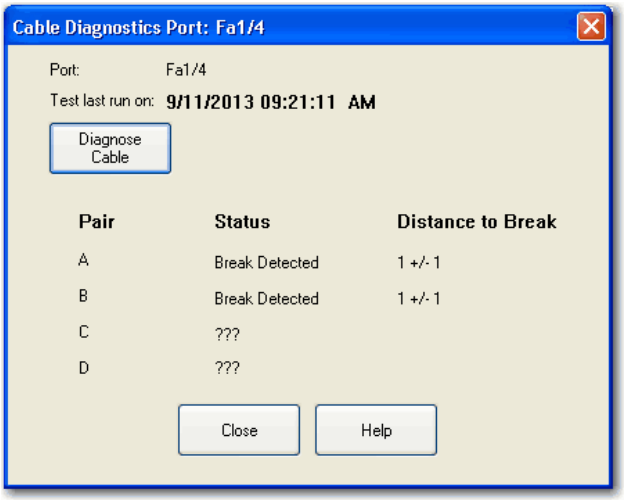


Table 118 - Cable Diagnostics Fields

Field	Description
Port	The port that is selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Test last run on	The time the test was last executed. The date time format is mm/dd/yy hh:mm:ss tt. If the test has never been run, the time and all distance and status information is blank.
Pair	Each pair of cables in the network individually listed. If pair does not exist or test has never beeto indicate run, this field is blank.
Status	Specifies the link state the last time the test was executed. If pair does not exist or test has never run, status is blank. For distance, if the pair is Normal status, 'No Break Detected' is shown. No distance is displayed.
Distance to Break	The distance to the break from the switch for each estimated pair with a plus or minus error value individually listed. A value is displayed only when the status of an existing pair is not Normal. This field is blank if the test was never run before. If a pair does not exist, '???' appears.
Diagnose Cable	Click to run the Diagnose Cable test. A connection interruption warning appears: • If you are sure that you want to continue with the test, click Yes. Be prepared to enter a valid password to run the test. • If you do not want to run the test, click No or close the window. **IMPORTANT:** To run a valid test on gigabit ports, you must first configure the gigabit port as an RJ45 media type in Device Manager, as described in Configure Port Settings on page 51. **IMPORTANT:** This test can interrupt connections to the module and to any other modules connected through this module. Also, the connection between workstation and controller can be interrupted. You must have the correct privilege to run this test.

DHCP Pool Display

In the Logix Designer application, you can view DHCP address pool information for the switch. You can view 0...15 pools. This information is gathered directly from the switch. Each row represents one instance, and instance values cannot be consecutive.

In the navigation pane, click DHCP Pool Display.

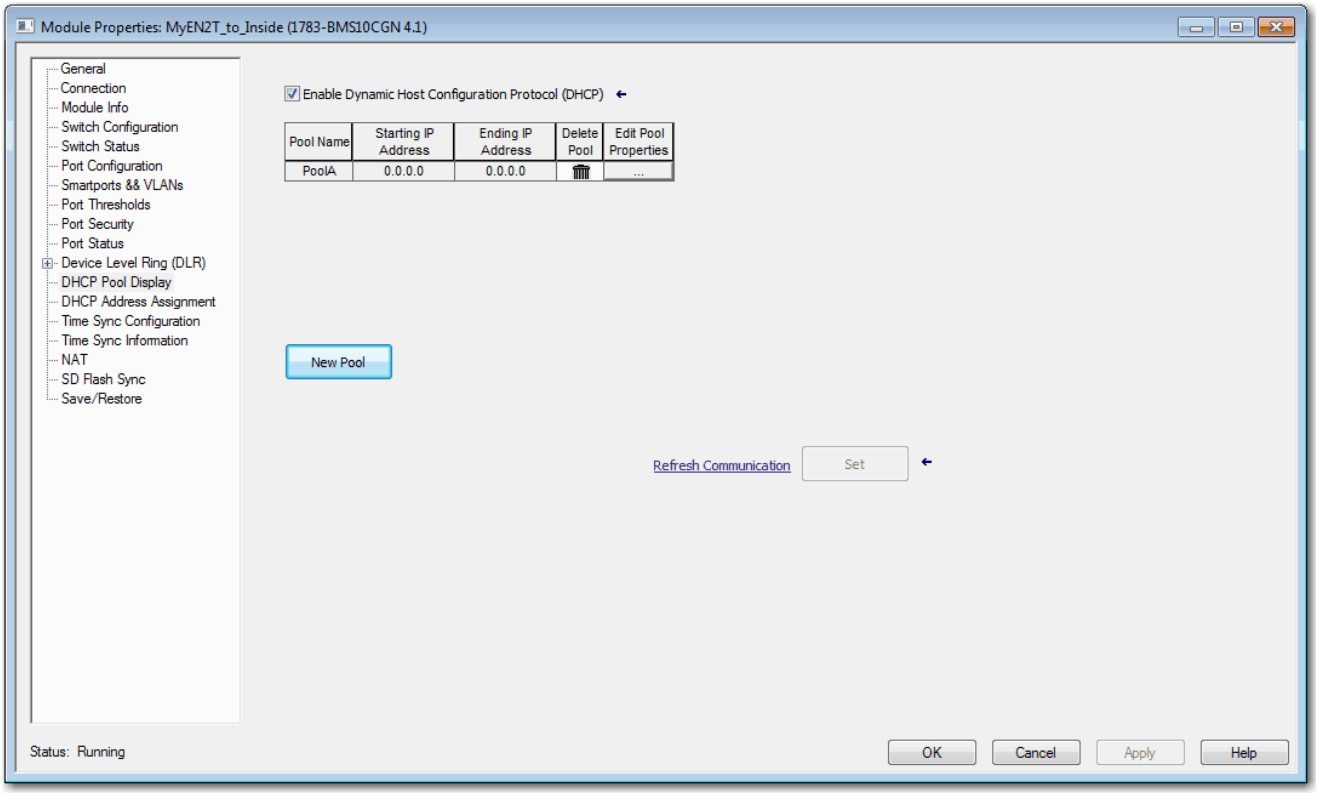


Table 119 - DHCP Pool Display Fields

Field	Description
Enable Dynamic Host Configuration Protocol (DHCP)	Enables or disables pools. If selected, all controls on the grid are set to online and the appropriate values are obtained from the switch and displayed. If cleared, all fields on the view become unavailable. From the keyboard, press Alt - D.
Pool Name	Displays the name of the DHCP IP address pool that is configured on the switch. A DHCP IP address pool is a range (or pool) of available IP addresses that the switch can assign to connected devices. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab.
Starting IP Address	Displays the starting IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers that are separated by periods (for example, 255.255.255.255). Each number can be from 0…255.
Ending IP Address	Displays the ending IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers that are separated by periods (for example, 255.255.255.255). Each number can be from 0…255.
Delete Pool	Click to delete currently selected DHCP pool row. Afterwards, if you click Set, a confirmation dialog box is displayed and all persistent addresses that are associated with the selected DHCP pool row are also deleted. Delete Pool is available only when the switch is online, the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is checked, and when the respective row is populated.
Edit Pool Properties	Click to display the DHCP Pool Definition and Edit dialog box and populate it with values from the instance that corresponds to the current row. The Edit column button is available only when the switch is online, the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is selected, and when the respective row is populated.
New Pool	Click to display the DHCP Pool Definition and Edit dialog box (all fields are blank and the Custom radio button is not selected). Additionally, a new row/instance is added to the grid on the Module Properties dialog box - DHCP Pool Display. From the keyboard, press Alt - N.

Troubleshoot the Switch

Topic	Page
Troubleshoot the Installation	418
Verify Boot Fast	421
Troubleshoot IP Addresses	421
Troubleshoot Device Manager	421
Troubleshoot Switch Performance	422
Access Direct Managed Mode	423
Restart or Reset the Switch	424
Recover the Switch Firmware	426
Reset the Switch to Factory Defaults	426
Troubleshoot a Firmware Update	427
Collect System and Configuration Information for Technical Support	428

This chapter helps you resolve issues that are related to Stratix® switches and perform common functions, such as reset the switch.

For more troubleshooting, see the following:

- Port Diagnostics on page 412
- Cable Diagnostics on page 414
- System Log Messages on page 392

See also Troubleshoot EtherNet/IP Networks, publication ENET-AT003.

Troubleshoot the Installation

The status indicators on the front panel provide troubleshooting information about the switch. They show power-on self-test (POST) failures, port connectivity problems, and overall switch performance. You can also get statistics from the browser interface, the command-line interface (CLI), or a Simple Network Management Protocol (SNMP) workstation.

Switch POST Results

As power is applied to the switch, it begins the POST, a series of tests that runs automatically to help ensure that the switch functions properly. It can take several minutes for the switch to complete POST.

POST starts with status indicator tests that cycle once through the EIP Mod, EIP Net, Setup, Pwr A, and Pwr B status indicators. While POST proceeds, the EIP Mod status indicator blinks green, and all other status indicators remain off.

If POST completes successfully, the Setup status indicator changes to solid green, and the other status indicators display their normal operating status. If the switch fails POST, the Setup status indicator turns red.



ATTENTION: POST failures are fatal to the switch. Contact your Rockwell Automation technical support representative if your switch does not pass POST.

POST Results with a Terminal

If you have a terminal that is connected to the console port, you can also view POST status and test results on the terminal. If the terminal displays unclear characters, try resetting the terminal-emulation software to 9600 bits per second.

Bad or Damaged Cable

Always make sure that the cable does not have marginal damage or failure. Even if a cable can connect at the physical layer, subtle damage to the wiring or connectors can corrupt packets.

This situation is likely when the port has many packet errors or the port constantly loses and regains the link. To troubleshoot, try the following:

- Swap the copper or fiber-optic cable with a known, undamaged cable.
- Look for broken, bent, or missing pins on cable connectors.
- Rule out any bad patch panel connections or media convertors between the source and destination.

  If possible, bypass the patch panel, or eliminate faulty media convertors (fiber-optic-to-copper).
- Try the cable in another port or interface to determine if the problem follows the cable.

Ethernet and Fiber Cables

Make sure that you have the correct cable type for the connection:

- Use Category 3 copper cable for 10-Mb/s UTP connections.
- You can use Category 5, 5e, or 6 UTP or STP cable for 10/100-Mbps connections.
- For 1000 Mbps (1 gigabit per second) connections, use Category 5e or Category 6 UTP or STP cable.
- For fiber-optic connectors, verify that you have the correct cable for the distance and the port type.
- Make sure that the connected device ports both match and use the same type of encoding, optical frequency, and fiber type.

Link Status

Verify that both sides have a network link. A broken wire or one shut down port can cause one side to show a link, but not the other side. A Link status indicator does not indicate that the cable is fully functional. The cable can encounter physical stress that causes it to function at a marginal level. If the Link status indicator for the port is not lit, do the following:

- Connect the cable from the switch to a known good device.
- Make sure that both ends of the cable are connected to the correct ports.
- Verify that both devices have power.
- Verify that you are using the correct cable type.
- Rule out loose connections. Sometimes a cable appears to be seated, but is not. Disconnect the cable, and then reconnect it.

Transceiver Issues

Use only Rockwell Automation SFP modules on the switch. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding identifies and validates that the module meets the requirements for the switch.

Check these items:

- Verify that the SFP module is valid and functional. Exchange a suspect module with a known good module. Verify that the module is supported on this platform.
- Use the CLI show interfaces command or the CLI show int status command to verify the error-disabled or shutdown status of the port or module. Re-enable the port if needed.
- Make sure that all fiber connections are properly cleaned and securely connected.

Port and Interface Settings

A cause of port connectivity failure can be a disabled port. Verify that the port or interface is not disabled or powered down for some reason. If a port or interface is manually shut down on one side of the link or the other side, the link does not come up until you re-enable the port. Use the CLI show interfaces privileged EXEC command to verify the port or interface error-disabled, disabled, or shutdown status on both sides of the connection. If needed, re-enable the port or the interface.

Verify Boot Fast

Boot Fast failures are potentially fatal to the switch. Contact your Rockwell Automation representative if your switch does not successfully complete Boot Fast. You can disable Boot Fast and run a power-on self-test (POST) by using the CLI.

Troubleshoot IP Addresses

The following table includes basic troubleshooting for issues that are related to the switch IP address.

Issue	Resolution
IP address is not received from the DHCP server	If the switch does not receive an IP address from an upstream device operating as a DHCP server, make sure that the device is operating as a DHCP server. Repeat Express Setup.
Switch has wrong IP address	If the switch is installed in your network but you cannot access the switch because it has the wrong IP address, assign a new switch IP address. Refer to Access Direct Managed Mode on page 423 to assign the IP address, and then update the switch IP address on the Express Setup window.

Troubleshoot Device Manager

The following table includes basic troubleshooting for issues that are related to Device Manager.

Issue	Resolution
Device Manager does not appear	If you cannot display Device Manager from your computer, make sure that you entered the correct switch IP address in the browser. If you entered the correct switch IP address in the browser, make sure that the switch and your computer are in the same network or subnetwork: • For example, if your switch IP address is 172.20.20.85 and your computer address is 172.20.20.84, both devices are in the same network. • For example, if your switch IP address is 172.20.20.85 and your computer IP address is 10.0.0.2, the devices are in different networks and cannot directly communicate without a router. You must either change the switch IP address or change the computer IP address. • If the issue persists, follow the procedure in Access Direct Managed Mode on page 423, and then update the switch network settings on the Express Setup window. • If the issue still persists, follow the procedure in the Recover the Switch Firmware on page 426.
Device Manager does not operate properly	Follow the procedure in Access Direct Managed Mode on page 423, and then update the switch network settings on the Express Setup window. If the issue persists, follow the procedure in Recover the Switch Firmware on page 426.
Device Manager is not accessible through the network	If you cannot access Device Manager remotely from a web browser, follow the procedure in the Access Direct Managed Mode on page 423.

Troubleshoot Switch Performance

The following table includes basic troubleshooting for issues that are related to switch performance.

Issue	Resolution
Speed, duplex, and autonegotiation	Port statistics that show a large amount of alignment errors, frame check sequence (FCS), or late-collisions errors can indicate a speed or duplex mismatch. Common speed and duplex issues occur when duplex settings are mismatched between two switches, between a switch and a router, or between the switch and a computer. These issues can occur from manually setting the speed and duplex or from autonegotiation issues between the two devices. A mismatch occurs under these circumstances: • A manually set speed or duplex parameter differs from the manually set speed or duplex parameter on the connected port. • A port is set to autonegotiate, and the connected port is set to full-duplex with no autonegotiation. To maximize switch performance and be sure of a link, follow one of these guidelines when changing the settings for duplex and speed: • Let both ports autonegotiate both speed and duplex. • Manually set the same speed and duplex parameters for the ports on both ends of the connection to the same values. • If a remote device does not autonegotiate, configure the duplex settings on the two ports to the same values. The speed parameter can adjust itself even if the connected port does not autonegotiate.
Autonegotiation and network interface cards (NICs)	Issues sometimes occur between the switch and third-party network interface cards (NICs). By default, the switch ports and interfaces are set to autonegotiate. It is common for devices like laptops or other devices to be set to autonegotiate as well, yet sometimes autonegotiation issues occur. To troubleshoot autonegotiation issues, try manually setting both sides of the connection. If the issues persist, try upgrading the NIC driver to the latest firmware or software.
Cable distance	If the port statistics show excessive FCS, late-collision, or alignment errors, verify that the cable distance from the switch to the connected device meets the recommended guidelines.

Access Direct Managed Mode

You can display Device Manager and manage the switch through a physical connection between one of the switch ports and your computer or laptop. This type of management connection is referred to as the Direct Managed mode. This mode is typically used to connect to the switch by using Device Manager when the IP address of the switch is unknown.

Before you can access Direct Managed mode, you must make sure of the following:

- You must have physical access to the switch.
- Make sure that at least one switch port is enabled and is not connected to a device.

To access the Direct Managed mode, follow these steps.

1. Press the Express Setup button until the Setup status indicator blinks green and the status indicator of an available switch downlink port blinks green.

   The port with a flashing green status indicator is designated as the Direct Managed mode port:

   - If all downlink ports are not connected to devices or if multiple downlink ports are connected to devices, the first available downlink port becomes the Direct Managed mode port.
   - If only one downlink port is connected to a device, that port is selected as the Direct Managed mode port.

   If there is no available switch downlink port to which to connect your computer or laptop, disconnect a device from one of the switch downlink ports. Press the Setup button until the Setup and port status indicators flash green.
2. To connect your computer to the switch port with the flashing status indicator, use a Category 5 Ethernet cable.
3. Wait until the port status indicators on the switch and your computer or laptop are solid green.

   The solid green indicators mean a successful connection between the two devices.
4. Start a web browser on your computer.

   A password prompt followed by the Device Manager window appears.

   If the Device Manager window does not appear, make sure that any pop-up blockers or proxy settings in your browser are disabled. Also, make sure that any wireless clients on your computer or laptop are disabled.

   If the Device Manager window still does not appear, enter a URL in your browser, such as http://www.rockwellautomation.com. The browser redirects to Device Manager.

Restart or Reset the Switch

If you cannot solve an issue by reconfiguring a feature, you can restart or reset the switch to solve the issue. If the issue exists after you reset the switch to its default settings, it is unlikely that the switch is causing the issue.

Option	Description
Restart	This option restarts the switch without turning off power. The switch retains its saved configuration settings during the restart process. However, Device Manager is unavailable during the process. When the process completes, the switch displays Device Manager.
Reset the switch to factory defaults	This option resets the switch, deletes the current configuration settings, returns to the factory default settings, and then restarts the switch. **ATTENTION:** When reset, the switch deletes all customized switch settings, including the IP address, and returns the switch to the factory default settings. The same software image is retained. You must reconfigure the basic switch settings with Express Setup.

IMPORTANT Connectivity of your devices to the network is interrupted when you restart or reset the switch.

Restart the Switch from Device Manager

From the Admin menu, choose Restart/Reset.

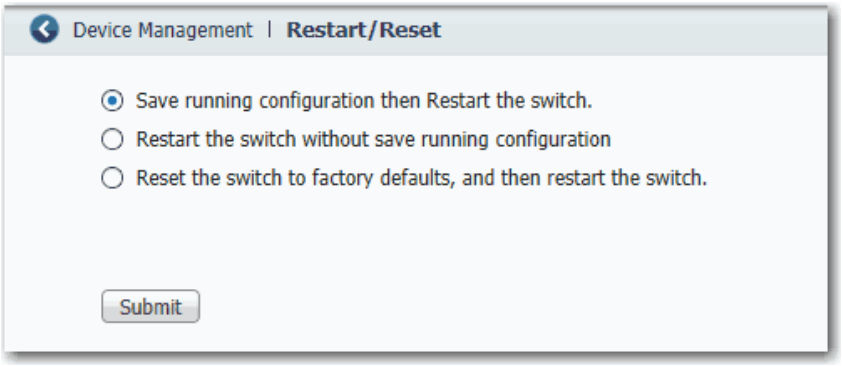


Table 120 - Restart/Reset Fields

Field	Description
Save running configuration and then restart the switch	Saves any changes in the running configuration before the switch restarts.
Restart the switch without saving running configuration	Restarts the switch with its previously saved configuration settings.
Reset the switch to factory defaults, and then restart the switch	Resets the device to the factory default settings, which deletes the current configuration settings, and then restarts the device. You lose connectivity with the device and must run Express Setup to reconfigure the device.

Restart the Switch from the Logix Designer Application

IMPORTANT All connections to or through the switch are closed when you reset a module. Connection loss can result in loss of control.

From Module Properties dialog box within the Studio 5000 Logix Designer® application, do the following.

1. In the navigation pane, click Module Info.
2. To perform a switch reset (power cycle) with the current configuration file, click Reset Module.

   A password prompt appears.
3. Enter your password and click Enter.

Reset the Switch to Factory Defaults



ATTENTION: Resetting the switch deletes all customized switch settings, including the IP address, and returns the switch to its factory default. The same software image is retained. To manage the switch or display Device Manager, you must reconfigure switch settings, as described in Chapter 2, and use the new IP address.

IMPORTANT Restarting the switch interrupts connectivity of your devices to the network.

From Device Manager, do the following.

1. From the Admin menu, choose Restart/Reset.
2. Click Reset the Switch.

   This option resets the switch, deletes the current configuration settings, returns to the factory default settings, and then restarts the switch.

   If you do not know the switch IP address, follow the procedure in the Access Direct Managed Mode section on page 423 to access Direct Managed mode.

Recover the Switch Firmware

Before you can recover switch firmware, make sure of the following:

- You have physical access to the switch.
- At least one switch port is enabled and is not connected to a device.

You can recover the switch firmware if needed, such as in these scenarios:

- The image is corrupted, as indicated by continuous attempts by the switch to restart.
- You deleted the image due to a failed firmware update.
- You forget the switch password.

When you recover switch firmware, all configuration settings are deleted, and the switch returns to its factory default settings.

Reset the Switch to Factory Defaults

This procedure resets the switch to its original factory settings. Any configuration changes that you have made are lost.

Reset a Stratix 5400, Stratix 5410, Stratix 5700, or ArmorStratix 5700 Switch

1. Make sure that the switch is fully powered up.

   IMPORTANT Do not perform this procedure while the switch is powering up.

2. Press and hold the Express Setup button for 10 seconds until the EIP Mod status indicator turns red, and then immediately release the Express Setup button.

   IMPORTANT If you hold the Express Setup button too long (approximately 20 seconds), the EIP Net and EIP Mod both turn red and the switch begins the power-on sequence. If this scenario occurs, you must power off and restart the switch to return to the factory default settings.

Reset a Stratix 8000/8300 Switch

1. Remove power from the switch.
2. Reapply power to the switch.
3. While the switch is powering up, press and hold the Express Setup button.
4. When the EIP Mod, EIP Net and Setup status indictors turn red, release the Express Setup button.

Troubleshoot a Firmware Update

If you attempted to update the switch firmware but received a message that the update failed, make sure that you still have access to the switch. If you still have switch access, follow these steps.

1. Make sure that you downloaded the correct .tar file from http://www.rockwellautomation.com.
2. If you downloaded the correct .tar file, refresh the browser session for Device Manager to verify connectivity between the switch and your computer or network drive.
   - If you have connectivity to the switch and Device Manager, retry the update.
   - If you do not have connectivity to the switch and Device Manager, refer to Recover the Switch Firmware on page 426.

Collect System and Configuration Information for Technical Support

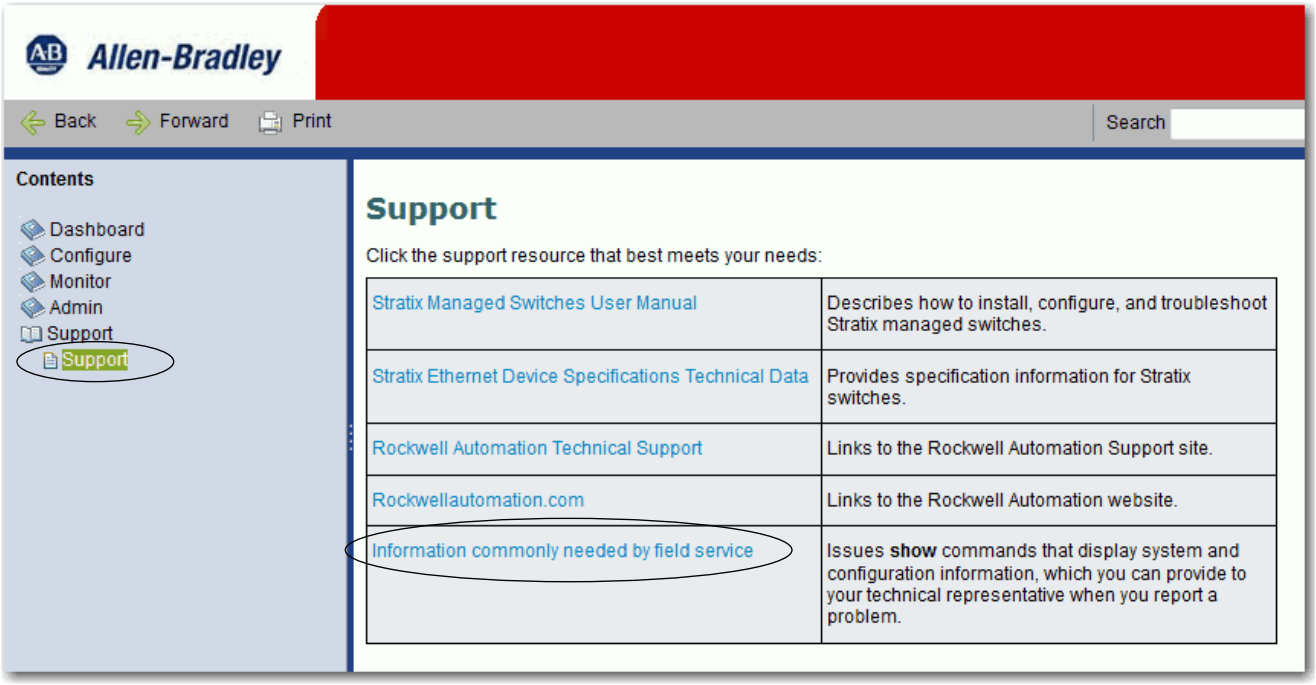
The Device Manager online Help provides a link that you can use to collect system and configuration information about the switch. When you click the link, the switch runs the **show tech-support** command via the command-line interface (CLI). This command generates information about the switch that can be useful to Technical Support when you report a problem.

To collect system and configuration information for Technical Support, follow these steps.

1. Click the Help icon in the upper-right corner of the Device Manager window.



2. In the Contents pane, click Support, and then click Information commonly needed by field service.



The switch runs the **show-tech support** command and displays system and configuration information in your browser window.

Data Types

Topic	Page
Stratix 5400 Data Types	430
Stratix 5410 Data Types	449
Stratix 5700 and ArmorStratix 5700 Data Types	454
Stratix 8000 and 8300 Data Types	481

In the Studio 5000 Logix Designer® application, predefined tags for Input and Output data types have a structure that corresponds to the switch selected when it was added to the I/O tree. Its members are named in accordance with the port names.

You can disable a switch port by setting the corresponding bit in the output tag. The output bits are applied every time that the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied.

The port is enabled if the corresponding output bit is 0. If you enable or disable a port by using Device Manager or the CLI, the port setting can be overridden by the output bits the next time they are applied. The output bits always take precedence, regardless of whether Device Manager or the CLI is used to enable or disable the port.

Stratix 5400 Data Types

The following tables list module-defined data types for Stratix® 5400 switches. The tables include information for input (I) and output (O).

8-port Switches

Catalog number 1783-HMS4C4CGN

Table 121 - Input Data Types (8-port switches)

AB:STRATIX_5400_8PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	

Table 121 - Input Data Types (8-port switches) (Continued)

AB:STRATIX_5400_8PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MinorAlarmRelay	BOOL	Decimal	AlarmRelay:1
MulticastGroupActive	DINT	Binary	

Table 122 - Output Data Types (8-port switches)

AB:STRATIX_5400_8PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8

12-port Switches

Catalog numbers 1783-HMS8T4CGN,1783-HMS8S4CGN, 1783-HMS4T4E4CGN

Table 123 - Input Data Types (12-port switches)

AB:STRATIX_5400_12PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6

Table 123 - Input Data Types (12-port switches) (Continued)

AB:STRATIX_5400_12PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MinorAlarmRelay	BOOL	Decimal	AlarmRelay:1
MulticastGroupActive	DINT	Binary	

Table 124 - Output Data Type (12-port switches)

AB:STRATIX_5400_12PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9

Table 124 - Output Data Type (12-port switches) (Continued)

AB:STRATIX_5400_12PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12

12-port Gigabit Switches

Catalog numbers 1783-HMS8TG4CGN, 1783-HMS8SG4CGN, 1783-HMS4EG8CGN, 1783-HMS8TG4CGR, 1783-HMS8SG4CGR, 1783-HMS4EG8CGR

Table 125 - Input Data Types (12-port Gb switches)

AB:STRATIX_5400_12PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_5Connected	BOOL	Decimal	LinkStatus:5
PortGi1_6Connected	BOOL	Decimal	LinkStatus:6
PortGi1_7Connected	BOOL	Decimal	LinkStatus:7
PortGi1_8Connected	BOOL	Decimal	LinkStatus:8
PortGi1_9Connected	BOOL	Decimal	LinkStatus:9
PortGi1_10Connected	BOOL	Decimal	LinkStatus:10
PortGi1_11Connected	BOOL	Decimal	LinkStatus:11
PortGi1_12Connected	BOOL	Decimal	LinkStatus:12
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortGi1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortGi1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortGi1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10

Table 125 - Input Data Types (12-port Gb switches) (Continued)

AB:STRATIX_5400_12PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortGi1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortGi1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortGi1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortGi1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortGi1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortGi1_5Utilization	SINT	Decimal	
PortGi1_6Utilization	SINT	Decimal	
PortGi1_7Utilization	SINT	Decimal	
PortGi1_8Utilization	SINT	Decimal	
PortGi1_9Utilization	SINT	Decimal	
PortGi1_10Utilization	SINT	Decimal	
PortGi1_11Utilization	SINT	Decimal	
PortGi1_12Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MinorAlarmRelay	BOOL	Decimal	AlarmRelay:1
MulticastGroupActive	DINT	Binary	

Table 126 - Output Data Type (12-port Gb switches)

AB:STRATIX_5400_12PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortGi1_5Disable	BOOL	Decimal	DisablePort:5
PortGi1_6Disable	BOOL	Decimal	DisablePort:6
PortGi1_7Disable	BOOL	Decimal	DisablePort:7
PortGi1_8Disable	BOOL	Decimal	DisablePort:8
PortGi1_9Disable	BOOL	Decimal	DisablePort:9
PortGi1_10Disable	BOOL	Decimal	DisablePort:10
PortGi1_11Disable	BOOL	Decimal	DisablePort:11
PortGi1_12Disable	BOOL	Decimal	DisablePort:12

16-port Switches

Catalog number 1783-HMS4S8E4CGN

Table 127 - Input Data Type (16-port switches)

AB:STRATIX_5400_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14

Table 127 - Input Data Type (16-port switches) (Continued)

AB:STRATIX_5400_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	

Table 127 - Input Data Type (16-port switches) (Continued)

AB:STRATIX_5400_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MinorAlarmRelay	BOOL	Decimal	AlarmRelay:1
MulticastGroupActive	DINT	Binary	

Table 128 - Output Data Type (16-port switches)

AB:STRATIX_5400_16PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13

Table 128 - Output Data Type (16-port switches) (Continued)

AB:STRATIX_5400_16PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16

16-port Gigabit Switches

Catalog number 1783-HMS4SG8EG4CGN, 1783-HMS4SG8EG4CGR

Table 129 - Input Data Type (16-port Gb switches)

AB:STRATIX_5400_16PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_5Connected	BOOL	Decimal	LinkStatus:5
PortGi1_6Connected	BOOL	Decimal	LinkStatus:6
PortGi1_7Connected	BOOL	Decimal	LinkStatus:7
PortGi1_8Connected	BOOL	Decimal	LinkStatus:8
PortGi1_9Connected	BOOL	Decimal	LinkStatus:9
PortGi1_10Connected	BOOL	Decimal	LinkStatus:10
PortGi1_11Connected	BOOL	Decimal	LinkStatus:11
PortGi1_12Connected	BOOL	Decimal	LinkStatus:12
PortGi1_13Connected	BOOL	Decimal	LinkStatus:13
PortGi1_14Connected	BOOL	Decimal	LinkStatus:14
PortGi1_15Connected	BOOL	Decimal	LinkStatus:15
PortGi1_16Connected	BOOL	Decimal	LinkStatus:16
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortGi1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7

Table 129 - Input Data Type (16-port Gb switches) (Continued)

AB:STRATIX_5400_16PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortGi1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortGi1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortGi1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortGi1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortGi1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortGi1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortGi1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortGi1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortGi1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortGi1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortGi1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortGi1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortGi1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortGi1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortGi1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortGi1_5Utilization	SINT	Decimal	
PortGi1_6Utilization	SINT	Decimal	
PortGi1_7Utilization	SINT	Decimal	
PortGi1_8Utilization	SINT	Decimal	
PortGi1_9Utilization	SINT	Decimal	
PortGi1_10Utilization	SINT	Decimal	
PortGi1_11Utilization	SINT	Decimal	

Table 129 - Input Data Type (16-port Gb switches) (Continued)

AB:STRATIX_5400_16PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_12Utilization	SINT	Decimal	
PortGi1_13Utilization	SINT	Decimal	
PortGi1_14Utilization	SINT	Decimal	
PortGi1_15Utilization	SINT	Decimal	
PortGi1_16Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MinorAlarmRelay	BOOL	Decimal	AlarmRelay:1
MulticastGroupActive	DINT	Binary	

Table 130 - Output Data Type (16-port Gb switches)

AB:STRATIX_5400_16PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortGi1_5Disable	BOOL	Decimal	DisablePort:5
PortGi1_6Disable	BOOL	Decimal	DisablePort:6
PortGi1_7Disable	BOOL	Decimal	DisablePort:7
PortGi1_8Disable	BOOL	Decimal	DisablePort:8
PortGi1_9Disable	BOOL	Decimal	DisablePort:9
PortGi1_10Disable	BOOL	Decimal	DisablePort:10
PortGi1_11Disable	BOOL	Decimal	DisablePort:11
PortGi1_12Disable	BOOL	Decimal	DisablePort:12
PortGi1_13Disable	BOOL	Decimal	DisablePort:13
PortGi1_14Disable	BOOL	Decimal	DisablePort:14
PortGi1_15Disable	BOOL	Decimal	DisablePort:15
PortGi1_16Disable	BOOL	Decimal	DisablePort:16

20-port Switches

Catalog number 1783-HMS16T4CGN

Table 131 - Input Data Type (20-port switches)

AB:STRATIX_5400_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortFa1_19Connected	BOOL	Decimal	LinkStatus:19
PortFa1_20Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12

Table 131 - Input Data Type (20-port switches) (Continued)

AB:STRATIX_5400_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortFa1_19UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortFa1_20UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortFa1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortFa1_20Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	

Table 131 - Input Data Type (20-port switches) (Continued)

AB:STRATIX_5400_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortFa1_19Utilization	SINT	Decimal	
PortFa1_20Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MinorAlarmRelay	BOOL	Decimal	AlarmRelay:1
MulticastGroupActive	DINT	Binary	

Table 132 - Output Data Type (20-port switches)

AB:STRATIX_5400_20PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortFa1_17Disable	BOOL	Decimal	DisablePort:17

Table 132 - Output Data Type (20-port switches) (Continued)

AB:STRATIX_5400_20PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortFa1_19Disable	BOOL	Decimal	DisablePort:19
PortFa1_20Disable	BOOL	Decimal	DisablePort:20

20-port Gigabit Switches

Catalog numbers 1783-HMS16TG4CGN, 1783-HMS8TG8EG4CGN, 1783-HMS16TG4CGR, 1783-HMS8TG8EG4CGR

Table 133 - Input Data Type (20-port Gb switches)

AB:STRATIX_5400_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_5Connected	BOOL	Decimal	LinkStatus:5
PortGi1_6Connected	BOOL	Decimal	LinkStatus:6
PortGi1_7Connected	BOOL	Decimal	LinkStatus:7
PortGi1_8Connected	BOOL	Decimal	LinkStatus:8
PortGi1_9Connected	BOOL	Decimal	LinkStatus:9
PortGi1_10Connected	BOOL	Decimal	LinkStatus:10
PortGi1_11Connected	BOOL	Decimal	LinkStatus:11
PortGi1_12Connected	BOOL	Decimal	LinkStatus:12
PortGi1_13Connected	BOOL	Decimal	LinkStatus:13
PortGi1_14Connected	BOOL	Decimal	LinkStatus:14
PortGi1_15Connected	BOOL	Decimal	LinkStatus:15
PortGi1_16Connected	BOOL	Decimal	LinkStatus:16
PortGi1_17Connected	BOOL	Decimal	LinkStatus:17
PortGi1_18Connected	BOOL	Decimal	LinkStatus:18
PortGi1_19Connected	BOOL	Decimal	LinkStatus:19
PortGi1_20Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3

Table 133 - Input Data Type (20-port Gb switches) (Continued)

AB:STRATIX_5400_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortGi1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortGi1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortGi1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortGi1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortGi1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortGi1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortGi1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortGi1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortGi1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortGi1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortGi1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi1_19UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi1_20UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortGi1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortGi1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortGi1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortGi1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortGi1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortGi1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortGi1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortGi1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortGi1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_20Threshold	BOOL	Decimal	ThresholdExceeded:20

Table 133 - Input Data Type (20-port Gb switches) (Continued)

AB:STRATIX_5400_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortGi1_5Utilization	SINT	Decimal	
PortGi1_6Utilization	SINT	Decimal	
PortGi1_7Utilization	SINT	Decimal	
PortGi1_8Utilization	SINT	Decimal	
PortGi1_9Utilization	SINT	Decimal	
PortGi1_10Utilization	SINT	Decimal	
PortGi1_11Utilization	SINT	Decimal	
PortGi1_12Utilization	SINT	Decimal	
PortGi1_13Utilization	SINT	Decimal	
PortGi1_14Utilization	SINT	Decimal	
PortGi1_15Utilization	SINT	Decimal	
PortGi1_16Utilization	SINT	Decimal	
PortGi1_17Utilization	SINT	Decimal	
PortGi1_18Utilization	SINT	Decimal	
PortGi1_19Utilization	SINT	Decimal	
PortGi1_20Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MinorAlarmRelay	BOOL	Decimal	AlarmRelay:1
MulticastGroupActive	DINT	Binary	

Table 134 - Output Data Type (20-Gb port switches)

AB:STRATIX_5400_20PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortGi1_5Disable	BOOL	Decimal	DisablePort:5
PortGi1_6Disable	BOOL	Decimal	DisablePort:6
PortGi1_7Disable	BOOL	Decimal	DisablePort:7
PortGi1_8Disable	BOOL	Decimal	DisablePort:8

Table 134 - Output Data Type (20-Gb port switches) (Continued)

AB:STRATIX_5400_20PORT_GB_MANAGED:0:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_9Disable	BOOL	Decimal	DisablePort:9
PortGi1_10Disable	BOOL	Decimal	DisablePort:10
PortGi1_11Disable	BOOL	Decimal	DisablePort:11
PortGi1_12Disable	BOOL	Decimal	DisablePort:12
PortGi1_13Disable	BOOL	Decimal	DisablePort:13
PortGi1_14Disable	BOOL	Decimal	DisablePort:14
PortGi1_15Disable	BOOL	Decimal	DisablePort:15
PortGi1_16Disable	BOOL	Decimal	DisablePort:16
PortGi1_17Disable	BOOL	Decimal	DisablePort:17
PortGi1_18Disable	BOOL	Decimal	DisablePort:18
PortGi1_19Disable	BOOL	Decimal	DisablePort:19
PortGi1_20Disable	BOOL	Decimal	DisablePort:20

Stratix 5410 Data Types

The following tables list module-defined data types for Stratix 5410 switches. The tables include information for input (I) and output (O).

Table 135 - Input Data Type

AB:STRATIX_5410_28PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_5Connected	BOOL	Decimal	LinkStatus:5
PortGi1_6Connected	BOOL	Decimal	LinkStatus:6
PortGi1_7Connected	BOOL	Decimal	LinkStatus:7
PortGi1_8Connected	BOOL	Decimal	LinkStatus:8
PortGi1_9Connected	BOOL	Decimal	LinkStatus:9
PortGi1_10Connected	BOOL	Decimal	LinkStatus:10
PortGi1_11Connected	BOOL	Decimal	LinkStatus:11
PortGi1_12Connected	BOOL	Decimal	LinkStatus:12
PortGi1_13Connected	BOOL	Decimal	LinkStatus:13
PortGi1_14Connected	BOOL	Decimal	LinkStatus:14
PortGi1_15Connected	BOOL	Decimal	LinkStatus:15
PortGi1_16Connected	BOOL	Decimal	LinkStatus:16
PortGi1_17Connected	BOOL	Decimal	LinkStatus:17
PortGi1_18Connected	BOOL	Decimal	LinkStatus:18
PortGi1_19Connected	BOOL	Decimal	LinkStatus:19
PortGi1_20Connected	BOOL	Decimal	LinkStatus:20
PortGi1_17Connected	BOOL	Decimal	LinkStatus:17
PortGi1_18Connected	BOOL	Decimal	LinkStatus:18
PortGi1_19Connected	BOOL	Decimal	LinkStatus:19
PortGi1_20Connected	BOOL	Decimal	LinkStatus:20
PortGi1_21Connected	BOOL	Decimal	LinkStatus:21
PortGi1_22Connected	BOOL	Decimal	LinkStatus:22
PortGi1_23Connected	BOOL	Decimal	LinkStatus:23
PortGi1_24Connected	BOOL	Decimal	LinkStatus:24
PortTe1_25Connected or PortGi1_25Connected	BOOL	Decimal	LinkStatus:25
PortTe1_26Connected or PortGi1_26Connected	BOOL	Decimal	LinkStatus:26

Table 135 - Input Data Type (Continued)

AB:STRATIX_5410_28PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortTe1_27Connected or PortGi1_27Connected	BOOL	Decimal	LinkStatus:27
PortTe1_28Connected or PortGi1_28Connected	BOOL	Decimal	LinkStatus:28
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortGi1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortGi1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortGi1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortGi1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortGi1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortGi1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortGi1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortGi1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortGi1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortGi1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortGi1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi1_19UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi1_20UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
PortGi1_21UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:21
PortGi1_22UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:22
PortGi1_23UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:23
PortGi1_24UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:24
PortTe1_25UnauthorizedDevice or PortGi1_25UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:25
PortTe1_26UnauthorizedDevice or PortGi1_26UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:26
PortTe1_27UnauthorizedDevice or PortGi1_27UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:27

Table 135 - Input Data Type (Continued)

AB:STRATIX_5410_28PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortTe1_28UnauthorizedDevice or PortGi1_28UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:28
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortGi1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortGi1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortGi1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortGi1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortGi1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortGi1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortGi1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortGi1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortGi1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_20Threshold	BOOL	Decimal	ThresholdExceeded:20
PortGi1_21Threshold	BOOL	Decimal	ThresholdExceeded:21
PortGi1_22Threshold	BOOL	Decimal	ThresholdExceeded:22
PortGi1_23Threshold	BOOL	Decimal	ThresholdExceeded:23
PortGi1_24Threshold	BOOL	Decimal	ThresholdExceeded:24
PortTe1_25Threshold or PortGi1_25Threshold	BOOL	Decimal	ThresholdExceeded:25
PortTe1_26Threshold or PortGi1_26Threshold	BOOL	Decimal	ThresholdExceeded:26
PortTe1_27Threshold or PortGi1_27Threshold	BOOL	Decimal	ThresholdExceeded:27
PortTe1_28Threshold or PortGi1_28Threshold	BOOL	Decimal	ThresholdExceeded:28
AllPortsUtilization	SINT	Decimal	

Table 135 - Input Data Type (Continued)

AB:STRATIX_5410_28PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortGi1_5Utilization	SINT	Decimal	
PortGi1_6Utilization	SINT	Decimal	
PortGi1_7Utilization	SINT	Decimal	
PortGi1_8Utilization	SINT	Decimal	
PortGi1_9Utilization	SINT	Decimal	
PortGi1_10Utilization	SINT	Decimal	
PortGi1_11Utilization	SINT	Decimal	
PortGi1_12Utilization	SINT	Decimal	
PortGi1_13Utilization	SINT	Decimal	
PortGi1_14Utilization	SINT	Decimal	
PortGi1_15Utilization	SINT	Decimal	
PortGi1_16Utilization	SINT	Decimal	
PortGi1_17Utilization	SINT	Decimal	
PortGi1_18Utilization	SINT	Decimal	
PortGi1_19Utilization	SINT	Decimal	
PortGi1_20Utilization	SINT	Decimal	
PortGi1_21Utilization	SINT	Decimal	
PortGi1_22Utilization	SINT	Decimal	
PortGi1_23Utilization	SINT	Decimal	
PortGi1_24Utilization	SINT	Decimal	
PortTe1_25Utilization or PortGi1_25Utilization	SINT	Decimal	
PortTe1_26Utilization or PortGi1_26Utilization	SINT	Decimal	
PortTe1_27Utilization or PortGi1_27Utilization	SINT	Decimal	
PortTe1_28Utilization or PortGi1_28Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupActive	DINT	Binary	

Table 136 - Output Data Type

AB:STRATIX_5410_28PORT_GB_MANAGED:0:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortGi1_5Disable	BOOL	Decimal	DisablePort:5
PortGi1_6Disable	BOOL	Decimal	DisablePort:6
PortGi1_7Disable	BOOL	Decimal	DisablePort:7
PortGi1_8Disable	BOOL	Decimal	DisablePort:8
PortGi1_9Disable	BOOL	Decimal	DisablePort:9
PortGi1_10Disable	BOOL	Decimal	DisablePort:10
PortGi1_11Disable	BOOL	Decimal	DisablePort:11
PortGi1_12Disable	BOOL	Decimal	DisablePort:12
PortGi1_13Disable	BOOL	Decimal	DisablePort:13
PortGi1_14Disable	BOOL	Decimal	DisablePort:14
PortGi1_15Disable	BOOL	Decimal	DisablePort:15
PortGi1_16Disable	BOOL	Decimal	DisablePort:16
PortGi1_17Disable	BOOL	Decimal	DisablePort:17
PortGi1_18Disable	BOOL	Decimal	DisablePort:18
PortGi1_19Disable	BOOL	Decimal	DisablePort:19
PortGi1_20Disable	BOOL	Decimal	DisablePort:20
PortGi1_21Disable	BOOL	Decimal	DisablePort:21
PortGi1_22Disable	BOOL	Decimal	DisablePort:22
PortGi1_23Disable	BOOL	Decimal	DisablePort:23
PortGi1_24Disable	BOOL	Decimal	DisablePort:24
PortTe1_25Disable or PortGi1_25Disable	BOOL	Decimal	DisablePort:25
PortTe1_26Disable or PortGi1_26Disable	BOOL	Decimal	DisablePort:26
PortTe1_27Disable or PortGi1_27Disable	BOOL	Decimal	DisablePort:27
PortTe1_28Disable or PortGi1_28Disable	BOOL	Decimal	DisablePort:28

Stratix 5700 and ArmorStratix 5700 Data Types

The following tables list module-defined data types for Stratix 5700 and ArmorStratix 5700 switches. The tables include information for input (I) and output (O).

6-port Gb Switches

Catalog numbers 1783-BMS4S2SGL, 1783-BMS4S2SGA,1783-BMS06SGL, 1783-BM06SGA, 1783-BMS06TGL, 1783-BMS06TGA

Table 137 - Input Data Types (6-port Gb switches)

AB:STRATIX_5700_6PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_1Connected	BOOL	Decimal	LinkStatus:5
PortGi1_2Connected	BOOL	Decimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	

Table 137 - Input Data Types (6-port Gb switches) (Continued)

AB:STRATIX_5700_6PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 138 - Output Data Type (6-port Gb switches)

AB:STRATIX_5700_6PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortGi1_1Disable	BOOL	Decimal	DisablePort:5
PortGi1_2Disable	BOOL	Decimal	DisablePort:6

6-port Switches

Catalog numbers 1783-BMS06SL, 1783-BMS06SA, 1783-BMS06TL, 1783-BMS06TA

Table 139 - Input Data Type (6-port switches)

AB:STRATIX_5700_6PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5

Table 139 - Input Data Type (6-port switches) (Continued)

AB:STRATIX_5700_6PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 140 - Output Data Type (6-port switches)

AB:STRATIX_5700_6PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6

8-port Switches

Catalog number 1783-ZMS8TA

Table 141 - Input Data Type (8-port switches)

AB:STRATIX_5700_8PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:5
PortFa1_8Connected	BOOL	Decimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	

Table 141 - Input Data Type (8-port switches) (Continued)

AB:STRATIX_5700_8PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 142 - Output Data Type (8-port switches)

AB:STRATIX_5700_8PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8

10-port Gb Switches

Catalog numbers 1783-BMS10CGL, 1783-BMS10CGA, 1783-BMS10CGN, 1783-BMS10CGP, 1783-ZMS4T4E2TGN, 1783-ZMS4T4E2TGP

Table 143 - Input Data Type (10-port Gb switches)

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8

Table 143 - Input Data Type (10-port Gb switches) (Continued)

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_1Connected	BOOL	Decimal	LinkStatus:9
PortGi1_2Connected	BOOL	Decimal	LinkStatus:10
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:10
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 144 - Output Data Type (10-port Gb switches)

AB:STRATIX_5700_10PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortGi1_1Disable	BOOL	Decimal	DisablePort:9
PortGi1_2Disable	BOOL	Decimal	DisablePort:10

10-port Switches

Catalog numbers 1783-BMS10CL, 1783-BMS10CA

Table 145 - Input Data Type (10-port switches)

AB:STRATIX_5700_10PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5

Table 145 - Input Data Type (10-port switches) (Continued)

AB:STRATIX_5700_10PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 146 - Output Data Type (10-port switches)

AB:STRATIX_5700_10PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10

16-port Switches

Catalog number 1783-ZMS16TA

Table 147 - Input Data Type (16-port switches)

AB:STRATIX_5700_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16

Table 147 - Input Data Type (16-port switches) (Continued)

AB:STRATIX_5700_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	

Table 147 - Input Data Type (16-port switches) (Continued)

AB:STRATIX_5700_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 148 - Output Data Type (16-port switches)

AB:STRATIX_5700_16PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16

20-port Gb Switches

Catalog numbers 1783-BMS20CGL, 1783-BMS20CGN, 1783-BMS20CGP, 1783-BMS20CGPK

Table 149 - Input Data Type (20-port Gb switches)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortGi1_1Connected	BOOL	Decimal	LinkStatus:19
PortGi1_2Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11

Table 149 - Input Data Type (20-port Gb switches) (Continued)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	

Table 149 - Input Data Type (20-port Gb switches) (Continued)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

18-port Gb Switches

Catalog numbers 1783-BMS12T4E2CGNK, 1783-BMS12T4E2CGP, 1783-BMS12T4E2CGL, 1783-ZMS8T8E2TGN, 1783-ZMS8T8E2TGP

Table 150 - Input Data Type (18-port Gb switches)

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12

Table 150 - Input Data Type (18-port Gb switches) (Continued)

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortGi1_1Connected	BOOL	Decimal	LinkStatus:19
PortGi1_2Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12

Table 150 - Input Data Type (18-port Gb switches) (Continued)

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 151 - Output Data Type (18-port Gb switches)

AB:STRATIX_5700_20PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5

Table 151 - Output Data Type (18-port Gb switches) (Continued)

AB:STRATIX_5700_20PORT_GB_MANAGED:0:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortGi1_1Disable	BOOL	Decimal	DisablePort:19
PortGi1_2Disable	BOOL	Decimal	DisablePort:20

20-port Gb Switches

Catalog numbers 1783-BMS20CGL, 1783-BMS20CGN, 1783-BMS20CGP, 1783-BMS20CGPK

Table 152 - Input Data Type (20-port Gb switches)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortGi1_1Connected	BOOL	Decimal	LinkStatus:19
PortGi1_2Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11

Table 152 - Input Data Type (20-port Gb switches) (Continued)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	

Table 152 - Input Data Type (20-port Gb switches) (Continued)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 153 - Output Data Type (20-port Gb switches)

AB:STRATIX_5700_20PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortFa1_17Disable	BOOL	Decimal	DisablePort:17

Table 153 - Output Data Type (20-port Gb switches) (Continued)

AB:STRATIX_5700_20PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortGi1_1Disable	BOOL	Decimal	DisablePort:19
PortGi1_2Disable	BOOL	Decimal	DisablePort:20

20-port Switches

Catalog numbers 1783-BMS20CL, 1783-BMS20CA

Table 154 - Input Data Type (20-port switches)

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortFa1_19Connected	BOOL	Decimal	LinkStatus:19
PortFa1_20Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3

Table 154 - Input Data Type (20-port switches) (Continued)

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortFa1_19UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortFa1_20UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortFa1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortFa1_20Threshold	BOOL	Decimal	ThresholdExceeded:20

Table 154 - Input Data Type (20-port switches) (Continued)

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortFa1_19Utilization	SINT	Decimal	
PortFa1_20Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 155 - Output Data Type (20-port switches)

AB:STRATIX_5700_20PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9

Table 155 - Output Data Type (20-port switches) (Continued)

AB:STRATIX_5700_20PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortFa1_17Disable	BOOL	Decimal	DisablePort:17
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortFa1_19Disable	BOOL	Decimal	DisablePort:19
PortFa1_20Disable	BOOL	Decimal	DisablePort:20

24-port Switches

Catalog number 1783-ZMS24TA

Table 156 - Input Data Type (24-port switches)

AB:STRATIX_5700_24PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16

Table 156 - Input Data Type (24-port switches) (Continued)

AB:STRATIX_5700_24PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortFa1_19Connected	BOOL	Decimal	LinkStatus:19
PortFa1_20Connected	BOOL	Decimal	LinkStatus:20
PortFa1_21Connected	BOOL	Decimal	LinkStatus:21
PortFa1_22Connected	BOOL	Decimal	LinkStatus:22
PortFa1_23Connected	BOOL	Decimal	LinkStatus:23
PortFa1_24Connected	BOOL	Decimal	LinkStatus:24
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortFa1_19UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortFa1_20UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
PortFa1_21UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:21
PortFa1_22UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:22
PortFa1_23UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:23
PortFa1_24UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:24
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4

Table 156 - Input Data Type (24-port switches) (Continued)

AB:STRATIX_5700_24PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortFa1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortFa1_20Threshold	BOOL	Decimal	ThresholdExceeded:20
PortFa1_21Threshold	BOOL	Decimal	ThresholdExceeded:21
PortFa1_22Threshold	BOOL	Decimal	ThresholdExceeded:22
PortFa1_23Threshold	BOOL	Decimal	ThresholdExceeded:23
PortFa1_24Threshold	BOOL	Decimal	ThresholdExceeded:24
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	

Table 156 - Input Data Type (24-port switches) (Continued)

AB:STRATIX_5700_24PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_18Utilization	SINT	Decimal	
PortFa1_19Utilization	SINT	Decimal	
PortFa1_20Utilization	SINT	Decimal	
PortFa1_21Utilization	SINT	Decimal	
PortFa1_22Utilization	SINT	Decimal	
PortFa1_23Utilization	SINT	Decimal	
PortFa1_24Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 157 - Output Data Type (24-port switches)

AB:STRATIX_5700_24PORT_MANAGED:0:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortFa1_17Disable	BOOL	Decimal	DisablePort:17
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortFa1_19Disable	BOOL	Decimal	DisablePort:19
PortFa1_20Disable	BOOL	Decimal	DisablePort:20
PortFa1_21Disable	BOOL	Decimal	DisablePort:21

Table 157 - Output Data Type (24-port switches) (Continued)

AB:STRATIX_5700_24PORT_MANAGED:0:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_22Disable	BOOL	Decimal	DisablePort:22
PortFa1_23Disable	BOOL	Decimal	DisablePort:23
PortFa1_24Disable	BOOL	Decimal	DisablePort:24

Stratix 8000 and 8300 Data Types

The following tables show input and output data types for all 26 ports of the switch, as well as port assignments for data types.

Table 158 - Input Data Types

Tag Name	Type	Description
Fault	DINT	If there is s communication fault between the controller and the switch, all 32 bits in the module fault word are set to 1.
AnyPortConnected	BOOL	Indicates that at least one port has an active link.
PortGi1_1Connected	BOOL	Indicates that a particular port has an active link. 0 = Link not active 1 = Link active
PortGi1_2Connected	BOOL	
PortFa1_1Connected	BOOL	
PortFa1_2Connected	BOOL	
PortFa1_3Connected	BOOL	
PortFa1_4Connected	BOOL	
PortFa1_5Connected	BOOL	
PortFa1_6Connected	BOOL	
PortFa1_7Connected	BOOL	
PortFa1_8Connected	BOOL	
PortFa2_1Connected	BOOL	
PortFa2_2Connected	BOOL	
PortFa2_3Connected	BOOL	
PortFa2_4Connected	BOOL	
PortFa2_5Connected	BOOL	
PortFa2_6Connected	BOOL	
PortFa2_7Connected	BOOL	
PortFa2_8Connected	BOOL	
PortFa3_1Connected	BOOL	
PortFa3_2Connected	BOOL	
PortFa3_3Connected	BOOL	
PortFa3_4Connected	BOOL	
PortFa3_5Connected	BOOL	
PortFa3_6Connected	BOOL	
PortFa3_7Connected	BOOL	
PortFa3_8Connected	BOOL	

Table 158 - Input Data Types (Continued)

Tag Name	Type	Description
AnyPortUnauthorizedDevice	BOOL	Indicates that an unauthorized MAC ID has attempted to communicate on any port.
PortGi1_1UnauthorizedDevice	BOOL	Indicates that an unauthorized MAC ID has attempted to communicate on a particular port. 0 = No mismatch 1 = Mismatch
PortGi1_2UnauthorizedDevice	BOOL	
PortFa1_1UnauthorizedDevice	BOOL	
PortFa1_2UnauthorizedDevice	BOOL	
PortFa1_3UnauthorizedDevice	BOOL	
PortFa1_4UnauthorizedDevice	BOOL	
PortFa1_5UnauthorizedDevice	BOOL	
PortFa1_6UnauthorizedDevice	BOOL	
PortFa1_7UnauthorizedDevice	BOOL	
PortFa1_8UnauthorizedDevice	BOOL	
PortFa2_1UnauthorizedDevice	BOOL	
PortFa2_2UnauthorizedDevice	BOOL	
PortFa2_3UnauthorizedDevice	BOOL	
PortFa2_4UnauthorizedDevice	BOOL	
PortFa2_5UnauthorizedDevice	BOOL	
PortFa2_6UnauthorizedDevice	BOOL	
PortFa2_7UnauthorizedDevice	BOOL	
PortFa2_8UnauthorizedDevice	BOOL	
PortFa3_1UnauthorizedDevice	BOOL	
PortFa3_2UnauthorizedDevice	BOOL	
PortFa3_3UnauthorizedDevice	BOOL	
PortFa3_4UnauthorizedDevice	BOOL	
PortFa3_5UnauthorizedDevice	BOOL	
PortFa3_6UnauthorizedDevice	BOOL	
PortFa3_7UnauthorizedDevice	BOOL	
PortFa3_8UnauthorizedDevice	BOOL	
AnyPortThreshold	BOOL	Indicates that unicast, multicast, or broadcast threshold limit has been exceeded on any port.

Table 158 - Input Data Types (Continued)

Tag Name	Type	Description
PortGi1_1Threshold	BOOL	Indicates that unicast, multicast, or broadcast threshold limit has been exceeded on a particular port. 0 = OK 1 = Threshold exceeded
PortGi1_2Threshold	BOOL	
PortFa1_1Threshold	BOOL	
PortFa1_2Threshold	BOOL	
PortFa1_3Threshold	BOOL	
PortFa1_4Threshold	BOOL	
PortFa1_5Threshold	BOOL	
PortFa1_6Threshold	BOOL	
PortFa1_7Threshold	BOOL	
PortFa1_8Threshold	BOOL	
PortFa2_1Threshold	BOOL	
PortFa2_2Threshold	BOOL	
PortFa2_3Threshold	BOOL	
PortFa2_4Threshold	BOOL	
PortFa2_5Threshold	BOOL	
PortFa2_6Threshold	BOOL	
PortFa2_7Threshold	BOOL	
PortFa2_8Threshold	BOOL	
PortFa3_1Threshold	BOOL	
PortFa3_2Threshold	BOOL	
PortFa3_3Threshold	BOOL	
PortFa3_4Threshold	BOOL	
PortFa3_5Threshold	BOOL	
PortFa3_6Threshold	BOOL	
PortFa3_7Threshold	BOOL	
PortFa3_8Threshold	BOOL	
AllPortsUtilization	SINT	The sum of the percentage of the bandwidth utilized of all ports on the switch.

Table 158 - Input Data Types (Continued)

Tag Name	Type	Description
PortGi1_1Utilization;	SINT	The percentage of the bandwidth utilized on a particular port.
PortGi1_2Utilization;	SINT	
PortFa1_1Utilization;	SINT	
PortFa1_2Utilization;	SINT	
PortFa1_3Utilization;	SINT	
PortFa1_4Utilization;	SINT	
PortFa1_5Utilization;	SINT	
PortFa1_6Utilization;	SINT	
PortFa1_7Utilization;	SINT	
PortFa1_8Utilization;	SINT	
PortFa2_1Utilization;	SINT	
PortFa2_2Utilization;	SINT	
PortFa2_3Utilization;	SINT	
PortFa2_4Utilization;	SINT	
PortFa2_5Utilization;	SINT	
PortFa2_6Utilization;	SINT	
PortFa2_7Utilization;	SINT	
PortFa2_8Utilization;	SINT	
PortFa3_1Utilization;	SINT	
PortFa3_2Utilization;	SINT	
PortFa3_3Utilization;	SINT	
PortFa3_4Utilization;	SINT	
PortFa3_5Utilization;	SINT	
PortFa3_6Utilization;	SINT	
PortFa3_7Utilization;	SINT	
PortFa3_8Utilization;	SINT	
MajorAlarmRelay	BOOL	Indicates whether the major alarm relay is on or off. 0 = Contact open (off) 1 = Contact closed (on)
MinorAlarmRelay	BOOL	Indicates whether the minor alarm relay is on or off. 0 = Contact open (off) 1 = Contact closed (on)
MulticastGroupsActive	DINT	The number of active multicast groups across all ports.

Table 159 - Output Data Types

Tag Name	Type	Description
AllPortsDisable	BOOL	Setting this bit disables all ports on the switch. 0 = Enable 1 = Disable
PortGi1_1Disable	BOOL	Setting a particular bit disables that particular port. 0 = Enable 1 = Disable
PortGi1_2Disable	BOOL	
PortFa1_1Disable	BOOL	
PortFa1_2Disable	BOOL	
PortFa1_3Disable	BOOL	
PortFa1_4Disable	BOOL	
PortFa1_5Disable	BOOL	
PortFa1_6Disable	BOOL	
PortFa1_7Disable	BOOL	
PortFa1_8Disable	BOOL	
PortFa2_1Disable	BOOL	
PortFa2_2Disable	BOOL	
PortFa2_3Disable	BOOL	
PortFa2_4Disable	BOOL	
PortFa2_5Disable	BOOL	
PortFa2_6Disable	BOOL	
PortFa2_7Disable	BOOL	
PortFa2_8Disable	BOOL	
PortFa3_1Disable	BOOL	
PortFa3_2Disable	BOOL	
PortFa3_3Disable	BOOL	
PortFa3_4Disable	BOOL	
PortFa3_5Disable	BOOL	
PortFa3_6Disable	BOOL	
PortFa3_7Disable	BOOL	
PortFa3_8Disable	BOOL	

Notes:

Port Assignments for CIP Data

Topic	Page
Stratix 5400 Port Assignments	488
Stratix 5410 Port Assignments	490
Stratix 5700 Port Assignments	491
ArmorStratix 5700 Port Assignments	492
Stratix 8000 and 8300 Port Assignments	493

The following tables identify the instance numbers of the Ethernet link objects that are associated with each port on the switch. Instance 0 does not apply to all ports as it does for bit maps.

The bit numbers identify each port when they are contained in a structure of all ports, such as in the output assembly. Bit 0 refers to any or all ports.

Stratix 5400 Port Assignments

Table 160 - 8- and 12-port Switches

Bit	1783-HMS4C4CGN	1783-HMS8T4CGN	1783-HMS8S4CGN	1783-HMS4T4E4CGN	1783-HMS8TG4CGN 1783-HMS8TG4CGR	1783-HMS8SG4CGN 1783-HMS8SG4CGR	1783-HMS4EG8CGN 1783-HMS4EG8CGR
0	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports
1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1
2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2
3	Gi1/3	Gi1/3	Gi1/3	Gi1/3	Gi1/3	Gi1/3	Gi1/3
4	Gi1/4	Gi1/4	Gi1/4	Gi1/4	Gi1/4	Gi1/4	Gi1/4
5	Fa1/5	Fa1/5	Fa1/5	Fa1/5	Gi1/5	Gi1/5	Gi1/5
6	Fa1/6	Fa1/6	Fa1/6	Fa1/6	Gi1/6	Gi1/6	Gi1/6
7	Fa1/7	Fa1/7	Fa1/7	Fa1/7	Gi1/7	Gi1/7	Gi1/7
8	Fa1/8	Fa1/8	Fa1/8	Fa1/8	Gi1/8	Gi1/8	Gi1/8
9		Fa1/9	Fa1/9	Fa1/9	Gi1/9	Gi1/9	Gi1/9
10		Fa1/10	Fa1/10	Fa1/10	Gi1/10	Gi1/10	Gi1/10
11		Fa1/11	Fa1/11	Fa1/11	Gi1/11	Gi1/11	Gi1/11
12		Fa1/12	Fa1/12	Fa1/12	Gi1/12	Gi1/12	Gi1/12
27	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1

Table 161 - 16- and 20-port Switches

Bit	1783-HMS4S8E4CGN	1783-HMS4SG8EG4CGN 1783-HMS4SG8EG4CGR	1783-HMS16T4CGN	1783-HMS16TG4CGN 1783-HMS16TG4CGR	1783-HMS8TG8EG4CGN 1783-HMS8TG8EG4CGR
0	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports
1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1
2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2
3	Gi1/3	Gi1/3	Gi1/3	Gi1/3	Gi1/3
4	Gi1/4	Gi1/4	Gi1/4	Gi1/4	Gi1/4
5	Fa1/5	Gi1/5	Fa1/5	Gi1/5	Gi1/5
6	Fa1/6	Gi1/6	Fa1/6	Gi1/6	Gi1/6
7	Fa1/7	Gi1/7	Fa1/7	Gi1/7	Gi1/7
8	Fa1/8	Gi1/8	Fa1/8	Gi1/8	Gi1/8
9	Fa1/9	Gi1/9	Fa1/9	Gi1/9	Gi1/9
10	Fa1/10	Gi1/10	Fa1/10	Gi1/10	Gi1/10
11	Fa1/11	Gi1/11	Fa1/11	Gi1/11	Gi1/11
12	Fa1/12	Gi1/12	Fa1/12	Gi1/12	Gi1/12
13	Fa1/13	Gi1/13	Fa1/13	Gi1/13	Gi1/13
14	Fa1/14	Gi1/14	Fa1/14	Gi1/14	Gi1/14
15	Fa1/15	Gi1/15	Fa1/15	Gi1/15	Gi1/15
16	Fa1/16	Gi1/16	Fa1/16	Gi1/16	Gi1/16
17			Fa1/17	Gi1/17	Gi1/17
18			Fa1/18	Gi1/18	Gi1/18
19			Fa1/19	Gi1/19	Gi1/19
20			Fa1/20	Gi1/20	Gi1/20
27	SVI1	SVI1	SVI1	SVI1	SVI1

Stratix 5410 Port Assignments

Bit	1783-IMS28NDC, 1783-IMS28NAC, 1783-IMS28GNDC, 1783-IMS28GNAC, 1783-IMS28RDC, 1783-IMS28RAC, 1783-IMS28GRDC, 1783-IMS28GRAC
0	Any/All ports
1	Gi1/1
2	Gi1/2
3	Gi1/3
4	Gi1/4
5	Gi1/5
6	Gi1/6
7	Gi1/7
8	Gi1/8
9	Gi1/9
10	Gi1/10
11	Gi1/11
12	Gi1/12
13	Gi1/13
14	Gi1/14
15	Gi1/15
16	Gi1/16
17	Gi1/17
18	Gi1/18
19	Gi1/19
20	Gi1/20
21	Gi1/21
22	Gi1/22
23	Gi1/23
24	Gi1/24
25	Te1/25 or Gi1/25
26	Te1/26 or Gi1/26
27	Te1/27 or Gi1/27
28	Te1/28 or Gi1/28

Stratix 5700 Port Assignments

Table 162 - 6- and 10-port Switches

Bit	1783-BMS4S2SGL, 1783-BMS4S2SGA, 1783-BMS06SL, 1783-BMS06SA, 1783-BMS06TL, 1783-BMS06TA, 1783-BMS06SGL, 1783-BMS06SGA	1783-BMS06TGL, 1783-BMS06TGA	1783-BMS10CL, 1783-BMS10CA	1783-BMS10CGL, 1783-BMS10CGA, 1783-BMS10CGP, 1783-BMS10CGN
0	Any/All ports	Any/All ports	Any/All ports	Any/All ports
1	Fa1/1	Fa/1	Fa1/1	Fa1/1
2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
5	Fa1/5	Gi1/1	Fa1/5	Fa1/5
6	Fa1/6	Gi1/2	Fa1/6	Fa1/6
7			Fa1/7	Fa1/7
8			Fa1/8	Fa1/8
9			Fa1/9	Gi1/1
10			Fa1/10	Gi1/2
27	SVI1	SVI1	SVI1	SVI1

Table 163 - 18- and 20-port Switches

Bit	1783-BMS12T4E2CGL, 1783-BMS12T4E2CGP, 1783-BMS12T4E2CGNK	1783-BMS20CL, 1783-BMS20CA	1783-BMS20CGL, 1783-BMS20CGN, 1783-BMS20CGP, 1783-BMS20CGPK
0	Any/All ports	Any/All ports	Any/All ports
1	Fa1/1	Fa1/1	Fa1/1
2	Fa1/2	Fa1/2	Fa1/2
3	Fa1/3	Fa1/3	Fa1/3
4	Fa1/4	Fa1/4	Fa1/4
5	Fa1/5	Fa1/5	Fa1/5
6	Fa1/6	Fa1/6	Fa1/6
7	Fa1/7	Fa1/7	Fa1/7
8	Fa1/8	Fa1/8	Fa1/8
9	Fa1/9	Fa1/9	Fa1/9
10	Fa1/10	Fa1/10	Fa1/10
11	Fa1/11	Fa1/11	Fa1/11
12	Fa1/12	Fa1/12	Fa1/12
13	Fa1/13	Fa1/13	Fa1/13
14	Fa1/14	Fa1/14	Fa1/14
15	Fa1/15	Fa1/15	Fa1/15
16	Gi1/1	Fa1/16	Fa1/16
17	Gi1/2	Fa1/17	Fa1/17
18	Gi1/3	Fa1/18	Fa1/18

Table 163 - 18- and 20-port Switches (Continued)

Bit	1783-BMS12T4E2CGL, 1783-BMS12T4E2CGP, 1783-BMS12T4E2CGNK	1783-BMS20CL, 1783-BMS20CA	1783-BMS20CGL, 1783-BMS20CGN, 1783-BMS20CGP, 1783-BMS20CGPK
19		Fa1/19	Gi1/1
20		Fa1/20	Gi1/2
27	SVI1	SVI1	SVI1

ArmorStratix 5700 Port Assignments

Bit	1783-ZMS8TA	1783-ZMS4T4E2TGP, 1783-ZMS4T4E2TGN	1783-ZMS16TA	1783-ZMS8T8E2TGP, 1783-ZMS8T8E2TGN	1783-ZMS24TA
0	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports
1	Fa1/1	Fa/1	Fa1/1	Fa1/1	Fa1/1
2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
5	Fa1/5	Fa1/5	Fa1/5	Fa1/5	Fa1/5
6	Fa1/6	Fa1/6	Fa1/6	Fa1/6	Fa1/6
7	Fa1/7	Fa1/7	Fa1/7	Fa1/7	Fa1/7
8	Fa1/8	Fa1/8	Fa1/8	Fa1/8	Fa1/8
9		Gi1/1	Fa1/9	Fa1/9	Fa1/9
10		Gi1/2	Fa1/10	Fa1/10	Fa1/10
11			Fa1/11	Fa1/11	Fa1/11
12			Fa1/12	Fa1/12	Fa1/12
13			Fa1/13	Fa1/13	Fa1/13
14			Fa1/14	Fa1/14	Fa1/14
15			Fa1/15	Fa1/15	Fa1/15
16			Fa1/16	Fa1/16	Fa1/16
17				Gi1/1	Fa1/17
18				Gi1/2	Fa1/18
19					Fa1/19
20					Fa1/20
21					Fa1/21
22					Fa1/22
23					Fa1/23
24					Fa1/24
27	SVI1	SVI1	SVI1	SVI1	SVI1

Stratix 8000 and 8300 Port Assignments

Bit	6-port Managed Ethernet Switch	10-port Managed Ethernet Switch	10-port Managed Ethernet Switch	14-port Managed Ethernet Switch	14-port Managed Ethernet Switch	14-port Managed Ethernet Switch	18-port Managed Ethernet Switch
0	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports
1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1
2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2
3	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1
4	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
5	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
6	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
7		Fa1/5			Fa1/5		Fa1/5
8		Fa1/6			Fa1/6		Fa1/6
9		Fa1/7			Fa1/7		Fa1/7
10		Fa1/8			Fa1/8		Fa1/8
11			Fa2/1	Fa2/1	Fa2/1	Fa2/1	Fa2/1
12			Fa2/2	Fa2/2	Fa2/2	Fa2/2	Fa2/2
13			Fa2/3	Fa2/3	Fa2/3	Fa2/3	Fa2/3
14			Fa2/4	Fa2/4	Fa2/4	Fa2/4	Fa2/4
15				Fa2/5			Fa2/5
16				Fa2/6			Fa2/6
17				Fa2/7			Fa2/7
18				Fa2/8			Fa2/8
19						Fa3/1	
20						Fa3/2	
21						Fa3/3	
22						Fa3/4	
23							
24							
25							
26							

Notes:

Port Numbering

Topic	Page
Stratix 5400 Port Numbering	496
Stratix 5410 Port Numbering	504
Stratix 5700 Port Numbering	505
ArmorStratix 5700 Port Numbering	512
Stratix 8000 and 8300 Port Numbering	515

Stratix 5400 Port Numbering

The port ID consists of the following:

- Port type (Gigabit Ethernet for Gigabit ports and Fast Ethernet for 10/100 Mbps ports)
- Unit number (always 1)
- Port number (1...20, depending on the catalog number)

Gigabit Ethernet is abbreviated as Gi and Fast Ethernet as Fa.

Table 164 - Stratix 5400 Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-HMS4C4CGN	8-port (4 combo Gigabit ports; 4 combo Ethernet ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
1783-HMS8T4CGN	12-port (4 combo Gigabit ports; 8 Ethernet ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
1783-HMS8S4CGN	12-port (4 combo Gigabit ports; 8 SFP ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12

Table 164 - Stratix 5400 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-HMS4T4E4CGN	12-port (4 combo Gigabit ports; 4 Ethernet ports; 4 PoE/PoE+ ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
1783-HMS8TG4CGN	12-port (8 Gigabit ports; 4 Gigabit combo ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12
1783-HMS8SG4CGN	12-port (4 Gigabit combo ports; 8 Gigabit SFP ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12
1783-HMS4EG8CGN	12-port (4 Gigabit ports; 4 Gigabit combo ports; 4 Gigabit PoE/PoE+ ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12

Table 164 - Stratix 5400 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-HMS4S8E4CGN	16-port (4 combo Gigabit ports; 8 PoE/PoE+ ports; 4 SFP ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
1783-HMS4SG8EG4CGN	16-port (4 Gigabit combo ports; 8 Gigabit PoE/PoE+ ports; 4 Gigabit SFP ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12
		13	Gi1/13
		14	Gi1/14
		15	Gi1/15
		16	Gi1/16

Table 164 - Stratix 5400 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-HMS16T4CGN	20-port (4 combo Gigabit ports; 16 Ethernet ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20
1783-HMS16TG4CGN	20-port (16 Gigabit ports; 4 Gigabit combo ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12
		13	Gi1/13
		14	Gi1/14
		15	Gi1/15
		16	Gi1/16
		17	Gi1/17
		18	Gi1/18
		19	Gi1/19
		20	Gi1/20

Table 164 - Stratix 5400 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-HMS8TG8EG4CGN	20-port (8 Gigabit ports; 4 Gigabit combo ports; 8 Gigabit PoE/PoE+ ports) managed switch; Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12
		13	Gi1/13
		14	Gi1/14
		15	Gi1/15
		16	Gi1/16
		17	Gi1/17
		18	Gi1/18
		19	Gi1/19
		20	Gi1/20
1783-HMS8TG4CGR	12-port (8 Ethernet ports; 4 Gigabit combo ports) managed switch; Layer 3 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12
1783-HMS8SG4CGR	12-port (4 Gigabit combo ports; 8 Gigabit SFP ports) managed switch; Layer 3 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12

Table 164 - Stratix 5400 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-HMS4EG8CGR	12-port (4 Gigabit ports; 4 Gigabit combo ports; 4 Gigabit PoE/PoE+ ports) managed switch; Layer 3 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12

Table 164 - Stratix 5400 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-HMS4SG8EG4CGR	16-port (4 Gigabit combo ports; 8 Gigabit PoE/PoE+ ports; 4 Gigabit SFP ports) managed switch; Layer 3 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12
		13	Gi1/13
		14	Gi1/14
		15	Gi1/15
		16	Gi1/16
1783-HMS16TG4CGR	20-port (16 Gigabit ports; 4 Gigabit combo ports) managed switch; Layer 3 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12
		13	Gi1/13
		14	Gi1/14
		15	Gi1/15
		16	Gi1/16
		17	Gi1/17
		18	Gi1/18
		19	Gi1/19
		20	Gi1/20

Table 164 - Stratix 5400 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-HMS8TG8EG4CGR	20-port (8 Gigabit ports; 4 Gigabit combo ports; 8 Gigabit PoE/PoE+ ports) managed switch; Layer 3 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
		11	Gi1/11
		12	Gi1/12
		13	Gi1/13
		14	Gi1/14
		15	Gi1/15
		16	Gi1/16
		17	Gi1/17
		18	Gi1/18
		19	Gi1/19
		20	Gi1/20

Stratix 5410 Port Numbering

The port ID consists of the following:

- Port type (Gigabit Ethernet or 10 Gigabit Ethernet)
- Unit number (always 1))
- Port number (1...28)

Gigabit Ethernet is abbreviated as Gi and 10 Gigabit Ethernet as Te.

Table 165 - Stratix 5410 Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-IMS28NDC	28-port (12 Gigabit PoE/PoE+ ports; 12 Gigabit+ 4 10 Gigabit SFP ports) managed switch; Layer 2 firmware; DC power supply	1	Gi1/1
		2	Gi1/2
1783-IMS28NAC	28-port (12 Gigabit PoE/PoE+ ports; 12 Gigabit+ 4 10 Gigabit SFP ports) managed switch; Layer 2 firmware; AC power supply	3	Gi1/3
		4	Gi1/4
1783-IMS28RDC	28-port (12 Gigabit PoE/PoE+ ports; 12 Gigabit+ 4 10 Gigabit SFP ports) managed switch; Layer 3 firmware; DC power supply	5	Gi1/5
		6	Gi1/6
1783-IMS28RAC	28-port (12 Gigabit PoE/PoE+ ports; 12 Gigabit+ 4 10 Gigabit SFP ports) managed switch; Layer 3 firmware; AC power supply	7	Gi1/7
		8	Gi1/8
1783-IMS28GNDC	28-port (12 Gigabit PoE/PoE+ ports; 16 Gigabit SFP ports) managed switch; Layer 2 firmware; DC power supply	9	Gi1/9
		10	Gi1/10
1783-IMS28GNAC	28-port (12 Gigabit PoE/PoE+ ports; 16 Gigabit SFP ports) managed switch; Layer 2 firmware; AC power supply	11	Gi1/11
		12	Gi1/12
1783-IMS28GRDC	28-port (12 Gigabit PoE/PoE+ ports; 16 Gigabit SFP ports) managed switch; Layer 3 firmware; DC power supply	13	Gi1/13
		14	Gi1/14
1783-IMS28GRAC	28-port (12 Gigabit PoE/PoE+ ports; 16 Gigabit SFP ports) managed switch; Layer 3 firmware; AC power supply	15	Gi1/15
		16	Gi1/16
		17	Gi1/17
		18	Gi1/18
		19	Gi1/19
		20	Gi1/20
		21	Gi1/21
		22	Gi1/22
		23	Gi1/23
		24	Gi1/24
		25	Te1/25 or Gi1/25
		26	Te1/26 or Gi1/26
		27	Te1/27 or Gi1/27
		28	Te1/28 or Gi1/28

Stratix 5700 Port Numbering

The port ID consists of the following:

- Port type (Gigabit Ethernet for Gigabit ports and Fast Ethernet for 10/100 Mbps ports)
- Unit number (always 1)
- Port number (1...2 for Gigabit ports, 1...18 for all others, depending on the catalog number)

Gigabit Ethernet is abbreviated as Gi and Fast Ethernet as Fa.

Table 166 - Stratix 5700 Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS4S2SGL	6-port (4 SFP slots; 2 SFP Gigabit slots) managed switch; lite firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS4S2SGA	6-port (4 SFP slots; 2 SFP Gigabit slots) managed switch; full firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SL	6-port (4 Ethernet ports; 2 SFP slots) managed switch; lite firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SA	6-port (4 Ethernet ports; 2 SFP slots) managed switch; full firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TL	6-port (6 Ethernet ports) managed switch; lite firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TA	6-port (6 Ethernet ports) managed switch; full firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SGL	6-port (4 Ethernet ports; 2 SFP Gigabit slots) managed switch; lite firmware	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2

Table 166 - Stratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BM06SGA	6-port (4 Ethernet ports; 2 SFP Gigabit slots) managed switch; full firmware	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS06TGL	6-port (4 Ethernet ports; 2 Gigabit ports) managed switch; lite firmware	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS06TGA	6-port (4 Ethernet ports; 2 Gigabit ports) managed switch; full firmware	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS10CL	10-port (8 Ethernet ports; 2 combo ports) managed switch; lite firmware	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CA	10-port (8 Ethernet ports; 2 combo ports) managed switch; full firmware	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CGL	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; lite firmware	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2

Table 166 - Stratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS10CGA	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; full firmware	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGN	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; full firmware; PTP; NAT	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGP	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; full firmware; PTP	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS12T4E2CGNK	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; full firmware; PTP; NAT; conformal coating	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Gi1/1 Gi1/2

Table 166 - Stratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS12T4E2CGP	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; full firmware; PTP	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		1	Gi1/1
		2	Gi1/2
1783-BMS12T4E2CGL	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; lite firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		1	Gi1/1
		2	Gi1/2
1783-BMS20CL	20-port (16 Ethernet ports; 2 SFP slots; 2 combo ports) managed switch; lite firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20

Table 166 - Stratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS20CA	20-port (16 Ethernet ports; 2 SFP slots; 2 combo ports) managed switch; full firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20
1783-BMS20CGL	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; lite firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

Table 166 - Stratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS20CGN	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; PTP; NAT	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2
1783-BMS20CGP	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; PTP	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

Table 166 - Stratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS20CGPK	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; PTP; conformal coating	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

ArmorStratix 5700 Port Numbering

The port ID consists of the following:

- Port type (Gigabit Ethernet for Gigabit ports and Fast Ethernet for 10/100 Mbps ports)
- Unit number (always 1)
- Port number (1...2 for Gigabit ports, 1...18 for all others, depending on the catalog number)

Gigabit Ethernet is abbreviated as Gi and Fast Ethernet as Fa.

Table 167 - ArmorStratix 5700 Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-ZMS8TA	8-port (8 Ethernet ports) managed switch; full firmware	1 2 3 4 5 6 7 8	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8
1783-ZMS4T4E2TGP	10-port (2 Gigabit ports; 4 Ethernet ports; 4 PoE/PoE+ ports) managed switch; full firmware; PTP	GE-1 GE-2 1 2 3 4 5 6 7 8	Gi1/1 Gi1/2 Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8
1783-ZMS4T4E2TGN	10-port (2 Gigabit ports; 4 Ethernet ports; 4 PoE/PoE+ ports) managed switch; full firmware; PTP; NAT	GE-1 GE-2 1 2 3 4 5 6 7 8	Gi1/1 Gi1/2 Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8
1783-ZMS16TA	16-port (16 Ethernet ports) managed switch; full firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16

Table 167 - ArmorStratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-ZMS8T8E2TGP	18-port (2 Gigabit ports; 8 Ethernet ports; 8 PoE/PoE+ ports) managed switch; full firmware; PTP	GE-1 GE-2 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi1/1 Gi1/2 Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16
1783-ZMS8T8E2TGN	18-port (2 Gigabit ports; 8 Ethernet ports; 8 PoE/PoE+ ports) managed switch; full firmware; PTP; NAT	GE-1 GE-2 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi1/1 Gi1/2 Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16

Table 167 - ArmorStratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-ZMS24TA	24-port (24 Ethernet ports) managed switch; full firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20
		21	Fa1/21
		22	Fa1/22
		23	Fa1/23
		24	Fa1/24

Stratix 8000 and 8300 Port Numbering

The port ID consists of the following:

- Port type (Gigabit Ethernet for Gigabit ports and Fast Ethernet for 10/100 Mbps ports)
- Unit number (1, 2, or 3)
- Port number (1...2 for Gigabits, 1...4 for the 6-port base and 1...8 for all others)

Gigabit Ethernet is abbreviated as Gi and Fast Ethernet as Fa.

For the expansion modules, the Fa# represents slot 2 o 3.

Table 168 - Stratix 8000/8300 Switch and Expansion Module Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MS06T	6-port (2 Gigabit ports; 4 Ethernet ports) base switch	Gigabit ports: 1 2 Fast Ethernet ports: 1 2 3 4	Gigabit ports: Gi1/1 Gi1/2 Fast Ethernet ports: Fa1/1 Fa1/2 Fa1/3 Fa1/4
1783-MS10T	10-port (2 Gigabit ports; 8 Ethernet ports) base switch	Gigabit ports: 1 2 Fast Ethernet ports: 1 2 3 4 5 6 7 8	Gigabit ports: Gi1/1 Gi1/2 Fast Ethernet ports: Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8
1783-RMS06T	6-port (2 Gigabit ports; 4 Ethernet ports) base switch	Gigabit ports: 1 2 Fast Ethernet ports: 1 2 3 4	Gigabit ports: Gi1/1 Gi1/2 Fast Ethernet ports: Fa1/1 Fa1/2 Fa1/3 Fa1/4
1783-RMS10T	10-port (2 Gigabit ports; 8 Ethernet ports) base switch	Gigabit ports: 1 2 Fast Ethernet ports: 1 2 3 4 5 6 7 8	Gigabit ports: Gi1/1 Gi1/2 Fast Ethernet ports: Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8

Table 168 - Stratix 8000/8300 Switch and Expansion Module Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MX04E	4-port (4 PoE ports) expansion module	1 2 3 4	Fa#/1 Fa#/2 Fa#/3 Fa#/4
1783-MX04T04E	8-port(4 Ethernet ports; 4 PoE ports) expansion module	1 2 3 4 5 6 7 8	Fa#/1 Fa#/2 Fa#/3 Fa#/4 Fa#/5 Fa#/6 Fa#/7 Fa#/8
1783-MX04S	4-port (4 SFP ports) expansion module	1 2 3 4	Fa#/1 Fa#/2 Fa#/3 Fa#/4
1783-MX08S	8-port (8 SFP ports) expansion module	1 2 3 4 5 6 7 8	Fa#/1 Fa#/2 Fa#/3 Fa#/4 Fa#/5 Fa#/6 Fa#/7 Fa#/8
1783-MX08T	8-port (8 Ethernet ports) expansion module	1 2 3 4 5 6 7 8	Fa#/1 Fa#/2 Fa#/3 Fa#/4 Fa#/5 Fa#/6 Fa#/7 Fa#/8
1783-MX08F	8-port (8 Ethernet ports) expansion module	1 2 3 4 5 6 7 8	Fa#/1 Fa#/2 Fa#/3 Fa#/4 Fa#/5 Fa#/6 Fa#/7 Fa#/8

Cables and Connectors

Topic	Page
Stratix 5410 Cables and Connectors	517
Stratix 5400 and 5700 Cables and Connectors	523
ArmorStratix 5700 Cables and Connectors	529
Stratix 8000/8300 Cables and Connectors	534

For recommended cables and SFP modules, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Stratix 5410 Cables and Connectors

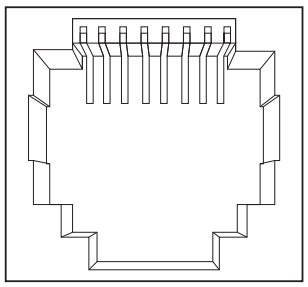
This section describes how to connect to ports on Stratix® 5410 switches.

10/100/1000 Ports

The 10/100/1000 Ethernet, PoE/PoE+ ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

Figure 60 - 10/100/1000 Connector Pinouts

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



Connect to 10BASE-T- and 100BASE-TX-Compatible Devices

The auto-MDIX feature is enabled by default. Follow these cabling guidelines when the auto-MDIX feature has been disabled.

When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as servers and routers, you can use a two or four twisted-pair, straight-through cable that is wired for 10BASE-T and 100BASE-TX.

To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side-by-side, with the tab at the back. The color of the wire that is connected to the pin on the outside of the left plug must differ from the color of the wire that is connected to the pin on the inside of the right plug.

Figure 70 and Figure 71 show the cable schematics.

Figure 61 - Two Twisted-pair Straight-through Cable Schematics

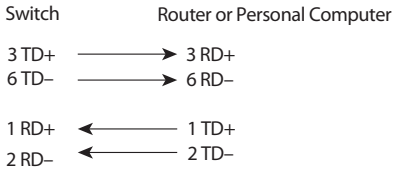
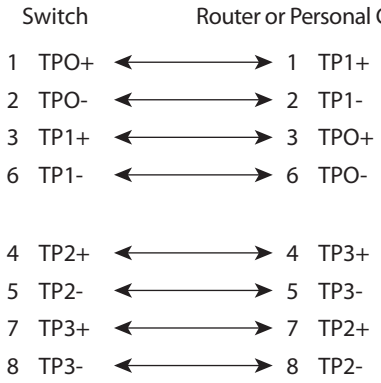


Figure 62 - Four Twisted-pair Straight-through Cable Schematics



When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable.

Use a straight-through cable to connect two ports when only one port is designated with an X. Use a crossover cable to connect two ports when both ports are designated with an X or when both ports do not have an X.

You can use Category 3, 4, or 5 cabling when connecting to 10BASE-T-compatible devices. You must use Category 5 cabling when connecting to 100BASE-TX-compatible devices.

IMPORTANT Use a four twisted-pair, Category 5 cable when connecting to a 1000BASE-T-compatible device or PoE port.

Figure 72 and Figure 73 show the cable schematics.

Figure 63 - Two Twisted-pair Crossover Cable Schematics

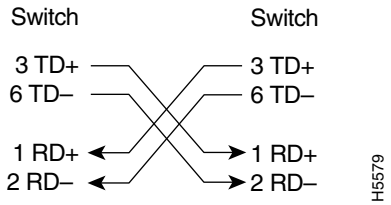
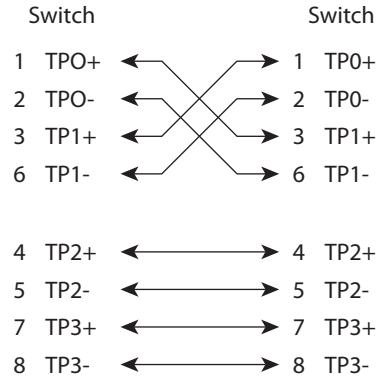


Figure 64 - Four Twisted-pair Crossover Cable Schematics

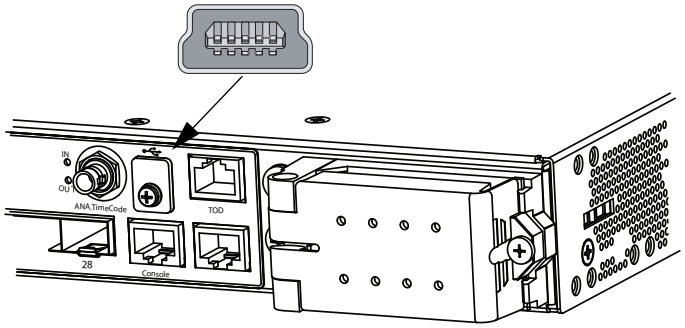


Console Ports

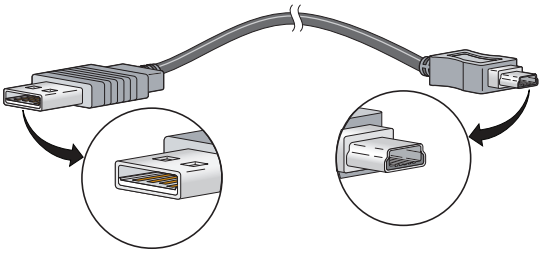
Console ports enable you to connect a switch to a computer if you use the Command-line interface (CLI) to configure and monitor a switch.

Stratix 5410 switches have these console ports:

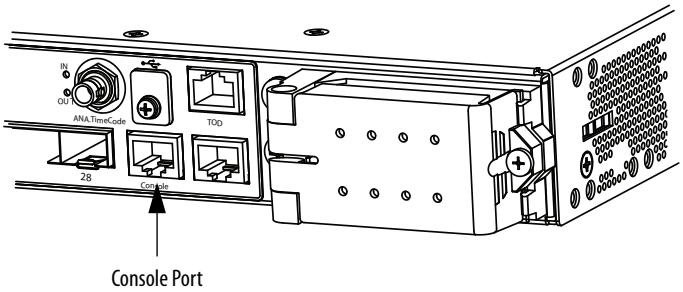
- A USB 5-pin mini-Type B port on the front panel



The USB console port uses a USB Type A to 5-pin mini-Type B cable. To use the USB cable, download the drivers for Microsoft Windows from http://www.rockwellautomation.com. The USB cable is not provided with the switch.



- RJ45 console port on the front panel



The following table lists the pinouts for the console port, the RJ45-to-DB-9 adapter cable, and the console device.

Table 169 - Pinouts with DB-9 Pin

Switch Console Port (DTE)	RJ45-to-DB-9 Terminal Adapter	Console Device
Signal	**DB-9 Pin**	**Signal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

The following table lists the pinouts for the console port, RJ45-to-DB-25 female DTE adapter, and the console device. The RJ45-to-DB-25 female DTE adapter is not supplied with the switch.

Table 170 - Pinouts with DB-25 Pin

Switch Console Port (DTE)	RJ45-to-DB-25 Terminal Adapter	Console Device
Signal	**DB-25 Pin**	**Signal**
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

Alarm Port

The front panel alarm port uses an RJ45 connector.

Figure 65 - Front Panel Alarm Connector

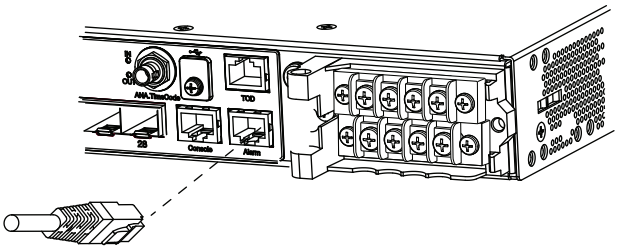
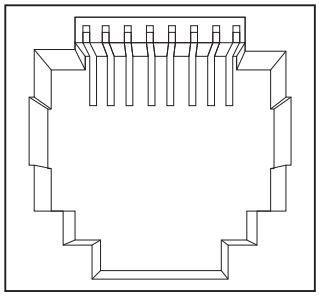


Figure 66 - Alarm Connector Pinout

Pin	Label
1	Alarm 1 input
2	Alarm 2 input
3	Alarm output normally closed
4	Alarm 3 input
5	Alarm 4 input
6	Alarm output normally open
7	Alarm output common
8	Alarm input common



Ethernet, PoE Port Cable Specifications

For Ethernet, PoE ports, use a Category 5 (Cat 5) cable with a distance of up to 100 m (328 ft).

Stratix 5400 and 5700 Cables and Connectors

This section describes how to connect to ports on Stratix 5400 and Stratix 5700 switches.

10/100 and 10/100/1000 Ports

The 10/100 and 10/100/1000 Ethernet ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

Figure 67 - 10/100 Connector Pinouts

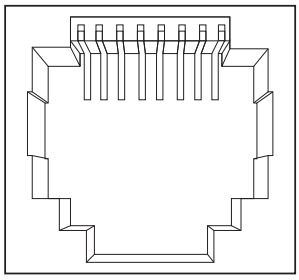
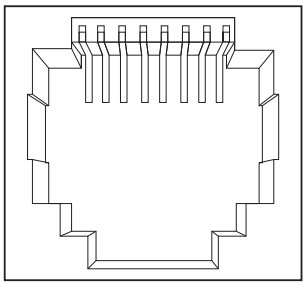
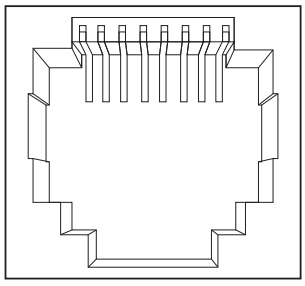
Pin	Label	1 2 3 4 5 6 7 8
1	RD+	
2	RD-	
3	TD+	
4	NC	
5	NC	
6	TD-	
7	NC	
8	NC	

Figure 68 - 10/100/1000 Connector Pinouts

Pin	Label	1 2 3 4 5 6 7 8
1	TP0+	
2	TP0-	
3	TP1+	
4	TP2+	
5	TP2-	
6	TP1-	
7	TP3+	
8	TP3-	

PoE ports integrate power and data signals on the same wires. The ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

Figure 69 - 10/100 PoE Connector Pinouts and Power Sourcing Equipment (PSE) Voltage

Pin	Label	Alternative A (MDI)	1 2 3 4 5 6 7 8
1	RD+	Positive V PSE	
2	RD-	Positive V PSE	
3	TD+	Negative V PSE	
4	NC		
5	NC		
6	TD-	Negative V PSE	
7	NC		
8	NC		

Connect to 10BASE-T- and 100BASE-TX-Compatible Devices

The auto-MDIX feature is enabled by default. Follow these cabling guidelines when the auto-MDIX feature has been disabled.

When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as servers and routers, you can use a two or four twisted-pair, straight-through cable that is wired for 10BASE-T and 100BASE-TX.

To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side-by-side, with the tab at the back. The color of the wire that is connected to the pin on the outside of the left plug must differ in color from the wire that is connected to the pin on the inside of the right plug.

Figure 70 and Figure 71 show the cable schematics.

Figure 70 - Two Twisted-pair Straight-through Cable Schematics

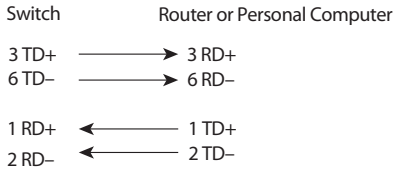
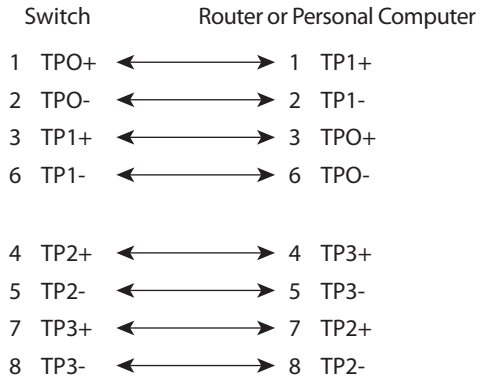


Figure 71 - Four Twisted-pair Straight-through Cable Schematics



When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable.

Use a straight-through cable to connect two ports when only one port is designated with an X. Use a crossover cable to connect two ports when both ports are designated with an X or when both ports do not have an X.

You can use Category 3, 4, or 5 cabling when connecting to 10BASE-T-compatible devices. You must use Category 5 cabling when connecting to 100BASE-TX-compatible devices.

IMPORTANT Use a four twisted-pair, Category 5 cable when connecting to a 1000BASE-T-compatible device or PoE port.

Figure 72 and Figure 73 show the cable schematics.

Figure 72 - Two Twisted-pair Crossover Cable Schematics

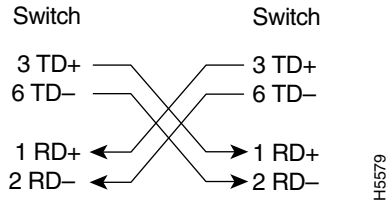
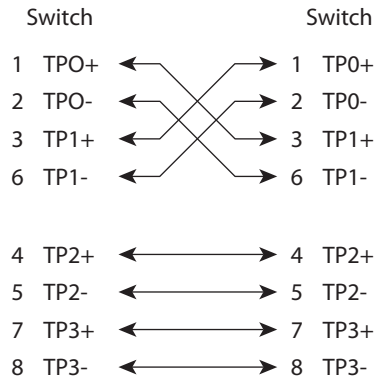


Figure 73 - Four Twisted-pair Crossover Cable Schematics

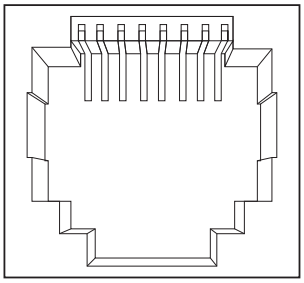


Dual-purpose Ports (combo ports)

The Ethernet port on a dual-purpose port uses standard RJ45 connectors. The following figure shows the pinouts.

Figure 74 - Ethernet Port RJ45 Connector

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



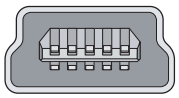
The SFP module slot on a dual-purpose port uses SFP modules for fiber-optic ports. The auto-MDIX feature is enabled by default.

Console Ports

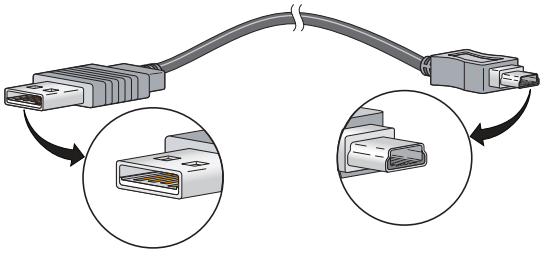
Console ports enable you to connect a switch to a computer if you use the Command-line interface (CLI) to configure and monitor a switch.

Stratix 5700 switches have these console ports:

- A USB 5-pin mini-Type B port on the front panel

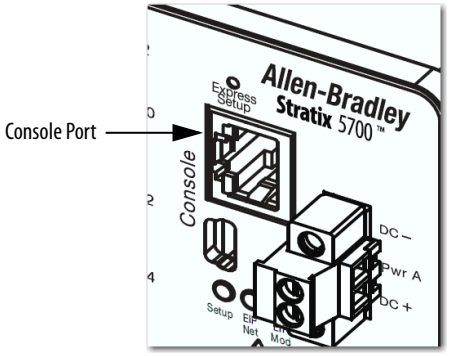


The USB console port uses a USB Type A to 5-pin mini-Type B cable. To use the USB cable, download the drivers for Microsoft Windows from http://www.rockwellautomation.com. The USB cable is not provided with the switch.



- RJ45 console ports on the front and rear panels

  Only one console port can be active at one time.



The following table lists the pinouts for the console port, the RJ45-to-DB-9 adapter cable, and the console device.

Table 171 - Pinouts with DB-9 Pin

Switch Console Port (DTE)	RJ45-to-DB-9 Terminal Adapter	Console Device
Signal	**DB-9 Pin**	**Signal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

The following table lists the pinouts for the console port, RJ45-to-DB-25 female DTE adapter, and the console device. The RJ45-to-DB-25 female DTE adapter is not supplied with the switch.

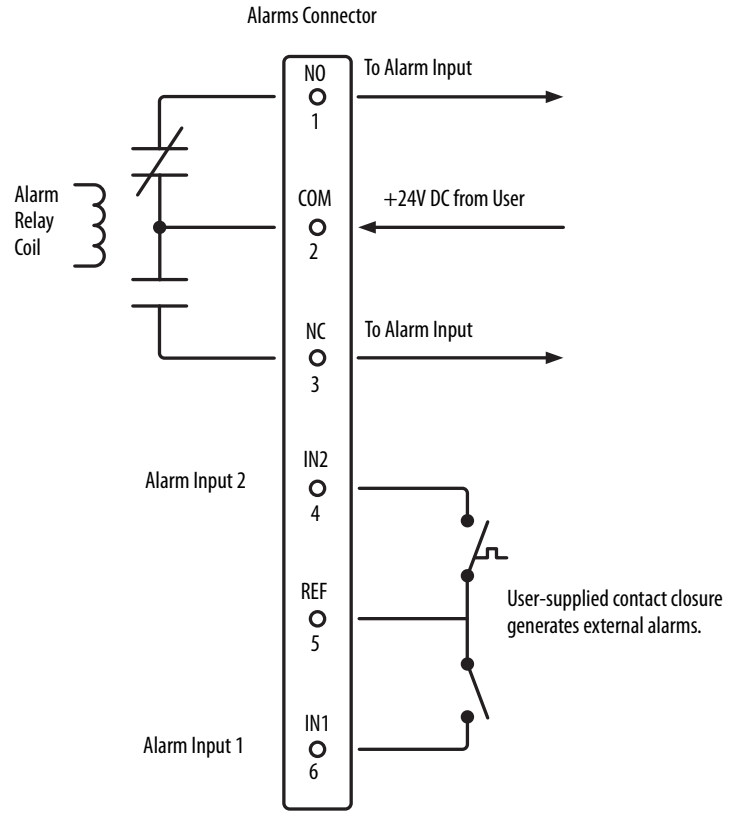
Table 172 - Pinouts with DB-25 Pin

Switch Console Port (DTE)	RJ45-to-DB-25 Terminal Adapter	Console Device
Signal	**DB-25 Pin**	**Signal**
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

Alarm Ports

The front-panel alarm-relay connector ports are described in the following illustration and table.

Figure 75 - Wiring Example for Alarm Inputs and Outputs



Label	Connection
NO	Alarm Output Normally Open (NO) connection
COM	Alarm Output Common connection
NC	Alarm Output Normally Closed (NC) connection
IN2	Alarm Input 2
REF	Alarm Input Reference Ground connection
IN1	Alarm Input 1

PoE Port Cable Specifications

For PoE ports, use a Category 5 (Cat 5) cable with a distance of up to 100 m (328 ft).

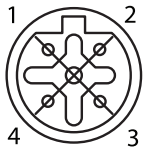
ArmorStratix 5700 Cables and Connectors

This section describes how to connect to ports on ArmorStratix 5700 switches. For connecting DC power to the power connector, see page 155.

10/100 Ports

The 10/100 Ethernet ports use M12 D-coded 4-pin connectors and Ethernet pinouts with twisted-pair crossovers or straight-through cables.

Figure 76 - 10/100 Connector Pinouts

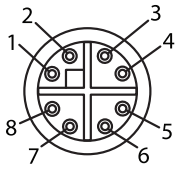


1	RD+
2	TD+
3	RD-
4	TD-

100/1000 Ports

The 100/1000 Ethernet ports use M12 X-coded 8-pin connectors and Ethernet pinouts with twisted-pair crossovers or straight-through cables.

Figure 77 - 100/1000 Connector Pinouts



1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DB-
5	BI_DD+
6	BI_DD-
7	BI_DC-
8	BI_DC+

Connect to 10BASE-T- and 100BASE-TX-Compatible Devices

The auto-MDIX feature is enabled by default. Follow these cabling guidelines when the auto-MDIX feature has been disabled.

When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as servers and routers, you can use a two or four twisted-pair, straight-through cable that is wired for 10BASE-T and 100BASE-TX.

To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side-by-side, with the tab at the back. The color of the wire that is connected to the pin on the outside of the left plug must differ in color from the wire that is connected to the pin on the inside of the right plug.

Figure 78 and Figure 79 show the cable schematics.

Figure 78 - Two Twisted-pair Straight-through Cable Schematics

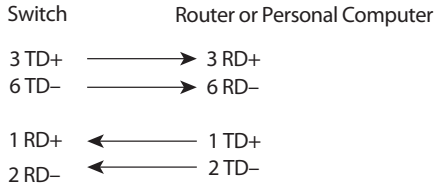
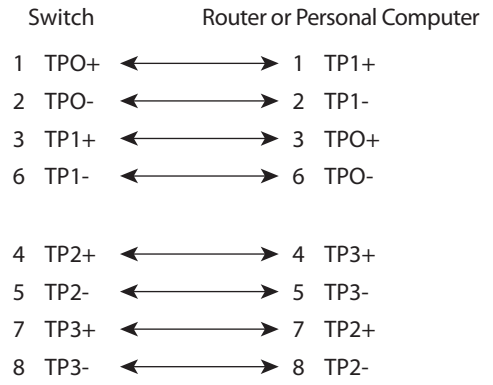


Figure 79 - Four Twisted-pair Straight-through Cable Schematics



When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable.

Use a straight-through cable to connect two ports when only one port is designated with an X. Use a crossover cable to connect two ports when both ports are designated with an X or when both ports do not have an X.

You can use Category 3, 4, or 5 cabling when connecting to 10BASE-T-compatible devices. You must use Category 5 cabling when connecting to 100BASE-TX-compatible devices.

IMPORTANT Use a four twisted-pair, Category 5 cable when connecting to a 1000BASE-T-compatible device or PoE port.

Figure 80 and Figure 81 show the cable schematics.

Figure 80 - Two Twisted-pair Crossover Cable Schematics

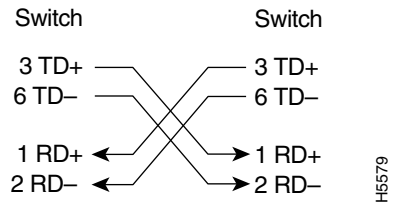
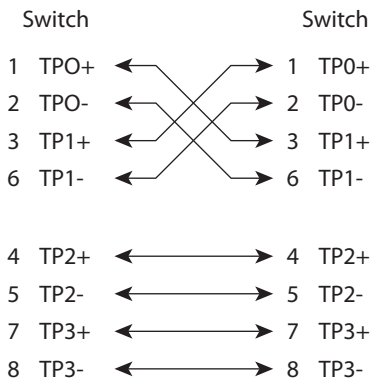


Figure 81 - Four Twisted-pair Crossover Cable Schematics



Console Port

ArmorStratix 5700 switches have one console port. The console port enables you to connect the switch to a computer if you use the Command-line interface (CLI) to configure and monitor the switch.

Connect to the console port with an M12-to-DB-9 cable (Figure 82):

- Obtain a male 5-pin DC Micro-style (M12) connector configuration cordset, such as Allen-Bradley Bulletin 889D.
- Obtain a DB-9 connector and attach it to one end of the cable.

Figure 82 - M12-to-DB-9 Cable

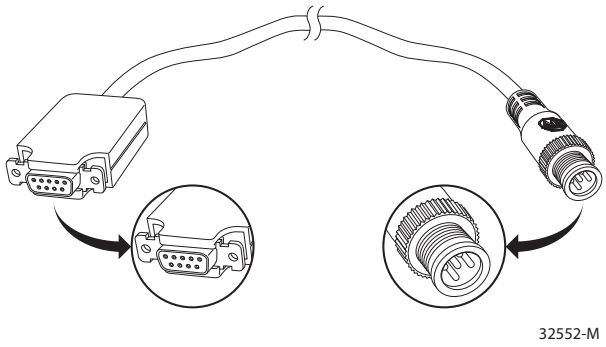
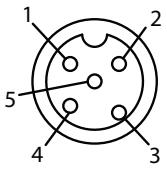
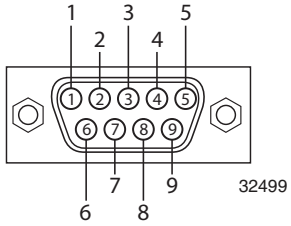


Figure 83 - Console Port Pinout



1	RTS
2	CTS
3	TXD
4	RXD
5	GND

Figure 84 - DB-9 Connector Pinout

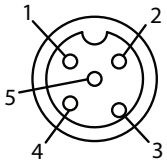


M8 Cable		DB9-S Connector	
Pin	**Function**	**Pin**	**Function**
1	RTS	8	CTS
2	CTS	7	RTS
3	TD	2	RD
4	RD	3	TD
5	GRND	5	GRND

Alarm Ports

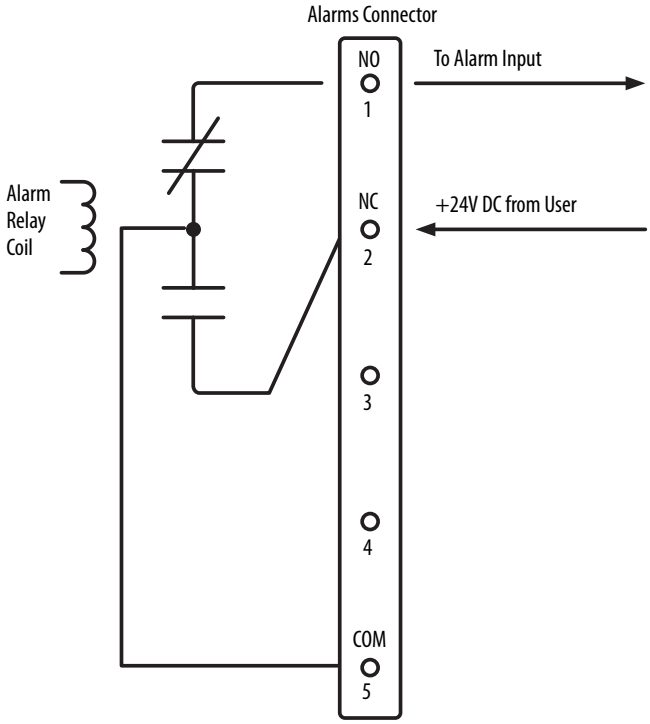
Alarm ports are included only on ArmorStratix 5700 switches with PoE. Figure 85 shows the front-panel alarm relay connector and ports. The alarm connector uses a male 5-pin DC Micro-style (M12) connector configuration cordset, such as Allen-Bradley Bulletin 889D.

Figure 85 - Alarm Connector Pinout



1	NO
2	NC
3	Unconnected
4	Unconnected
5	Common

Figure 86 - Wiring Example for Alarm Inputs and Outputs



Label	Connection
NO	Alarm Output Normally Open (NO) connection
NC	Alarm Output Normally Closed (NC) connection
Unconnected	Unconnected
Unconnected	Unconnected
COM	Alarm Output Common connection

PoE Port Cable Specifications

For PoE ports, use a Category 5 (Cat 5) cable with a distance of up to 100 m (328 ft).

Stratix 8000/8300 Cables and Connectors

This section describes how to connect to ports on Stratix 8000/8300 switches.

10/100 and 10/100/1000 Ports

The 10/100 and 10/100/1000 Ethernet ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

TIP The auto-MDIX feature is enabled by default.

Figure 87 - 10/100 Connector Pinouts

Pin	Label
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

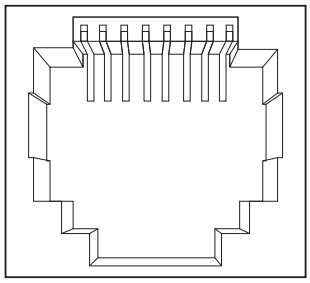
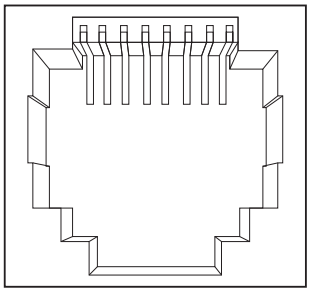


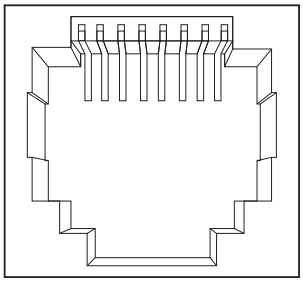
Figure 88 - 10/100/1000 Connector Pinouts

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



The PoE ports on the PoE expansion modules integrate power and data signals on the same wires. The ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

Figure 89 - 10/100 PoE Connector Pinouts and Power Sourcing Equipment (PSE) Voltage

Pin	Label	Alternative A (MDI)	1 2 3 4 5 6 7 8
1	RD+	Positive V PSE	
2	RD-	Positive V PSE	
3	TD+	Negative V PSE	
4	NC		
5	NC		
6	TD-	Negative V PSE	
7	NC		
8	NC		

Connect to 10BASE-T- and 100BASE-TX-compatible Devices

When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as servers and routers, you can use a two or four twisted-pair, straight-through cable that is wired for 10BASE-T and 100BASE-TX.

To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side-by-side, with the tab at the back. The color of the wire that is connected to the pin on the outside of the left plug must differ in color from the wire that is connected to the pin on the inside of the right plug.

Figure 90 and Figure 91 show the cable schematics.

Figure 90 - Two Twisted-pair Straight-through Cable Schematics

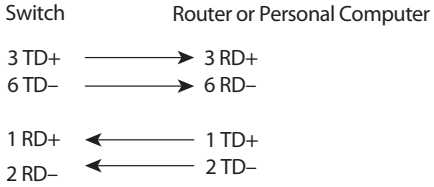
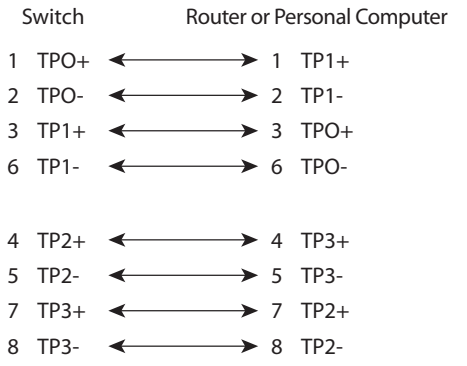


Figure 91 - Four Twisted-pair Straight-through Cable Schematics



When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable.

Use a straight-through cable to connect two ports only when one port is designated with an X. Use a crossover cable to connect two ports when both ports are designated with an X or when both ports do not have an X.

You can use Category 3, 4, or 5 cabling when connecting to 10BASE-T-compatible devices. You must use Category 5 cabling when connecting to 100BASE-TX-compatible devices.

IMPORTANT Use a four twisted-pair, Category 5 cable when connecting to a 1000BASE-T-compatible device or PoE port.

Figure 92 and Figure 93 show the cable schematics.

Figure 92 - Two Twisted-pair Crossover Cable Schematics

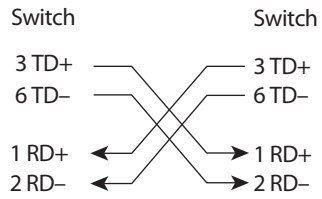
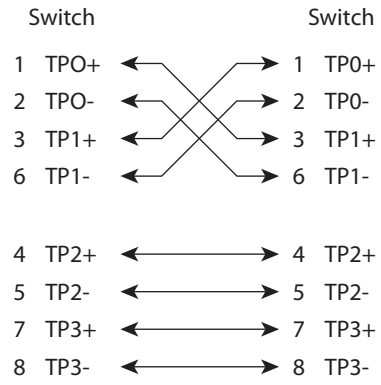


Figure 93 - Four Twisted-pair Crossover Cable Schematics

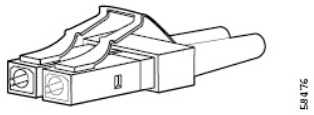


100Base-FX Ports

The 100Base-FX ports use the following:

- LC connectors, as shown in the following figure
- 50/125- or 62.5 /125-micron multimode fiber-optic cables

Figure 94 - Fiber-optic SFP Module LC Connector



ATTENTION: Invisible laser radiation can be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

SFP Transceiver Ports

The switch uses SFP transceivers for fiber-optic uplink ports.

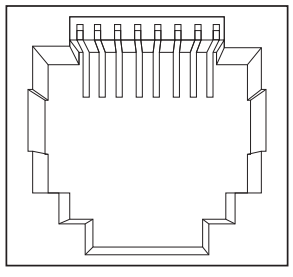
ATTENTION: Invisible laser radiation can be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

Dual-purpose Ports

The Ethernet port on a dual-purpose port uses standard RJ45 connectors. The following figure shows the pinouts.

Figure 95 - Ethernet Port RJ45 Connector

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



The SFP module slot on a dual-purpose port uses SFP modules for fiber-optic ports.

IMPORTANT The auto-MDIX feature is enabled by default.

Console Port

The console port enables you to connect the switch to a computer if you use the Command-line interface (CLI) to configure and monitor the switch.

The console port uses an 8-pin RJ45 connector. The supplied RJ45-to-DB-9 adapter cable connects the console port of the switch to a computer. Obtain an RJ45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal.

Table 173 lists the pinouts for the console port, the RJ45-to-DB-9 adapter cable, and the console device.

Table 173 - Pinouts with CB-9 Pin

Switch Console Port (DTE)	RJ45-to-DB-9 Terminal Adapter	Console Device
Signal	**DB-9 Pin**	**Signal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

The following table lists the pinouts for the console port, RJ45-to-DB-25 female DTE adapter, and the console device.

The RJ45-to-DB-25 female DTE adapter is not supplied with the switch.

Table 174 - Pinouts with DB-25 Pin

Switch Console Port (DTE)	RJ45-to-DB-25 Terminal Adapter	Console Device
Signal	**DB-25 Pin**	**Signal**
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

PoE Port Cable Specifications

For PoE ports, use a Category 5 (Cat 5) cable with a distance of up to 100 m (328 ft).

Notes:

Numerics

10/100 ports
- cable lengths 75, 130
- connecting to 93, 124, 152

10/100/1000 ports
- cable lengths 75, 102, 130
- connecting to 93, 124, 152

A

access Device Manager 48

ACLs 184 . . . 189

adapter pinouts
- RJ45-to-DB-25 adapter 539
- RJ45-to-DB-9 adapter 538
- terminal
  - RJ45-to-DB-25 521, 527
  - RJ45-to-DB-9 521, 527

address aliasing 252

address translation 254

airflow around switch 160

airflow, required clearance 102

alarm relay connections 91, 92, 150, 151
- connection procedures 92, 151

alert log 392

allocation, memory 30

announce interval 206

assign VLANs to NAT instance 260

Auto mode, PoE 316

auto-MDIX 94, 125, 153, 537

autonegotiation 93, 124, 152
- Duplex mode 52
- speed 52
- troubleshoot 422

B

Boundary mode 194, 197

broadcast storms 309

C

cable diagnostics 392

cables
- connect to 10BASE-T and 100BASE-TX compatible devices 535
- connect to console port 538
- connect to copper ports 180
- connect to dual-purpose ports 537
- connect to dual-purpose uplink ports 181
- connect to fiber ports 182, 537
- connect to PoE ports 95, 154, 180
- console 162
- crossover
  - four twisted-pair pinout, 1000BASE-T ports 519, 525, 531
  - identifying 518, 524, 530
  - using 518, 524, 531
- damaged 419
- detect with auto-MDIX 77, 104, 133, 163
- Ethernet and fiber 419
- identify 535
- PoE module specifications 539
- straight-through
  - two twisted-pair pinout 518, 524, 530
  - using 518, 524, 530

cabling
- auto-MDIX 94, 125, 153

CIP
- data 45
- enable on VLAN 40
- network connections 19

clearance 75, 102, 131, 160

CLI
- access via console port 70
- access via SSH 40, 70

clock modes
- Boundary 194, 205
- End to End Transparent 195, 207
- Forward 195, 207
- NTP-PTP 195, 208

CompactFlash card 182

connect
- Direct Managed mode 423
- properties 57
- to 10/100/1000 ports 93, 124, 152
- to DC power 79, 83, 107, 134, 139
- to external alarm devices 90, 92, 123, 149, 151
- to SFP modules 95, 126, 155

connectors and cables
- 10/100/1000 518, 524, 530, 531, 535, 536
- console 521, 527, 538, 539
- dual-purpose 525, 537
- SC connectors 537
- SFP module ports 537

console port
- specifications 521, 527, 538, 539

crossover cable
- pinout
  - four twisted-pair, 1000BASE-T ports 519, 525, 531
- pinouts 536

cryptographic IOS software 212

customization
- DHCP persistence 241
- DHCP server 238, 243
- IP address
  - DHCP IP address pool 240
  - switch port 241, 242
- IP address (for connected devices) 238, 241, 243
- Smartport roles 350

D

DC power 134, 139

DC power, connect to 79, 83, 107

default gateway
NAT 255, 266, 278, 289
default router 240
default VLAN 353, 365
delay request interval 206
denial-of-service attack 309
Device Manager
access 48
hardware requirements 47
overview 47
software requirements 47
Device-level ring. *See* DLR
DHCP
clients 405
for ring devices 222
IP address pool 239
persistence 241
server 238
status 405
troubleshoot 421
Direct Managed mode 423
DLR
configure via Device Manager 226
configure via Logix Designer application 230
considerations 216
DHCP 222, 235
overview 212
redundant gateways 217, 234
status 406
DNS server1 and 2 240
domain name 240
dual-purpose ports
connectors and cables 525, 537
Duplex mode
default 52
setting 52
troubleshoot 422

E

EIGRP 332 . . . 337
electrical noise, avoiding 75, 102, 131, 160
electrostatic discharge 74, 100, 135, 161
End to End Transparent mode 195, 199, 207
EtherChannels
configure via Device Manager 246
configure via Logix Designer application 247
example 245
overview 244
EtherNet/IP CIP interface 19
EtherNet/IP protocol 350, 403
EtherNet/IP QuickConnect technology 19
expansion modules
installation 164
explicit messaging 19
Express Setup
button 32
global macro 44
Long Press mode 37
Medium Press mode 36
modes 34
Multi-mode 34
requirements 30
Short Press mode 35
Single-mode 38
external alarms 178

F

factory default settings 37, 426
firmware upgrade, troubleshoot 427
Forward mode 195, 201
front panel
clearance 75, 102, 131, 160
Full-duplex mode 52
functional ground lug warning 81, 138

G

global macros
for CIP traffic 44
for motion traffic 44, 249
grounding procedures 81, 82, 137, 139

H

Half-duplex mode 52
hardware features 22
hardware requirements
Device Manager 47
high priority PoE ports 314
horizontal stacking
stacking, horizontal 250

I

IEEE power classifications 315
IGMP snooping
and address aliasing 252
definition 252
implicit messaging 19
installation
attach the power and relay connector 85, 93, 124, 143, 152
DIN rail 80, 136
expansion modules 164
grounding procedures 81, 82, 137, 139
mount Stratix 5410 on a rack 107
mount Stratix 5410 on a wall 111
POST 79, 107, 134, 135
pre-installation information and guidelines 75, 102, 131
procedure 76, 103, 131, 160
required clearance 102, 160
verify switch operation 79, 107, 134
wire relays 90, 92, 123, 149, 151

IOS software
cryptographic 212
non-cryptographic 212
IP address
customization
connected devices 238, 243
DHCP IP address pool 240
switch port 241, 242
DHCP IP address pool
ending range 240
starting range 240
switch port 242
assigning 242
deleting 242
modifying 242
translation 254
troubleshoot 421
DHCP 421
wrong IP address 421

L

LC connector 537
lease length 240
link integrity, verify with REP 328
lite versus full firmware 20
locate switch
via Device Manager 374
via Logix Designer application 389
Long Press mode Express Setup
overview 34
run 37
low priority PoE ports 314

M

macros
default global 248
Motion Prioritized QoS 248
QoS Priority Map 248
QoS Priority Queue 248
management interface 47
NAT 261
management VLAN 43, 365
Medium Press mode Express Setup
overview 34
requirements 30
run 36
memory 30
MIBs, supported 348
mismatch prevention, Smartport roles 351
mode
Access 350
Boundary 194, 197, 205
DHCP Server 238
Direct Managed 423
DLR 226, 227
dual power 191
End to End Transparent 195, 199, 207
EtherChannel 245, 246
Express Setup 34
Forward 195, 201, 207
NTP-PTP Clock 195, 202, 208
PoE 316, 321, 324
REP 329
Restrict 304
Spanning Tree Learning 79, 107, 134
STP 362, 364
Trunk 350
module-defined data types 429
monitor
alert log 392
CIP 403
DHCP clients 405
DLR 406
port diagnostics 412
port mirroring 301
PRP 410
Motion Prioritized QoS macro 248
multicast storm 309
Multi-mode Express Setup
overview 34
requirements 30

N

NAT
configuration considerations 261
configuration overview 254
configure via Device Manager Web interface 262 . . . 273
configure via Logix Designer application 274, 285, 286
definition 254
diagnostics 396, 399 . . . 402
management interface 261
traffic permits and fixups 262, 273, 285
translation entry types 259
network address translation. *See* NAT
network settings
configure via Device Manager 39
configure via Logix Designer application 42
noise, electrical 75, 102, 131, 160
NTP
configure via Device Manager 295
overview 295
NTP-PTP Clock mode 195, 202, 208

O

OSPF 337 . . . 343
Overview tab, dashboard 395

P

parts list 76, 103, 132, 162
pinouts
- 10/100 ports 537
- crossover cables 536
  - four twisted-pair, 1000BASE-T ports 519, 525, 531
- PoE 523, 535
- RJ45-to-DB-25 adapter 539
- RJ45-to-DB-25 terminal adapter 521, 527
- RJ45-to-DB-9
  - adapter 538
  - terminal adapter 521, 527
- SFP module 537
- straight-through cables
  - two twisted-pair 518, 524, 530, 535

PoE
- attach power connector 178
- cable specifications 539
- configure via Device Manager Web interface 314
- connect to port 180
- features 314 . . . 319
- initial power allocation 315
- pinouts 523, 535
- power connector 132, 162
- power management modes 316
- powered device detection 315
- wire DC power source 144, 174

pool name 242
pop-up blockers 48, 423
port
- assignments for CIP data 487, 495
- configuration 59
- dual-purpose 96, 155
- numbering 52
- roles 352
- security 303, 304
- status 391
- threshold 311
- thresholds 312
- type 329

port mirroring
- configure via Device Manager 302
- overview 301

port settings
- auto-MDIX 52
- description 52
- descriptions of 51
- Duplex mode 52
- enable/disable 52
  - default 52
- speed 52
  - default 52

POST
- description 79, 107, 134
- results 79, 107, 134

power 79, 107
- connect to
  - DC 83

power and relay connector
- connecting to the switch 85, 93, 124, 143, 152

power classifications 315
power priority 321
prevent electrostatic discharge 74, 100, 135, 161
proxy settings 48, 423
PRP
- configure Device Manager 298
- overview 297
- status 410

PTP
- configure via Device Manager 196
- configure via Logix Designer application 204

PTP modes
- Boundary 194, 205
- End to End Transparent 195, 207
- Forward 195, 207
- NTP-PTP Clock 195, 208

Q

Qos Priority Map macro 248
QoS Priority Queue macro 248
QoS settings
- default 44, 248
- motion traffic 248

QuickConnect technology 19

R

rear panel
- clearance 75, 102, 131, 160

Receive Detail tab, dashboard 395
recovery
- firmware upgrade 427
- switch software 426

redundancy
- EtherChannel 246

redundant gateway 217 . . . 221, 230, 406, 408
relays
- wire 92, 151

removing SFP modules 89, 122, 148
REP 325
- open segment 326
- ring segment 327
- segments
  - characteristics 327
- verify link integrity 328

REP Admin VLAN 329
REP segments 325
- configure 329

reset factory defaults 426
reset, troubleshoot 425
Resilient Ethernet Protocol
- see REP 325

restart with factory default settings 37
RJ45 connector, console port 538
RSLinx software 44

RSTP
features 362
RSWho 44

S

SC connector 537
SD card
install or remove 78, 105, 133
synchronize
configuration 65
synchronize IOS files 65
SD Flash Sync 67
SDM template 345
security
configure for ports 304
violations 304
segment ID 329
segment topology change notices
See also STCNs 330
settings, factory default 37
SFP modules
bale-clasp latch removal 89, 122, 148
connect to 95, 126, 155
connectors 537
Short Press mode Express Setup
overview 34
run 35
Single-mode Express Setup
run 38
Smartport roles
applying 352
changing VLAN memberships 353
customization 353
optimize ports 350
mismatch prevention 351
Smartport roles and VLANs 358
SNMP
configuring 349
MIBs supported 348
snooping, DHCP 222, 228, 236
snooping, IGMP 252
software features 21
customization
DHCP persistence settings 241
DHCP server settings 238, 243
Smartport roles 350
troubleshoot
firmware upgrade 68
software requirements
Device Manager 47
Spanning Tree Protocol 325
See also Rapid Spanning Tree Protocol
specifications 13
speed
setting 52
troubleshoot 422
SSH, enable 41, 70
Static mode, PoE 317
STCN interface 330
STCN segment 330
STCN STP 330
storm control
described 309
thresholds 309
straight-through cable
pinout
two twisted-pair 10/100 ports 518, 519, 524, 525, 530, 531, 535, 536
Stratix switch families 18
subnet mask
DHCP IP address pool 240
subnet translation 259, 266, 270, 272, 276, 280
switch
configuration properties 58
installation
attach PoE power connector 178
CompactFlash card 182
connect to copper ports 180
connect to dual-purpose uplink ports 181
connect to PoE port 180
DC power and relay connector 177
expansion modules 164
ground 171
mount on DIN rail 166
mount on wall or panel 168
parts list 76, 103, 132, 162
procedure 76, 103, 131, 160
tools 77, 104, 132, 163
troubleshoot 418
wire DC power source 172
wire external alarms 178
manage via Device Manager 47
monitor
alert log 392
port mirroring 301
reset to factory defaults 426
status 388
troubleshoot 417
Device Manager display 421
Device Manager not accessible 421
Device Manager problems 421
DHCP 421
Direct Managed mode 423
firmware upgrade 427
IP address problems 421
reset switch 425
switch software 426
wrong IP address 421
verify operation 79, 134
switch software, troubleshoot 426
sync interval 206
sync limit 206

T

Telnet 70
threshold
port 311
traffic level 309

time synchronization
configure via Device Manager 196
configure via Logix Designer application 204
timing message settings 196, 204
traffic fixups and NAT 262, 273, 285
traffic permits and NAT 262, 273, 285
traffic suppression 309
translate IP addresses 254
translation entry types 259
Transmit Detail tab, dashboard 395
troubleshoot
Device Manager display 421
Device Manager not accessible 421
DHCP 421
Direct Managed mode 423
firmware upgrade 68, 427
IP address problems 421
reset switch 425
speed, duplex, and autonegotiation 422
switch 417
switch performance 422
switch software 426
wrong IP address 421

U

unicast storm 309
upgrade firmware 68

V

verify switch operation 79, 107, 134
VLAN memberships
changing 353
prerequisite 353
VLANs
assign to NAT instance 260, 265, 269, 276, 279
default VLAN 365
enable CIP 40
grouping different users 367
isolate traffic 367
management VLAN 365

Rockwell Automation Support

Use the following resources to access support information.

Technical Support Center	Knowledgebase Articles, How-to Videos, FAQs, Chat, User Forums, and Product Notification Updates.	https://rockwellautomation.custhelp.com/
Local Technical Support Phone Numbers	Locate the phone number for your country.	http://www.rockwellautomation.com/global/support/get-support-now.page
Direct Dial Codes	Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.	http://www.rockwellautomation.com/global/support/direct-dial.page
Literature Library	Installation Instructions, Manuals, Brochures, and Technical Data.	http://www.rockwellautomation.com/global/literature-library/overview.page
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	http://www.rockwellautomation.com/global/support/pcdc.page

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

Rockwell Automation maintains current product environmental information on its website at http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

Allen-Bradley, ArmorStratix, Rockwell Automation, Rockwell Software, RSLinx, RSLogix 5000, RSNetWorx, Stratix, Studio 5000, and Studio 5000 Logix Designer are trademarks of RockwellAutomation, Inc.

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

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

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-UM007F-EN-P - September 2016
Supersedes Publication 1783-UM007E-EN-P - June 2016

Copyright © 2016 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.