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

by ROCKWELL AUTOMATION

User Manual

Original Instructions

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 11
About This Publication 11
Inclusive Terminology 11
Summary of Changes 11
Additional Resources 12

Chapter 1

About the Switches

Stratix Managed Switches 14
Stratix 5700 Lite Versus Full Firmware Features 15
Software Features 16
Hardware Features 18
Memory Allocation 20

Chapter 2

Get Started

Express Setup Overview 23
Express Setup Requirements 23
Express Setup Button 24
Multimode Express Setup 26
Run Multimode Express Setup in Short Press Mode 27
Run Multimode Express Setup in Medium Press Mode 28
Run Multimode Express Setup in Long Press Mode 29
Singlemode Express Setup 30
Configure Network Settings via Device Manager 31
Apply the PnP Setup Mode 31
Apply the Express Setup Configuration 33
Configure Network Settings via the Logix Designer Application 36
Default Global Macro 38
Linx-based Software and Network Who Support 38
Electronic Data Sheet (EDS) Files 38
Data Accessible with CIP 39
Configuration via Device Manager 40
Access Device Manager 41
Configure Port Settings 45
Configuration via the Studio 5000 Environment 47
General Properties 48
Connection Properties 50
Switch Configuration 51
Port Configuration 52
Port States during Program Mode and Connection Faults 54
User Administration via Device Manager 55

Configuration Files 56
Manage Configuration Files via Device Manager 56
Manage Configuration Files via the Logix Designer Application 57
Secure Digital (SD) Card 58
Synchronize the SD Card via Device Manager 58
Synchronize the SD Card via the Logix Designer Application 62
CompactFlash Memory Card 63
Firmware Updates 63
Cisco Network Assistant 65
Command-line Interface 65
Connect to the Console Port 65
Enable SSH or Telnet in Device Manager 66
FactoryTalk Network Manager 66

Chapter 3

Configure Switch Features

Authentication, Authorization, and Accounting (AAA) 68
Configure AAA via Device Manager 68
Server/Server Groups Tab 69
TACACS+ Subtab 69
RADIUS Subtab 71
Server Groups Subtab 72
AAA Methods 74
AAA Interface 83
Access Control Lists (ACLs) 84
Configure ACLs via Device Manager 85
Alarms 88
Configure Alarms via Device Manager 88
CIP Sync Time Synchronization (Precision Time Protocol) 93
IEEE 1588 Power Profile 93
Power 2017 Profile 94
Boundary Mode 94
DSCP Values for PTP 95
End to End Transparent Mode 96
Peer to Peer Transparent Mode 96
Forward Mode 96
NTP-PTP Clock Mode 96
Configure Time Synchronization via Device Manager 97
Configure Time Synchronization via the Logix Designer Application 105
View Time Sync Information in the Logix Designer Application 110

Cryptographic IOS 111
Device Level Ring (DLR) Topology 112
DLR Requirements and Restrictions 113
DLR Features. 113
DLR Port Choices 114
Configure DLR via Device Manager 115
Configure DLR via the Logix Designer Application 118
Configure a Switch as a Ring Supervisor and DHCP Server 124
DLR VLAN Trunking 125
Configure DLR VLAN Trunking via Device Manager 125
Dynamic Host Configuration Protocol (DHCP) Persistence 126
Configure DHCP Persistence via Device Manager 128
Configure DHCP Persistence via the Logix Designer Application 131
Enhanced Interior Gateway Routing Protocol (EIGRP) 135
Configure EIGRP via Device Manager 136
EtherChannels. 139
Configure EtherChannels via Device Manager. 142
Configure EtherChannels via the Logix Designer Application . . . 145
Feature Mode. 147
Global Navigation Satellite System (GNSS) 148
GNSS Hardware. 148
GNSS Software. 148
GNSS Signaling 149
GNSS Considerations 149
Configure GNSS. 150
High-availability Seamless Redundancy (HSR). 150
Horizontal Stacking. 150
Hot Standby Router Protocol (HSRP) 153
HSRPv1-Version 1. 153
HSRPv2-Version 2 153
Configure HSRP via Device Manager 154
HSR-HSR (Quadbox) 155
Internet Group Management Protocol (IGMP) Snooping with Querier 156
Configure IGMP Snooping with Querier via Device Manager . . . 157
Internet Protocol Device Tracking (IPDT) 158
Configure IPDT via Device Manager. 158
Link Layer Discovery Protocol (LLDP) 159
Configure LLDP 160
Maximum Transmission Unit (MTU) 160
Configure the MTU via Device Manager 161
Motion Prioritized QoS Macros 162
Configure Motion Prioritized QoS Macros via Device Manager 162

NetFlow 163
NetFlow Templates 164
Configure NetFlow via Device Manager 165
Apply a NetFlow Configuration via Device Manager 166
Network Address Translation (NAT) 167
Configuration Overview 167
VLAN Assignments 173
Configuration Considerations 174
Traffic Permits and Fixups 174
Configure NAT via Device Manager 175
Configure NAT via the Logix Designer Application 185
Configure NAT via the Logix Designer Application (Stratix 5410 Switches) 195
View Address Translations in Linx-based Software 201
Network Time Protocol (NTP) 202
Configure NTP in Device Manager 203
Configure NTP via the Logix Designer Application 204
Open Shortest Path First (OSPF) Routing Protocol 206
Configure OSPF via Device Manager 207
Parallel Redundancy Protocol (PRP) 211
RedBox PRP Channel Groups 212
Traffic and Supervisory Frames 213
Node and VDAN Limitations 213
Configuration Considerations 213
Configure a RedBox via Device Manager 214
Troubleshoot PRP via Device Manager 217
View PRP configuration via the Logix Designer Application 217
PRP Channel Groups 218
Port Mirroring 219
Configure Port Mirroring in Device Manager 219
Port Security 220
Dynamic Secure MAC ID 221
Static Secure MAC ID 221
Enhanced Port Security 221
Security Violations 222
Configure Port Security via Device Manager 222
Configure Port Security via the Logix Designer Application 223
Port Thresholds 226
Incoming (storm control) 226
Outgoing (rate limiting) 227
Default Port Thresholds Configuration 227
Configure Port Thresholds via Device Manager 228
Configure Port Thresholds via the Logix Designer Application 228

Power over Ethernet (PoE) 231
Powered Device Detection and Initial Power Allocation 232
Power Management Modes 233
Configure PoE Ports via Device Manager 237
Configure PoE via the Logix Designer Application 239
PROFINET 241
Configure PROFINET Traffic Forwarding 241
Configure a Stratix 5700 or ArmorStratix 5700 Switch for PROFINET Management 243
Verify the GSD File 245
Monitor and Maintain PROFINET 245
Resilient Ethernet Protocol (REP) 246
REP Open Segment 247
REP Ring Segment 248
Access Ring Topologies 248
Link Integrity 249
Configure REP via Device Manager 250
Resilient Ethernet Protocol (REP) Negotiated 251
Configure REP Negotiated via Device Manager 251
Routing, Layer 3 253
Routing, Static and Connected 254
Reallocate Switch Memory for Routing via Device Manager 255
Enable and Configure Routing via Device Manager 256
Simple Network Management Protocol (SNMP) 257
Supported MIBs 258
Configure SNMP via Device Manager 261
Use SNMP Management Applications 261
Smartports 262
Custom Smartport Roles 263
Avoid Smartport Mismatches 263
Configure Smartports via Device Manager 264
Assign Smartports and VLANs via the Logix Designer Application 270
Spanning Tree Protocol (STP) 272
Configure STP via Device Manager 273
Configure STP via the Logix Designer Application 276
Utility Features 277
GOOSE Messaging Support 277
SCADA Protocol Classification 277
IEEE 1588 Power Profile 277
Virtual Local Area Networks (VLANs) 277
Management VLAN 278
Configure VLANs via Device Manager 279
Configure VLANs via the Logix Designer Application 280
VLAN 0 Priority Tagging 281
802.1Q Tagging 281
Native VLANs 281
VLAN 0 Priority Tagging and Priority Values 281
Configure VLAN 0 Priority Tagging 282

Monitor the Switch

Chapter 4

Switch Status via Device Manager 283
Front Panel 284
Switch Information 294
Switch Health 294
Port Utilization 295
Switch Status via the Logix Designer Application 296
Port Status 299
System Log Messages 300
Trends 301
Port Statistics 302
NAT Statistics 303
Monitor NAT Statistics via Device Manager 303
Monitor NAT Statistics via the Logix Designer Application 306
NetFlow 309
REP Status 311
CIP Status 311
DHCP Clients 313
DLR Status 313
Monitor DLR Status via Device Manager 314
Monitor DLR Status via the Logix Designer Application 316
PRP Status 317
PTP Serviceability 320
Messages 320
Errors 321
History 322
Histogram 323
STP Status 325
Port Diagnostics 327
Neighbors 329
Cable Diagnostics 330
Diagnose Cables via Device Manager 330
Diagnose Cables via the Logix Designer Application 331

Chapter 5

Troubleshoot the Switch

Troubleshoot the Installation 333
- Switch POST Results 333
- POST Results with a Terminal 334
- Bad or Damaged Cable 334
- Ethernet and Fiber Cables 334
- Link Status 335
- SFP Module Issues 335
- Port and Interface Settings 335

Verify Boot Fast 336
Troubleshoot IP Addresses 336
Troubleshoot Device Manager 336
Troubleshoot Switch Performance 337
Restart or Reset the Switch 337
- Restart or Reset the Switch from Device Manager 338
- Reset the Switch via the Express Setup Button 338
- Restart the Switch from the Logix Designer Application 338

Troubleshoot a Firmware Update 339
Collect System and Configuration Information for Technical Support . 339

Appendix A

Data Types

Stratix 5400 Data Types 342
- 8-port Switches 342
- 12-port Switches 343
- 12-port Gigabit Switches 345
- 16-port Switches 347
- 16-port Gigabit Switches 349
- 20-port Switches 351
- 20-port Gigabit Switches 353

Stratix 5410 Data Types 356
Stratix 5700 and ArmorStratix 5700 Data Types 360
- 6-port Gb Switches 360
- 6-port Switches 361
- 8-port Switches 362
- 10-port Gb Switches 363
- 10-port Switches 365
- 16-port Switches 366
- 20-port Gb Switches 368
- 18-port Gb Switches 370
- 20-port Gb Switches 373
- 20-port Switches 375
- 24-port Switches 378

Stratix 8000 and 8300 Data Types 381

Appendix B

Port Assignments for CIP Data

Stratix 5400 Port Assignments 387
Stratix 5410 Port Assignments 388
Stratix 5700 Port Assignments 389
ArmorStratix 5700 Port Assignments 390
Stratix 8000 and 8300 Port Assignments 390

Appendix C

Port Numbering

Stratix 5400 Port Numbering. 393
Stratix 5410 Port Numbering 398
Stratix 5700 Port Numbering. 399
ArmorStratix 5700 Port Numbering. 404
Stratix 8000 and 8300 Port Numbering 406

Appendix D

Cables and Connectors

Stratix 5410 Cables and Connectors 409
- 10/100/1000 Ports. 409
- Connect to 10BASE-T- and 100BASE-TX-compatible Devices . . . 410
- Console Ports 412
- Alarm Port 414
- Ethernet, PoE Port Cable Specifications 414

Stratix 5400 and 5700 Cables and Connectors. 415
- 10/100 and 10/100/1000 Ports 415
- Connect to 10BASE-T- and 100BASE-TX-compatible Devices . . . 416
- Dual-purpose Ports (combo ports). 418
- Console Ports 419
- Alarm Ports 421
- PoE Port Cable Specifications. 421

ArmorStratix 5700 Cables and Connectors 422
- 10/100 Ports. 422
- 100/1000 Ports 422
- Connect to 10BASE-T- and 100BASE-TX-compatible Devices . . . 423
- Console Port 424
- Alarm Ports 426
- PoE Port Cable Specifications. 426

Stratix 8000/8300 Cables and Connectors 427
- 10/100 and 10/100/1000 Ports 427
- Connect to 10BASE-T- and 100BASE-TX-compatible Devices . . . 428
- 100Base-FX Ports. 429
- SFP Transceiver Ports. 430
- Dual-purpose Ports 430
- Console Port 431
- PoE Port Cable Specifications. 431

Index 433

About This Publication

This publication describes how to set up, configure, and troubleshoot Stratix® switches.

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

Inclusive Terminology

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology.

We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Summary of Changes

This manual contains new and updated information.

Topic	Page
Stratix 5700 Lite Versus Full Firmware Features	15
Software Features	16
Source Wildcard	86
Dest Wildcard	86
A stack of switches must meet these minimum requirements:	151
Hot Standby Router Protocol (HSRP)	153
Wiring Example for Alarm Inputs and Outputs	421

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 specifications for the switches and other devices.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001	Represents a collaborative development effort from Rockwell Automation and Cisco Systems. The design guide is built on, and adds to, design guidelines from the Cisco Ethernet-to-the-Factory (EttF) solution and the Rockwell Automation Integrated Architecture™. The design guide focuses on the manufacturing industry.
Stratix 5400 Ethernet Managed Switches Installation Instructions, publication 1783-IN014	Describes how to install the switches.
Stratix 5410 Ethernet Managed Switches and Power Supply Installation Instructions, publication 1783-IN015	
Stratix 5700 Ethernet Managed Switches Installation Instructions, publication 1783-IN016	
ArmorStratix 5700 Ethernet Managed Switches Installation Instructions, publication 1783-IN017	
Stratix 8000 and 8300 Ethernet Managed Switches Installation Instructions, publication 1783-IN012	
Ethernet Design Considerations Reference Manual, publication ENET-RM002	Describes how to implement a system based on the EtherNet/IP™ platform.
Device Manager web interface online help (provided with the switch)	Provides context-sensitive information on how to configure and use the switch.
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.

About the Switches

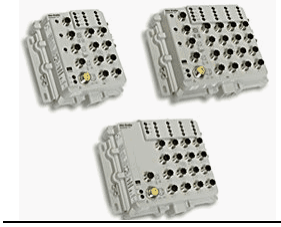
Topic	Page
Stratix Managed Switches	14
Stratix 5700 Lite Versus Full Firmware Features	15
Software Features	16
Hardware Features	18
Memory Allocation	20

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.

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.

Stratix Managed Switches

The following table describes the Stratix managed 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, 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.

Stratix 5700 Lite Versus Full Firmware Features

The following table lists the features available for Stratix 5700 Full versus 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 205 on page 399.

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
VLAN Trunk Protocol (VTP)	VTP versions 1 2, and 3	VTP versions 1, 2, and 3
EtherChannel (link aggregation)		•
Port Threshold (Storm control and traffic shaping)		•
IPv6 support		•
Access Control Lists (ACL)		•
Routing, static and connected		•
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 (SPAN)	•	•
RSPAN		•
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 114	

Software Features

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

- See Configuration via Device Manager on page 40
- See Configuration via the Studio 5000 Environment on page 47

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

Table 1 - Software Features

Feature	Switches	Device Manager	Logix Designer Application
Authentication, Authorization, and Accounting (AAA)	Stratix 5400 switches Stratix 5410 Stratix 5700 switches ArmorStratix 5700 switches	Yes	No
Access Control Lists (ACLs)	All	Yes	No
Alarms	All	Yes	No
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 and 8300 switch base units (PTP traffic can be only forwarded through expansion modules)	Yes	No
Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) neighbor monitoring	Stratix 5400 switches Stratix 5410 switches Stratix 5700 switches ArmorStratix 5700 switches Stratix 8000 switches	Yes	No
Device Level Ring (DLR) topology	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	Yes	No
Dynamic Host Configuration Protocol (DHCP) Persistence	All	Yes	Yes
DHCP for ring devices	Stratix 5400 switches Stratix 5700 switches ArmorStratix 5700 switches	Yes	Yes
Enhanced Interior Gateway Routing Protocol (EIGRP)	Stratix 5400 switches with Layer 3 firmware Stratix 5410 switches with Layer 3 firmware Stratix 8300 base units	Yes	No
EtherChannels	All	Yes	No
Global Navigation Satellite System (GNSS)	Stratix 5410 series B switches with IOS release 15.2(6)E0a and later	No	No
Generic Object Oriented Substation Events (GOOSE) Messaging Support	Stratix 5400 switches	No	No
Horizontal stacking	Stratix 5410 switches: 1783-IMS28NAC, 1783-IMS28RAC, 1783-IMS28NDC, 1783-IMS28RDC	No	No
High-availability Seamless Redundancy (HSR)	Stratix 5400 switches	No	No
HSR-HSR (Quadbox)	Stratix 5400 switches	No	No
IEEE 1588 Power Profile	Stratix 5400 switches	Yes	No
Internet Group Management Protocol (IGMP) Snooping with Querier	All	Yes	No
Internet Protocol Device Tracking (IPDT)	Stratix 5400 switches Stratix 5410 switches Stratix 5700 switches ArmorStratix 5700 Switches	Yes	No
MACsec	Stratix 5400 switches Stratix 5410 switches	No	No
Maximum transmission unit (MTU)	All	Yes	No

Table 1 - Software Features (Continued)

Feature	Switches	Device Manager	Logix Designer Application
Motion prioritized QoS macros	Stratix 5400 switches Stratix 5410 switches Stratix 5700 switches with Full firmware ArmorStratix 5700 switches	Yes	No
Multimode Express Setup	All	Yes	Yes
NetFlow	Stratix 5400 switches Stratix 5410 switches	Yes	No
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	Yes	Yes
Network Time Protocol	All	Yes	Yes
Parallel Redundancy Protocol (PRP)	Stratix 5400 switches Stratix 5410 switches	Yes	Yes
Port mirroring (SPAN)	All	Yes	No
Port security	All	Yes	Yes
Port thresholds	All	Yes	Yes
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 and 8300 expansion modules: 1783-MX04E, 1783-MX04T04E	Yes	Yes
PROFINET	All switches support PROFINET traffic forwarding and VLAN 0 priority tagging Stratix 5700 and ArmorStratix switches support PROFINET management via General Station Description (GSD) files	No	No
Resilient Ethernet Protocol (REP)	All	Yes	No
Routing, Layer 3	Stratix 5400 switches with Layer 3 firmware Stratix 5410 switches with Layer 3 firmware Stratix 8300 base units	Yes	No
Routing, static and connected	All	Yes	No
RSPAN	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 and 8300 switch base units (PTP traffic can be only forwarded through expansion modules)	No	No
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	Yes	No
Supervisory Control and Data Acquisition (SCADA)	Stratix 5400 switches	No	No
Simple Network Management Protocol (SNMP)	All	Yes	No
Smartports	All	Yes	Yes
Spanning Tree Protocol (STP)	All	Yes	Yes
TrustSec	Stratix 5400 switches Stratix 5410 switches	No	No
Virtual local area networks (VLANs)	All	Yes	Yes
VLAN 0 priority tagging	All	Yes	No

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 2 on page 18.
- For Stratix 5410 switches, see Table 3 on page 19.
- For supported SFP modules, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Table 2 - Hardware Features for Stratix 5400, Stratix 5700, ArmorStratix 5700, and Stratix 8000/8300 Switches

Feature	Description
Power and relay connectors	To 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. The relays can be activated for environmental, power supply, and port status alarm conditions. An alarm can be configured 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), any alarm condition can be associated 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 fails, 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, USB-RJ45, or 9300-USBCBL-CNSL 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 424. • Stratix 8000/8300 switches—Connect to the console port with an RJ45-to-DB-9, USB-RJ45 or 9300-USBCBL-CNSL 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. The copper RJ45 ports can be set to operate at 10 Mbps, 100 Mbps, or 1000 Mbps, full-duplex, or half-duplex. They can be configured as fixed 10 Mbps, 100 Mbps, or 1000 Mbps (Gigabit) Ethernet ports, and the duplex setting can be configured. 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. **IMPORTANT:** Copper SFP modules cannot be used in dual-purpose (combo) ports.
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-Mbps, 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.
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 3 - 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 through which you can connect four alarm inputs and one alarm output for environmental, power supply, and port status conditions. Also, 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, USB-RJ45 or 9300-USBCBL-CNSL 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 231, 238, and 240. 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	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 navigation satellite system (GNSS)	Requires Stratix 5410 series B switches with IOS release 15.2(6)E0a and later. Stratix 5410 series B switches have a built-in GNSS receiver that enables the switch to determine its own location and get an accurate time from a satellite constellation. The switch can then become the Grandmaster clock for time distribution in the network. For more information about GNSS, see page 148. The GPS status indicator on the front panel of the switch provides GNSS status as described on page 289.
Inter-Range Instrumentation Group (IRIG) time codes	Not available in the current release.
Time of day (ToD) synchronization	Not available in the current release.

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 the following templates.

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

Table 4 - Stratix 5400 Templates

Feature	Memory Allocation			
	IPv4 Default	Dual IPv4/IPv6 Default	IPv4 Routing	Dual IPv4/IPv6 Routing
Unicast MAC IDs	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 5 - Stratix 5410 Layer 2 Firmware Model Template

Feature	Memory Allocation
Unicast MAC IDs	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 the following templates.

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

Table 6 - Stratix 5410 Layer 3 Firmware Model Templates

Feature	Memory Allocation			
	Default	Dual-default	IPv4 Routing	Dual-routing
Unicast MAC IDs	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
- LAN base Routing
- Dual IPv4 and IPv6

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 7 - Stratix 5700 and ArmorStratix 5700 Templates

Feature	Memory Allocation		
	Default	LAN Base Routing	Dual IPv4 and IPv6
Unicast MAC IDs	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
- LAN base Routing

For static and connected routing, or if you have more than 180 IGMP groups or multicast routes, you can use the LAN base 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.

Stratix 8000 and ArmorStratix 8300 Templates

Feature	Memory Allocation	
	Default	LAN Base Routing
Unicast MAC IDs	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	23
Multimode Express Setup	26
Singlemode Express Setup	30
Configure Network Settings via Device Manager	31
Configure Network Settings via the Logix Designer Application	36
Default Global Macro	38
Linx-based Software and Network Who Support	38
Configuration via Device Manager	40
Configuration via the Studio 5000 Environment	47
User Administration via Device Manager	55
Configuration Files	56
Secure Digital (SD) Card	58
CompactFlash Memory Card	63
Firmware Updates	63
Cisco Network Assistant	65
Command-line Interface	65

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 37.

Express Setup Requirements

Multimode and singlemode versions of Express Setup are available depending on your switch and IOS release:

- With IOS release **15.2(4)EA3 or later**, all switches use multimode Express Setup as described on page 26.
- With IOS release **15.2(4)EA or earlier**, all switches use singlemode Express Setup as described on page 30.

Multimode 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.

Table 8 - Hardware and Software Requirements

Component	Requirement
Hardware	
Processor	1 GHz or faster 32 bit (x86) or 64 bit (x64)
RAM	1 GB RAM (32-bit) or 2 GB RAM (64-bit)
Hard disk space	16 GB (32-bit) or 20 GB (64-bit)
Software	
Operating system	Windows 7
Web browser	• Internet Explorer 10 and later • Firefox 48 and later • Chrome 62 and later
Computer-to-switch connection (Singlemode Express Setup or multimode 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:

- Singlemode Express Setup or multimode 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 domain name system (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.

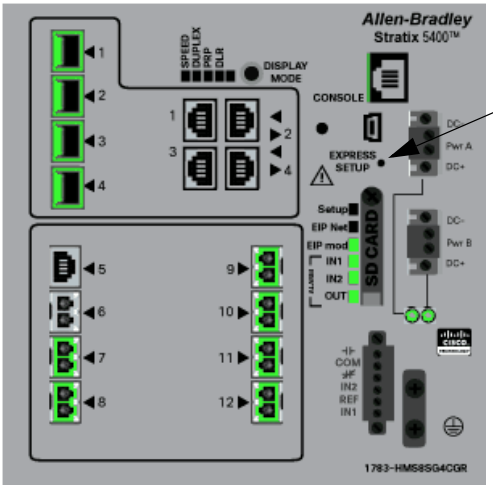
- For Stratix 5700 or ArmorStratix 5700 switches, make sure that the SD card is **not** inserted.

Express Setup Button

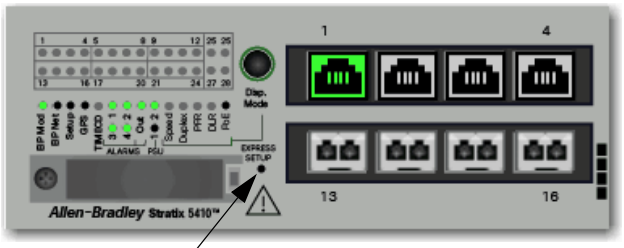
Use the Express Setupbutton on the physical switch to perform Express Setup. This Express Setup button is recessed behind the panel. To reach the button, use a small tool, such as a paper clip.

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

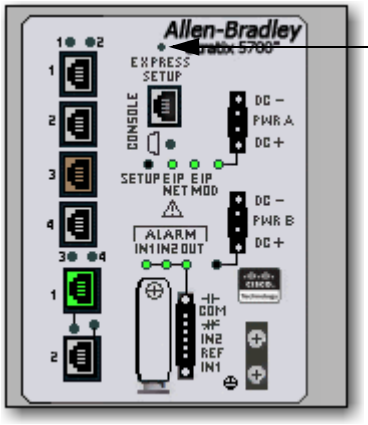
Stratix 5400 Switch



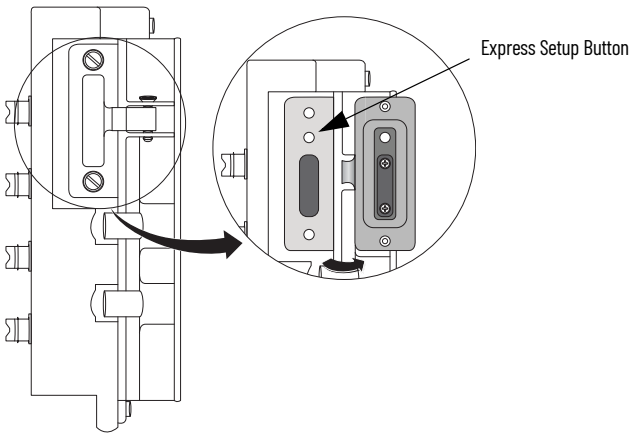
Stratix 5410 Switch



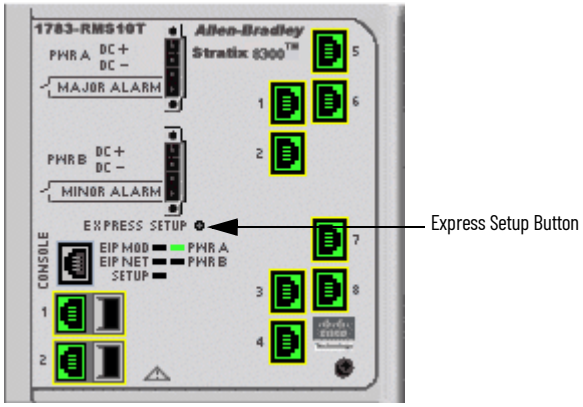
Stratix 5700 Switch



ArmorStratix 5700 Switch



Stratix 8000/8300 Switch



Multimode Express Setup

Multimode 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 27.
- 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 28.
- Long Press mode—You want to reset the switch to use factory default settings. To run Long Press mode, see page 29.

Table 9 summarizes the function of each mode.

Table 9 - Multimode 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 alternates between 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. • DHCP returns the IP address that VLAN 1 is configured with. • The default login credentials are set to the following: – User name: [no user name/blank] – Password: **switch** • CIP™ (Common Industrial Protocol) 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 Multimode 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 multimode 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 flash 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...5, and then release.

   The switch selects a port to use for Express Setup.

4. Connect a Category 5 Ethernet cable from the switch port that flashes 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 that is connected to the computer changes from a green flash to steady 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 multimode Express Setup is different than the IP address for singlemode Express Setup.

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

5. Proceed to Configure Network Settings via Device Manager on page 31.

Run Multimode 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 that is configured to assign the switch an IP address. You can configure a switch to be a DHCP server as described on page 117.

To run multimode 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 flash 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 indicator 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 following occurs:
   - 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.
   - DHCP returns the IP address that VLAN 1 is configured with.
   - 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 31.
   - To complete the configuration via the Logix Designer application, see page 36.

Run Multimode 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.

Singlemode Express Setup

To run singlemode 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 flash 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 multimode 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 switch port that flashes 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 31.

Configure Network Settings via Device Manager

You can apply one of the following setup modes to the switch after you run Express Setup as described on page 23:

- Express Setup—Enables the switch to operate as a managed switch with a default configuration that supports industrial automation applications. Express Setup is the default setup mode.
- Plug-n-Play (PnP)—allows the switch to be configured by a PNP server on the network.

  Configure PnP server settings to enable the switch to send a work request to a PnP server for further device configuration. The PnP agent is a software application on the switch. When the switch is first powered on, the embedded PnP agent discovery process wakes in the absence of the startup configuration file and attempts to discover the PnP server address. The PnP agent uses methods like DHCP and DNS to acquire the PnP server IP address. Once a server is found and the connection is established, the agent performs activities, such as configuration, image, license, and file updates by communicating with the server.

  If an auto discovery mechanism is not available, you can use the PnP configuration option from Express Setup to configure the initial switch settings and PnP server information.

Apply the PnP Setup Mode

To apply the PnP setup mode to the switch, follow these steps.

1. Access Device Manager as described on page 41.

   If the Express Setup page 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 popup blockers are disabled on your browser.
   - Verify that any wireless interface is disabled on the computer.
2. From the Select device initial setup mode pull-down menu, choose PnP.
3. Complete the fields as described in Table 10 and click Submit.

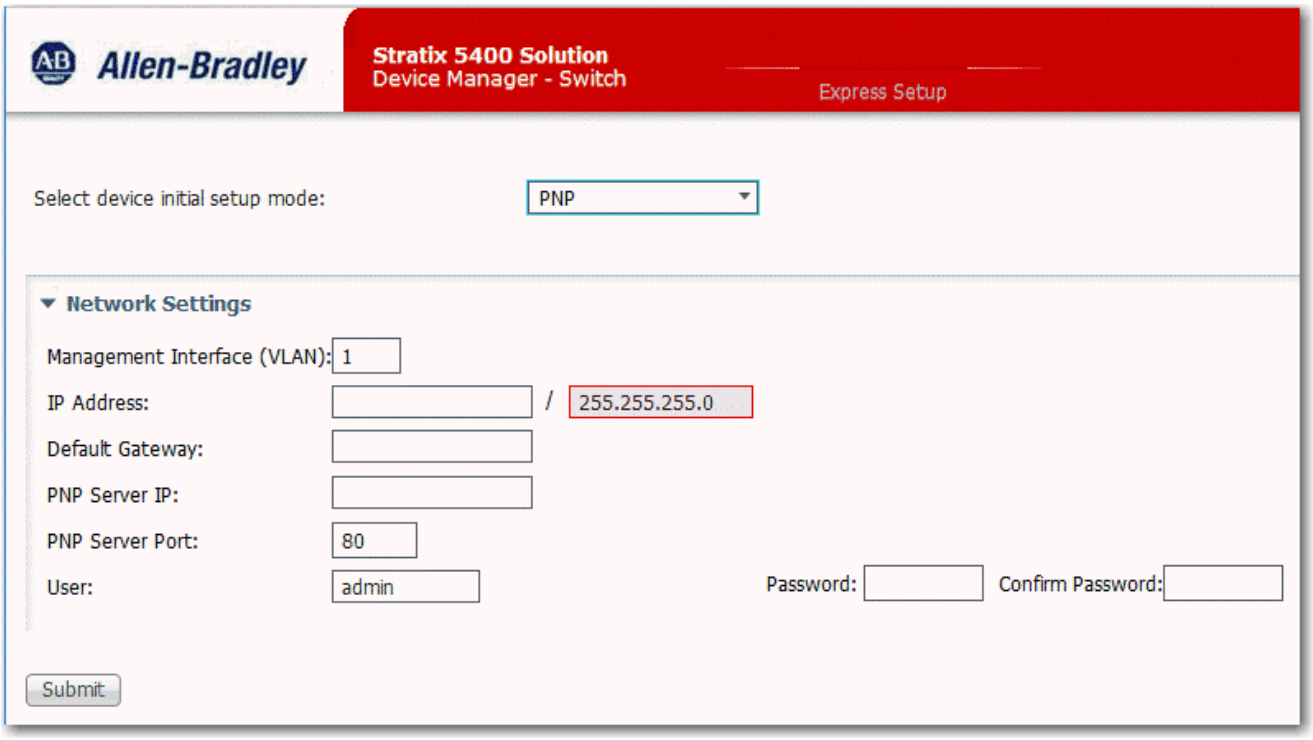


Table 10 - PNP Mode Fields

Field	Description
Management Interface (VLAN)	The 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. The management VLAN provides broadcast control and security for management traffic that must be limited to a specific group of users. The management VLAN also provides secure administrative access to all devices in the network. Choose a VLAN as the management VLAN. The default management VLAN ID is 1. **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 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. Make sure that the IP address that you assign to the switch is not being used by another device in your network.
Default Gateway	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, leave this field blank. 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.
PNP Server IP	The IP address of the PnP server.
PNP Server Port	The port number to use to connect to the PnP server.
User	Enter the user name for the switch.
Password, Confirm Password	The password for the switch: • Can have a max of 63 alphanumeric characters • Can start with a number • Is case-sensitive • Can have embedded spaces • Cannot be one digit • Cannot contain a question mark or a tab • Cannot have spaces at the beginning or the end The default password is **switch**. However, to complete initial setup, you must change the default password. 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.

Apply the Express Setup Configuration

To apply the Express Setup configuration to the switch, follow these steps.

1. Access Device Manager as described on page 41.

   If the Express Setup page 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 popup blockers are disabled on your browser.
   - Verify that any wireless interface is disabled on the computer.
2. From the Select device initial setup mode pull-down menu, choose Express Setup.
3. Complete the fields as described in Table 11.

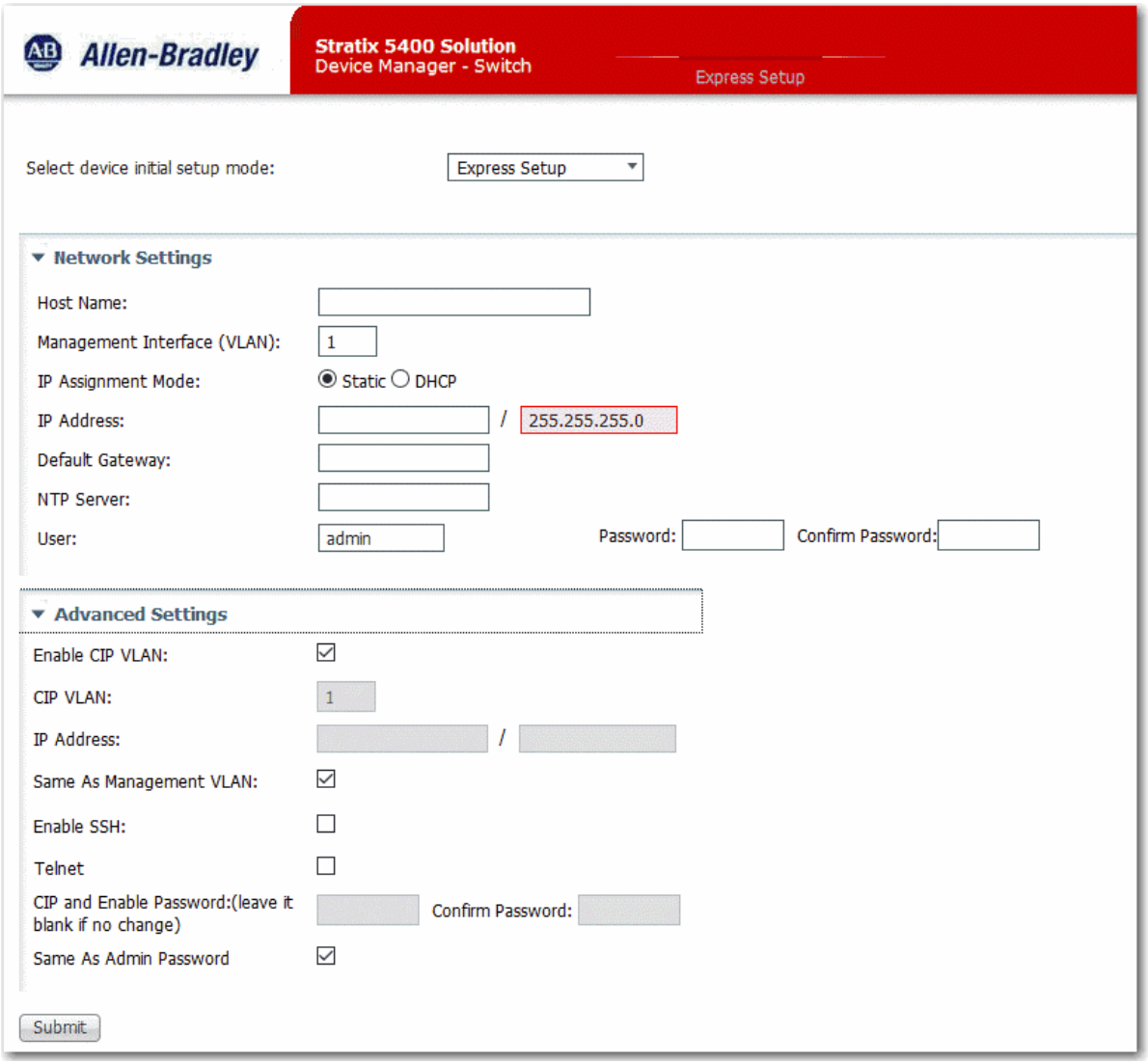


Table 11 - Express Setup Mode Fields

Field	Description
Network Settings	
Host Name	The name of the switch.
Management Interface (VLAN)	The 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. The management VLAN 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. The management VLAN 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 singlemode Express Setup: 1...1001 Valid IDs for multimode 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 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, confirm that the IP address is not within the address range 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 multimode Express Setup in Medium Press mode, the IP address field displays the address that is 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. Be 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	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 for the switch. The default value is admin.
Password, Confirm Password	The password for the switch: • Can have up to 63 alphanumeric characters • Can start with a number • Is case-sensitive • Can have embedded spaces • Cannot be one digit • Cannot contain a question mark or a tab cannot contain spaces at the beginning or the end To complete initial setup, you must change 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 Enable CIP VLAN to enable CIP on a VLAN. You can specify the settings that are required for CIP or check the Same As Management VLAN checkbox.
CIP VLAN	The VLAN on which 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 CIP 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 Same As Management VLAN checkbox to make the settings for the CIP VLAN the same as the management VLAN.
Enable SSH	Check SSH to enable Secure Shell (SSH) sessions on the switch. SSH must be enabled to securely access the switch via the command-line interface (CLI). For more information about the CLI, see page 65.

Table 11 - Express Setup Mode Fields (Continued)

Field	Description
Telnet	Check Telnet to enable Telnet. You can use Telnet to access the switch via the command-line interface (CLI). For more information about the CLI, see page 65. Telnet uses the local account user name and password. **IMPORTANT:** We recommend that you use SSH instead of Telnet for access to the switch. SSH provides more security for remote connections than Telnet by providing strong encryption.
CIP and Enable Password, Confirm Password	Enter the CIP and Enable password, or leave this field blank if you do not want to change the password. Reenter the password to confirm.
Same As Admin Password	Check Same As Admin Password to set the password that is used for CIP to the same user password specified under Network Settings.

4. Click Submit.

   The switch initializes its configuration for typical industrial EtherNet/IP™ applications by running the global macro as described on page 37. You can then log on to Device Manager for further configuration or exit the application.

5. 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.

6. If you used singlemode Express Setup or multimode 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.
7. For Stratix 5400 and 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 58.
   - To synchronize the SD card via the Logix Designer application, see page 62.

After initial 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, access the Express Setup page from the Admin menu in Device Manager.

Configure Network Settings via the Logix Designer Application

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

1. Add the switch to a controller project as described on page 47.
2. Configure general properties as described page 48.

   Be sure to specify the IP address that is 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.

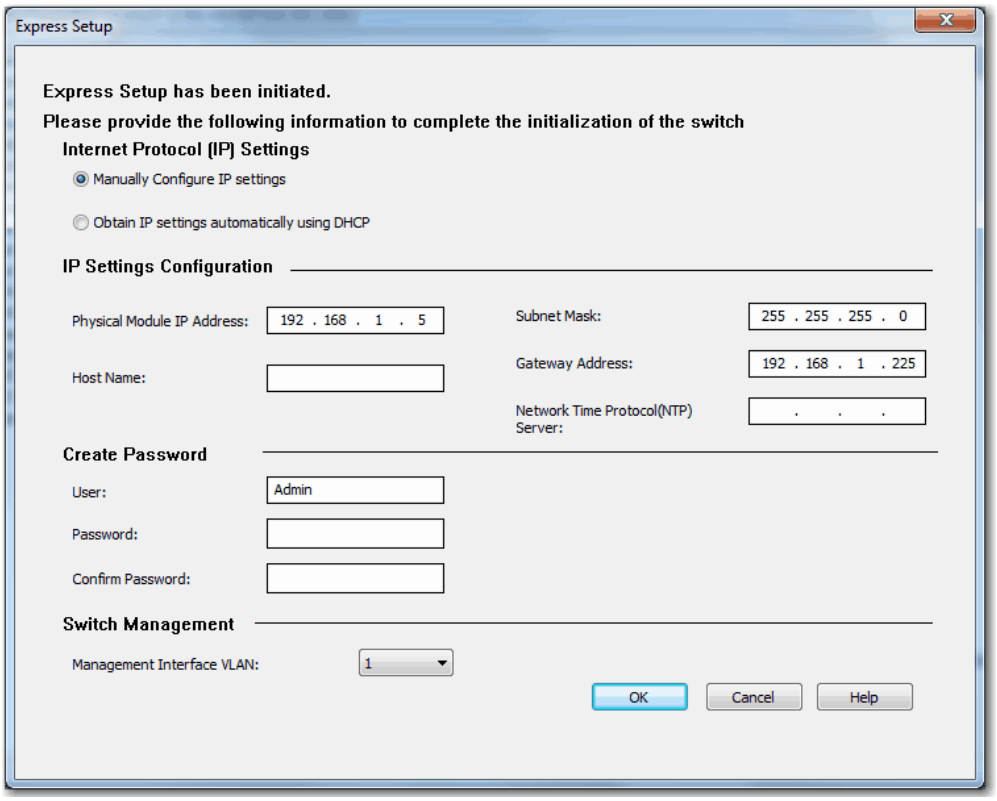


Table 12 - Express Setup Fields

Field	Description
Internet Protocol (IP) Settings	Click the method to use for assigning the switch an IP address: • Manually Configure IP settings (default)—The switch uses a manually assigned, static IP address. If you manually assign the switch IP address on a DHCP-server network, confirm 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 by 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 that is 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.
Subnet Mask	Displays the IP address that is 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).

Table 12 - Express Setup Fields (Continued)

Field	Description
Gateway Address	Displays the gateway address that is 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	Enter the user name for the switch. The default value is admin.
Password, Confirm Password	The password for the switch: • Can have up to 63 alphanumeric characters • Can start with a number • Is case-sensitive • Can have embedded spaces • Cannot be one digit • Cannot contain a question mark or a tab • Does not allow spaces at the beginning or the end The default password is 'switch.' To complete initial setup, you must change 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. The management VLAN 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. The management VLAN 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 37. You can perform for further configuration or close 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 62.

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
- Configure CIP settings based on the options chosen in Express Setup
- 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 that is 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 162.

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 65, to run the global macro.

Linx-based 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 Linx-based software RSWho function. RSWho enables you to locate and identify your switch on the network by using the electronic data sheet (EDS) files. CIP must be enabled on the switch to use this feature.

To access the RSWho function, from the Linx-based 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:

- Linx-based software
- Studio 5000® programming environment
- RSNetWorx for EtherNet/IP software

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

- By downloading it from The Product Compatibility and Download Center (PCDC).
- By using the EDS Hardware Installation tool included in the Studio 5000 environment.

Data Accessible with CIP

The CIP interface lets you access the information in Table 13.

Table 13 - 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
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 ID 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

Table 13 - Data Accessible with CIP (Continued)

Data Type	Details
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, 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 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:

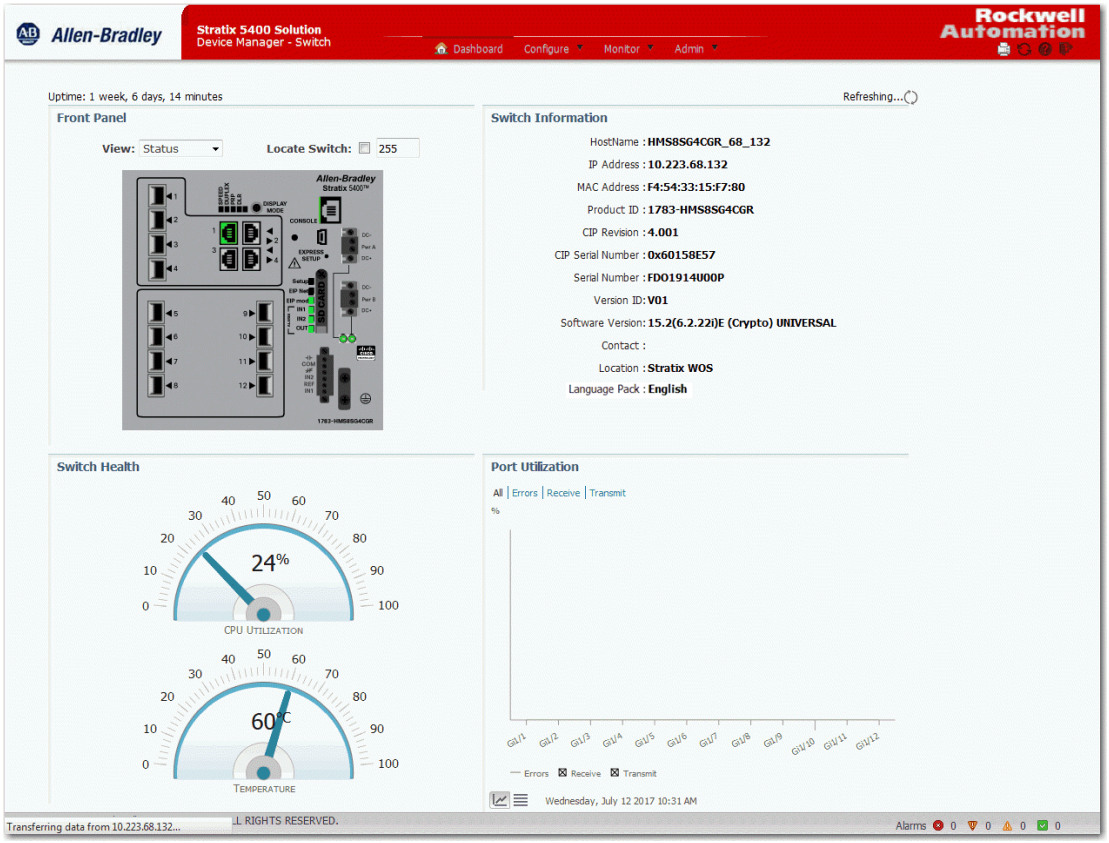
- Displays real-time views of switch configuration and performance
- Simplifies configuration tasks with features such as Smartports
- Uses graphical, color-coded displays, such as the front panel view and animated indicators to simplify monitoring tasks
- Provides alert tools to help you identify and solve networking problems

Table 14 - 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 drive space	16 GB (32 bit) or 20 GB (64 bit)
Number of colors	256
Resolution	1024 x 768
Font size	Small

Table 15 - Device Manager Software Requirements

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



Access Device Manager

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

To make sure that Device Manager runs properly, disable any popup blockers or proxy settings in your browser. Device Manager verifies the browser version when starting a session to be sure that the browser is supported.

IMPORTANT With IOS release 15.2(6)E0a and later, Device Manager has an auto-logout feature:

- If you upgrade to IOS release 15.2(6)E0a and use the Express Setup process, Device Manager automatically logs you out if you are inactive for 20 minutes or longer.
- If you reset the switch to factory defaults or configure it via the CLI instead of Express Setup, Device Manager automatically logs out after 3 minutes of inactivity.

To configure the inactivity timeout value for Device Manager sessions, use the following CLI command:

ip http session-idle-timeout [seconds]

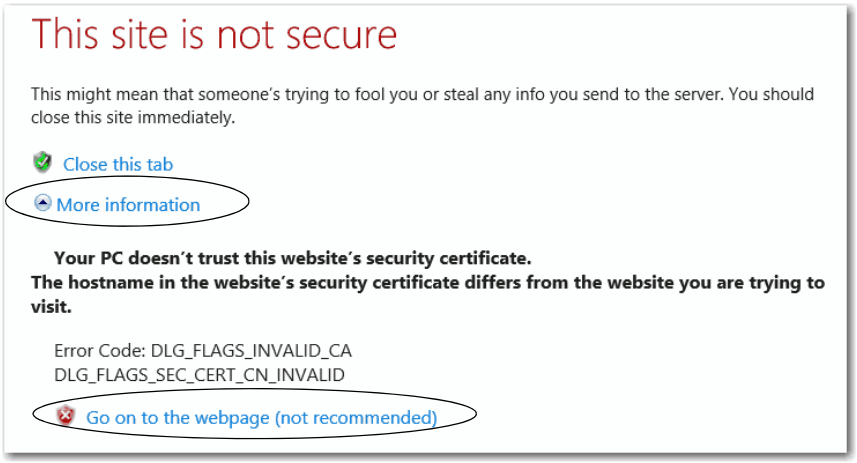
Example: ip http session-idle-timeout 1200

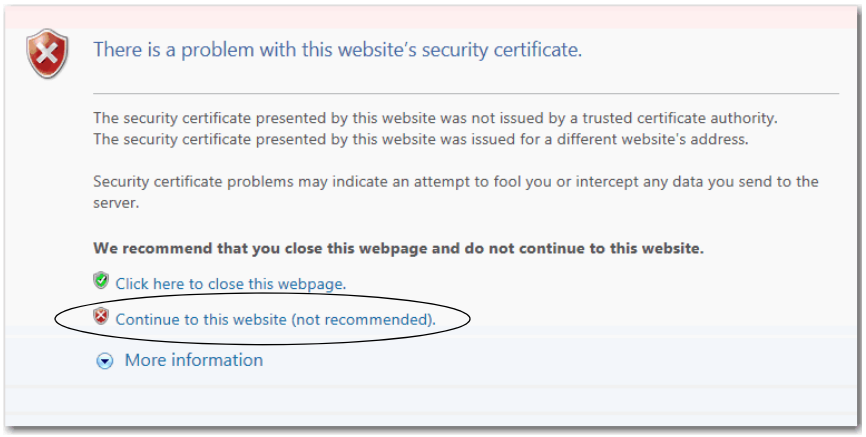
To access Device Manager, follow these steps.

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

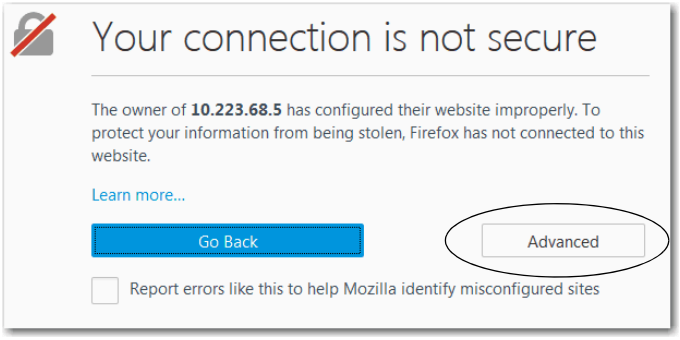
IMPORTANT If you configured bookmarks for accessing previous versions of Device Manager, be sure to recreate new bookmarks. Addresses that end with /homed.shtml do not provide the latest login authentication method.

2. (Internet Explorer). If one of the following messages appears, click the links circled in the following images to proceed to Device Manager.

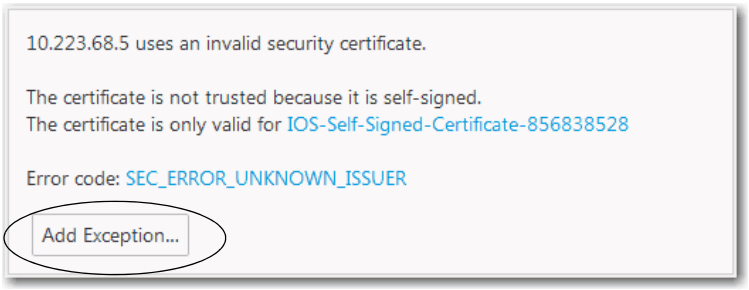




3. (Firefox). If the following message appears, do the following:
   a. Click Advanced.

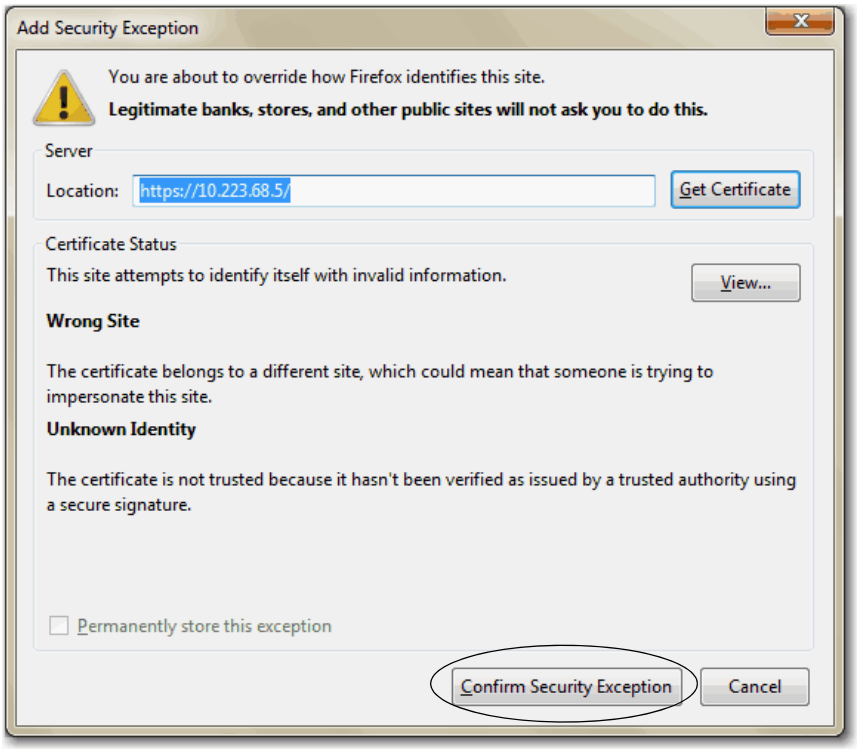


b. Click Add Exception.

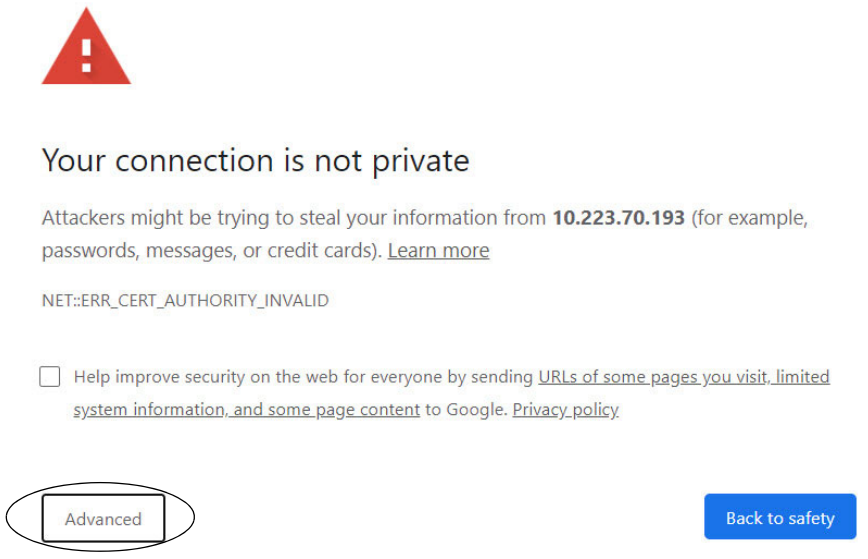


c. Click Confirm Security Exception.

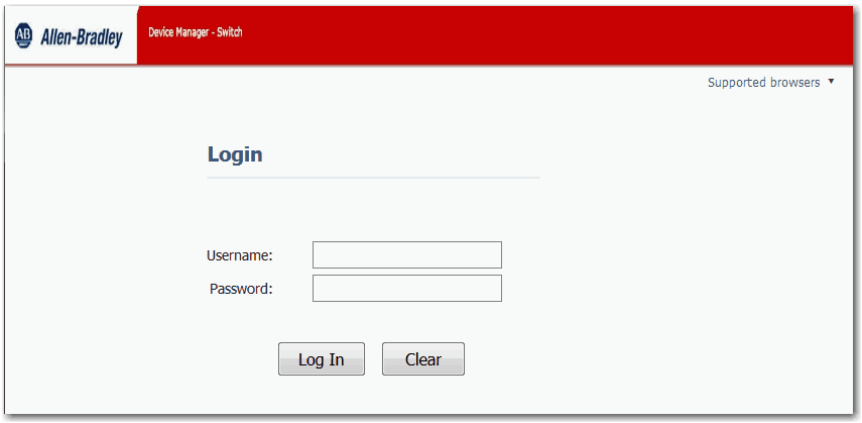
IMPORTANT Do not check Permanently store this exception. Permanent storage of the exception can cause issues to arise.



4. (Chrome). If the following messages appears, click Advanced to proceed to Device Manager.



5. On the Login page, enter the switch user 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. You can also configure port settings in the Logix Designer application, as described on page 52.

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

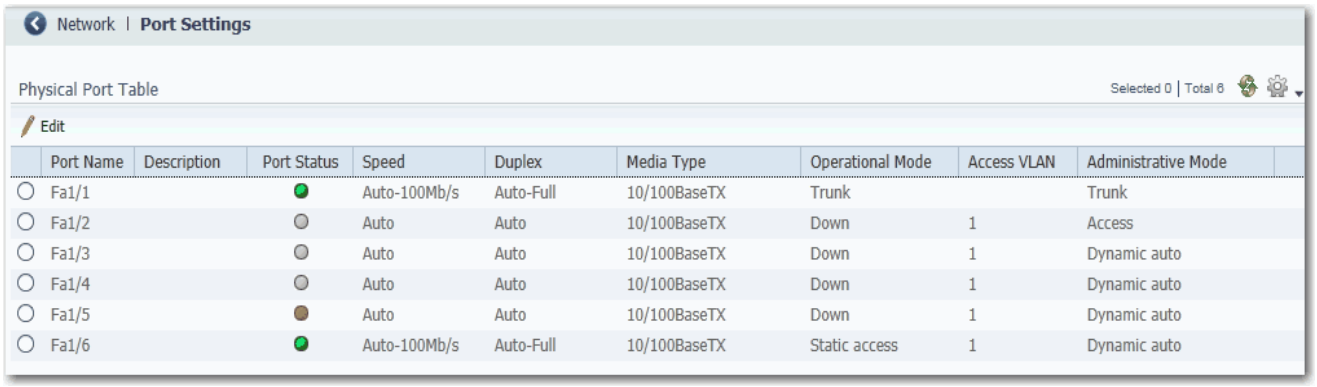


Table 16 lists the basic settings for the switch ports. To change these settings, click the radio button next to the port name and click Edit to display the Edit Physical Port page.

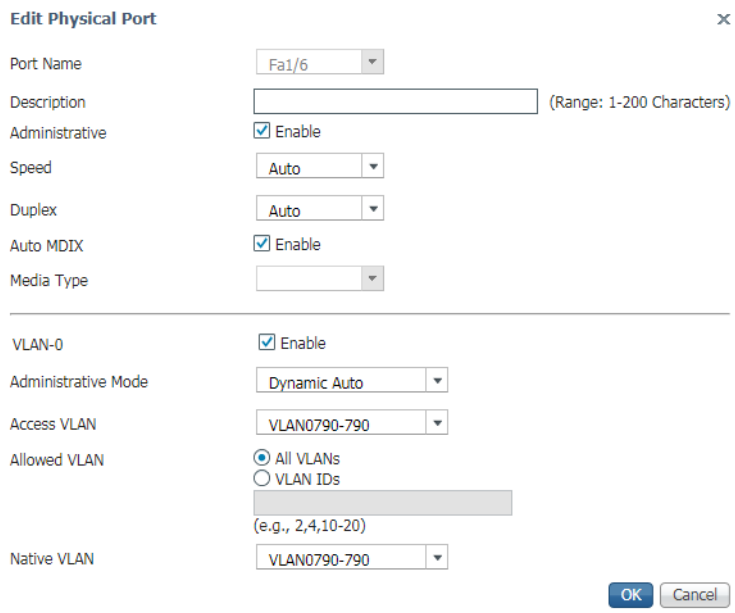


Table 16 - Port Settings

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. For more information, see Appendix C.
Description	The description of the switch port. We recommend that you provide a port description to help identify the port during monitoring and troubleshooting. The description can be the location of the connected device or the name of the person who uses the connected device.
Port Status	(Appears only on the Edit Physical Port page; not editable). Indicates whether a device is connected to the port: • Green = Connected • Gray = Not connected
Speed	The operating speed of the switch port. If the connected device can negotiate the link speed with the switch port, choose Auto (autonegotiation). We recommend that you use Auto speed so that the speed of the switch port automatically matches the speed of the connected device. If the connected device requires a specific speed, change the speed of the switch port. Default: Auto
Duplex	The duplex mode of the switch port: • Auto—(Autonegotiation). The connected device can negotiate the duplex mode with the switch. In the Physical Port table, the negotiated setting is Auto-Full or Auto-Half. If the port is not connected or has not completed negotiation, the status is Auto. • Half— (Half-duplex mode). The connected device must alternate sending or receiving data. • Full— (Full-duplex mode). Both devices can send data simultaneously. 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 Auto mode so that the mode on the switch port automatically matches the mode of the connected device. If the connected device requires a specific duplex mode, change the mode of the switch port. Default: Auto
Auto MDIX	(Appears only on the Edit Physical Port page). When enabled, this feature detects the port cable (straight-through or crossover) and configures the port pinouts, speed, and duplex mode to communicate correctly with the connected device. This setting is not available on SFP module ports. Default: Enabled
Media Type	(Applies to dual-purpose uplink ports). The active port type (either the RJ45 port or the SFP module port) of a dual-purpose uplink port. 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—Only the SFP module port of a dual-port is active. You can set the speed and duplex settings. Auto-MDIX is not available. For Gigabit Ethernet SFP ports, you can set the speed and duplex to Auto or 1000 Mb/s. This configures the port not to negotiate a device that does not support autonegotiation. • RJ45—Only the RJ45 port of a dual-port is active. You can enter the settings for port speed and duplex or choose Auto MDIX. • Auto—(Autonegotiation). The switch detects whether the RJ45 port or the SFP module port is connected and uses the port accordingly. Only one port can be active at a time. If both ports are connected to the network, the SFP module port has priority. The speed and duplex are set to Auto. Default: Auto
Operational Mode	(Appears only in the Physical Port table). The operational state of the port. Displays the administrative mode or Down if disabled.
VLAN-0	(Appears only on the Edit Physical Port page). Enables the system to handle 802.1Q Ethernet frames with VLAN ID 0, which are called priority tagged frames. The purpose of priority tagged frames is to give priority to the frames with no significance to the VLAN ID. For example, PROFINET messaging requires priority tagged frames to pass PROFINET messages through the switch. For more information about VLAN 0 priority tagging, see page 281. Default: Enabled
Administrative Mode	Choose one of the following administrative modes: • Access—The port is in permanent nontrunking mode and negotiates to convert the neighboring link into a nontrunk link even if the neighboring port is a trunk port. 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 port is in permanent Trunk mode and negotiates to convert the neighboring link into a trunk link even if the neighboring port is not a trunk port. If you choose this option, also choose whether to allow All VLANs or specified VLAN IDs. Also, choose the trunk native to the VLAN. • Dynamic Auto—The port converts the link to a trunk link if the neighboring port is set to Trunk mode or Dynamic Desirable mode. This mode is the default setting. If you choose this option, specify and access VLAN to use when the link is in access mode and a native VLAN to use when the link is in trunk mode. Also specify whether to allow all VLANs or specified VLAN IDs when the link is in trunk mode. • Dynamic Desirable—If the neighboring port is set to Trunk, Dynamic Desirable, or Auto mode, the port converts the link to a trunk link. If you choose this option, specify and access VLAN to use when the link is in access mode and a native VLAN to use when the link is in trunk mode. Also choose whether to allow all VLANs or specified VLAN IDs when the link is in Trunk mode. • Routed—The port 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 port, except that it does not support VLAN subports. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 port only and does not support Layer 2 protocols. Default: Dynamic Auto
Access VLAN	The VLAN that a port belongs to and carries traffic for when the port is configured as or is acting as a nontrunking port.
Allowed VLAN	(Appears only on the Edit Physical Port page). The VLANs for which the port handles traffic when the port is configured as or is dynamically acting as a trunking port: • To allow traffic on all available VLANs, click All VLANs. • To limit traffic to specific VLANs, click VLAN IDs and enter the VLAN numbers.
Native VLAN	(Appears only on the Edit Physical Port page). The VLAN that transports untagged packets.

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.

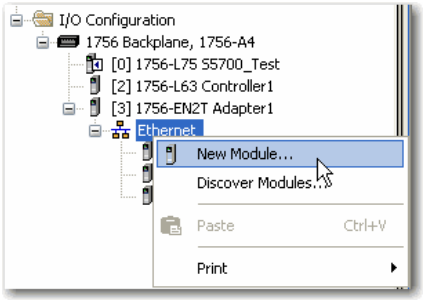
Table 17 - Logix Designer Application Hardware Requirements

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	USB Drive or Downlaod
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)

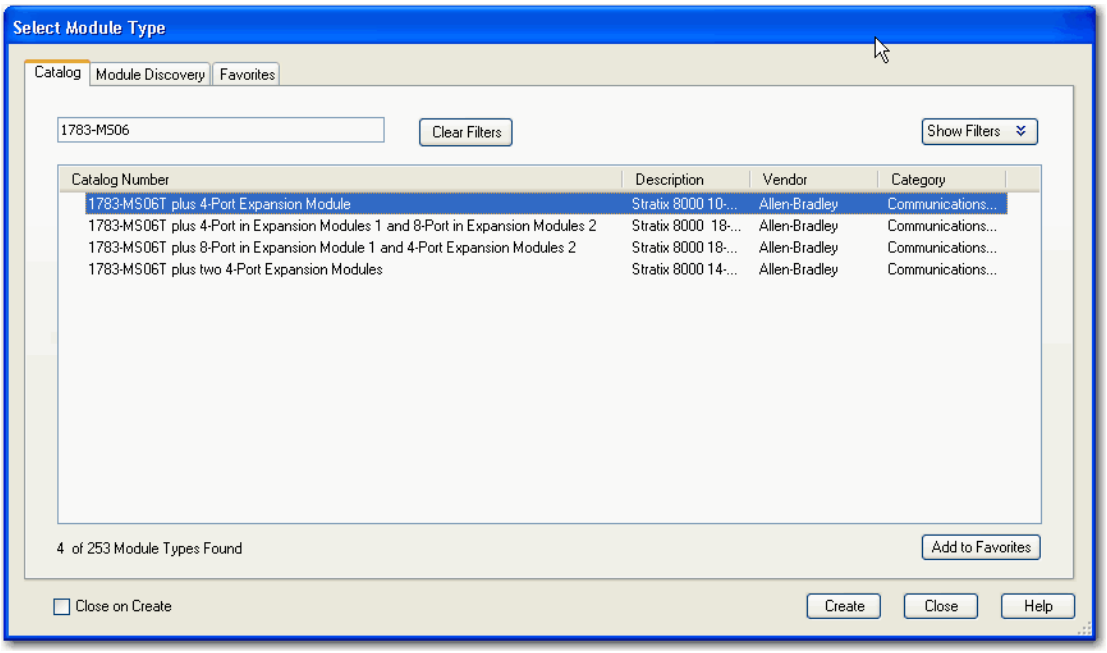
To add the switch to a controller project in the Logix Designer application, follow these steps.

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.

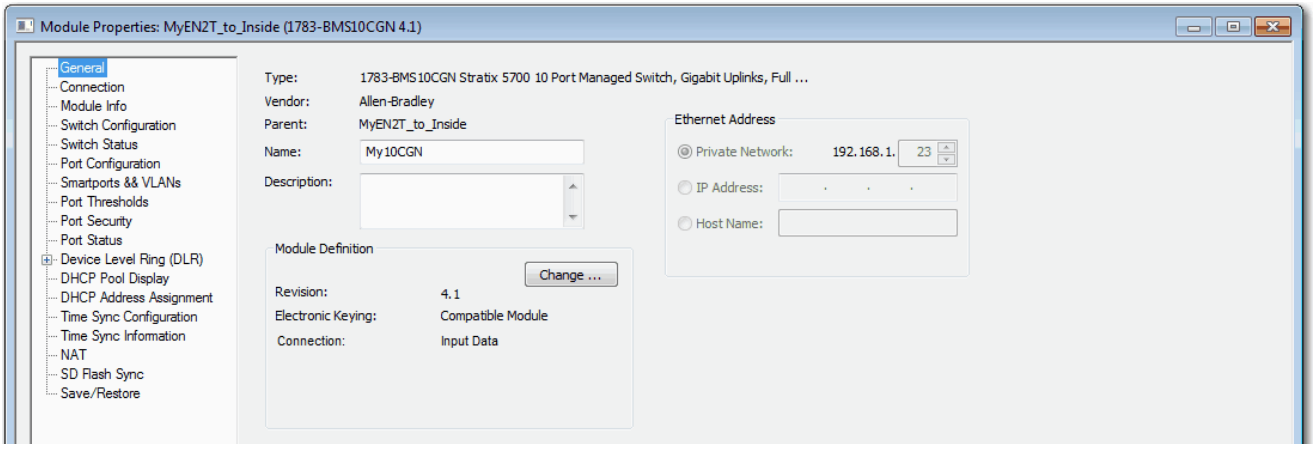


If you do not see the switch on the list, you can obtain the AOP from the Rockwell Automation support website:
http://www.rockwellautomation.com/support/

General Properties

To configure general properties, follow these steps.

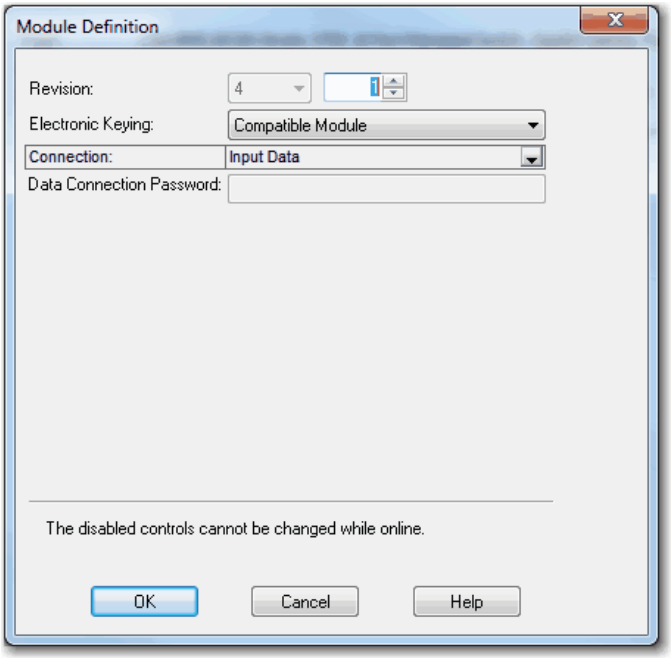
1. In the navigation pane, click General and complete the fields.



IMPORTANT Make sure that the IP address and host name match the values that 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.
IP Address	Choose one of the following: • Private Network—The IP address of your private network. • IP Address—The IP address that is 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 port 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 Keying - allows the AOP to connect to the switch with matching major revision and any minor revision. • Exact Match - requires both major and minor to match for connection. • Disable Keying - the AOP will connect regardless of major and minor version numbers.
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 output bits from the controller on the next cyclic update of the I/O connection can override the port setting. 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.

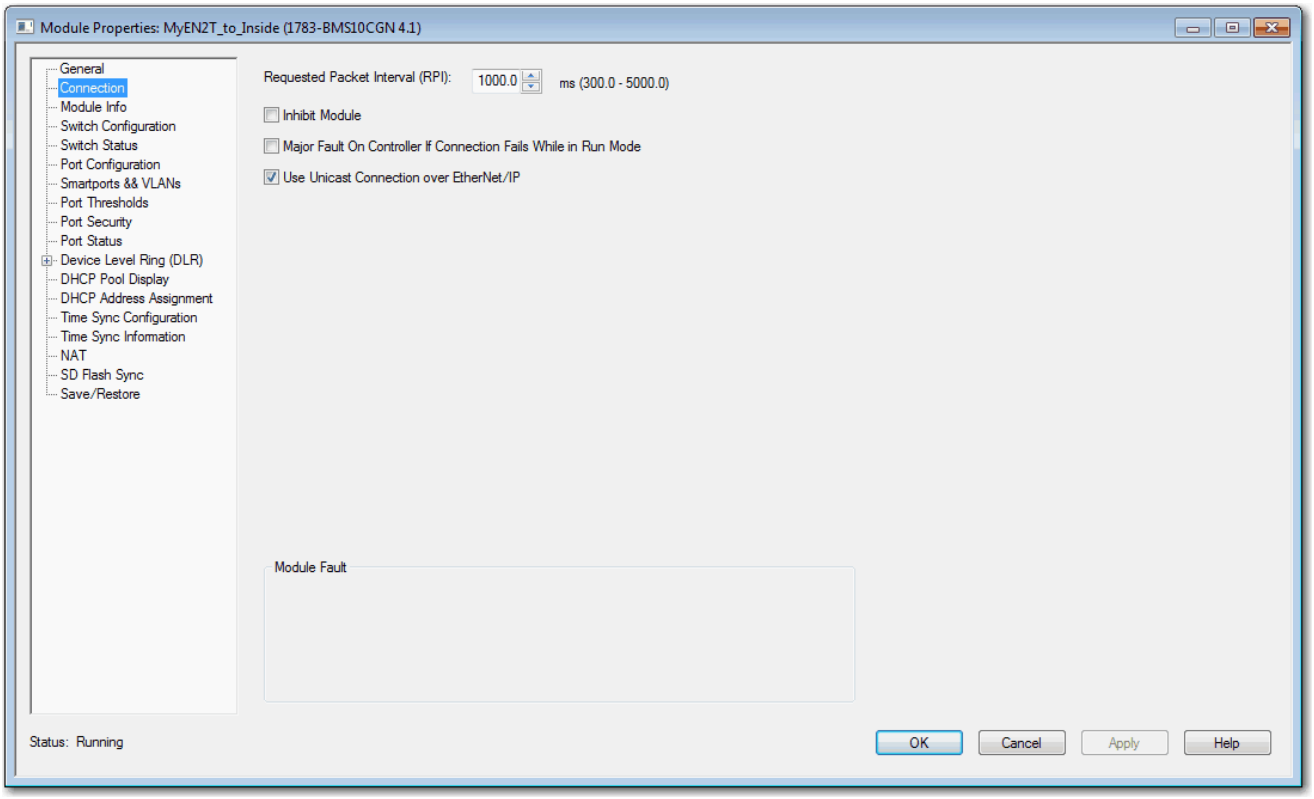


Table 18 - Connection Fields

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

In the navigation pane, click Switch Configuration.

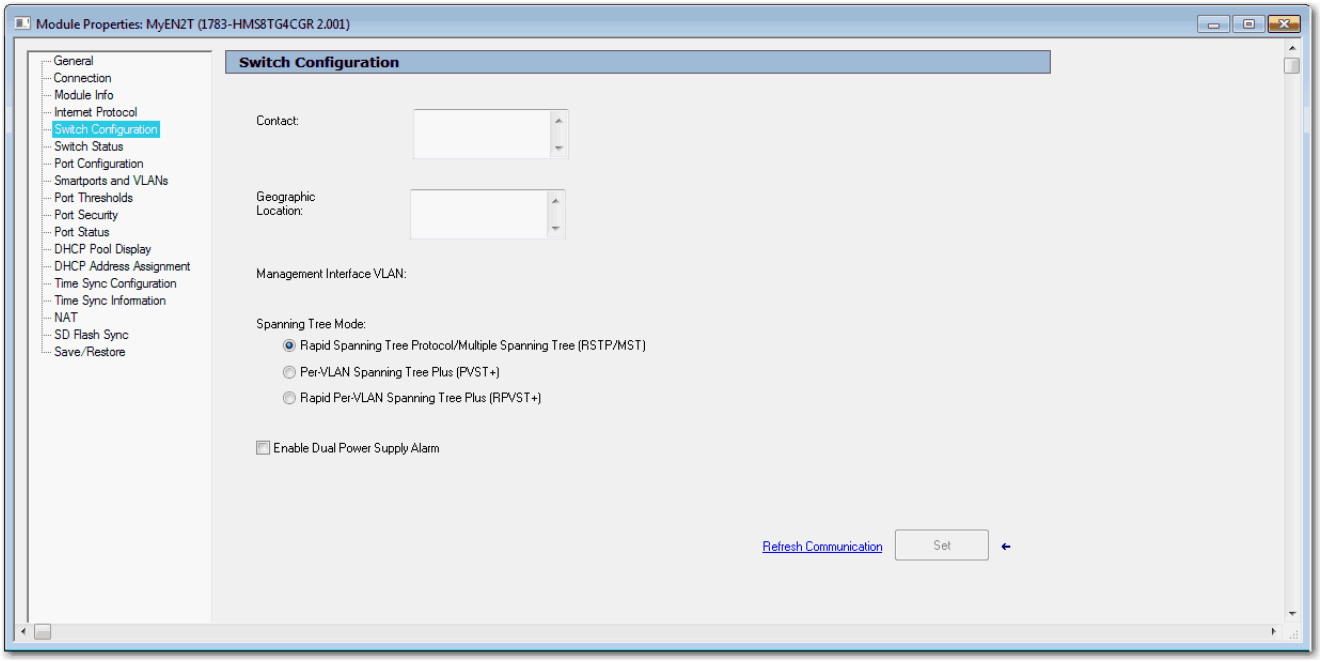


Table 19 - Switch Configuration Fields

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. The management VLAN 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. The management VLAN 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	See Spanning Tree Protocol (STP) on page 272.
Enable Dual-Power Supply Alarm	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. You can also configure port settings in the Device Manager, as described on page 45.

In the navigation pane, click Port Configuration.

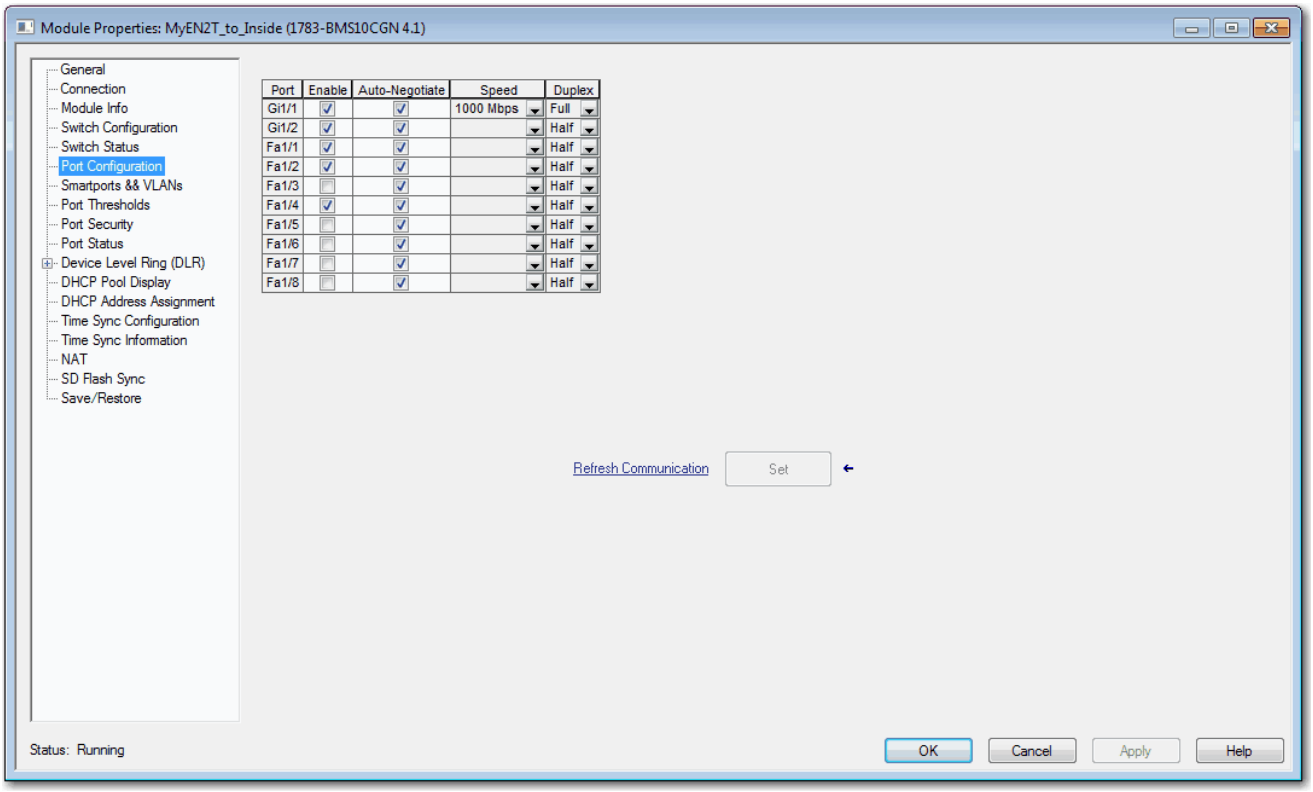


Table 20 - Port Configuration Fields

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 20 - 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 ports 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.

Port States during Program Mode and Connection Faults

You can configure the state of each port when these changes occur at the controller:

- The controller transitions to Program mode
- Communication is disrupted between the controller and the switch

In the navigation pane, click Fault/Program Action.

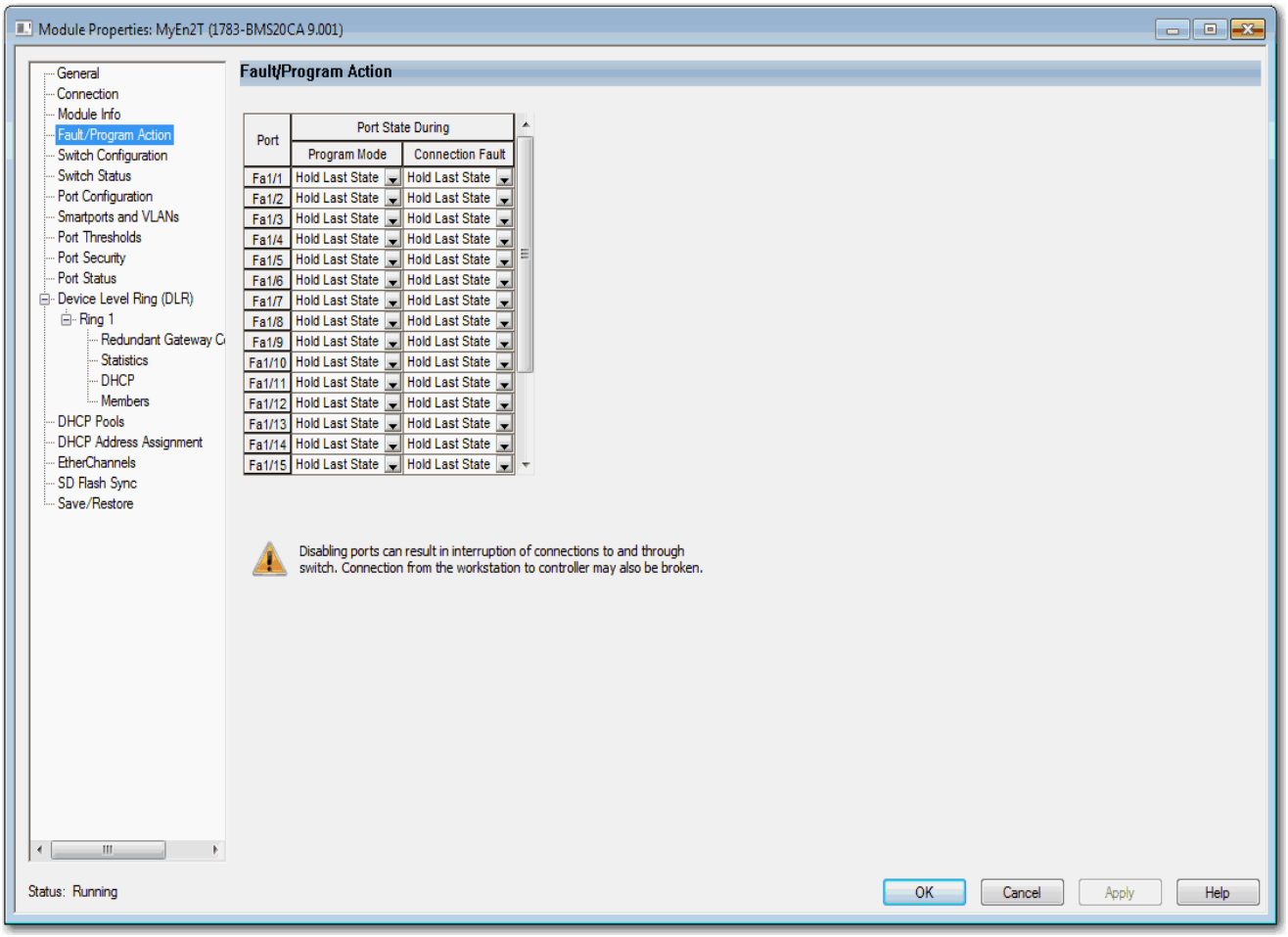


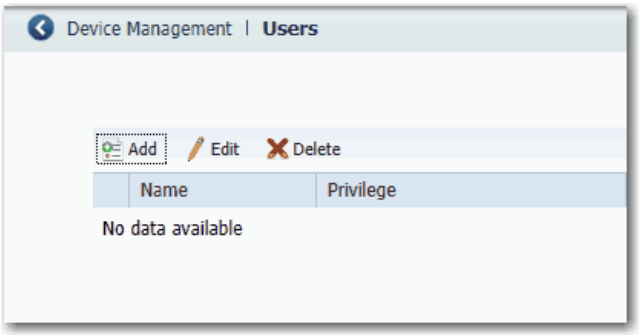
Table 21 - Fault/Program Action Fields

Field	Description
Port	Displays the port type and port number: • Fa—Fast Ethernet • Gi—Gigabit Ethernet • Te—10 Gigabit Ethernet
Program Mode	Choose what happens at the port when the controller transitions to Program mode: • Hold Last State—The port maintains the current state. • Disable—The port is disabled. • Enable—The port is enabled. The default is Hold Last Sate.
Connection Fault	Choose what happens at the port when communication is lost between the controller and the switch: • Hold Last State—The port maintains the current state. • Disable—The port is disabled. • Enable—The port is enabled. The default is Hold Last Sate.

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 22.

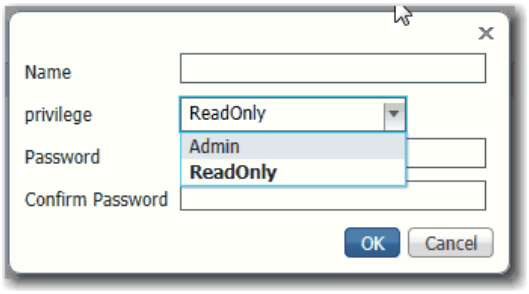


Table 22 - Add User Fields

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. • Read-only—Users can only view switch status and monitor information.
Password, Confirm Password	The password that is required for access with this user name.

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 Admin 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.

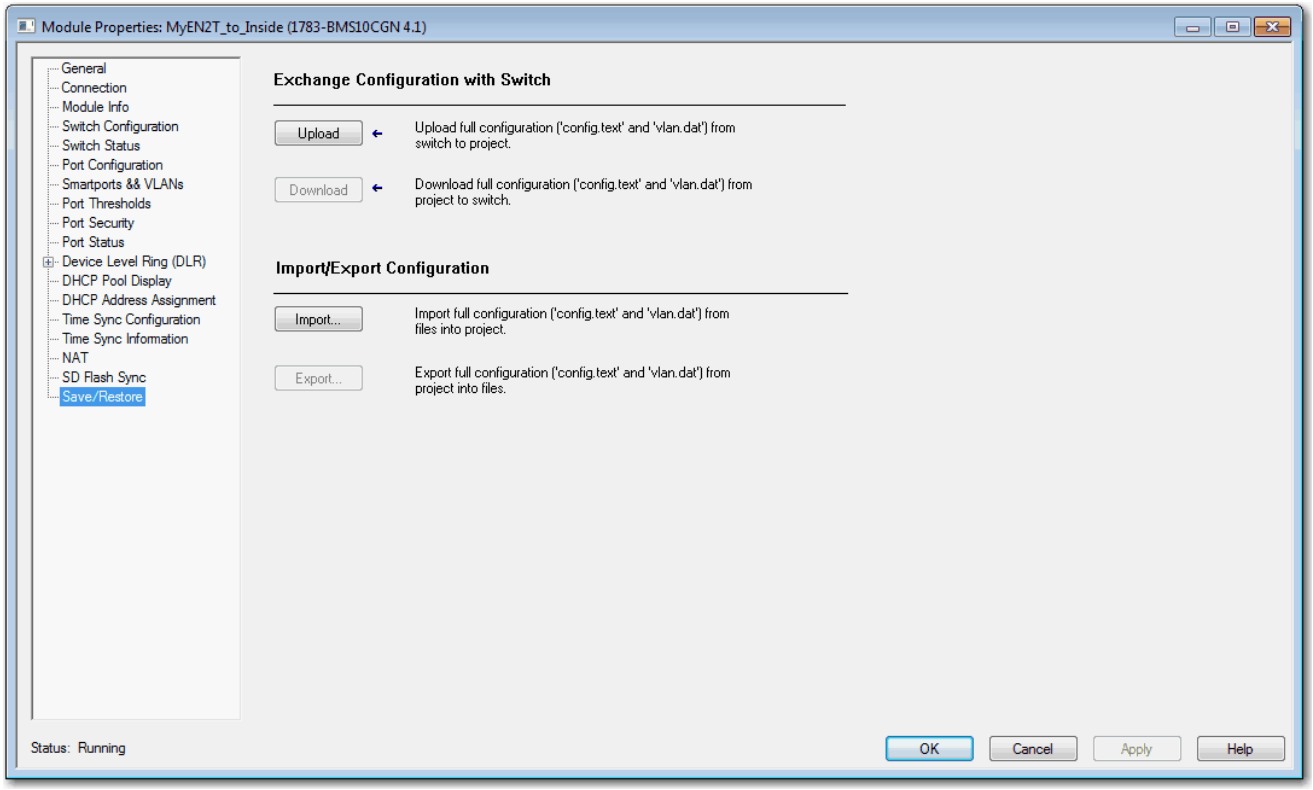
Manage Configuration Files via the Logix Designer Application

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 their 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 Automation 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 if it fails.
- Duplicate configurations when you are deploying a new network.
- Synchronize the initial configuration and firmware of a 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 configuration files 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 startup 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 accessible.
- Changes that are made by using the CLI or the Logix Designer application 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 the lock 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

In Device Manager, you can use the Sync page to display SD card and sync status and to synchronize files.

To enable manual sync or automated sync, from the Admin menu, choose Sync:

- For manual synchronization options, click the Manual Sync tab.
- For auto synchronization options, click the Auto Sync tab.

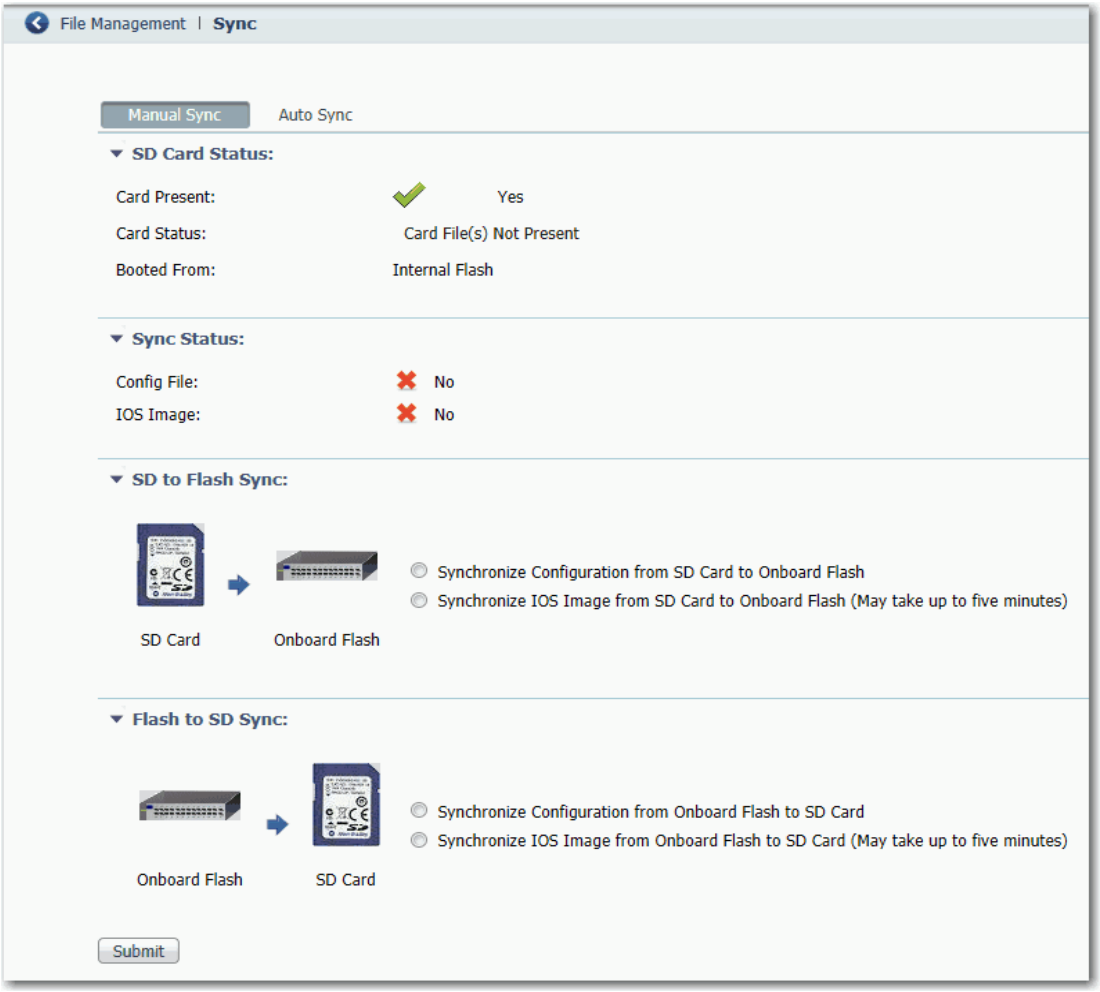


Table 23 - Manual Sync Fields

Field	Description
SD Card Status	Displays whether an SD card is present and whether the switch was started from the SD card.
Sync Status	Displays whether the configuration and firmware image files are synchronized.
SD to Flash Sync	Click whether to synchronize the configuration or the firmware image from the SD card to the internal memory of the switch.
Flash to SD Sync	Click whether to synchronize the configuration or the firmware image from the internal memory of the switch to the SD card.

As of IOS 15.2(6)E1 and later, Device Manager provides new auto sync options for Stratix 5700 and ArmorStratix 5700 switches, as shown in the following figure. These options are not mutually exclusive. You can enable one or all auto sync options as described in Table 24. If all options on the Auto Sync tab are disabled, then synchronization only occurs manually when you submit an option on the Manual Sync tab.

You can use the Auto Sync at Reboot option to copy a configuration and firmware image from an SD card onto multiple switches without using Device Manager Express Setup. The configuration and firmware image on the SD card automatically syncs with internal memory after startup.

When you update a Stratix 5700 or ArmorStratix 5700 switch with IOS 15.2(6)E1 or later, the synchronization options that were configured in the earlier version are retained.

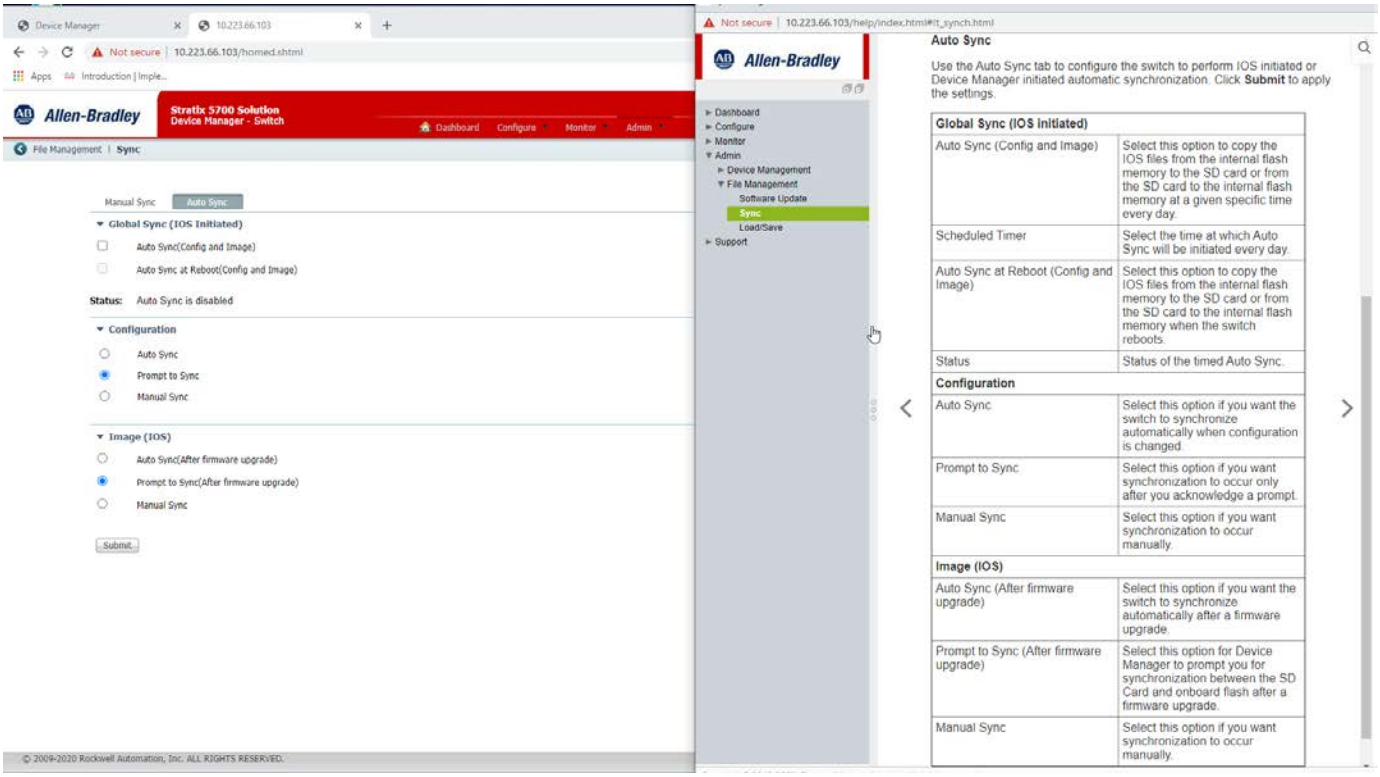


Table 24 - Auto Sync Fields for Stratix 5700 and ArmorStratix 5700 Switches

Field	Description
Global Sync (IOS Initiated)	
Auto Sync (Config and Image)	Use this feature to copy the IOS files from the internal flash memory to the SD card or from the SD card to the internal flash memory at a given specific time every day.
Scheduled Timer	Use this feature to Select the time at which Auto Sync will be initiated every day
Auto Sync at Reboot (Config and Image)	Use this feature to Select this option to copy the IOS files from the internal flash memory to the SD card or from the SD card to the internal flash memory when the switch reboots
Status	The status of the timed auto sync.
Configuration	
Auto Sync	Use this feature for the switch to synchronize automatically when the configuration is changed.
Prompt to Sync	Use this feature for synchronization to occur only after a prompt is acknowledged.
Manual Sync	Use this feature for the synchronization to occur manually.
Image (IOS)	

Table 24 - Auto Sync Fields for Stratix 5700 and ArmorStratix 5700 Switches

Field	Description
Auto Sync (After Firmware Upgrade)	Use this feature for the switch to synchronize automatically after a firmware upgrade.
Prompt to Sync (After Firmware Upgrade)	Use this feature for synchronization between the SD Card and an on-board flash after a firmware upgrade.
Manual Sync	Use this feature for the synchronization to occur manually.

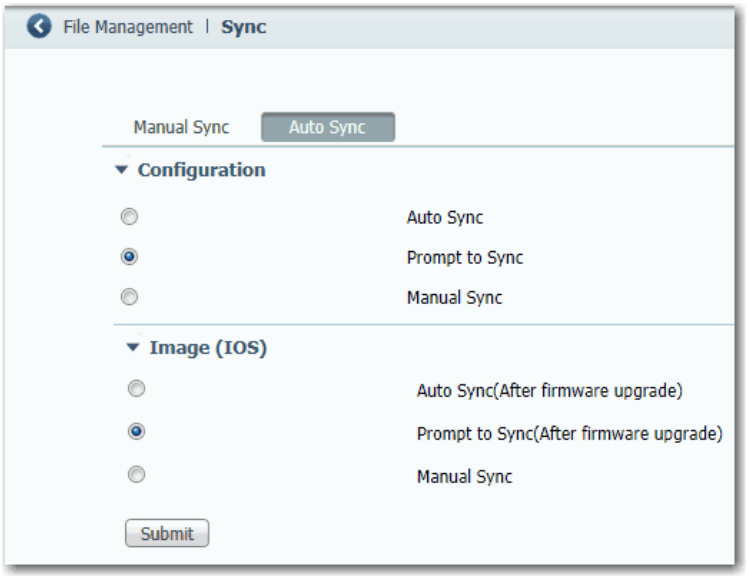


Table 25 - Auto Sync Fields for Stratix 5400 and 5410 Switches

Field	Description
Configuration	
Auto Sync	Automatically synchronizes 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 update)	Automatically sync the changed configuration when firmware is upgraded.
Prompt to Sync (After firmware update)	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 firmware image.

In the navigation pane, click SD Flash Sync.

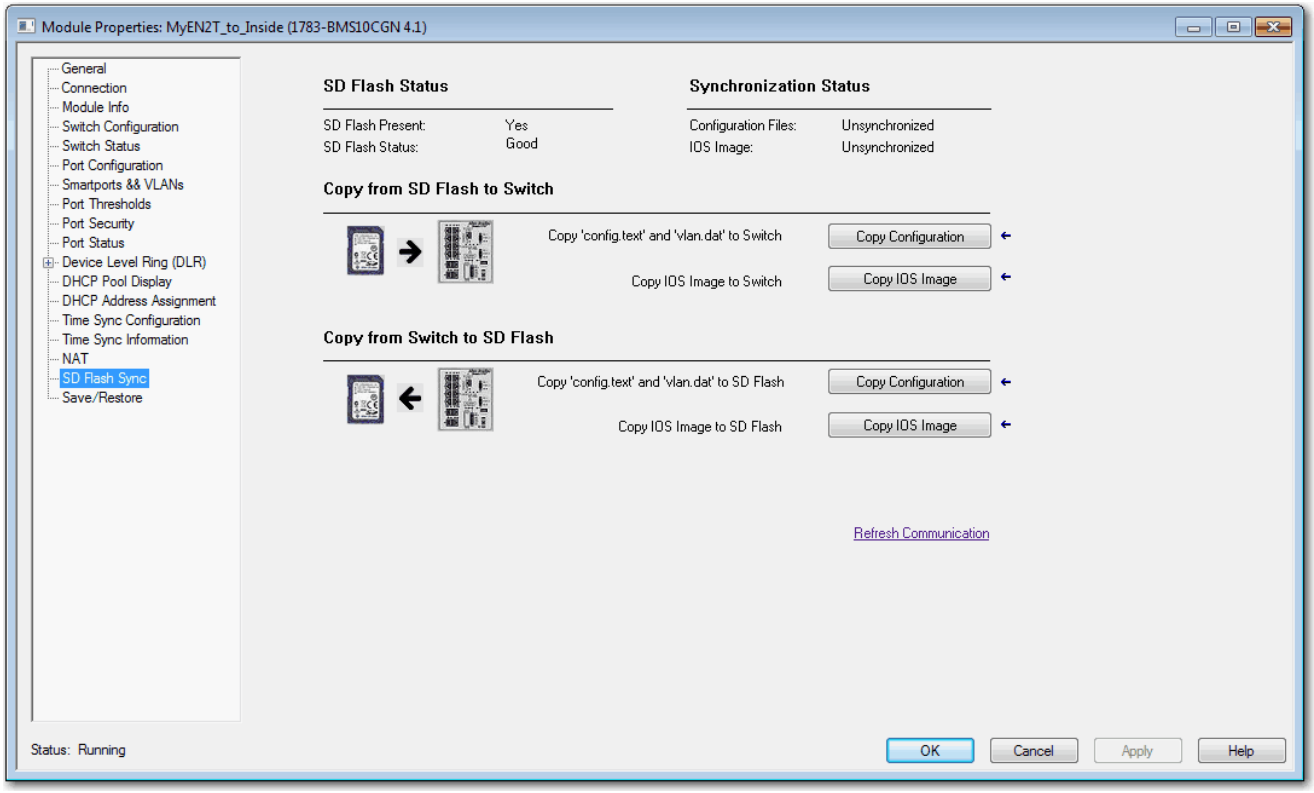


Table 26 - SD Flash Sync Fields

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

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 of the switch as it runs, the switch continues to function. However, Device Manager is no longer available.

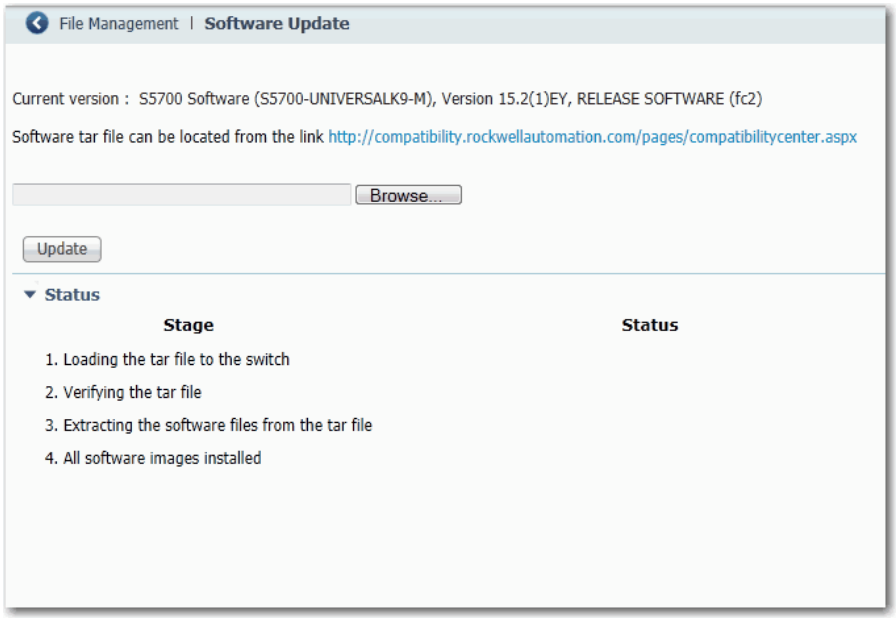
If you change the switch configuration after the card is removed, the changes are applied and used by the switch. However, the changes are not saved. If you insert the CompactFlash card later, the previous changes are still not saved to the card. Only changes that are made while the card is inserted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

Each time a change is made with the card installed, both Device Manager and the Logix Designer application 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 the Cisco 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

Apart from Device Manager and the Logix Designer application, you can manage the switch from the Cisco IOS command-line interface (CLI). This interface enables you to execute Cisco IOS commands by using a router console or terminal or by using remote access methods.

You can use the following connection methods:

- Connect directly to the switch console port
- Enable Secure Shell (SSH) or Telnet in Device Manager

For more information about how to use the CLI, refer to www.cisco.com.

Connect to the Console Port

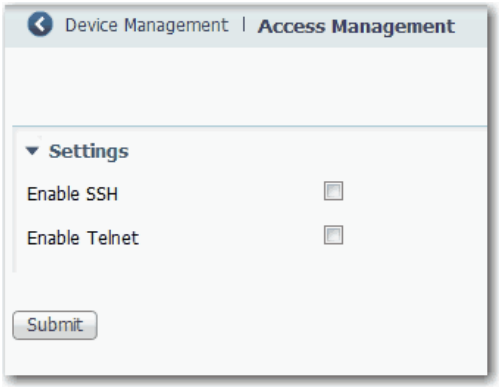
1. Connect to the console port in one of these ways:
   - To connect to the standard 9-pin serial port on a computer, use an RJ45-to-DB-9, USB-RJ45 or, 9300-USBCBL-CNSL adapter cable.
   - (Stratix 5400, 5410, 5700, and ArmorStratix 5700 switches). Use a standard mini-USB cable to connect to the mini-USB port on a computer. If you use the USB cable, download the drivers from http://www.rockwellautomation.com.
2. Connect the other end of the cable to the console port on the switch.
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
   - No flow control

Enable SSH or Telnet in Device Manager

SSH provides a secure, remote connection to the switch and more security for remote connections than Telnet by providing strong encryption.

IMPORTANT For secure network access, we recommend that you do not use Telnet. For new switch configurations with IOS release 15.2(5)EA.fc4 and later, Telnet is disabled by default. For information about default settings after an upgrade, see page 337.

1. From the Admin menu, choose Access Management.
2. To allow Secure Shell (SSH) sessions on the switch, check Enable SSH.
3. To allow Telnet sessions on the switch, check Enable Telnet.
4. Click Submit.



FactoryTalk Network Manager

FactoryTalk® Network Manager™ software provides insight into the design, and health of an industrial automation network. Use FactoryTalk Network Manager (FTNM) to view your network topology and manage switch-level alarms as they happen. Monitor the health of network devices and reduce downtime to improve overall automation equipment efficiency.

FTNM:

- Discovers both network and end devices including devices across a controller backplane
- Generates an overall topology and a device-centric view of plant floor assets for increased network visibility
- Captures managed switch level alarms and events for more precise troubleshooting
- Provides historical data and logging for analysis and resolution
- Provides configuration, compare and restore, and backup and firmware revision management of Stratix® managed switches for simplified deployment and maintenance

For more information on FTNM see the Factory Talk Network Manger Quick Start Guide.

Configure Switch Features

Topic	Page
Authentication, Authorization, and Accounting (AAA)	68
Access Control Lists (ACLs)	84
Alarms	88
CIP Sync Time Synchronization (Precision Time Protocol)	93
Device Level Ring (DLR) Topology	112
DLR VLAN Trunking	125
Dynamic Host Configuration Protocol (DHCP) Persistence	126
Enhanced Interior Gateway Routing Protocol (EIGRP)	135
EtherChannels	139
Feature Mode	147
Global Navigation Satellite System (GNSS)	148
GOOSE Messaging Support	277
High-availability Seamless Redundancy (HSR)	150
Hot Standby Router Protocol (HSRP)	153
IEEE 1588 Power Profile	93
Internet Group Management Protocol (IGMP) Snooping with Querier	156
Internet Protocol Device Tracking (IPDT)	158
Link Layer Discovery Protocol (LLDP)	159
Maximum Transmission Unit (MTU)	160
Motion Prioritized QoS Macros	162
NetFlow	163
Network Address Translation (NAT)	167
Network Time Protocol (NTP)	202
Open Shortest Path First (OSPF) Routing Protocol	206
Parallel Redundancy Protocol (PRP)	211
Port Mirroring	219
Port Security	220
Port Thresholds	226
Power over Ethernet (PoE)	231
PROFINET	241
Resilient Ethernet Protocol (REP)	246
Resilient Ethernet Protocol (REP) Negotiated	251
Routing, Static and Connected	254
SCADA Protocol Classification	277
Simple Network Management Protocol (SNMP)	257
Smartports	262
Spanning Tree Protocol (STP)	272
Virtual Local Area Networks (VLANs)	277
VLAN 0 Priority Tagging	281

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 Stratix 5700 Lite Versus Full Firmware Features on page 15 and Software Features on page 16.

Authentication, Authorization, and Accounting (AAA)

AAA Network Security Services provide the primary framework for intelligently controlling access to resources, policy enforcement, and usage audits.

Terminal Access Controller Access-Control System Plus (TACACS+) and Remote Authentication Dial-In User Service (RADIUS) are two security protocols that control access to networks. The switch performs as a TACACS+or RADIUS client to authenticate and authorize users.

AAA is available in Device Manager on the Stratix® 5400, Stratix 5410, Stratix 5700, and ArmorStratix™ 5700 switches.

Configure AAA via Device Manager

To configure AAA, you define servers and server groups and a named list of AAA methods, and then apply the list to various interfaces. The method list defines the types of security services to be performed and the sequence in which they are performed. The method list must be applied to a specific interface before any of the defined methods are performed.

You can configure up to two servers each for TACACS+ and RADIUS. TACACS+ uses TCP for communication between the client and the server, and RADIUS uses UDP.

You can configure a server or change a server setting in Device Manager:

The AAA dialog box features three tabs: Servers/Server Groups, AAA Methods, and AAA Interface.

The AAA Methods tab is used to configure the AAA methods and associate each method type to the server group created on the Server/Server Groups tab.

The AAA Interface tab is used to associate the method lists created on the AAA Methods tab to the interfaces (Console, VTY[SSH/Telnet], and DM). The method lists created on the AAA Interface tab are available in the Authentication pull-down menu.

Enable AAA

1. From the Configure menu, under Security, choose AAA. The AAA dialog box appears.
2. Check Enable AAA Model to enable the AAA access control system on the switch.

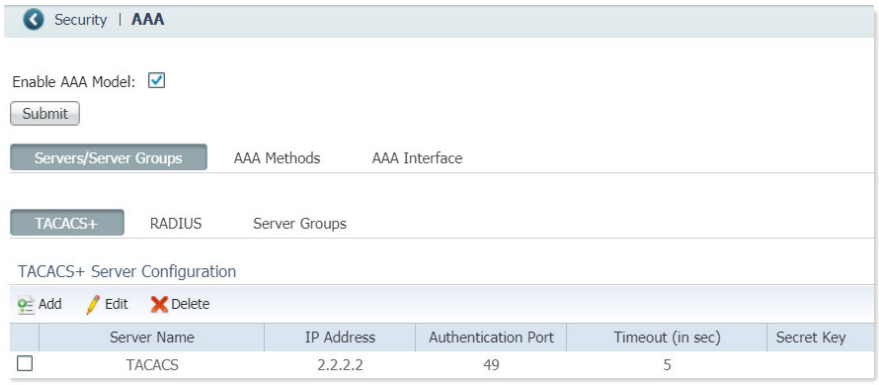
IMPORTANT	If the Enable AAA Model checkbox is clear, AAA mode is disabled on the switch, and the switch reverts to pre-AAA configurations. Also, if you disable AAA, you are notified that the connectivity to the switch through Device Manager could be affected. Confirm that users are configured in the local database to allow continued access to the switch.

Server/Server Groups Tab

The Servers/Server Groups tab contains three subtabs: TACACS+, RADIUS, and Server Groups.

TACACS+ Subtab

The TACACS+ tab allows you to add, edit, and delete a TACACS+ server.



Add a TACACS+ server

1. Click Add.
2. Add the TACACS+ server information per Table 27.
3. Click Save. The configured server is populated to the list.

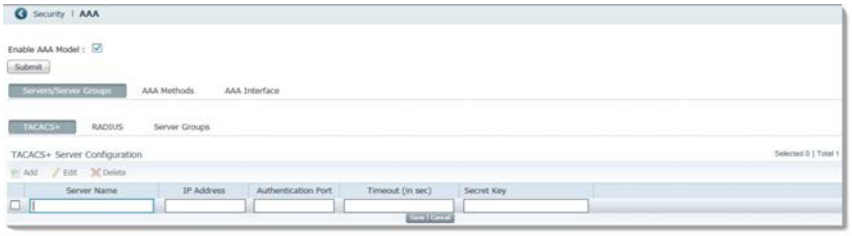
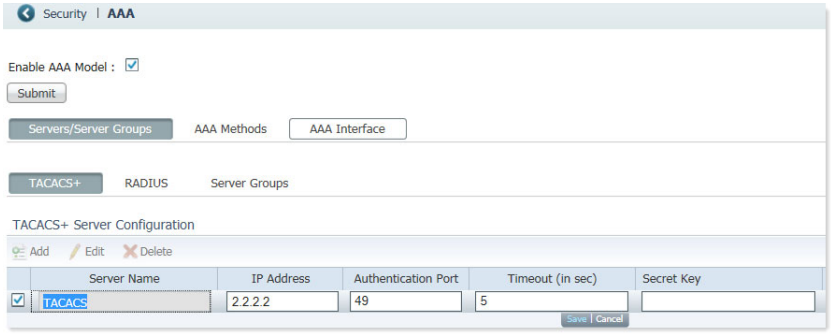


Table 27 - TACACS+ Server Configuration

Field	Description
Server Name	Enter the name of the server.
IP Address	Enter the IP address of the TACACS+ server.
Authentication Port	Enter the TACACS+ server port number. Valid range: 1...65535 Default: 49
Timeout (in seconds)	Enter the time interval for the switch to wait for a response from the TACACS+ server to reply before resending communication. Valid range: 1...1000 Default: 5
Secret Key	Enter the secret key text string to provide encryption for the TACACS+ server communications.

Edit a TACACS+ server

1. Check the checkbox of the row to edit.
2. Click Edit. All fields except Server Name are editable.
3. Change TACACS+ server information per Table 27.
4. Click Save. The updated server information appears in the server configuration list.



Delete a TACACS+ server

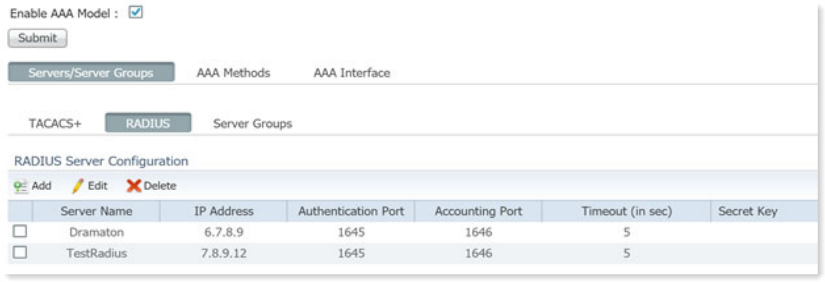
1. Check the checkbox of the row to delete.
2. Click Delete. The server information is removed from the server configuration list.

To delete a server that is a member of an existing server group, you must first remove the server from the group.

IMPORTANT If you delete a server, it cannot be used on the other tabs.

RADIUS Subtab

The RADIUS subtab allows the user to add, edit, and delete a RADIUS server.



Add a RADIUS server

1. Click Add.
2. Enter the RADIUS server information per Table .
3. Click Save. The configured server is populated to the list.

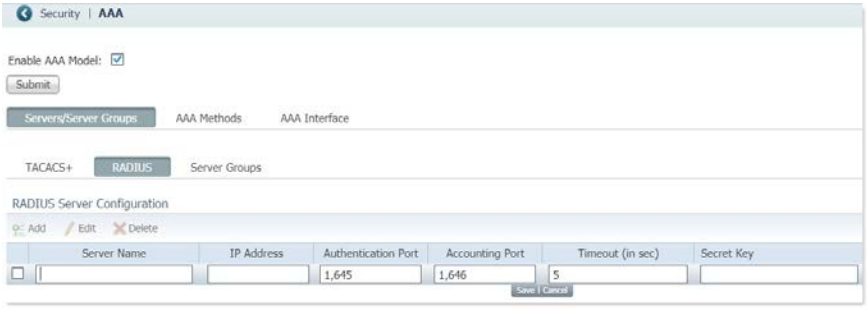


Table 28 - Radius Server Configuration Fields

Field	Description
Server Name	Enter the name of the server.
IP Address	Enter the IP address of the RADIUS server.
Authentication Port	Enter the RADIUS UDP destination port for authentication requests. Default: 1645
Accounting Port	Enter the RADIUS UDP destination port for accounting requests. Default: 1646
Timeout (in sec)	Enter the time interval for the switch to wait for a response from the RADIUS server to reply before resending communication. Valid range: 1...1000 Default: 5
Secret Key	Enter the secret key text string to provide encryption for the RADIUS server communications.

Edit RADIUS Server Information

1. Check the checkbox of the row to edit.
2. Click Edit. All fields except Server Name are editable.
3. Change RADIUS server information per Table .
4. Click Save. The updated server information appears in the server configuration list.

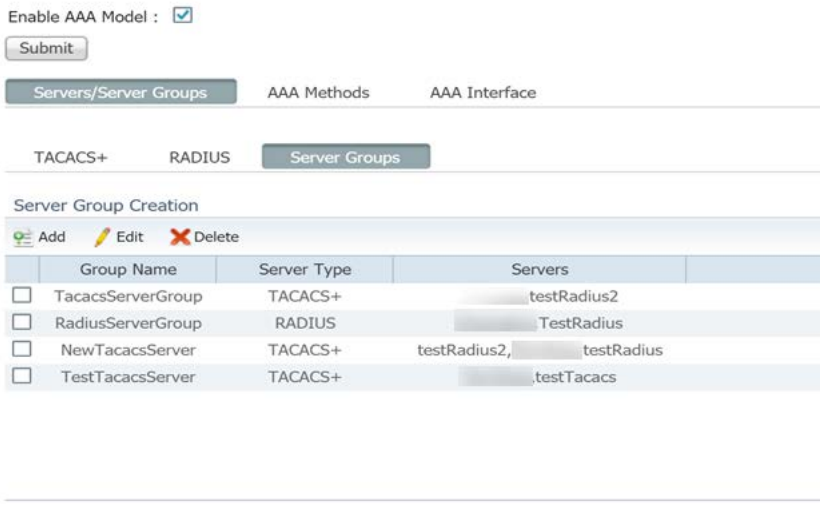
Delete a RADIUS Server

1. Check the checkbox of the row to delete.
2. Click Delete. The server information is removed from the server configuration list, and the Total is decremented as long as the server is not used on other tabs.

To delete a server that is a member of an existing server group, you must first remove the server from the group.

Server Groups Subtab

The Server Groups subtab allows you to group, in method lists, the TACACS+ or RADIUS servers from the TACACS+ or RADIUS tabs. TACACS+ or RADIUS servers must be configured to create a server group.



Add a Server Group

1. Click Add.

IMPORTANT A server group cannot be created with both TACACS+ and RADIUS servers.

2. Enter server group information per Table .

3. To move servers between the Available and Assigned Servers lists, click the arrows. Click OK.

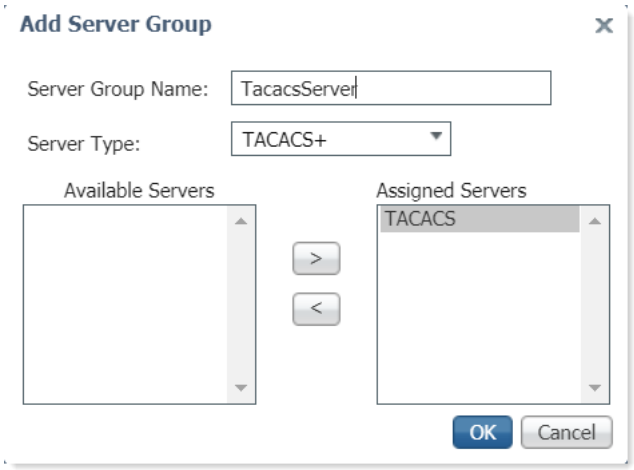
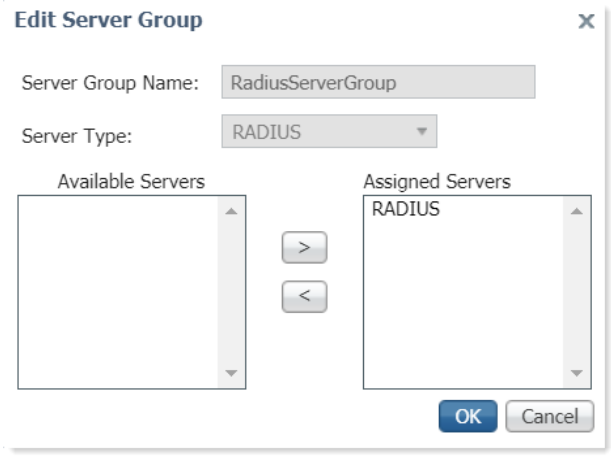


Table 29 - Add Server Group Configuration Fields

Field	Description
Server Group Name	Enter the name of the server group.
Server Type	Choose the server type from the pull-down menu: TACACS+ or RADIUS.
Available Servers	Choose from the list of available servers in the left column to assign to the group.
Assigned Servers	Lists the assigned servers.

Edit a RADIUS Server

1. Click Edit.
2. To move servers between the Available and Assigned Servers lists, click the arrows.
3. Click OK.



Delete a Server Group

IMPORTANT To delete a server group that is used in an existing AAA method, you must first remove the server group from the method.

1. Check the corresponding checkbox of the server group row to delete.
2. Click Delete. The server group is removed from the server group list, and the Total is decremented.

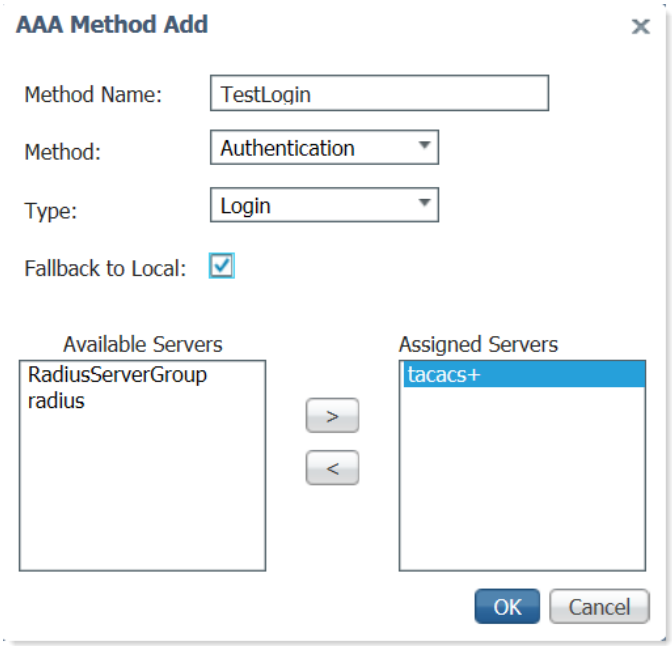
AAA Methods

Click on the AAA Methods tab to configure the AAA methods and associate each method type to the server group created on the Server/Server Groups tab.

Add Authentication Method

To add an authentication method, use the following steps.

1. Click Add.
2. Enter the name of the AAA method.
3. Choose Authentication from the Method pull-down menu.
4. Choose Login from the Type pull-down menu.
5. Check Fallback to Local.
6. Choose from the available servers in the left column and use the arrows to assign the server to the group.
7. Use the arrows to move servers to and from the list of assigned servers.



8. Click OK.

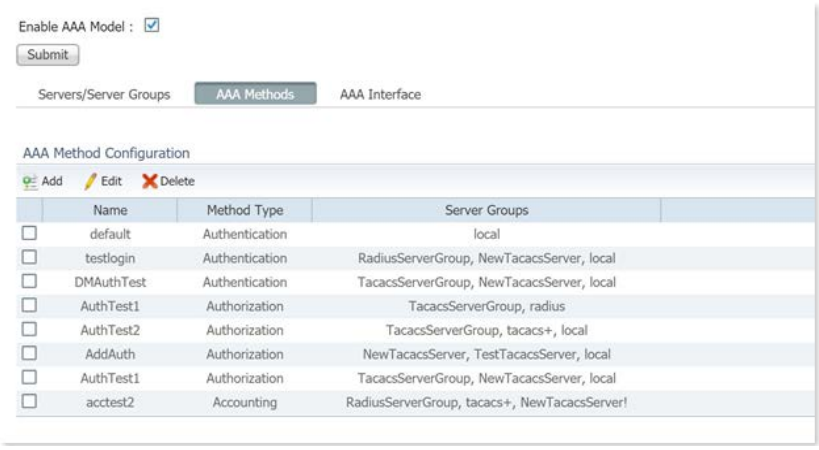


Table 30 - AAA Method Add Authentication Configuration Fields

Field	Description
Method Name	The name of the AAA method.
Method	The AAA Method options dynamically change Type options: • Authentication - identifies user based on username and password (login) • Authorization - allows access based on user identity • Accounting - Exec Commands, Exec(Shell), and System options are supported
Type	• Login - authentication uses the local username database.
Fallback to Local	Specifies the use of the local database for authentication if all configured methods fail.
Available Servers	Servers available for assignment to the group.
Assigned Servers	List of assigned servers.

Add Authorization Methods

This section covers the two types of authorization methods: Exec(Shell) and Exec Commands.

Exec(Shell)

Exec(Shell) runs authorization to determine if the user is allowed to run an EXEC shell.

Add an Exec(Shell) authorization method

1. Click Add.
2. Enter the name of the AAA method.
3. Choose Authorization from the Method pull-down menu.
4. Choose Exec(Shell) from the Type pull-down menu.
5. Check Fallback to Local.
6. Choose from the available servers in the left column and use the arrows to assign the server to the group.
7. Click OK.

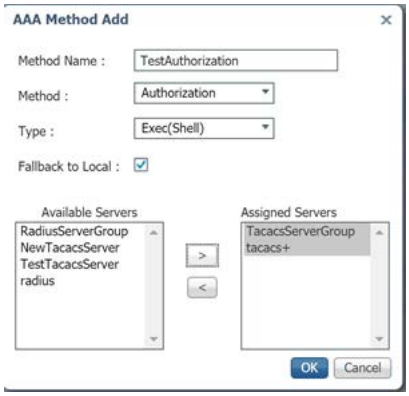


Table 31 - Exec(Shell) Authorization Configuration Fields

Field	Description
Method Name	The name of the AAA method.
Method	The AAA Method options dynamically change Type options: • Authentication - identifies user based on username and password (login) • Authorization - allows access based on user identity • Accounting - Exec Commands, Exec(Shell), and System options are supported
Type	• Exec(Shell) - determines if a user is allowed to run an EXEC shell • Exec Commands - determines if a user can execute a command in place of the current shell
Fallback to Local	Specifies the use of the local database for authentication if all configured methods fail.
Available Servers	Servers available for assignment to the group.
Assigned Servers	List of assigned servers.

Exec Commands

Exec Commands runs authorization for all commands at the specified privilege level. Valid privilege-level entries are integers 0...15. Device Manager supports only read-only (level 5) and admin (level 15) privileges. Therefore, methods to be applied to Device Manager must be configured with 5 and 15.

Add an Exec Commands Authorization Method.

1. Click Add.
2. Enter the name of the AAA method.
3. Choose Authorization from the Method pull-down menu.
4. Choose Exec Commands from the Type pull-down menu.
5. Enter the number of the privilege level.
6. Check Fallback to Local.
7. Choose from the available servers in the left column and use the arrows to assign the server to the group.

8. Click OK

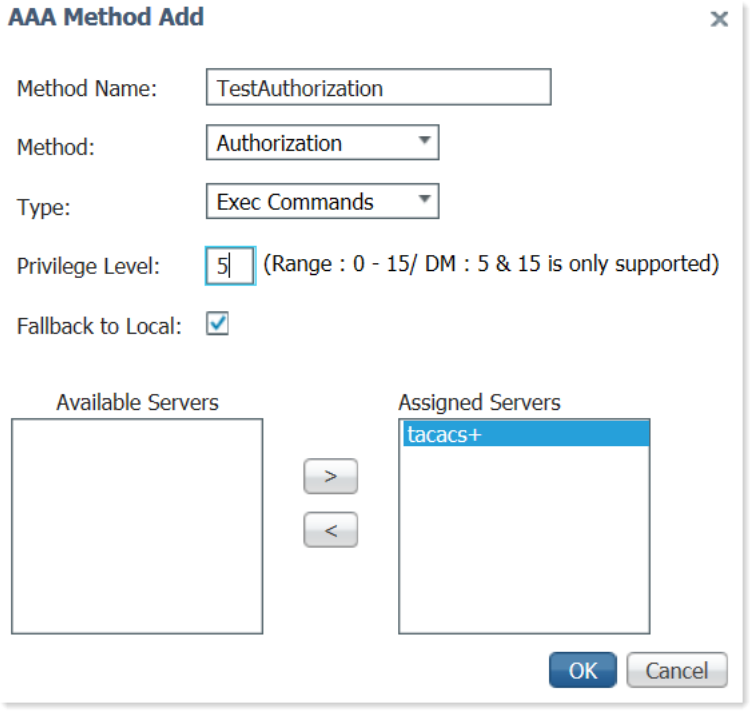


Table 32 - Exec Commands Authorization Fields

Field	Description
Method Name	The name of the AAA method.
Method	The AAA Method options dynamically change Type options: • Authentication - identifies user, based on username and password (login) • Authorization - allows access based on user identity • Accounting - Exec Commands, Exec(Shell), and System options are supported
Type	• Exec(Shell) - determines if a user is allowed to run an EXEC shell • Exec Commands - determines if a user can execute a command in place of the current shell • System - accounts for all system-level events
Privilege Level	Specifies Privilege Level
Fallback to Local	Specifies the use of the local database for authentication if all configured methods fail.
Available Servers	Servers available for assignment to the group.
Assigned Servers	List of assigned servers.

IMPORTANT The DM interface supports Admin and read-only privileges only. Therefore, the method lists for Authorization and Accounting are shown with Exec Commands with privilege levels 5 and 10 only.

Add Accounting Methods

This section covers the four types of accounting methods.

IMPORTANT The DM interface supports Admin and read-only privileges only. Therefore, the method lists for Authorization and Accounting are shown with Exec Commands with privilege levels 5 and 10 only.

Exec(Shell)

Exec Shell runs accounting for the EXEC shell session.

Add an Exec(Shell) Accounting Method

1. Click Add.
2. Enter the name of the AAA method.
3. Choose Accounting from the Method pull-down menu.
4. Choose Exec(Shell) from the Type pull-down menu.
5. Choose start-stop from the Accounting Type pull-down menu.
6. Choose from the available servers in the left column and use the arrows to assign the server to the group.
7. Click OK

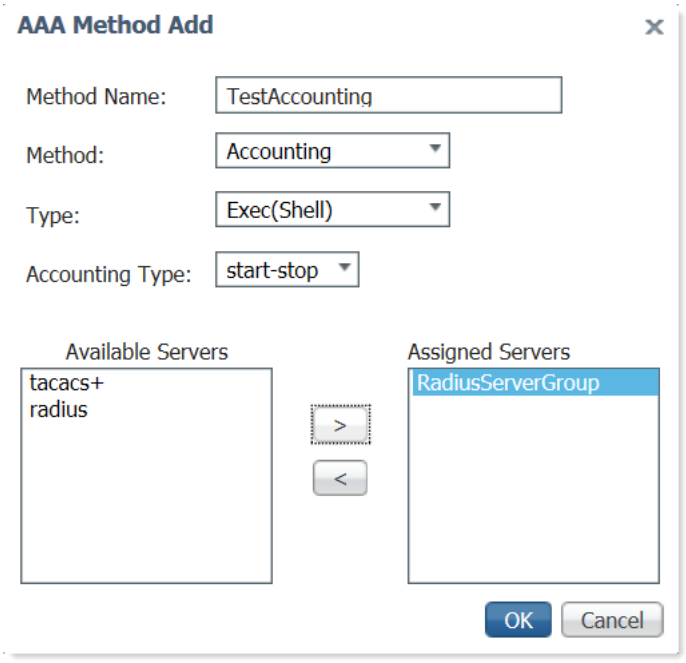


Table 33 - Accounting Exec(Shell) Fields

Field	Description
Method Name	The name of the AAA method.
Method	The AAA Method options dynamically change Type options: • Authentication - identifies user, based on username and password (login) • Authorization - allows access based on user identity • Accounting - Exec Commands, Exec(Shell), and System options are supported
Type	• Exec(Shell) - determines if a user is allowed to run an EXEC shell • Exec Commands - determines if a user can execute a command in place of the current shell • System - accounts for all system-level events
Accounting Type	• Start-stop - sends the accounting record as soon as a session begins • Stop-only - sends the accounting record only when the session ends • None - no authentication check is performed
Available Servers	Servers available for assignment to the group.
Assigned Servers	List of assigned servers.

Exec Commands

This section covers two accounting types of Exec Commands, which run accounting for all commands at the specified privilege level. Valid privilege level entries are integers 0…15. Device Manager supports only read-only (level 5) and admin (level 15) privileges. Therefore, methods applied to Device Manager must be configured with 5 and 15.

Accounting Exec Commands Stop-only

Accounting type stop-only sends a stop accounting record for all cases including authentication failures.

Add an Exec Commands Stop-only Accounting Method

1. Click Add.
2. Enter the name of the AAA method.
3. Choose Accounting from the Method pull-down menu.
4. Choose Exec Commands from the Type pull-down menu.
5. Enter the number of the privilege level.
6. Choose stop-only from the Accounting Type pull-down menu.
7. Choose from the available servers in the left column and use the arrows to assign the server to the group.

8. Click OK

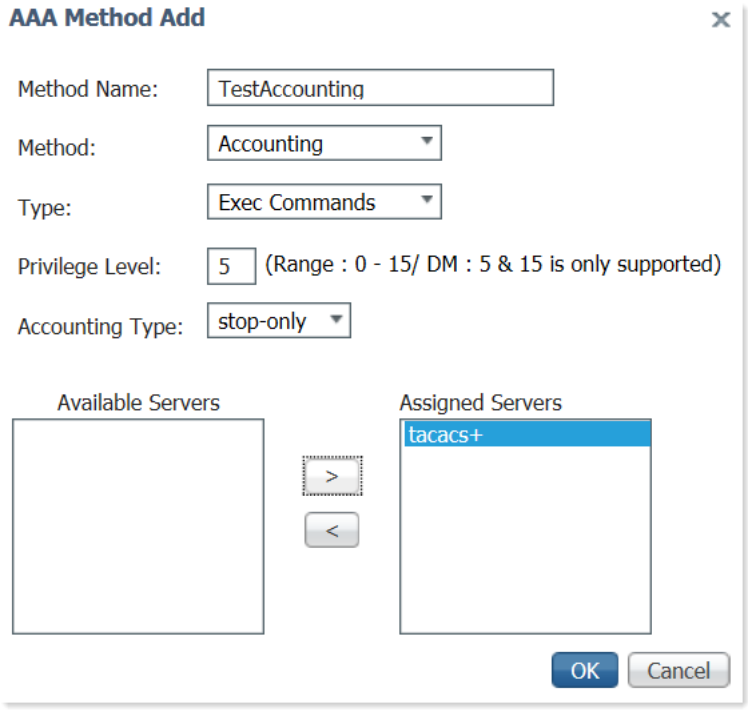


Table 34 - Accounting Exec Commands Stop-only Fields

Field	Description
Method Name	The name of the AAA method.
Method	The AAA Method options dynamically change Type options: • Authentication - identifies user, based on username and password (login) • Authorization - allows access based on user identity • Accounting - Exec Commands, Exec(Shell), and System options are supported
Type	• Exec Commands - determines if a user can execute a command in place of the current shell • Exec(Shell) - determines if a user is allowed to run an EXEC shell • System - accounts for all system-level events
Privilege Level	Specifies Privilege Level
Accounting Type	• Start-stop - sends the accounting record as soon as a session begins • Stop-only - sends the accounting record only when the session ends • None - no authentication check is performed
Available Servers	Servers available for assignment to the group.
Assigned Servers	List of assigned servers.

Accounting Exec Commands none

Add an Exec Commands None Accounting Method:

1. Click Add.
2. Enter the name of the AAA method.
3. Choose Accounting from the Method pull-down menu.
4. Choose Exec Commands from the Type pull-down menu.
5. Enter the number of the privilege level.
6. Choose none from the Accounting Type pull-down menu.

7. Click OK

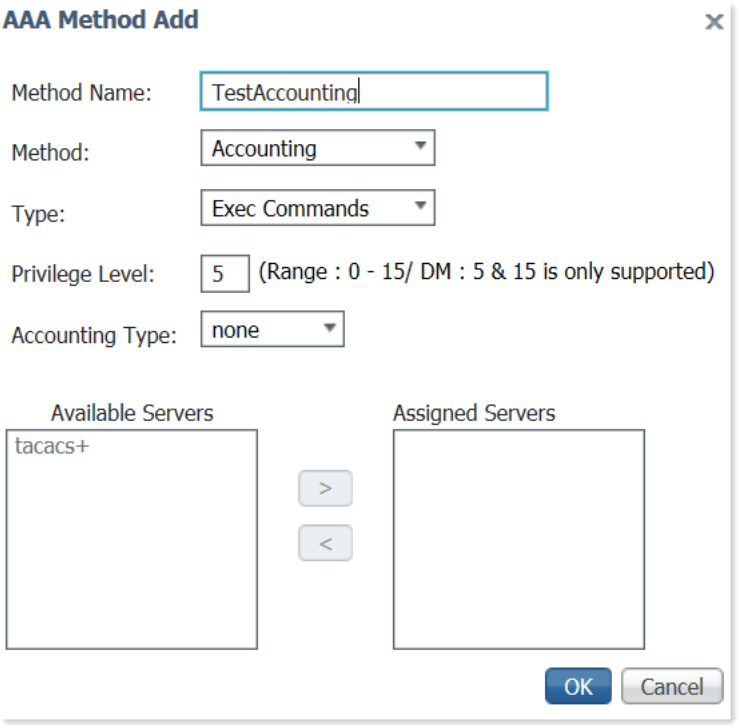


Table 35 - Accounting Exec Commands None Fields

Field	Description
Method Name	The name of the AAA method.
Method	The AAA Method options dynamically change Type options: • Authentication - identifies user based on username and password (login) • Authorization - allows access based on user identity • Accounting - Exec Commands, Exec(Shell), and System options are supported
Type	• Exec Commands - determines if a user can execute a command in place of the current shell • Exec(Shell) - determines if a user is allowed to run an EXEC shell • System - accounts for all system-level events
Privilege Level	Specifies Privilege Level
Accounting Type	• Start-stop - sends the accounting record as soon as a session begins • Stop-only - sends the accounting record only when the session ends • None - no authentication check is performed
Available Servers	Servers available for assignment to the group.
Assigned Servers	List of assigned servers.

System

System performs accounting for all system-level events that are not associated with users, such as reloads.

Accounting Type System start-stop

Accounting type System start-stop sends a system-level accounting record as soon as a session begins.

Add an Exec Commands Start-stop Accounting Method

1. Click Add.
2. Choose Accounting from the Method pull-down menu.
3. Choose System from the Type pull-down menu.
4. Choose start-stop from the Accounting Type pull-down menu.
5. Click OK

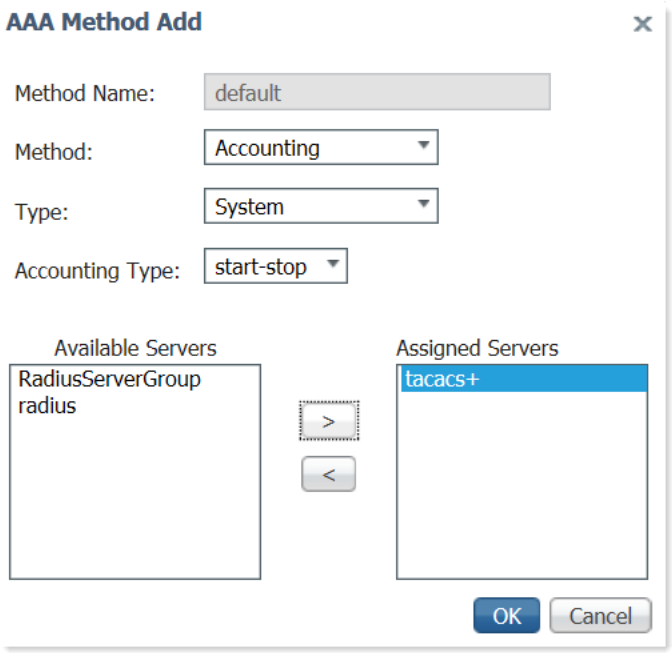


Table 36 - Accounting System Fields

Field	Description
Method Name	Field is not editable and auto-populated with default.
Method	The AAA Method options dynamically change Type options: • Authentication - identifies user based on username and password (login) • Authorization - allows access based on user identity • Accounting - Exec Commands, Exec(Shell), and System options are supported
Type	• Exec Commands - determines if a user can execute a command in place of the current shell • Exec(Shell) - determines if a user is allowed to run an EXEC shell • System - accounts for all system-level events
Accounting Type	• Start-stop - sends the accounting record as soon as a session begins • None - no authentication check is performed
Available Servers	Use the arrows to move servers to and from the list of available servers.
Assigned Servers	Use the arrows to move servers to and from the list of assigned servers.

EXAMPLE: Accounting Type System none

Accounting type System none does not perform an authentication check.

Add a System None Accounting Method:

1. Click Add.
2. Choose Accounting from the Method pull-down menu.
3. Choose System from the Type pull-down menu.
4. Choose none from the Accounting Type pull-down menu.
5. Click OK.

Edit AAA Methods

Aside from server assignments, only the Fallback to Local checkbox can be edited on the AAA Method Add authentication and authorization dialog boxes. The accounting dialog box does not have the Fallback to Local checkbox. All other fields are not editable on any of the AAA Method Add dialog boxes.

TACACS+ or RADIUS servers must be configured to edit a AAA method.

AAA Interface

Use the AAA Interface tab to associate the method lists created on the AAA Methods tab to the interfaces (Console, VTY[SSH/Telnet], and DM). The method lists created on the AAA Interface tab are available in the Authentication pull-down menu.

To associate each interface with a method, use the following steps.

1. Choose the Authentication method from the pull-down menu.
2. Check the method name of the Authorization method.
3. Check the name of the Accounting method.
   - Device Manager supports only read-only (level5) and admin (level 15) privileges. Therefore, only methods that are configured with 5 and 15 are available for the DM interface.
   - Only Accounting methods configured with Exec Commands are available for the DM interface configuration.

IMPORTANT Any change to Authentication and Authorization of the DM interface results in a redirect to the DM login page.

4. Click Submit.

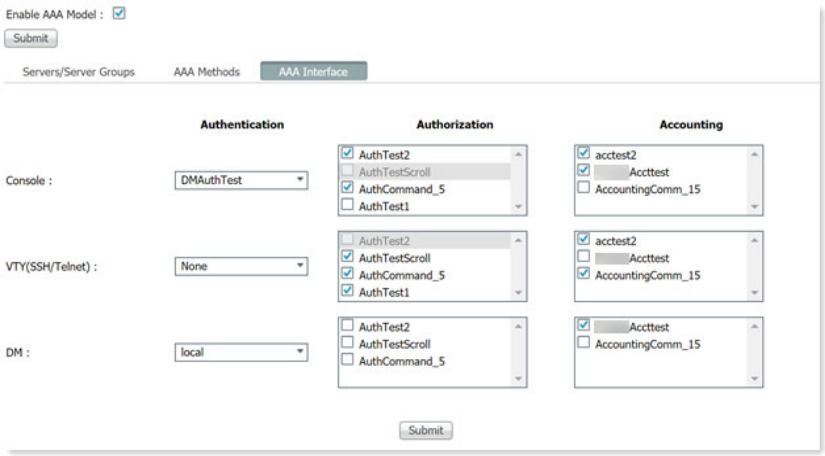


Table 37 - AAA Interface Fields

Field	Descriptions
Authentication	Choose the Authentication method from the pull-down menu.
Authorization	Check the method name of the Authorization method.
Accounting	Check the name of the Accounting method.

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.

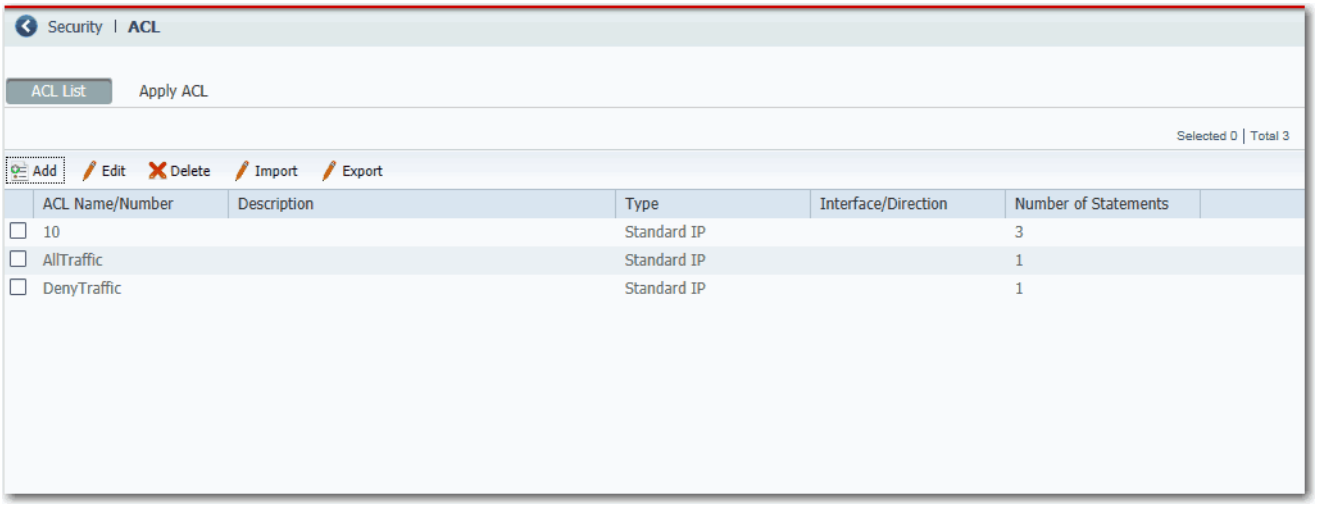
An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies whether to permit or deny packets. An ACE also specifies a set of conditions a packet must satisfy to match the ACE. The meaning of permit or deny depends on the context in which the ACL is used.

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

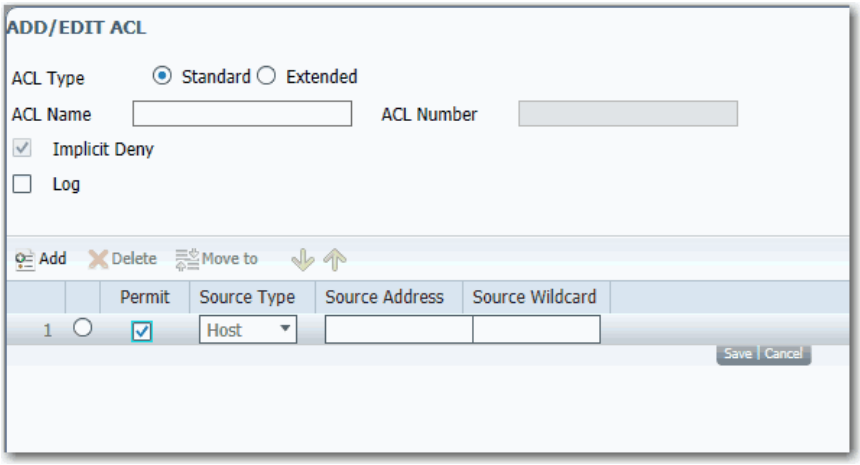
The ACL page shows the standard and extended ACLs defined on the switch. Once you add an ACL to the ACL List tab, you can apply it to a port and specify a direction on the Apply ACL tab.

To configure an ACL, from the Configure menu, choose ACL.



Create an ACL

1. From the ACL page, click the ACL List tab.
2. Click Add and complete the fields in the header area.

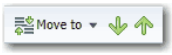


Field	Description
ACL Type	Click Standard or Extended: • Standard (default)—Uses source addresses. • Extended—Uses source and destination addresses and optional protocol type information.
ACL Name	Type an alphanumeric name to identify the ACL. Named access lists are more convenient than numbered access lists. 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.

Field	Description
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 Log 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. The source wildcard is an inverted subnet mask. For example, a subnet mask of 255.255.255.0 inverts to a wildcard mask of 0.0.0.255.
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. The source wildcard is an inverted subnet mask. For example, a subnet mask of 255.255.255.0 inverts to a wildcard mask of 0.0.0.255.
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 

.

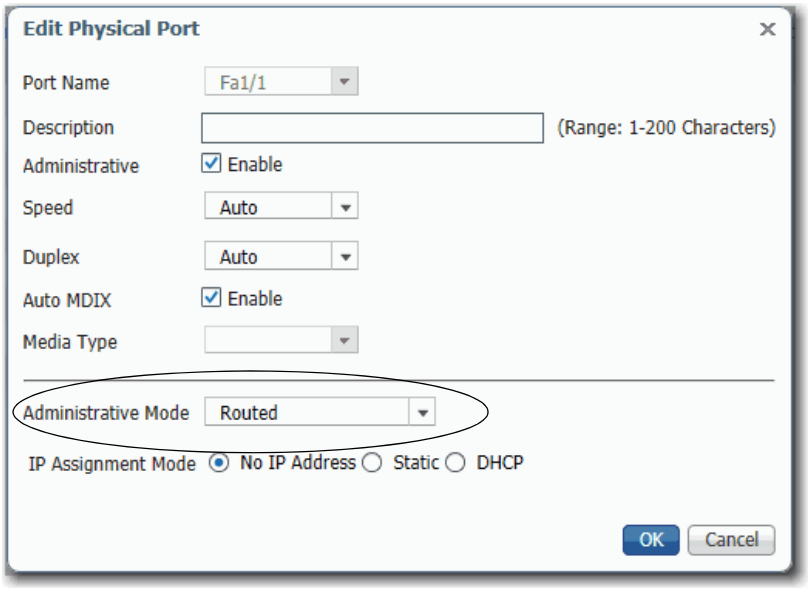
IMPORTANT The order of the conditions is critical to whether a packet is forwarded. The first condition in the list that matches a packet allows the packet to be forwarded. After the first match, the switch stops testing.

7. Click Submit.

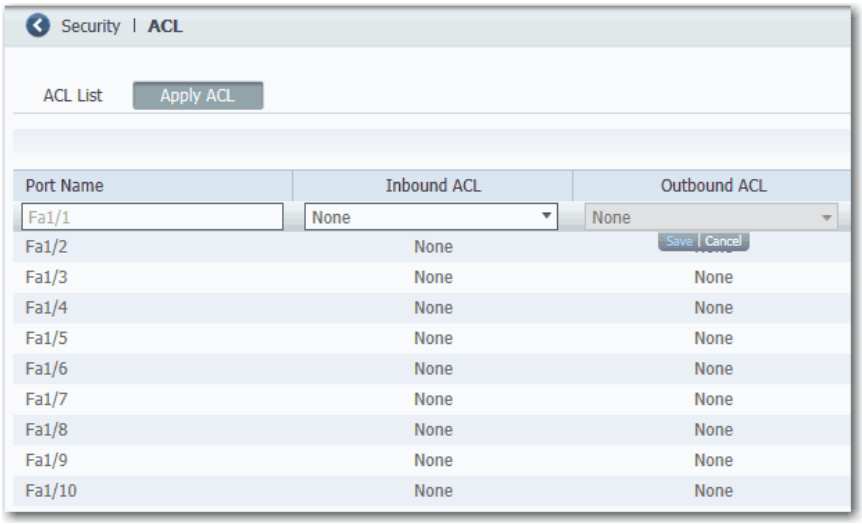
Apply an ACL to a Port

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 that are assigned to an Access VLAN. You can configure these port settings in the Administrative Mode field on the Edit Physical Port page. For more information about port setting configuration, see page 52.



1. From the ACL page, 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.

Switch	Alarm Description
Stratix 5400 switch	You can connect two alarm inputs from external devices to the switch, 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	You can connect two alarm inputs from external devices to the switch, 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 (N.O.) and one normally closed (N.C.) 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 a condition does not match its parameters, the switch triggers an alarm or system message. By default, the switch sends the system messages to the Syslog. 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.

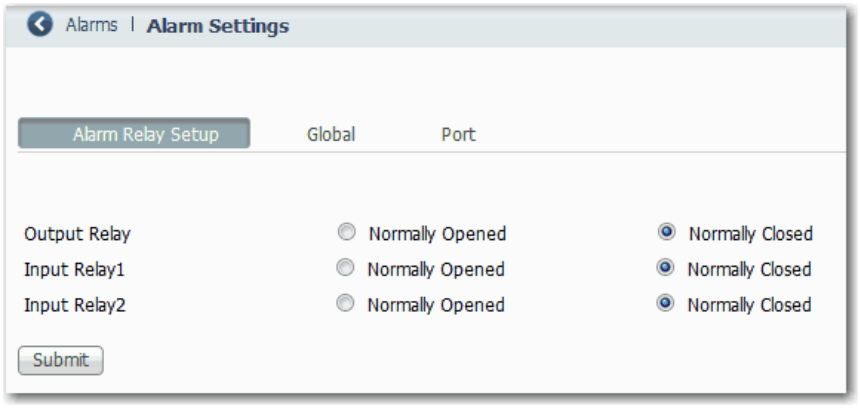
Alarm Relay Settings

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.

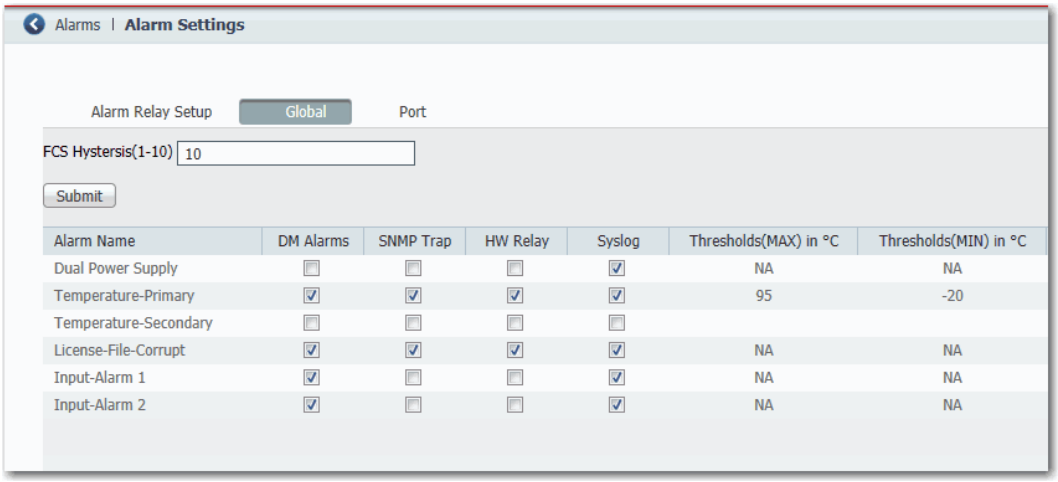
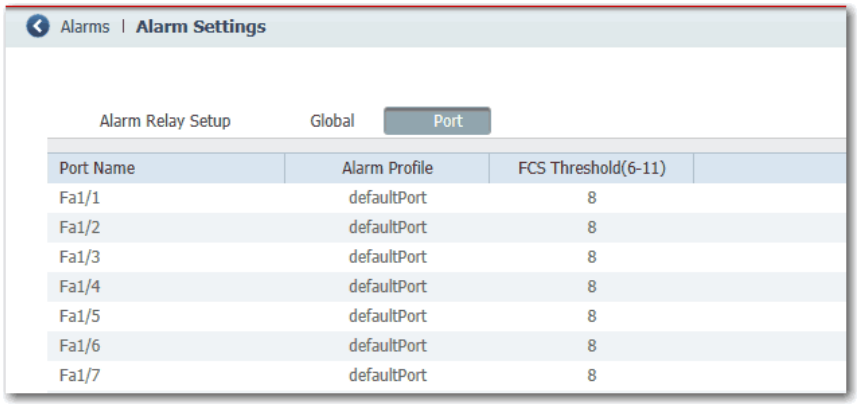


Table 38 - Global Tab Fields

Field	Description
FCS Hysteresis (1-10)	The frame check sequence (FCS) error hysteresis threshold determines when an alarm condition is cleared. This value is expressed as a percentage of fluctuation from the FCS bit error rate. The default global setting is 10 percent. You can adjust the percentage to help 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. Also, this setting can be configured on an individual port by clicking the Port tab.
Alarm Name	These types of alarms can be enabled or disabled on a global level: • 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—An alarm is 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— An alarm is 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 page.
HW Relay	If the alarm relay is triggered, the switch sends a fault signal to a connected external alarm device, such as a bell or light.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Monitor > Syslog page.
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.



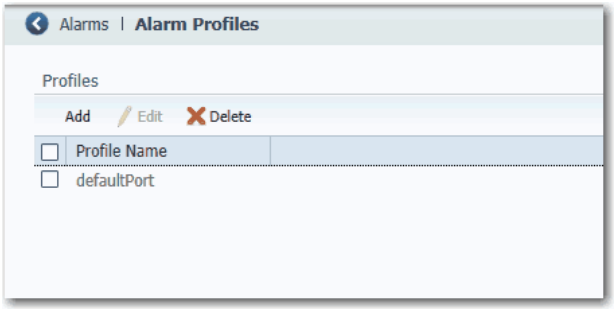
For each port, choose an Alarm Profile and set the FCS threshold. The frame check sequence (FCS) error hysteresis threshold is expressed as a percentage of fluctuation from the FCS bit error rate. The default port setting is 8 percent. You can adjust the percentage to help prevent toggling the alarm 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 page, you can configure the alarms and actions for an alarm profile.

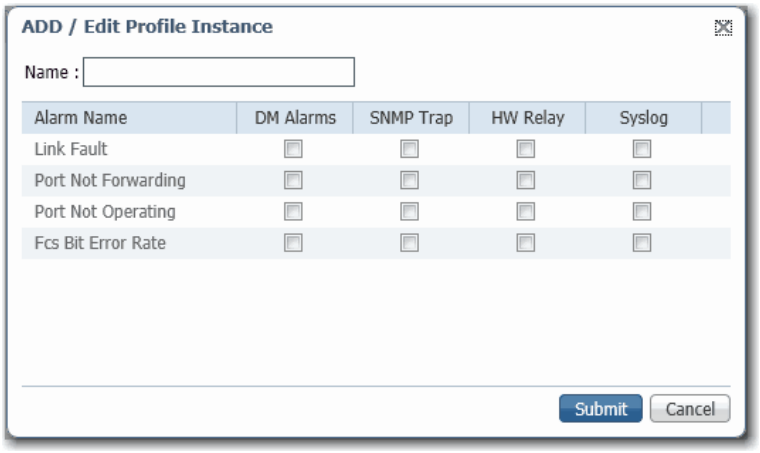


Table 39 - Add/Edit Profile Instance Fields

Field	Description
Name	A unique name for the alarm profile.
Alarm Name	The alarm profile can include these alarms: • Link Fault—The switch generates a Link Fault alarm when problems with the physical layer of a port cause unreliable data transmission. A typical Link Fault condition is loss of signal or clock. The Link Fault alarm is cleared automatically when the condition is cleared. • Port Not Forwarding—The switch generates a Port Not Forwarding alarm when a port is not forwarding packets. This alarm is cleared automatically when the port begins to forward packets. • Port Not Operating—The switch generates a Port Not Operating alarm when a port fails during the startup self-test. When triggered, the Port Not Operating alarm is only cleared when the switch is restarted and the port is operational. • Fcs Bit Error Rate—The switch generates an FCS Bit Error Rate alarm when the actual FCS bit error-rate is close to the configured rate.
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 page.
HW Relay	If the alarm relay is triggered, the switch sends a fault signal to a connected external alarm device, such as a bell or light.
Syslog	Alarm traps are recorded in the Syslog. You can view the Syslog on the Monitor > Syslog page.

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 16.

To configure PTP, you choose one of these clock modes:

- Boundary
- End to End Transparent
- Peer to Peer Transparent
- Forward
- NTP-PTP Clock

For more information about these modes, refer to the Converged Plantwide Ethernet Design and Implementation Guide, publication ENET-TD001.

IEEE 1588 Power Profile

The IEEE 1588 Power Profile feature is available only on the Stratix 5400 and 5410 switches.

The IEEE 1588 Power Profile defines specific or allowed values for PTP networks used in utility applications. The defined values include the optimum physical layer, higher-level protocol for PTP messages, and the preferred best master clock algorithm. The Power Profile values ensure consistent and reliable network time distribution in utility applications.

The switch is optimized for PTP as follows:

- Hardware—the switch uses field-programmable gate array (FPGA) and the physical layer of the OSI model (PHY) for the PTP function. The PHY time stamps the Fast Ethernet and Gigabit Ethernet ports.
- Software—in Power Profile mode, the switch uses the configuration values defined in the IEEE 1588 Power Profile standard.

The following table lists the configuration values defined in IEEE 1588 Power Profile and the values that the switch uses for each PTP profile mode.

Table 40 - Configuration Values for the IEEE PTP Power Profile and Switch Modes

PTP Field	Power Profile Value	Switch Configuration Value	
		Power Profile Mode	**Default Profile Mode**
Message Transmission	Ethernet 802.3 with Ethertype 0X88F7. PTP messages are sent as 802.1Q tagged Ethernet frames with a default VLAN 0 and 0 and default priority 4.	**Access Ports**—Untagged Layer 2 packets. **Trunk Ports**—802.1Q tagged Layer 2 packets with native VLAN on the port and default priority value of 4.	Layer 3 packets. By default, 802.1Q tagging is disabled.
MAC address—Non-peer delay messages	01-1B-19-00-00-00	01-1B-19-00-00-00	01-1B-19-00-00-00
MAC address—Peer delay messages	01-80-C2-00-00-0E	01-80-C2-00-00-0E	Not applicable to this mode.
Domain number	0	0	0
Path delay calculation	Peer-to-peer transparent clocks	Peer-to-peer transparent clocks using the peer_delay mechanism	End-to-end transparent clocks using the delay-request mechanism
BMCA	Enabled	Enabled	Enabled
Clock type	Two-step clocks are supported	Two-step	Two-step
Time scale	Epoch(1)	Epoch	Epoch
Grandmaster ID and local time determination	PTP-specific TLV (type, length, value) to indicate Grandmaster ID	PTP-specific TLV to indicate Grandmaster ID	PTP-specific TLV to indicate Grandmaster ID
Time accuracy over network hops	Over 16 hops, slave device synchronization accuracy is within 1 µs.	Over 16 hops, slave device synchronization accuracy is within 1 µs.	Not applicable in this mode.

(1) Epoch = Elapsed time since epoch start.

Power 2017 Profile

The power 2017 profile extends the capabilities of Power profile and is only supported in Peer to Peer Transparent Clock mode.

The most noticeable difference between Power and Power 2017 is the use of domain number 254 in Power 2017. Power 2017 can be used for power system applications requiring high-precision time synchronization, device interoperability, and failure management.

Boundary Mode

In Boundary mode, the switch participates in the selection of 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 that is connected to the switch, the switch synchronizes as a child to that 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 that is caused by clock offsets and network delays. This mode can reduce 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.

DSCP Values for PTP

This feature allows for the configuration of Differentiated Services Code Point (DSCP) values for PTP packets through the CLI. The change in DSCP value is kept in sync with changes made through CIP. These changes are allowed only when the device is in the Boundary clock or ntp-ptp clock mode and configured in the Default Profile.

DSCP values are used for QoS configuration to prioritize IP packets as they pass through the network. The default values are 59 for PTP Event messages, and 47 for PTP General messages. The DSCP value is placed in the TOS field of the IP header.

Figure 1 - DSCP Configuration Screen

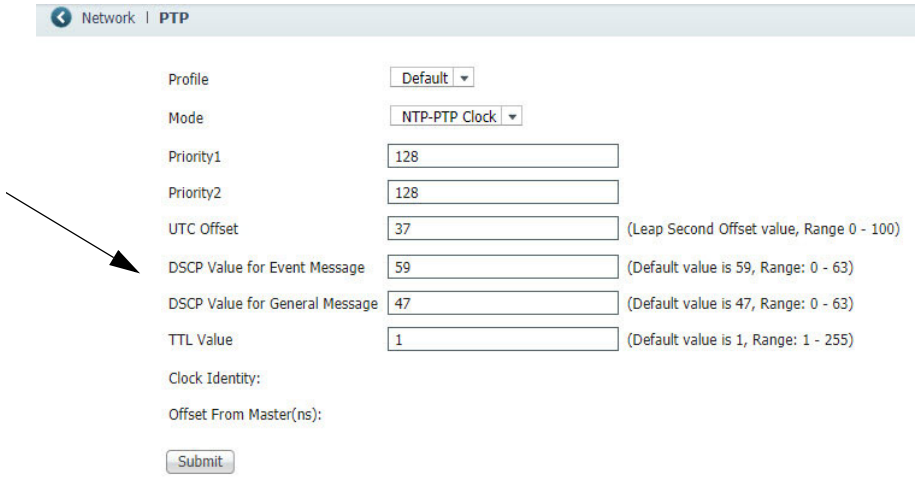


Table 41 - DSCP Values for PTP

Message	Description	Timestamp	Range
DSCP Value for Event Message	DSCP messages are used for QOS configuration to prioritize the PTP packets as they pass through the network.	Yes	0...63 (Default 59)
DSCP Value for General Message		No	0...63 (Default 47)

End to End Transparent Mode

IMPORTANT End to End Transparent mode does not work with redundant gateways in a Device Level Ring (DLR) topology. For more information about redundant gateways, see page 101.

In End to End Transparent mode, the switch transparently synchronizes all clocks with the master clock that is connected to it. All ports are enabled by default. This device corrects the delay that is incurred by every packet that passes 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.

Peer to Peer Transparent Mode

In Peer to Peer Transparent mode, the switch acts as a transparent clock to improve synchronization between the master and slave clocks. The transparent clock measures the time that the packet spends passing through the switch and adjusts for packet delay caused by varying queuing delays as the packets pass through the switch.

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

NTP-PTP Clock mode is available in 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). This will take the Time of Day (ToD) reference from NTP and apply it to your PTP system.
- If configured as a secondary Grandmaster, the switch functions as a boundary clock to forward time, helping to maintain 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.

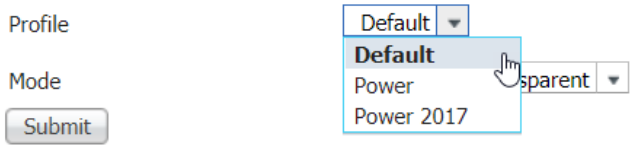
NTP-PTP Clock mode enables tightly controlled PTP zones, such as motion applications, to maintain time relative to other devices outside the PTP zone that use NTP. In this scenario, NTP-PTP clock time is beneficial for logging and event tracking.

Before you configure a switch to use NTP-PTP clock mode, do the following:

- Configure NTP as described on page 202. While NTP-PTP Clock mode requires only one NTP time source, as a best practice, we recommend that you configure two or more NTP time sources.
- Make sure that the NTP clock is stable.
- Know the priority settings that are assigned to other PTP devices, so that you can configure the switch as the Grandmaster.

Configure Time Synchronization via Device Manager

1. From the Configure menu, choose PTP.
2. To configure your profile, choose either Default for the CIP Sync profile, Power for the power profile, or Power 2017 from the Profile pull-down menu.



The Power 2017 profile is only available in the End to End Transparent mode.

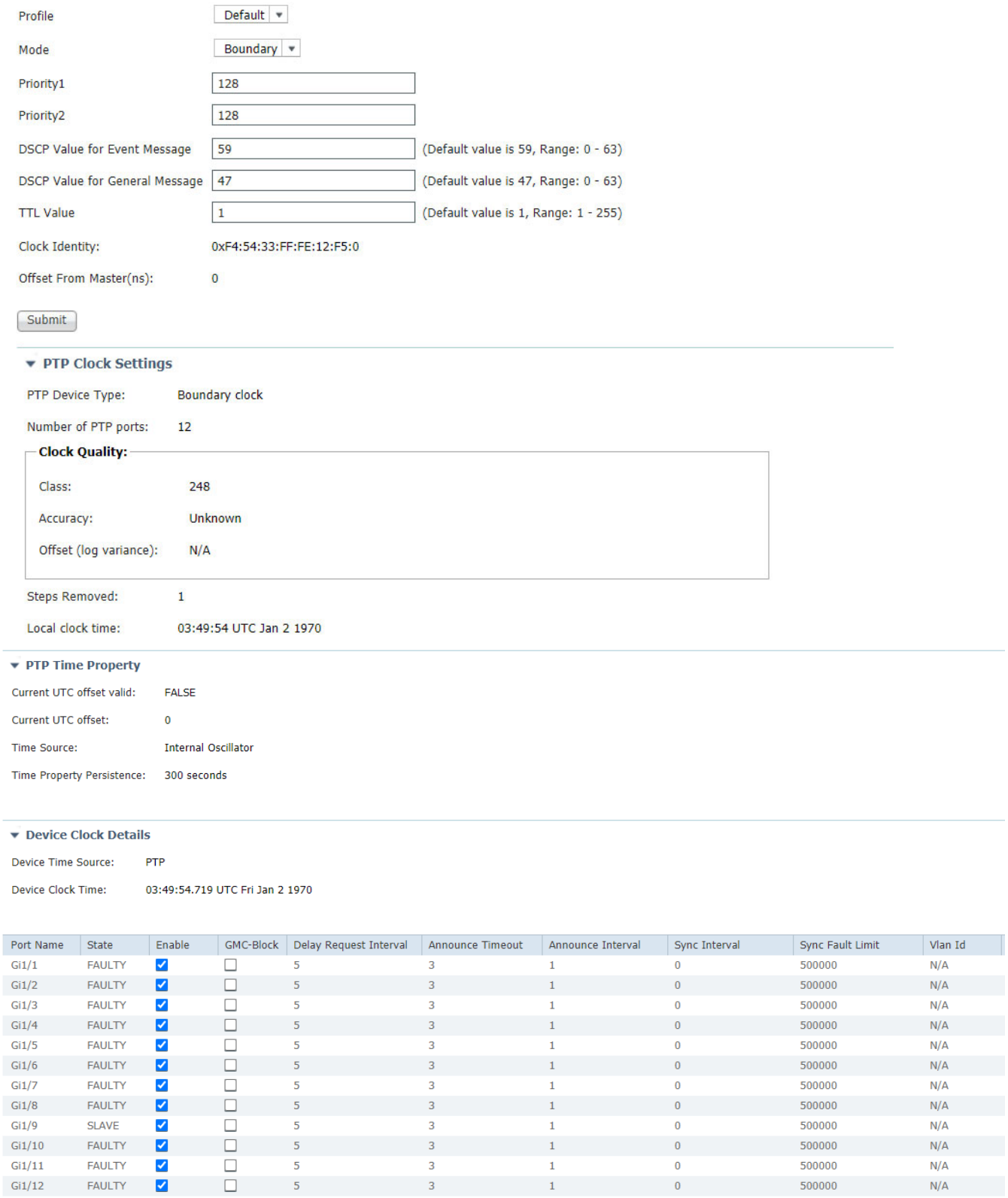
3. From the Mode pull-down menu, choose a mode.

   The modes and fields that appear vary based on the switch model and mode setting.
4. Click Submit.
5. To complete the remaining fields, refer to the figure and table that corresponds to your mode.

Mode	Page
Configure Boundary Mode	98
Configure End to End Transparent Mode	101
Configure Peer to Peer Transparent Mode	102
Configure Forward Mode	102
Configure NTP-PTP Clock Mode	103

Configure Boundary Mode

Figure 2 - Boundary Mode



Port Name	State	Enable	GMC-Block	Delay Request Interval	Announce Timeout	Announce Interval	Sync Interval	Sync Fault Limit	Vlan Id
Gi1/1	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/2	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/3	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/4	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/5	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/6	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/7	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/8	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/9	SLAVE	☑	☐	5	3	1	0	500000	N/A
Gi1/10	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/11	FAULTY	☑	☐	5	3	1	0	500000	N/A
Gi1/12	FAULTY	☑	☐	5	3	1	0	500000	N/A

Table 42 - Boundary Mode Fields

Field	Description
General Settings	
Priority 1	The clock selection process is determined by the relative priority of the switches in the network. Priority 1 is used to override the default criteria for best master clock selection. Range: 0...255 Default: 128
Priority 2	A tie-breaker between two devices that are equally matched in the default criteria. For example, you can give a specific switch priority over other identical switches. Range: 0...255 Default: 128
DSCP Value for Event Message	Differentiated Services Code Point (DSCP) value for Event messages (PTP messages that are tagged with a timestamp). DSCP values are used for Quality of Service (QoS) configuration to prioritize the PTP packets as they pass through the network. Range: 0...63 Default: 59
DSCP Value for General Message	DSCP value for general messages (PTP messages that are not tagged with a timestamp). DSCP values are used for QoS configuration to prioritize the PTP packets as they pass through the network. Range: 0...63 Default: 47
TTL Value	Configure the Time To Live (TTL) value for PTP multicast packets so that PTP multicast traffic can pass through non-PTP capable devices. Range: 1...255 Default: 1
Clock Identity	Displays a unique identifier for the clock.
Offset from Master	Displays the time offset in nanoseconds between the slave and master clocks.
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 that are 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.
Time Source	Displays the time source that is 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 that is 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—10 Gigabit 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 help 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 synchronizes 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 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.
GMC-Block	This feature prevents certain interface ports from transitioning to a PTP Slave state to protect from rogue PTP devices on the edge of the network. The feature provides configuration knobs to mark specific interfaces on the switch. The default configuration on the interface should not have this feature enabled.

Table 42 - Boundary Mode Fields (Continued)

Field	Description
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, which are specified as the logarithmic mean in seconds, that must pass without receipt of an announce message from the parent or Grandmaster clock before the switch selects a new parent or Grandmaster clock. Valid values: 2...10 Default: 3 (8 seconds)
Announce Interval	Type the time interval, which is 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, which is specified as the logarithmic mean in seconds, to send 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: 500000 nanoseconds **IMPORTANT:** In systems that have tightly controlled networks, we recommend using 5000...10000 nanoseconds for the sync limit. These networks have a critical need to keep 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.

Configure End to End Transparent Mode

Figure 3 - End to End Transparent Mode

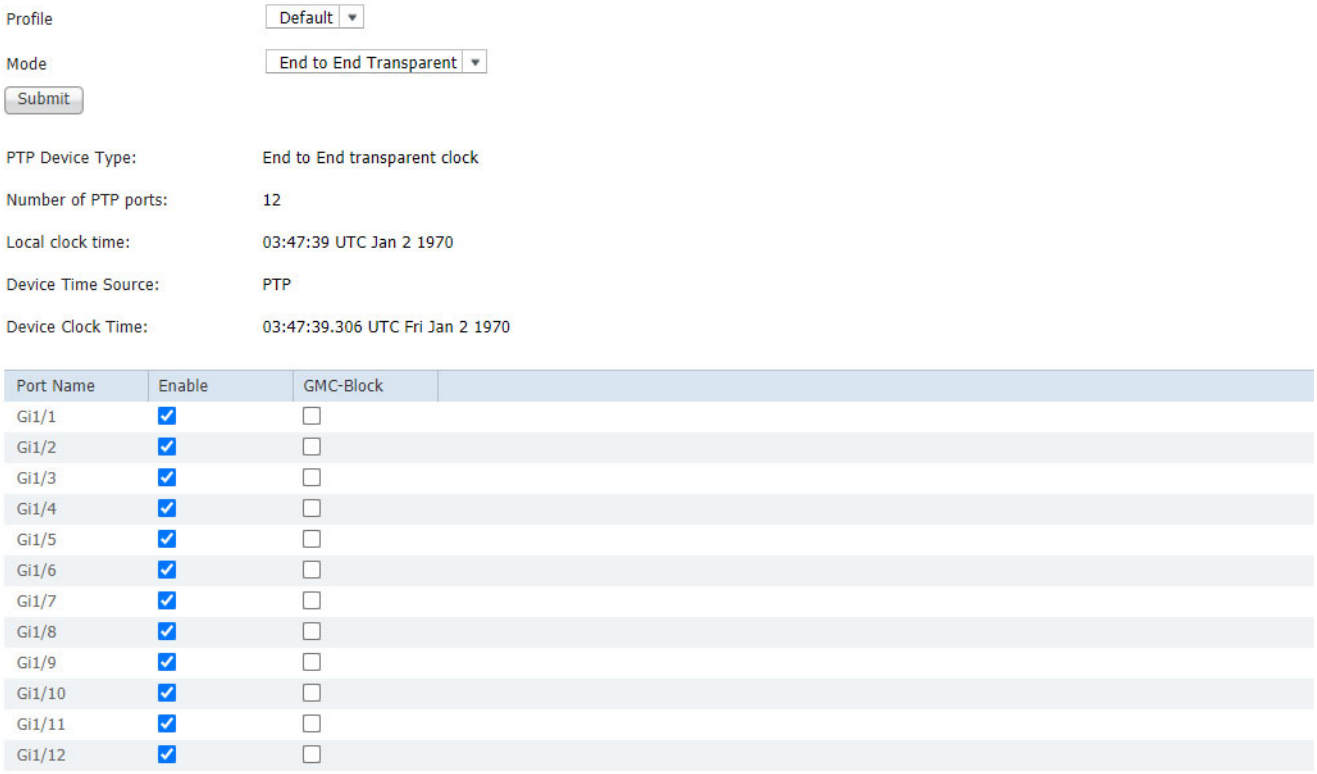


Table 43 - End to End Transparent Mode Fields

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 that are assigned to the PTP clock.
Local clock time	Displays the time stamp of the local clock.
Device Time Source	Displays the time source that is 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—10 Gigabit 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 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.
GMC-Block	This feature prevents certain interface ports from transitioning to a PTP Slave state to protect from rogue PTP devices on the edge of the network. The feature provides configuration knobs to mark specific interfaces on the switch. The default configuration on the interface should not have this feature enabled.

Configure Peer to Peer Transparent Mode

Figure 4 - Peer to Peer Transparent Mode

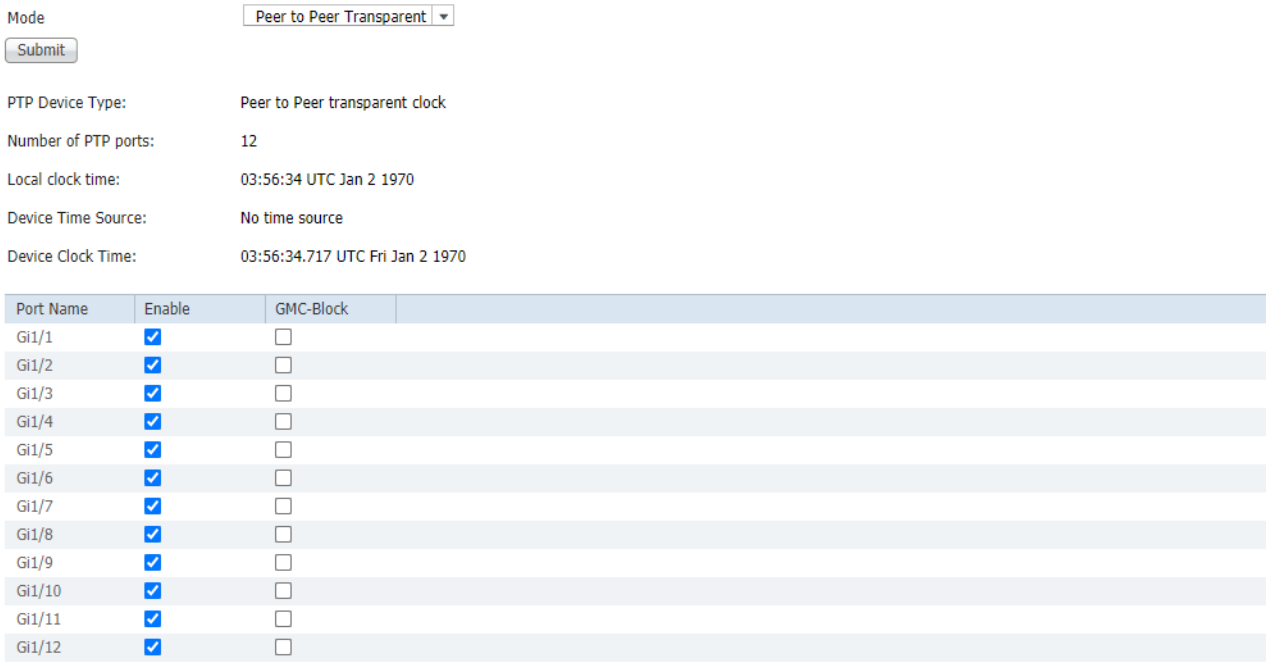


Table 44 - Peer to Peer Transparent Mode Fields

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 that are assigned to the PTP clock.
Local clock time	Displays the time stamp of the local clock.
Device Time Source	Displays the time source that is 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—10 Gigabit 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 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.

Configure Forward Mode

Figure 5 - Forward Mode

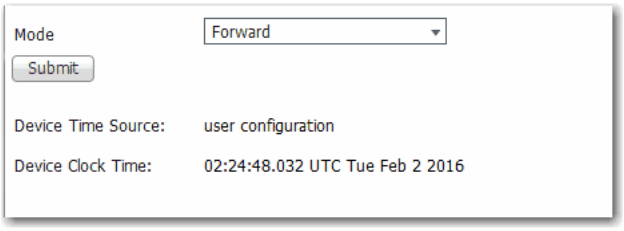


Table 45 - Forward Mode Fields

Field	Description
Device Time Source	Displays the time source that is used by the switch.
Device Clock Time	Displays the time on the switch, obtained from the time source.

Configure NTP-PTP Clock Mode

Figure 6 - NTP-PTP Clock Mode

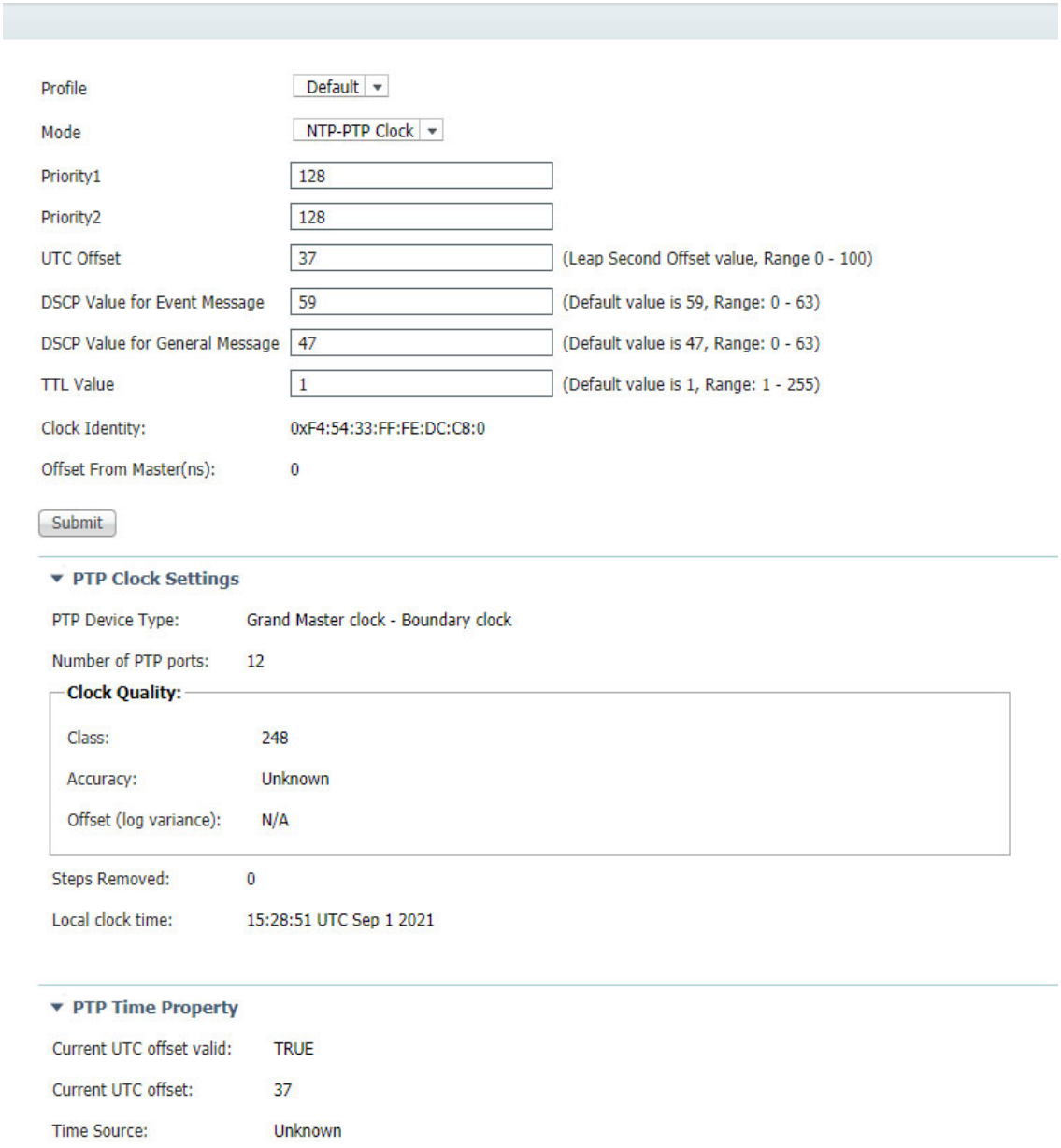


Table 46 - NTP-PTP Clock Mode Fields

Field	Description
General Settings	
Priority 1	The clock selection process is determined by the relative priority of the switches in the network. Priority 1 is used to override the default criteria for best master clock selection. Range: 0...255 Default: 128
Priority 2	A tie-breaker between two devices that are equally matched in the default criteria. For example, you can give a specific switch priority over other identical switches. Range: 0...255 Default: 128
UTC Offset	UTC Offset allows you to configure the adjust-time, which causes the derived PTP time to remain in time with the International Atomic Time (TAI) clock. The PTP announce message carries the leap second offset value. Range: 0...100
DSCP Value for Event Message	Differentiated Services Code Point (DSCP) value for Event messages (PTP messages that are tagged with a timestamp). DSCP values are used for Quality of Service (QoS) configuration to prioritize the PTP packets as they pass through the network. Range: 0...63 Default: 59
DSCP Value for General Message	DSCP value for general messages (PTP messages that are not tagged with a timestamp). DSCP values are used for QoS configuration to prioritize the PTP packets as they pass through the network. Range: 0...63 Default: 47
TTL Value	Configure the Time To Live (TTL) value for PTP multicast packets so that PTP multicast traffic can pass through non-PTP capable devices. Range: 1...255 Default: 1
Clock Identity	Displays a unique identifier for the clock.
Offset from Master	Displays the time offset in nanoseconds between the slave and master clocks.
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 that are 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.
Time Source	Displays the time source that is used by the Grandmaster clock.
Device Clock Details	
Device Time Source	Displays the time source that is 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—10 Gigabit 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 help 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 synchronizes 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 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.

Table 46 - NTP-PTP Clock 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, which are specified as the logarithmic mean in seconds, that must pass without receipt of an announce message from the parent or Grandmaster clock before the switch selects a new parent or Grandmaster clock. Valid values: 2...10 Default: 3 (8 seconds)
Announce Interval	Type the time interval, which is 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, which is specified as the logarithmic mean in seconds, to send 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 in nanoseconds before PTP attempts to reacquire synchronization. Valid values: 50...500000000 ns Default: 500000 ns **IMPORTANT:** In fully time aware systems, we recommend setting the default value to 10000 ns. In systems with motion applications, we recommend setting the default value to 5000 ns.
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	106
End to End	107
Forward	108
NTP-PTP Clock	108

Figure 7 - Boundary Mode

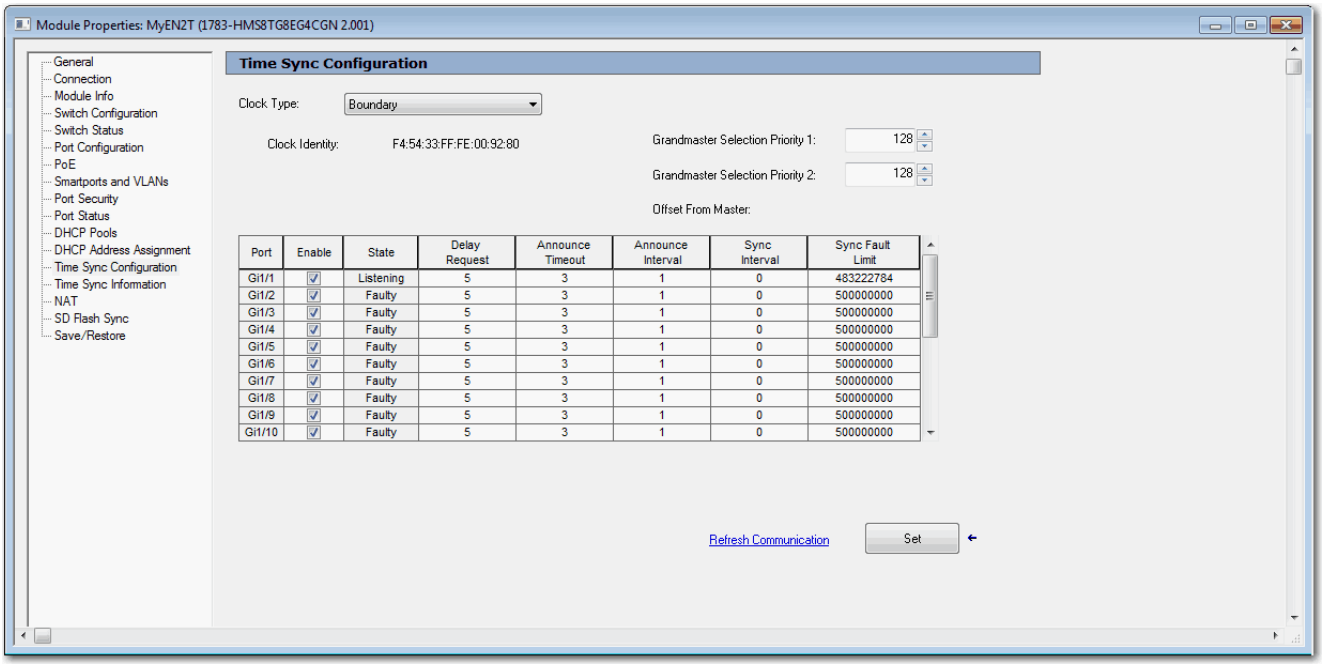


Table 47 - Boundary Mode

Field	Description
Clock Identity	Displays a unique identifier for the clock.
Grandmaster Selection Priority 1	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—10 Gigabit 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 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 help 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 synchronizes 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 47 - 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, which are specified as the logarithmic mean in seconds, that must pass without receipt of an announce message from the parent or Grandmaster clock before the switch selects a new parent or Grandmaster clock. Valid values: 2...10 Default: 3 (8 seconds)
Announce Interval	Type the time interval, which is 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, which is specified as the logarithmic mean in seconds, to send 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:** When changing PTP timing message settings, remember that the system does not operate properly unless all devices in the system have the same values.

Figure 8 - End-to-End Transparent Mode

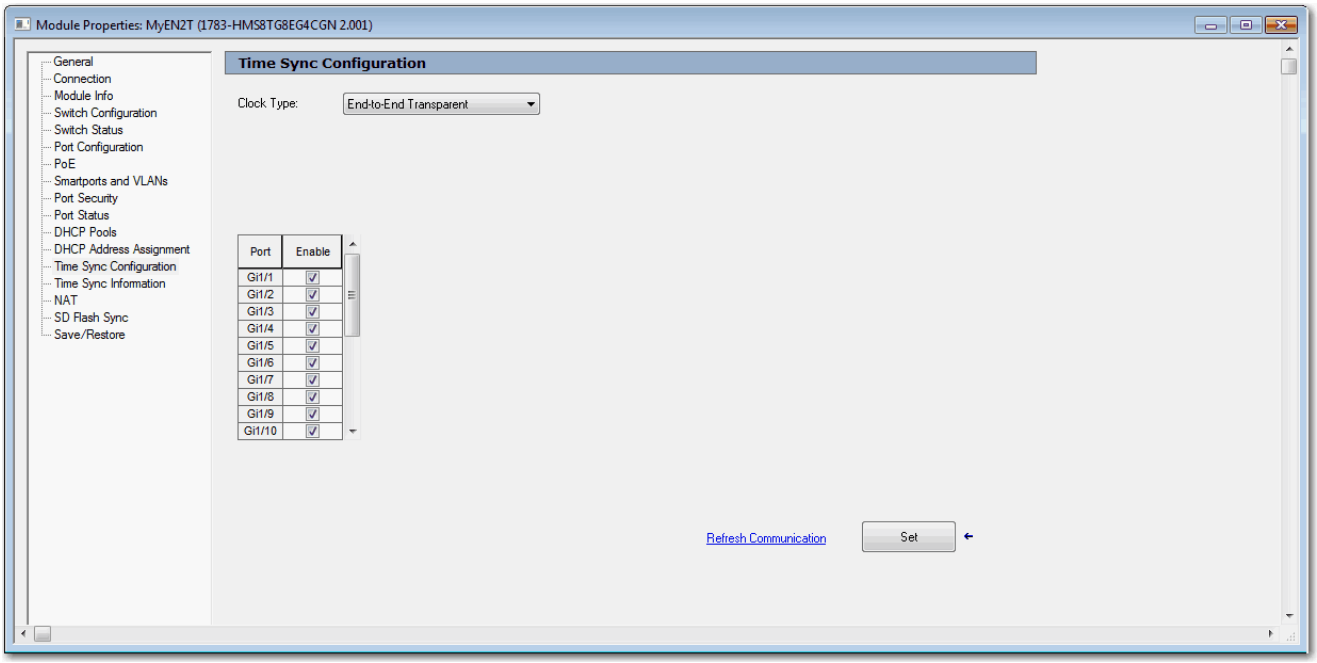


Table 48 - End to End Transparent Mode Fields

Field	Description
Port	Displays the port type and port number: • Fa—Fast Ethernet • Gi—Gigabit Ethernet • Te—10 Gigabit 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 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

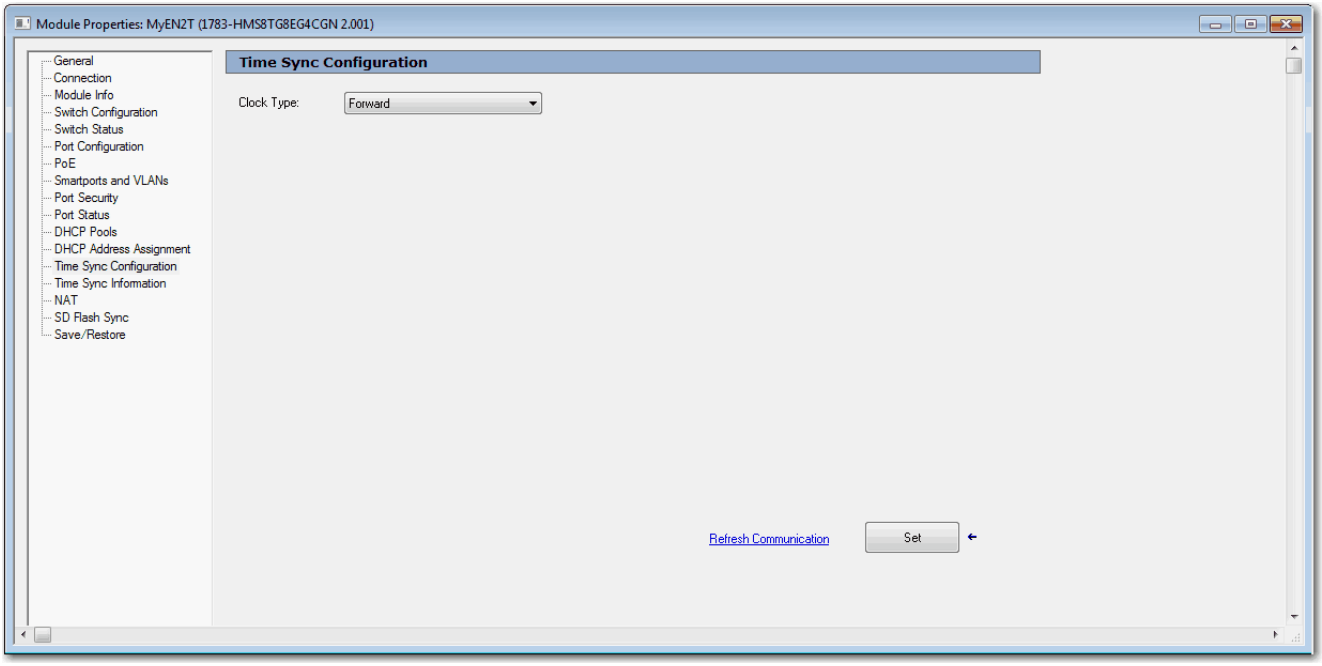


Figure 10 - NTP-PTP Mode

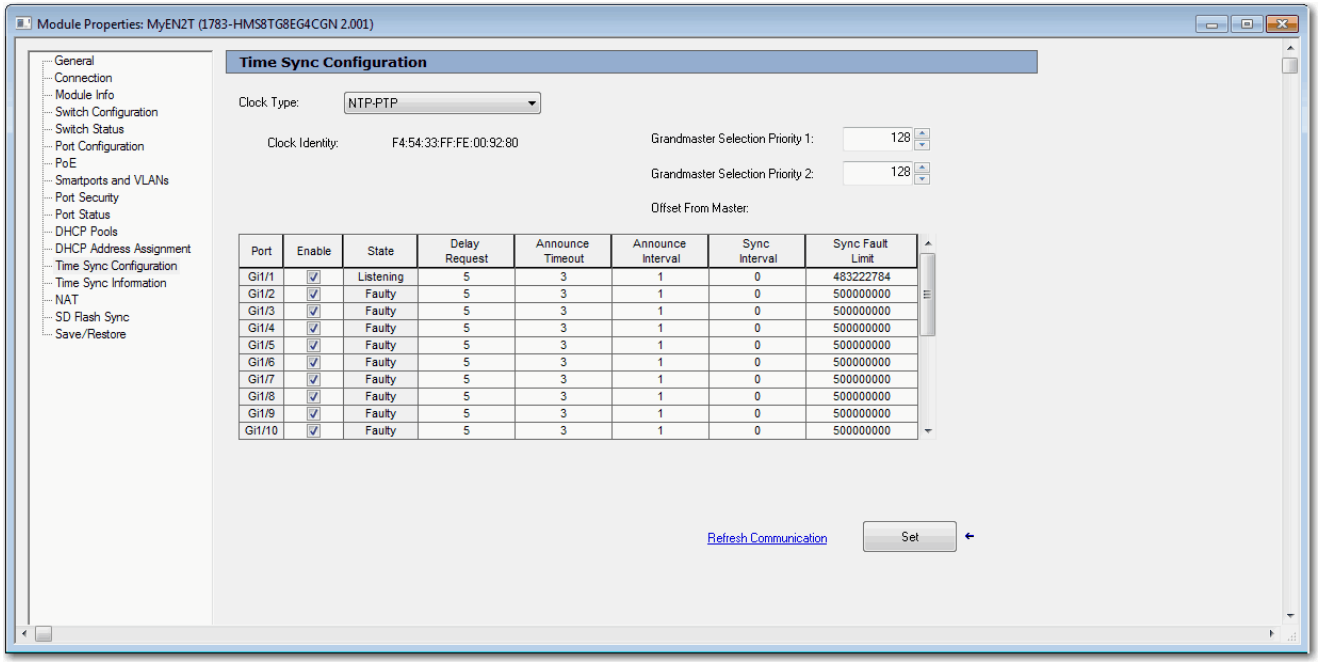


Table 49 - NTP-PTP Mode Fields

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—10 Gigabit 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 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 help 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 synchronizes 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.
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, which are specified as the logarithmic mean in seconds, that must pass without receipt of an announce message from the parent or Grandmaster clock before the switch selects a new parent or Grandmaster clock. Valid values: 2…10 Default: 3 (8 seconds)
Announce Interval	Type the time interval, which is 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, which is specified as the logarithmic mean in seconds, to send 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:** When changing PTP timing message settings, remember that the system does not operate properly unless all devices in the system have the same values.

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 through the IEEE 1588 V 2 End to End Transparent clock mechanism.

Figure 11 - Time Sync Information

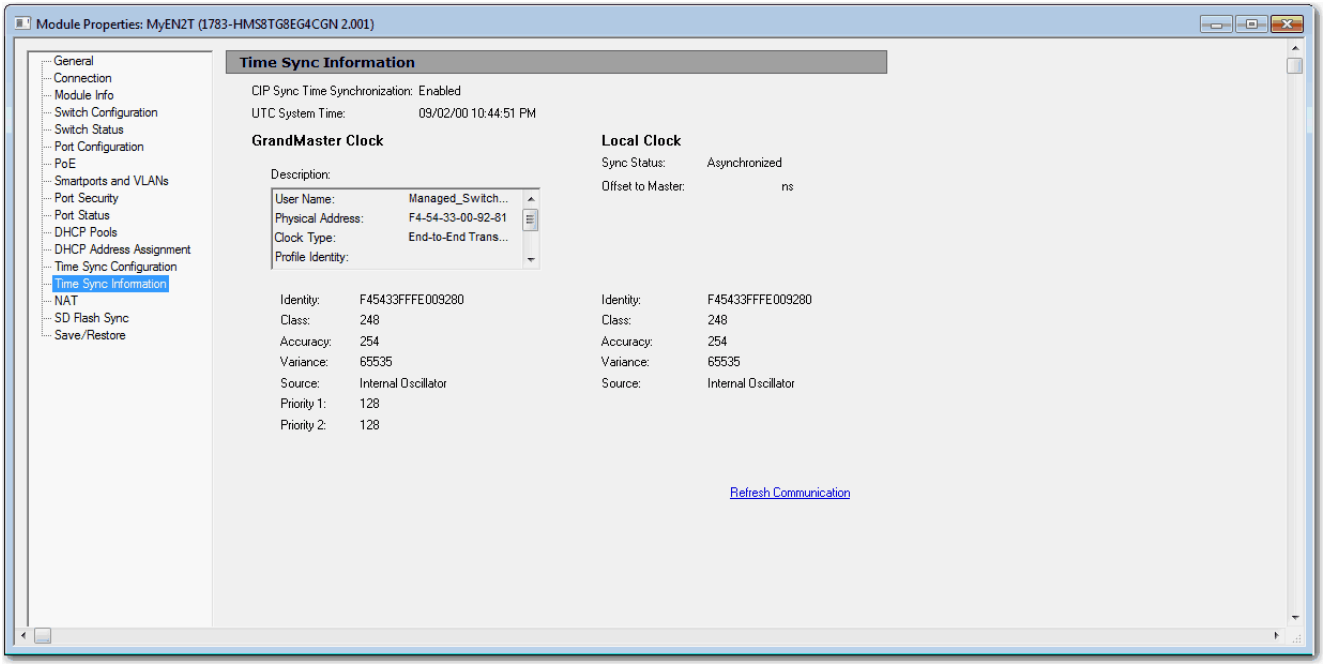


Table 50 - Time Sync Information Fields

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 that starts at 25 ns and ends 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 of 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.

Table 50 - Time Sync Information Fields (Continued)

Field	Description
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 unsynchronized 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 ID into the identifier. • The DeviceNet™ and ControlNet™ protocols encode the Vendor ID and serial number into the identifier.
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 that starts at 25 ns and ends 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 of 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 release 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 the Device Manager. For instructions on accessing the Device Manager via secure connection, see Access Device Manager on page 41.

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 http becomes the default protocol for Device Manager.
- If you upgrade the switch to the non-cryptographic IOS, Telnet remains enabled, SSH remains disabled, and https remains the default protocol for Device Manager.

Device Level Ring (DLR) Topology

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

A DLR network includes the following types of ring nodes:

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

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

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

DLR Requirements and Restrictions

You can configure Stratix 5400 switches and some models of Stratix 5700 and ArmorStratix 5700 switches to participate in a DLR network. For a list of switches that support DLR, see Software Features on page 16.

To be DLR capable, a Stratix 5400 switch must be configured for DLR feature mode, see Feature Mode on page 147.

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.

In a network configured for DLR DHCP, each switch in the ring must have a statically assigned address. Switches in the ring cannot have addresses that are assigned via DLR DHCP.

The DLR DHCP feature requires the DHCP participant list to be created. This list is created when the DLR ring is closed with no faults. The DLR DHCP participant list is maintained until power cycle of the switch. The DLR ring will not provide IP addresses unless the participant list exists. Once the participant list exists, IP addresses will be distributed even when there is a fault in the ring.

DLR Features

The following table lists DLR features supported by Stratix switches. Examples of DLR networks with these features and configuration considerations are described in the EtherNet/IP Device Level Ring Application Technique, publication ENET-AT007.

Feature	Description	Supported Switches
Redundant gateways	Redundant gateways are multiple switches that are connected to one DLR network and connected together through the rest of the network. Redundant gateways provide DLR network resiliency to the rest of the network.	Stratix 5400, Stratix 5700, ArmorStratix 5700 switches that support DLR also support redundant gateways.
DLR DHCP	A switch configured as a DLR ring supervisor can also act as a DHCP server to assign designated IP addresses to ring participants. Assignment of IP addresses is based on ring participant position. If a ring participant fails, a replacement device can be installed in the same position in the ring and automatically receive the same IP address as the replaced device. However, the DLR ring will not provide an IP address unless the participant list exists. This list is created when the DLR ring is closed with no faults.	Stratix 5400, Stratix 5700, ArmorStratix 5700 switches that support DLR also support DLR DHCP.
Multiple rings	Switches compatible with multiple rings support as many as three rings per switch. The rings can share a VLAN, or each ring can be on it sown VLAN.	Stratix 5400 switches support multiple rings. Stratix 5700 and ArmorStratix 5700 switches support only one ring per switch.
DLR VLAN trunking	DLR VLAN trunking allows switches with multiple VLANs to be connected in a DLR network.	Stratix 5400, Stratix 5700, and ArmorStratix 5700 switches.

DLR Port Choices

Table 51 and Table 52 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. See Smartports on page 262.

Table 51 - 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 1783-HMS8TG4CGR	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS8SG4CGN 1783-HMS8SG4CGR	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS4EG8CGN 1783-HMS4EG8CGR	1, 5, 9	2, 6, 10	3, 7, 11	4, 8, 12	1, 7, 9	2, 8,10
1783-HMS16TG4CGN 1783-HMS16TG4CGR	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS8TG8EG4CGN 1783-HMS8TG8EG4CGR	1, 5	2, 6	3, 7	4, 8	9	10
1783-HMS4SG8EG4CGN 1783-HMS4SG8EG4CGR	1, 5, 9	2, 6, 10	3, 7, 11	4, 8, 12	1, 7, 13	2, 8, 14

Table 52 - DLR Port Choices for Stratix 5700 and ArmorStratix 5700 Switches

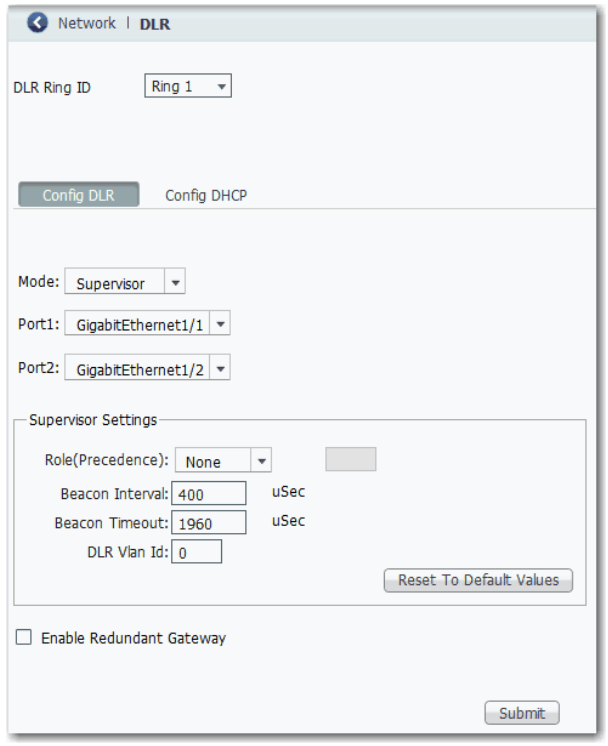
Switch	**Port**							
1783-BMS10CGP	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2				
1783-BMS10CGN	Fa 1/7	Fa 1/8	Gi 1/1	Gi 1/2				
1783-BMS12T4E2CGL	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2				
1783-BMS12T4E2CGP	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2				
1783-BMS12T4E2CGNK	Fa 1/15	Fa 1/16	Gi 1/1	Gi 1/2				
1783-BMS20CL	Fa 1/15	Fa 1/16			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				

Configure DLR via Device Manager

From the Configure menu, choose DLR. On the Stratix 5400 switch, choose which ring to configure:

- To configure the switch as a ring node or a ring supervisor, complete the fields as described in Table 53 on page 116.
- To configure redundant gateways, complete the fields as described in Table 53 on page 116.
- To configure DLR DHCP, complete the fields as described in Table 54 on page 117.

Configure Ring Node, Ring Supervisor, and Redundant Gateways via Config DLR



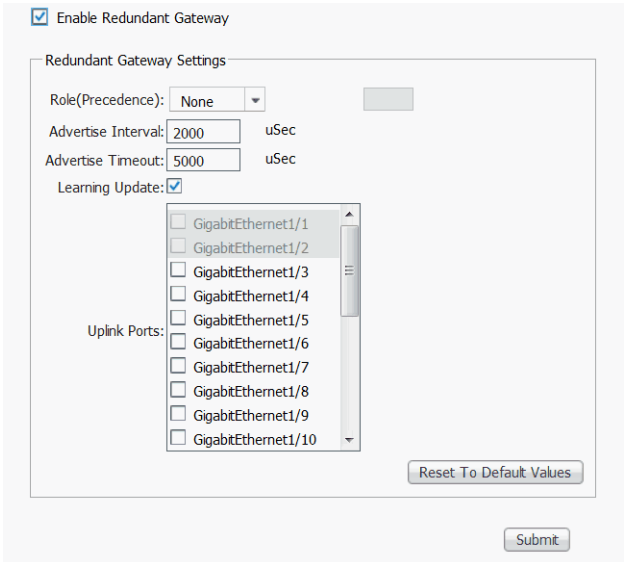


Table 53 - Config DLR Fields

Field	Description
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 ID 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 that the 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)
Redundant Gateway Settings	
Enable Redundant Gateway	Check Enable Redundant Gateway to activate the configuration of Redundant Gateway Settings. 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 ID becomes 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
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 Learning Update to activate learning update messages. Default: Enabled
Uplink Ports	Check Uplink Ports for each uplink port on which to enable redundant gateway.

Configure DLR DHCP via Config DHCP

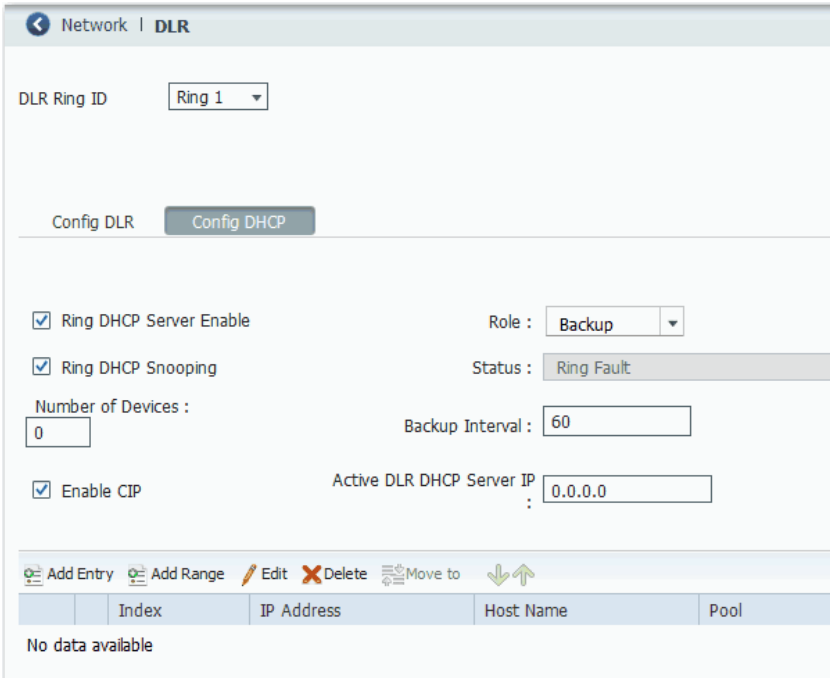


Table 54 - Config DHCP Fields

Field	Description
Ring DHCP Server Enable	Check Ring DHCP Server Enable to activate 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 Ring DHCP Snooping 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
Enable CIP	When the role of the ring DHCP server is Backup, check Enable CIP to enter the active ring DHCP server CIP IP address.
Active DLR DHCP Server IP	(Available only when Enable CIP is checked). Type the active ring DHCP server CIP IP address, which allows the backup ring DHCP server to sync information with the active ring DHCP server.
Add Range	To add a range of IP addresses to the DLR DHCP configuration table, click Add Range: • 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 in Dynamic Host Configuration Protocol (DHCP) Persistence. DHCP persistence and DLR DHCP can coexist, but cannot share the same pool.
Edit	To edit an existing entry, select the entry in the table and click Edit.
Delete	To delete an entry, select the entry in the table and click Delete.
Add Individual IP Addresses	
Add Entry	To add IP addresses individually to the DLR DHCP configuration table, click Add Entry. The Add Entry dialog box displays.
Index	Type a value that indicates the location of the ring device. Valid values: 2 ...255.

Table 54 - Config DHCP Fields (Continued)

Field	Description
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 in Dynamic Host Configuration Protocol (DHCP) Persistence.
Add a Range of IP Addresses	
Add Range	To add a range of IP addresses to the DLR DHCP configuration table, click Add Range. The Add Range dialog box displays.
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 in Dynamic Host Configuration Protocol (DHCP) Persistence. DHCP persistence and DLR DHCP can coexist, but cannot share the same pool.
Grid Fields	
Index	Indicates the ring member location. Valid values: 2...255
IP Address	Indicates IP address of the ring member.
Host Name	Indicates host name that is associated with the IP address of the ring member.
Pool	Indicates the name of the pool of IP addresses available for DLR DHCP. The DHCP pool must be previously configured on the Global Settings tab on the DCHP page. See Dynamic Host Configuration Protocol (DHCP) Persistence.

Configure DLR via the Logix Designer Application

In the navigation pane, click DLR. You then choose which ring to configure. Stratix 5700 and ArmorStratix 5700 switches support one ring. Stratix 5400 switches support three rings:

- To configure the switch as a ring node, complete the fields as described in Table 55 on page 119.
- To configure the switch as a ring supervisor, click Ring 1, Ring 2, or Ring 3, and then complete the fields as described in Table 56 on page 120.
- To configure redundant gateways, expand Ring 1, Ring 2, or Ring 3, click Redundant Gateway Configuration, and then complete the fields as described in Table 57 on page 122.
- To configure DLR DHCP, expand Ring 1, Ring 2, or Ring 3, click DHCP, and then complete the fields as described in Table 58 on page 123.

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 316.

Configure Ring Node via DLR View

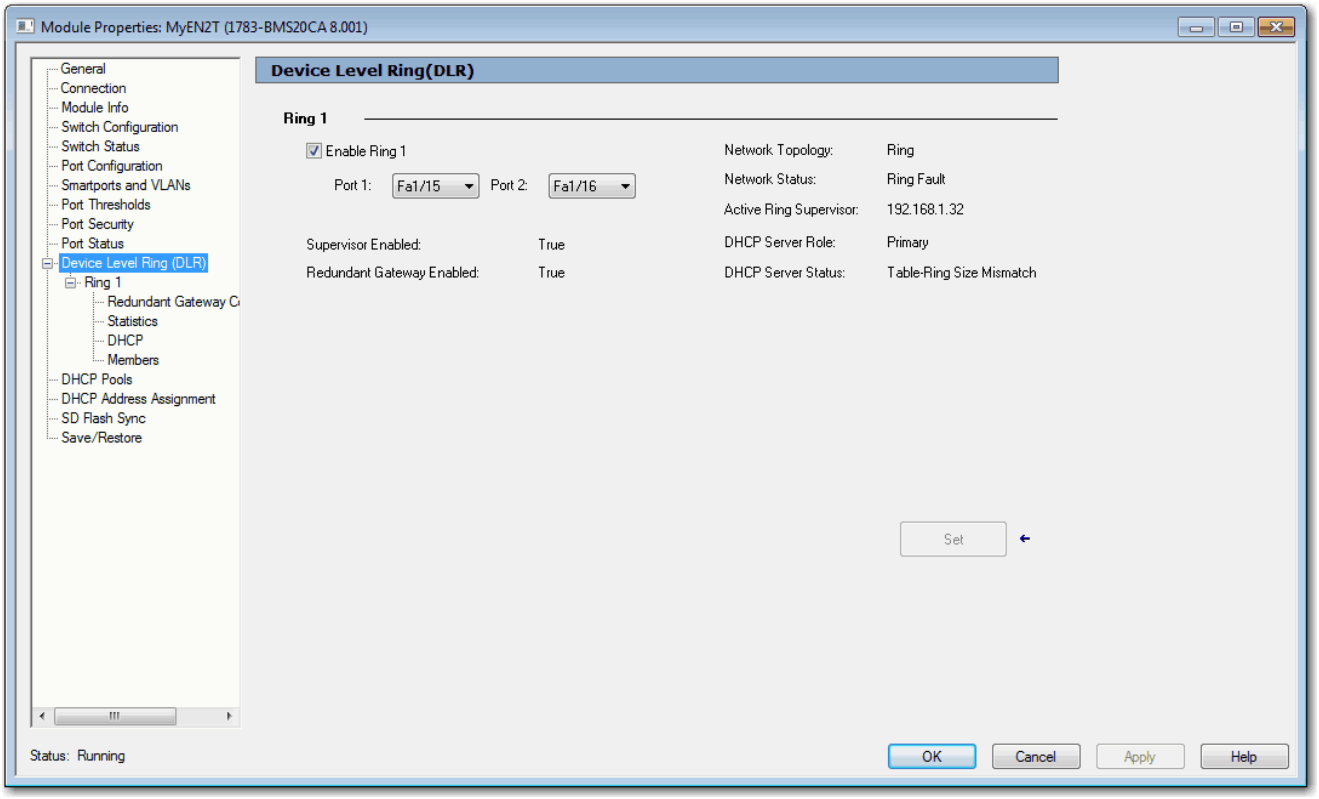


Table 55 - Device Level Ring (DLR) Fields

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 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 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 55 - Device Level Ring (DLR) Fields (Continued)

Field	Description
Active Ring Supervisor	Displays the IP address of the active ring supervisor.
DHCP 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

Configure Ring Supervisor via DLR - Ring View

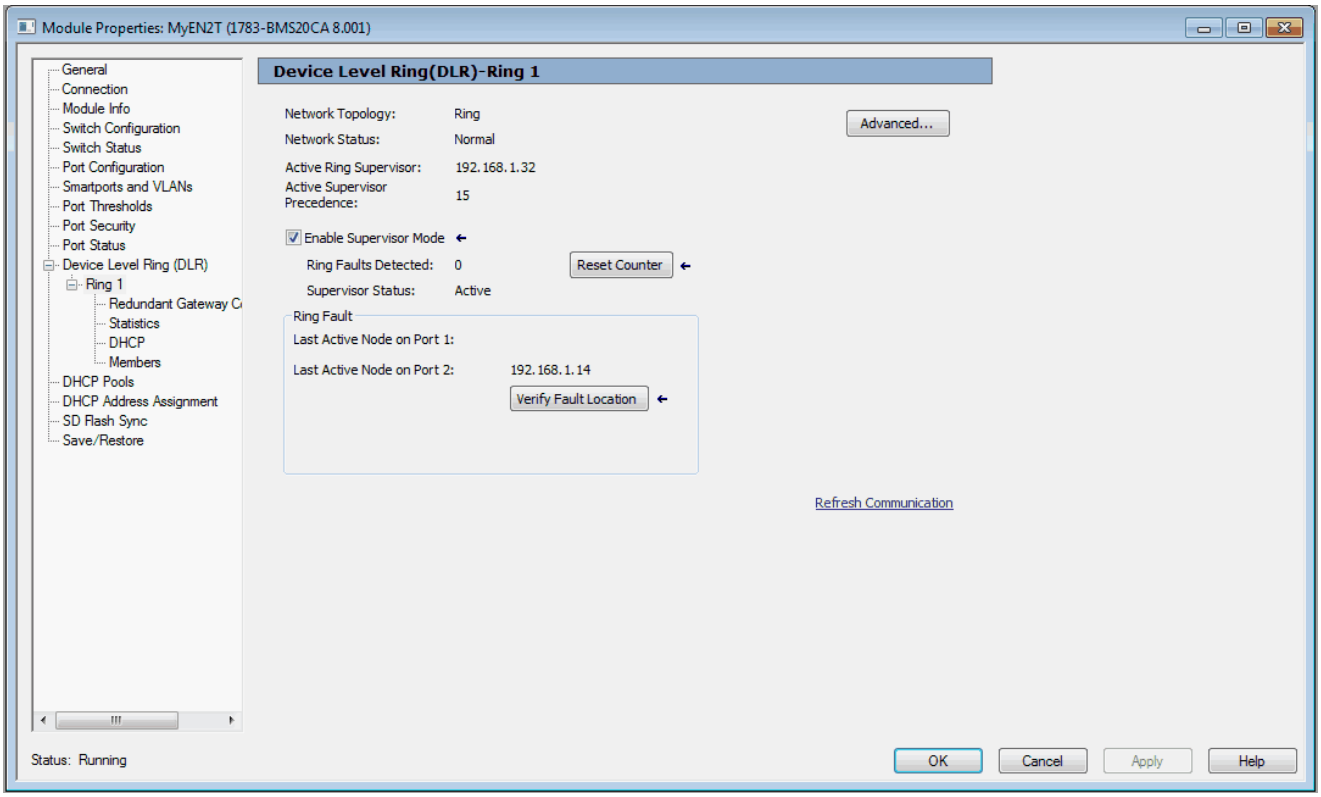


Table 56 - Ring 1/Ring 2/Ring 3 Fields

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.
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.

Table 56 - Ring 1/Ring 2/Ring 3 Fields (Continued)

Field	Description
Enable Supervisor Mode	Check Enable Supervisor Mode 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.
Advanced Network Configuration	
Advanced	Click Advanced. The Advanced Network Configuration dialog box appears. The configuration fields are available only after you click Advanced.
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 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 3 view. 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 ID becomes the active supervisor. Valid values: 0…255 The default precedence is 0. The highest precedence is 255.
Beacon Interval	Type an interval for the supervisor to transmit beacon frames. Valid values: 200…100,000 µs The default interval is 400 µs.
Beacon Timeout	Type the amount of time that the 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.

Configure Redundant Gateway via DLR - Ring - Redundant Gateway Configuration View

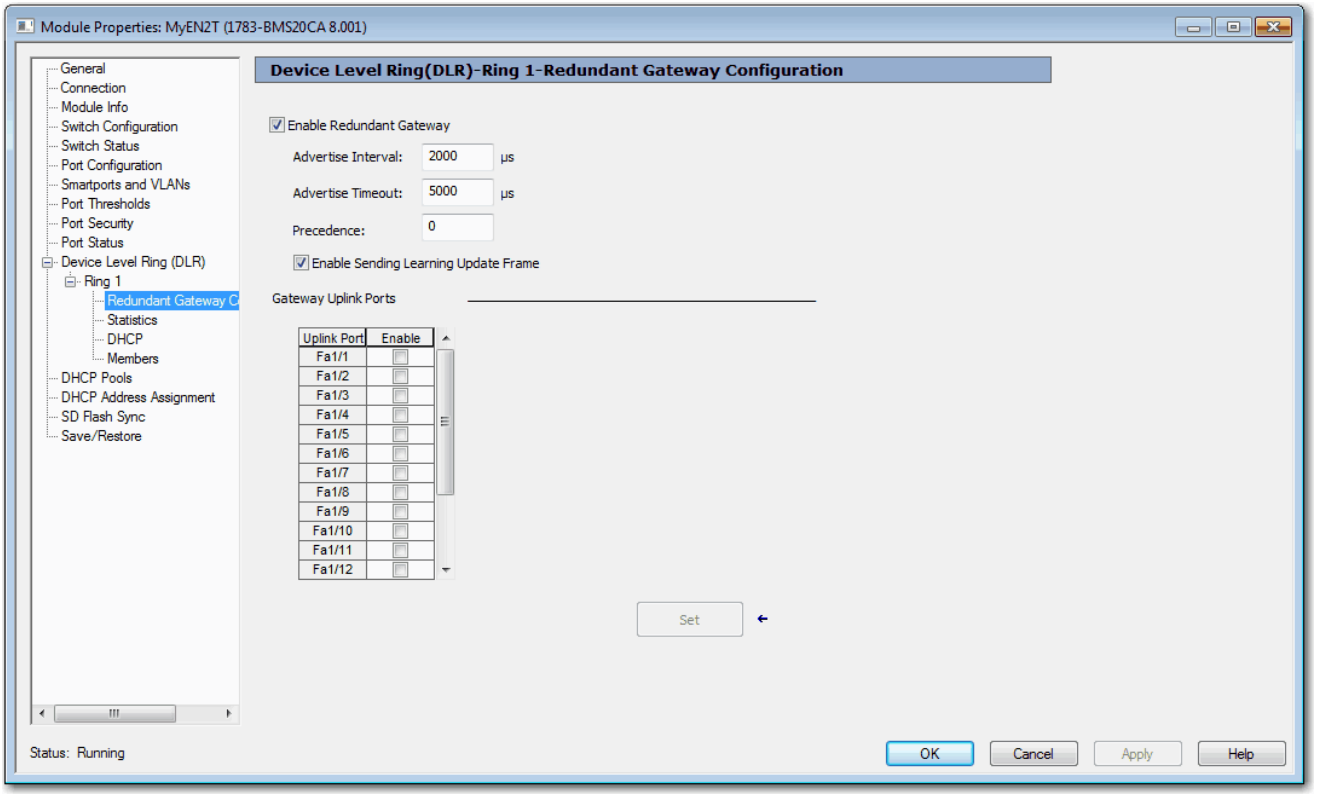


Table 57 - Redundant Gateway Configuration Fields

Field	Description
Enable Redundant Gateway	Check Enable Redundant Gateway to activate 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
Precedence	Choose a role to assign to the redundant gateway that corresponds to a predefined precedence value. The switch transmits the precedence value in advertise messages and is used to select the redundant gateway when multiple redundant gateways are configured. A higher value means higher precedence. When two DLR redundant gateways have the same precedence, the device with the numerically highest MAC ID becomes 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 Enable Sending Learning Update Frame to activate learning update messages. Default: Enabled
Gateway Uplink Ports	Check Enable for each uplink port on which to activate redundant gateway.

Configure DHCP and DHCP Snooping via DLR - Ring - DHCP View

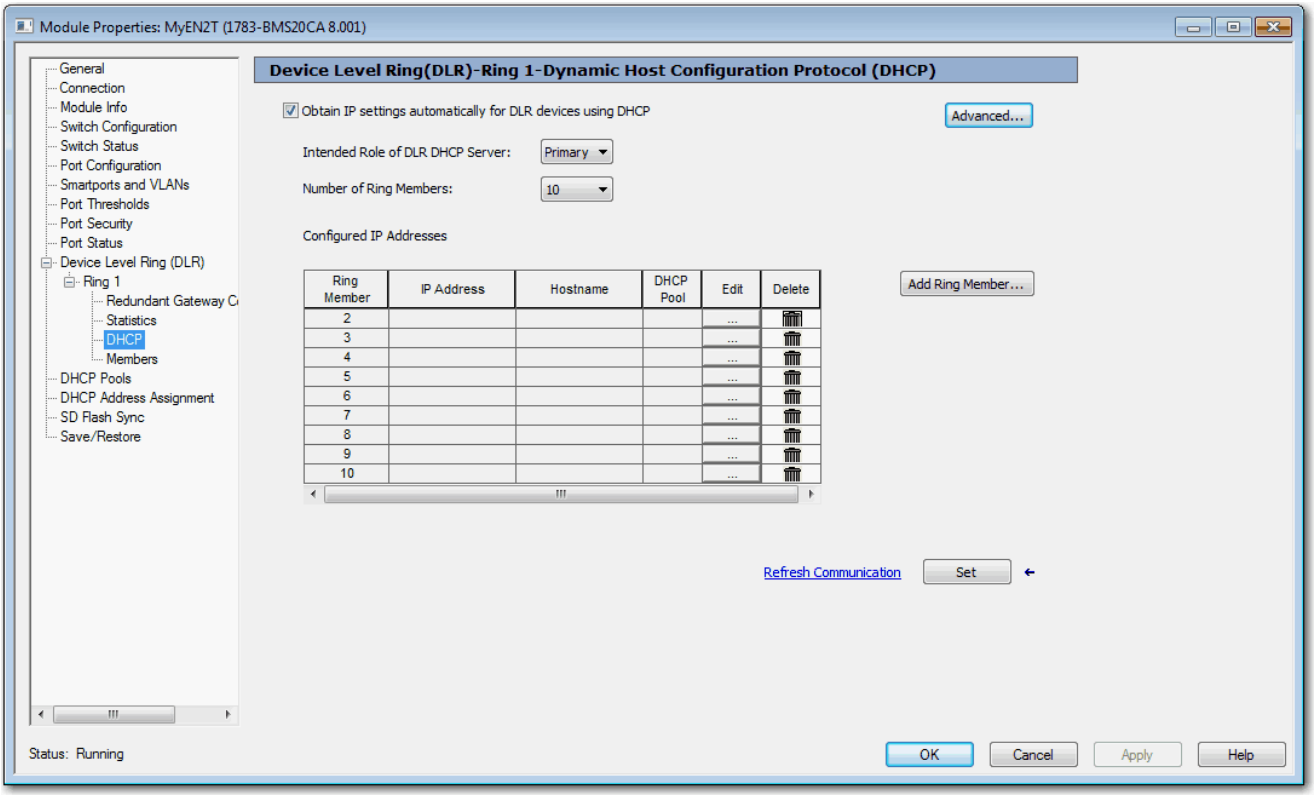


Table 58 - DHCP Fields

Field	Description
Obtain IP settings automatically for DLR devices using DHCP	Check Obtain IP settings automatically for DLR devices using DHCP to enable the ring DHCP server on the supervisor device.
Intended Role of DHCP Server	Choose the role to assign to the DHCP server: • Primary—The supervisor functions as the active ring DHCP server. • Backup—The 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.
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 that is specified in DHCP IP address pool. To assign IP addresses to ring members, see Add a Ring Member.
Hostname	Displays the name for the host that is associated with the ring member.
DHCP Pool	Displays the name of the DHCP IP address pool that is configured on the switch.
Add a Ring Member	
Add Ring Member	Click Add Ring Member. The Add Ring Member dialog box appears. The configuration fields are available only after you click Add Ring Member.
DHCP Pool	Choose the name of the IP address pool to use for ring devices. This pool must be previously configured as described in Configure the DHCP IP Address Pool on page 129. DLR DHCP can coexist with DHCP Persistence, but cannot share the same pool.
Add a Single Ring Member into Table	To assign an IP address to a ring member, click Add a Single Ring Member into Table, and then complete 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.
Add Multiple Ring Members into Table	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 start and end locations of the ring members. • IP Address...To—Type the start and end IP addresses for the ring members.
DLR DHCP Snooping	
Advanced	Click Advanced. The Advanced dialog box appears. The Enable DCHP Snooping checkbox is available only after you click Advanced.
Enable DLR DCHP Snooping	Check Enable DHCP Snooping. 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. You must disable DHCP snooping to use DHCP server functionality outside of the ring.

Configure a Switch as a Ring Supervisor and DHCP Server

For a detailed example of how to configure this type of network, see the EtherNet/IP Device Level Ring Application Technique, publication ENET-AT007.

Configure the primary ring server first, then configure the backup ring server.

IMPORTANT In a network configured for DLR DHCP, each switch in the ring must have a statically assigned address. Switches in the ring cannot have addresses that are assigned via DLR DHCP.

Configure the Active Ring Supervisor/Primary Ring DHCP Server

Complete these instructions via Device Manager or the Logix Designer application:

- Enable DHCP and DHCP snooping.
- Configure an IP address pool for ring devices.
- Configure the switch as a ring supervisor. Be sure to enable Supervisor mode and set the role precedence to Primary.
- Configure DHCP. Be sure to enable the ring DHCP server, choose the Primary role, specify the number of ring devices, and add entries to the DHCP configuration table.
- Verify that the CIP VLAN is enabled on the switch and note the VLAN ID. You can enable the CIP VLAN in Express Setup.

Configure the Backup Ring Supervisor/Backup Ring DHCP Server

Complete these instructions via Device Manager or the Logix Designer application:

- Enable DHCP and DHCP snooping.
- Configure the switch as a backup ring supervisor—be sure to enable DLR Supervisor mode with a role precedence of Backup 1.
- Configure DLR DHCP—be sure to enable the ring DHCP server and choose the Backup role.
- Verify that the CIP VLAN is enabled on the switch. You can enable this setting in the Advanced Settings under Express Setup.

After all actions are completed, connect cables in the ring and verify that all ring devices are assigned the correct IP addresses.

DLR VLAN Trunking

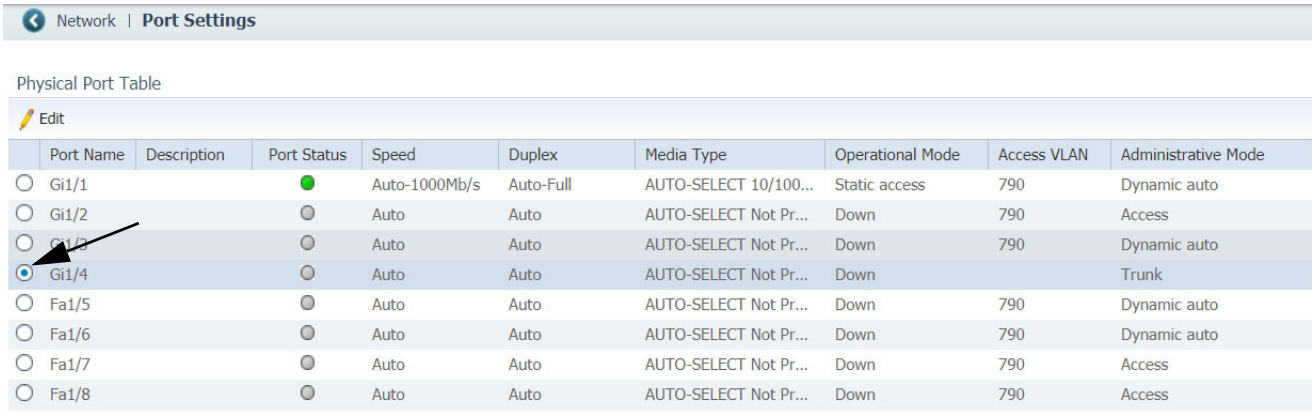
A trunk is a connection between switches that carries traffic from multiple VLANs. DLR VLAN trunking allows switches with multiple VLANs to be connected in a DLR network. As traffic passes from one switch to the next in a ring, the traffic can either remain on the same VLAN or pass to different VLANs via routing. For examples and configuration considerations for DLR VLAN Trunking, see the EtherNet/IP Device Level Ring Application Technique, publication ENET-AT007.

Configure DLR VLAN Trunking via Device Manager

IMPORTANT For best performance, Stratix 5400 switches are recommended.

To configure DLR VLAN Trunking via Device Manager:

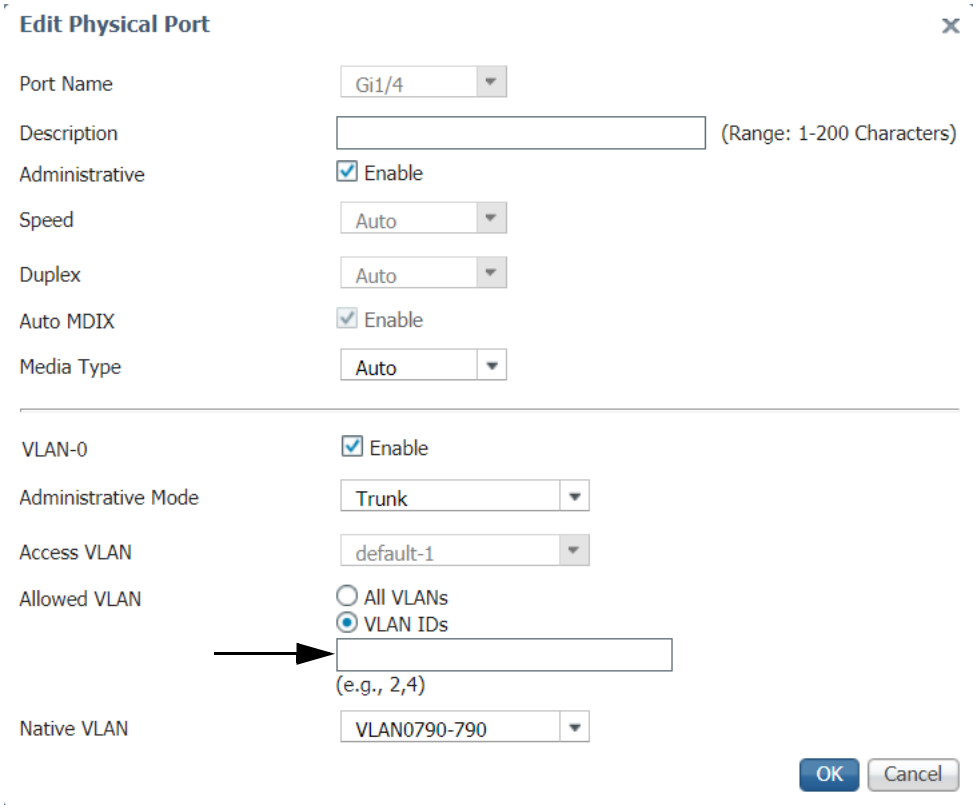
1. Configure both DLR ports for your ring as identical trunk ports. For more information about trunk port configuration, see Configure Port Settings.



2. From the Configure menu, choose Port Settings from the Network section. Choose the trunk port on which to specify allowed VLANs, and then click Edit.
3. On the Edit Physical Port screen, Specify Allowed VLANs—the VLAN traffic you want on the DLR network—and click OK.

IMPORTANT The All VLANs option is not supported for DLR trunking.

4. Enable DLR on the same trunk port. For more information, see Configure DLR via Device Manager.



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. This new IP address 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. If you have an application that includes a backup DHCP server in a DLR network, other DHCP features (including DHCP persistence) are not supported on the active DHCP server or the backup DHCP server.

You can assign an IP address from the IP address pool to a specific switch port. A device that is connected to that switch port always receives the address that you assigned to the port regardless of its MAC ID.

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 keep the switch from responding when it receives a request, check the Reserve Only box on the DHCP page.

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 keep the IP address from being overridden, enable DHCP snooping on the appropriate VLAN. 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.

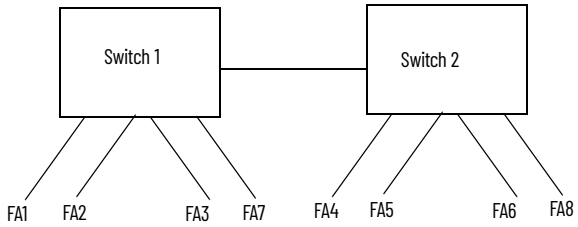


Table 59 - DHCP Persistence Behavior

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.

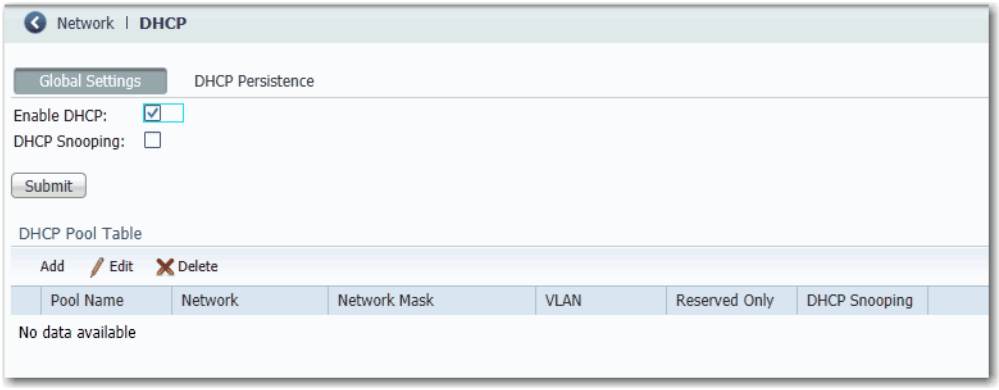
Configure DHCP Persistence via Device Manager

To configure DHCP persistence, complete this process.

1. Configure the DHCP server.
2. Configure the IP address pool.
3. Assign an IP address to a switch port.

Configure the DHCP Server.

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 that are 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.

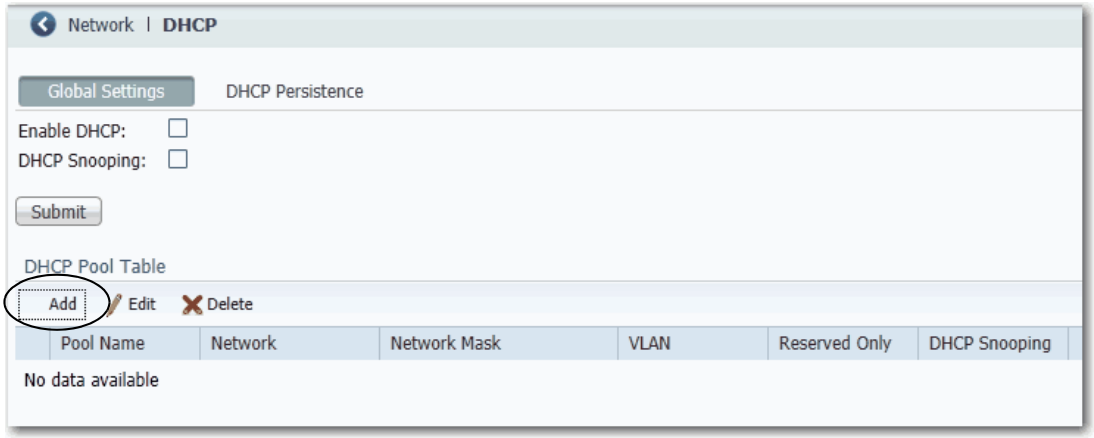
5. Click Submit.

Configure the DHCP IP Address Pool

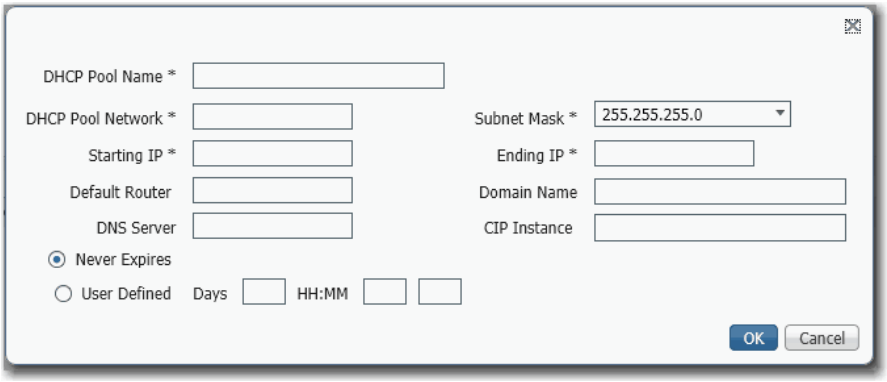
Once DHCP is enabled, you can create the DHCP address pool.

IMPORTANT If you are configuring DCHP for ring devices, to avoid switch failure upon a switchover, do not create an IP address pool for the backup ring DHCP server. The backup ring DHCP server receives IP addresses from the active ring DHCP server.

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.

Assign an IP Address to a Switch Port

To manage switch port IP addresses, click the DHCP Persistence tab.

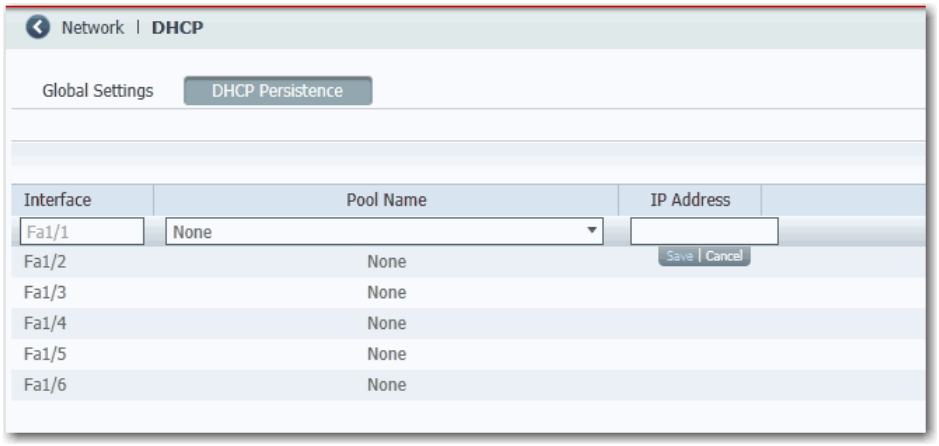


Table 60 - DHCP Persistence Fields

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.

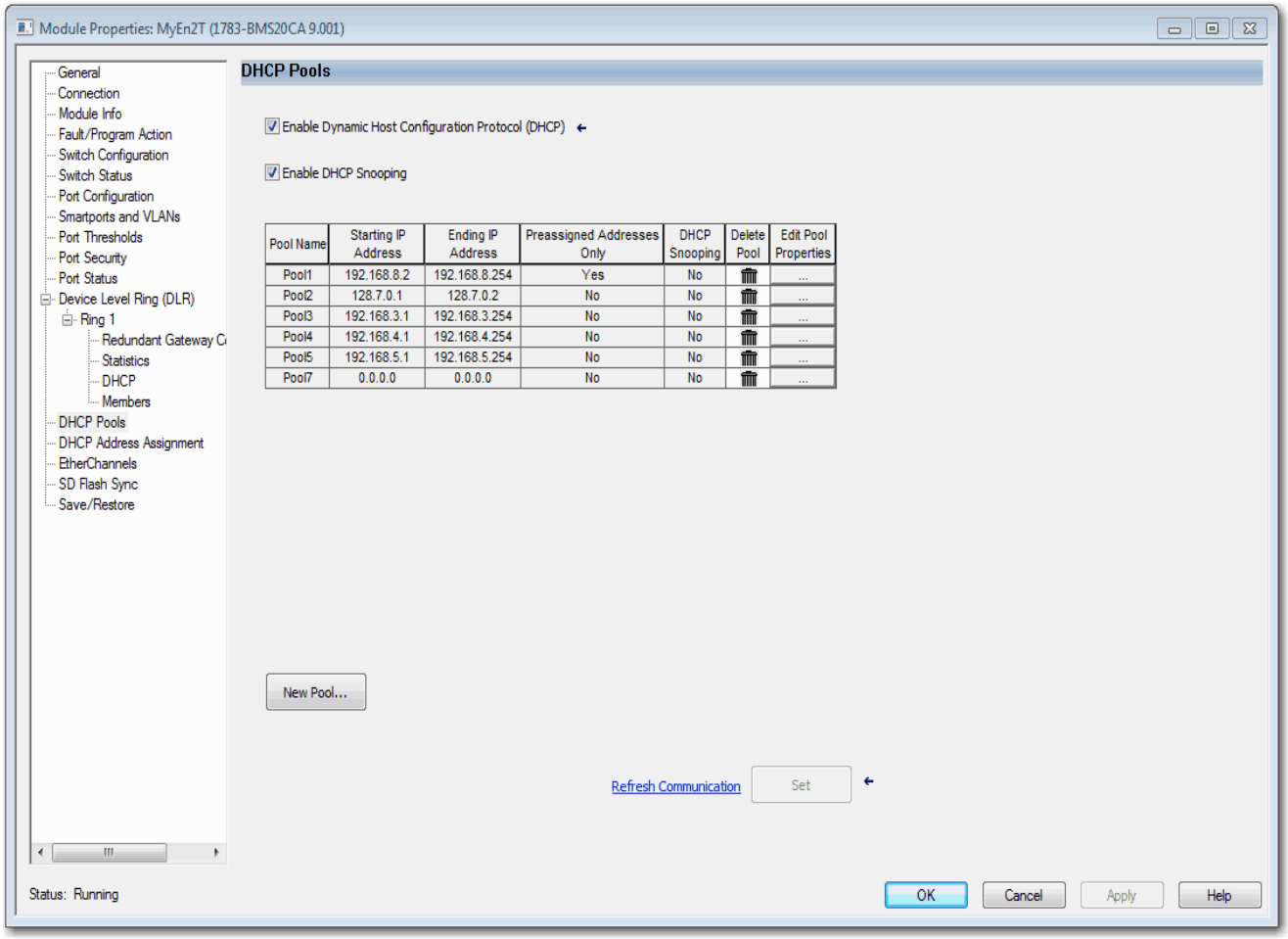
Configure DHCP Persistence via the Logix Designer Application

To configure DHCP persistence, complete this process.

1. Configure the DHCP server.
2. Configure the IP address pool.
3. Assign an IP address to a switch port.

Configure the DHCP Server

1. In the navigation pane, click DHCP Pools.



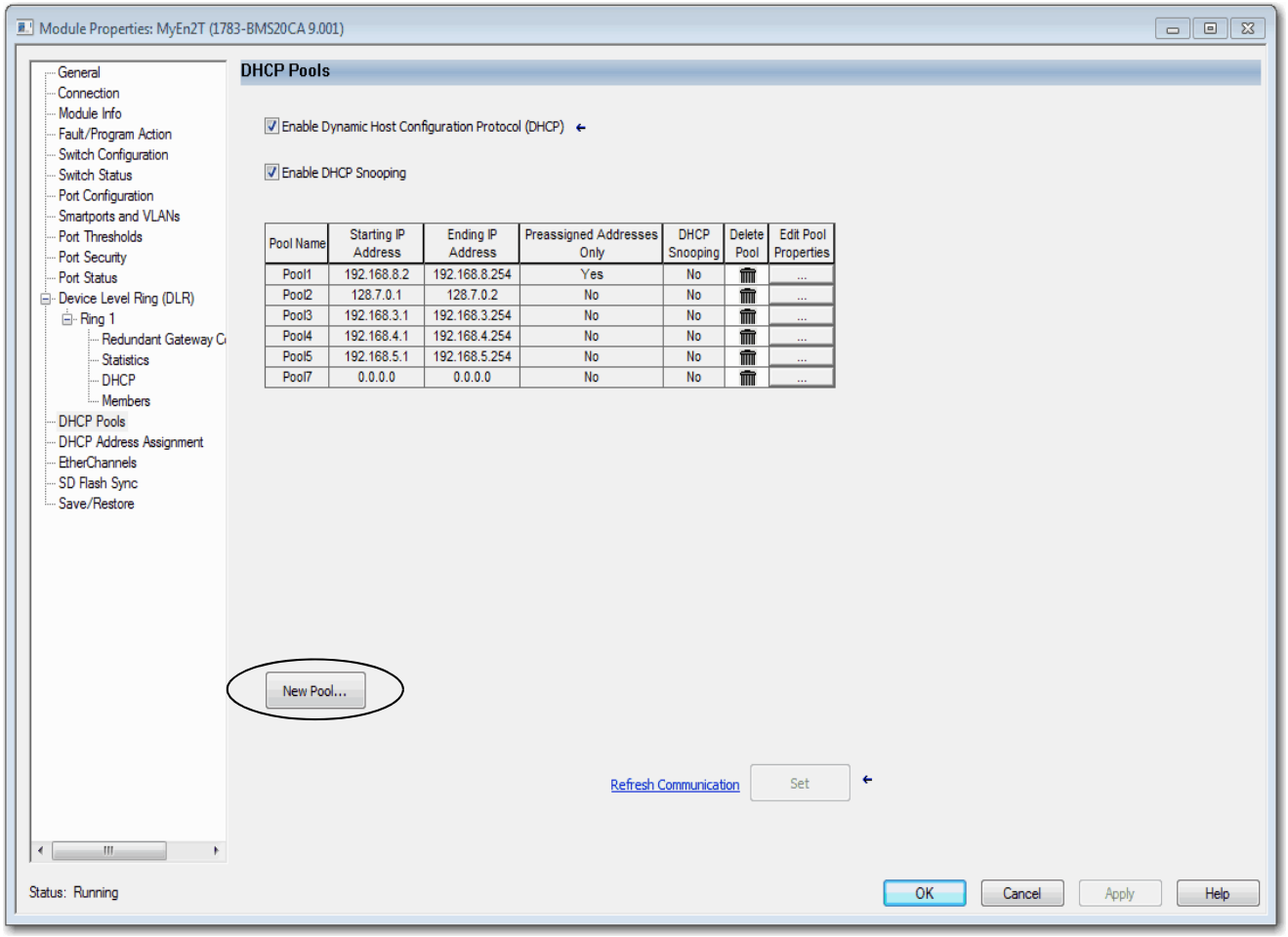
2. Check Enable Dynamic Host Configuration Protocol (DHCP).
3. To enable DHCP snooping, check Enable DHCP Snooping.

   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 that are 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.

Configure the DHCP IP Address Pool

Once DHCP is enabled, you can create the DHCP address pool.

1. In the navigation pane, click DHCP Pools.
2. Click New Pool.



3. Complete the fields and click Close.

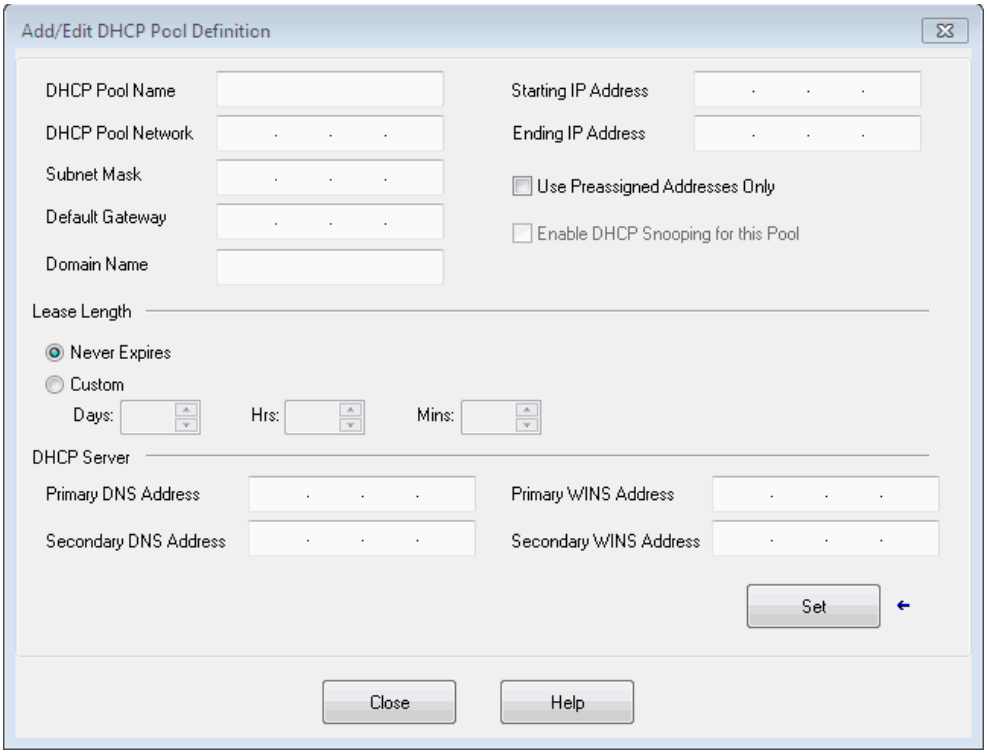


Table 61 - Add/Edit DCHP Pool Definition Fields

Field	Description
DHCP Pool Name	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.
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.
Default Gateway	The default gateway IP address for the DHCP client. The format is a 32-bit numeric address that is written as four numbers separated by periods (for example, 255.255.255.255). Each number can be from 0... 255.
Domain Name	The domain name for the DHCP client.
Starting IP Address	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 Address	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.
Use Preassigned Addresses Only	If checked, IP addresses are assigned only when configured for specific ports on the DHCP Address Assignment or DLR DHCP views.
Enable DHCP Snooping for this Pool	If checked, devices only receive address assignments from the connected switch.
Never Expires or Custom	The duration of the lease for an IP address that is assigned to a DHCP client. Click one of the following: • Never Expires • Custom If you click Custom, enter the duration of the lease in the numbers of days, hours, and minutes. This lease length is used for all assignments.
Primary DNS Address	The IP addresses of the primary domain name system (DNS) IP servers available to a DHCP client.
Secondary DNS Address	The IP addresses of the secondary domain name system (DNS) IP servers available to a DHCP client.
Primary WINS Address	The IP address of the primary Microsoft NetBIOS name server (WINS server) available to a DHCP client.
Secondary WINS Address	The IP address of the secondary Microsoft NetBIOS name server (WINS server) available to a DHCP client.

Assign an IP Address to a Switch Port

In the navigation pane, click DHCP Address Assignment.

You can assign a specific IP address to each port, so that the device that is attached to a given port receives the same IP address.

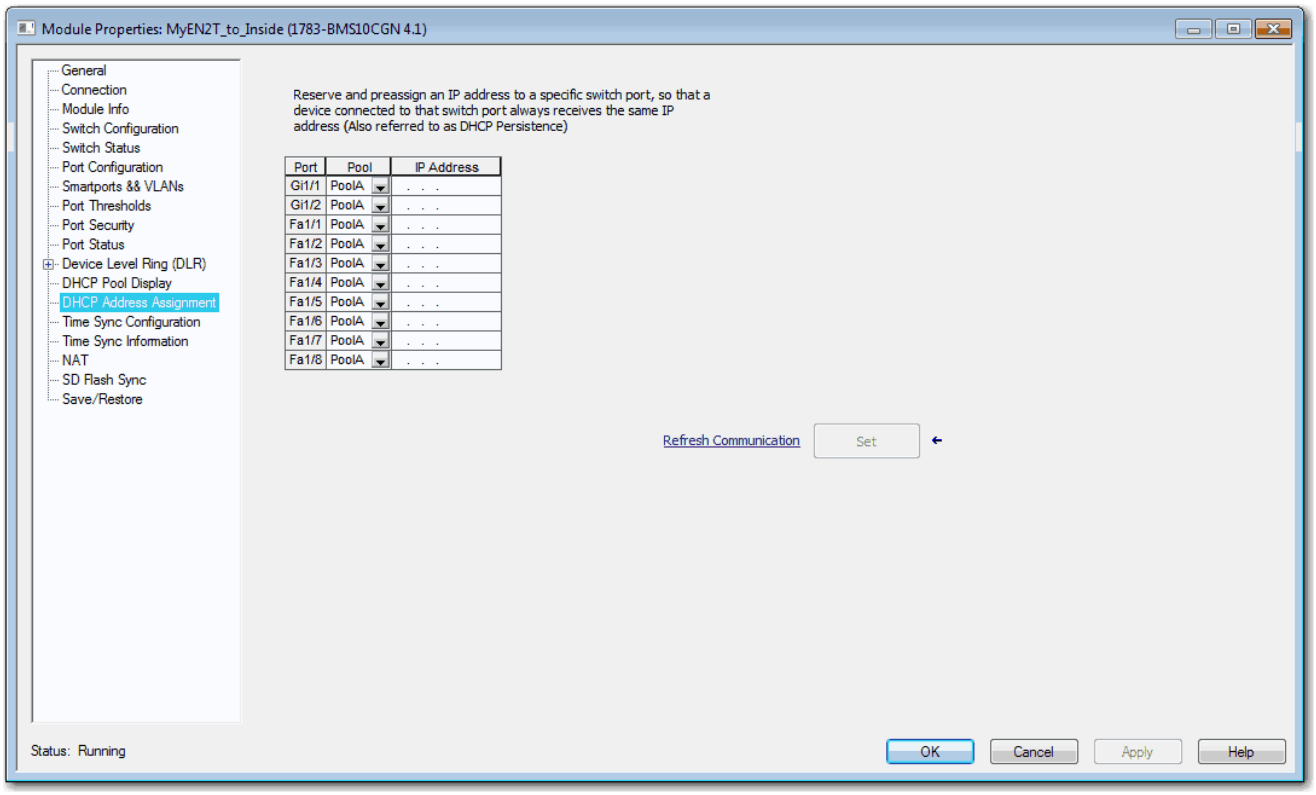


Table 62 - DHCP Address Assignment Fields

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.

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is available on the following switches:

- Stratix 5400 with Layer 3 firmware
- Stratix 5410 with Layer 3 firmware
- Stratix 8300 base units

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 unaffected by topology changes are not involved in re-computations.

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.

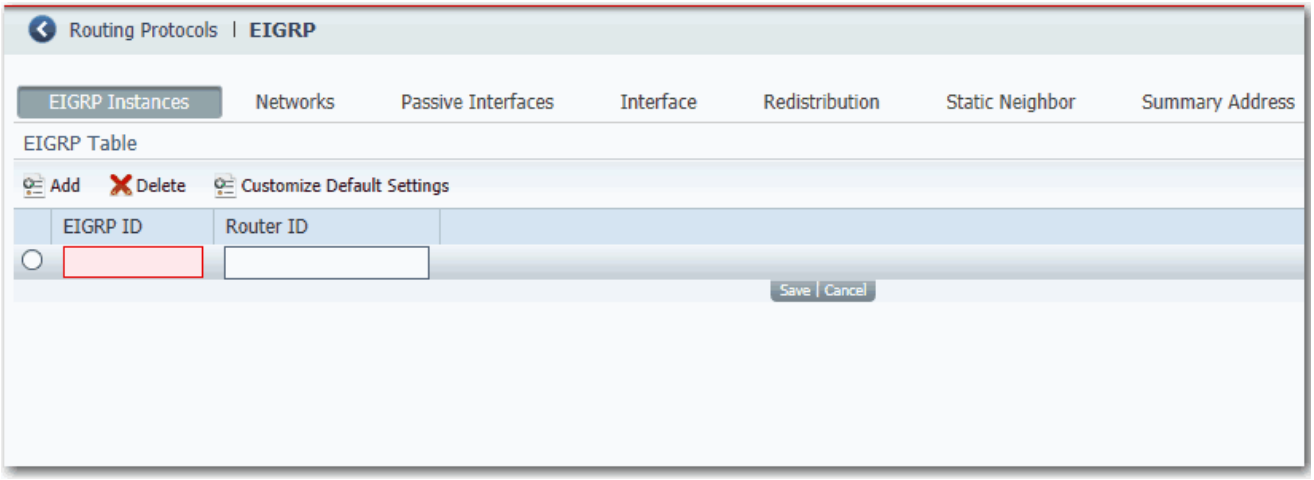


Table 63 - EIGRP Fields

Field	Description
EIRGP Instances—Add EIGRP instances to the EIGRP table. To customize the default settings for an instance, see page 138.	
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 help 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 Passive 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
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 do not change the default state of split horizon unless you are certain that your application requires the change to advertise routes properly.
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 helps prevent 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.

Table 63 - EIGRP Fields (Continued)

Field	Description
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 in which 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 in which 255 is 100 percent loading
MTU	Type the smallest allowed value for the maximum transmission unit (MTU) in bytes. Valid values: 1…65535
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.

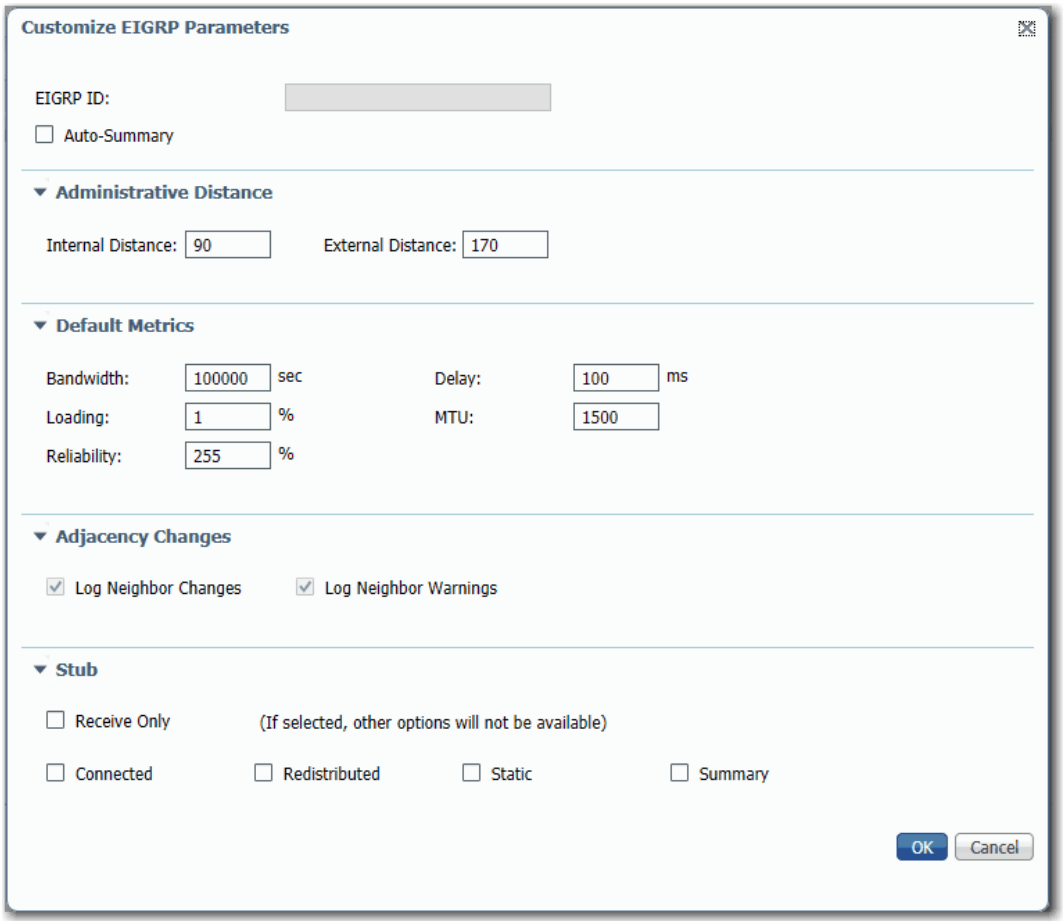


Table 64 - Customize EIGRP Parameters

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 in which 255 is 100 percent loading
Reliability	Type a number that represents likelihood of successful packet transmission. Valid values: 0...255 in which 255 means100 percent reliability; 0 means no reliability

Table 64 - Customize EIGRP Parameters (Continued)

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 helps prevent 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

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 65 shows the maximum number of EtherChannels available per switch. Each EtherChannel can consist of up to eight compatible, configured Ethernet ports.

Table 65 - 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 switches with Full firmware.

Figure 12 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 12 - EtherChannel Example

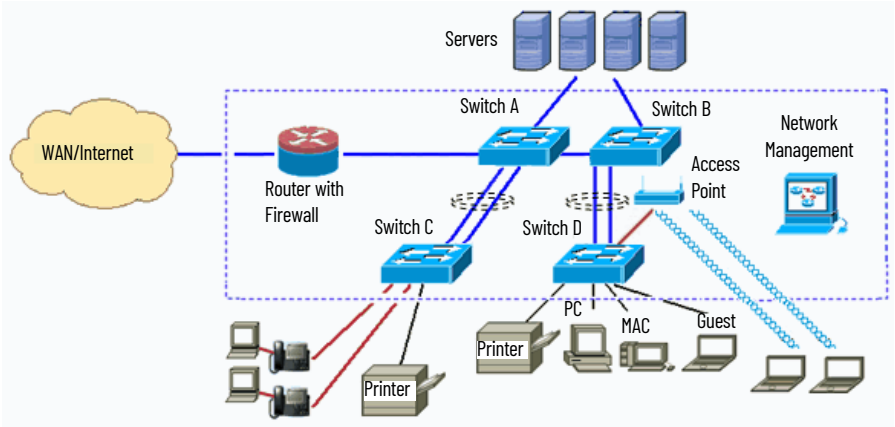


Table 66 describes the modes that you can assign to an EtherChannel:

Table 66 - 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 the initiation of 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 be configured in the Static mode also; otherwise, packet loss can occur.

If a link within an EtherChannel fails, traffic that was 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.

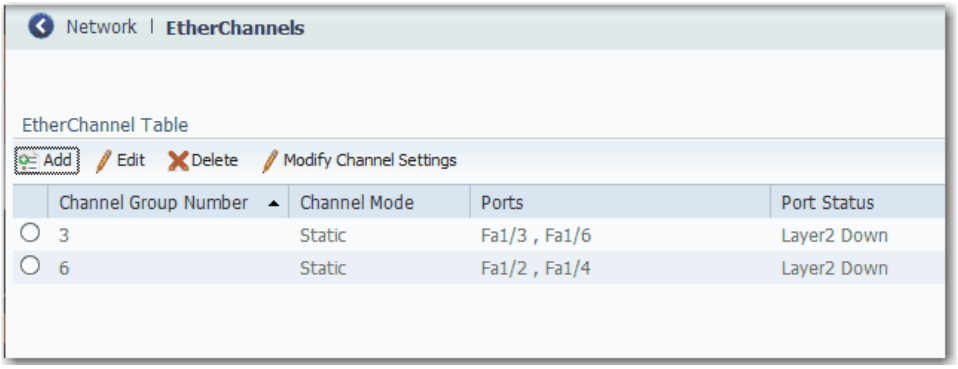


Table 67 - EtherChannel Fields

Field	Description
Channel Group Number	A number to identify the EtherChannel. See Table 65 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:** Be sure that all ports in an EtherChannel are configured with the same speed and duplex mode. See Table 66 for a description of EtherChannel modes.
Ports	The ports that can participate in the EtherChannel.
Port Status	The status of the group.

You can add, edit, or delete an EtherChannel:

- To add an EtherChannel, click Add. Complete the fields that are described in Table 68 and click OK.
- To edit an EtherChannel, click the radio button next to the EtherChannel and click Edit. Complete the fields that are described in Table 68 and click OK.
- To modify EtherChannel settings, such as speed, duplex mode, and VLAN assignments, click the radio button next to the EtherChannel and click Modify Channel Settings. Complete the fields that are described in Table 69 and click OK.
- To delete an EtherChannel, click the radio button next to the EtherChannel and click Delete.

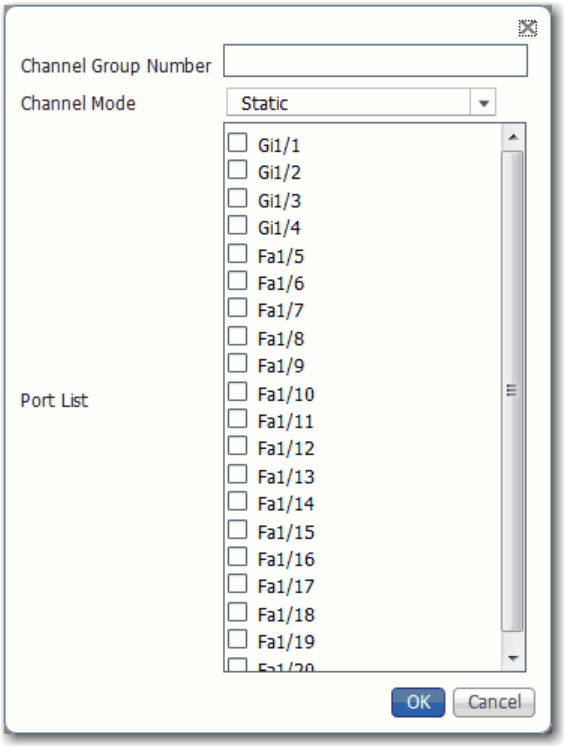


Table 68 - Add/Edit EtherChannel Dialog Box

Field	Description
Channel Group Number	Type a number to identify the EtherChannel.
Channel Mode	Choose a mode to assign to the EtherChannel. For a description of each mode, see Table 66 on page 141.
Port List	Check the checkbox next to each port to assign to the EtherChannel.

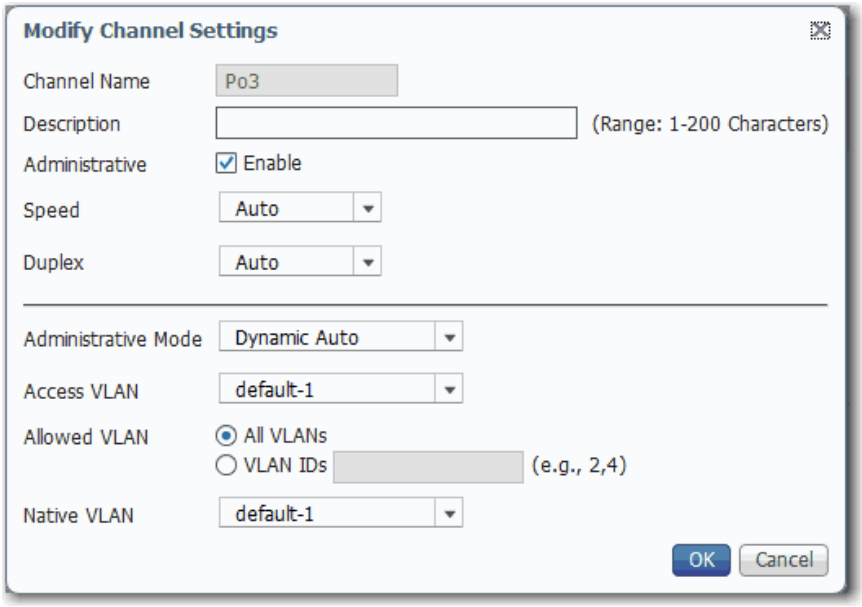


Table 69 - Modify Channel Settings Dialog Box

Field	Description
Channel Name	Displays the name that is assigned to the channel.
Description	Type a description of the channel.
Administrative	Check Enable to make the channel active. Clear Enable to make the channel inactive.
Speed	Choose the operating speed of the channel. If the connected device can negotiate the link speed with the channel, choose Auto (autonegotiation). Default: Auto
Duplex	Choose the duplex mode of the channel: • Auto—(Autonegotiation). The connected device can negotiate the duplex mode with the channel. If the channel is not connected or has not completed negotiation, the status is Auto. • Half— (Half-duplex mode). The connected device must alternate sending or receiving data. • Full— (Full-duplex mode). Both devices can send data simultaneously. Default: Auto
Administrative Mode	Choose one of the following administrative modes: • Access—The channel 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 channel 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 channel 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 channel 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 channel 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 that run the IP base or IP services image. Default: Dynamic Auto
Access VLAN	Choose the VLAN that the channel belongs to and carries traffic for when the channel is configured as or is acting as a nontrunking interface.
Allowed VLAN	Choose the VLANs for which this channel handles traffic when the channel is configured as or is dynamically acting as a trunking interface: • To allow traffic on all available VLANs, click All VLANs. • To limit traffic to specific VLANs, click VLAN IDs and enter the VLAN numbers.
Native VLAN	Choose the VLAN that transports untagged packets.

Configure EtherChannels via the Logix Designer Application

In the navigation pane, click EtherChannels.

You can add, edit, and delete EtherChannel members.

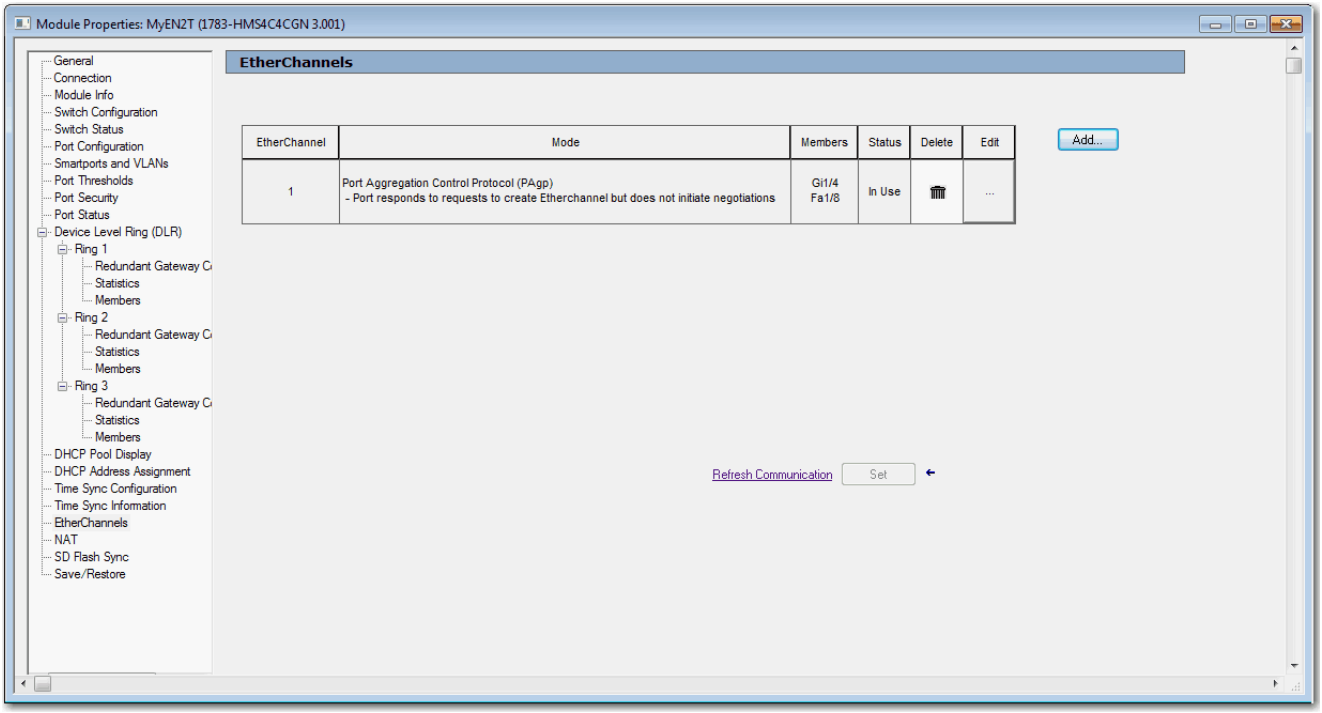


Table 70 - EtherChannels Fields

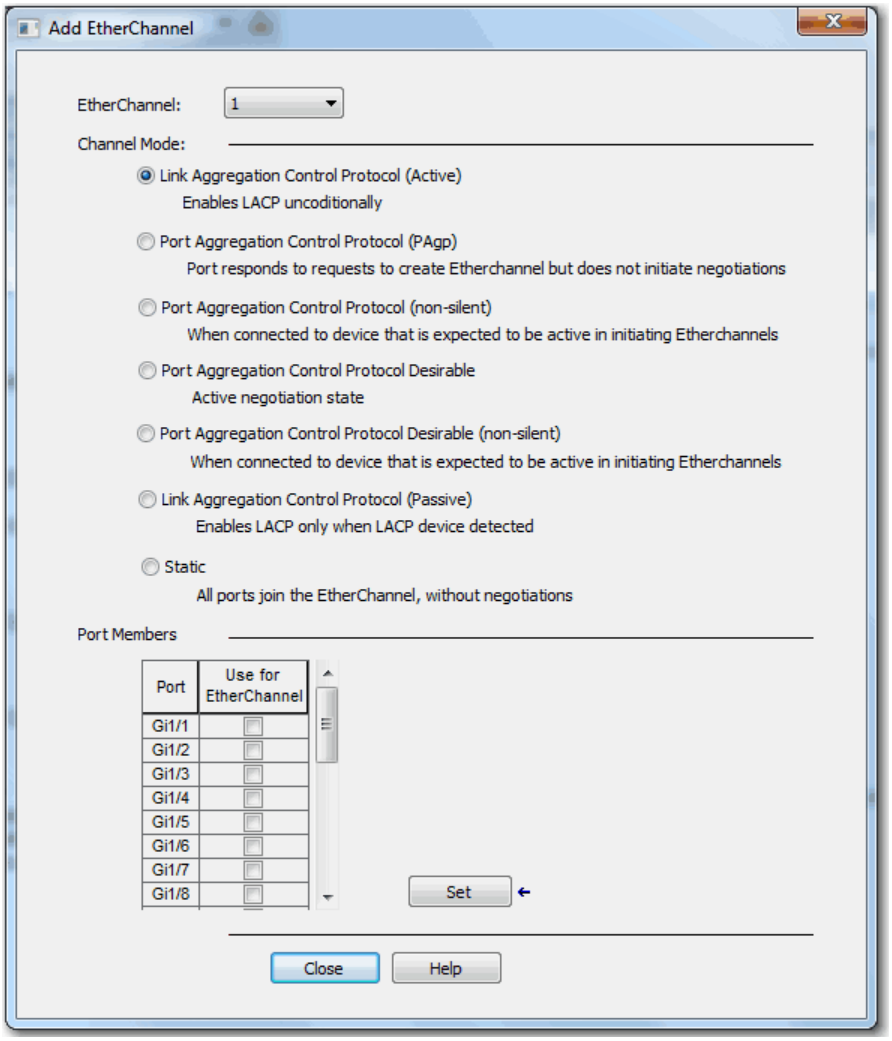
Field	Description
EtherChannel	A number to identify the EtherChannel. See Table 65 for the maximum number of EtherChannels available per switch.
Mode	Determines how ports become active. With all modes except Static, negotiations occur to determine which ports become active. Incompatible ports are put 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 66 for a description of EtherChannel modes.
Members	The ports that can participate in the EtherChannel.
Status	The status of the group.

Add an EtherChannel

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 66 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.



Feature Mode

Feature mode is available on Stratix 5400 switches. Feature mode provides efficient allocation of resources on the switch to support the operation of multiple, time-sensitive features. There are two modes, each with a profile customized for certain features, as shown in Table 71. The switch is configured to use DLR as the default mode. In a running system, if you deactivate the current active Feature mode, the default mode is applied.

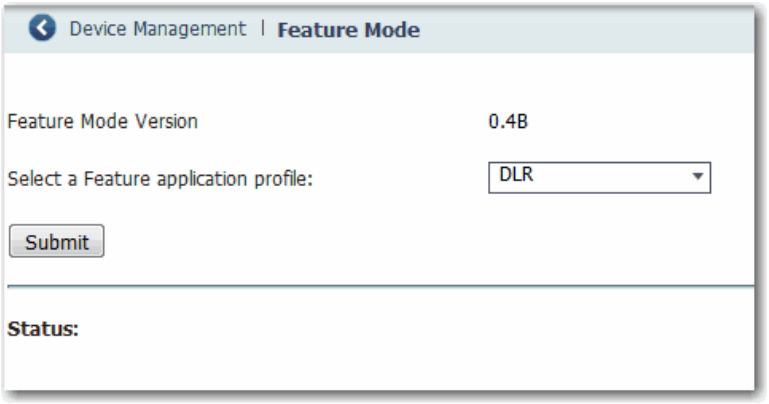
Table 71 - Feature Modes

Mode	Features Enabled
DLR (default)	• PTP • NAT • DLR • PRP
HSR	• PTP • NAT • PRP • HSR

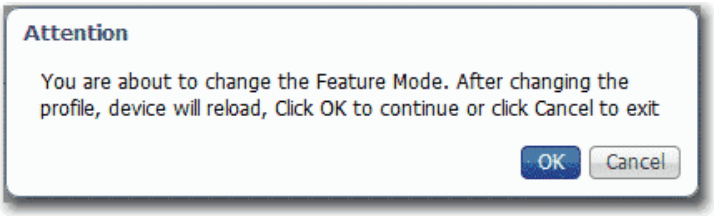
IMPORTANT Before changing the Feature mode, we recommend removing any configurations that are related to the current active Feature mode because those configurations are not valid for the new mode.

To apply a feature mode, follow these steps.

1. From the Admin menu, choose Feature Mode.
2. From the pull-down menu, choose a mode and click Submit.



3. When prompted to restart the switch, click OK.



The Status area of the page displays the status of the mode change and reload operation. After the restart, the status message prompts you to log out and log in again for the new mode to take effect.

Global Navigation Satellite System (GNSS)

IMPORTANT GNSS is supported only on Stratix 5410 series B switches with IOS release 15.2(6)E0a and later.

To use the GNSS software feature on the switch, you must obtain an external GPS antenna from a third-party manufacturer.

The built-in GNSS receiver enables a Stratix 5410 switch to determine its own location and get an accurate time from a satellite constellation. The switch can then become the Grandmaster clock for time distribution in the network.

GNSS Hardware

The switch uses a GNSS receiver with precise frequency and phase outputs for the host system. When connected to an external GNSS antenna, the receiver can acquire GNSS satellite signals, track as many as 32 GNSS satellites, and compute location, speed, heading, and time. It provides an accurate one pulse-per-second (PPS) and stable 10 MHz frequency output. For more information, see GNSS Signaling on page 149.

GNSS hardware supports the following frequency bands:

- GPS/NAVSTAR—Global Positioning System (USA: L1)
- GLONASS—Global'naya Navigatsionnaya Sputnikovaya Sistema (Russia: L1/G1)
- BeiDou—China (including B1-2)

IMPORTANT The Galileo satellite system is not available in the current release.

GNSS Software

As of IOS release 15.2(6)E0a and later, the GNSS software feature performs the following functions:

- Configures the GNSS receiver.
- After the receiver gains lock, the software performs the following functions once per second:
  - Reads the new time and date.
  - Reads the corresponding pulse-per-second (PPS) time stamp from the hardware.
  - Feeds the time and date and PPS time stamp into the Time Services SW Virtual Clock/Servo for GNSS. The GNSS SW Virtual Clock time can then be used to drive Precision Time Protocol (PTP) output.

GNSS Signaling

There are two stages in the process for the GNSS receiver to acquire satellites and provide timing signals to the host system:

- Self-survey mode—On reset, the GNSS receiver comes up in Self-survey mode and attempts to lock on to a minimum of four different satellites to obtain a 3-D fix on its current position. It computes nearly 2000 different positions for these satellites, which takes about 35 minutes. Also during this stage, the GNSS receiver is able to generate accurate timing signals and achieve normal (locked to GPS) state. Because the timing signal that is obtained during Self-survey mode can be off by 20 seconds, the software collects PPS data only during Over-determined (OD) Clock mode.

  After the self-survey process is complete, the results are saved to the internal memory of the GNSS receiver, which speeds up the transition to OD mode the next time the self-survey process runs. You can manually restart the self-survey process by using the command-line interface (CLI). After the self-survey process completes again, the software updates the results in the internal memory of the GNSS receiver.
- Over-determined (OD) Clock mode—The device transitions to OD mode when self-survey process is complete and the position information is stored in memory on the switch. In OD mode, the GNSS receiver outputs timing information that is based on satellite positions that are obtained during Self-survey mode.

The GNSS receiver remains in OD mode until there is a reason to leave it, such as the following reasons:

- Detection of a position relocation of the antenna of more than 100 m (328 ft), which triggers an automatic restart of the self-survey process.
- Manual restart of the self-survey process via the CLI.

After the GNSS receiver locks on to a satellite system, it sends a 10 ms-wide PPS pulse and the current time and date according to the satellite system to the time service.

GNSS Considerations

Consider these guidelines and limitations when configuring GNSS:

- GNSS is available as a timing source for PTP only.
- GNSS is available as a timing source for PTP only when PTP is in NTP-PTP Clock mode.
- Syslog messages are sent when the following GNSS events occur:
  - GNSS is in Self-survey mode.
  - GNSS reaches OD mode.
  - GNSS firmware update is in progress, complete, or failed.
- If the switch is the PTP Grandmaster clock and it loses the antenna signal, the clock quality can degrade, and this can result in a Grandmaster clock switchover.
- The GPS antenna alarm does not trigger an external relay alarm.

Configure GNSS

You can configure GNSS as a time source for PTP by using the CLI. For instructions on how to configure GNSS via the CLI, refer to documentation available at http://www.Cisco.com.

By default, GNSS is disabled. The following table lists other default settings.

Parameter	Default
Cable delay—The amount of time to compensate for cable delay in nanoseconds.	0
Antenna power—Antenna power input voltage.	5
Constellation—The satellite constellation that GNSS detects and locks to.	GPS
Anti-jam—The number of satellites required for a valid timing fix: • Enabled—A minimum of two satellites is required for a fix in Over-determined (OD) Clock mode, and three satellites are required for the first fix in Self-survey mode. • Disabled—Only one satellite is required for a valid timing fix.	Enabled

High-availability Seamless Redundancy (HSR)

HSR is available on Stratix 5400 switches. HSR is defined in International Standard IEC 62439-3-2016 clause 5.

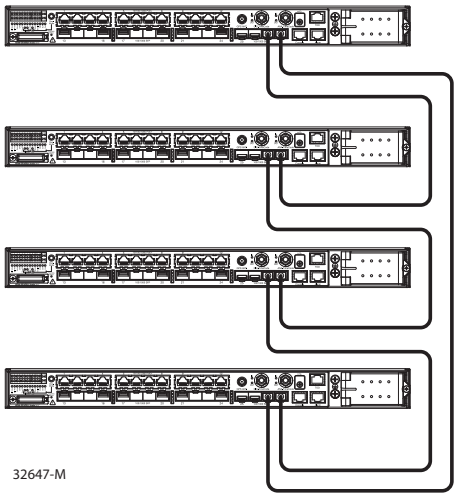
For instructions on how to configure HSR via the CLI, refer to documentation available at http://www.Cisco.com.

IMPORTANT To use HSR, be sure that the switch is using the HSR feature application profile as described on page 147.

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. You can support up to as many as 48 port channels.

Figure 13 - 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 greater 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 1783-IMS28RAC 1783-IMS28NDC 1783-IMS28RDC	Te1/25 Te1/26 Te1/27 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 the template of the master switch, apply the matching SDM template separately before you connect the switch to the stack.

When connecting ports between switches in a stacked Stratix 5410 configuration, the horizontal stack port must be the same between both ports.

You can configure a stack in either a Ring topology (Figure 14) or a Linear topology (Figure 15).

Figure 14 - Switch Stack in a Ring Topology

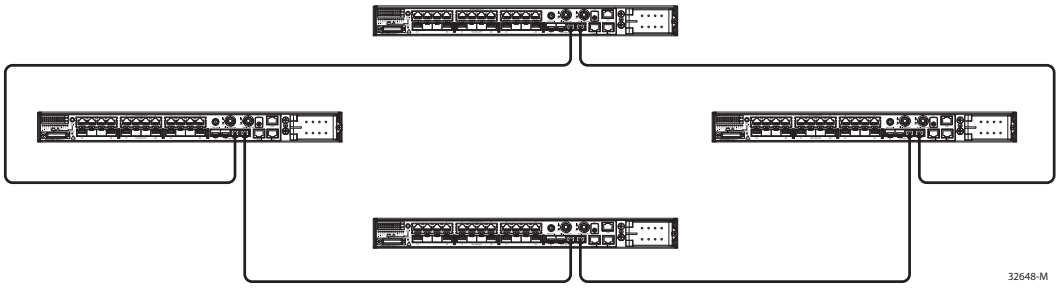


Figure 15 - Switch Stack in a Linear Topology

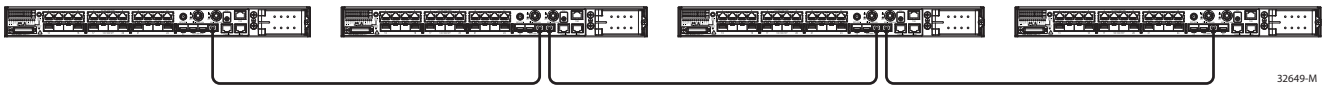


Table 72 lists the supported features for horizontal stacking.

Table 72 - 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 • Border Gateway Protocol (BGP) • Enhanced Interior Gateway Routing Protocol (EIGRP) • Layer 3 host configuration • Open Shortest Path First (OSPF) • Policy Based Routing (PBR) • Protocol Independent Multicast (PIM) • Static routes • Virtual Routing and Forwarding (VRF)
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

Features that are not listed in Table 72 are not supported. Unsupported features include, but are not limited to, Device Manager, CIP, Layer 2 NAT, PRP, and PTP.

Hot Standby Router Protocol (HSRP)

Hot Standby Router Protocol (HSRP) provides high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address.

HSRP routes IP traffic without relying on the availability of any single router. This enables a set of router interfaces to work together to present the appearance of a one virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers.

HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address if the designated active router fails.

You can configure multiple HSRP groups among switches that are operating in Layer 3 to make more use of the redundant routers. To do so, specify a group number for each HSRP command group you configure for an interface. For example, you can configure an interface on switch 1 as an active router and one on switch 2 as a standby router. You can also configure another interface on switch 2 as an active router with another interface on switch 1 as its standby router.

The switch supports two HSRP versions.

HSRPv1-Version 1

The HSRPv1 is the default version. This version has the following features:

- The HSRP group number can be from 0 to 255.
- HSRPv1 uses the multicast address 224.0.0.2 to send hello packets.

HSRPv2-Version 2

The HSRPv2 has the following features:

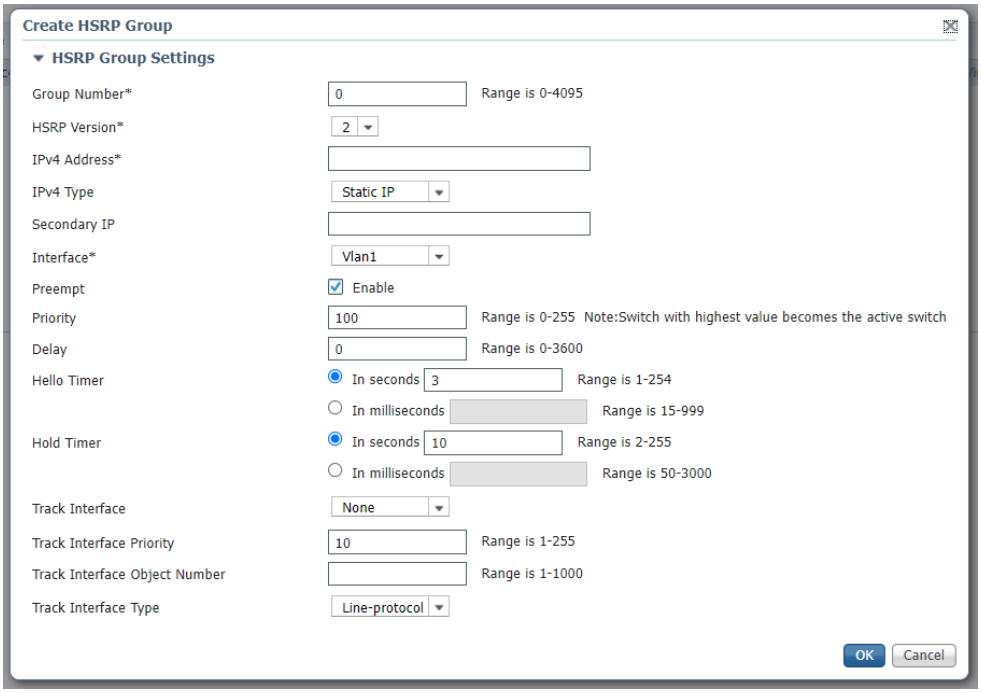
- To match the HSRP group number to the VLAN ID of a subinterface, HSRPv2 can use a group number from 0 to 4095 and a MAC address from 0000.0C9F.F000 to 0000.0C9F.FFFF.
- HSRPv2 uses the multicast address 224.0.0.102 to send hello packets. HSRPv2 and CGMP leave processing are no longer mutually exclusive, and both can be enabled simultaneously.
- HSRPv2 has a different packet format than HRSPv1.

Configure HSRP via Device Manager

To configure an HSRP Group via Device Manger, use the following steps:

1. On the Configuration > Redundancy Protocols > HSRP page, click Add.

2. Configure settings for the HSRP group based on the following table and image.



Setting	Description
Group Number	The group number on the interface for which HSRP is being enabled. Range: 0...255 Default: 0
HSRP Version	The version of HSRP: • HSRPv1 - Default • HSRPv2
IPv4 Address	The virtual IP address of the hot standby router interface.
IPv4 Type	Static IP - Not configurable
Secondary IP	Optional secondary IP address of the hot standby router interface.
Interface	The Layer 3 interface on which you want to enable HSRP.
Preempt	To allow the local router to assume control as the active router when the router has a higher priority than the active router, select this checkbox.
Priority	Priority value value that is used in choosing the active router. Range: 0...255 Default: 100 The router with the highest priority value becomes the active router.
Delay	Delay value to cause the local router to postpone taking over the active role for the configured number of seconds. Range: 0...3600 (1 hour) Default: 0 (no delay before taking over)

Setting	Description
Hello Timer	Set the value for the time between hello packets in seconds or milliseconds.: Range in seconds: 1…254. Default: 3. Range In milliseconds: 15…999. There is no default.
Hold Timer	The time before other routers declare the active router or the standby router to be down. Set the value in seconds or milliseconds: Range in seconds: 2…255. Default: 10. Range in milliseconds: 50…3000. There is no default.
Track Interface	Select an interface for Track Interface if you want to specify another interface on the router for the HSRP process to monitor to alter the HSRP priority for a given group. If the line protocol of the specified interface goes down, the HSRP priority is reduced. This means that another HSRP router with higher priority can become the active router if that router has standby preempt enabled.
Track Interface Priority	Priority value for the tracked interface to specify how much to decrement the Hot Standby priority when the tracked interface goes down. When the tracked interface comes back up, the priority is incremented by the same amount. Range is 1…255 Default: 10
Track Interface Object Number	Number for the tracked interface from 1…1000.
Track Interface Type	The type of interface to be tracked.

3. Click OK.

HSR-HSR (Quadbox)

HSR-HSR topology is available on Stratix 5400 switches and allows for the connection of multiple HSR rings, which mainly optimizes scaling and segregation of traffic between related devices. The switch functions as a quadbox, with two ports on one ring, and two ports on a second ring.

HSR-HSR is configured via the CLI.

For instructions on how to configure HSR-HSR via the CLI, refer to documentation available at http://www.Cisco.com.

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 ID or to any reserved multicast MAC IDs (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address alias issues.

Table 73 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 73 - Default Supported Multicast Groups

Switch	Default Multicast Groups
Stratix 5400 and Stratix 5410 switches	1024
Stratix 5700 and ArmorStratix 5700 switches	256
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 that run IGMP V1. The switch has a built-in querier function, and the global macro enables on IGMP snooping and the querier.

Configure IGMP Snooping with Querier via Device Manager

IMPORTANT In a PRP system, follow these guidelines:

- To enable multicast traffic filtering on both LANs, configure IGMP querier on a RedBox.
- Enable IGMP General Query (see Configure a RedBox via Device Manager).
- To avoid a single point of failure with the loss of a querier, configure at least two queriers in the PRP network.
- Disable IGMP querier on each LAN A and LAN B infrastructure switch.

From the Configure menu, choose IGMP Snooping.

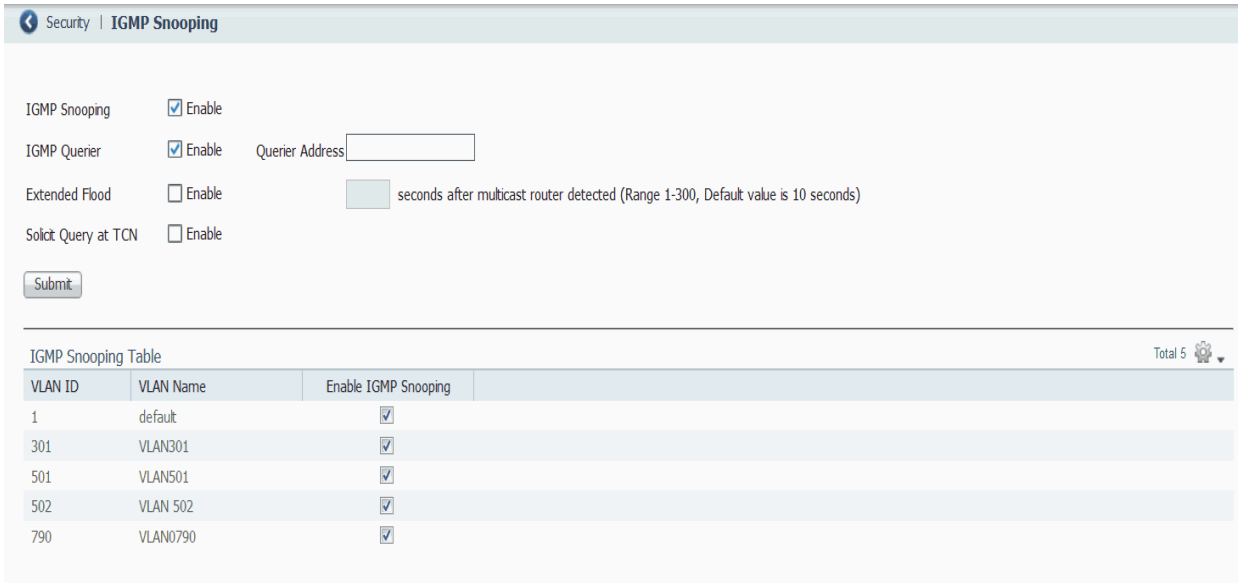


Table 74 - IGMP Snooping Fields

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

Internet Protocol Device Tracking (IPDT)

IPDT is enabled automatically when an IPDT-dependent feature, such as NetFlow, is configured or enabled on the switch. The IPDT feature is available on the Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 switches.

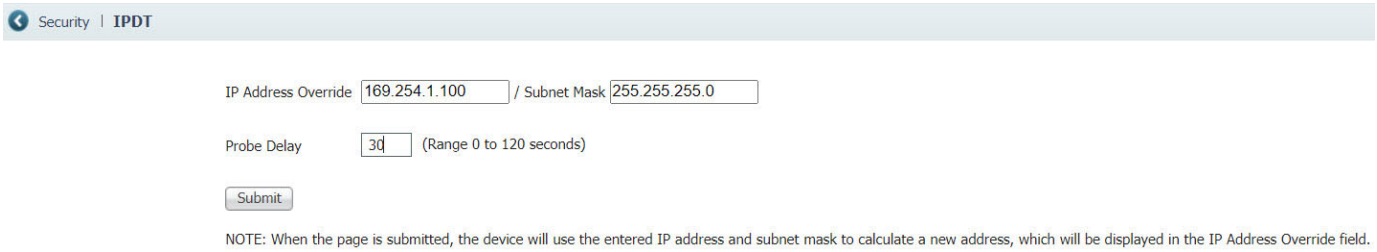
The switch maintains an IPDT table, which contains the IP addresses of detected devices. The switch detects the presence of connected IP devices by monitoring Address Resolution Protocol (ARP) packets. The switch can also detect IP devices through DHCP requests if DHCP snooping is enabled.

When IPDT is enabled, Device Manager displays a message, prompting you to configure an IP address override. Configure the address to avoid duplicate IP address issues.

Configure IPDT via Device Manager

To configure the IPDT, follow these steps.

1. From the Configure menu, choose IPDT under the Security section.



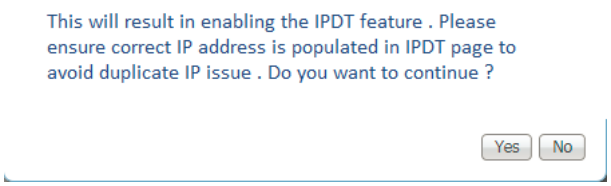
IMPORTANT When you run Express Setup, the default value is 169.254.1.100 and the probe delay is 15 seconds.

2. Complete the fields in Table 2 and click Submit.

Table 75 - IPDT Fields

Field	Description
IP Address Override/Mask	Enter an IP address and subnet mask that does not need to belong to the switch for use as the source address in ARP probes generated by IPDT.
Probe Delay	Enter the delay time of IP tracking probes The range is 0...120 seconds. The default is 30.

3. Click Yes to the warning message to enable this IPDT feature.



Link Layer Discovery Protocol (LLDP)

LLDP is defined in international standard IEEE 802.1AB and 802.3. Network devices use LLDP to advertise information about themselves to other devices on the network. Because LLDP runs over the data-link layer, two systems that run different network layer protocols can learn about each other.

LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as type-length-value (TLV) structures. LLDP supported devices can use TLV structures to receive and send information to their neighbors. By using LLDP, devices can advertise details, such as configuration information, device capabilities, and device identity.

Table 76 describes the TLV structures.

Table 76 - LLDP TLV Structures

TLV Structure	Description
4-wire-power-management	The 4-pair related capabilities and requirements of Cisco Universal Power Over Ethernet (UPOE) devices.
mac-phy-cfg	The IEEE 802.3 MAC/Phy configuration/status.
management-address	The IP address used for management.
port-description	The source port.
port-vlan	The VLAN present on the access port.
power-management	The power classes, wattage requirements, and priority of PoE devices.
system-capabilities	The device features.
system-description	The IOS version.
system-name	The device name.

Configure LLDP

On the LLDP tab, complete the fields in as described in Table 77, and then click Apply to Device.

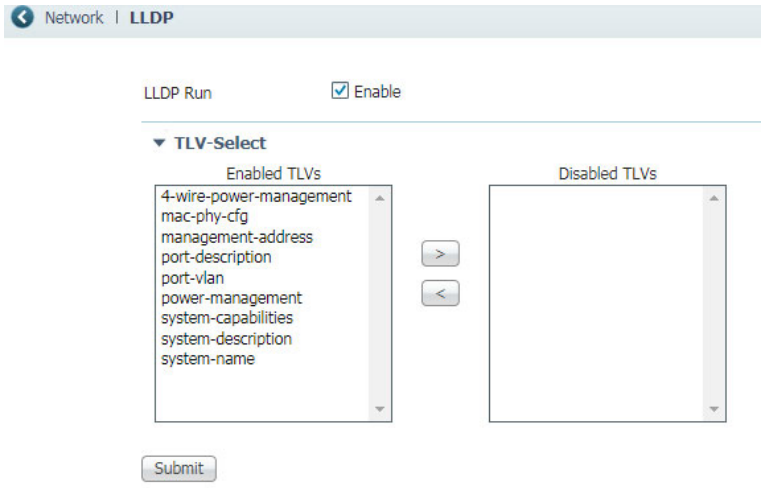


Table 77 - Discovery Protocols—LLDP

Field	Description
LLDP	Click to enable or disable LLDP. LLDP is disabled by default.
TLVs	Specify which TLV structures to enable or disable by moving them to the respective columns. For a description of each TLV structure, see Table 76 on page 159. By default, all TLV structures are enabled.

Maximum Transmission Unit (MTU)

The MTU defines the largest size of frames that an interface can send or receive in a network transaction.

In Device Manager, you can change the following MTU settings on the switch:

- System MTU—Applies to all interfaces.
- Jumbo MTU—Overrides the system MTU on all Gigabit Ethernet and 10-Gigabit Ethernet interfaces.

IMPORTANT In a PRP system, you must set the jumbo MTU size to at least 1506 on all switches in LAN A and LAN B. This size enables the switch to pass a full-sized packet with the PRP trailer attached. This MTU value is not required for a switch that is configured as a RedBox. For more information about PRP and frame size requirements, see the EtherNet/IP Parallel Redundancy Protocol Application Technique, publication ENET-AT006.

Configure the MTU via Device Manager

To configure the MTU, follow these steps.

1. From the Admin menu, choose MTU.
2. Complete the fields as described in Table 78 and click Submit.

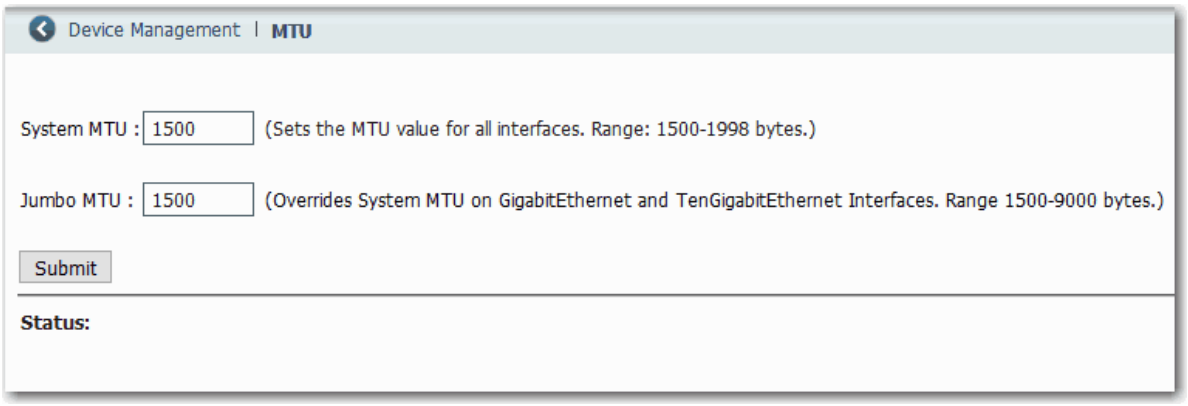
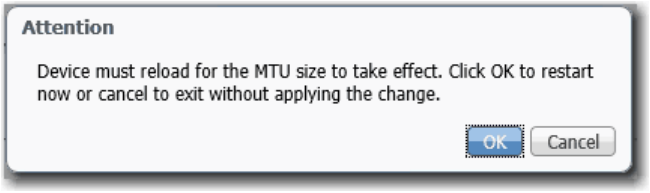


Table 78 - MTU Fields

Field	Description
System MTU	Sets the MTU value for all interfaces. Valid values: 1500...1918 bytes
Jumbo MTU	Overrides the system MTU on all Gigabit Ethernet and 10-Gigabit Ethernet interfaces. Valid values: 1500...9000 bytes

3. When the following message appears, click OK and restart the switch.



Motion Prioritized QoS Macros

During Express Setup, the switch applies QoS settings that are 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 79 - 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

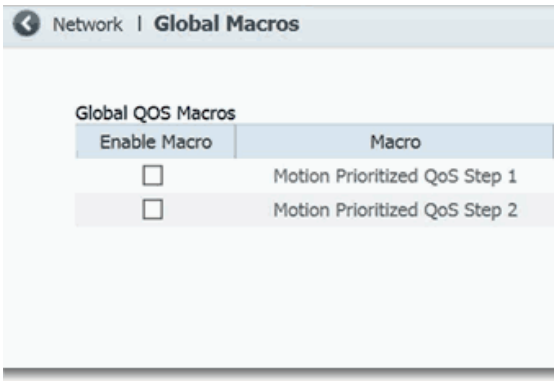
From the Configure menu, choose Global Macros:

- 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 that are applied during Express Setup remain active.

Stratix 5700, ArmorStratix 5700, and Stratix 8000 Switches



Stratix 5400 and 5410 Switches

NetFlow

NetFlow is available on Stratix 5400 and 5410 switches. NetFlow provides traffic flow monitor services, including network traffic accounting, usage-based network billing, network planning, security, denial-of-service, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing.

A flow is a unidirectional stream of packets that have the same flow key values. NetFlow consists of these components:

- Flow Record—A flow record defines the unique keys that are used to identify packets in the flow, and other fields that NetFlow gathers for the flow. Device Manager provides predefined flow record templates that you can use to configure NetFlow and begin to monitor the network traffic.
- Flow Monitor—Flow monitors are applied to ports to perform network traffic monitoring. Flow data is collected from the network traffic and added to the flow monitor cache during the monitoring process based on the key and nonkey fields in the flow record. You define the size of the data that you want to collect for a flow by using a monitor.
- Flow Sampler—Flow samplers are used to reduce the load on the switch that is running NetFlow by limiting the number of packets that are selected for analysis. Samplers use random sampling techniques.

  Flow sampling exchanges monitoring accuracy for router performance. When you apply a sampler to a flow monitor, the overhead load on the switch that is running the flow monitor is reduced because the monitor must analyze fewer packets. The reduction in packets causes a corresponding reduction in the accuracy of the information that is stored in the cache of the flow monitor.
- Flow Exporter—You can export the data that NetFlow gathers for your flow by using an exporter. Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage.

There can be one record per monitor and one monitor per port. You can have multiple exporters per monitor. The flow records, flow monitor, flow exporter, and sampler cannot be modified once applied to a port.

There are two primary methods to access NetFlow data:

- The command-line interface (CLI)—Use show commands to view data and troubleshoot.
- An application reporting tool—Export flows to a reporting server, which is known as a NetFlow collector. The NetFlow collector uses the flows to produce reports for traffic and security analysis.

For more information about NetFlow, see www.cisco.com.

NetFlow Templates

Table 80 describes the predefined flow record templates.

Table 80 - NetFlow Templates

Template	Record	Description
Application Traffic	match ipv4 protocol match ipv4 source address match ipv4 destination address match transport source-port match transport destination-port collect transport tcp flags collect counter packets long collect timestamp sys-uptime first collect timestamp sys-uptime last	Monitors application traffic.
Security	match ipv4 tos match ipv4 protocol match ipv4 source address match ipv4 destination address match transport source-port match transport destination-port collect transport icmp ipv4 type collect transport icmp ipv4 code collect transport tcp flags collect counter packets long collect timestamp sys-uptime first collect timestamp sys-uptime last	Monitors packets for network security.
Capacity Planning	match ipv6 protocol match ipv6 source address match ipv6 destination address match transport source-port match transport destination-port collect interface input collect interface output collect counter packets long	Monitors packets to analyze network capacity and usage.
StealthWatch	match datalink mac source address input match datalink mac destination address input match ipv4 tos match ipv4 protocol match ipv4 source address match ipv4 destination address match transport source-port match transport destination-port collect transport tcp flags collect interface input collect interface output collect counter bytes long collect timestamp sys-uptime first collect timestamp sys-uptime last	Monitors packets to detect threats and security vulnerabilities.

Configure NetFlow via Device Manager

Add a NetFlow configuration to create the monitor and associated exporter and sampler.

To add a NetFlow configuration, follow these steps.

1. From the Configure menu, choose NetFlow.
2. On the Configure NetFlow tab, click Add.
3. Complete the fields as described in Table 81 and click OK.

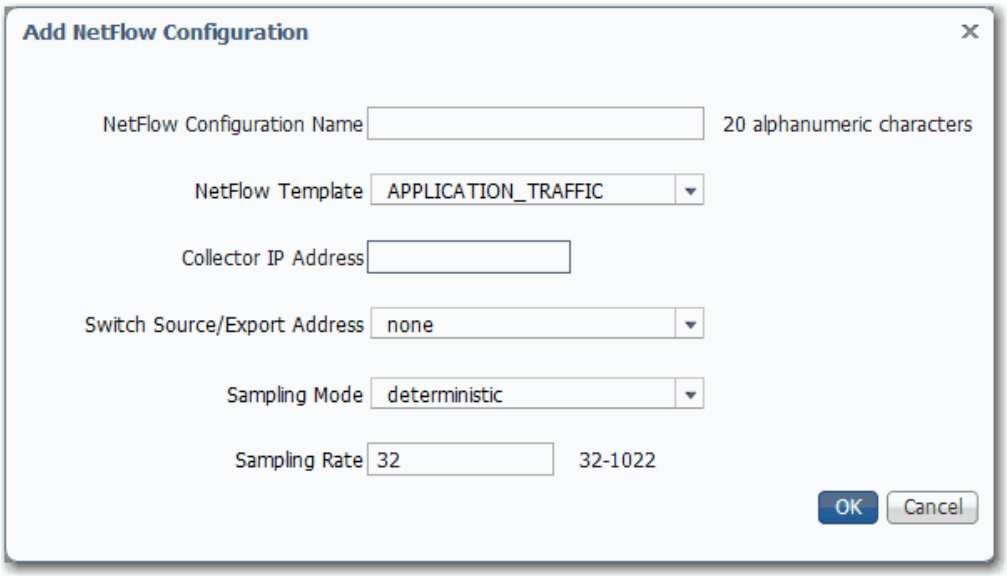


Table 81 - Add NetFlow Configuration Fields

Field	Configuration
NetFlow Configuration Name	Enter a name for the NetFlow configuration.
NetFlow Template	Choose a predefined flow record template from the pull-down menu. • APPLICATION_TRAFFIC—Monitors application traffic. • SECURITY—Monitors packets for network security. • CAPACITY_PLANNING—Monitors packets to analyze network capacity and usage. • STEATH_WATCH—Monitors packets to detect threats and security vulnerabilities.
Collector IP Address	Enter the IP address of the collector device (flow analyzer) where records are sent.
Switch Source/Export Address	Choose the switch IP address to be used for connecting with the collector device.
Sampling Mode	Choose the mode to use in the selection of network traffic: • deterministic—Enables deterministic mode sampling for the sampler. This mode selects every nth packet for NetFlow processing, as specified by Sampling Rate. For example, if you set the sampling rate to 1 out of 100 packets, then NetFlow samples the 1st, 101st, 201st, 301st, and so on packets. • random—Enables random mode sampling for the sampler. Incoming packets are randomly selected so that one out of each n sequential packets is selected on average for NetFlow processing at the rate that is specified in Sampling Rate. For example, if you set the sampling rate to 1 out of 100 packets, then NetFlow might sample the 5th packet and then the 120th, 199th, 302nd, and so on. This sample configuration provides NetFlow data on 1 percent of total traffic. • full netflow—All packets that arrive on the interface are sampled. When this mode is selected, the Sampling Rate option is not available.
Sampling Rate	Enter the rate (one out of every n packets) at which packets are selected for NetFlow processing. For n, you can specify 32...1022 packets. The default is 32.

Apply a NetFlow Configuration via Device Manager

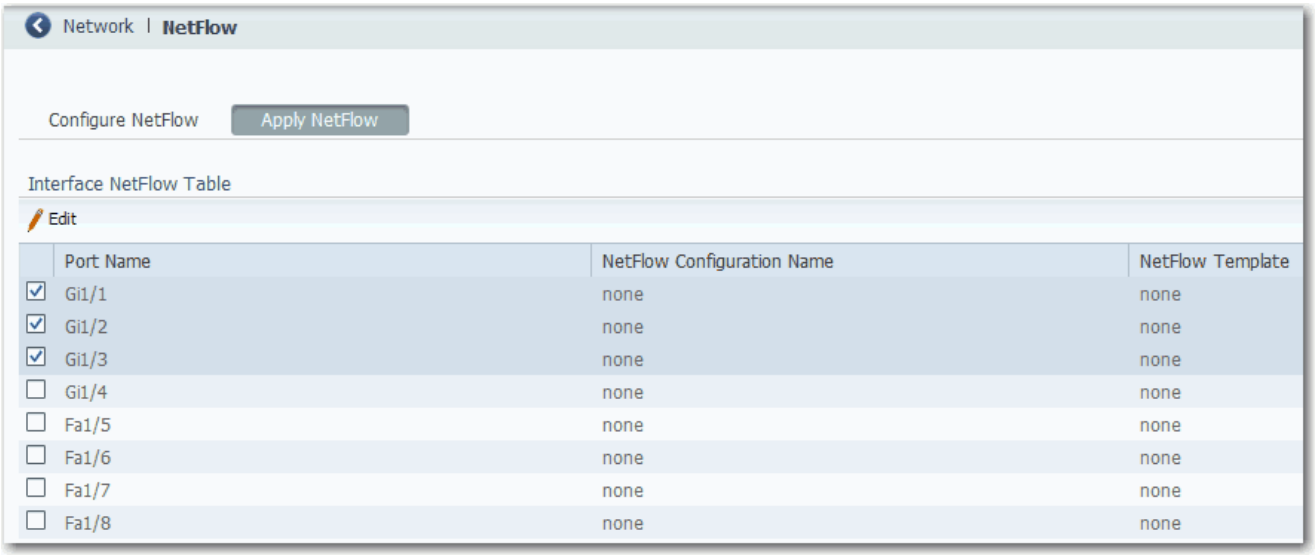
When you apply a NetFlow configuration (flow monitor with a sampler) to a port, the sampled packets are analyzed at the rate that is specified by the sampler and compared with the flow record that is associated with the flow monitor. If the analyzed packets meet the criteria specified by the flow record, they are added to the flow monitor cache.

IMPORTANT When you apply a NetFlow configuration to a port, IP Device Tracking (IPDT) is enabled on the port. IPDT can cause duplicate IP address detection on some EtherNet/IP modules. For more information, see the Rockwell Automation Knowledgebase Answer ID 568750.

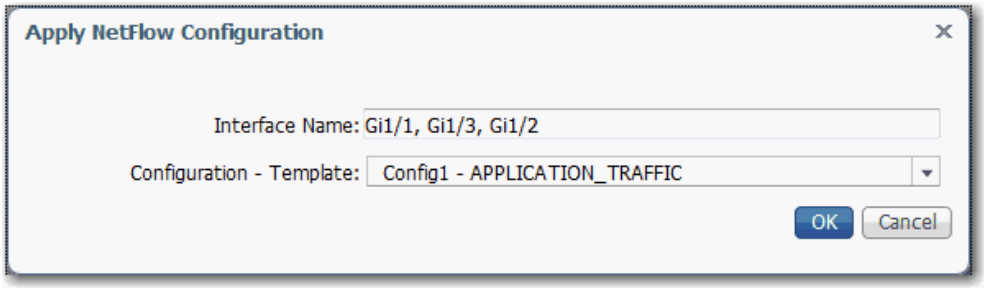
To apply a NetFlow configuration to ports, follow these steps.

1. From the Configure menu, choose NetFlow.
2. Click the Apply NetFlow tab.
3. To select a port, click the port name and click Edit.

   You can select multiple ports and apply the same NetFlow configuration to them at one time.



4. On the Apply NetFlow Configuration dialog box, choose the NetFlow configuration to apply to the port and click OK.



Network Address Translation (NAT)

For a list of switches that support NAT, see page 16.

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.

If traffic is routed through a Layer 3 switch or router (Figure 16 and Figure 17), you define the following:

- A private-to-public translation for each device on the private subnet that communicates on the public subnet.(2)
- 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.

(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.

(2) Machines that communicate with each other within the same VLAN and subnet across a NAT boundary also require public-to-private translations.

Figure 16 - Layer 3 Example with NAT in Stratix 5700 Switch

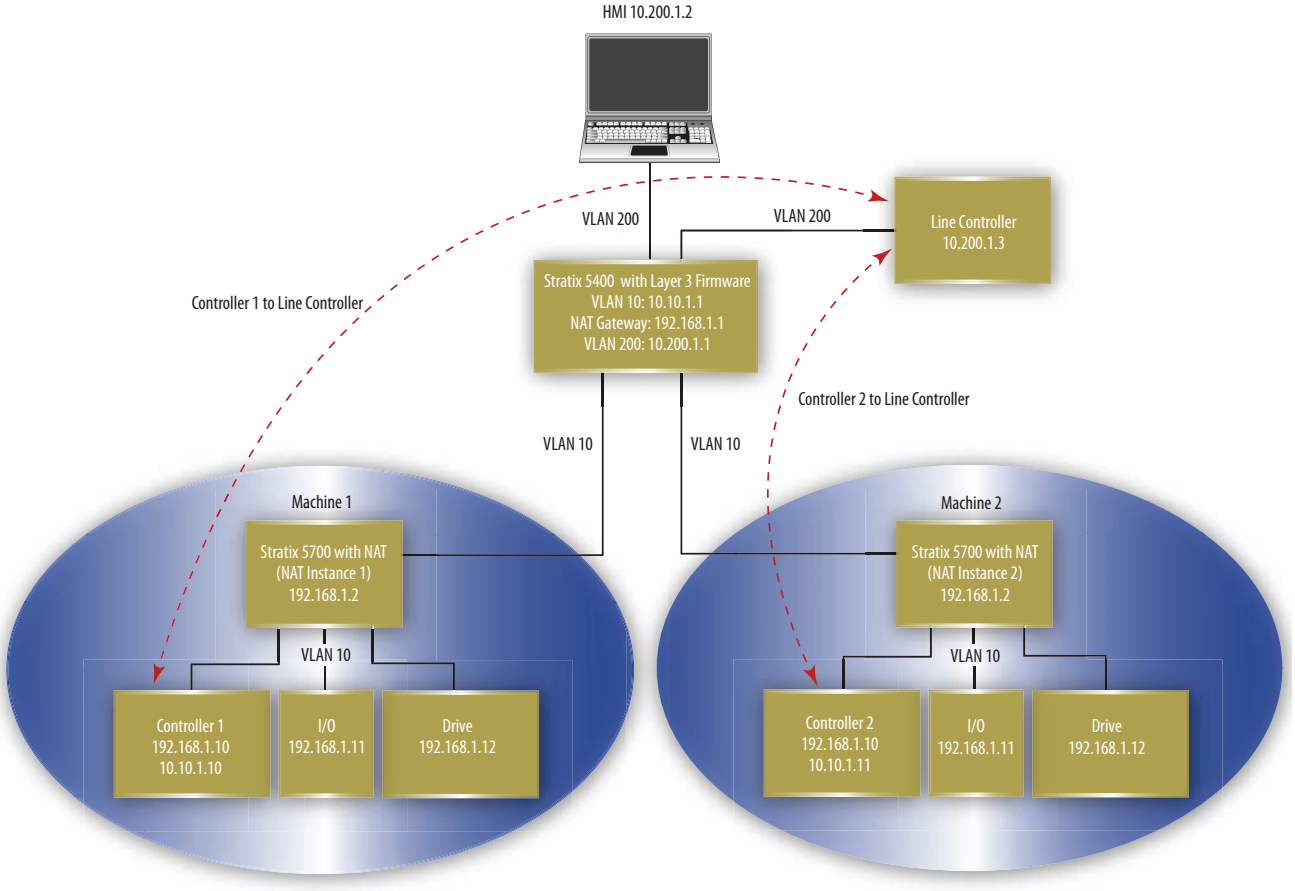
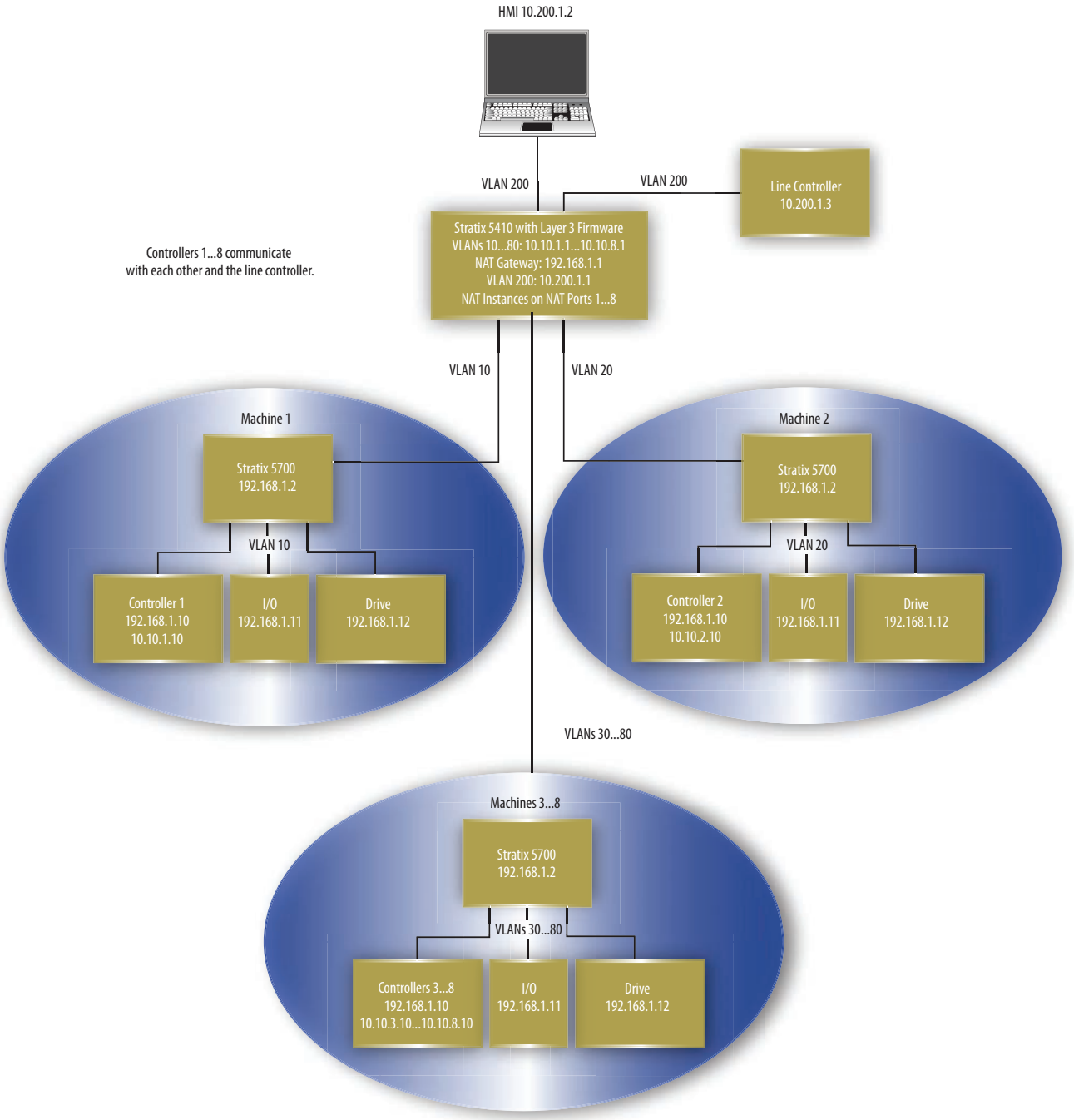


Figure 17 - Layer 3 Example with NAT in Stratix 5410 Layer 3 Firmware Model



If traffic is routed through a Layer 2 switch (Figure 18 and Figure 19), 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 18 - Layer 2 Example with NAT in Stratix 5700 Switch

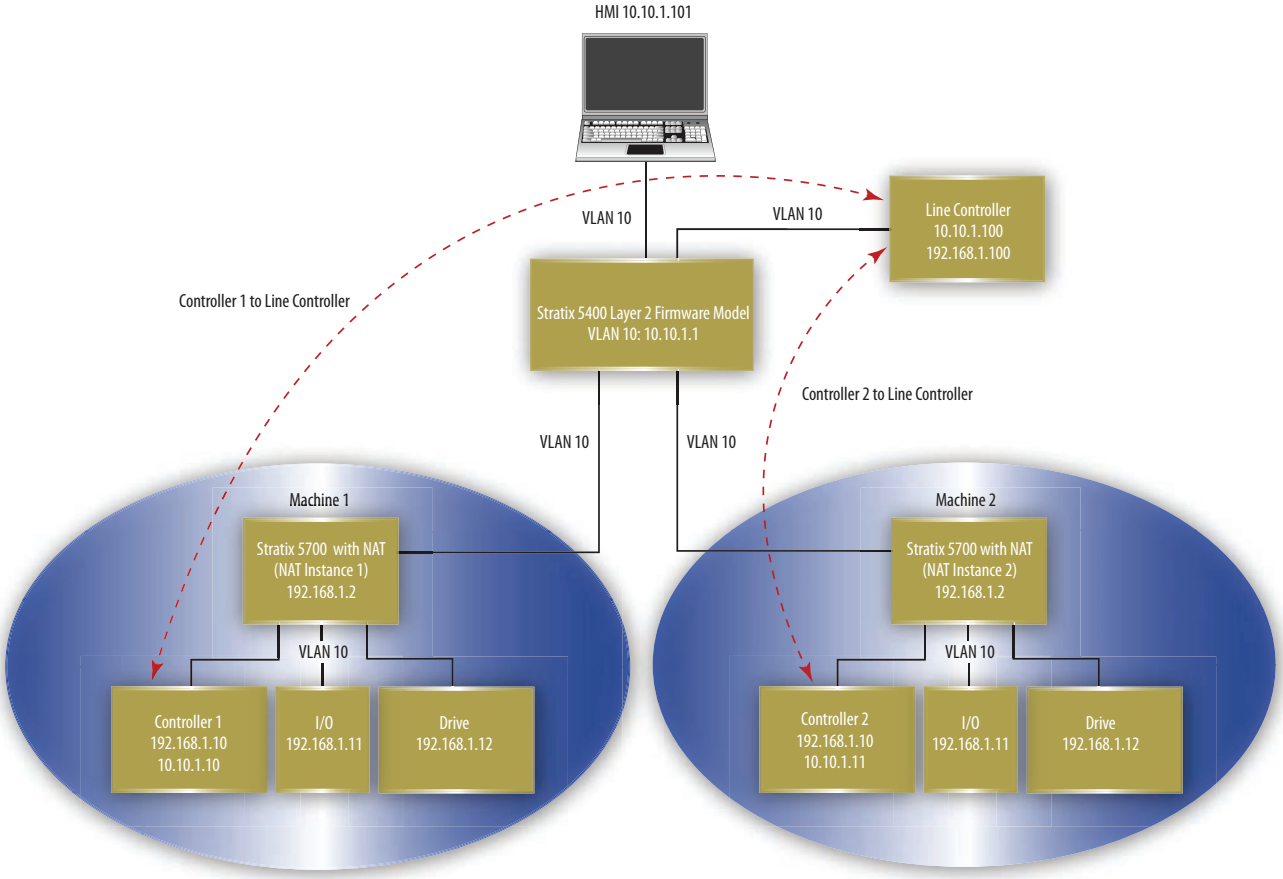
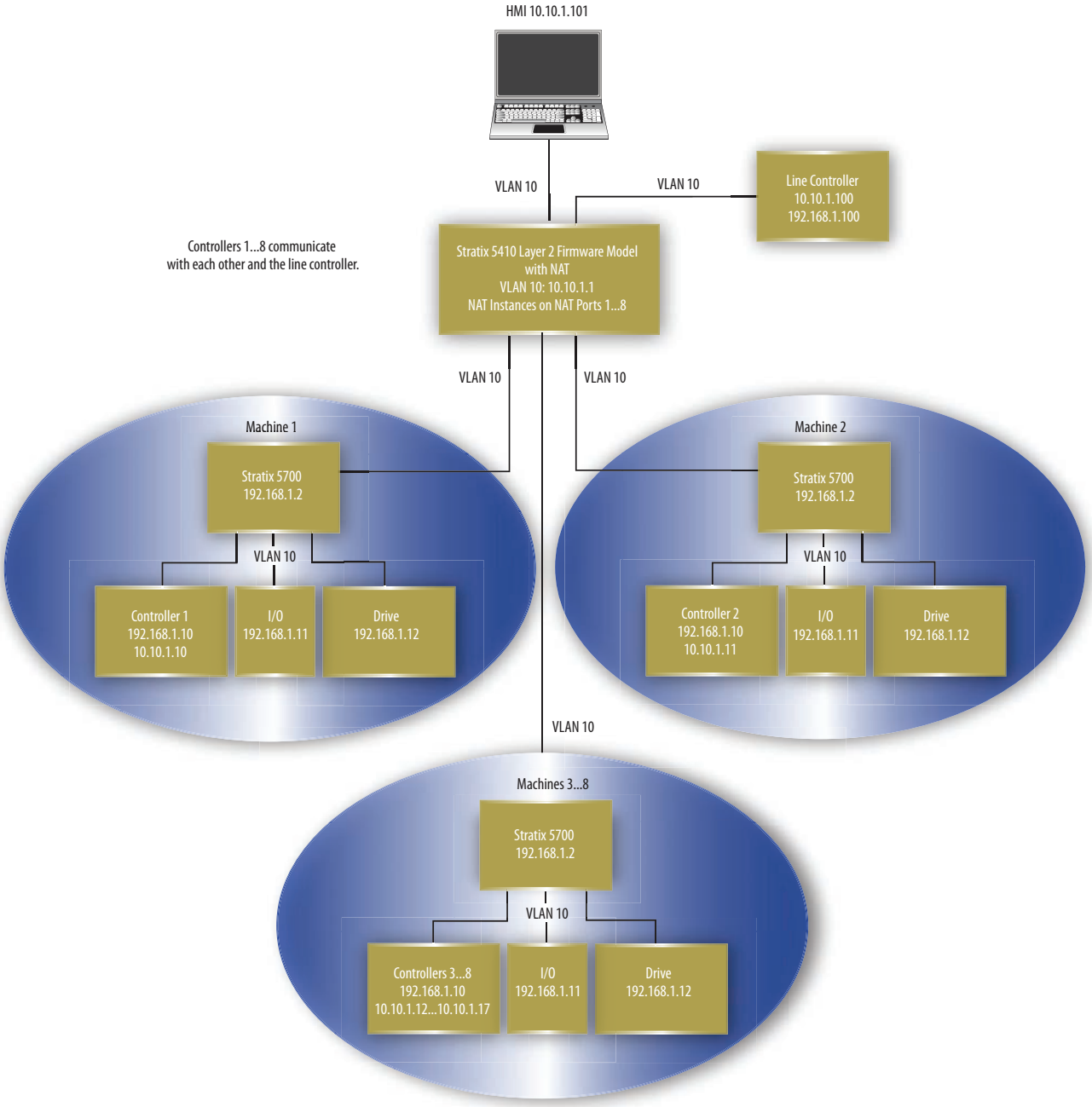


Figure 19 - Layer 2 Example with NAT in Stratix 5410 Layer 2 Firmware Model



An address translation can be one of three types. The type of translation determines the number of translation entries as shown in Table 82.

Table 82 - 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

Single 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 that allows one translation entry for many addresses.

Table 83 defines the maximum number of translation entries that are allowed per switch.

Table 83 - 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 that is 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 before 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(1)
Downlink Ports	0	0	8(1)
Translation Entries(2)	128	128	256(3)

(1) Both uplink and downlink ports can be configured for as many as 8 NAT ports.
(2) A subnet translation counts as only one translation entry, but includes translations for many devices
(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 16 and Figure 19.
- Create NAT Instances for Traffic Routed through a Layer 2 Switch

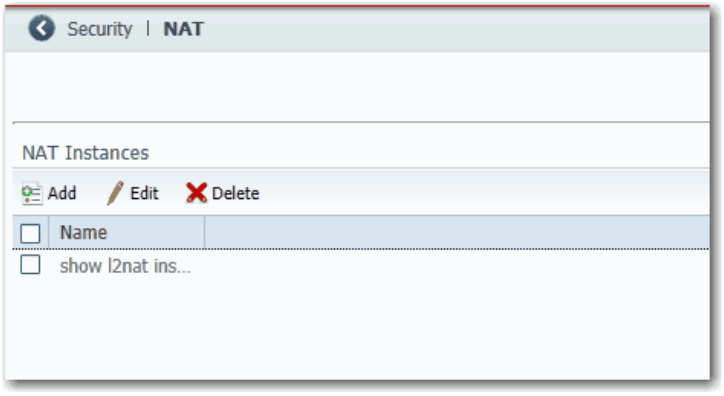
  For an example of this application, see Figure 18 and Figure 19.

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.

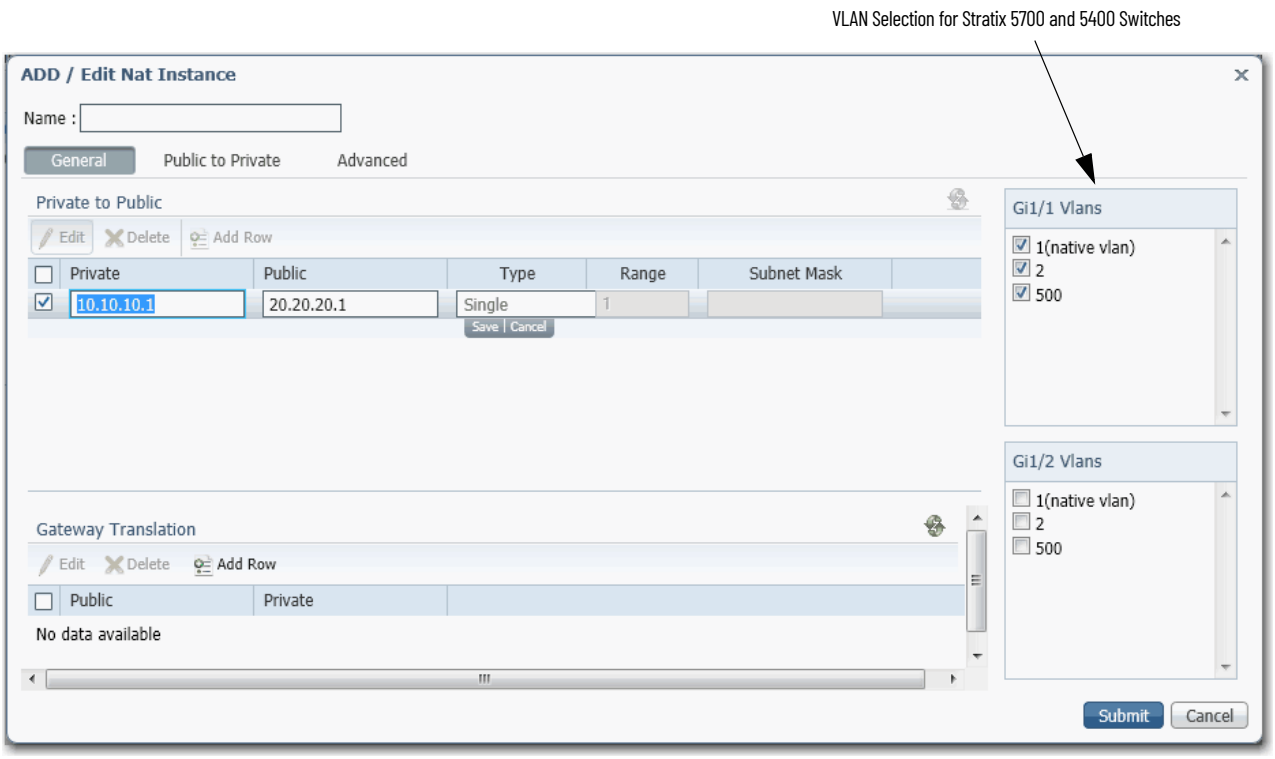
IMPORTANT	As a result of Layer 2 forwarding, current traffic sessions remain established until manually disconnected. If you change an existing translation, you must manually disconnect all associated traffic sessions before the new translation can take effect.

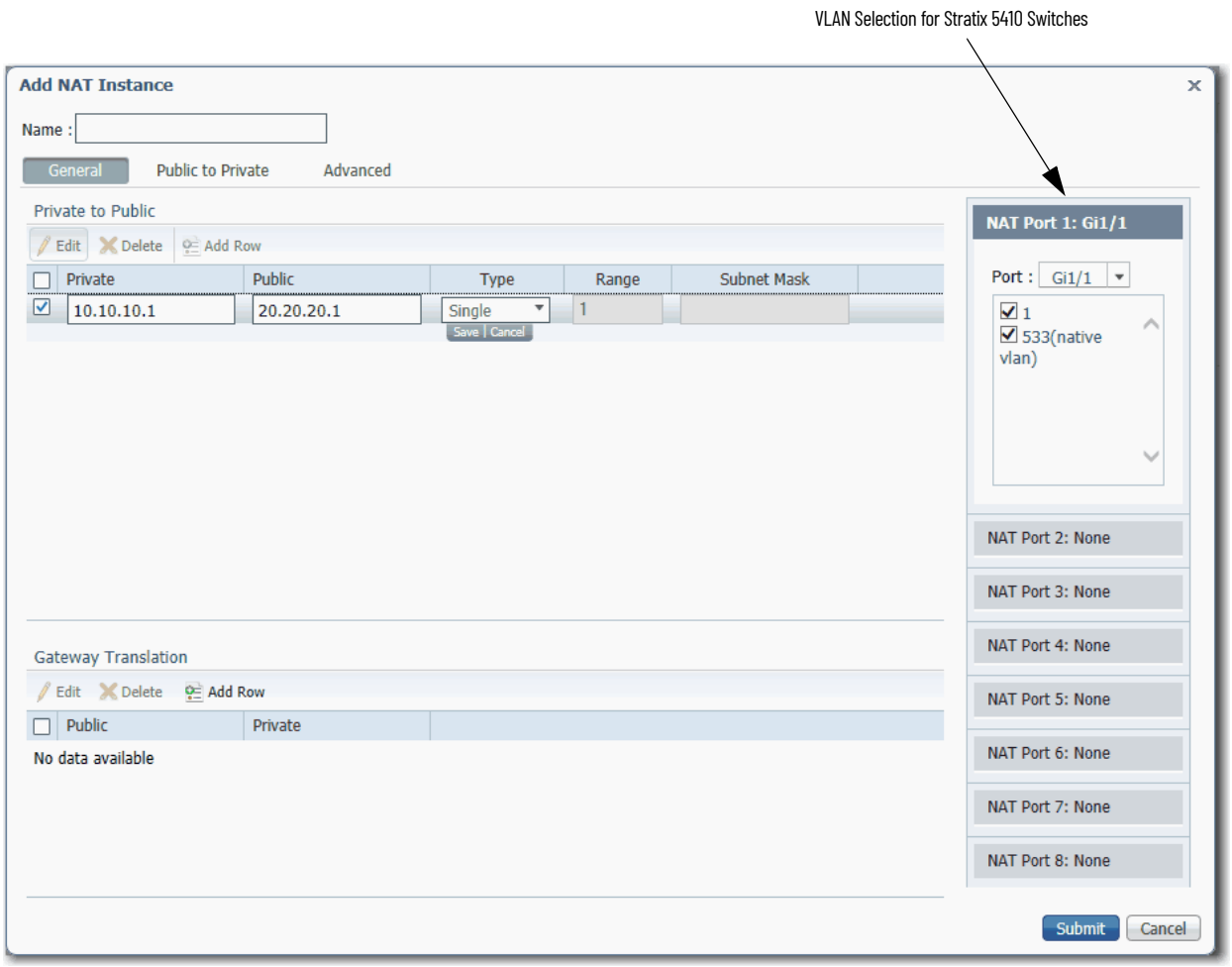
Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router

1. From the Configure menu, choose NAT to display the NAT page.



2. Click Add to display the General tab of the Add/Edit NAT Instance page.





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 you choose 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 173.

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

Field	Description	
Public IP Address	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.	
	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 end in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	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:** 10.200.1.16
Type	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.	
Range	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.	
Subnet Mask	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)	

6. In the Gateway Translation area, click Add Row, complete the fields, and click Save.

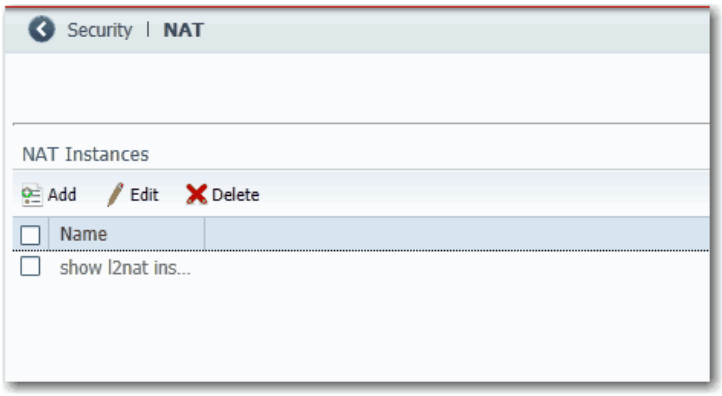
   The gateway translation enables devices on the public subnet to communicate with devices on the private subnet.

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.

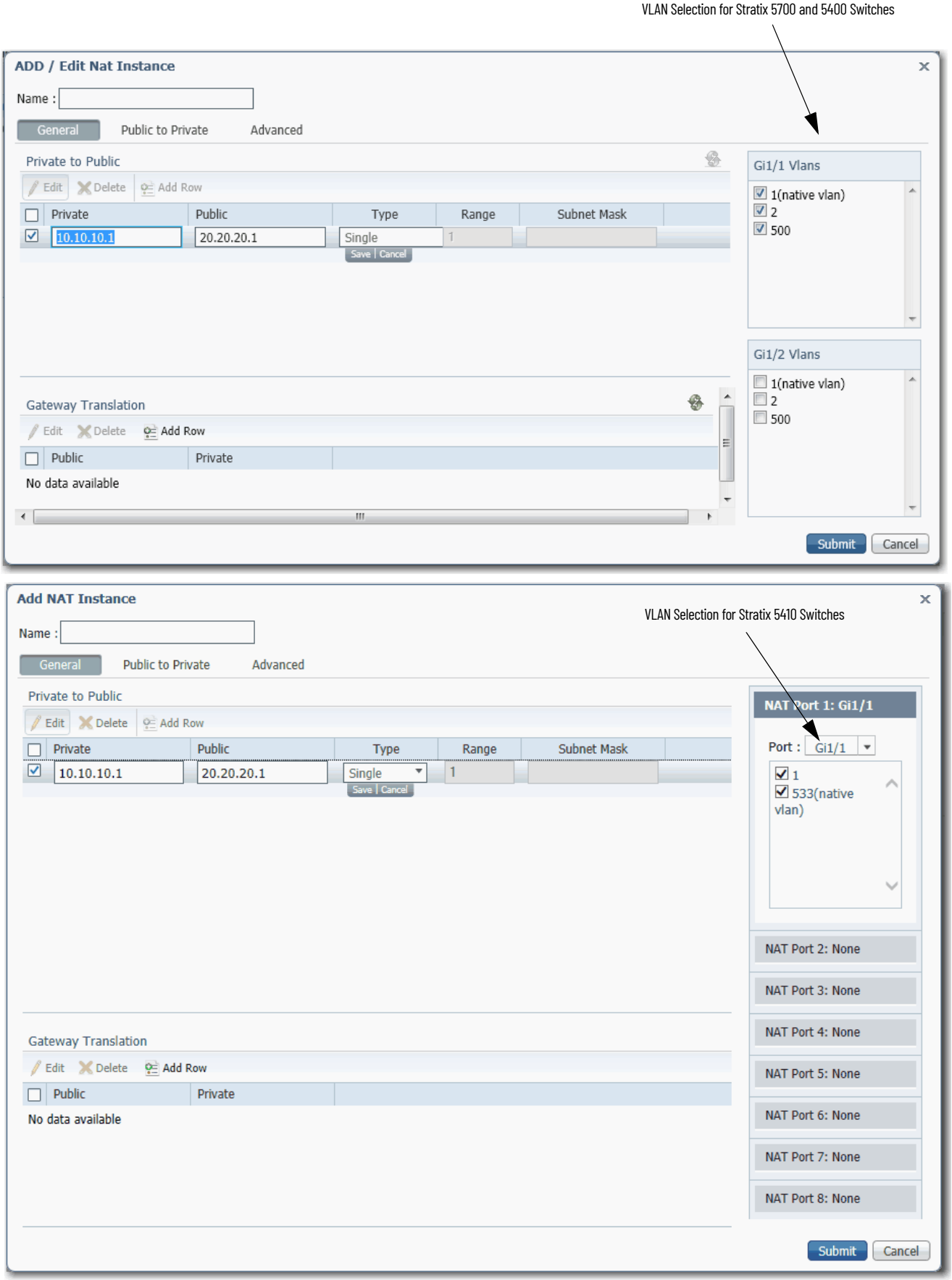
7. (Optional). To configure traffic permits and packet fixups, see Configure Traffic Permits and Fixups on page 184.
8. Click Submit.

Create NAT Instances for Traffic Routed through a Layer 2 Switch

1. From the Configure menu, choose NAT to display the NAT page.



2. Click Add to display the General tab of the Add/Edit NAT Instance page.



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 you choose 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.

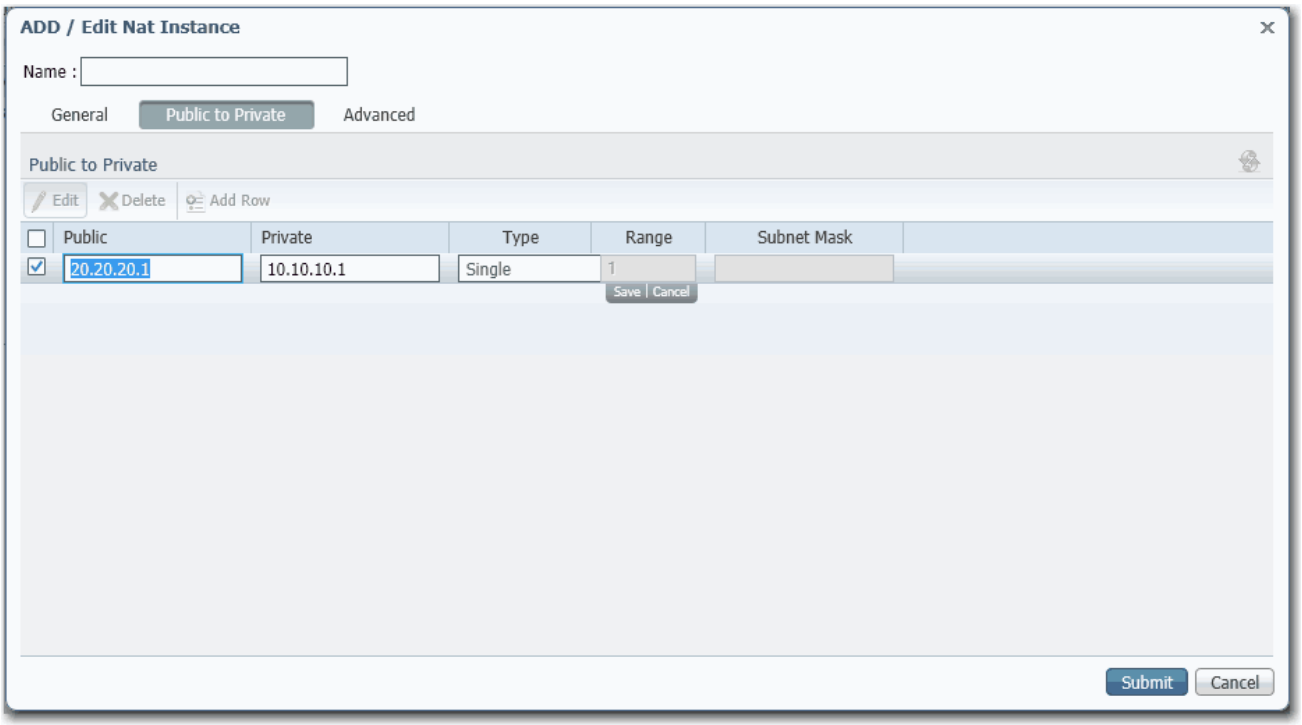
   For more information about VLAN assignments, see page 173.

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 colspan="2">Description</th></tr>
<tr><td rowspan="8">Public IP Address</td><td colspan="2">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.</td></tr>
<tr><td>Subnet Mask</td><td>Starting Public Subnet Address</td></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>
<tr><td>Type</td><td colspan="2">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 colspan="2">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 colspan="2">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.

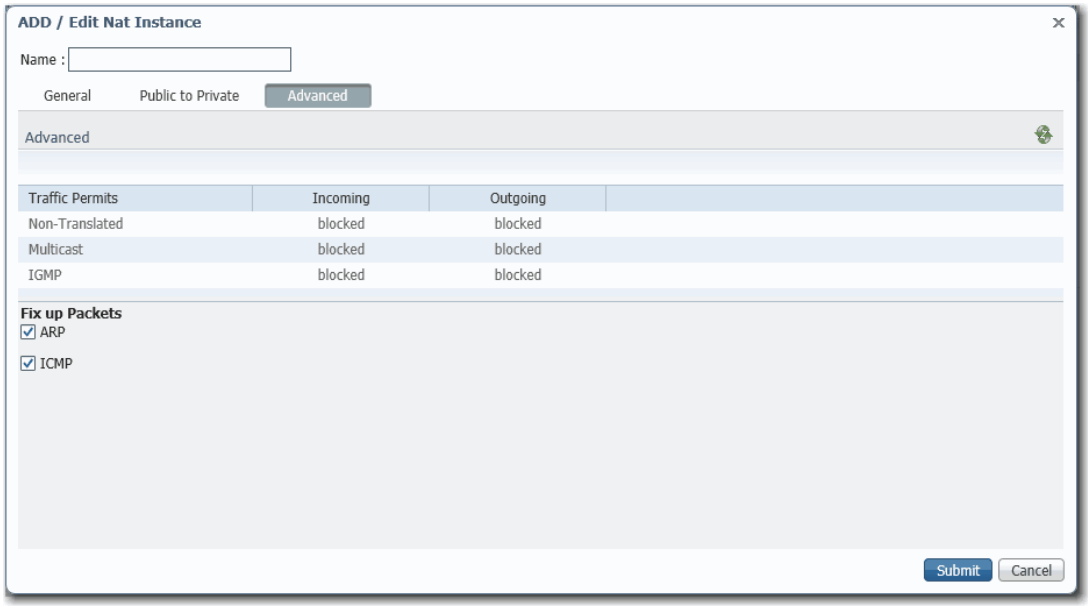
Field	Description	
Public IP Address	Type a public IP address: • To translate one address, type the existing address for the device on the public subnet. • To translate a range of addresses, type the first address in the range of sequential addresses. • To translate addresses in a subnet, type the existing 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 end in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	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:** 10.200.1.16
Private IP Address	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.	
	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:** 10.200.1.16
Type	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.	
Range	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.	
Subnet Mask	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)	

8. (Optional). To configure traffic permits and packet fixups, see Configure Traffic Permits and Fixups.
9. On the NAT page, click Submit.

Configure Traffic Permits and Fixups

Use caution when you configure traffic permits and fixups. We recommend that you use the default values.

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 195.

In the navigation pane, click NAT.

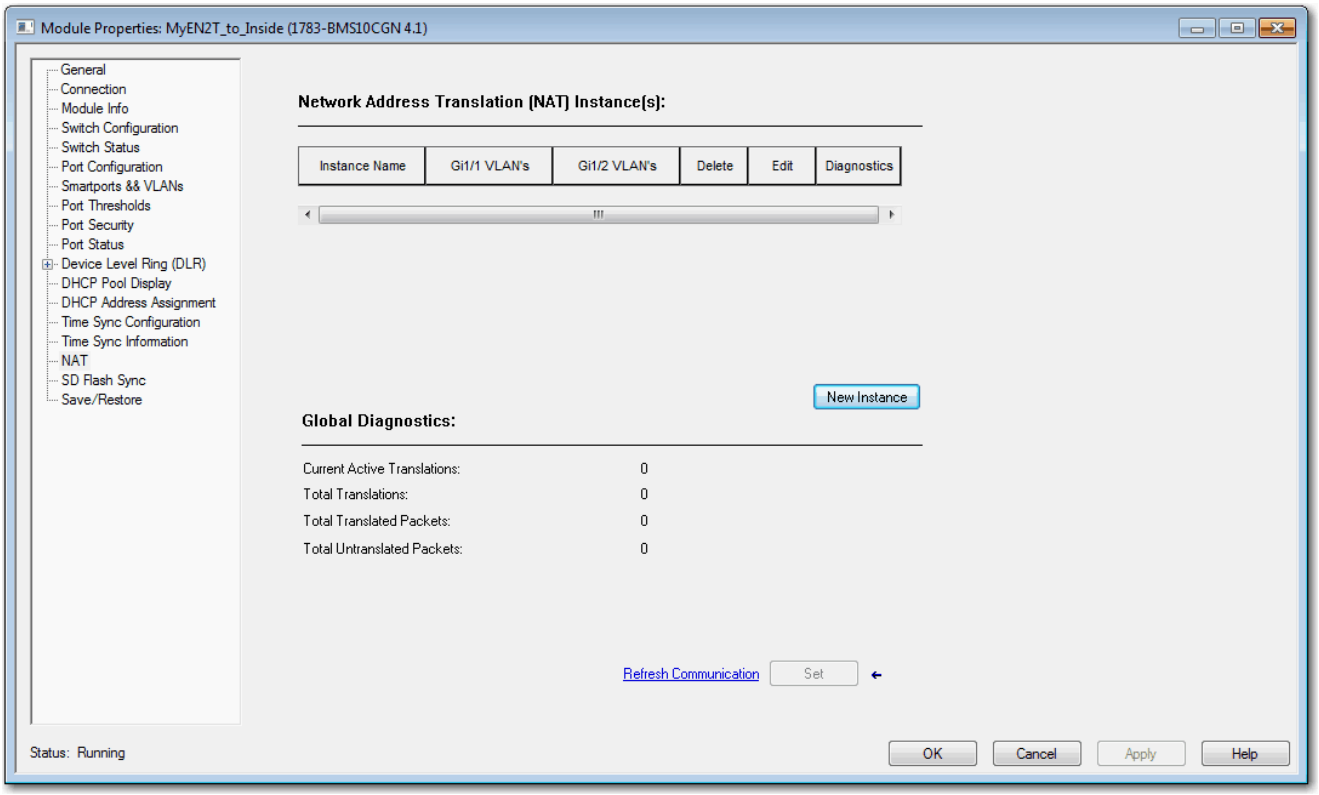


Table 84 - NAT Fields

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 306.
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 17 on page 169.
- Create NAT Instances for Traffic Routed through a Layer 2 Switch

For an example of this application, see Figure 18 on page 170.

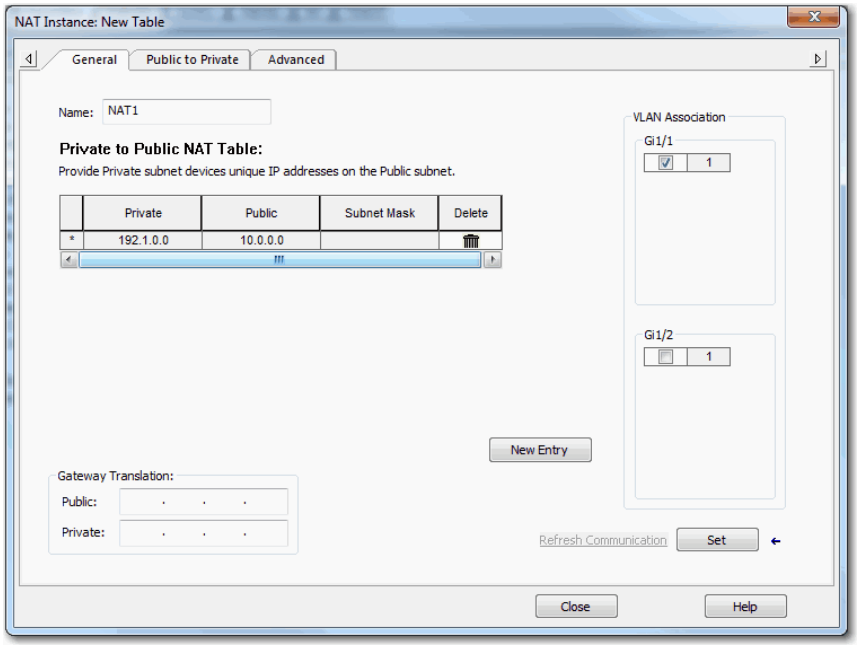
IMPORTANT Configure all Smartport roles and VLANs before creating NAT instances.

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

1. From the NAT view, click New Instance to display the General tab.



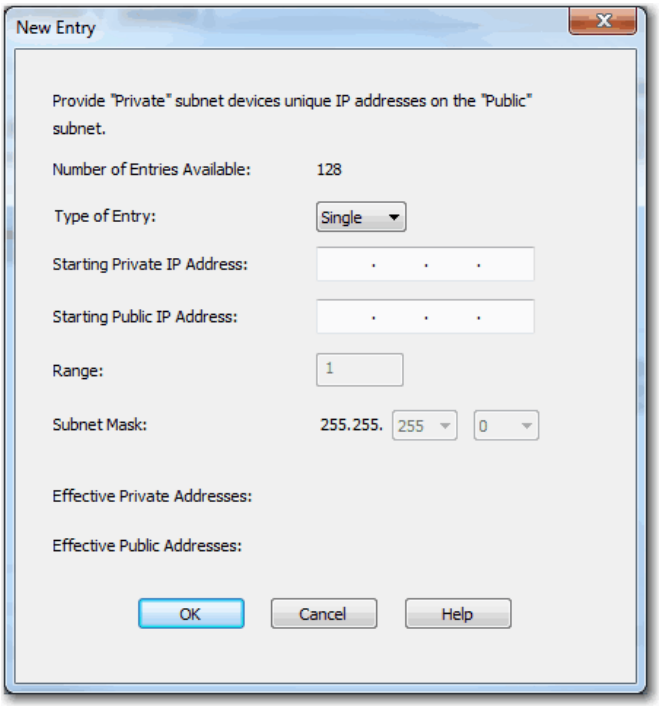
2. In the Name field, type a unique name to identify the instance.

   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 173.

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 85.
   - To translate a range of addresses for devices on the private subnet that communicates on the public subnet, see Table 86.
   - To translate all addresses in the private subnet or a portion of the private subnet, see Table 87.

Table 85 - 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 86 - 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.

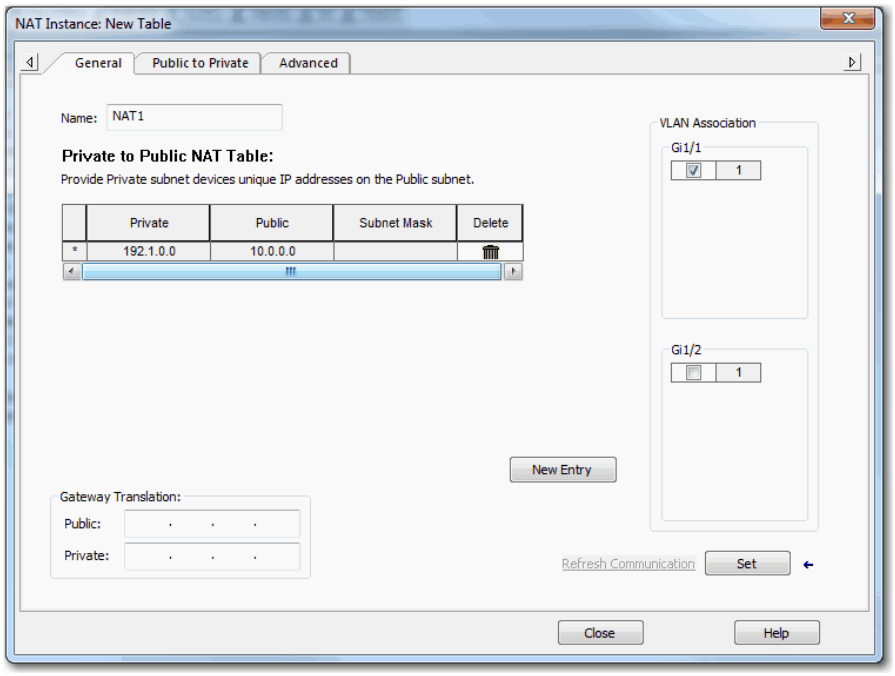
Table 87 - Subnet Translation

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 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
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 end in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	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:** 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. 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 184.
9. Click Set.

Create NAT Instances for Traffic Routed through a Layer 2 Switch

1. From the NAT view, click New Instance to display the General tab.



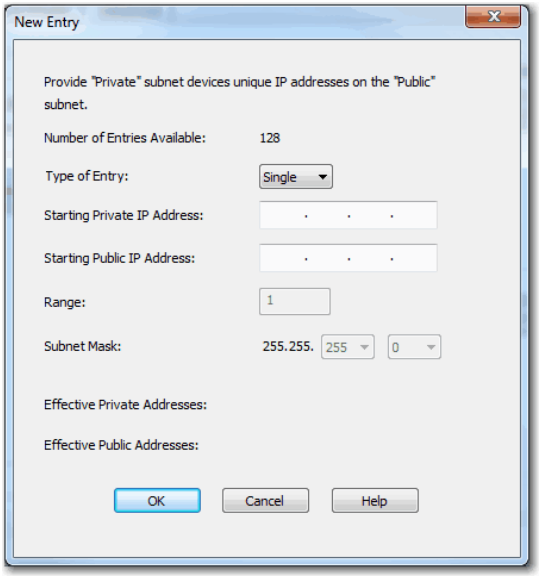
2. In the Name field, type a unique name to identify the instance.

   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 173.

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 88.
   - To translate a range of addresses for devices on the private subnet that communicates on the public subnet, see Table 89
   - To translate all addresses in the private subnet or a portion of the private subnet, see Table 90.

Table 88 - 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 89 - 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.

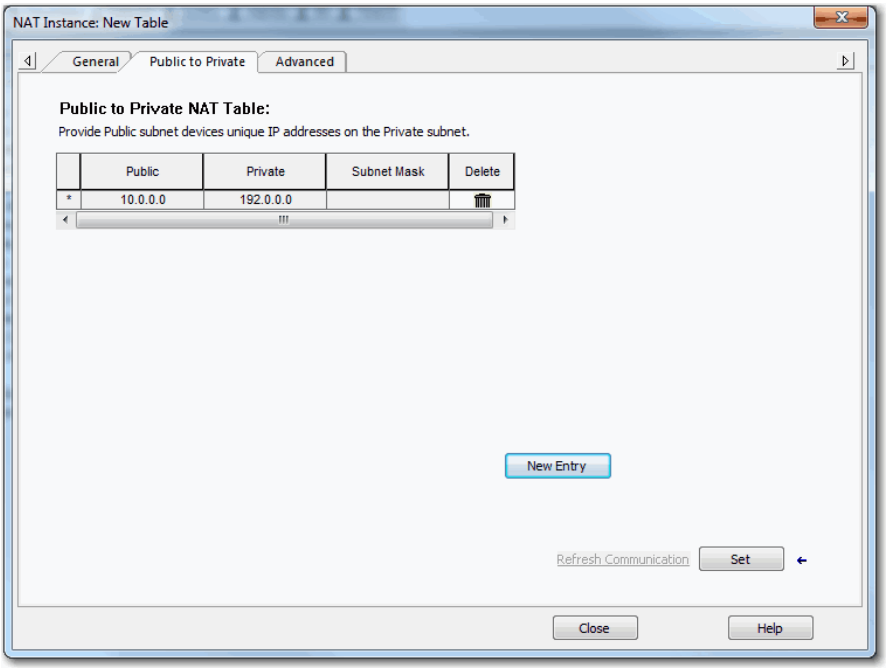
Table 90 - Subnet Translation

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 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

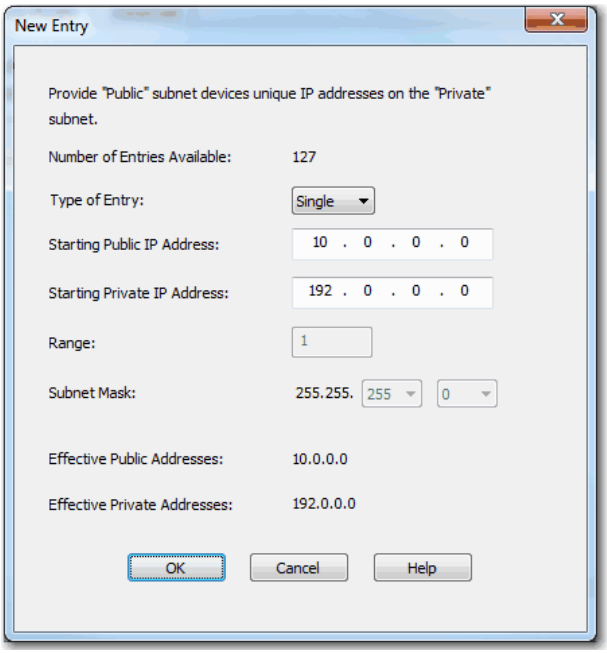
Table 90 - Subnet Translation (Continued)

Field	Description	
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 end in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	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:** 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 91.
   - To translate a range of addresses for devices on the public subnet that communicates on the private subnet, see Table 92.
   - To translate a range of addresses for devices on the public subnet that communicates on the private subnet, seeTable 93.

Table 91 - 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 92 - 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 93 - Subnet Translation

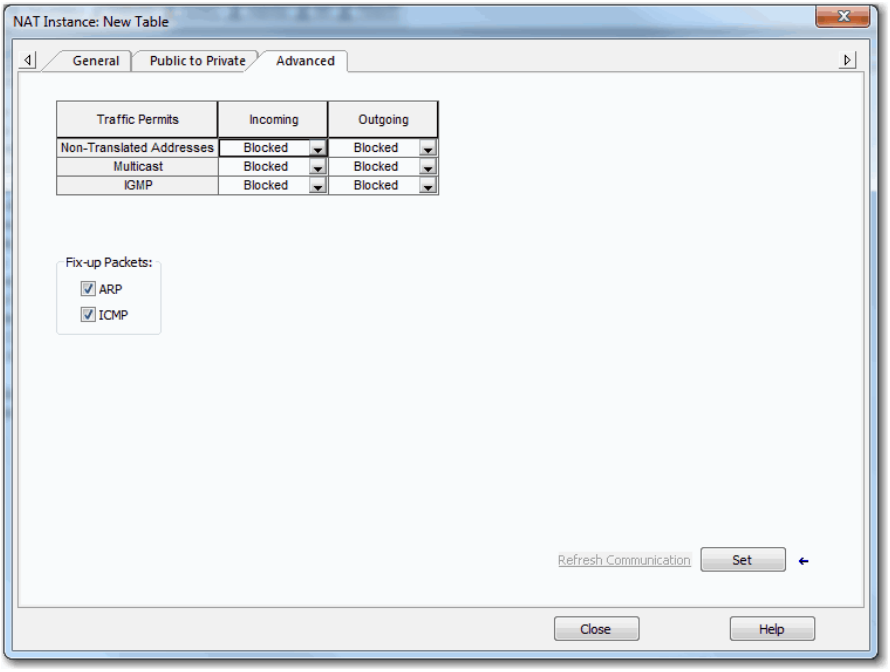
Field	Description	
Type of Entry	Choose Subnet.	
Starting Public IP Address	Type the existing starting address for a device on the public subnet. This address must correspond to the size of the subnet mask to translate.	
	Subnet Mask	Starting Public Subnet Address
	255.255.0.0	The last two octets must 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 end in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	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:** 10.200.1.16
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 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
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 184.
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.

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.

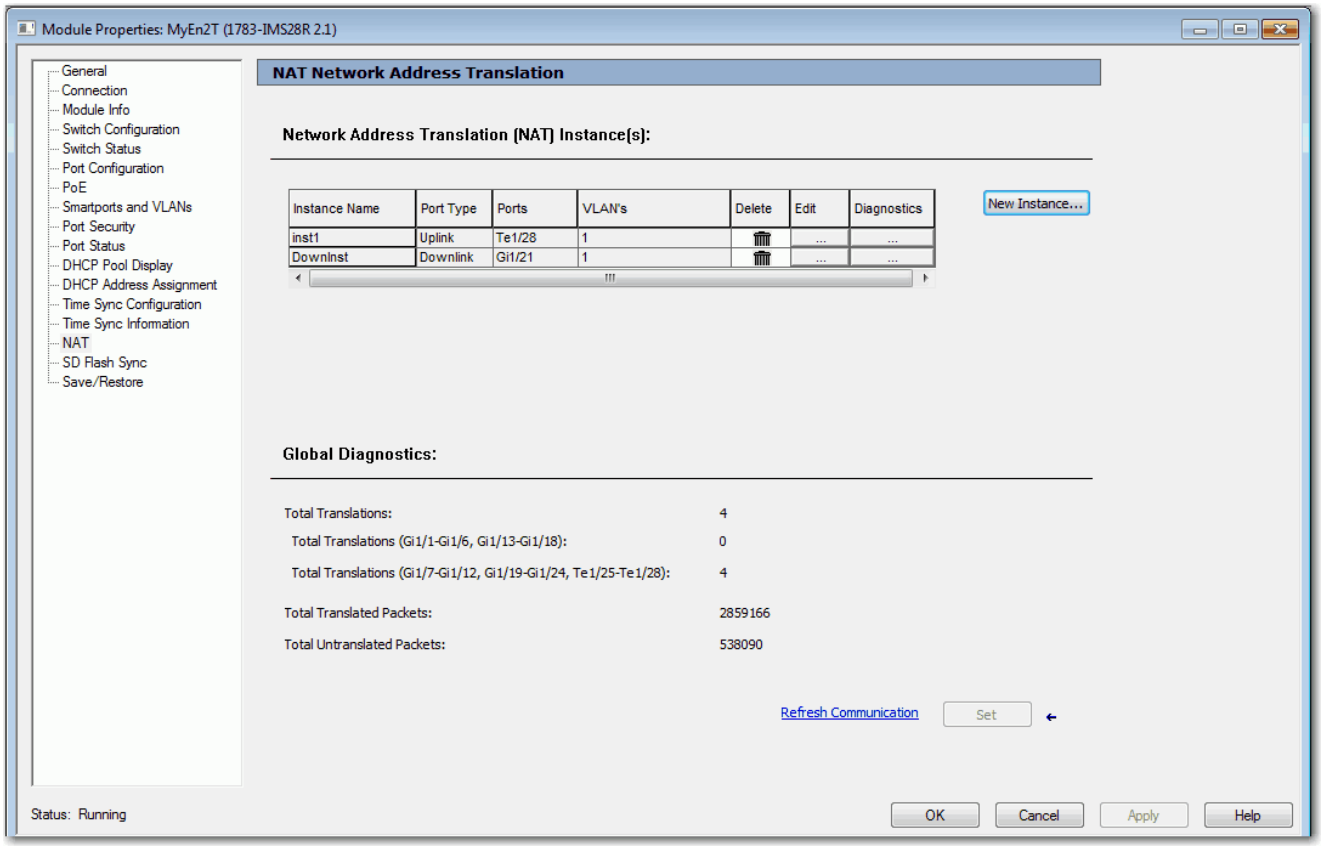


Table 94 - NAT Fields

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 306.
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 through all NAT instances without being translated.

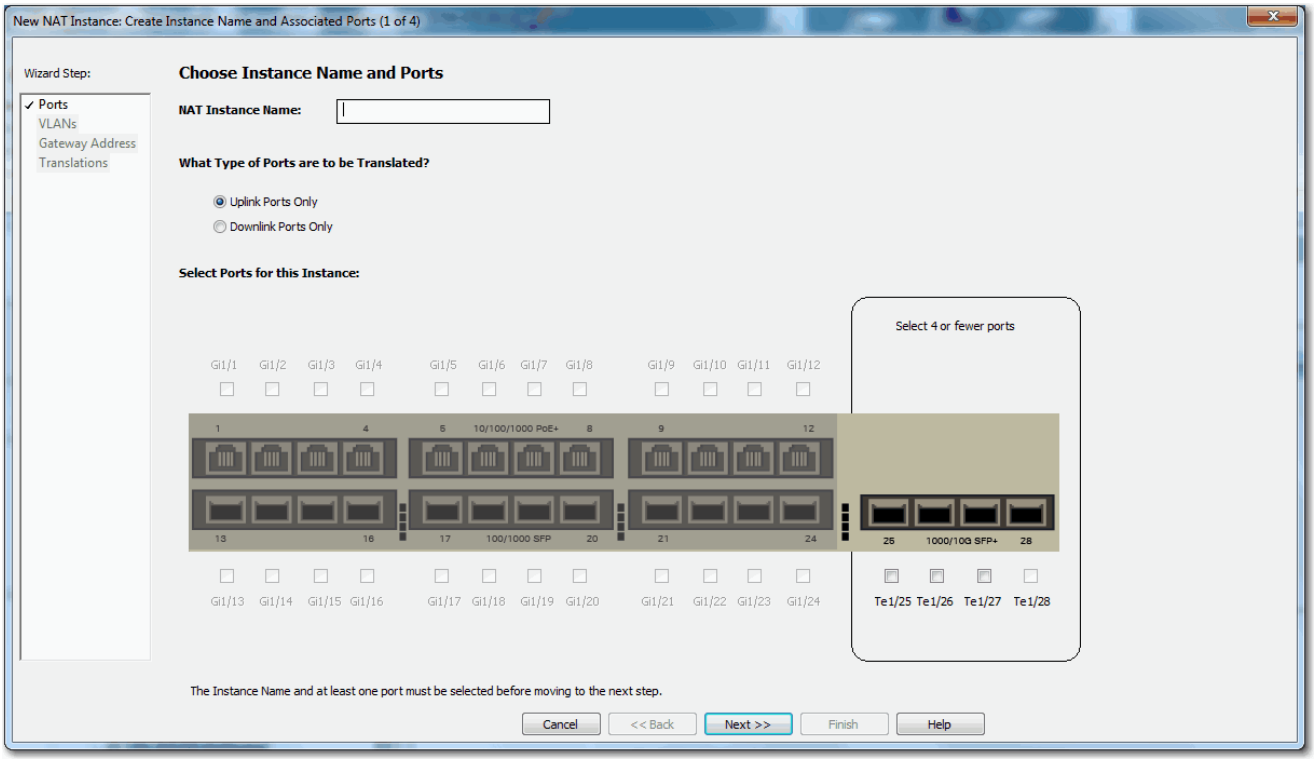
To create a NAT instance, follow these steps.

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.

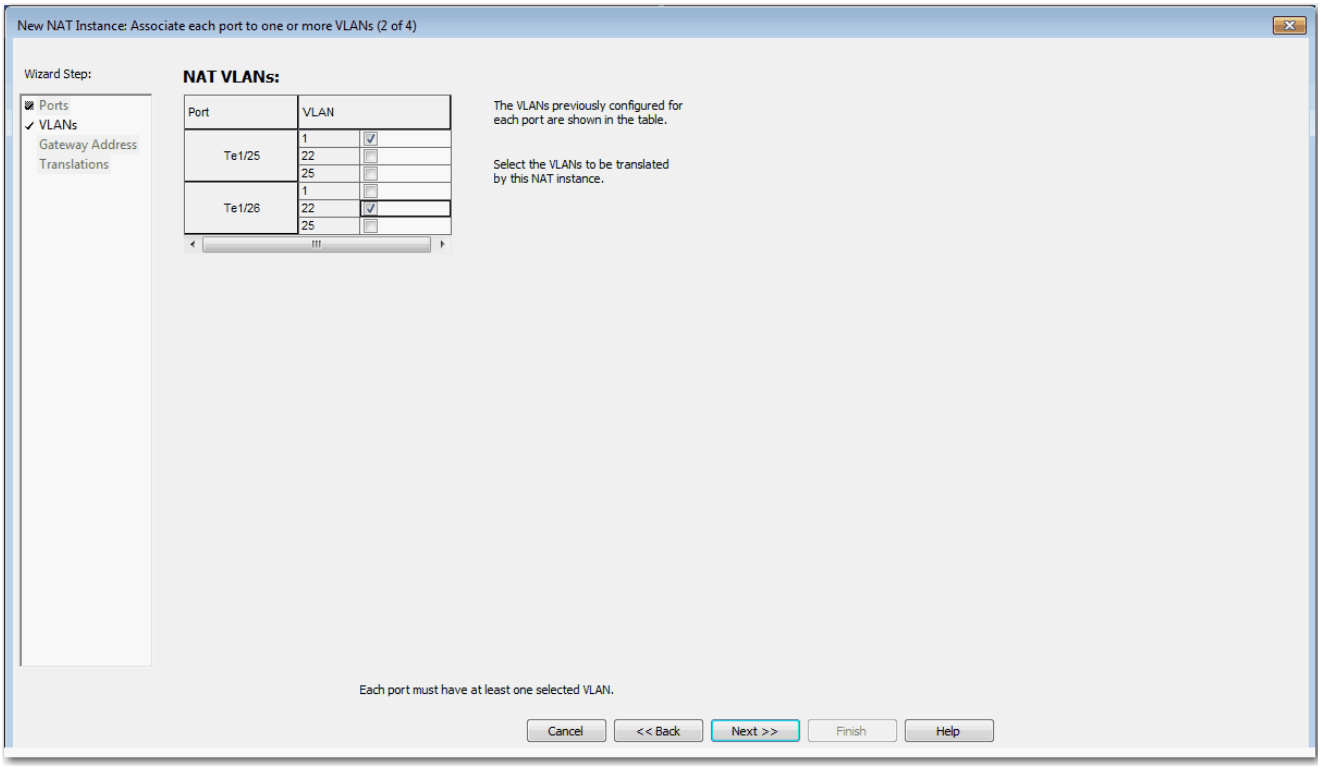


2. Configure the ports to assign to the instance.
   a. In the NAT Instance Name field, type a unique name to identify the instance.
   b. Click the type of ports to assign to the NAT instance:
   - Uplink Ports Only (Te1/25...Te1/28)
   - (Default) Downlink Ports Only (Gi1/1...Gi1/24)

   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.



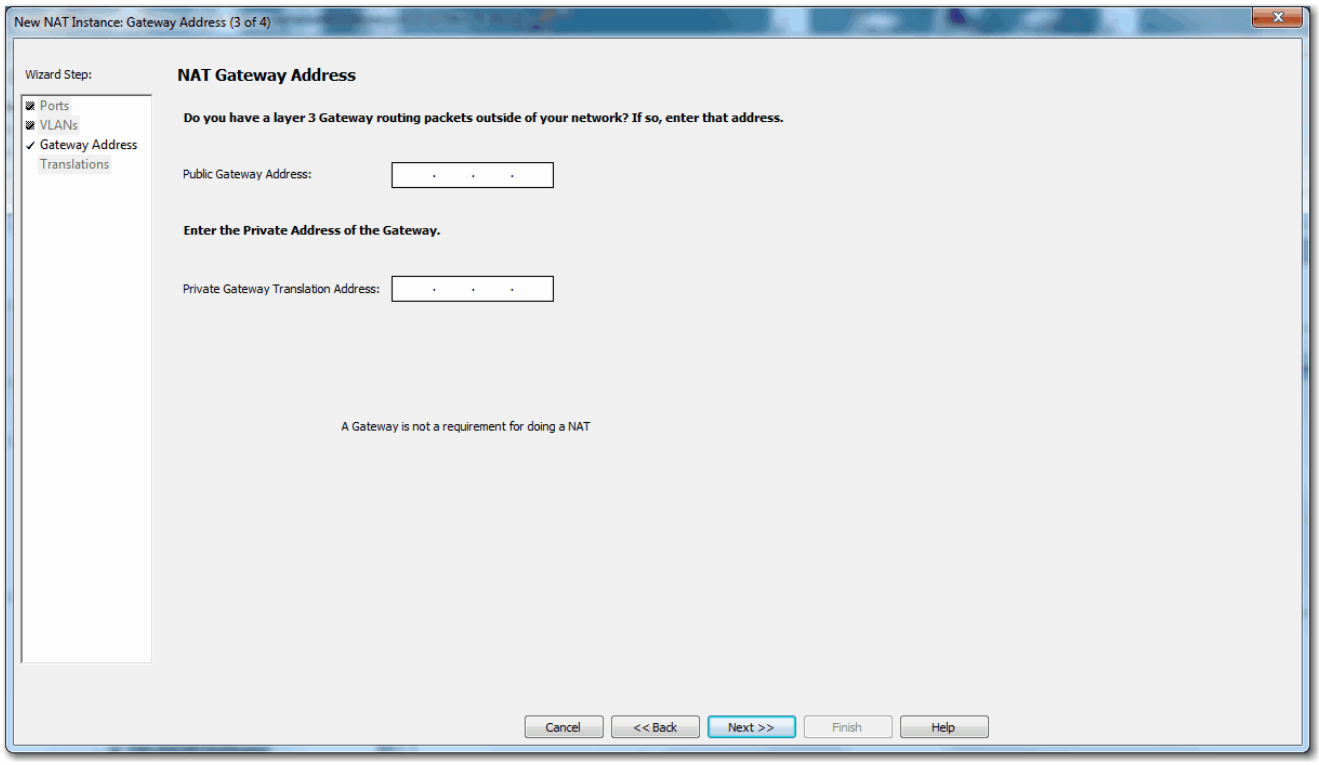
4. For each port, select one or more VLANs to assign to the NAT instance.

   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.

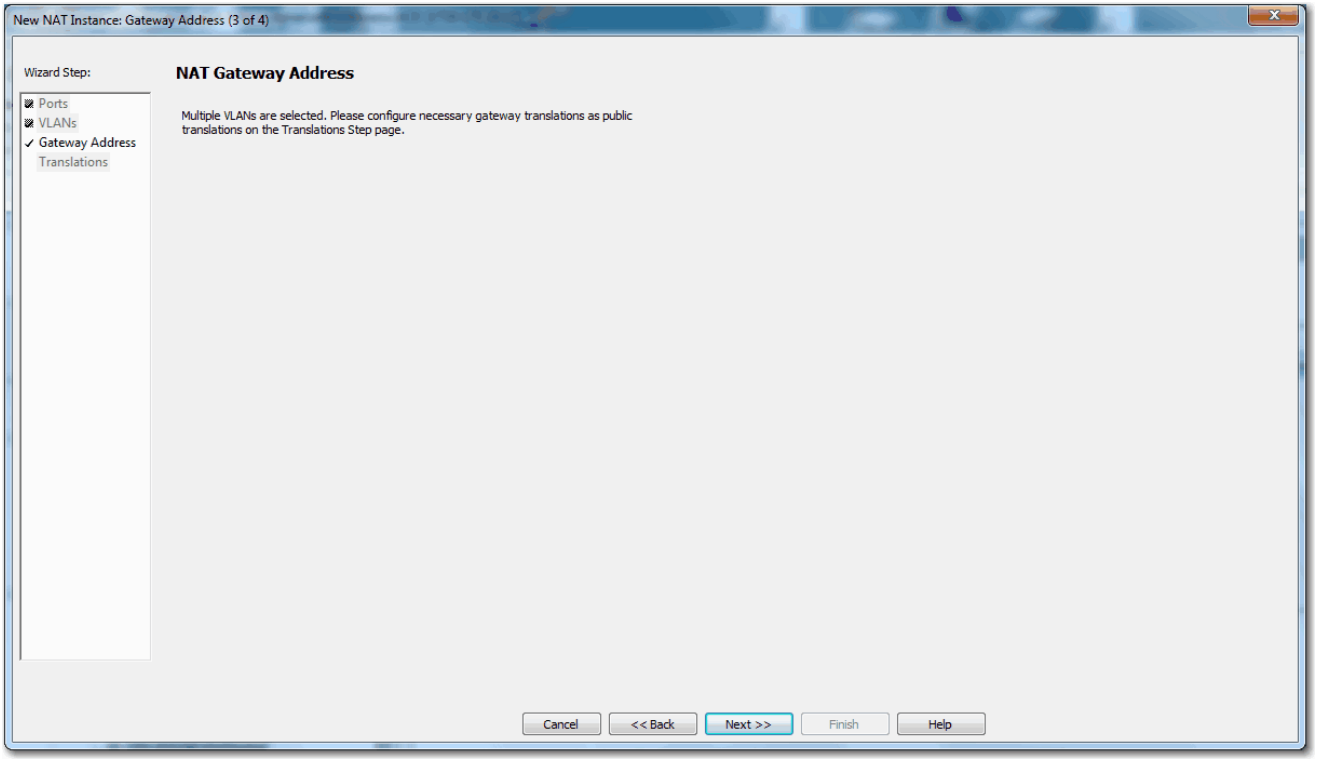
5. Click Next to display the Gateway Address view.

   If you assigned only one VLAN to the NAT instance and use a Layer 3 gateway, specify the following addresses:

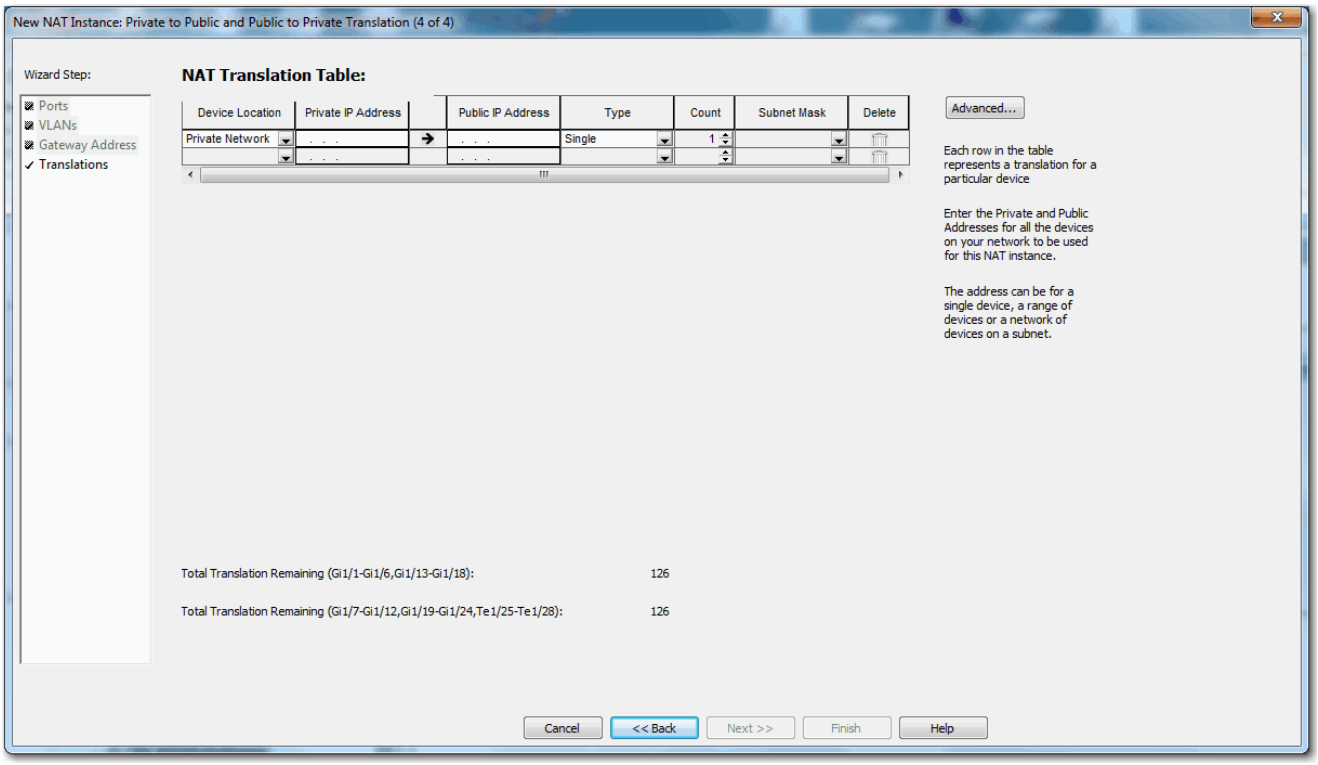
   - Public Gateway Address—Type the default gateway address of the Layer 3 switch or router for this subnet.
   - Private Gateway Translation Address—Type a unique IP address to represent the Layer 3 switch or router on the private network.



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.

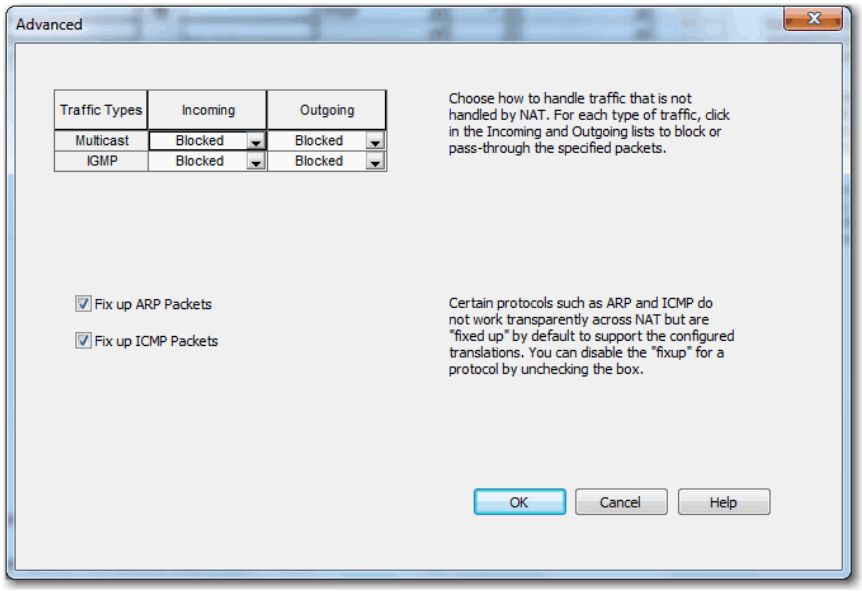
Field	Description
Device Location	Choose the type of network on which the device resides: • Private Network • Public Network
Private IP Address	Specify a private IP address. Single translations: • If the device is on a private network, type the existing address for the device. • If the device is on a 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 95 on page 200.
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 95 on page 200.
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.

Field	Description
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 95 - 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 end 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 end 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.



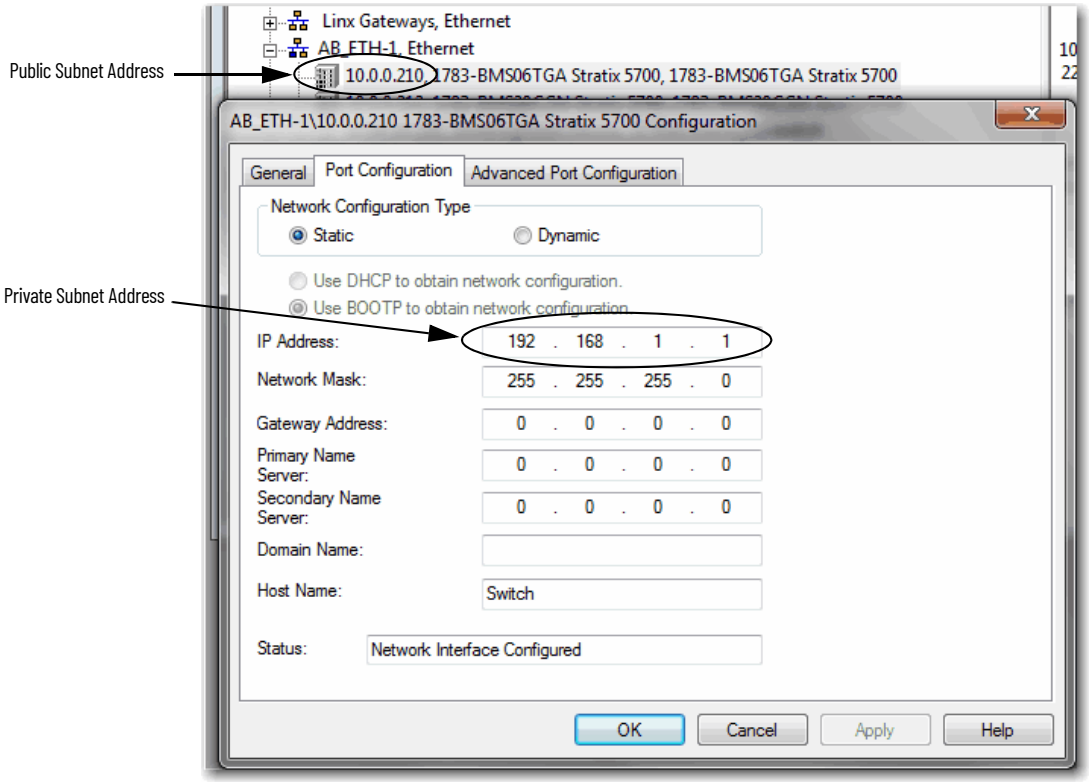
9. In the Incoming and Outgoing fields for each type of traffic, choose one of these options:
   - Pass-Through—Permit unsupported packets to pass across the NAT boundary.
   - Blocked—Drop unsupported packets.
10. To disable protocol fixups for ARP, clear the Fix up ARP checkbox.
11. To disable protocol 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 Linx-based Software

The Ethernet driver in Linx-based 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 Linx-based software. However, its private subnet address appears in the configuration properties of the device.

Figure 20 - Public and Private Subnet Addresses in Linx-based Software



Network Time Protocol (NTP)

Network Time Protocol (NTP), defined in RFC 1305, is the traditional method of clock synchronization across packet-based networks. NTP uses a two-way time transfer mechanism between a master and a slave.

NTP can synchronize devices in a tightly controlled network. The switch can use NTP as a time source for PTP, which lets you correlate data that is generated in the PTP network with data in the enterprise data center running NTP. For information about NTP to PTP time conversion configuration, see page 96.

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.

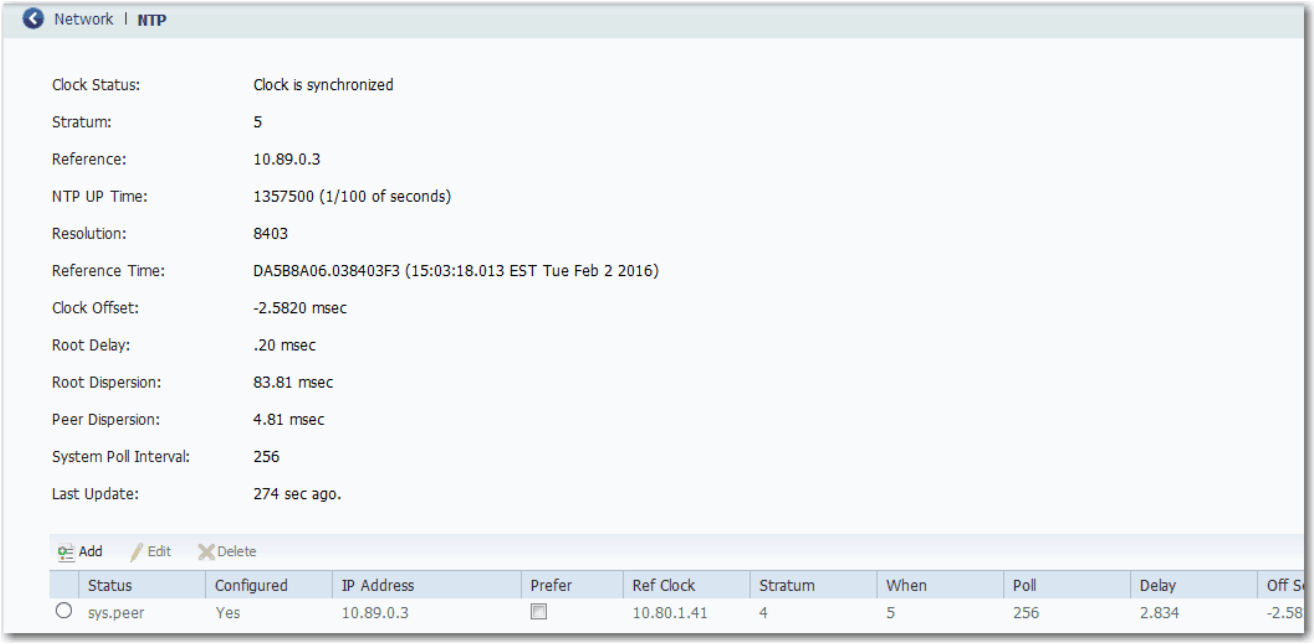


Table 96 - NTP Fields

Field	Description
Clock Status	Displays the 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.
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.

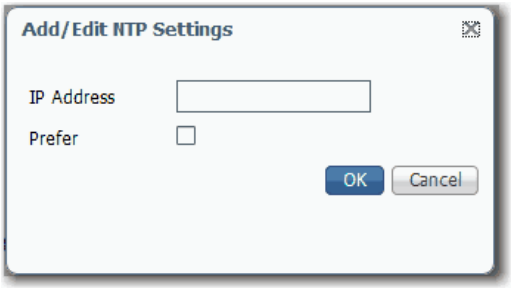
Table 96 - NTP Fields (Continued)

Field	Description
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.

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.

Configure NTP via the Logix Designer Application

In the navigation pane, click NTP.

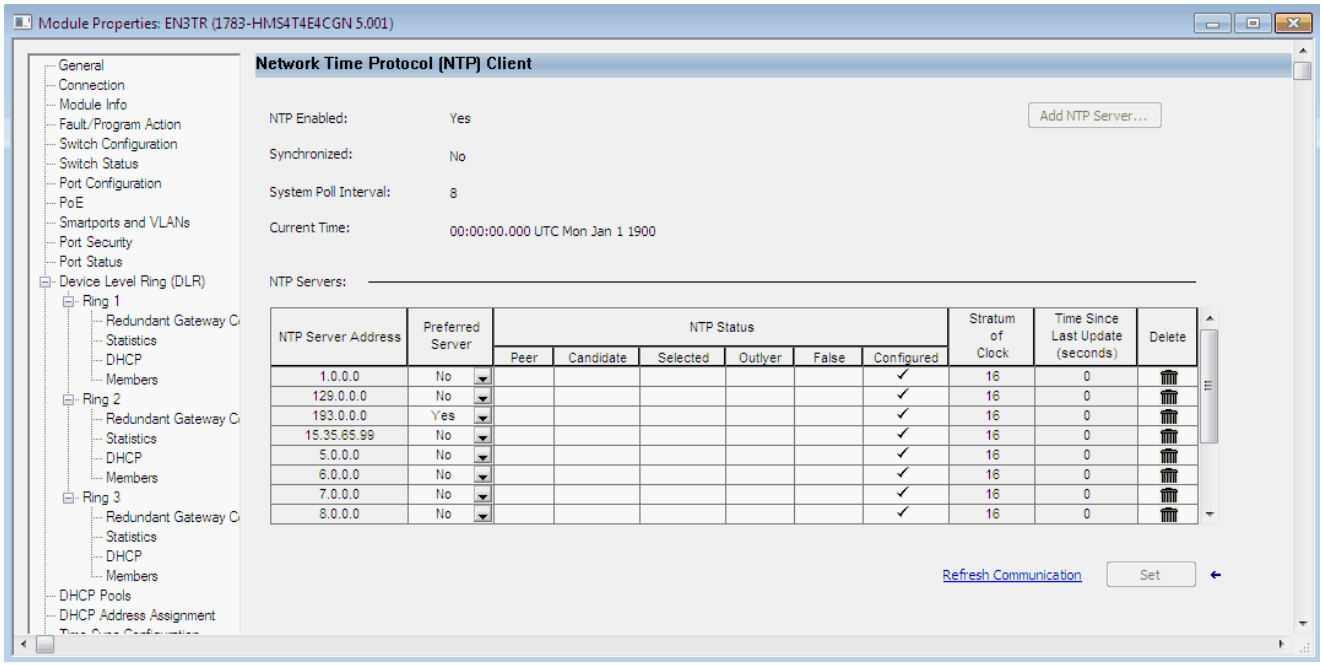


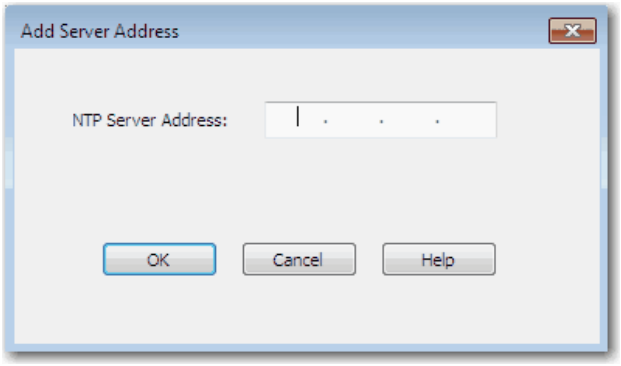
Table 97 - Network Time Protocol (NTP) Client Fields

Field	Description
NTP Enabled	Displays whether NTP is enabled or disabled.
Synchronized	Displays the status of NTP clock synchronization: • Synchronized • Unsynchronized
System Poll Interval	Displays the poll interval of the peer.
Current Time	Displays the reference time stamp.
NTP Server 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.
Preferred Server	Choose whether the peer or server is the preferred one that provides synchronization.
NTP Status	Displays the status of the NTP peer association.
Stratum of Clock	Displays the stratum of the peer.
Time Since Last Update (seconds)	Displays the time the system last updated its NTP information.

You can add, edit, and delete NTP associations on the Network Time Protocol (NTP) Client view. You can add multiple NTP servers.

To add an association, follow these steps.

1. Click Add NTP Server.



2. In the NTP Server Address field, specify one of the following and click OK:
   - 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.

   The IP address you specify appears in the NTP Servers table.
3. To make the peer or server the preferred one that provides synchronization, choose Yes in the Preferred Server column.

Open Shortest Path First (OSPF) Routing Protocol

OSPF is available on the following switches:

- Stratix 5400 with Layer 3 firmware
- Stratix 5410 with Layer 3 firmware
- Stratix 8300 base units

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 also can be exported into RIP.
- Plain text and message digest algorithm 5 (MD5) authentication among routers that are neighbors 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 that all routers have a coordinated configuration.

Configure OSPF via Device Manager

From the Configure menu, choose OSPF.

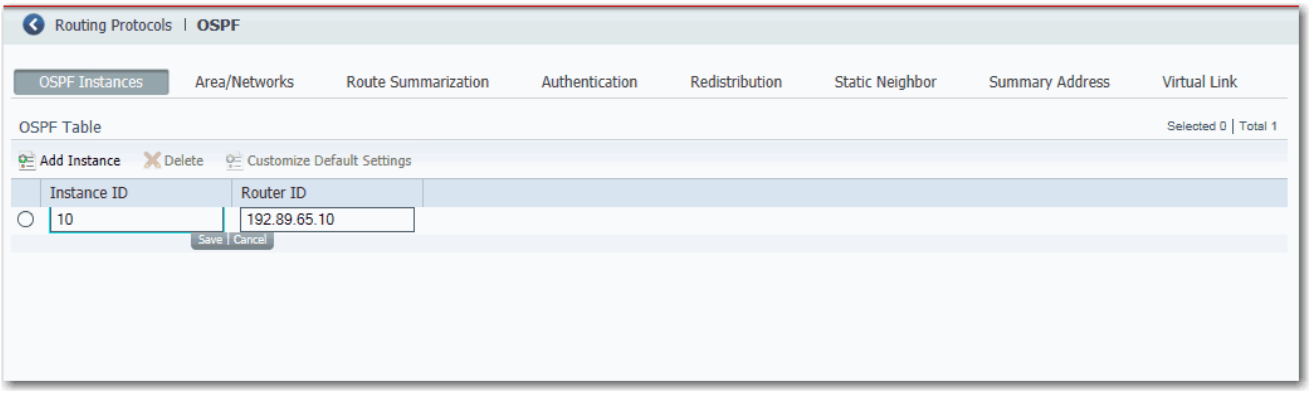


Table 98 - OSPF Fields

Field	Description
OSPF Instances—Add OSPF instances to the OSPF table. To customize the default settings for an instance, see page 210.	
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
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. Route 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 threat actors to subvert routing information.	

Table 98 - OSPF Fields (Continued)

Field	Description
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—Redistribute 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 98 - 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 non-backbone 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 must be greater than zero. LSAs in the update packet are aged by this increment 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.

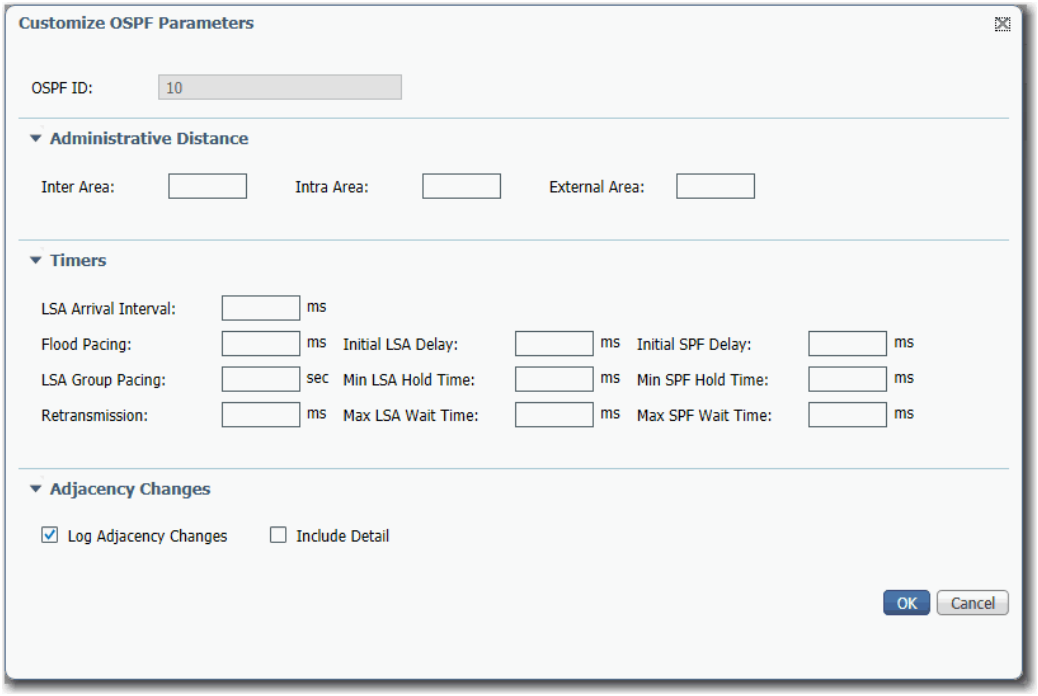


Table 99 - Customize OSPF Parameters

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 that arrives 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
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 pace timers are suitable for most OSPF deployments. Do not change the packet pace 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 the 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, check summed, 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

Table 99 - Customize OSPF Parameters (Continued)

Field	Description
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

Parallel Redundancy Protocol (PRP)

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

A PRP network includes the following components.

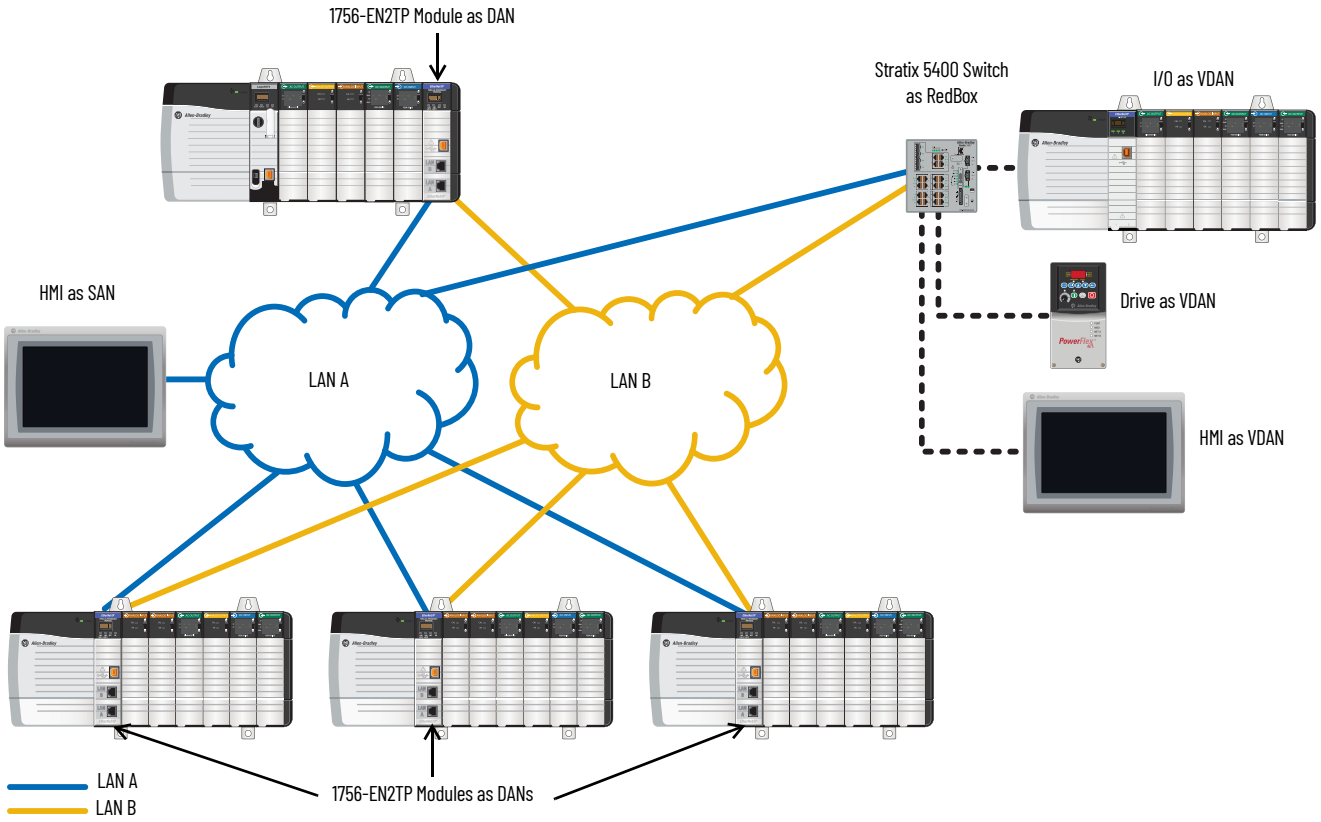
Component	Description
LAN A and LAN B	Redundant, active Ethernet networks that operate in parallel.
Double attached node (DAN)	An end device with PRP technology that connects to both LAN A and LAN B.
Single attached node (SAN)	An end device without PRP technology that connects to either LAN A or LAN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

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

You can configure either a Stratix 5400 or 5410 switch as a RedBox. Figure 21 illustrates the Stratix 5400 switch as RedBox.

IMPORTANT Before connecting the cables between devices in a PRP system, complete the configuration of the devices.

Figure 21 - PRP Topology with Stratix 5400 Switch as RedBox



RedBox PRP Channel Groups

For RedBox functionality, Stratix 5400 and 5410 switches have designated ports for PRP channel groups. A PRP channel group is a logical interface that aggregates two Gigabit Ethernet physical ports into a single link. In the channel group, the lower numbered Gigabit Ethernet member port is the primary port that connects to LAN A. The higher numbered port is the secondary port that connects to LAN B. The PRP channel remains up as long as at least one of these member ports remains up and sends traffic. When both member ports are down, the channel is down.

The following table shows the available PRP channel group ports for switches that are configured as a RedBox.

Switch	Channel Group	Member Ports
Stratix 5400	1	Gi1/1 and Gi1/2
	2(1)	Gi1/3 and Gi1/4
Stratix 5410	1	Gi1/17 and Gi1/18
	2	Gi1/19 and Gi1/20

(1) Channel 2 is only available in an HSR feature mode.

Traffic and Supervisory Frames

Traffic that egresses the RedBox PRP channel group can be destined to either SANs connected only on either LAN A or LAN B or to DANs. To avoid duplication of packets for SANs, the switch learns source MAC IDs from supervisory frames for DAN entries and non-PRP frames for SAN entries. Learned MAC IDs are maintained in the Node table. When forwarding packets out of the PRP channel to SAN MAC IDs, the switch looks up the entry and determines which LAN to send to rather than duplicating the packet.

A RedBox with VDANs sends supervisory frames on behalf of those VDANs. For traffic entering on all other ports and exiting PRP channel ports, the switch learns source MAC IDs, adds them to the VDAN table, and starts sending supervisory frames for these addresses. Learned VDAN entries are subject to aging.

All Allen-Bradley products with PRP technology support supervisory frames. If your PRP system includes a device that does not support supervisory frames, the switch identifies the device as a DAN, even if it is a SAN or VDAN. In this scenario, we recommend that you manually add the device to the Node or VDAN table, so the switch can correctly identify the device as a DAN, SAN, or VDAN and manage traffic appropriately.

Node and VDAN Limitations

When you configure nodes and VDANs, be aware of the following limitations:

- The switch supports a maximum of 512 SAN and DAN entries in the Node table.
- Hash collisions can limit the number of MAC IDs. If the Node table is out of resources for learning a MAC ID from a node, the switch treats that node as a DAN by default.
- After restarting and before any MAC ID is learned, the switch temporarily treats an unlearned node as a DAN and duplicates the egress packets until an ingress packet or supervisory frame is received from the node to populate an entry into the Node table.
- The switch supports a maximum of 512 VDAN entries in the VDAN table. If the VDAN table is full, the switch cannot send supervisory frames for new VDANs.

Configuration Considerations

- Device IP addresses
- Frame sizes
- Spanning Tree Protocol (STP)
- Multicast traffic and IGMP querier
- CIP Sync time synchronization (Precision Time Protocol)

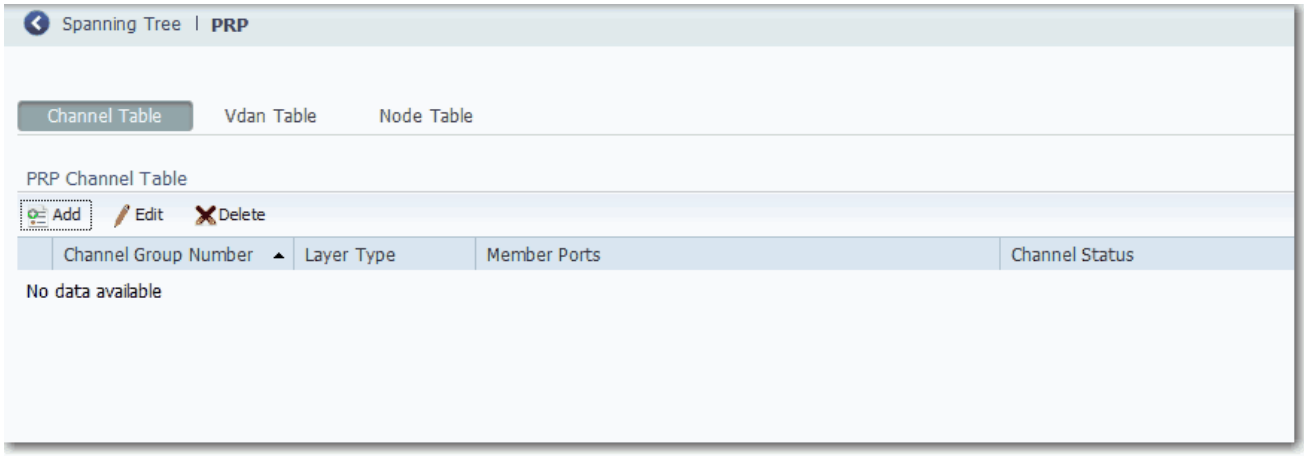
For requirements related to these features, see the EtherNet/IP Parallel Redundancy Protocol Application Technique, publication ENET-AT006.

Configure a RedBox via Device Manager

IMPORTANT You are only required to add nodes to the VDAN or Node table if you are using a PRP device that does not support supervisory frames. All Allen-Bradley products with PRP technology support supervisory frames. For more information, see Traffic and Supervisory Frames on page 213.

To configure a Stratix 5400 or 5410 switch as a RedBox, follow these steps.

1. From the Configure menu, choose PRP.



2. Add PRP channel groups.
   a. Click the Channel Table tab.
   b. Click Add.
   c. Complete the fields that are described in Table 100 and click OK.

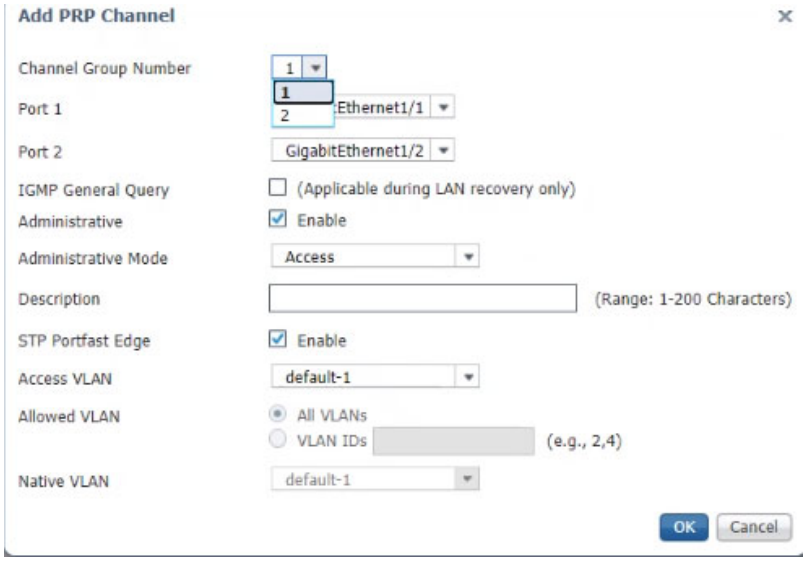


Table 100 - Add PRP Channel Fields

Field	Description
Channel Group Number	Choose a channel group number: • Stratix 5400 and Stratix 5410 switches provide 2 channel groups[1]
Port 1	Choose a port to be a member of the channel group.
Port 2	Choose a port to be a member of the channel group.

Table 100 - Add PRP Channel Fields (Continued)

Field	Description
IGMP General Query	(Add/Edit PRP Channel window only). Check IGMP General Query to prompt the PRP RedBox to send general query packets for PRP LAN recovery. If a PRP LAN is down, a querier update is triggered for faster multicast reconvergence. General queries collect multicast group membership information. To enable IGMP General Query, you must first check IGMP Querier on the IGMP Snooping page.
Administrative	Check Enable to activate the switch ports. By default, the ports are enabled. Clear the Enable checkbox to disable the switch ports.
Administrative Mode	Choose one of the following modes for PRP channel group: • Access (default)—The channel group carries traffic for a single VLAN. • Trunk—The channel group carries traffic for multiple VLANs. • Routed—Layer 3
Description	Type a description for the PRP channel. The description can contain a maximum of 200 characters.
STP Portfast Edge	Improves the spanning-tree convergence time on PRP LAN-A and LAN-B. Enabling STP Portfast Edge is optional on the PRP channel interface but highly recommended.
Access VLAN	(Access mode only). Choose the VLAN to which the PRP channel group belongs. 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 or use a dash for ranges, such as 1,5,7-12,17.
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—Manually assign a static IP address. Type the IP address and the subnet mask. • DHCP—Allow a DHCP server to assign an IP address automatically.

(1) Channel 2 is only available in an HSR feature mode.

After you have added a PRP channel group, the fields in Table 101 display.

Table 101 - PRP Channel Table Fields

Field	Description
Channel Group Number	See the description in Table 100.
Layer Type	(Not editable). Displays Layer2 or Layer3.
Member Ports	Displays the ports in the PRP channel. Member ports are dependent on the switch: • Stratix 5400, Port 1, Gi1/1 and Gi1/2 • Stratix 5410, Port 1, Gi1/17 and Gi1/18. Port 2, Gi1/19 and Gi1/20
Channel Status	(Not editable). Displays the status of the group: • InUse • Not-InUse • Not-InUse (Admin Down)

You can edit or delete a PRP channel group.

- To edit a PRP channel group, click the radio button next to the Channel Group Number and click Edit. Complete the fields in Table 100 and click OK.
- To delete a PRP channel group, click the radio button next to the Channel Group Number and click Delete.

3. To add a VDAN to the VDAN table, do the following.
   a. Click the VDAN Table tab
   b. Complete the fields in Table 102 and click OK.

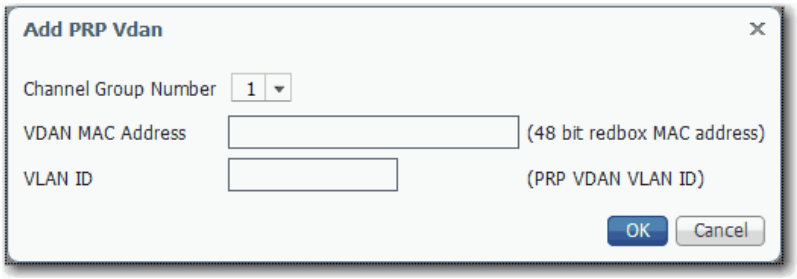


Table 102 - Add PRP VDAN Fields

Field	Description
Channel Group Number	Choose a channel group number: • Stratix 5400 switches provide 1 channel group • Stratix 5410 switches provide 2 channel groups
VDAN MAC Address	Type the MAC ID of the VDAN.
VLAN ID	(Access mode only). Choose the VLAN associated with the PRP channel group. The default value is **default-1**.

You can delete a single entry, or delete all entries, from the VDAN table.

- To delete a VDAN, click the radio button next to the Channel Group Number and click Delete.
- To delete all information from the VDAN table, click Clear All.

4. To add a DAN or SAN to the Node table, do the following.
   a. Click the Node Table tab.
   b. Click Add, complete the fields as described in Table 103 and click OK.

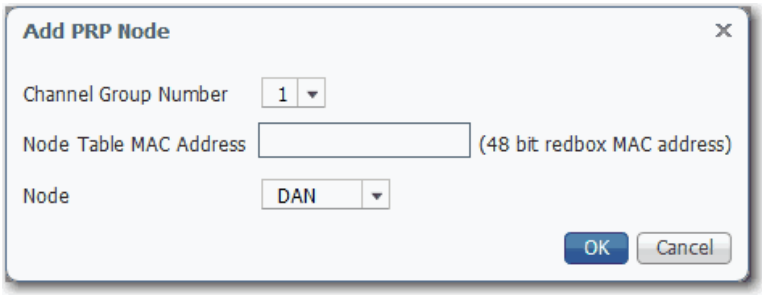


Table 103 - Add PRP Node Fields

Field	Description
Channel Group Number	Choose a channel group number: • Stratix 5400 switches provide 1 channel group • Stratix 5410 switches provide 2 channel groups
Node Table MAC Address	Type the MAC ID of the DAN or SAN.
Node	Choose the type of PRP node: • DAN (default)—Double attached node • SAN-A—Single attached node on LAN A • SAN-B—Single attached node on LAN B

You can delete a single entry, or delete all entries, from the Node table.

- To delete a Node, click the radio button next to the Channel Group Number and click Delete.
- To delete all information from the Node table, click Clear All.

Troubleshoot PRP via Device Manager

If you encounter problems accessing the Device Manager, web browsing, or using remote desktop on a switch, verify the MTU size for frames. The jumbo MTU size must be set to 1506 for all switches in LAN A and LAN B.

If you cannot access Device Manager, use one of following methods to access the switch:

- Use the CLI as described on page 65.
- Use a computer-to-switch connection with a straight-through or crossover Category 5 Ethernet cable.

For more diagnostic methods, see the EtherNet/IP Parallel Redundancy Protocol Application Technique, publication ENET-AT006.

View PRP configuration via the Logix Designer Application

Configuration of a Stratix 5400 or 5410 switch as a RedBox is accomplished by using the Device Manager or CLI. Use the Logix Designer application to view the active PRP settings.

In the navigation pane, click Parallel Redundancy Protocol (PRP).

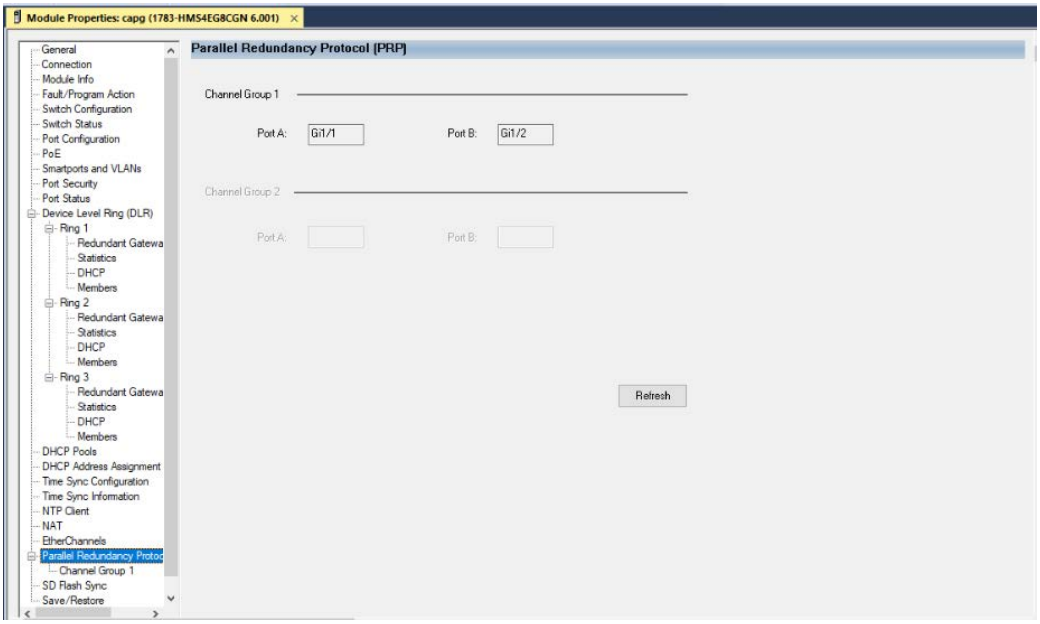


Table 104 - Parallel Redundancy Protocol (PRP) fields

Field	Description
Channel Group Number	Channel group number: • Stratix 5400 switches provide 1 channel group • Stratix 5410 switches provide 2 channel groups
Port	Displays the ports in the PRP channel. Member ports are dependent on the switch: • Stratix 5400, Port A, Gi1/1 and Gi1/2 • Stratix 5410, Port A, Gi1/17 and Gi1/18. Port B, Gi1/19 and Gi1/20

PRP Channel Groups

The Channel Group page displays the diagnostics for active PRP ports.

- Stratix 5400 switches display one channel group
- Stratix 5410 switches display two channel groups

In the navigation pane, click Channel Group.

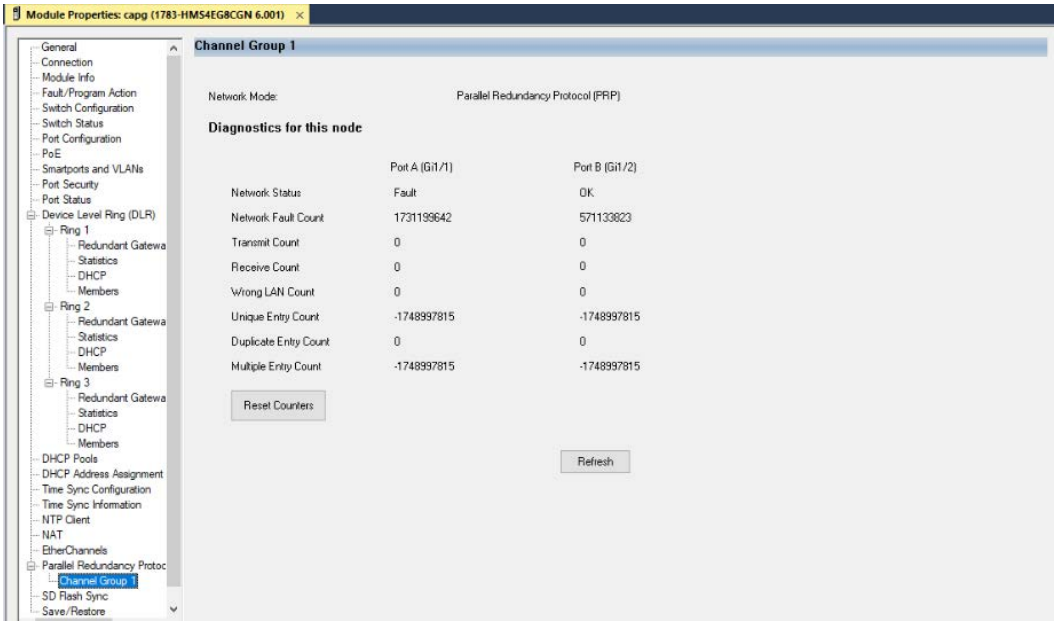


Table 105 - Channel Group Fields

Field	Description
Network Status	Displays the status of the port: • Fault (Network is inactive due to a current fault) • OK (Network is active)
Network Fault Count	Displays the number of times the Network Status parameter has shown a Fault since the last Reset Counters operation or since the last power cycle.
Transmit Count	Displays the number of PRP-tagged frames that are transmitted since the last Reset Counters operation or since the last power cycle.
Receive Count	Displays the number of PRP-tagged frames that are received since the last Reset Counters operation or since the last power cycle.
Wrong LAN Count	Displays the number of PRP-tagged frames that are received on the wrong LAN since the last Reset Counters operation or since the last power cycle.
Unique Entry Count	Displays the number of PRP-tagged frames that are received on one LAN, but not received on the other LAN, since the last Reset Counters operation, or since the last power cycle.
Duplicate Entry Count	Displays the number of PRP-tagged frames received that were already received on another LAN since the last Reset Counters operation or since the last power cycle. This count increments during normal operation, and is not an indication of a fault.
Multiple Entry Count	Displays the number of PRP-tagged frames for which multiple duplicates were received on each LAN since the last Reset Counters operation, or since the last power cycle.

Port Mirroring

Port mirroring is for advanced users with experience in the troubleshooting of 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 debug 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.

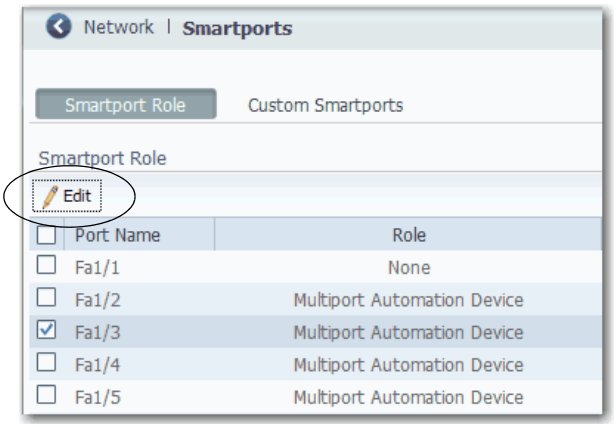
IMPORTANT	Port mirroring is a tool for the analysis of end node traffic. Because the switch can filter certain network control traffic, we recommend that you do not use port mirroring when you require an exact copy of all network traffic.

IMPORTANT	Port mirroring does not work on PRP channel ports.

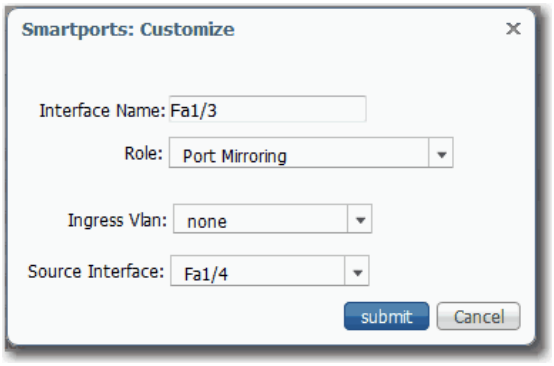
Configure Port Mirroring in Device Manager

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.

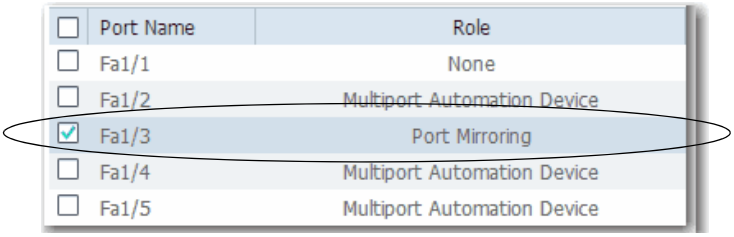


3. Complete the fields, and then click Submit.



Field	Description
Interface Name	Displays the port that 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 that 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 ID-based port security. A MAC ID is a unique address that is assigned to each Ethernet-capable device. Switches can enforce communication either dynamically or statically per MAC ID.

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 IDs of those devices. Static port security adds devices to the port security table on a per MAC ID basis. With static dynamic port security, only devices with the MAC IDs 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 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 106 - 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 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.

Enhanced Port Security

Enhanced port security provides a utility substation to prevent illegal spoofing of a tele-protection relay MAC address. An illegal MAC address needs to be identified. Once it is identified, the switch logs this event for actions to be taken.

Security Violations

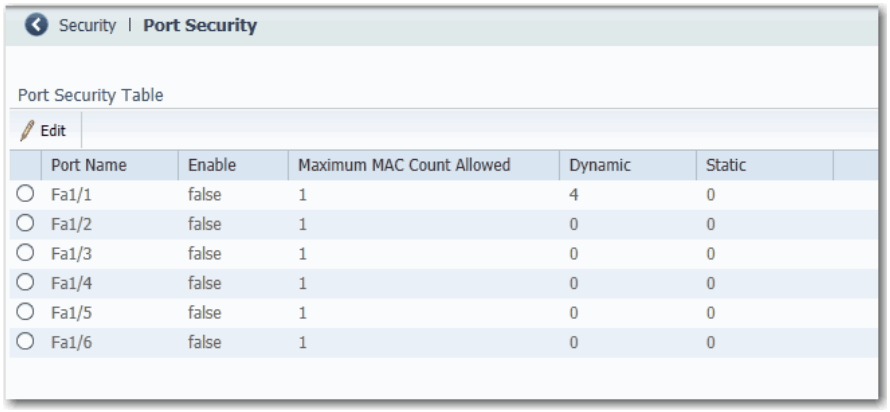
It is a security violation when one of these situations occurs:

- The maximum number of secure MAC IDs that have been configured for a port are in the address table. A station whose MAC ID 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 IDs 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:

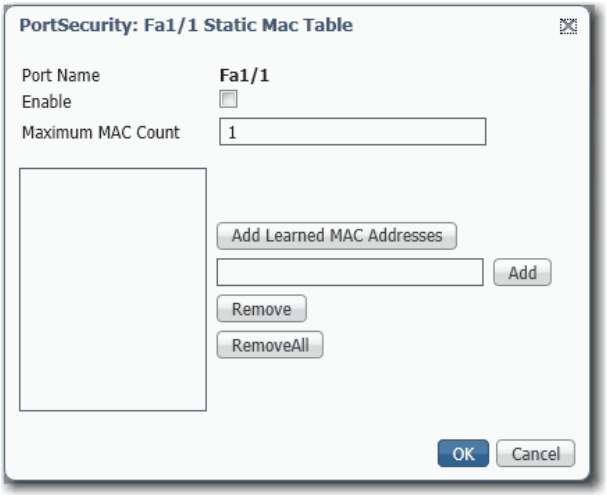
- A device, which has a MAC ID different from any identified secure MAC IDs, attempts to access the switch port.
- The number of MAC IDs on the port exceeds the maximum number that is supported on the port.

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 ID configuration by selecting Add Learned MAC Addresses on the Static MAC Address Table.
- The ability to add and remove manually MAC IDs on a per port basis.

To change the static MAC IDs 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 IDs as follows:
   - To add the existing MAC IDs of devices that are currently connected to a port, click Add Learned MAC Addresses.
   - To add a specific MAC ID to the table, type a MAC ID in the format fields and click Add.
   - To remove a MAC ID from the table, select the MAC ID and click Remove.
   - To clear the 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 224.

Figure 22 - Port Security

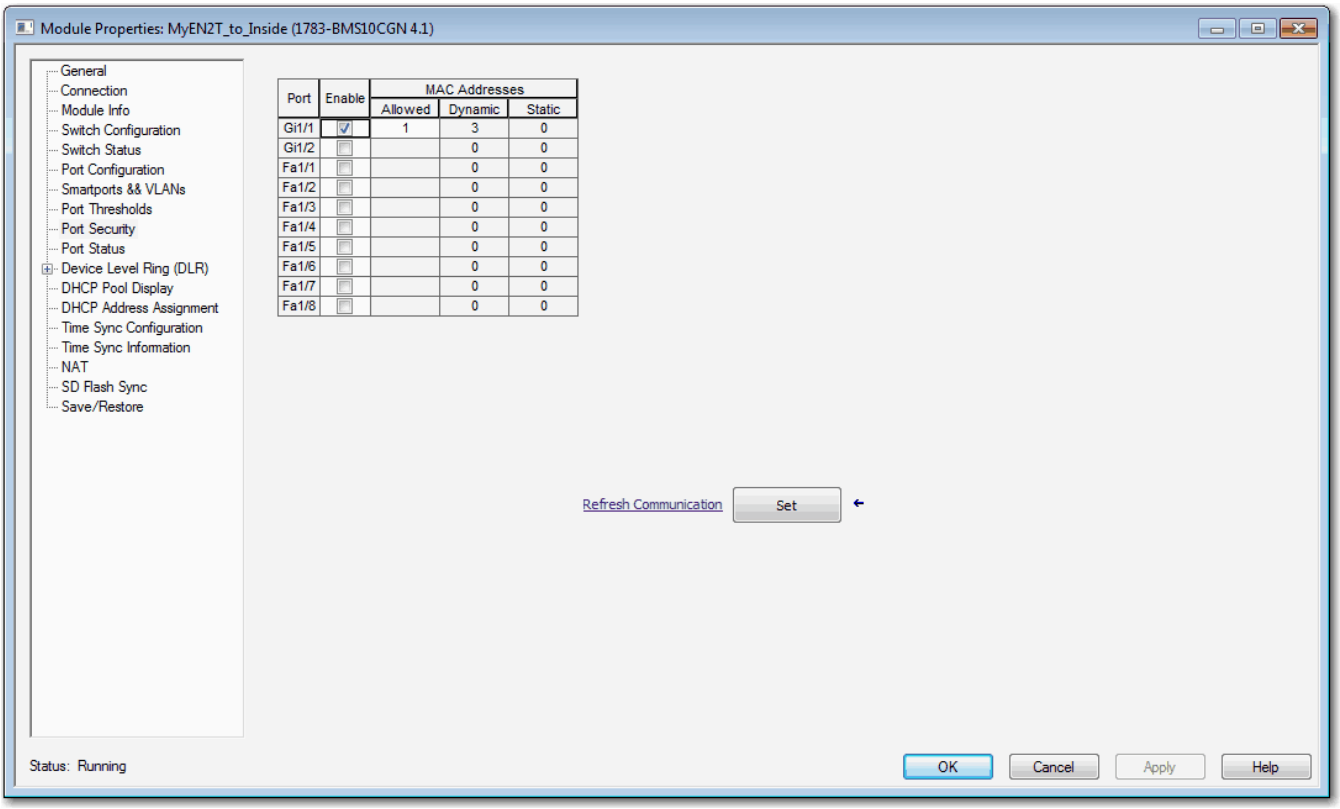


Table 107 - Port Security Fields

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 IDs. • Allowed—1...80. • Dynamic—The number of MAC IDs (devices) currently connected to the port that is not manually (statically) defined. • Static—The number of MAC IDs (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 23 - Advanced Port Configuration for Stratix 8000/8300 Switches

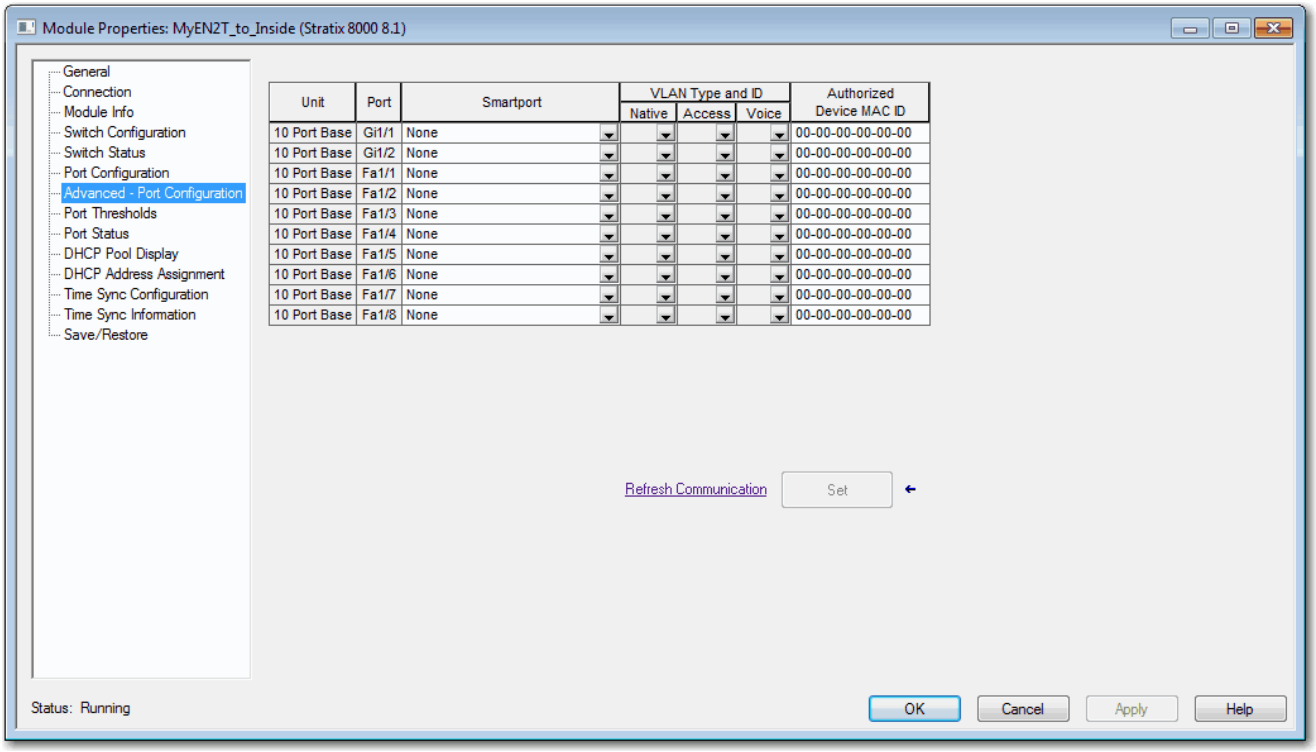


Table 108 - Advanced Port Configuration Fields for Stratix 8000/8300 Switches

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 270.
VLAN Type and ID	
Authorized Device MAC ID	To authorize a specific MAC ID to communicate on the port, type the MAC ID of the device that is connected to the port. You can authorize only one MAC ID to communicate on the port. If other MAC IDs 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 ID is also known as MAC ID, physical address, or hardware address. Each node on the network has a unique MAC ID. The MAC ID is six hexadecimal numbers, such as 00-00-BC-22-A0-D8.

Port Thresholds

Port thresholds help prevent traffic disruption on a LAN 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, which create excessive traffic and degrade 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:

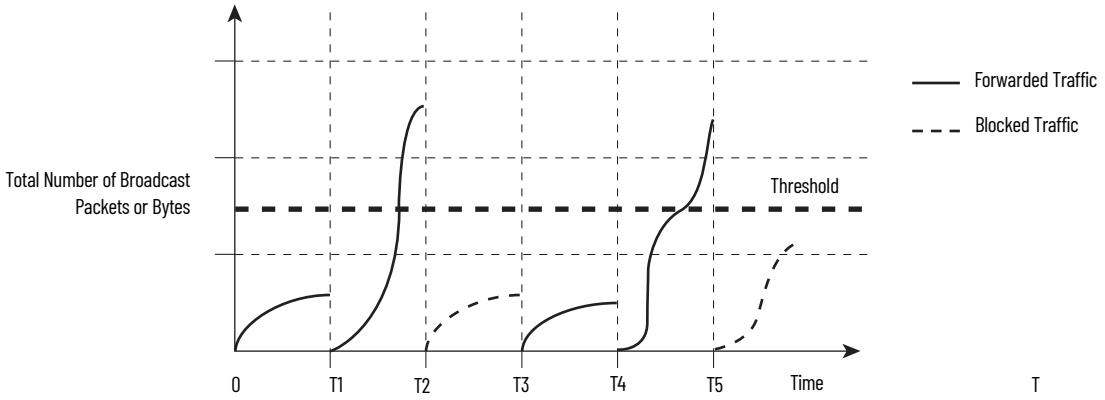
- Bandwidth as a percentage of the total available bandwidth of the port that is open for use by the broadcast, multicast, or unicast traffic.
- Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received.
- Traffic rate in bits per second at which broadcast, multicast, 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 also can 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 24 - 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. Limit bandwidth to specific users and ports to help control network congestion, enable high performance, create efficient networks, and help prevent a few devices from monopolizing the 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, 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.

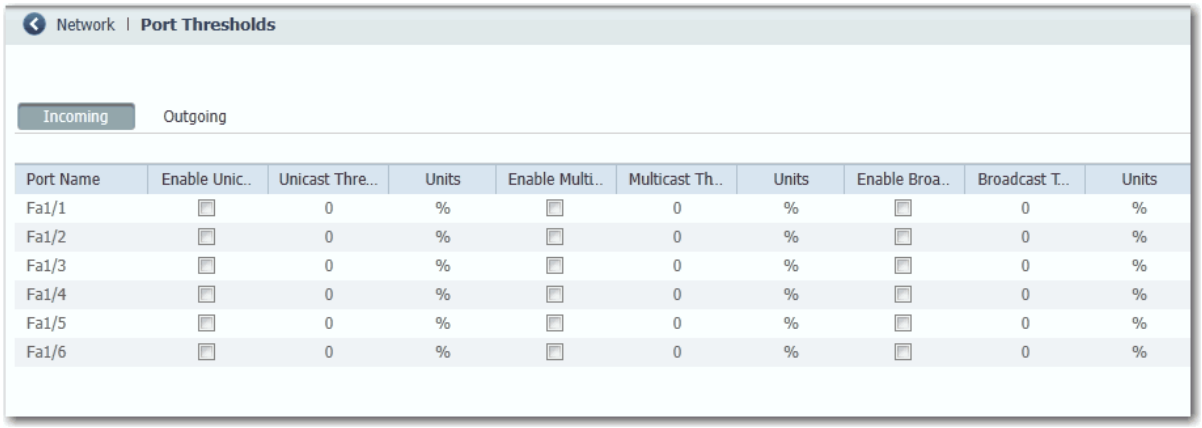


Table 109 - Port Threshold Fields

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 25 - Port Thresholds 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

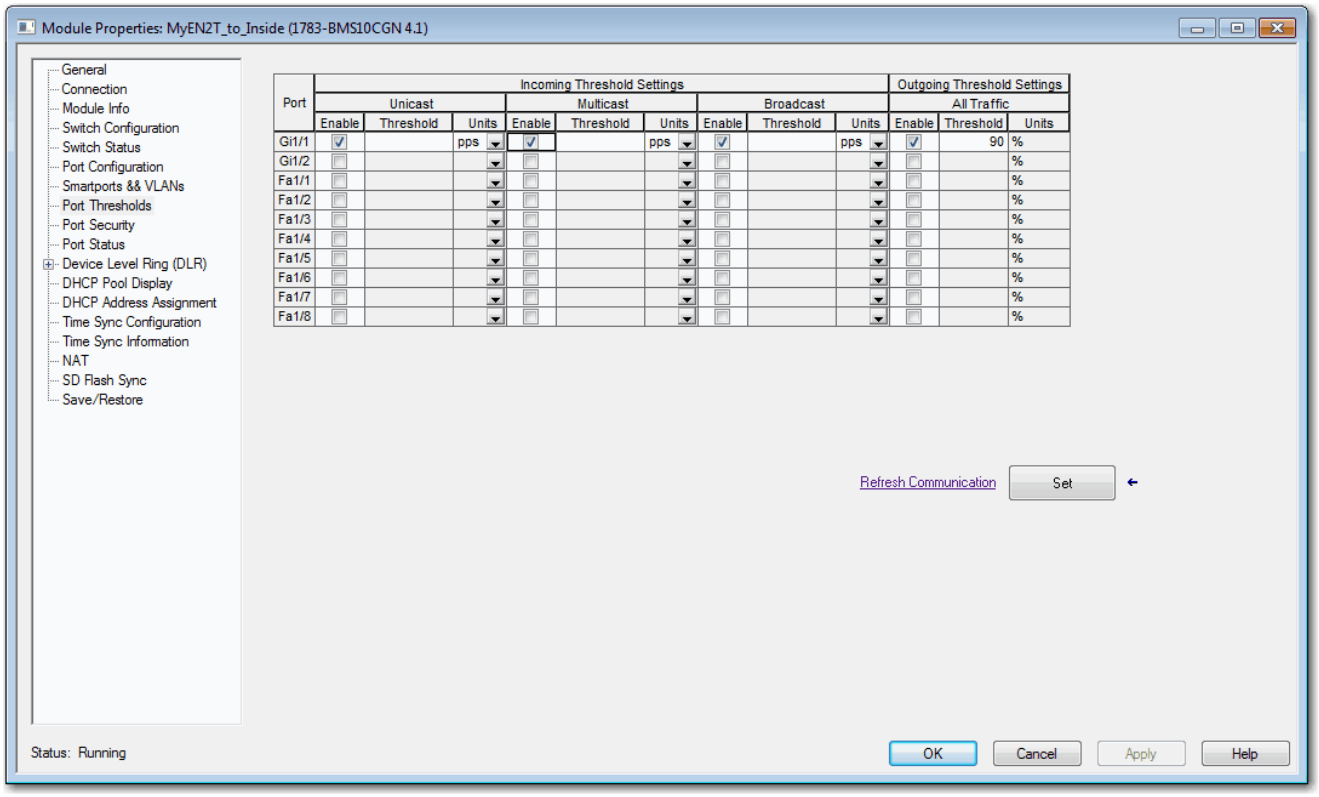

Module Properties: MyEN2T_to_Inside (1783-BMS10CGN 4.1)
General
Connection
Module Info
Switch Configuration
Switch Status
Port Configuration
Smartports && VLANs
Port Thresholds
Port Security
Port Status
Device Level Ring (DLR)
DHCP Pool Display
DHCP Address Assignment
Time Sync Configuration
Time Sync Information
NAT
SD Flash Sync
Save/Restore
Port
Incoming Threshold Settings
Unicast
Multicast
Broadcast
Outgoing Threshold Settings
All Traffic
Enable
Threshold
Units
Gi1/1 pps pps 90 %
Gi1/2 %
Fa1/1 %
Fa1/2 %
Fa1/3 %
Fa1/4 %
Fa1/5 %
Fa1/6 %
Fa1/7 %
Fa1/8 %
Refresh Communication
Set
Status: Running
OK
Cancel
Apply
Help

Figure 26 - Port Thresholds for Stratix 8000/8300 Switches

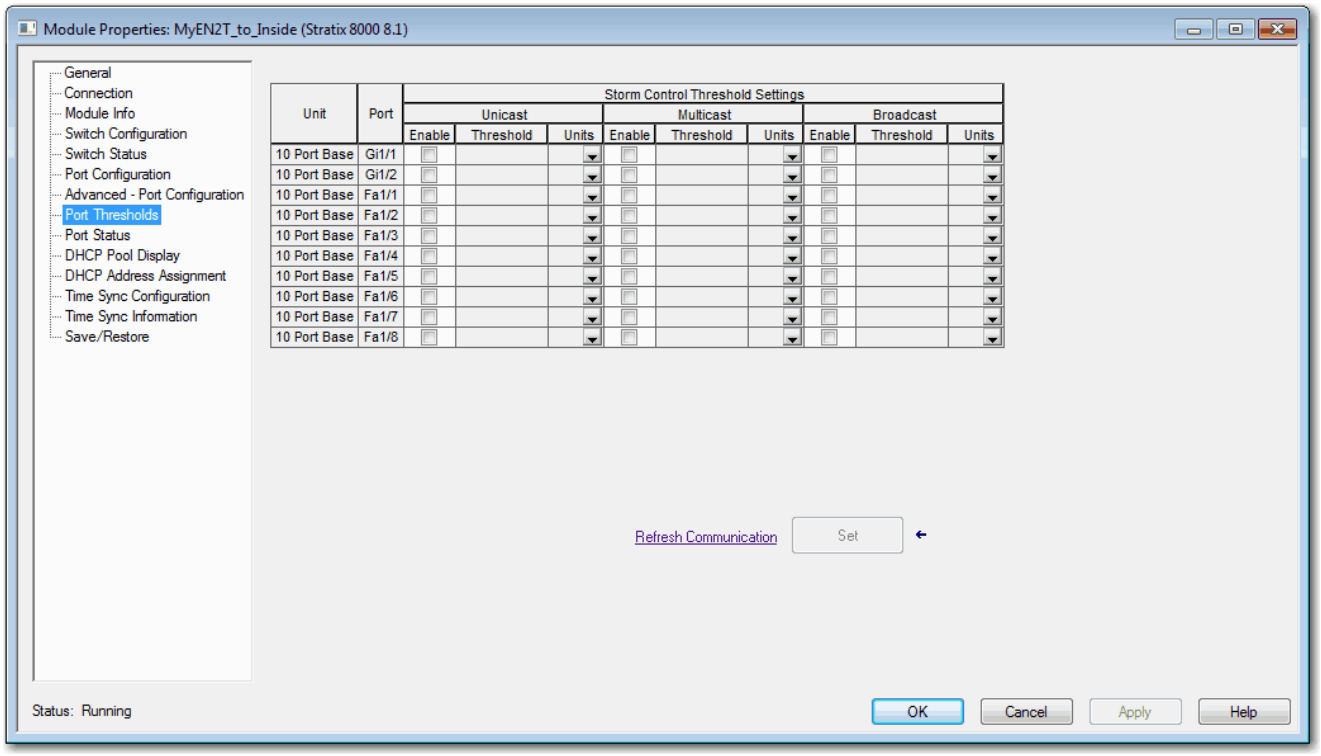


Table 110 - Port Threshold Fields for Stratix 8000/8300 Switches

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 that consumes 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 according to port number from highest to lowest.

PoE and PoE+ features are supported on switches and expansion modules with PoE ports when a correct power supply is connected to the switch.

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, be 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. If 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.

IMPORTANT Rockwell Automation recommends that you review the installation of the PoE-powered end device per IEEE standards. The PoE-powered end device receives its ground reference from the ground of the switch and therefore the PoE end device should not be tied to a separate ground. Review the IEEE 802.3af-2003 - Standard for Information Technology.

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 111 lists these levels.

Table 111 - 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 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 be sure that power is never applied to a PoE port; the port becomes 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 a powered device consumes 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:

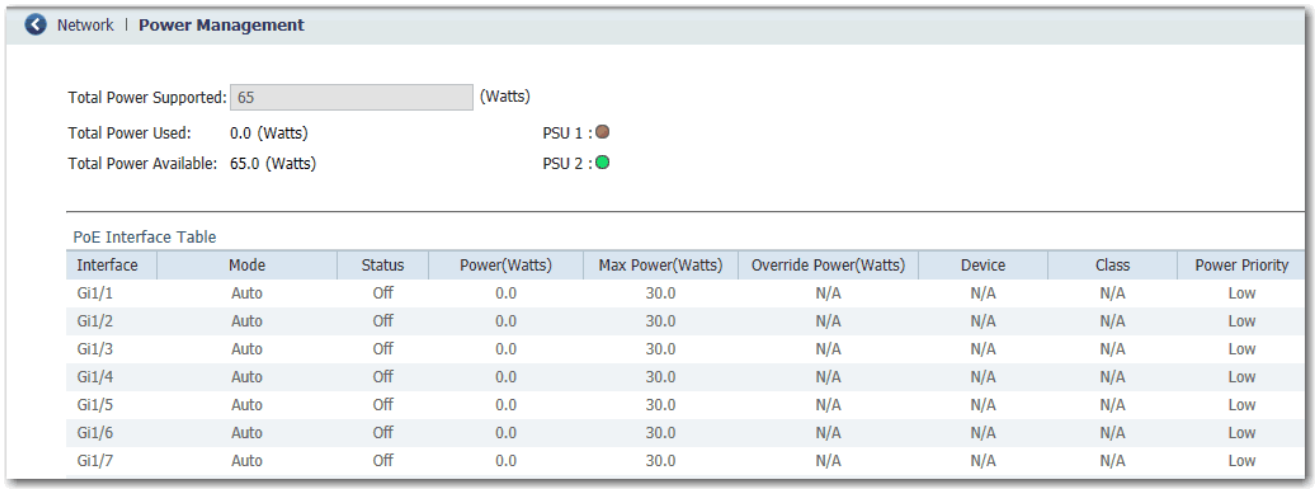
- If a power supply is removed and replaced by a new power supply with less power and there is insufficient power for the powered devices, power is denied to PoE ports that are in Auto mode. If there is still insufficient power, power is denied to PoE ports in Static mode. In both cases, power is denied 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

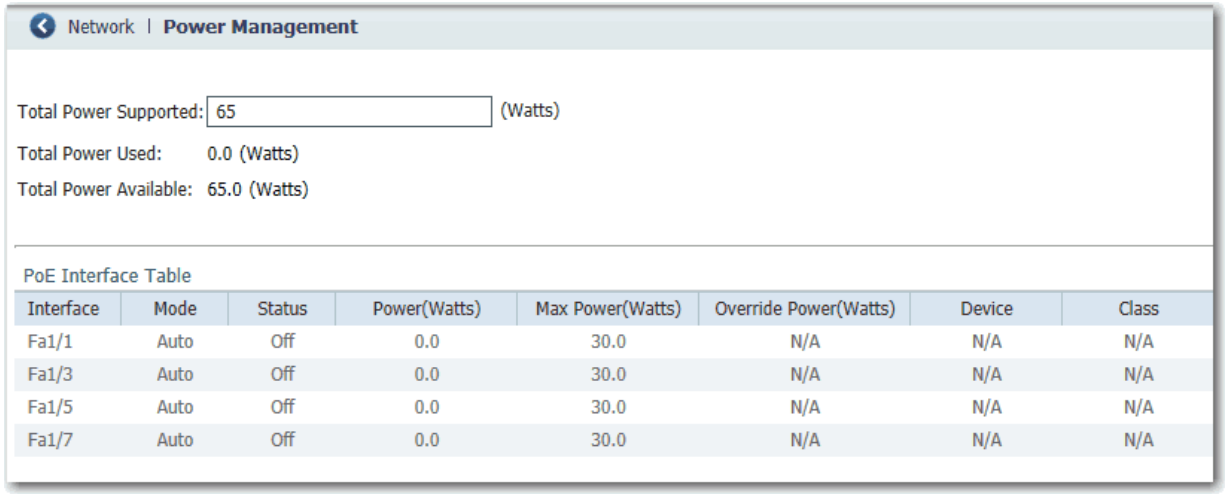
From the Configure menu, choose Power Management.

Figure 27 - PoE Configuration for Stratix 5410 Switches



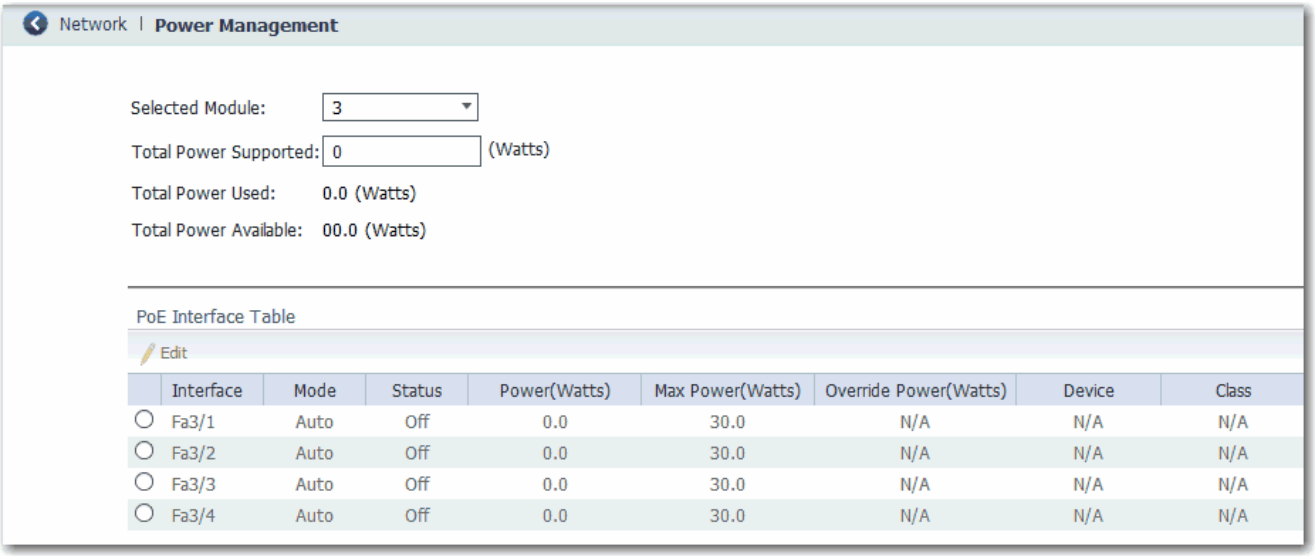
Interface	Mode	Status	Power(Watts)	Max Power(Watts)	Override Power(Watts)	Device	Class	Power Priority
Gi1/1	Auto	Off	0.0	30.0	N/A	N/A	N/A	Low
Gi1/2	Auto	Off	0.0	30.0	N/A	N/A	N/A	Low
Gi1/3	Auto	Off	0.0	30.0	N/A	N/A	N/A	Low
Gi1/4	Auto	Off	0.0	30.0	N/A	N/A	N/A	Low
Gi1/5	Auto	Off	0.0	30.0	N/A	N/A	N/A	Low
Gi1/6	Auto	Off	0.0	30.0	N/A	N/A	N/A	Low
Gi1/7	Auto	Off	0.0	30.0	N/A	N/A	N/A	Low

Figure 28 - PoE Configuration for Stratix 5400, Stratix 5700, and ArmorStratix 5700 Switches



Interface	Mode	Status	Power(Watts)	Max Power(Watts)	Override Power(Watts)	Device	Class
Fa1/1	Auto	Off	0.0	30.0	N/A	N/A	N/A
Fa1/3	Auto	Off	0.0	30.0	N/A	N/A	N/A
Fa1/5	Auto	Off	0.0	30.0	N/A	N/A	N/A
Fa1/7	Auto	Off	0.0	30.0	N/A	N/A	N/A

Figure 29 - PoE Configuration for Stratix 8000/8300 Switches



	Interface	Mode	Status	Power(Watts)	Max Power(Watts)	Override Power(Watts)	Device	Class
○	Fa3/1	Auto	Off	0.0	30.0	N/A	N/A	N/A
○	Fa3/2	Auto	Off	0.0	30.0	N/A	N/A	N/A
○	Fa3/3	Auto	Off	0.0	30.0	N/A	N/A	N/A
○	Fa3/4	Auto	Off	0.0	30.0	N/A	N/A	N/A

Table 112 - 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 damage 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.
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 233.
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, configure an override to allow 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 111 on page 232.
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 30 - PoE Configuration for Stratix 5410 Switches

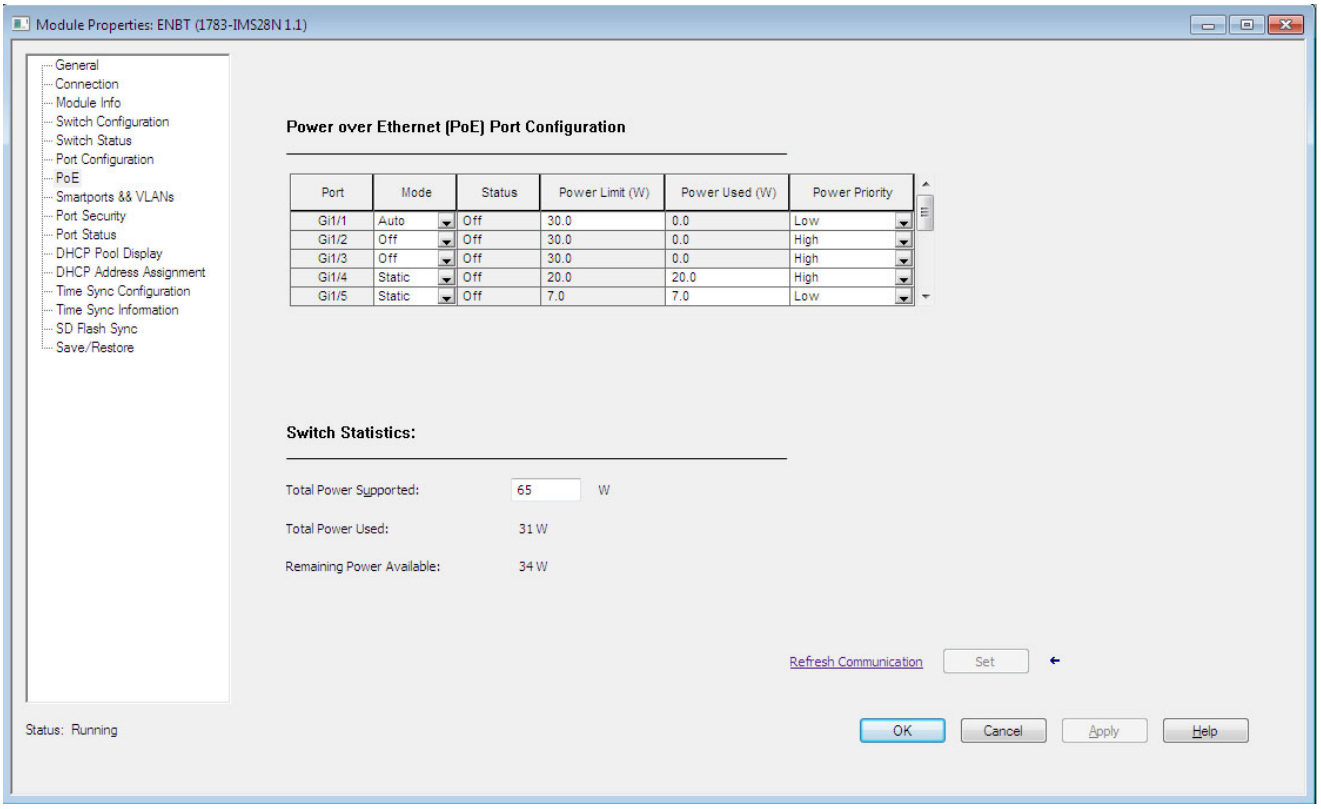


Figure 31 - PoE Configuration for Stratix 5400, Stratix 5700, and ArmorStratix 5700 Switches

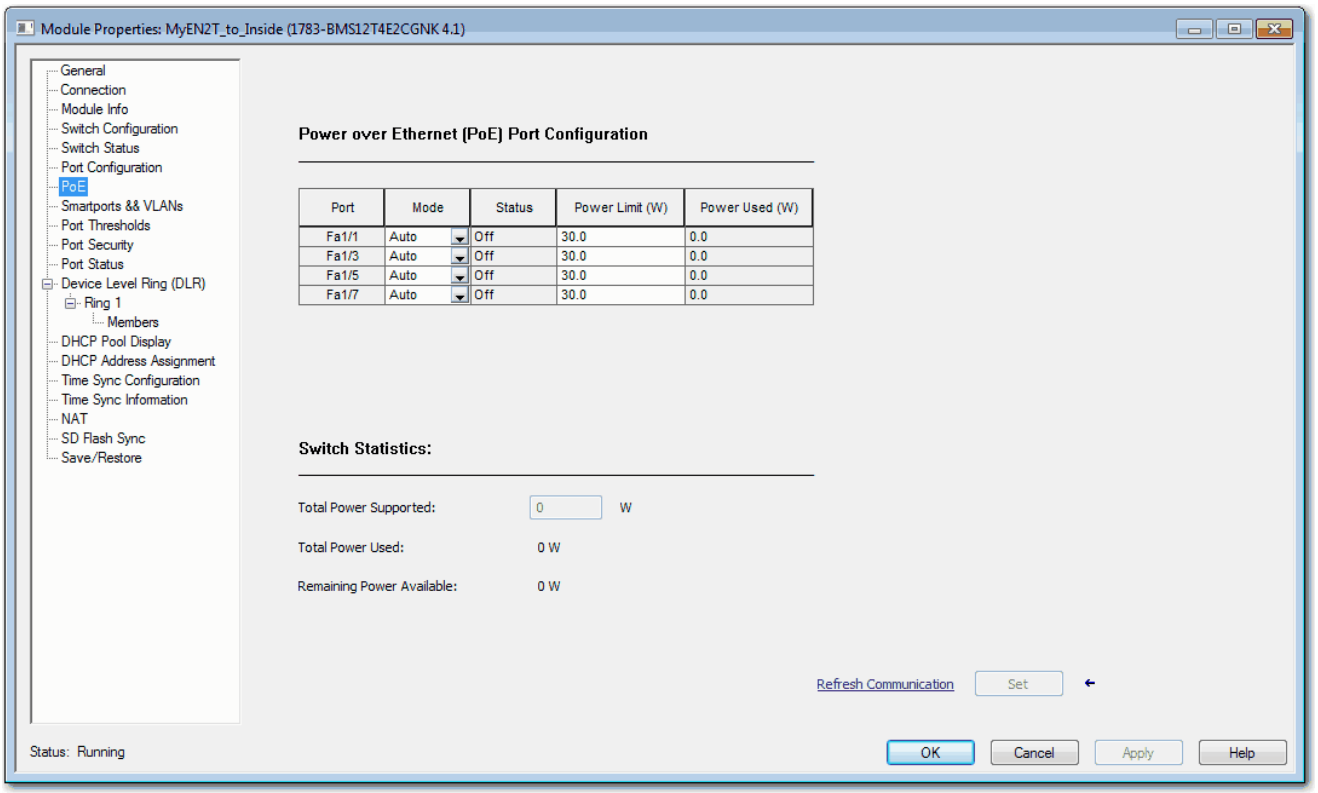


Figure 32 - PoE Configuration for Stratix 8000/8300 Switches

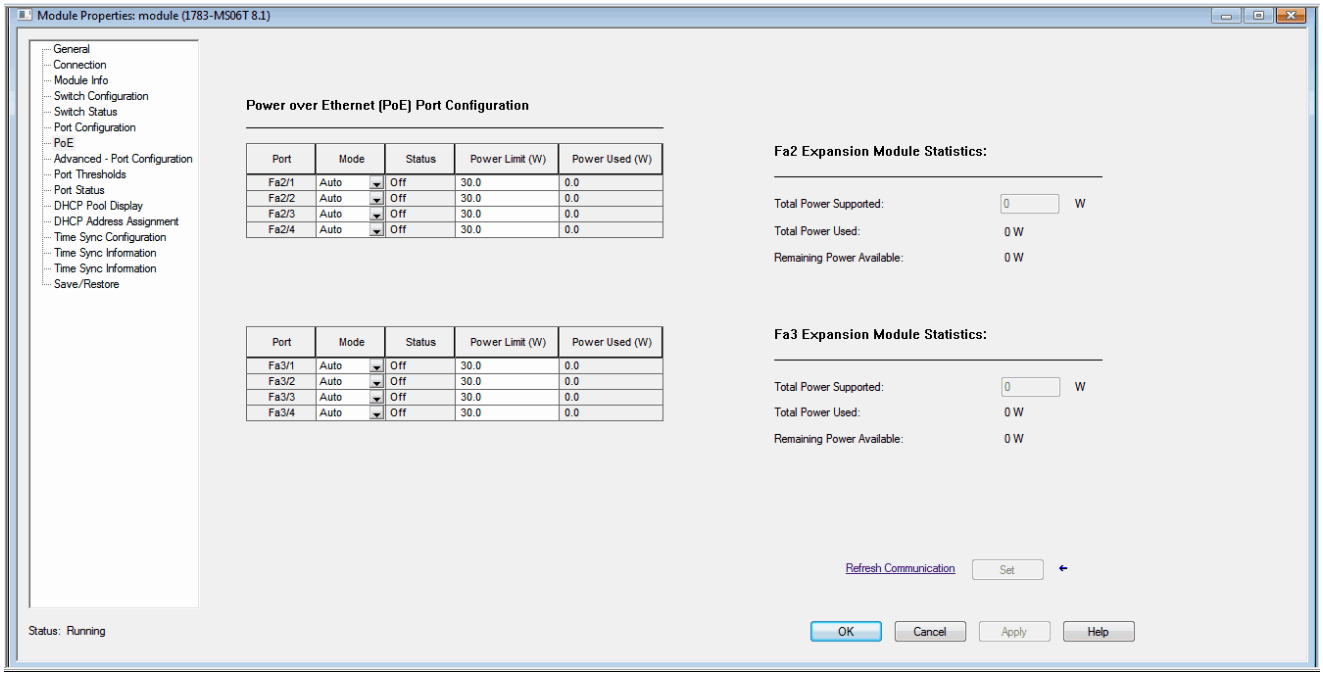


Table 113 - PoE Fields

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 233.
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

Table 113 - PoE Fields (Continued)

Field	Description
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 damage 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.

PROFINET

PROFINET is the PROFIBUS International (PI) open Industrial Ethernet Standard that uses TCP/IP and IT standards for automation control.

Stratix switches support the following PROFINET features:

- All switches support the forwarding of these PROFINET traffic types:
  - TCP/IP
  - Real-Time (RT)

  Stratix switches do not support the forwarding of Isochronous Real-Time (IRT) traffic.
- Stratix 5700 and ArmorStratix 5700 switches support PROFINET management via General Station Description (GSD).

PROFINET conformance classes define the capabilities of a device. All Stratix switches are Conformance Class B certified.

Configure PROFINET Traffic Forwarding

PROFINET traffic forwarding requires that the switch is configured for VLAN 0 priority tagging:

- In IOS Release 15.2(6)E0a and later, PROFINET traffic is configured for VLAN 0 tagging by default and no configuration is required. You can change the default configuration on the Edit Physical Port page in Device Manager. See page 45.
- In IOS Release 15.2(5)EA.fc4 and earlier, use the CLI to configure VLAN 0 priority tagging for PROFINET support. By default, VLAN 0 is disabled.

For more information about VLAN 0 priority tagging, see page 281.

To configure VLAN 0 priority tagging to support PROFINET in IOS 15.2(5)EA.fc4 and earlier, follow these steps.

1. Start a CLI session.

   For more information about the CLI, see page 65.
2. At the prompt, connect to the switch by entering the switch user name and password.
3. Enter privileged EXEC mode: Type **enable**, and then press Enter.

   In privileged EXEC mode, the CLI prompt ends with a pound sign as follows: Switch#
4. Enter global configuration mode: Type **configure terminal**, and then press Enter.
5. To configure VLAN 0 priority tagging on an access port, type the commands in Table 114.
   or
   To configure VLAN 0 priority tagging on a trunk port, type the commands in Table 115.

   For a tagging on a trunk port, be sure that the switch uses the IEEE 802.1Q (DOT1Q) standard.

   Press Enter to execute each command.

Table 114 - CLI Commands for VLAN 0 Priority Tagging—Access Ports

	Command	Description
Step 1	interface [interface id]	Identifies the port on which to forward PROFINET traffic.
Step 2	switchport mode access	Configures the port as an access port.
Step 3	switchport voice vlan [vlan id]	Configures the voice VLAN as the PROFINET VLAN.
Step 4	spanning-tree portfast	Enables PortFast on the port.

Example	`Switch(config)#interface fa1/3`
	`Switch(config-if)#switchport mode access`
	`Switch(config-if)#switchport voice vlan 10`
	`Switch(config-if)#spanning-tree portfast`	

Table 115 - CLI Commands for VLAN 0 Priority Tagging—Trunk Ports

	Command	Description
Step 1	interface [interface id]	Identifies the port on which to forward PROFINET traffic.
Step 2	switchport trunk native [vlan id]	Configures the native VLAN as the PROFINET VLAN.
Step 3	switchport mode trunk	Configures the port as a trunk port.
Step 4	spanning-tree portfast	Enables PortFast on the port.

Example	`Switch(config)#interface fa1/5`
	`Switch(config-if)#switchport trunk native vlan 2`
	`Switch(config-if)#switchport mode trunk`
	`Switch(config-if)#spanning-tree portfast`	

Configure a Stratix 5700 or ArmorStratix 5700 Switch for PROFINET Management

Stratix 5700 and ArmorStratix 5700 switches contain a PROFINET GSD (General Station Description) file that contains basic information about the switch for data exchange between the I/O controller, the I/O supervisor, and the I/O devices, including the switch. Each PROFINET I/O device must have an associated GSD file that describes the properties of the device and contains all this information that is required for configuration:

- Device identification information (device ID, vendor ID and name, product family, and number of ports)
- Number and types of connected modules
- Error text for diagnostic information
- Communication parameters for I/O devices, including the minimum cycle time, the reduction ratio, and the watchdog time
- Configuration data for the I/O modules, including speed, duplex, VLAN, port security information, alarms, and broadcast-rate-limiting thresholds
- Parameters configured for I/O modules

IMPORTANT You must use the GSD file that is associated with the IOS release on the switch to manage your PROFINET network. To verify that the GSD file on the switch matches the GSD file in your controller configuration software, see Verify the GSD File on page 245.

The GSD file name includes the last modification date and represents the version of the file, for example GSDML_V2.32-Rockwell-S5700-xxxxxx where xxxxx is the modification date. The date is updated when changes are made to the GSD file with each IOS release.

Stratix 5700 and ArmorStratix 5700 switches store the GSD file and image files of the switch models in a file named Rockwell_S5700_GSD.zip. The file is in the IOS folder on the switch.

To configure a Stratix 5700 or ArmorStratix 5700 switch for PROFINET management, use this process. By default, PROFINET is disabled.

1. Download the GSD file from the switch.
   a. In the IOS folder on the switch, locate the Rockwell_S5700_GSD.zip file.
   b. Extract the GSD file in .xml format and the associated image files in .bmp format.
2. Install the GSD file to your controller configuration software.

   A single GSD file adds all Stratix 5700 and ArmorStratix 5700 catalog numbers to the hardware catalog in your controller configuration software.
3. Add the Stratix switch to use for PROFINET management to your controller project.

4. In the device configuration of your controller project, enter a PROFINET device name.

   IMPORTANT To enable PROFINET, you must know the PROFINET device name exactly as it appears in your controller project.

5. To use combo ports on the switch for PROFINET, add the ports to the device configuration in your controller project.
6. Start a CLI session.

   For more information about the CLI, see page 65.

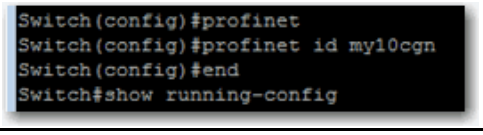
7. At the prompt, connect to the switch by entering the switch user name and password.
8. Enter privileged EXEC mode: Type **enable**, and then press Enter.

   In privileged EXEC mode, the CLI prompt ends with a pound sign as follows: Switch#

9. Enter global configuration mode: Type **configure terminal**, and then press Enter.
10. To enable PROFINET on the switch, type the commands in Table 116.

    Press Enter to execute each command.

Table 116 - CLI Commands to Enable PROFINET

	Command	Description
Step 1	profinet	Enables PROFINET on the switch.
Step 2	profinet id [PROFINET device name]	Sets the PROFINET device identifier (ID). **IMPORTANT:** This ID must match the PROFINET device name that you specified for the switch in your controller project. The maximum length is 240 characters. The only special characters that are allowed are the period (.) and hyphen (-), and they are allowed only in specific positions within the ID string. It can have multiple labels within the string. Each label can be from 1 to 63 characters, and labels must be separated by a period (.). The final character in the string must not be zero (0). For more details about PROFINET ID configuration, see the PROFINET specification, document number TC2-06-0007a, filename PN-AL-protocol_2722_V22_Oct07, available from PROFIBUS.
Step 3	profinet vlan [vlan id]	(Optional). Changes the VLAN number. The default VLAN number is 1. The VLAN ID range is 1...4094.
Step 4	end	Returns to privileged EXEC mode.
Step 5	show running-config	Verifies your entries.
Step 6	copy running-config startup-config	(Optional). Saves your entries in the configuration file.
Example		

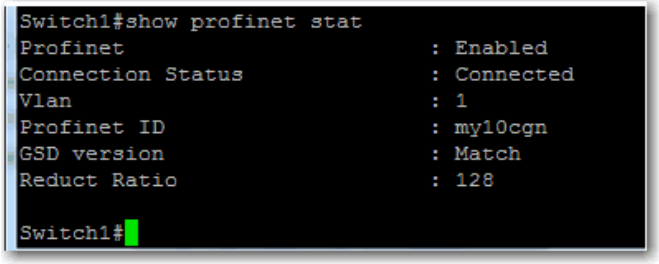
Verify the GSD File

To verify that the GSD file for the switch matches the GSD file in the controller configuration software, do the following.

1. Establish a connection between the switch and the I/O controller.
2. Start a CLI session.
3. Enter the following command in the CLI and press Enter:

   show profinet status

   As shown in the following example, the GSD version line shows whether the GSD file is a match or mismatch.



Monitor and Maintain PROFINET

Use the following commands in the CLI to display the PROFINET configuration.

Command	Purpose
show profinet sessions	Displays the currently connected PROFINET sessions.
show profinet status	Displays the status of the PROFINET subsystem.
show lldp neighbor interface x/x detail	Displays information about the adjacent interface.

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. Select the Switch for Automation Smartport to enable 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 that contains 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.

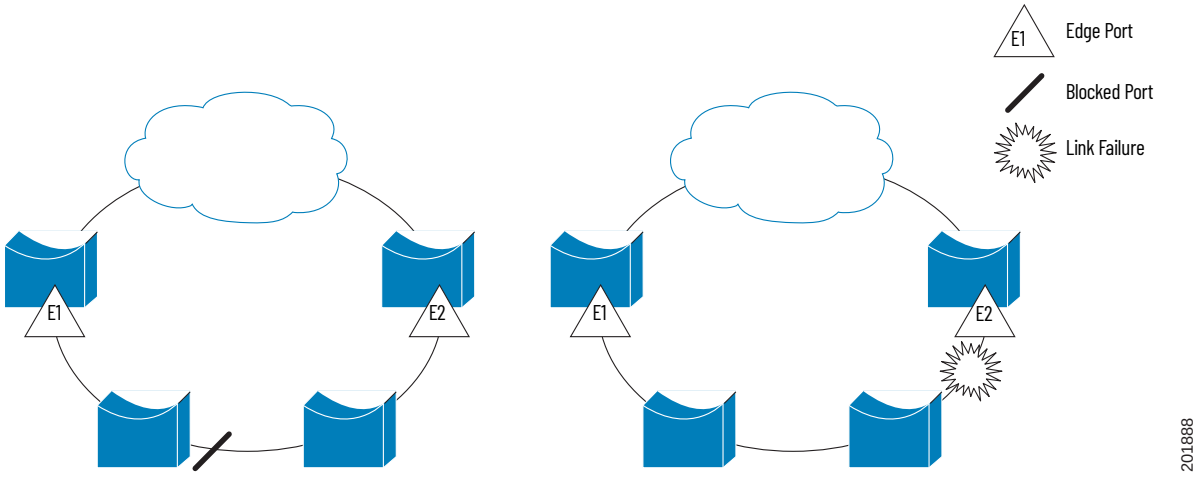
Figure 33 shows an example of a segment consisting of six ports that are spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), one port is blocked, shown by the diagonal line. When there is a failure in the network, 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 33 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 33 - Open Segment Example

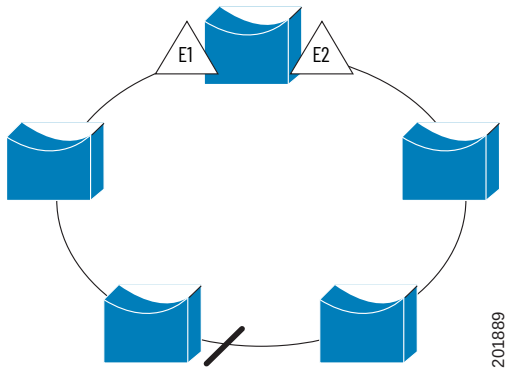


REP Ring Segment

The segment that is shown in Figure 34, 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 34 - Ring Segment Example



REP segments have these characteristics:

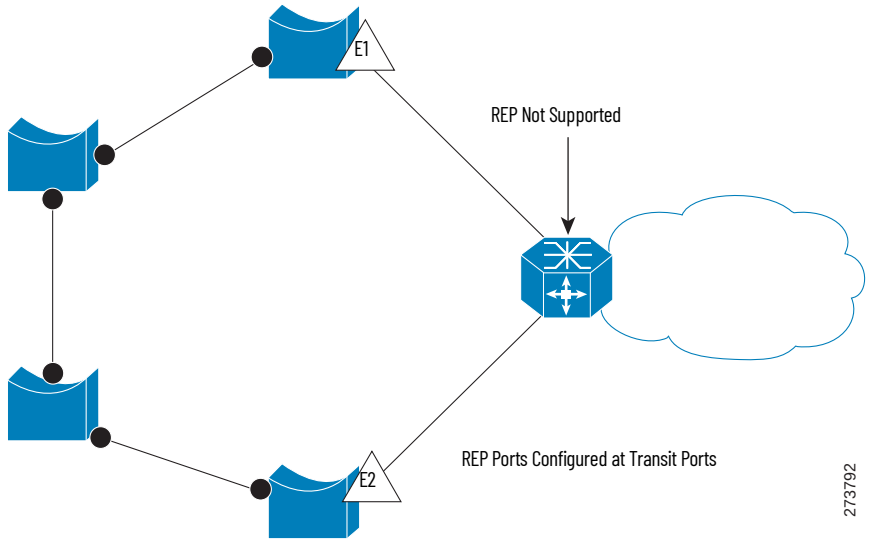
- If all ports in the segment are operational, one port (referred to as the alternate port) is in the blocked state for each VLAN.
- If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational and causes a link failure, all ports forward traffic on all VLANs to support ongoing connectivity.
- If there is 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 35. 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 sending 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 35, E1 or E2 can be configured as the primary no-neighbor port.

Figure 35 - 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. To configure 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 ID (unique in the network). When a segment port is coming up, its LSL starts to send 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.

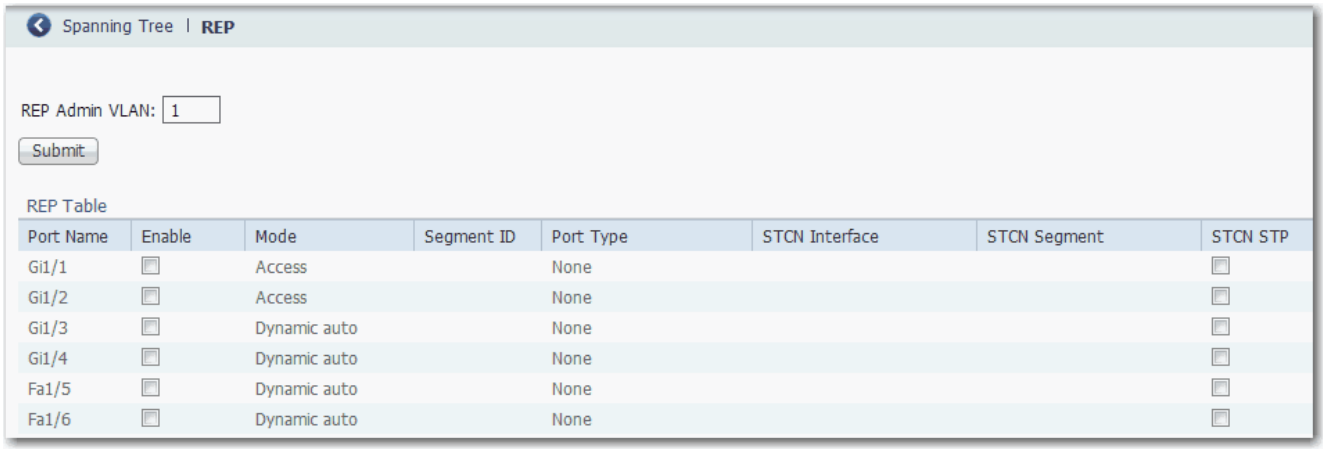


Table 117 - REP Fields

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).
Enable	If Enable is checked, REP is enabled on the port.
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. To configure 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.
STCN Interface	Optionally, configure the port to send Segment Topology Change Notices (STCNs) when the topology changes. If you configure this option, also specify the segment ID that receives the STCNs from this 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 valid range is 1...1024. You can also configure a sequence of segments.
STCN STP	Check STCN STP to send STCNs to STP networks. Be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces. By default, the checkbox is cleared.

Resilient Ethernet Protocol (REP) Negotiated

The REP Negotiated feature allows for communication over a running REP ring when a new Stratix switch is inserted, either as a new or replacement node, the new switch will pass through REP messages but will not be part of a REP topology until configured.

REP Negotiated is available on the Stratix 5400 and Stratix 8000 switches.

Configure REP Negotiated via Device Manager

To configure REP Negotiated via Device Manager:

1. From the Configure menu, choose REP from the Redundancy Protocols section.
2. To create a REP Negotiated ring, choose the REP Negotiated tab.
3. Enter the REP Admin VLAN number or keep the default.
4. Check BPDU Leak to enable it.
5. Check REP Negotiated.
6. Enter the Segment ID.
7. Click Submit.
8. After you submit your changes, click anywhere in a row of the REP table to configure the following:
   - Port Type
   - STCN Interface
   - STCN Segment
   - STCN STP
   - Rx State

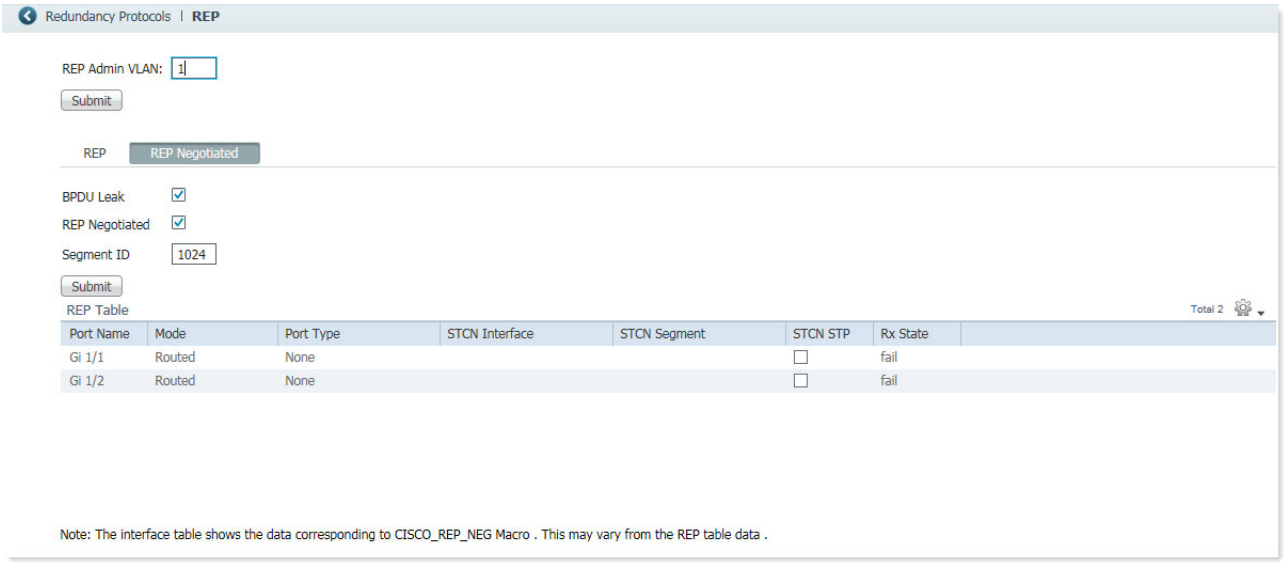


Table 118 - REP Negotiated Fields

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.
BPDU (Bridge Protocol Data Unit) Leak	BPDU leaking is enabled by default, which transparently forwards REP BPDUs between two ring ports when there is no REP configured on the switch.
REP Negotiated	Enables the Segment ID text box. Migrates devices to be part of the REP ring. Clear to use STP.
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 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.
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. To configure 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. • Transit—A non-edge port in the REP segment.
STCN Interface	Optionally configures the port to send Segment Topology Change Notices (STCNs) when the topology changes. If you configure this option, also specify the segment ID that receives the STCNs from this 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	Configures STCNs to a segment ID. The valid range is 1…1024. You can also configure a sequence of segments.
STCN STP	Sends STCNs to STP networks. Be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces. By default, the checkbox is cleared.
Rx State	The REP port state.

BPDU Leak and REP Negotiated are mutually exclusive and coexist.

From the CLI, individual ports can be turned on and off; but on the deployment topology, it makes sense to enable on both ports. Therefore, on the Device Manager page, REP Negotiation is enabled either for both or none.

Routing, Layer 3

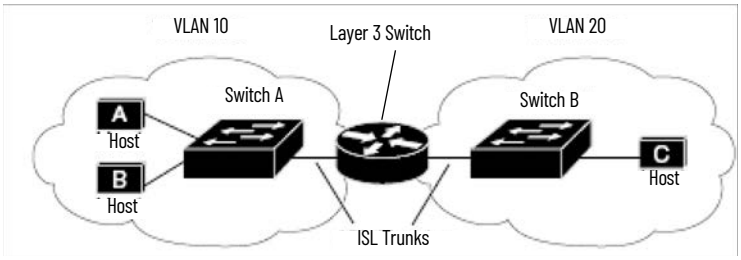
Layer 3 routing is available on the following switches:

- Stratix 5400 with Layer 3 firmware
- Stratix 5410 with Layer 3 firmware
- Stratix 8300 base units

Layer 3 routing uses IP address information to map subnetworks 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. To configure VLANs helps to 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 36 shows a basic routing topology.

Figure 36 - 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.

Stratix switches that support Layer 3 routing can route packets by using these methods.

Table 119 - Routing Methods

Feature	Description
EIGRP	See Enhanced Interior Gateway Routing Protocol (EIGRP) on page 135.
OSPF	See Open Shortest Path First (OSPF) Routing Protocol on page 206.
Static and connected routing	See Routing, Static and Connected on page 254.

Table 119 - Routing Methods

Feature	Description
Dynamic routing	Dynamic routing protocols are used by Layer 3 switches to calculate dynamically the best route for traffic forwarding. 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 speed 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 CLI for routing configuration, see the Cisco IE3000 Switch Command-Line Interface Manual, available from http://www.Cisco.com.

Routing, Static and Connected

Static and connected routing is available on the following switches:

- Stratix 5400
- Stratix 5410
- Stratix 5700 switches with Full firmware
- ArmorStratix 5700
- Stratix 8000 and 8300

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 help 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

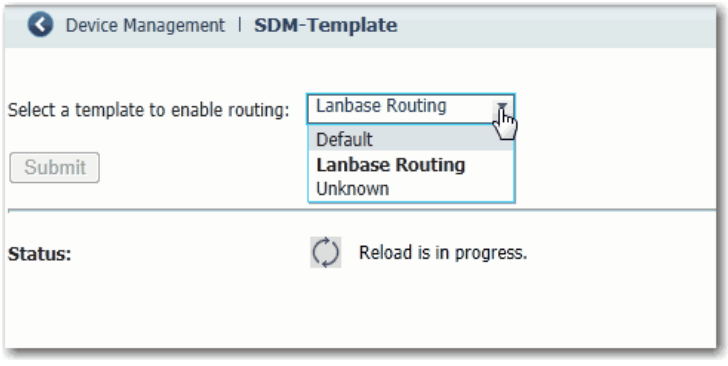
   Enable and configure static routing, which also enables connected routing by default.

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.(1)

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



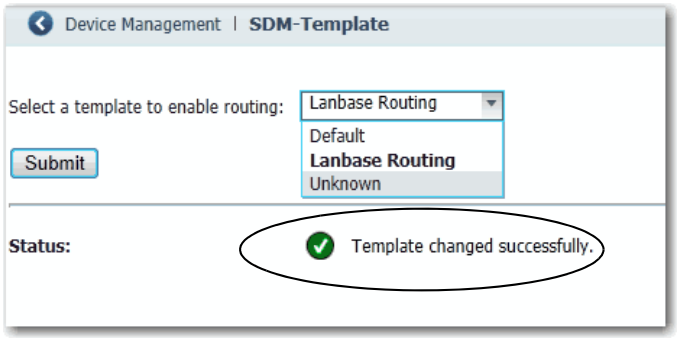
3. Click Submit.

(1) You do not need to change the default SDM template to Lanbase Routing for Stratix 5400 and Stratix 5410.

4. When a message appears prompting you to continue, click OK.

IMPORTANT The process of changing the template causes the switch to restart.

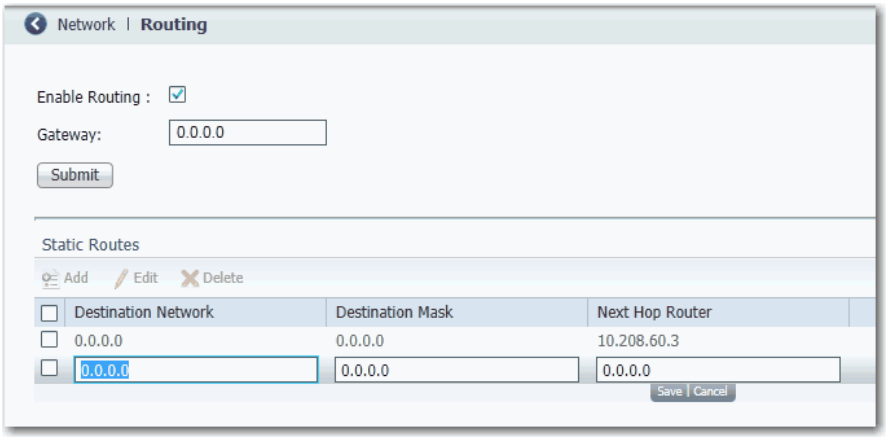
A message appears once the process is complete.



Enable and Configure Routing via Device Manager

Before you can enable routing, you must reallocate switch memory for routing as described on page 255.

From the Configure menu, choose Routing.



From the Routing page, 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 Routing, Layer 3 on page 253.

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

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 258 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 that are 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 designed 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 help prevent the contents from being exposed on the network.

Supported MIBs

Stratix managed switches support the following MIBs.

Table 120 - Supported MIBs for Stratix 5400 and 5410 Switches

MIB Name		
BRIDGE-MIB	CISCO-IPSLA-AUTOMEASURE-MIB	CISCO-VLAN-MEMBERSHIP-MIB
CALISTA-DPA-MIB	CISCO-IPSLA-ECHO-MIB	CISCO-VRF-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-IPSLA-ETHERNET-MIB	CISCO-VTP-MIB
CISCO-AUTH-FRAMEWORK-MIB	CISCO-IPSLA-JITTER-MIB	DIFFSERV-MIB
CISCO-BGP4-MIB	CISCO-L2L3-INTERFACE-CONFIG-MIB	ENTITY-MIB
CISCO-BRIDGE-EXT-MIB	CISCO-L2NAT-MIB	ETHERLIKE-MIB
CISCO-BULK-FILE-MIB	CISCO-LAG-MIB	HC-RMON-MIB
CISCO-CABLE-DIAG-MIB	CISCO-LICENSE-MGMT-MIB	IEC-62439-3-MIB
CISCO-CALLHOME-MIB	CISCO-MAC-AUTH-BYPASS-MIB	IEEE8021-CFM-MIB
CISCO-CAR-MIB	CISCO-MAC-NOTIFICATION-MIB	IEEE8021-CFM-V2-MIB
CISCO-CDP-MIB	CISCO-MEMORY-POOL-MIB	IEEE8021-PAE-MIB
CISCO-CEF-MIB	CISCO-MRP-MIB	IEEE8023-LAG-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-OSPF-MIB	IF-MIB
CISCO-CLASS-BASED-QOS-MIB	CISCO-OSPF-TRAP-MIB	IGMP-MIB
CISCO-CLUSTER-MIB	CISCO-PAE-MIB	IP-FORWARD-MIB
CISCO-CONFIG-COPY-MIB	CISCO-PAGP-MIB	IP-MIB
CISCO-CONFIG-MAN-MIB	CISCO-PIM-MIB	IPMROUTE-STD-MIB
CISCO-CONTEXT-MAPPING-MIB	CISCO-PING-MIB	LLDP-EXT-DOT3-MIB
CISCO-DATA-COLLECTION-MIB	CISCO-PKI-MIB	LLDP-EXT-MED-MIB
CISCO-DEVICE-LOCATION-MIB	CISCO-PORT-QOS-MIB	LLDP-EXT-PNO-MIB
CISCO-DHCP-SNOOPING-MIB	CISCO-PORT-SECURITY-MIB	LLDP-MIB
CISCO-EIGRP-MIB	CISCO-PORT-STORM-CONTROL-MIB	NETRANGER
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-POWER-ETHERNET-EXT-MIB	NOTIFICATION-LOG-MIB
CISCO-ENERGYWISE-MIB	CISCO-PRIVATE-VLAN-MIB	OLD-CISCO-CHASSIS-MIB
CISCO-ENTITY-ALARM-MIB	CISCO-PROCESS-MIB	OLD-CISCO-CPU-MIB
CISCO-ENTITY-FRU-CONTROL-MIB	CISCO-PRODUCTS-MIB	OLD-CISCO-FLASH-MIB
CISCO-ENTITY-SENSOR-MIB	CISCO-PTP-MIB	OLD-CISCO-INTERFACES-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	OLD-CISCO-IP-MIB

Table 120 - Supported MIBs for Stratix 5400 and 5410 Switches (Continued)

MIB Name		
CISCO-ENVMON-MIB	CISCO-RTTMON-ICMP-MIB	OLD-CISCO-MEMORY-MIB
CISCO-ERR-DISABLE-MIB	CISCO-RTTMON-IP-EXT-MIB	OLD-CISCO-SYS-MIB
CISCO-ETHER-CFM-MIB	CISCO-RTTMON-MIB	OLD-CISCO-SYSTEM-MIB
CISCO-FLASH-MIB	CISCO-RTTMON-RTP-MIB	OLD-CISCO-TCP-MIB
CISCO-FLOW-METADATA-MIB	CISCO-SNMP-TARGET-EXT-MIB	OLD-CISCO-TS-MIB
CISCO-FTP-CLIENT-MIB	CISCO-STACK-MIB	OSPFV3-MIB
CISCO-HSRP-EXT-MIB	CISCO-STACKMAKER-MIB	POWER-ETHERNET-MIB
CISCO-HSRP-MIB	CISCO-STACKWISE-MIB	RMON-MIB
CISCO-IETF-BFD-MIB	CISCO-STP-EXTENSIONS-MIB	RMON2-MIB
CISCO-IETF-DOT3-OAM-MIB	CISCO-SYSLOG-MIB	SMON-MIB
CISCO-IETF-ISIS-MIB	CISCO-SYSTEM-EXT-MIB	SNMP-COMMUNITY-MIB
CISCO-IF-EXTENSION-MIB	CISCO-TCP-MIB	SNMP-FRAMEWORK-MIB
CISCO-IGMP-FILTER-MIB	CISCO-TRUSTSEC-INTERFACE-MIB	SNMP-MPD-MIB
CISCO-IMAGE-MIB	CISCO-TRUSTSEC-MIB	SNMP-NOTIFICATION-MIB
CISCO-IP-STAT-MIB	CISCO-TRUSTSEC-POLICY-MIB	SNMP-PROXY-MIB
CISCO-IP-URPF-MIB	CISCO-TRUSTSEC-SERVER-MIB	SNMP-TARGET-MIB
CISCO-IPMROUTE-MIB	CISCO-TRUSTSEC-SXP-MIB	SNMP-USM-MIB
CISCO-IPSEC-FLOW-MONITOR-MIB	CISCO-UDLDP-MIB	SNMP-VIEW-BASED-ACM-MIB
CISCO-IPSEC-MIB	CISCO-VLAN-GROUP-MIB	SNMPv2-MIB
CISCO-IPSEC-PROVISIONING-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	

Table 121 - Supported MIBs for Stratix 5700 and ArmorStratix 5700 Switches

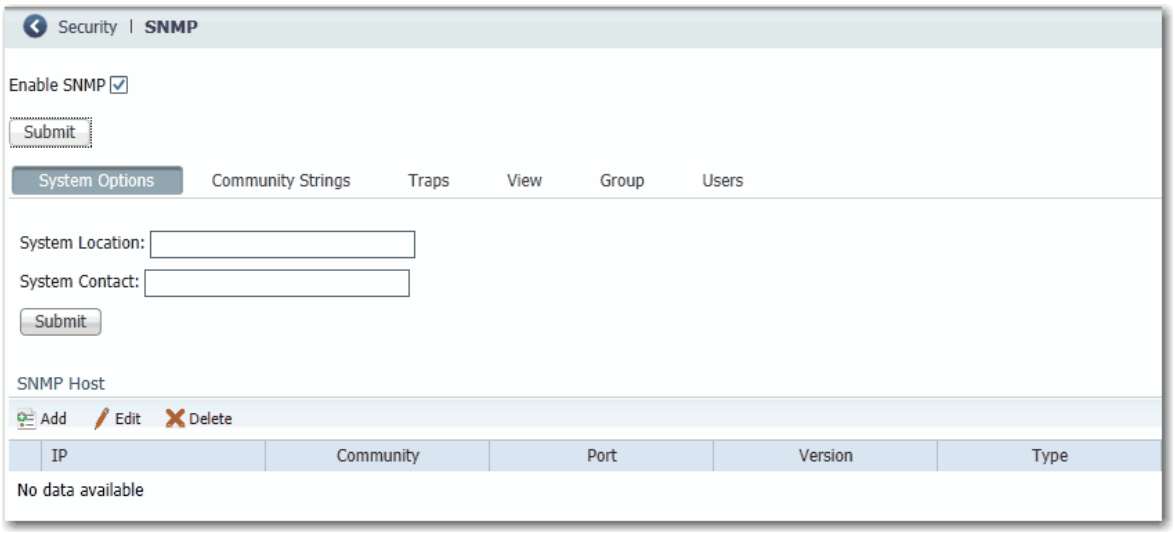
MIB Name			
BRIDGE-MIB	CISCO-IPMROUTE-MIB	CISCO-UDLDP-MIB	SNMP-FRAMEWORK-MIB
CALISTA-DPA-MIB	CISCO-IPSEC-FLOW-MONITOR-MIB	CISCO-VLAN-GROUP-MIB	SNMP-MPD-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-IPSEC-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	SNMP-NOTIFICATION-MIB
CISCO-AUTH-FRAMEWORK-MIB	CISCO-IPSEC-PROVISIONING-MIB	CISCO-VLAN-MEMBERSHIP-MIB	SNMP-PROXY-MIB
CISCO-BRIDGE-EXT-MIB	CISCO-IPSLA-AUTOMEASURE-MIB	CISCO-VRF-MIB	SNMP-TARGET-MIB
CISCO-BULK-FILE-MIB	CISCO-IPSLA-ECHO-MIB	CISCO-VTP-MIB	SNMP-USM-MIB
CISCO-CABLE-DIAG-MIB	CISCO-IPSLA-JITTER-MIB	DIFFSERV-MIB	SNMP-VIEW-BASED-ACM-MIB
CISCO-CALLHOME-MIB	CISCO-L2NAT-MIB	ENTITY-MIB	SNMPv2-MIB
CISCO-CAR-MIB	CISCO-LAG-MIB	ETHERLIKE-MIB	
CISCO-CDP-MIB	CISCO-LICENSE-MGMT-MIB	HC-RMON-MIB	
CISCO-CEF-MIB	CISCO-MAC-AUTH-BYPASS-MIB	IEEE8021-PAE-MIB	
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-MAC-NOTIFICATION-MIB	IEEE8023-LAG-MIB	
CISCO-CLASS-BASED-QOS-MIB	CISCO-MEMORY-POOL-MIB	IF-MIB	
CISCO-CLUSTER-MIB	CISCO-MRP-MIB	IGMP-MIB	
CISCO-CONFIG-COPY-MIB	CISCO-OSPF-MIB	IP-FORWARD-MIB	
CISCO-CONFIG-MAN-MIB	CISCO-OSPF-TRAP-MIB	IP-MIB	
CISCO-CONTEXT-MAPPING-MIB	CISCO-PAE-MIB	IPMROUTE-STD-MIB	
CISCO-DATA-COLLECTION-MIB	CISCO-PAGP-MIB	LLDP-EXT-DOT3-MIB	
CISCO-DEVICE-LOCATION-MIB	CISCO-PIM-MIB	LLDP-EXT-MED-MIB	
CISCO-DHCP-SNOOPING-MIB	CISCO-PING-MIB	LLDP-EXT-PNO-MIB	
CISCO-EIGRP-MIB	CISCO-PKI-MIB	LLDP-MIB	
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-PORT-QOS-MIB	MAU-MIB	
CISCO-ENERGYWISE-MIB	CISCO-PORT-SECURITY-MIB	NETRANGER	
CISCO-ENTITY-ALARM-MIB	CISCO-PORT-STORM-CONTROL-MIB	NOTIFICATION-LOG-MIB	
CISCO-ENTITY-FRU-CONTROL-MIB	CISCO-POWER-ETHERNET-EXT-MIB	OLD-CISCO-CHASSIS-MIB	
CISCO-ENTITY-SENSOR-MIB	CISCO-PRIVATE-VLAN-MIB	OLD-CISCO-CPU-MIB	
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-PROCESS-MIB	OLD-CISCO-FLASH-MIB	
CISCO-ENVMON-MIB	CISCO-PRODUCTS-MIB	OLD-CISCO-INTERFACES-MIB	

Table 121 - Supported MIBs for Stratix 5700 and ArmorStratix 5700 Switches (Continued)

MIB Name			
CISCO-ERR-DISABLE-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	OLD-CISCO-IP-MIB	
CISCO-FLASH-MIB	CISCO-RTTMON-ICMP-MIB	OLD-CISCO-MEMORY-MIB	
CISCO-FLOW-METADATA-MIB	CISCO-RTTMON-IP-EXT-MIB	OLD-CISCO-SYS-MIB	
CISCO-FTP-CLIENT-MIB	CISCO-RTTMON-MIB	OLD-CISCO-SYSTEM-MIB	
CISCO-HSRP-EXT-MIB	CISCO-RTTMON-RTP-MIB	OLD-CISCO-TCP-MIB	
CISCO-HSRP-MIB	CISCO-SNMP-TARGET-EXT-MIB	OLD-CISCO-TS-MIB	
CISCO-IETF-BFD-MIB	CISCO-STACK-MIB	OSPFV3-MIB	
CISCO-IF-EXTENSION-MIB	CISCO-STACKMAKER-MIB	POWER-ETHERNET-MIB	
CISCO-IGMP-FILTER-MIB	CISCO-STP-EXTENSIONS-MIB	RMON-MIB	
CISCO-IMAGE-MIB	CISCO-SYSLOG-MIB	RMON2-MIB	
CISCO-IP-STAT-MIB	CISCO-TCP-MIB	SMON-MIB	
CISCO-IP-URPF-MIB	CISCO-TRUSTSEC-SXP-MIB	SNMP-COMMUNITY-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 FTNM or HP OpenView to configure and manage the switch. Refer to Simple Network Management Protocol (SNMP) on page 257 for more information.

Smartports

Smartports are recommended configurations for 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. Port roles also help to prevent port misconfigurations.

Use Smartport roles immediately after the initial setup of the switch to configure the switch ports before they connect to devices.

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 the 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.

- You cannot configure port roles on routed ports.

The port roles that are described in Table 122 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 122 - 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 that are connected to multiport EtherNet/IP devices. Devices include multiport EtherNet/IP devices that are 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 Rapid 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 computers that are running virtualization software. Virtual Desktop for Automation can be used with devices running up to two MAC IDs: • 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 122 - Smartport Roles (Continued)

Port Role	Description
Wireless for Automation (Single VLAN)	Apply this role to ports to be connected to wireless access points that use a single VLAN.
Wireless for Automation (Multi VLAN)	Apply this role to ports to be connected to wireless access points that use multiple VLANs.
Port Mirroring	Apply this role to ports monitored by a network analyzer. For more information about port mirroring, see page 219.
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 263.

Custom Smartport Roles

You can create and modify as many as 10 custom Smartport roles for various 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:

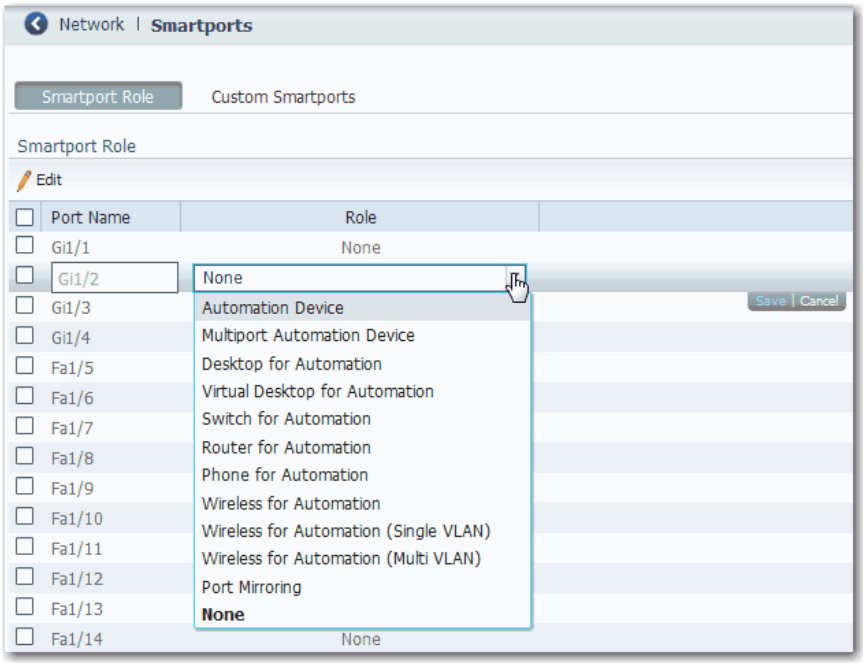
- Affect the behavior of the attached device
- Lower network performance (reduce the level of Quality of Service [QoS]) on CIP, voice, wireless, switch, and router traffic
- Reduce restrictions on guest access to the network
- Reduce protection from denial-of-service (DoS) attacks on the network
- Disable 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 the devices.

Configure Smartports via Device Manager

IMPORTANT When you change the Smartport role for a port, the switch sets the VLAN assigned to the port back to the default VLAN 1. You must reassign VLANs to a port after changing its Smartport role.

From the Configure menu, choose Smartports.



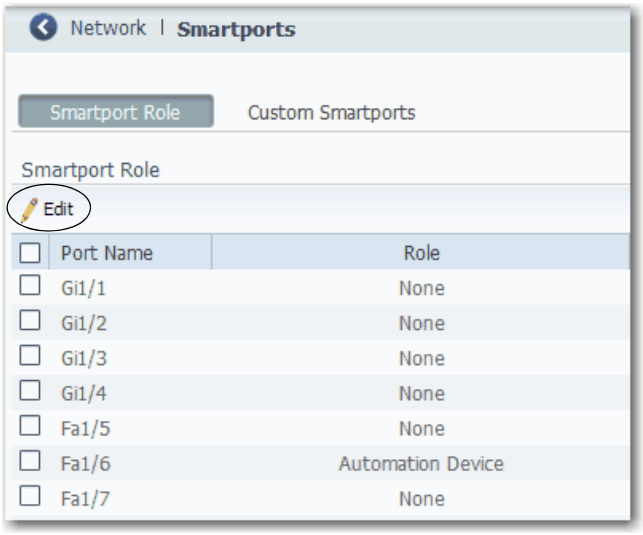
Apply a Smartport Role

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.

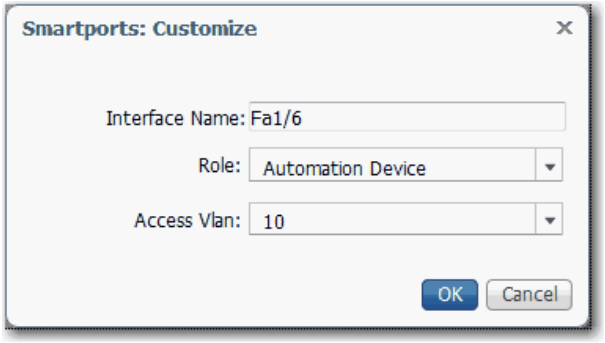
Assign a Port to a VLAN

Before changing virtual local area network (VLAN) assignments, understand what a VLAN is, its purpose, and how to create a VLAN. See page 277 for more information about VLANs.

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 and click OK.



Manage Custom Smartport Macros

Custom Smartports macros are 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.

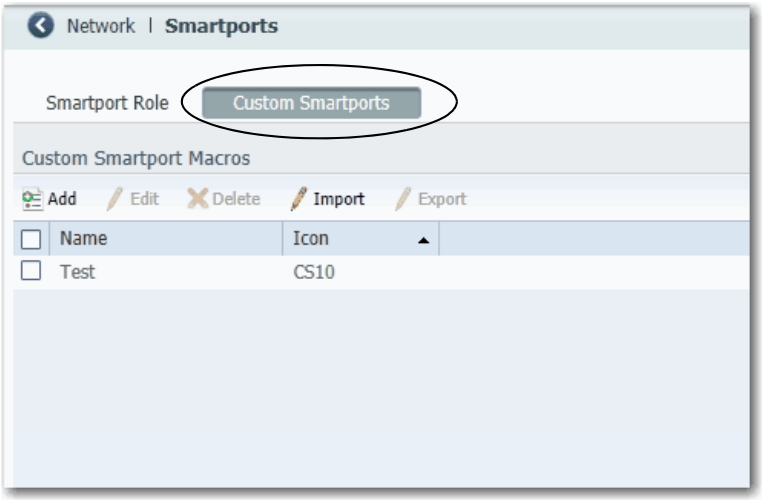
   The definition can contain up to 3000 characters. Enter the antimacro commands with one command per line. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro.

7. Click Submit.
8. To discard any unsaved changes, click Cancel.

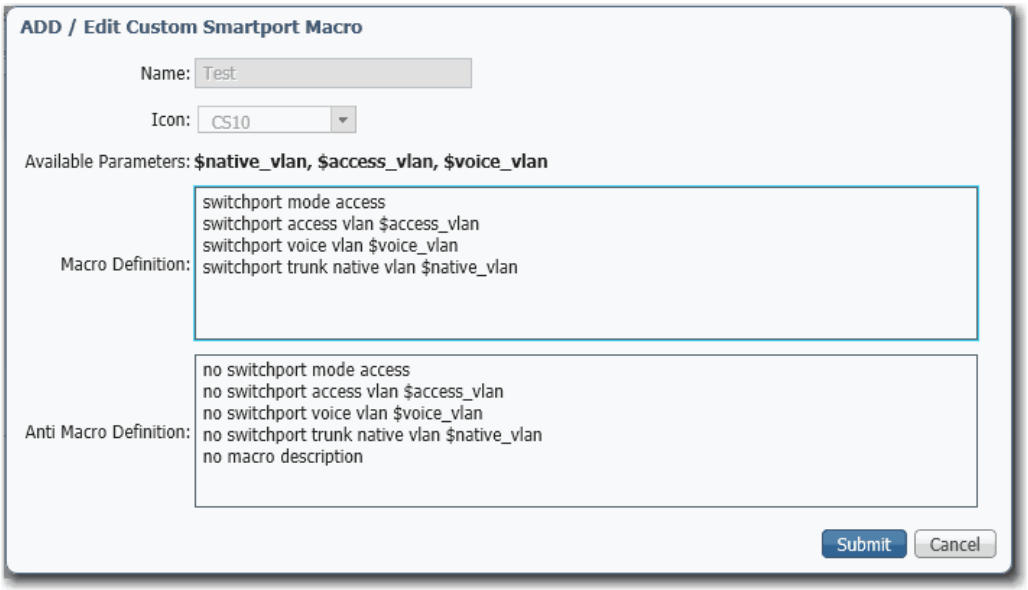
Modify the Definition of a Custom Smartports Macro

You cannot modify a custom Smartports macro that is 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.

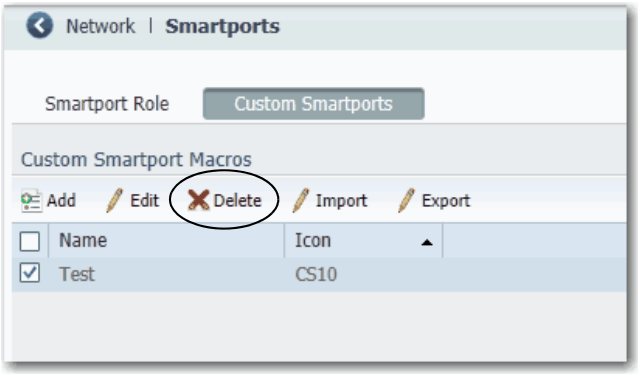


5. Change the definitions as needed.
6. Click Submit.

Delete a Custom Smartports Macro

You cannot delete a custom Smartports macro that is in use.

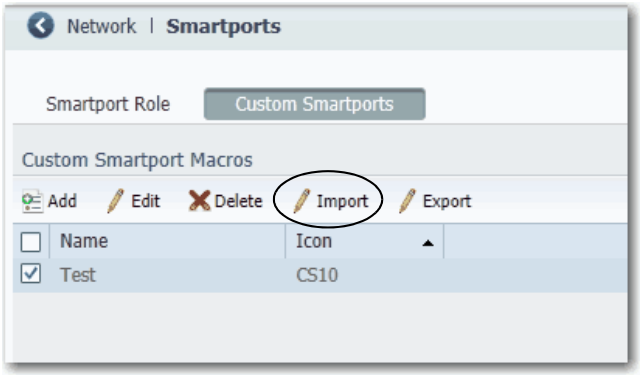
1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.
3. Check the checkbox next to the macro to delete.



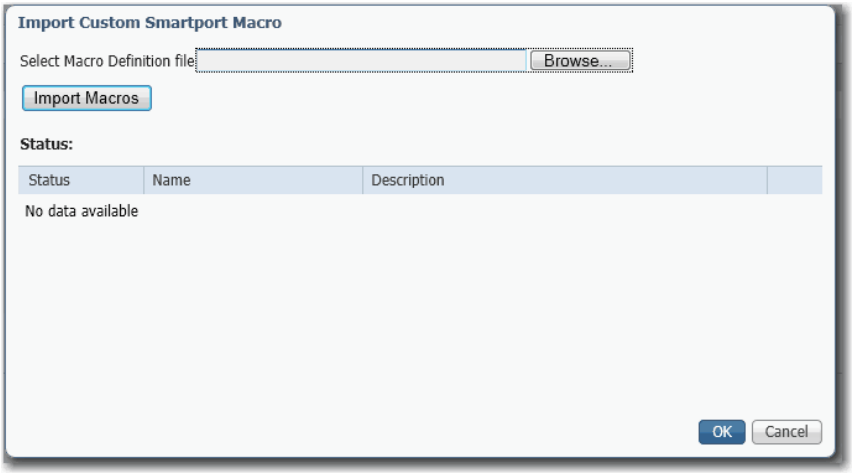
4. Click Delete.

Import a Custom Smartports Macro

1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.
3. Click Import.



4. Click Browse.

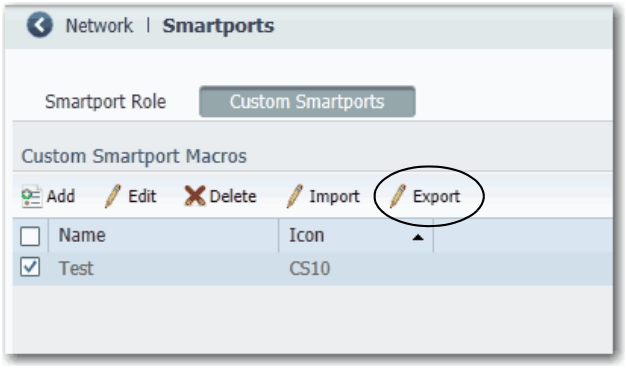


5. Select the macro file on your computer or network drive.

   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.



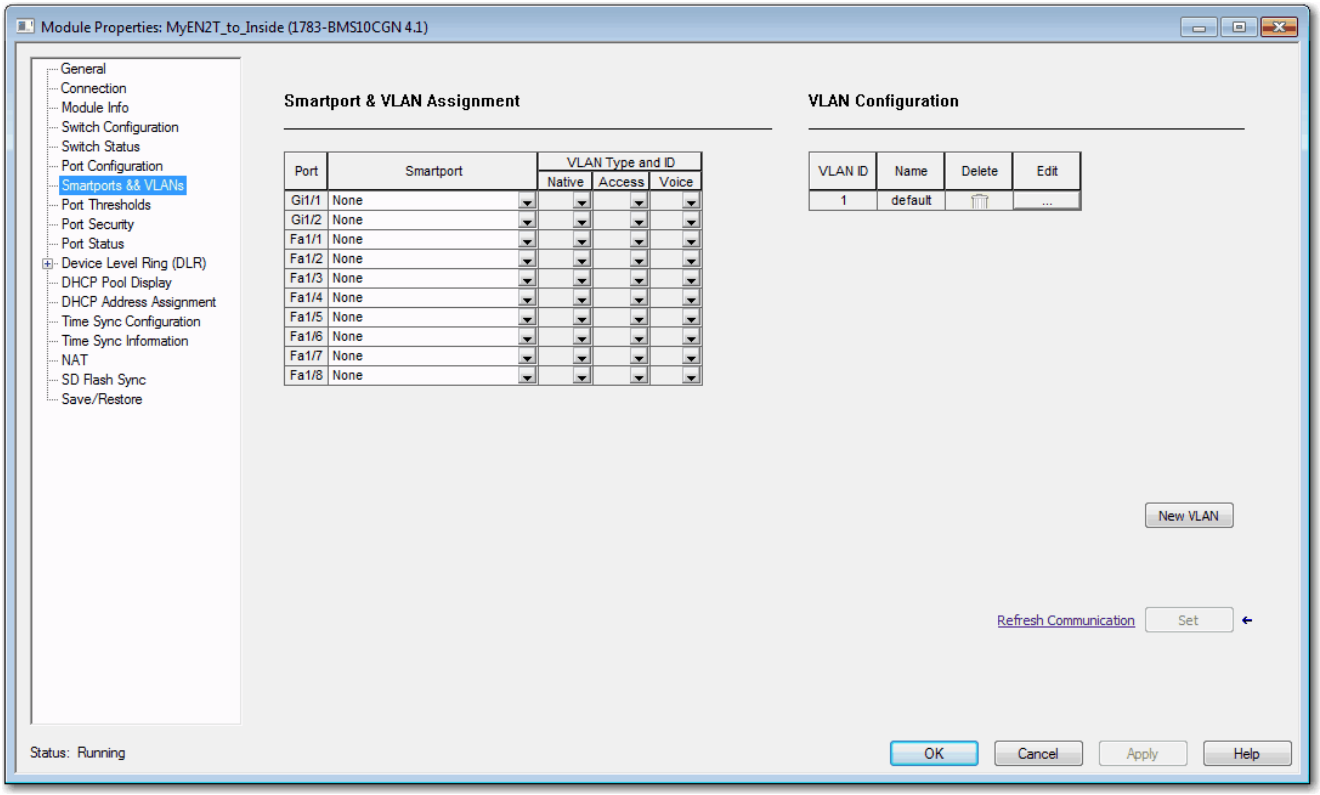
5. Save the resulting file.

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 270.

Figure 37 - Smartport & VLAN Assignment



For Stratix 8000/8300 switches, in the navigation pane, click Advanced Port Configuration.

Figure 38 - Advanced Port Configuration for Stratix 8000/8300 Switches

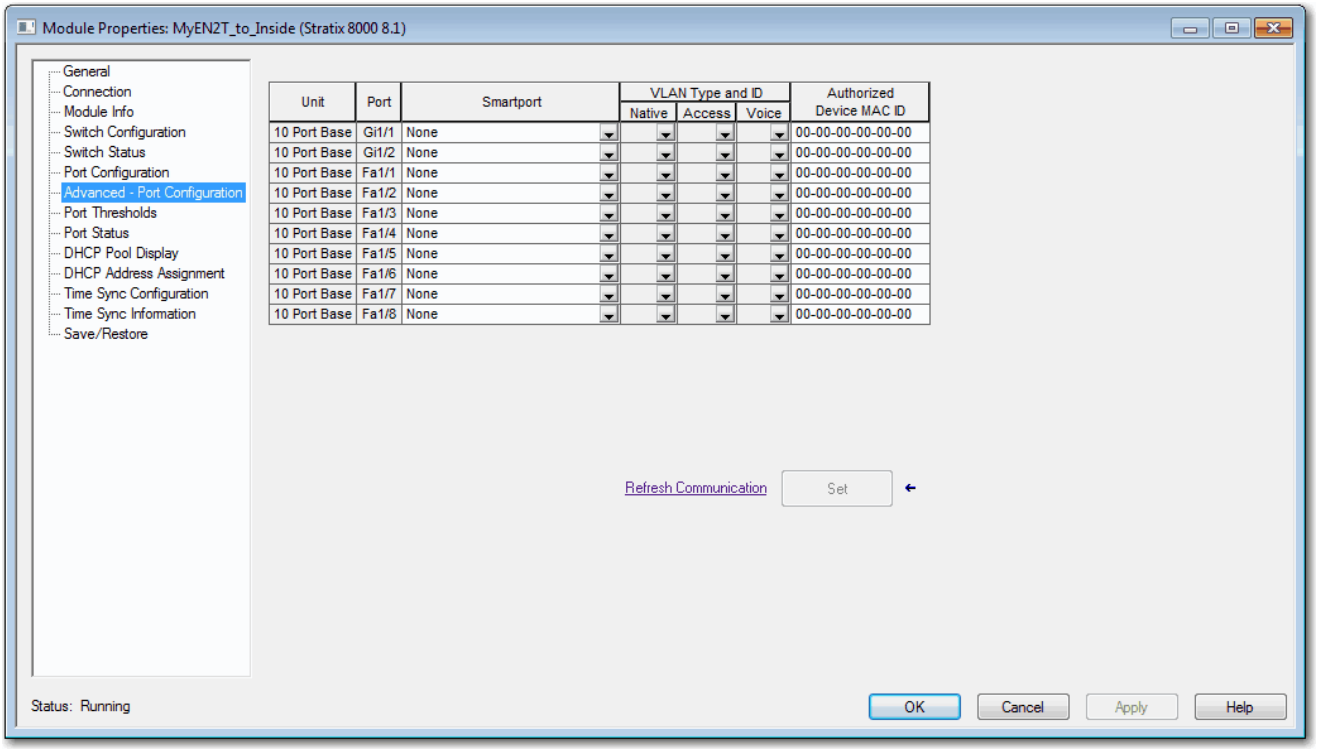


Table 123 - Smartport and VLAN Assignment Fields

Field	Description
Unit (Stratix 8000/8300 switches)	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	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 122 on page 262. The Smartport roles are recommended configurations for the ports. These configurations are referred to as port roles. They optimize the switch connections and help verify security, transmission quality, and reliability to traffic from the switch ports. These configurations also help to 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. Be 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 multiple 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 to make sure 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 223.

Spanning Tree Protocol (STP)

STP, the IEEE 802.1D bridge protocol, is a Layer 2 link management protocol that provides path redundancy and helps to prevent loops in the network. The switch supports the following STP versions:

- Multiple Spanning Tree Protocol (MSTP) based on the IEEE 802.1s standard.

  MSTP uses Rapid Spanning Tree Protocol (RSTP) for rapid convergence. This mode maps a group of VLANs into a single spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning tree instances required to support many VLANs. MSTP is the default STP mode.

- Per VLAN Spanning Tree Plus (PVST+) protocol based on the IEEE 802.1D standard.

  PVST+ runs on each VLAN on the switch up to the maximum supported, to help create a loop-free path through the network. PVST+ provides Layer 2 load balancing for the VLAN on which it runs. You can create different logical topologies by using the VLANs on your network to make sure that all of your links are used but that no one link is oversubscribed. Each instance of PVST+ on a VLAN has a single root switch. This root switch propagates the spanning-tree information that is associated with that VLAN to all other switches in the network. Because each switch has the same information about the network, this process maintains the network topology.

- Rapid per VLAN Spanning Tree Plus (Rapid PVST+) protocol based on the IEEE 802.1w standard.

  RPVST+ is the same as PVST+ except that it uses a rapid convergence that is based on the IEEE 802.1w standard. To provide rapid convergence, the rapid PVST+ immediately deletes dynamically learned MAC ID entries on a per-port basis upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC ID entries. Only one version can be active on the switch at any time. For example, all VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.

In MSTP mode, the switch supports a maximum of 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

In PVST+ or rapid-PVST+ mode, the switch supports a maximum of 128 spanning tree instances.

We recommend that you leave STP enabled to help prevent network loops and provide a redundant path if the active path becomes unavailable.

IMPORTANT To disable STP can affect connectivity to the network.

Configure STP via Device Manager

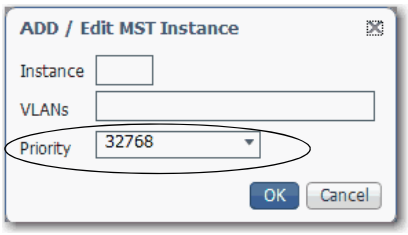
From the Configure menu, choose STP Settings.

Global Settings

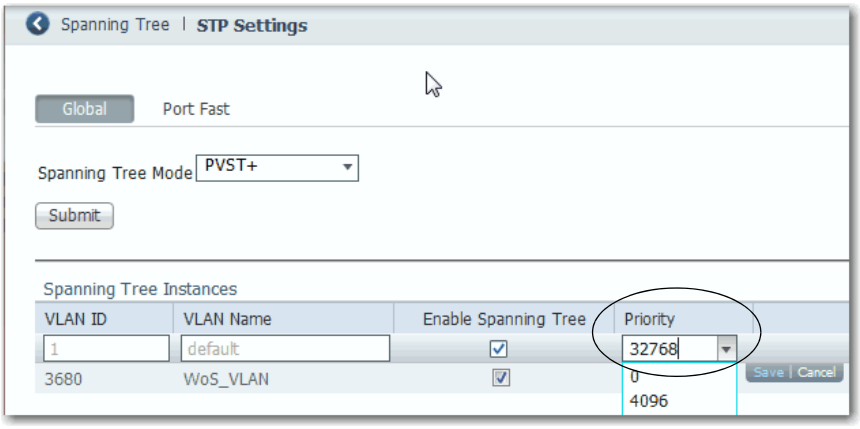
On the Global tab, you can choose an STP mode and configure spanning tree instances.

For each VLAN or VLAN group, the switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC ID in the VLAN becomes the root switch:

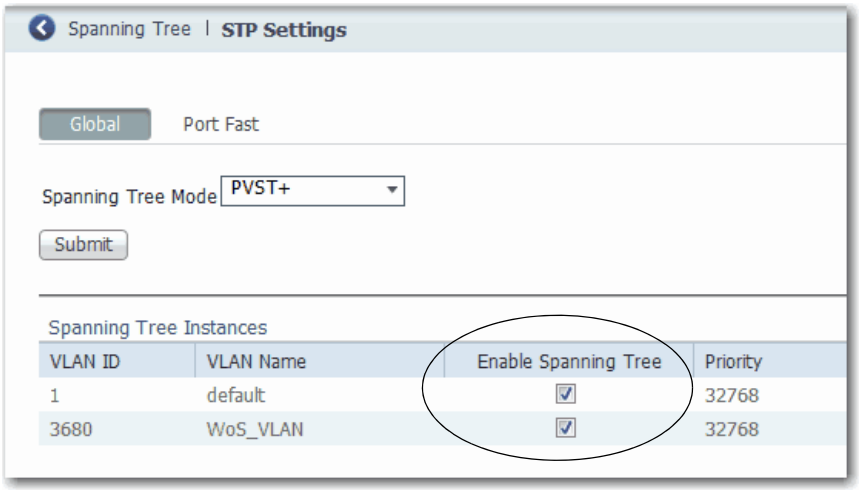
- For MST mode, you can choose a priority value when adding or editing an MST instance.



- For PVST+ or Rapid PVST+ modes, you can choose a priority value for each VLAN in the Spanning Tree Instances table.

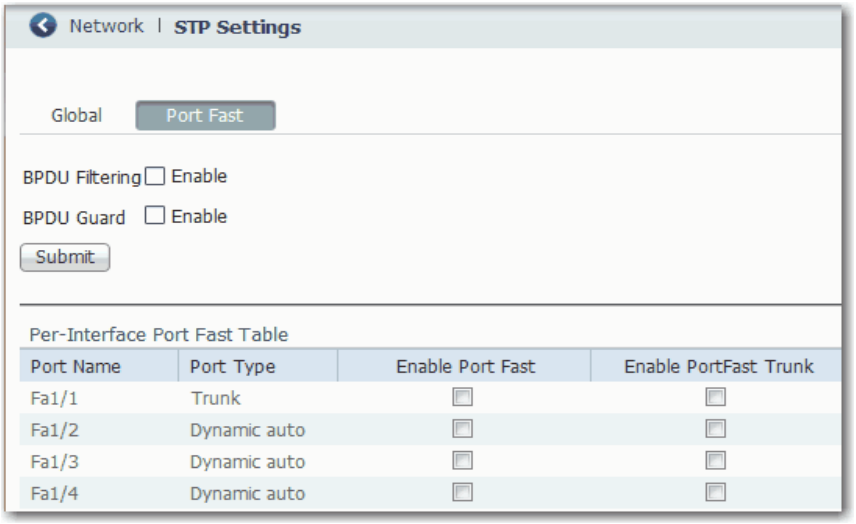


For PVST+ or Rapid PVST+ modes, you can enable or disable STP on each VLAN.



PortFast Settings

On the PortFast tab, you can change the way that STP is implemented on individual ports.



PortFast features are typically enabled on only 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.

IMPORTANT In a PRP system, PortFast must be enabled on downlink ports for infrastructure switches in LAN A, LAN B, and the RedBox. BPDU Filtering must be enabled on the RedBox.

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 help prevent a rogue device from interfering with your STP topology. However, we recommend that you use these features with caution:

- BPDU Filtering—This PortFast feature blocks the send and receipt of BPDUs through all 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.
- BPDU Guard—This PortFast feature shuts down a port if it receives a BPDU.

If you enable both of these features, BPDU Guard has no effect because BPDU Filtering helps prevent the port from receiving any BPDUs.

Per Interface PortFast Table

Spanning tree requires a port 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 connection.

To enable PortFast and apply the selected BPDU features to a port, select the port and do one of the following:

- If the Administrative mode for the port is Access, check Enable Port Fast.
- If the Administrative mode for the port is Trunk or Dynamic Auto, check Enable PortFast Trunk.

For more information about the Administrative mode for ports, see Configure Port Settings on page 45.

When applied to a port, these Smartport roles automatically enable PortFast:

- Automation Device
- Multiport Automation Device
- Desktop for Automation
- Virtual Desktop for Automation
- Router for Automation
- Phone for Automation

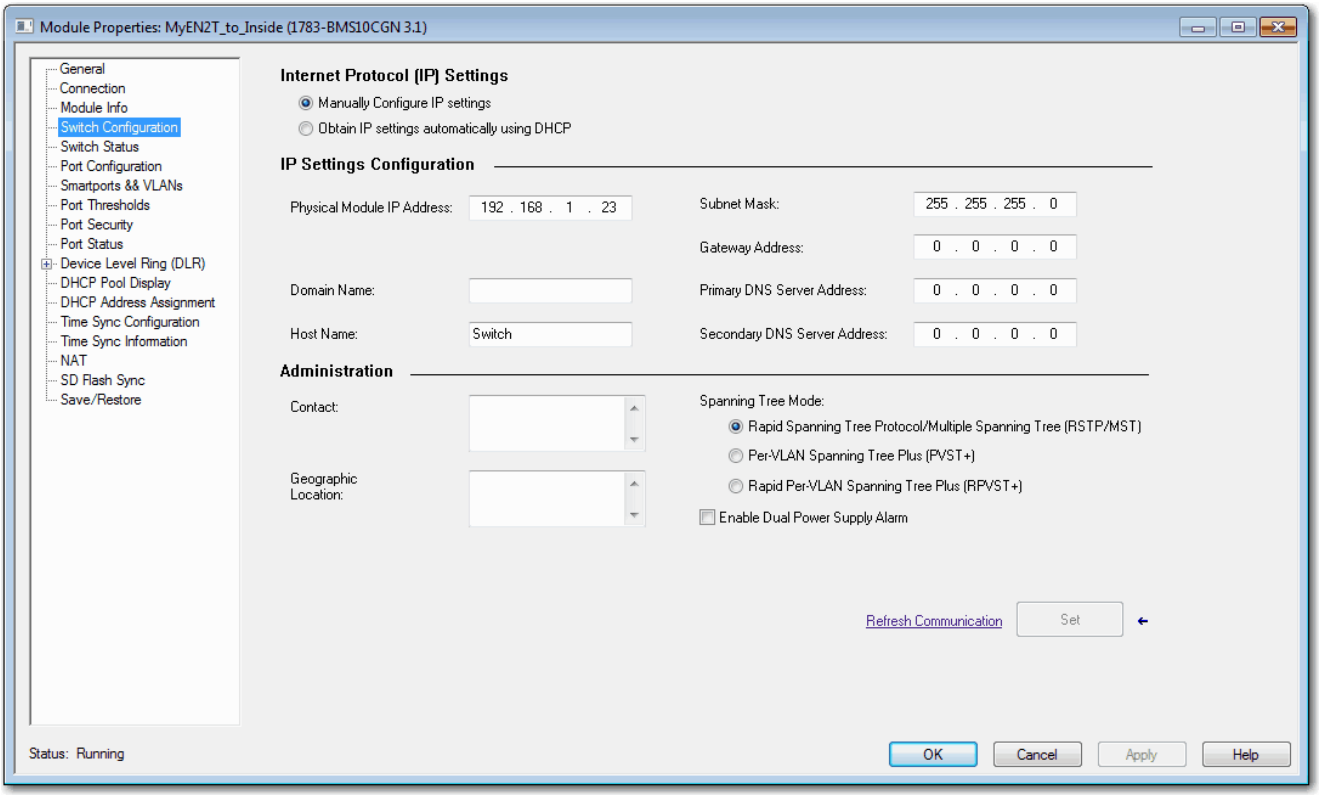
Configure STP via the Logix Designer Application

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 choose an STP mode. MST/RSTP is the default mode. For more information about each mode, see page 272.

Figure 39 - Switch Configuration for Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 Switches



Utility Features

GOOSE Messaging Support

GOOSE (Generic Object Oriented Substation Events) messaging is available on Stratix 5400 switches. GOOSE is defined in International Standard IEC 61850-8-1.

GOOSE messaging provides support for classification and prioritization of GOOSE messages via QoS.

For instructions on how to configure GOOSE messaging via the CLI, refer to documentation available at http://www.Cisco.com.

SCADA Protocol Classification

SCADA (Supervisory Control and Data Acquisition) Protocol Classification is available on Stratix 5400 switches.

SCADA Protocol Classification provides support for classification and prioritization of MODBUS TCP messages via QoS.

For instructions on how to configure SCADA via the CLI, refer to documentation available at http://www.Cisco.com.

IEEE 1588 Power Profile

Information about IEEE 1588 Power Profile can be found in the CIP Sync Time Synchronization (Precision Time Protocol) section of this document, on page 93.

Virtual Local Area Networks (VLANs)

A VLAN is a logical segment of the network that isolates traffic types and helps prevent collisions among data packets. The isolation of different types of traffic helps to preserve the quality of the transmission and to minimize excess traffic among the logical segments. VLANs also reduce the amount of administrative effort that is required to examine requests to network resources.

You can assign each switch port to a VLAN as described on page 265:

- Devices that are attached to switch ports with the same VLAN can communicate only with each other and can share data.
- Devices that are attached to switch ports with different VLANs cannot communicate with each other through the switch, unless the switch is configured for routing.
- All ports are initially assigned to the default VLAN, which is VLAN 1.

IMPORTANT A Layer 3 switch or router must be configured to enable routing across multiple VLANs and additional security policies must be set.

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 that VLAN assignments are correct.

IMPORTANT	If your network uses a DHCP server, be sure that the server can access all devices in all VLANs.

We recommend that you first determine your VLAN needs before creating VLANs. For more information about VLANs, refer to these publications:

- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001
- Ethernet Design Considerations, publication ENET-RM002

The switch supports a maximum of 255 VLANs, including the default VLAN. Each VLAN has a name and ID number. The ID can be from 1...1001 and 1005...4094.

With custom Smartport roles, you can specify the type of VLAN you want to implement on a port. For more information about custom Smartport roles, see page 263.

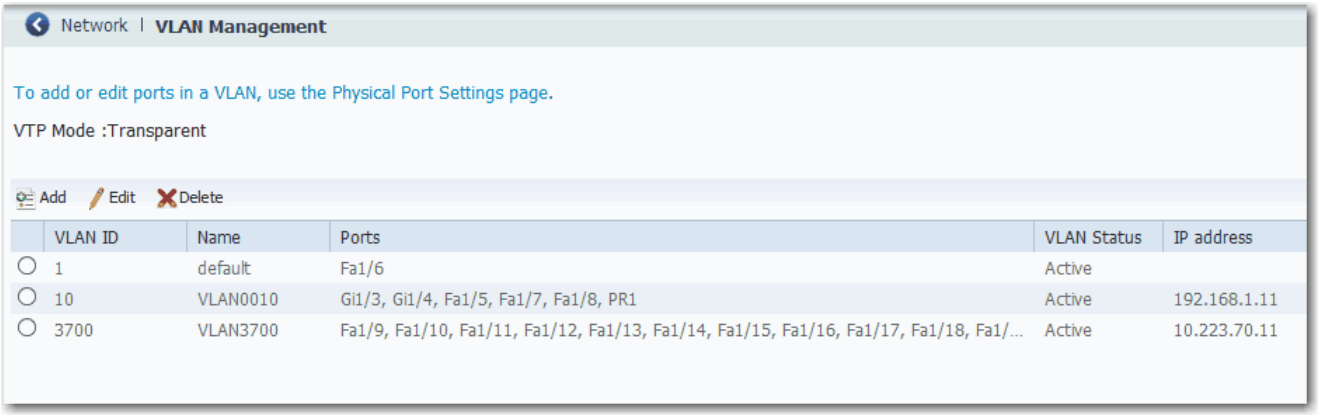
Management VLAN

VLAN 1 is the default VLAN and 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. You can assign a management VLAN on the Express Setup page in either Device Manager or the Logix Designer application.

Configure VLANs via Device Manager

From the Configure menu, choose VLAN Management.

You can add, edit, and delete VLANs.



To assign a VLAN to a port when applying a Smartport role, see page 265.

To assign a VLAN to a port from the Port Settings page, see page 45.

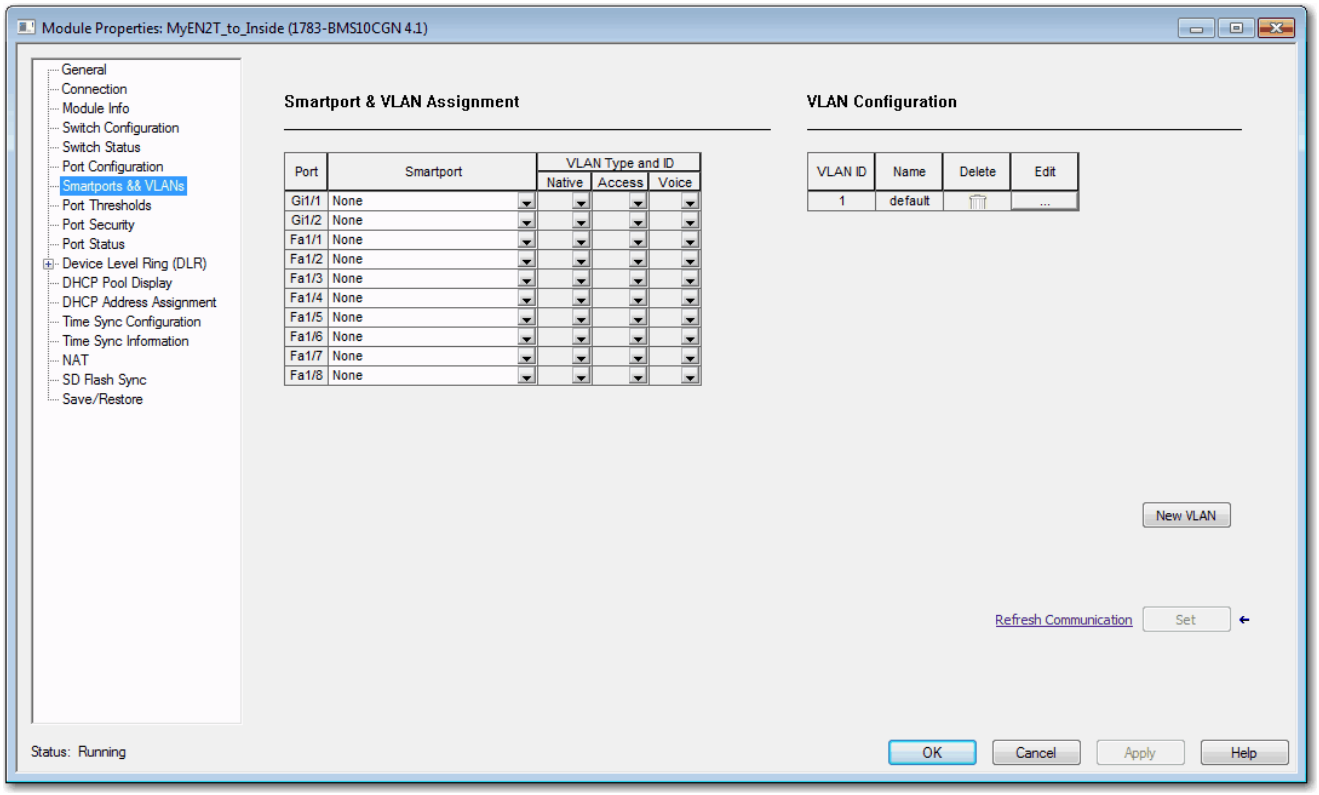
Configure VLANs via the Logix Designer Application

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 40 - VLAN Configuration for Stratix 5400, Stratix 5410, Stratix 5700, and ArmorStratix 5700 Switches



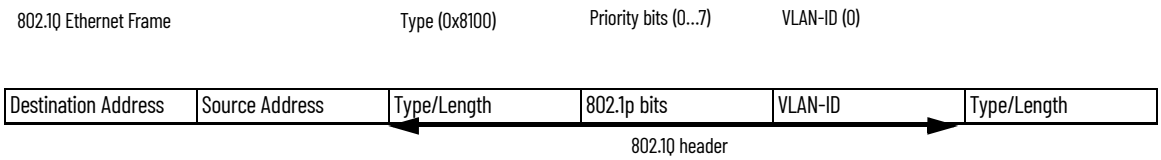
To assign ports to VLANs, see Assign Smartports and VLANs via the Logix Designer Application on page 270.

VLAN 0 Priority Tagging

VLAN 0 priority tagging enables 802.1Q Ethernet frames to be transmitted with the VLAN ID set to zero. For example, you can use this feature to forward PROFINET traffic through the switch. These frames are called priority tagged frames. Set the VLAN ID tag to zero to allow the VLAN ID tag to be ignored and the Ethernet frame to be processed according to the priority configured in the 802.1P bits of the 802.1Q Ethernet frame header.

802.1Q Tagging

The 802.1Q standard defines a system of VLAN tagging for Ethernet frames and also contains a provision for a Quality of Service (QoS) prioritization scheme that is known as 802.1P, which indicates the priority level of the frame. The 802.1Q standard adds this information to the Ethernet header, as shown in the figure. The priority level values range from zero (best effort) to seven (highest). These values can be used to prioritize different classes of traffic. The VLAN ID tag specifies the VLAN to which the frame belongs. The priority bits define the priority with which the frames are processed.



Native VLANs

When a particular VLAN ID is assigned as a native VLAN on an Ethernet interface, frames in the native VLAN transmitted from the Ethernet interface are not tagged. Similarly, any untagged frames that are received on the Ethernet interface are associated with the native VLAN on that interface. The Ethernet interface can still receive both tagged and untagged frames. The tagged frames are associated with the VLAN ID in the 802.1Q header (see above). Untagged frames do not contain priority bits in the Ethernet frame header and are treated as best effort. On ingress, Ethernet packets that are tagged with VLAN 0 are associated with the native VLAN of the interface.

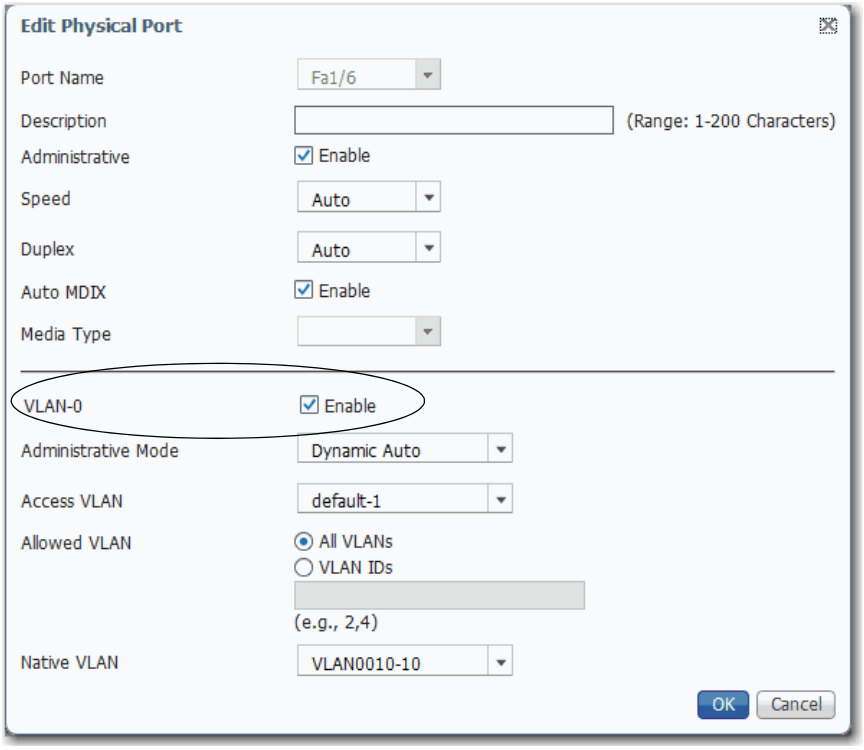
VLAN 0 Priority Tagging and Priority Values

When VLAN 0 priority tagging is configured on the interface, the 802.1P priority bits are retained on ingress for the VLAN 0 tagged Ethernet frames. To retain the 802.1P priority bits of the VLAN 0 Ethernet packets on egress, the egress interface must be in trunk mode, and the native VLAN cannot be the same native VLAN as the ingress interface. When these frames are received at the destination, the header is stripped off and the frame is processed as per the configuration of the 802.1P priority bits. If the VLAN ID has a nonzero value, the header is retained and the frame is transmitted to the specified VLAN. High priority frames are sent ahead of low-priority frames.

Configure VLAN 0 Priority Tagging

All switches support VLAN 0 priority tagging:

- In IOS Release 15.2(6)E0a and later, you can enable or disable VLAN 0 on the Edit Physical Port page in Device Manager as described on page 45. By default, VLAN 0 is enabled.



- In IOS Release 15.2(5)EA.fc4 and earlier, you must use the CLI to enable VLAN 0 priority tagging. By default, VLAN 0 is disabled.

  To configure VLAN 0 tagging for PROFINET traffic via the CLI, see page 241.

Chapter 4

Monitor the Switch

Topic	Page
Switch Status via Device Manager	283
Switch Status via the Logix Designer Application	296
System Log Messages	300
Trends	301
Port Statistics	302
NAT Statistics	303
NetFlow	309
REP Status	311
CIP Status	311
DHCP Clients	313
DLR Status	313
PRP Status	317
PTP Serviceability	320
STP Status	325
Port Diagnostics	327
Neighbors	329
Cable Diagnostics	330

Switch Status via Device Manager

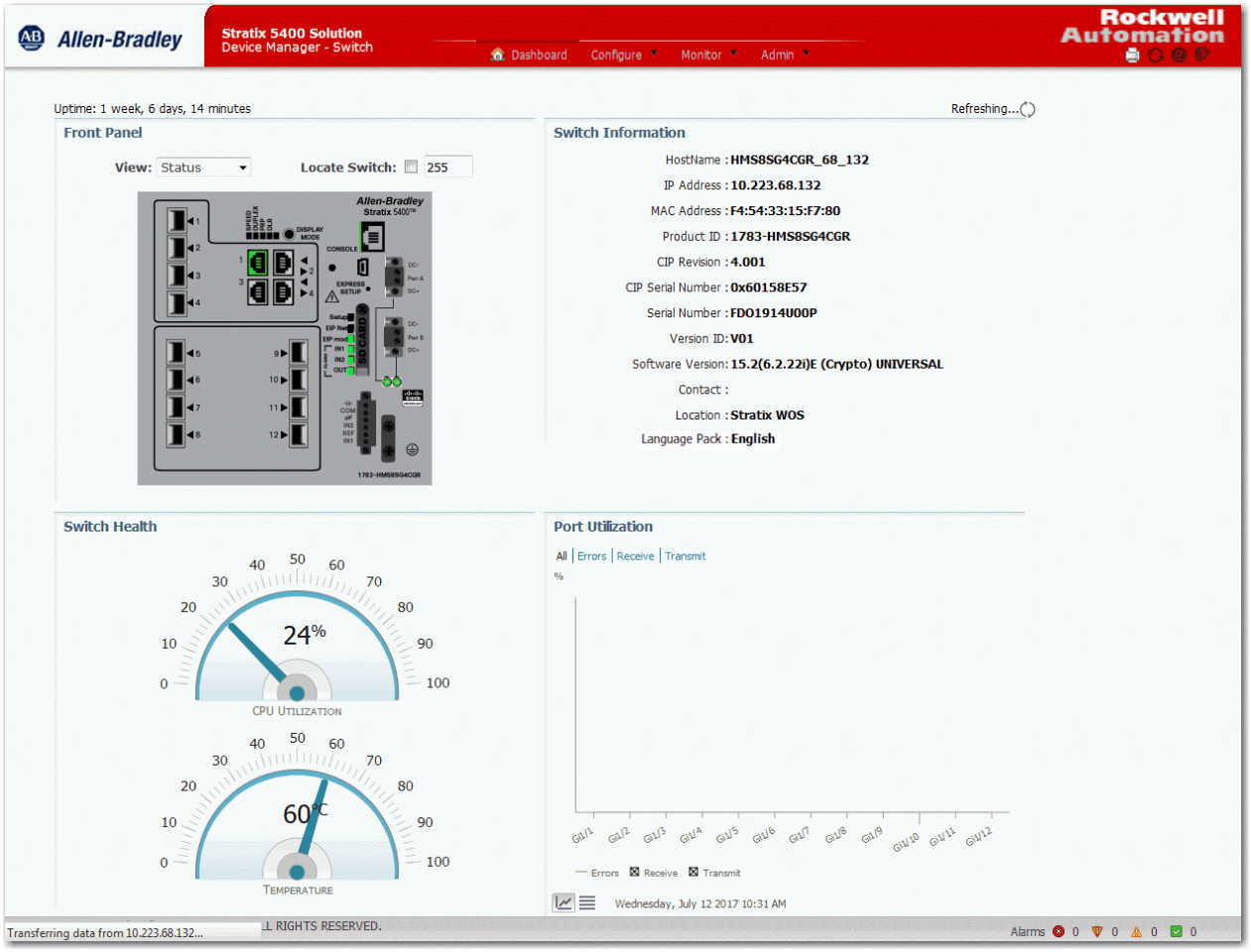
The Dashboard page in Device Manager lets you monitor switch status and performance.

The Dashboard page is similar to the Monitor > Trends page. The Dashboard page displays the instantaneous status while the Trends page 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 page, see page 301.

The Front Panel has four areas to monitor the status of the switch:

- Front Panel as described on page 284
- Switch Information as described on page 294
- Switch Health as described on page 294
- Port Utilization as described on page 295

Figure 41 - Dashboard Window

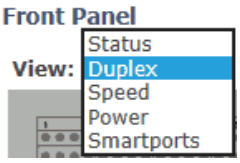


Front Panel

The Front Panel view on the dashboard is a graphical display of the switch front panel, with color-coded switch components that indicate status. The status indicators on the view in Device Manager match the status indicators on the physical switch:

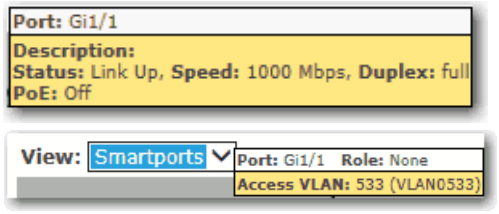
- System status indicators let you monitor the status of the switch, network status, power, and alarms.
- Port status indicators let you monitor the status of each port. Each combo port has two indicators: one for the SFP module and one for the RJ45 connector. You can change the behavior of the port 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 42 - Front Panel View Menu



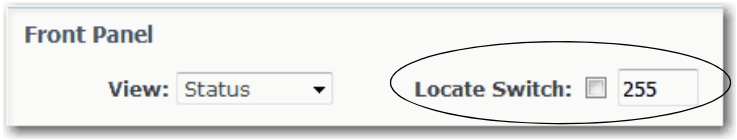
To display specific information about the port and its status, hover your mouse pointer over a port image. When you choose Smartports from the View pull-down menu, the hover text for a port image shows the Smartport role and VLAN assigned to the port.

Figure 43 - 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.

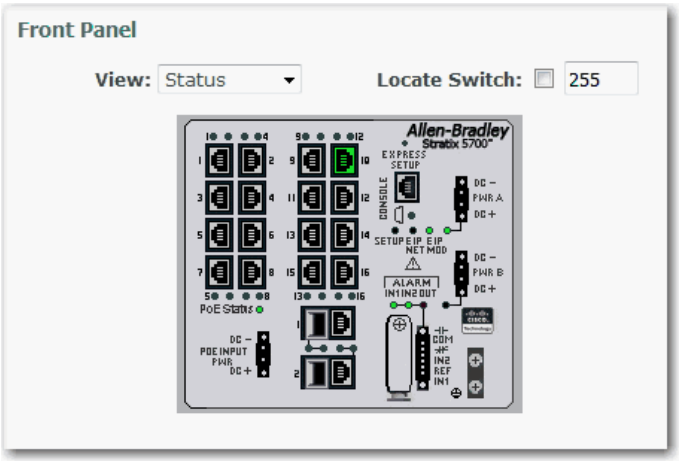
Figure 44 - Locate Switch Checkbox



When you check the Locate Switch checkbox, the system status indicators on the physical switch (Setup, EIP NET, EIP Mod, Alarm) flash green to indicate 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

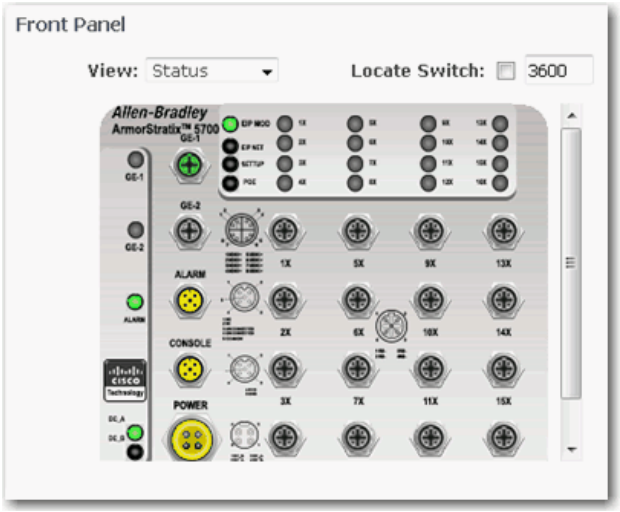


Table 124 - Stratix 5700 and ArmorStratix 5700 System Status Indicators

Indicator	Status	Description
Setup	The Setup status indicator shows the status of the initial setup of the switch. The behavior of the Setup status indicator varies depending on whether you run single-mode or multi-mode Express Setup. In multi-mode Express Setup, the behavior varies based on whether you run Short Press, Medium Press, or Long Press mode. For details about the Setup status indicator behavior during Express Setup, refer to Chapter 2, Get Started.	
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 is detected.
	Flashing red	Major alarm is detected.
	Solid red	Minor alarm is 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.

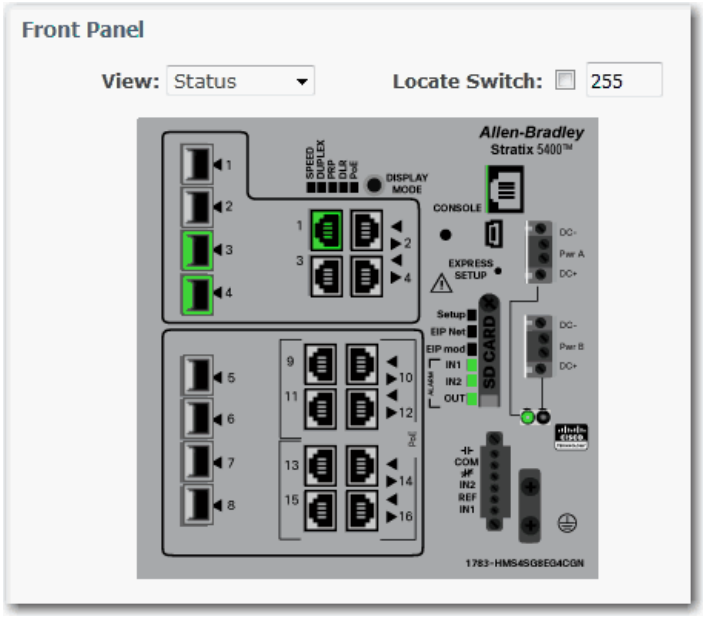
Table 125 - Stratix 5700 and ArmorStratix 5700 Port Status Indicators

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 is 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.	

Table 125 - Stratix 5700 and ArmorStratix 5700 Port Status Indicators (Continued)

Mode	Status	Description
	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



Along with the View modes on the Dashboard page, 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. 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 127.

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 45 - Stratix 5400 Display Modes

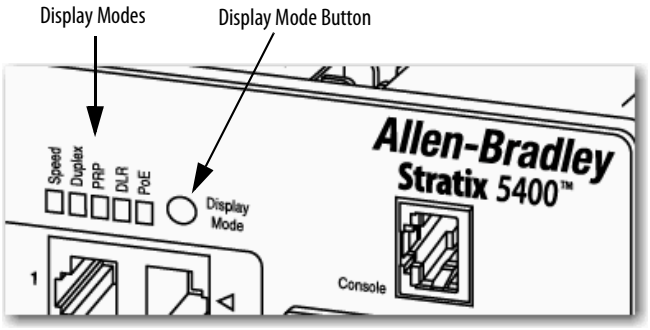


Table 126 - Stratix 5400 System Status Indicators

Indicator	Status	Description
Setup	The Setup status indicator shows the status of the initial setup of the switch.The Setup status indicator shows the status of the initial setup of the switch. The behavior of the Setup status indicator varies depending on whether you run single-mode or multi-mode Express Setup. In multi-mode Express Setup, the behavior varies based on whether you run Short Press, Medium Press, or Long Press mode. For details about the Setup status indicator behavior during Express Setup, refer to Chapter 2, Get Started.	
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 is detected.
	Flashing red	Major alarm is detected.
	Solid red	Minor alarm is 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.

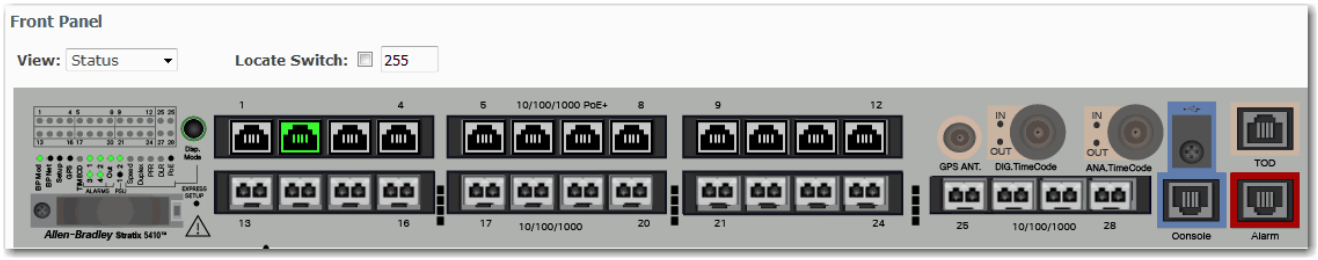
Table 127 - Stratix 5400 Port Status Indicators

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.	

Table 127 - Stratix 5400 Port Status Indicators

Mode	Status	Description
	Off	No link is 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 211.	
	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 page, 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 129.

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 46 - Stratix 5410 Display Modes

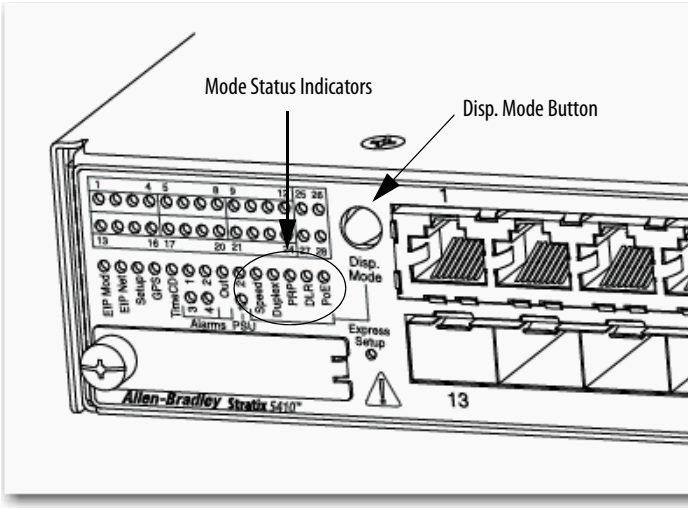


Table 128 - Stratix 5410 System Status Indicators

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. The behavior of the Setup status indicator varies depending on whether you run single-mode or multi-mode Express Setup. In multi-mode Express Setup, the behavior varies based on whether you run Short Press, Medium Press, or Long Press mode. For details about the Setup status indicator behavior during Express Setup, refer to Chapter 2, Get Started.	
GPS	Supported only on Stratix 5410 series B switches with IOS Release 15.2(6)E0a and later. Indicates the status of the global navigation satellite system (GNSS).	

Table 128 - Stratix 5410 System Status Indicators (Continued)

Indicator	Status	Description
	Off	GNSS is not operational.
	Solid green	• GNSS is in a normal state and Self-survey mode is complete. • GNSS has a valid signal.
	Flashing green	• GNSS is in Self-survey mode. • The signal is lost.
	Solid amber	• GNSS receiver firmware update is in process. After the GNSS receiver firmware update is complete, GNSS is reset and the status indicator flashes green as the self-survey process starts after reset. • A GNSS error occurred, such as antenna open, antenna shorted, or no tracking satellite.
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 is detected.
	Solid red	Minor alarm is detected.
	Flashing red	Major alarm is detected.
	Alternating green and red	Critical alarm is 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 is detected.
	Solid red	Alarm is 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 129 - 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 is 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 211.	
	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.

Table 129 - Stratix 5410 Port Status Indicators

Mode	Status	Description
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 is 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 is failing on this high priority port.
	Solid amber	PoE is enabled on the port, but has failures.

Stratix 8000/8300 Front Panel

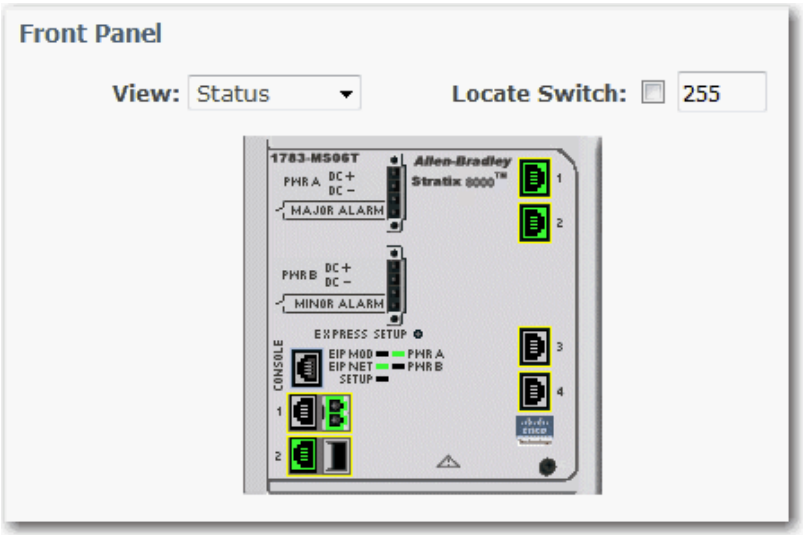


Table 130 - Stratix 8000/8300 System Status Indicators

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 300.
	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 300.
	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. The behavior of the Setup status indicator varies depending on whether you run single-mode or multi-mode Express Setup. In multi-mode Express Setup, the behavior varies based on whether you run Short Press, Medium Press, or Long Press mode. For details about the Setup status indicator behavior during Express Setup, refer to Chapter 2, Get Started.	
Pwr A and Pwr B	The Pwr status indicators show the DC power status.	

Table 130 - Stratix 8000/8300 System Status Indicators (Continued)

Indicator	Status	Description
	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 131 - 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 132 - 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 page.
IP Address	The IP address of this switch. You can configure this setting on the Admin > Express Setup page.
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 page.
Location	The physical location of this switch. You can set this parameter on the Configure > SNMP page.
Language Pack	The Language Pack is determined by the browser settings. Static data is localized.

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 301 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 302 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.

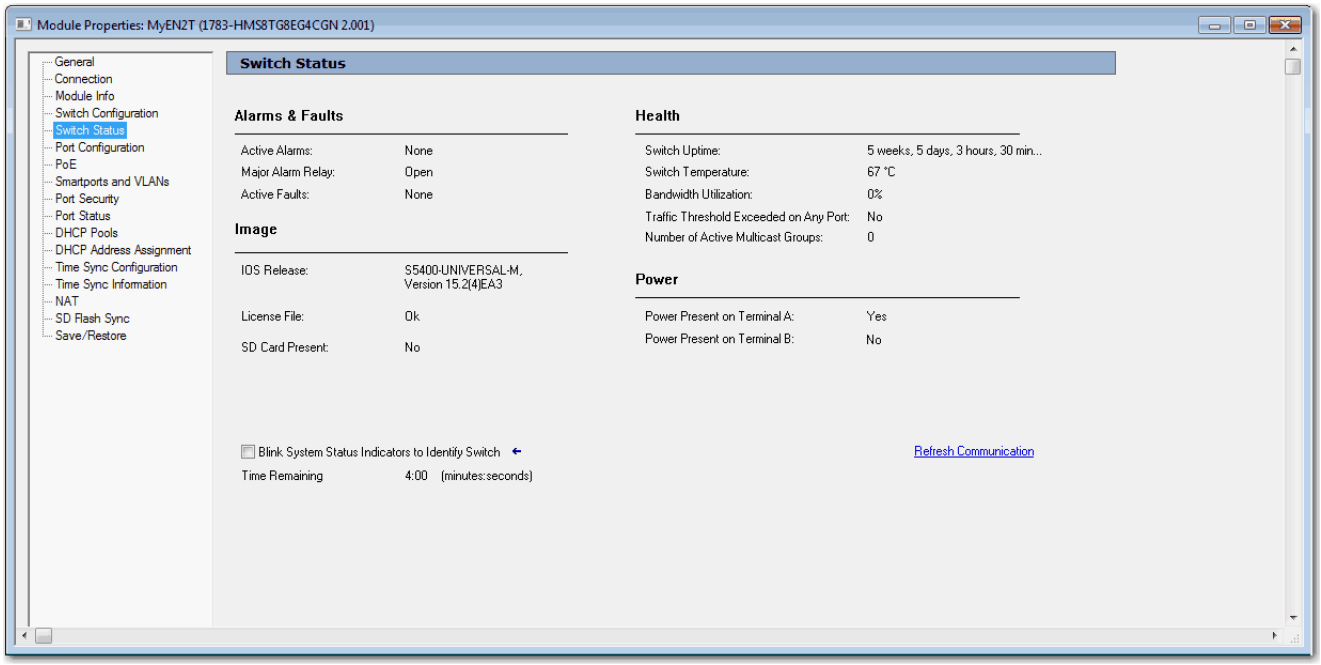


Table 133 - Switch Status Fields

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 Yes or No 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.
SD Card Present	Displays whether the SD card is installed.
Power	
Power Present on Terminal A	Displays Yes or No to indicate whether power is present on Terminal A.
Power Present on Terminal B	Displays Yes or No to indicate whether power is present on Terminal B.

Table 133 - Switch Status Fields (Continued)

Field	Description
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 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 that remains 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.

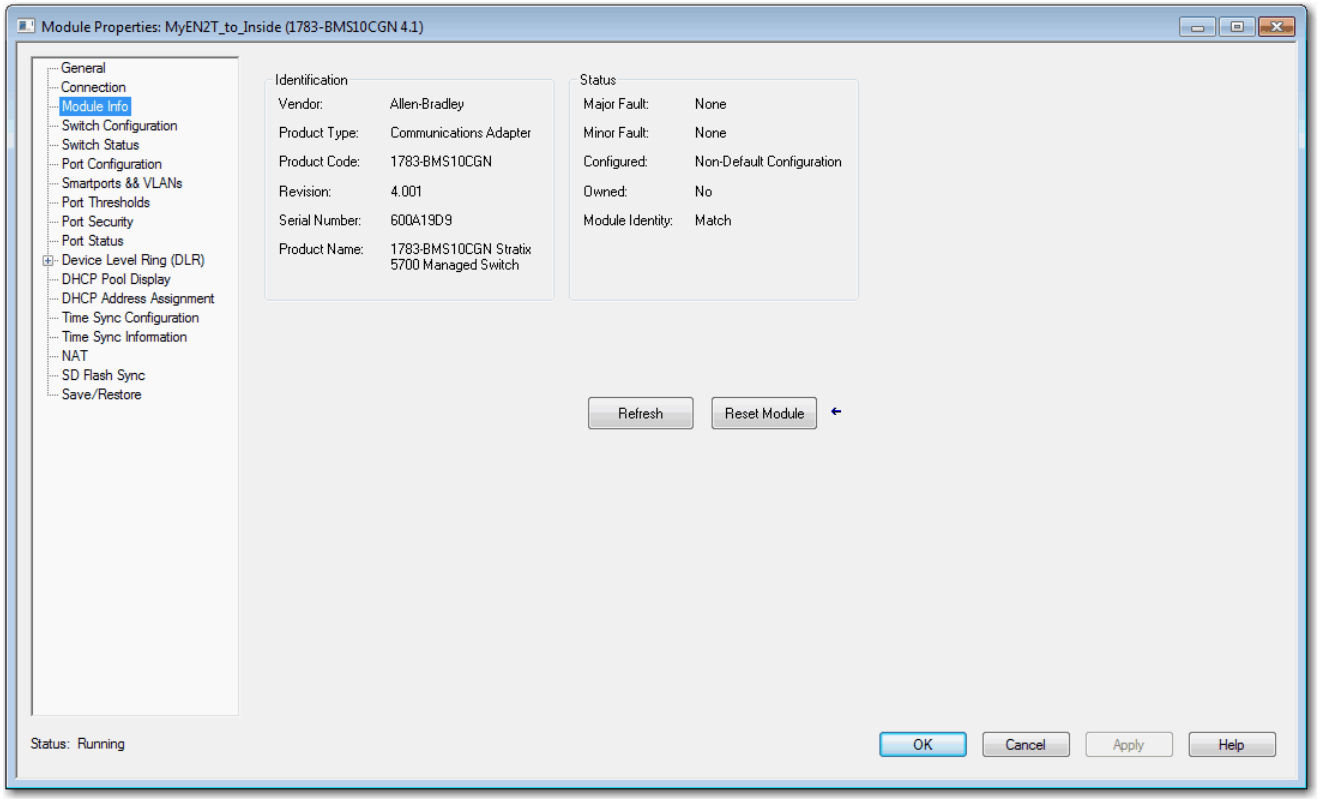


Table 134 - Module Info Fields

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 consider 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.

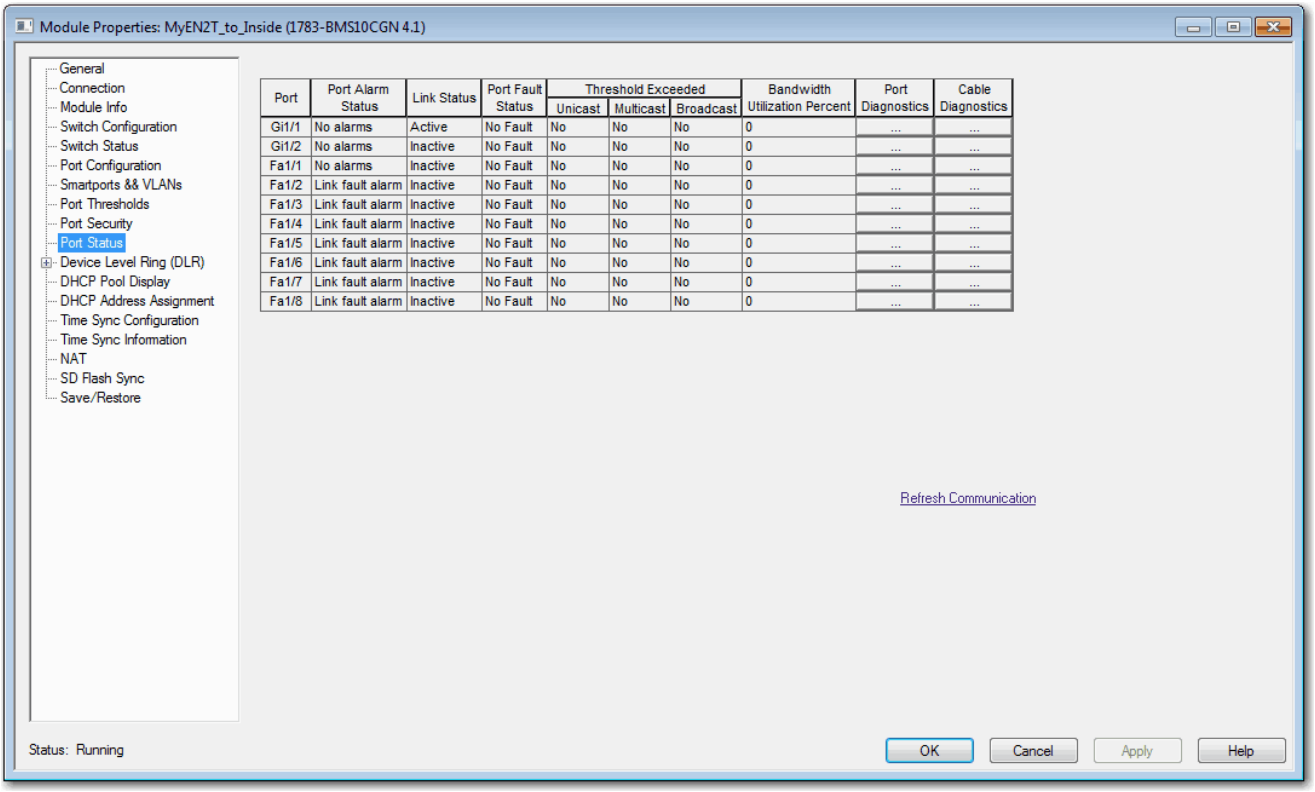


Table 135 - Port Status Fields

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
Threshold Exceeded	Displays unusual changes for these types of network traffic: • Unicast—Displays Yes or No to indicate whether the current unicast traffic has exceeded the threshold value. • Multicast—Displays Yes or No to indicate whether the current multicast traffic has exceeded the threshold value. • Broadcast—Displays Yes or No to indicate whether the current broadcast traffic has exceeded the threshold value.

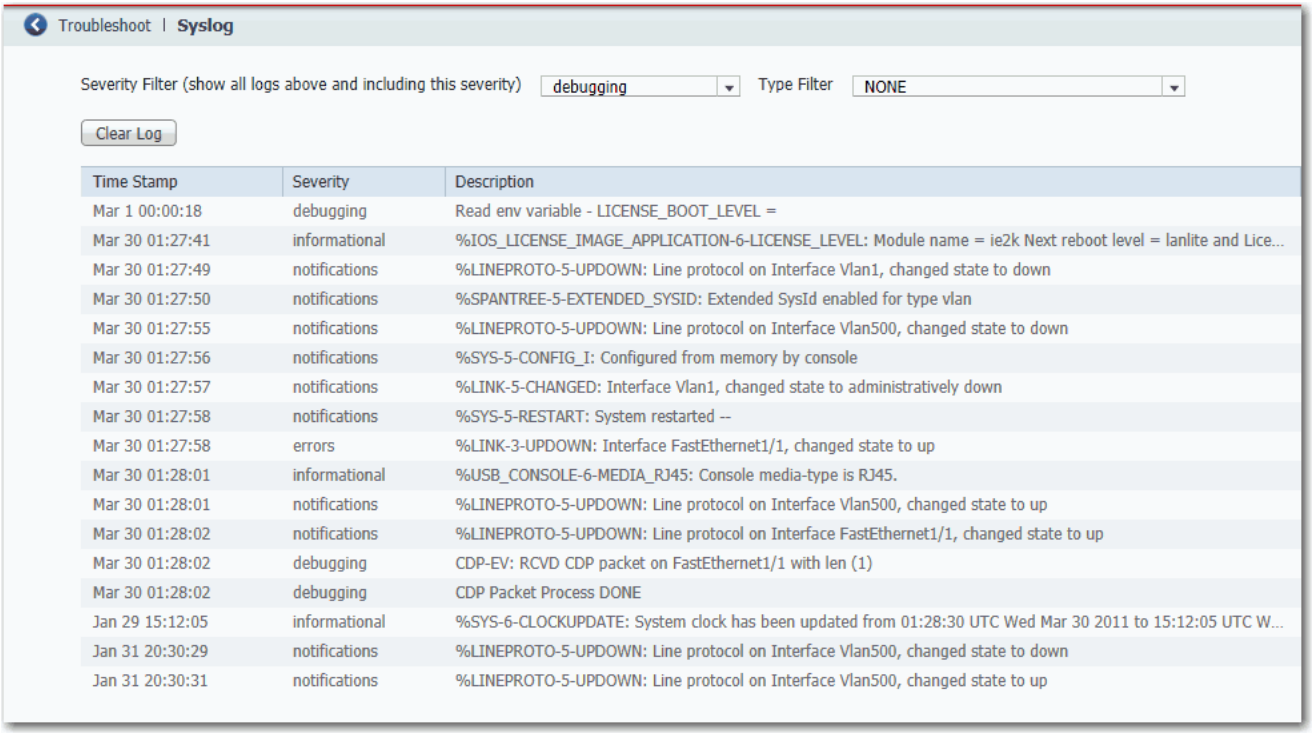
Table 135 - Port Status Fields (Continued)

Field	Description
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 325.
Cable Diagnostics	Click to display information to diagnose a cable issue for the corresponding port. See page 329.

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 page.

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 136 - Syslog Fields

Field	Description
Time Stamp	The date and time the event occurred. Use the Express Setup page 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.

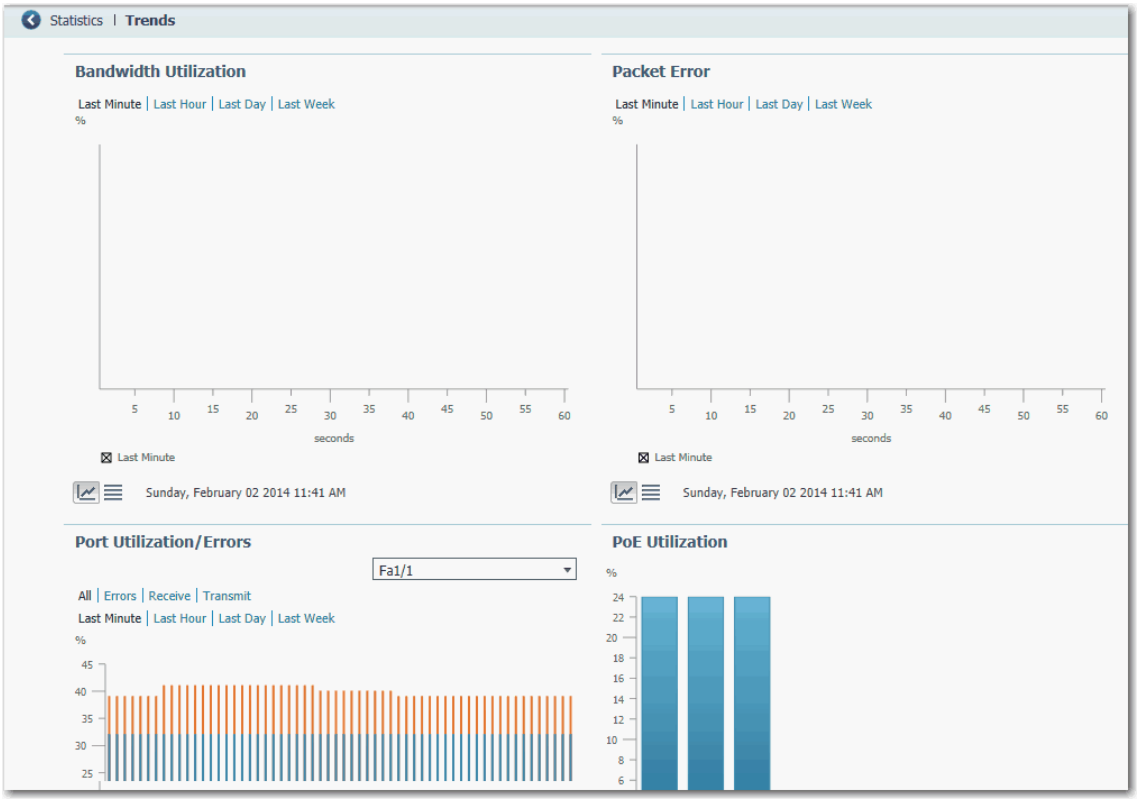


Table 137 - Trends Graphs

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. If you use Parallel Redundancy Protocol (PRP), ports that belong to a PRP channel configured on a RedBox are marked with an asterisk (*). For more information about configuring PRP channels, see page 214.

From the Monitor menu, choose Port Statistics.

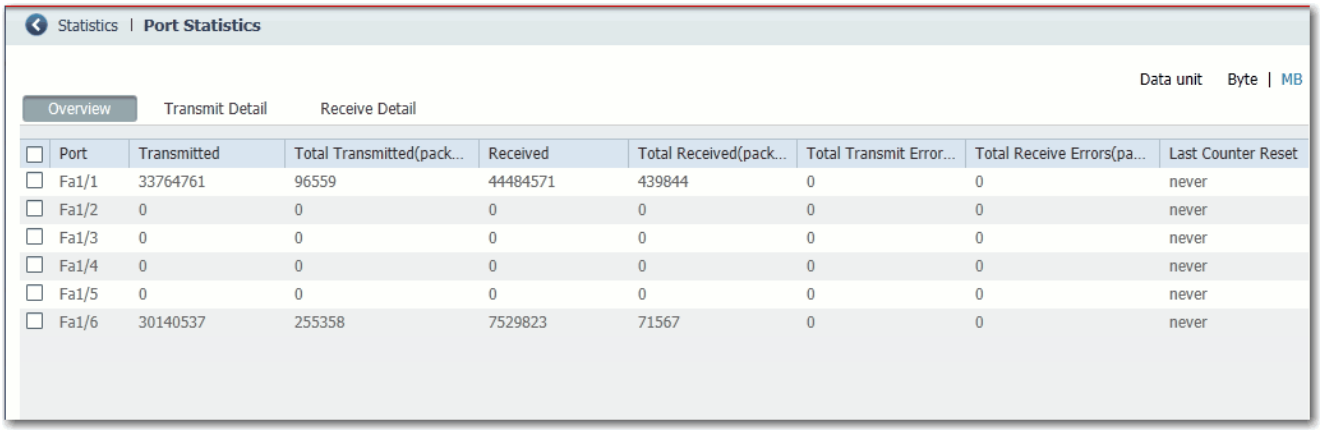


Table 138 - Port Statistics

Tab	Description
Overview	Displays 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	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	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 47 - NAT Statistics for Stratix 5400 and 5700 Switches

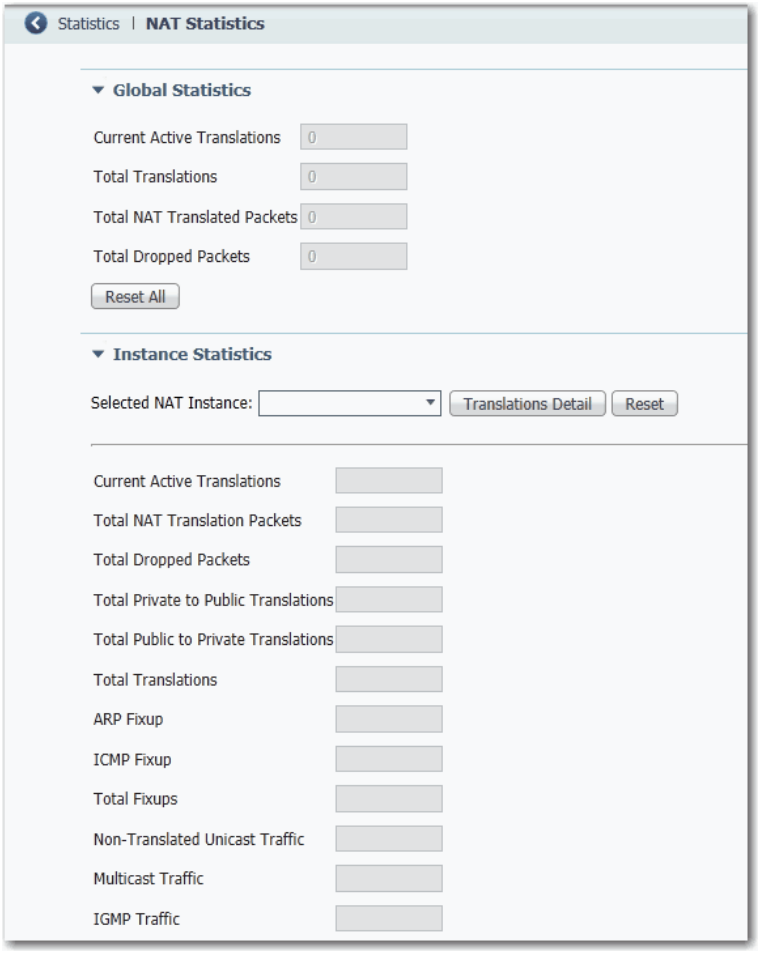


Figure 48 - NAT Statistics for Stratix 5410

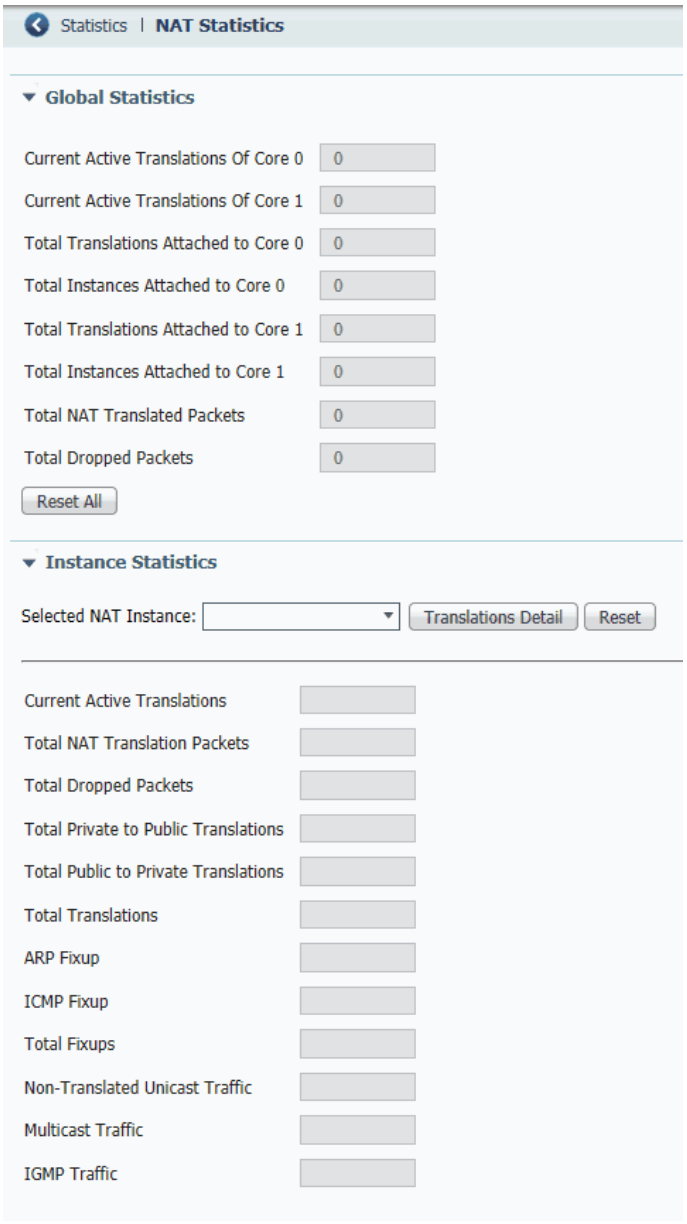


Table 139 - NAT Statistics

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.

Table 139 - NAT Statistics (Continued)

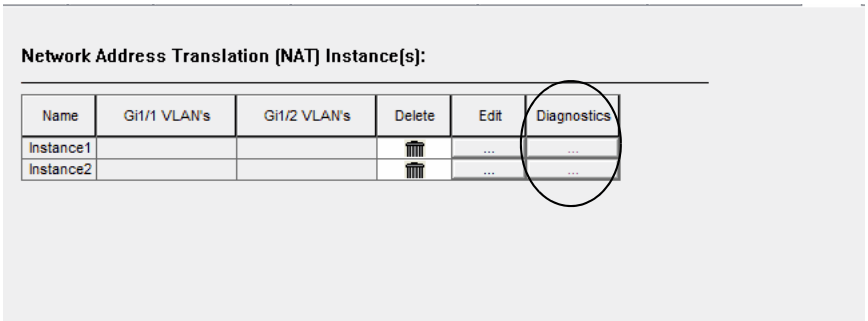
Field	Description
Total Dropped Packets	The total number of packets that have been dropped across all NAT instances for all ports.
Instance Statistics	
Selected Instance	From the pull-down menu, choose the instance for which to view statistics.
Current Active Translations	The number of translations that 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.

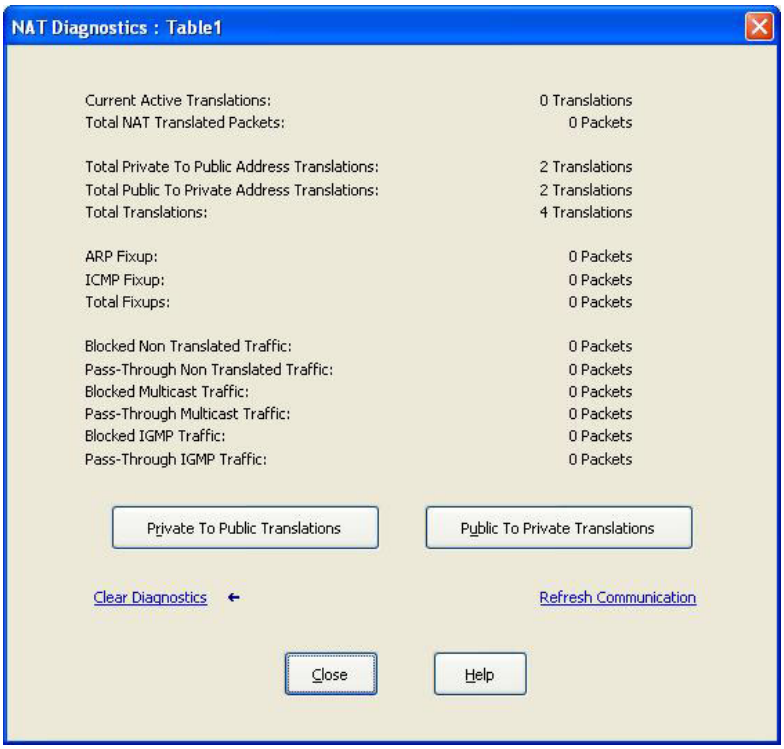


Table 140 - NAT Diagnostics per Instance

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. See Table 141.
Public to Private Translations	Click to view public-to-private translation diagnostics for the instance. See Table 142.

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.

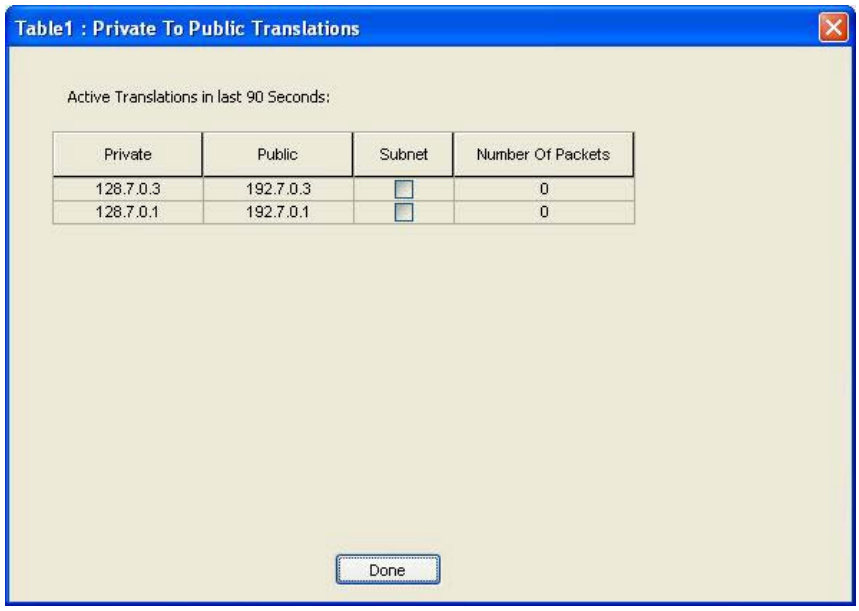


Table 141 - Private-to-Public Translation Diagnostics

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.

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.

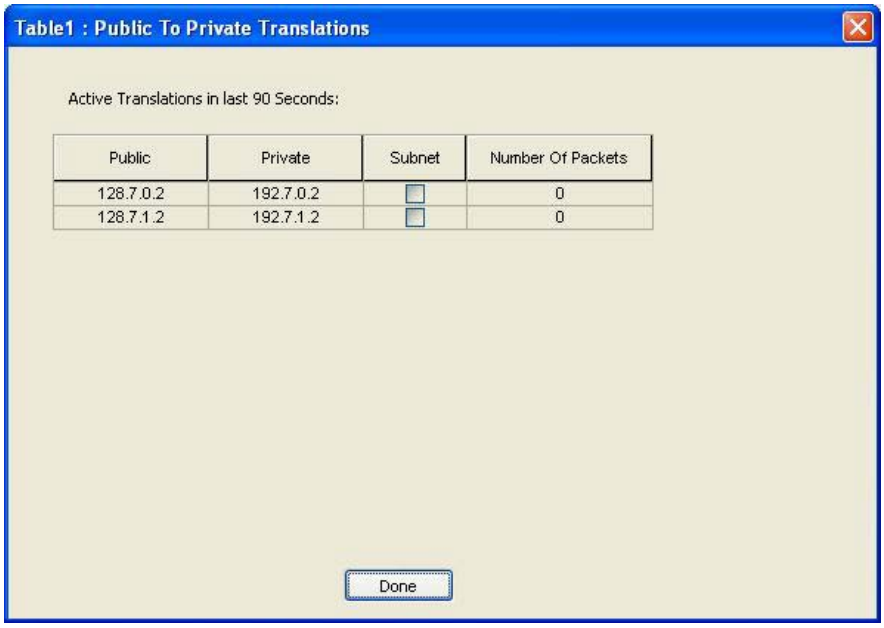


Table 142 - Public-to-Private Translation Diagnostics

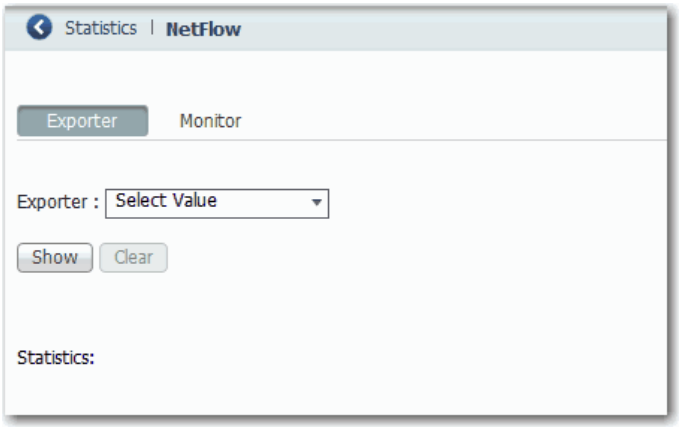
Field	Description
Public	Displays the unique IP address on the public subnet that represents the corresponding IP address on the private subnet.
Private	Displays the IP address on the private subnet that was changed to a unique IP address on the public subnet.
Subnet	Indicates whether the translation is part of a Subnet entry type.
Number of Packets	Displays the number of packets that contain the translation.

NetFlow

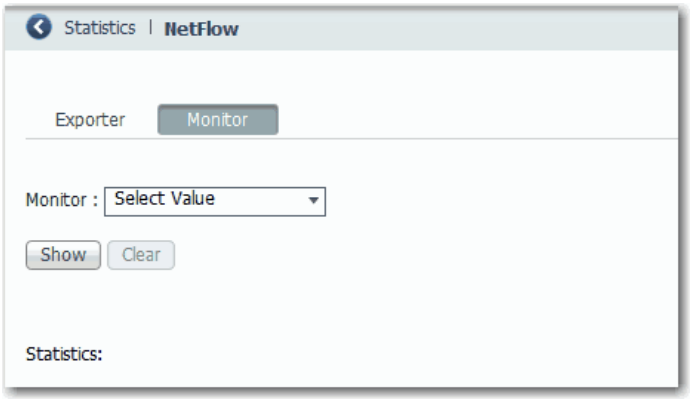
In Device Manager, you can view NetFlow exporter and monitor cache statistics. The key components of NetFlow are the cache that stores IP flow information, and the export mechanism that sends NetFlow data to a network management collector, such as the NetFlow Collection Engine. NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. NetFlow maintains a flow record within the cache for each active flow. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device, such as the NetFlow Collection Engine.

From the Monitor menu, choose NetFlow:

- On the Exporter tab, choose a flow exporter from the pull-down menu or choose ALL to display statistics for all flow exporters that are configured on the switch. Click Show to display statistics. Click Clear to clear the statistics.



- On the Monitor tab, choose a flow monitor from the pull-down menu. Click Show to display statistics. Click Clear to clear the statistics.

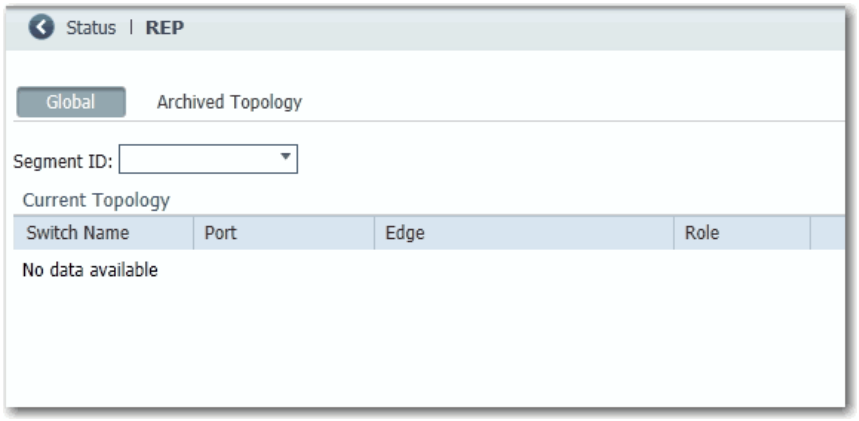


REP Status

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 page 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.

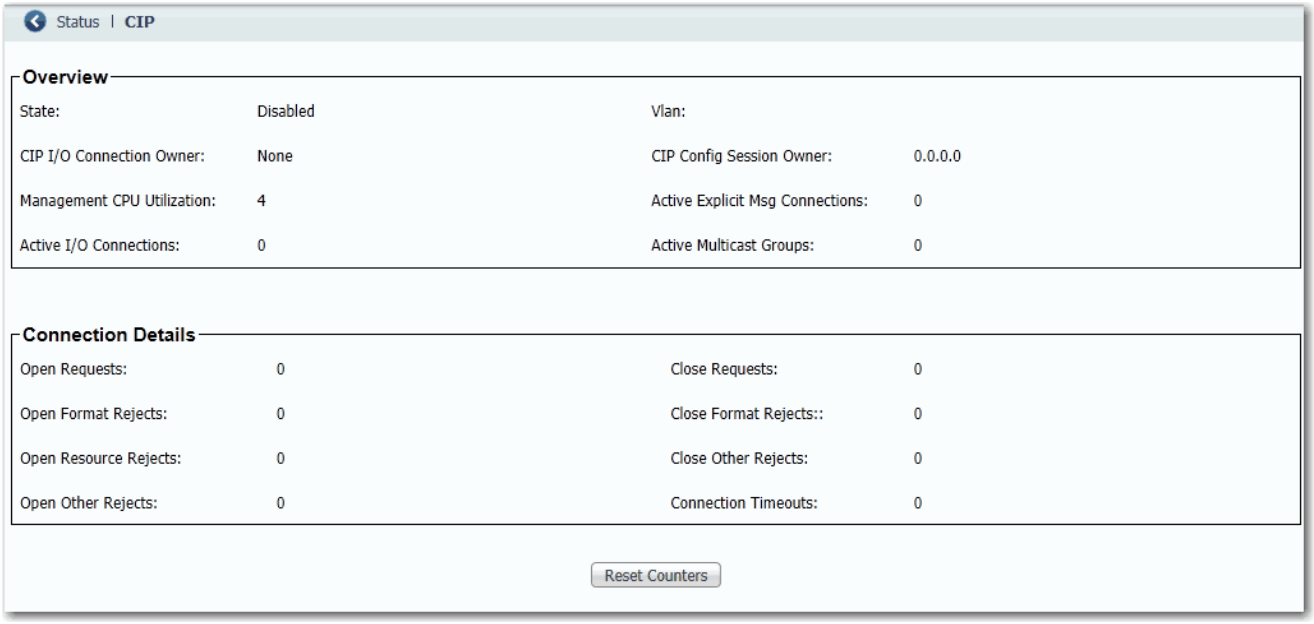


Table 143 - CIP Status Fields

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 313.

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.

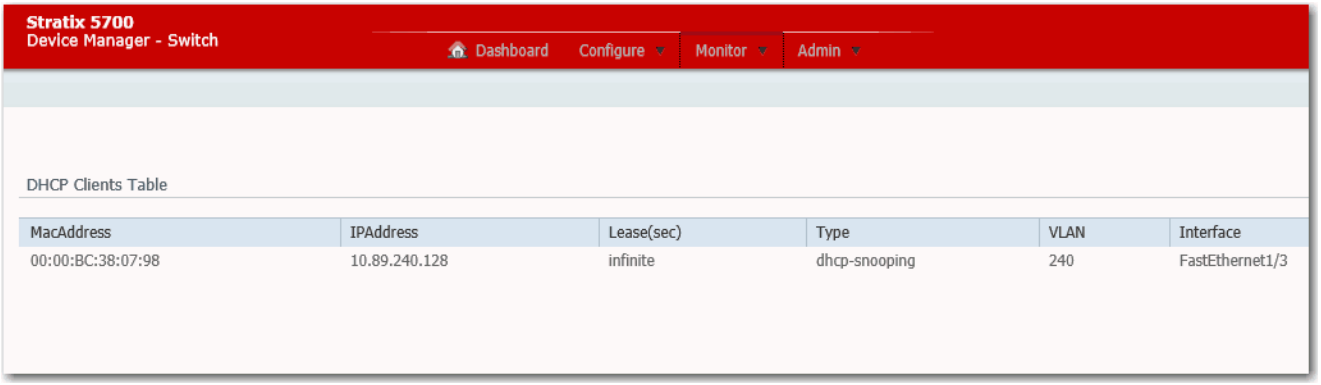


Table 144 - DHCP Clients Table Fields

Field	Description
MAC Address	The MAC ID 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

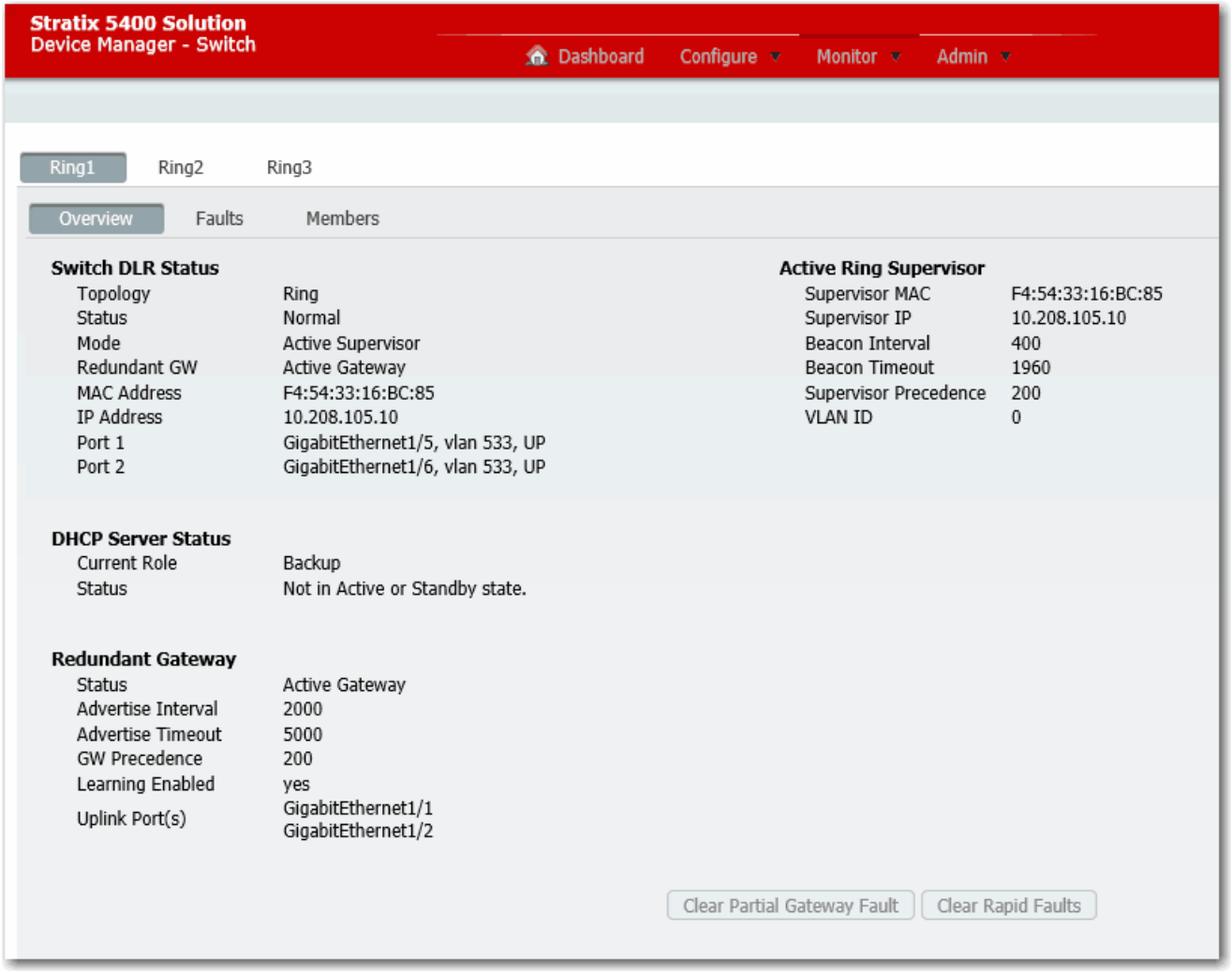
From the Monitor menu, choose DLR:

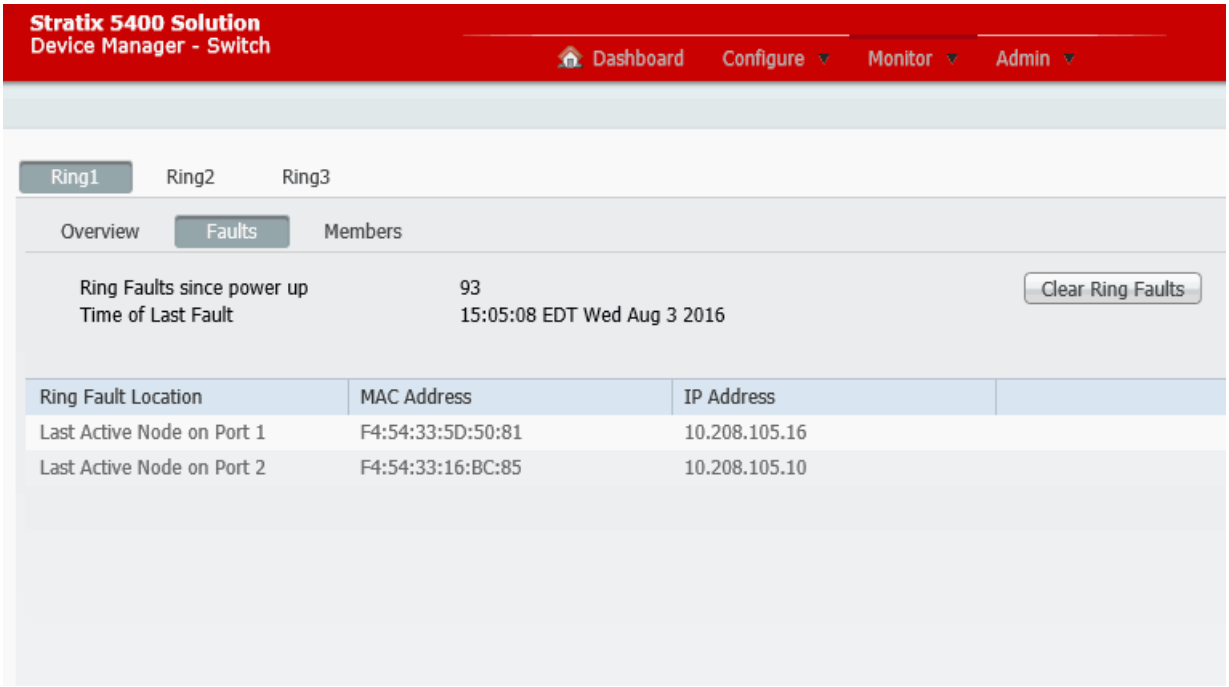
- The Overview tab shows the status and parameters that are configured for the switch, redundant gateway, ring DHCP server, and the active ring supervisor.

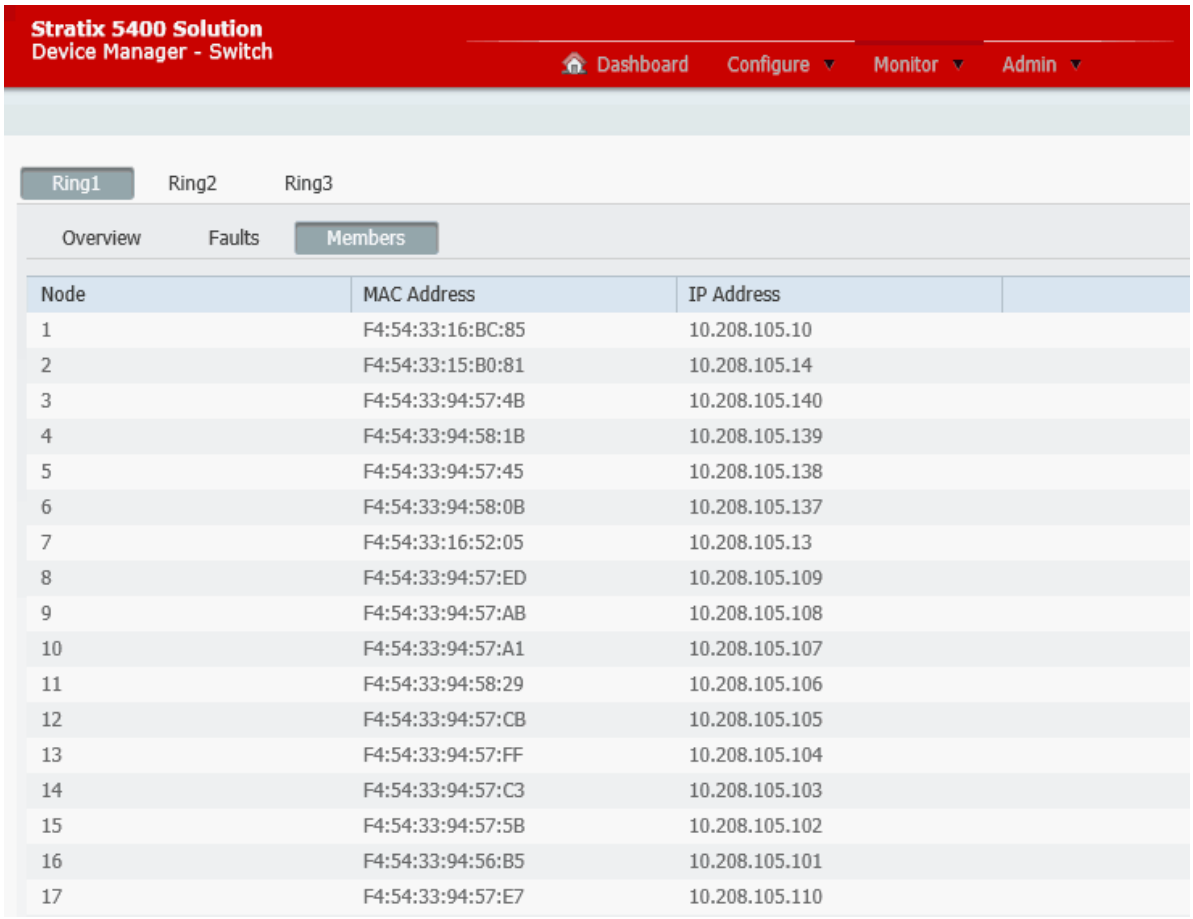
  You can also clear these faults:

  - 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.







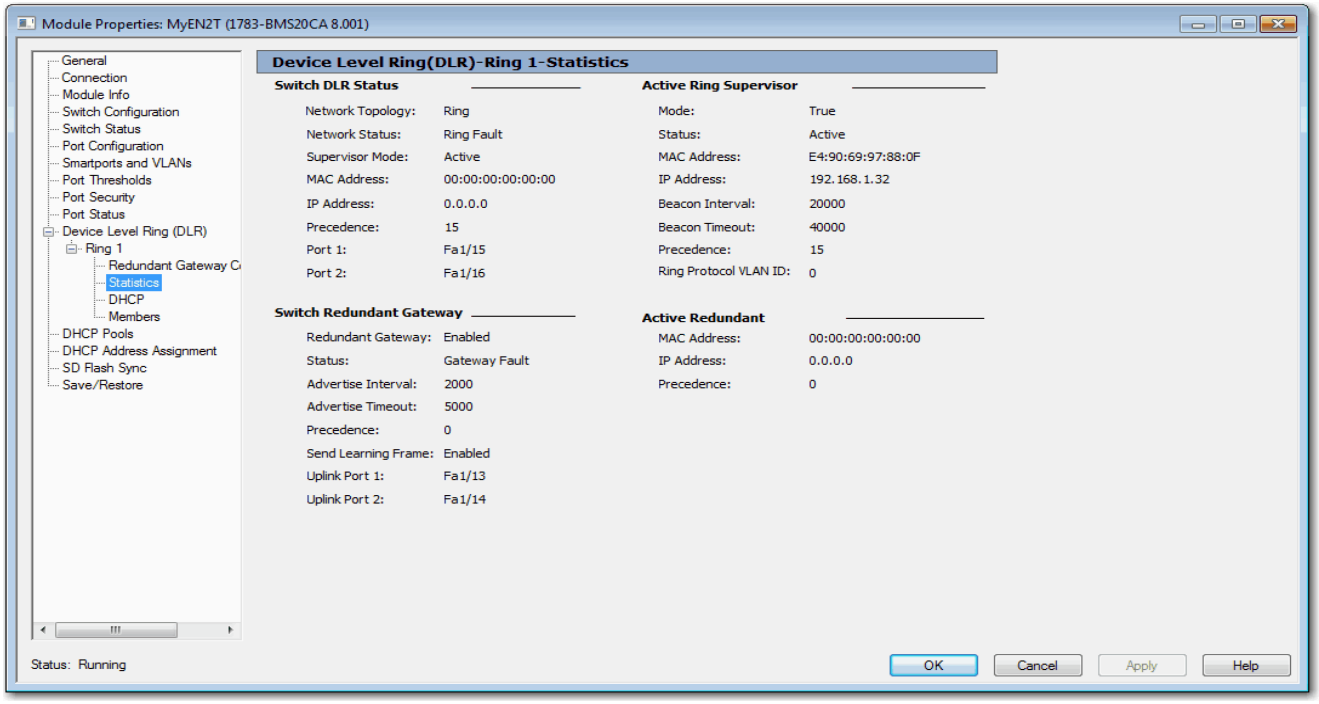
Node	MAC Address	IP Address
1	F4:54:33:16:BC:85	10.208.105.10
2	F4:54:33:15:B0:81	10.208.105.14
3	F4:54:33:94:57:4B	10.208.105.140
4	F4:54:33:94:58:1B	10.208.105.139
5	F4:54:33:94:57:45	10.208.105.138
6	F4:54:33:94:58:0B	10.208.105.137
7	F4:54:33:16:52:05	10.208.105.13
8	F4:54:33:94:57:ED	10.208.105.109
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

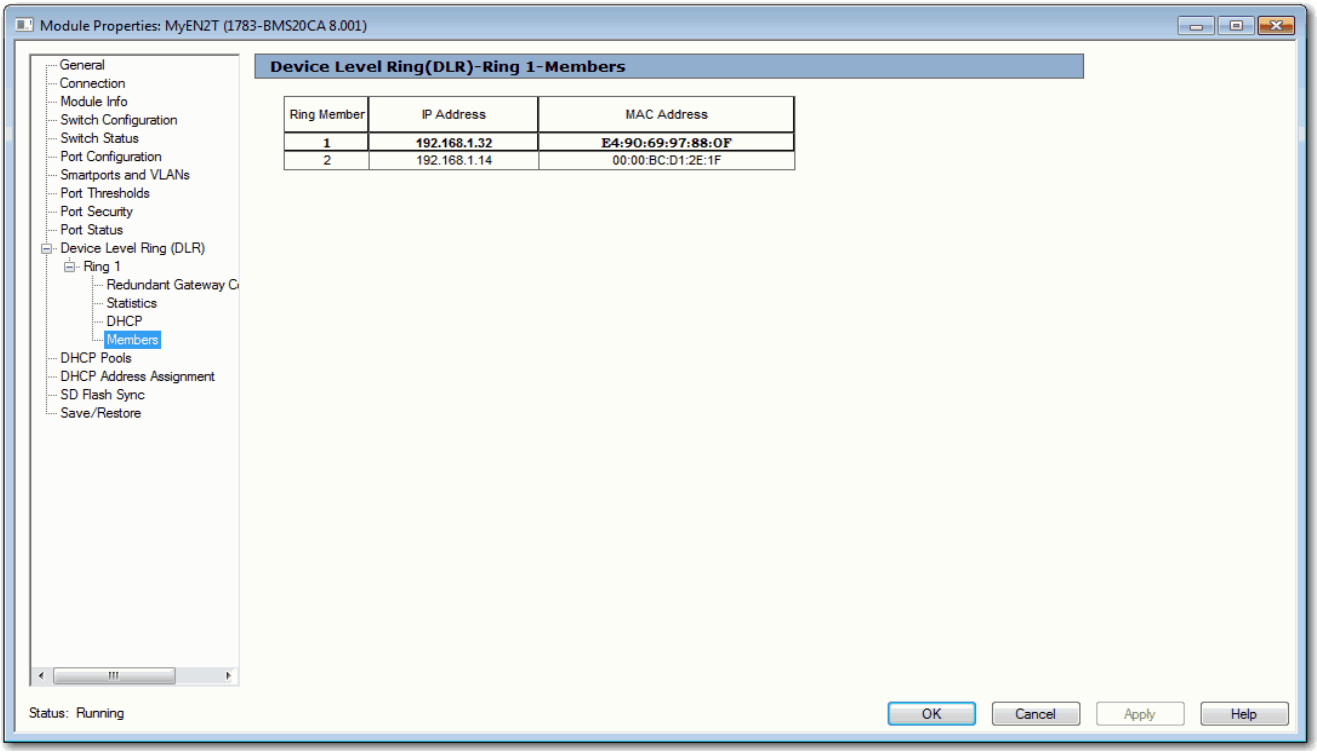
Monitor DLR Status via the Logix Designer Application

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.





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 IDs and the number of static nodes for each PRP channel group, as well as table entries. The Node table shows the total number of MAC IDs and MAC IDs 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 211.
- Stratix 5400 Display Modes on page 288
- Stratix 5410 Display Modes on page 290

From the Monitor menu, choose PRP.

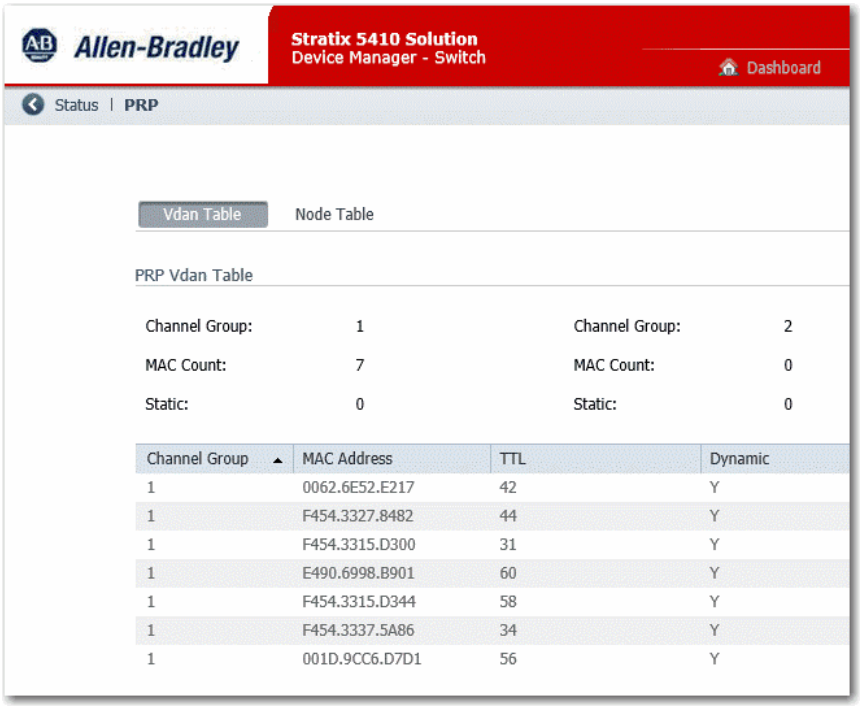


Table 145 - VDAN Table Fields

Field	Description
Channel Group 1, 2	The number of the PRP channel group.
MAC Count	The number of static and dynamic MAC IDs 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 Count	The MAC ID of the VDAN.
TTL	The amount of time before the learned MAC ID expires.
Dynamic	Whether or not (Y or N) the entry was added as a learned MAC ID.

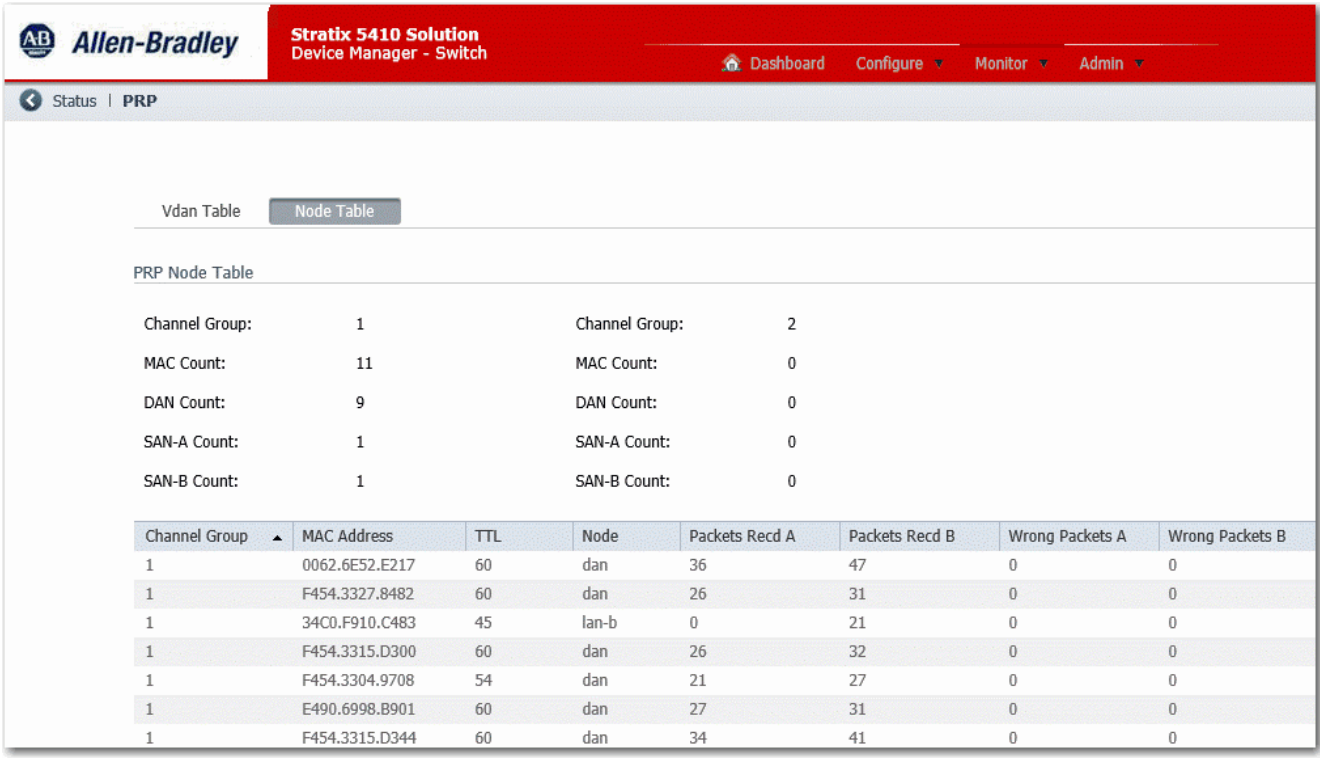


Table 146 - Node Table Fields

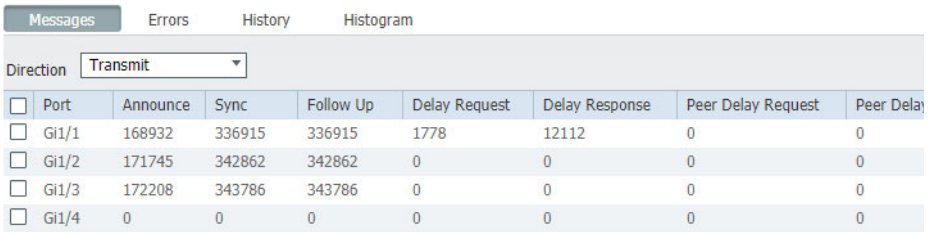
Field	Description
Channel Group 1, 2	The number of the PRP channel group.
MAC Count	The number of static and dynamic MAC IDs for the channel group.
DAN	The number of dual attached node (DAN) MAC IDs for the channel group.
SAN-A	The number of single attached nodes (SANs) on LAN A.
SAN-B	The number of single attached nodes (SANs) on LAN B.
Grid Fields	
Channel Group	The channel group of the associated entry.
MAC Address	The MAC ID of the DAN or SAN.
TTL	The amount of time before the learned MAC ID 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.

PTP Serviceability

In Device Manger, choose the Monitor Tab. Under the Monitor Tab, you see the PTP Serviceability page to display statistics and information for Precision Time Protocol (PTP).

PTP statistics can help you troubleshoot and monitor the performance of PTP in the network. The main features of PTP Serviceability are:

- Messages: Display counter information for the PTP messages sent and received.
- Errors: Display counter information for the PTP errors that occurred on the various ports.
- History: Display the historical maximum and minimum values for the offset from master and mean path delay for the last 5 seconds, 15 seconds, in increments up to 15 days, and for greater than 15 days.
- Histogram: Display a visual representation of the historical maximum and minimum values for the mean path delay and offset from master.



Click Clear Counters at the bottom of the PTP Serviceability page to reset counters to zero.

Messages

Table 147 shows the various types of PTP messages.

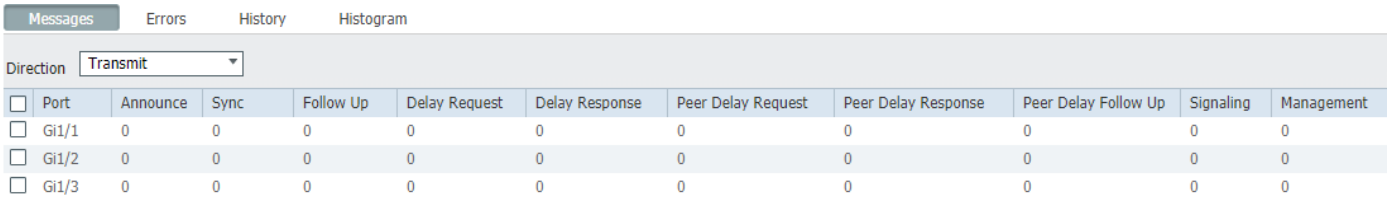


Table 147 - Message Definitions

Direction	Use the pull-down menu to select the direction of the data displayed in the table: Input or Output.
Port	The port type and number.
Announce	General message, not tagged with a timestamp, used to establish a master-slave hierarchy.
Sync	Event message tagged with a timestamp when data packets reach or leave a port and used to synchronize ordinary and boundary clocks.
Follow Up	General message, not tagged with a timestamp, used to synchronize ordinary and boundary clocks.
Delay Request	Event message tagged with a timestamp when data packets reach or leave a port and used to synchronize ordinary and boundary clocks.
Delay Response	General message, not tagged with a timestamp, used to synchronize ordinary and boundary clocks.
Peer Delay Request	Event message tagged with a timestamp when data packets reach or leave a port and used to measure the link delay in transparent clocks.
Peer Delay Response	Event message tagged with a timestamp when data packets reach or leave a port and used to measure the link delay in transparent clocks.

Table 147 - Message Definitions

Peer Delay Follow Up	General message, not tagged with a timestamp, used to measure the link delay in transparent clocks.
Signaling	General message, not tagged with a timestamp, used to carry information, requests, and commands between clocks
Management	General message, not tagged with a timestamp, that communicates information and commands used to manage clocks.

Errors

PTP errors are categorized in the following four ways.

- Field Mismatch Errors
- Unexpected Messages
- Duplicate Messages
- Generic Errors

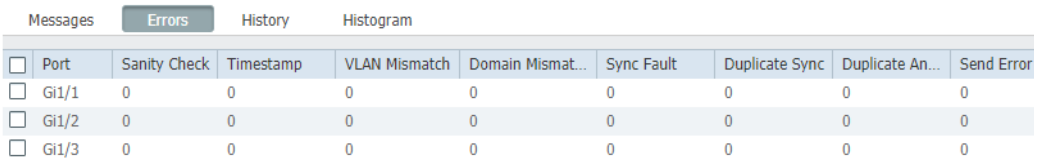


Table 148 - Field Mismatch Errors

Sanity Check	The PTP message header fields of ingress PTP packets are invalid.
Blocked Port	The PTP messages, except Peer-Delay messages, are received on REP/STP blocked ports.
VLAN Mismatch	The VLAN ID of ingress PTP messages differ from the VLAN ID configured in the PTP VLAN command.
Domain Mismatch(1)	The domain number field of ingress PTP messages differ from the configured PTP clock domain The PTP domain number configured in the PTP domain command.
Timestamp	—
Invalid Parent ID(1)	The source port identity of ingress PTP messages is different from parent port identity of the local PTP clock.
Invalid GMC ID(1)	The Grandmaster clock identity of ingress announce messages has an invalid value. The Grandmaster clock identity of ingress announce messages is the same as the clock identity of the local PTP clock.
Invalid Sequence ID(1)	The sequence ID field of ingress PTP messages has an invalid value. The sequence ID of the follow-up message differs from the sequence ID of the preceding sync message.
Sync Fault	The PTP clock offset value has exceeded the "sync limit" value that is configured on the PTP slave port. The value that is configured for PTP sync limit on the interface, which is in the PTP SLAVE state.

(1) Applicable only in Boundary Clock mode.

Table 149 - Unexpected Messages

Unmatched Follow-up	The switch received a Follow-up message when there was no outstanding SYNC message for which it expected a Follow-up.
Unmatched Delay Response	The switch received a Delay Response without sending a Delay Request.
Unmatched Peer Delay Response	The switch received a Peer Delay Response message without sending a Peer Delay Request.
Unmatched Peer Delay Response Follow-up	The switch received a Peer Delay Response Follow-up message without sending a Peer Delay Request.

Table 150 - Duplicate Messages(1)

Duplicate Sync	This counter indicates the number of duplicate PTP Sync messages received by the switch.
Duplicate Announce	This counter indicates the number of duplicate PTP Announce messages received by the switch.

(1) Duplicates are identified by checking the PTP sequence number on received messages.

Table 151 - Generic Errors

Send Error	This counter indicates the number of PTP messages that could not be sent due to failures. PTP software can fail to send PTP messages due to reasons such as memory allocation failure, failure to obtain the correct outgoing interface information, and so on.
Miscellaneous Error	This counter indicates the number of miscellaneous errors that have occurred in the PTP protocol. Any error other than the previous errors is classified as a miscellaneous error.
Rogue-Master-Sync	This counter indicates the number of Sync messages blocked on the port when GMC-Block is enabled for the port. In Boundary or Transparent clock mode, the GMC-Block per-port setting prevents the port from transitioning to the PTP SLAVE state to protect from rogue PTP devices on the Edge of the network.
Rogue-Master-Announce	This counter indicates the number of Announce messages blocked on the port when GMC-Block is enabled for the port.
Rogue-Master-FwUp	This counter indicates the number of Follow up messages blocked on the port when GMC-Block is enabled for the port.

History

Messages Errors History Histogram

Options	5 seconds	15 secon...	1 minute	5 minutes	15 minut...	1 hour	5 hours	15 hours	1 day	5 days	15 days	>15 days
Max offset from master(ns)	980	747	832	899	1200	1807	1652	1772	1772	1772	1772	1772
Min offset from master(ns)	-366	-156	-835	-1198	-1044	-2175	-1577	-1585	-2818	-2818	-2818	-2818
Max mean path delay(ns)	910	929	952	952	1051	1051	1089	1163	1163	1163	1163	1163
Min mean path delay(ns)	910	910	910	855	821	718	668	668	0	0	0	0

Information in the History tab is only available when the switch is operating in Grandmaster Boundary Clock (GMC-BC) or Boundary Clock (BC) modes. If the switch is the Master or Grandmaster clock, these values are zero.

The History is the difference between the time on the slave clock and the master. It is the measure of how accurately the slave synchronizes with the master clock. This measurement indicates the amount of inaccuracy that is brought by switch as a boundary clock.

Mean path delay is the average time that is taken by PTP frames to travel between master and slave. This measurement does not indicate the performance or accuracy of the switch or servers. A small mean path delay is useful for obtaining baseline results. A large mean path delay with high levels of jitter is representative of a complex DataCenter with buffering and latency spikes, control protocols running, a high rate of traffic, and so on.

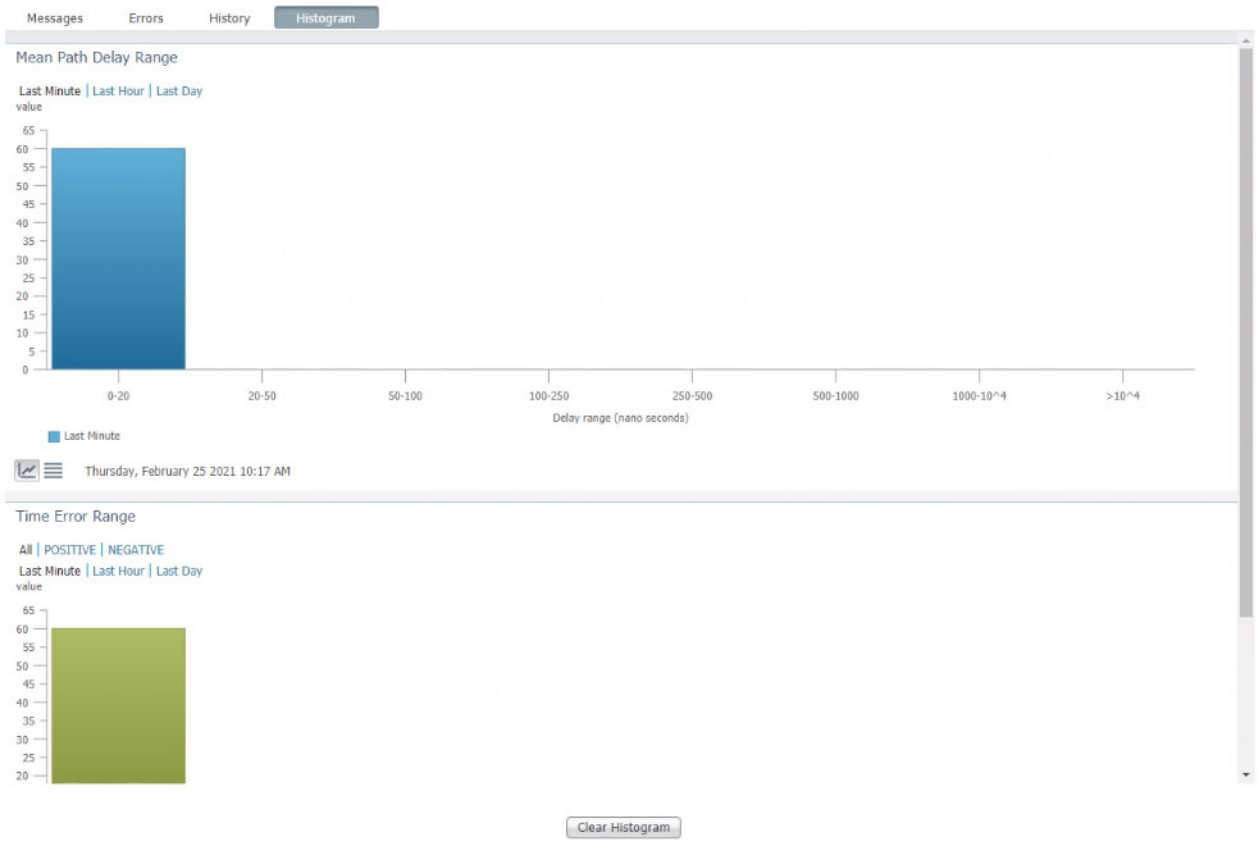
High history and delay values can indicate a problem, for example, when a device goes down in the network and the link to the master is available but not viable. Ideally, history and delay values must be as small as possible. Some PTP modes or profiles might cause higher history values.

Offset and delay values are shown for the last day and the past 5 seconds, 15 seconds, 1 minute, 5 minutes, 15 minutes, 1 hour, 5 hours, 15 hours, 1 day (same as last day), 5 days, 15 days, and more than 15 days.

Table 152 - History Values

Max Offset From Master	The maximum difference, in nanoseconds, between the time on the slave clock and the master.
Min Offset From Master	The minimum difference, in nanoseconds, between the time on the slave clock and the master.
Max Mean Path Delay	The maximum average time, in nanoseconds, taken by PTP frames to travel between master and slave.
Min Mean Path Delay	The minimum average time, in nanoseconds, taken by PTP frames to travel between master and slave.

Histogram



The Histogram tab provides a graphical display of the PTP data in the following table.

Table 153 - Histogram PTP Data

Mean Path Delay Range	Available when the clock mode is boundary or gmc-boundary. This histogram shows data for mean path delay. Mean path delay values are divided into ranges. These ranges are in the following list. • 0…20 nanoseconds • 20…50 nanoseconds • 50…100 nanoseconds • 100…250 nanoseconds • 250…500 nanoseconds • 500…1000 nanoseconds • 1000…10,000 nanoseconds • Greater than 10,000 nanoseconds. Click Last Minute to show the data for the last 60 seconds, click Last Hour to show the data for the last 1 hour, and click Last Day to show data for the last 24 hours. Click the icons below the histogram to toggle between graph and table formats.
Offset Range	Available when the clock mode is boundary. This histogram shows data for offset from master. Offset Range values are divided into ranges. These ranges are in the following list. • 0…20 nanoseconds • 20…50 nanoseconds • 50…100 nanoseconds • 100…250 nanoseconds • 250…500 nanoseconds • 500…1000 nanoseconds • 1000…10,000 nanoseconds • Greater than 10,000 nanoseconds. Click All, POSITIVE or NEGATIVE to show the positive, negative, or all variation in the offset from master. Click Last Minute to show the data for the last 60 seconds, click Last Hour to show the data for the last 1 hour, and click Last Day to show data for the last 24 hours. Click the icons below the histogram to toggle between graph and table formats.
Time Error Range	Displayed when the clock mode is e2etransparent. This histogram shows data for time-error (frequency error * residence time). Time Error Range values are divided into ranges. These ranges are in the following list. • 0…20 nanoseconds • 20…50 nanoseconds • 50…100 nanoseconds • 100…250 nanoseconds • 250…500 nanoseconds • 500…1000 nanoseconds • 1000…10,000 nanoseconds Greater than 10,000 nanoseconds. Click All, POSITIVE or NEGATIVE to show the positive, negative, or all variation in the time error. Click Last Minute to show the data for the last 60 seconds, click Last Hour to show the data for the last 1 hour, and click Last Day to show data for the last 24 hours.

Click the icons below the histogram to toggle between graph and table formats.

STP Status

In Device Manager, you can view spanning tree information for Multiple Spanning Tree (MST) or Rapid Spanning Tree Protocol (RSTP).

From the Monitor menu, choose STP.

On the RSTP tab, choose a VLAN ID to monitor and click Submit.

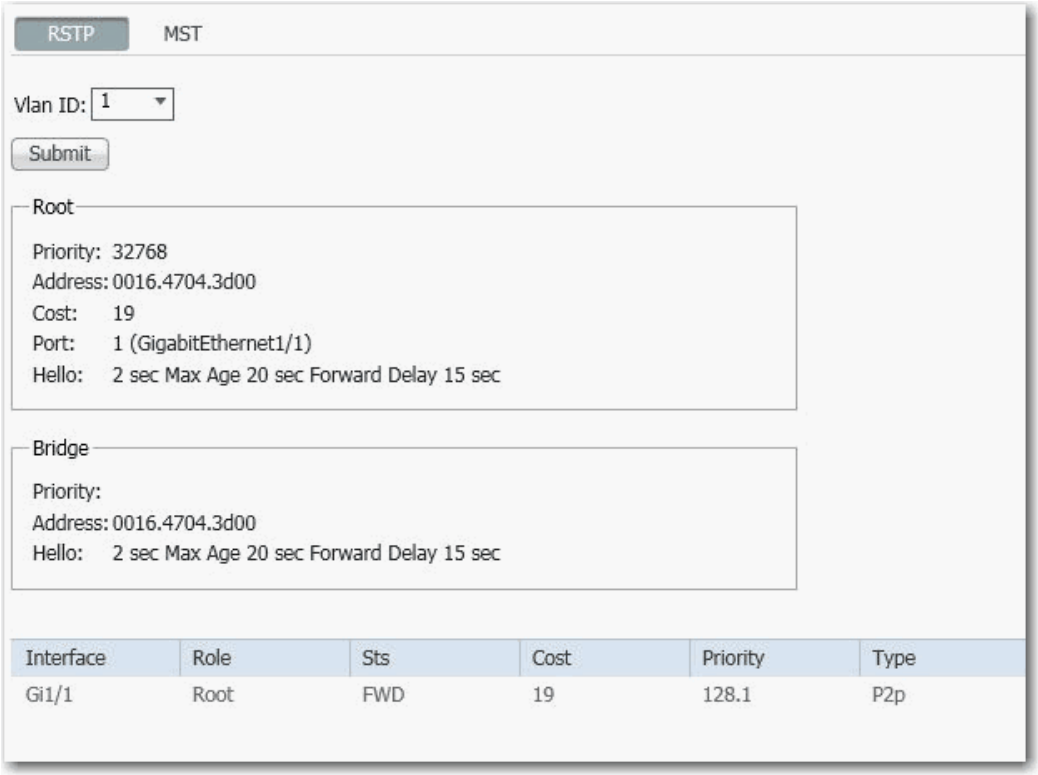


Table 154 - RSTP Tab Fields

Field	Description
Root	
Priority	The priority indicator.
Address	The MAC ID of the port.
Cost	The cost associated with the port.
Port	The identifier of the named port.
Hello	The amount of time, in seconds, that the bridge sends bridge protocol data units (BPDUs).
Max Age	The amount of time, in seconds, that a bridge protocol data unit (BPDU) packet should be considered valid.
Forward Delay	The amount of time, in seconds, that the port spends in listening or learning mode.
Bridge	
Priority	The priority indicator.
Address	The MAC ID of the port.
Hello	The amount of time, in seconds, that the bridge sends bridge protocol data units (BPDUs).
Max Age	The amount of time, in seconds, that a BPDU packet should be considered valid.
Forward Delay	The amount of time, in seconds, that the port spends in listening or learning mode.
Port Statistics	
Interface	The interface type and number of the port.
Role	Current 802.1w role: • Boun—Boundary • Desg—Designated • Root • Altn—Alternate • Back—Backup

Table 154 - RSTP Tab Fields (Continued)

Field	Description
Sts	Spanning-tree states: • BLK—Blocked: The port is still sending and listening to BPDU packets but is not forwarding traffic. • DIS—Disabled: The port is not sending or listening to BPDU packets and is not forwarding traffic. • FWD—Forwarding: The port is sending and listening to BPDU packets and forwarding traffic. • LBK—Loopback: The port recieves its own BPDU packet back. • LIS—Listening: The port spanning tree initially starts to listen for BPDU packets for the root bridge. • LRN—Learning: The port sets the proposal bit on the BPDU packets it sends out.
Cost	The STP path cost associated with the port.
Priority	The priority indicator.
Type	The link type of the port: • P2p—Point to point: The interface is a point-to-point link. • Shr—Shared: The interface is a shared medium.

On the MST tab, choose an MST instance ID to monitor and click Submit.

Table 155 - MST Tab Fields

Field	Description
Vlans Mapped	The VLANs mapped to the selected instance.
Root	
Priority	The priority indicator.
Address	The MAC ID of the port.
Cost	The root path cost.
Port	The root port ID.
Rem hops	The number of hops remaining of the maximum hop count after each downstream switch decrements the hop count.
Bridge	

Table 155 - MST Tab Fields (Continued)

Field	Description
Priority	The priority indicator.
Address	The MAC ID of the port.
Port Statistics	
Interface	The interface type and number of the port.
Role	The current 802.1w role: • Boun—Boundary • Desg—Designated • Root • Altn—Alternate • Back—Backup
Sts	Spanning-tree states: • BLK—Blocked: The port is still sending and listening to BPDU packets but is not forwarding traffic. • DIS—Disabled: The port is not sending or listening to BPDU packets and is not forwarding traffic. • FWD—Forwarding: The port is sending and listening to BPDU packets and forwarding traffic. • LBK—Loopback: The port recieves its own BPDU packet back. • LIS—Listening: The port spanning tree initially starts to listen for BPDU packets for the root bridge. • LRN—Learning: The port sets the proposal bit on the BPDU packets it sends out.
Cost	The path cost of the port.
Priority	The port priority.
Type	Link type of the port: • P2p—Point to point: The interface is a point-to-point link. • Shr—Shared: The interface is a shared medium.

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	...	...

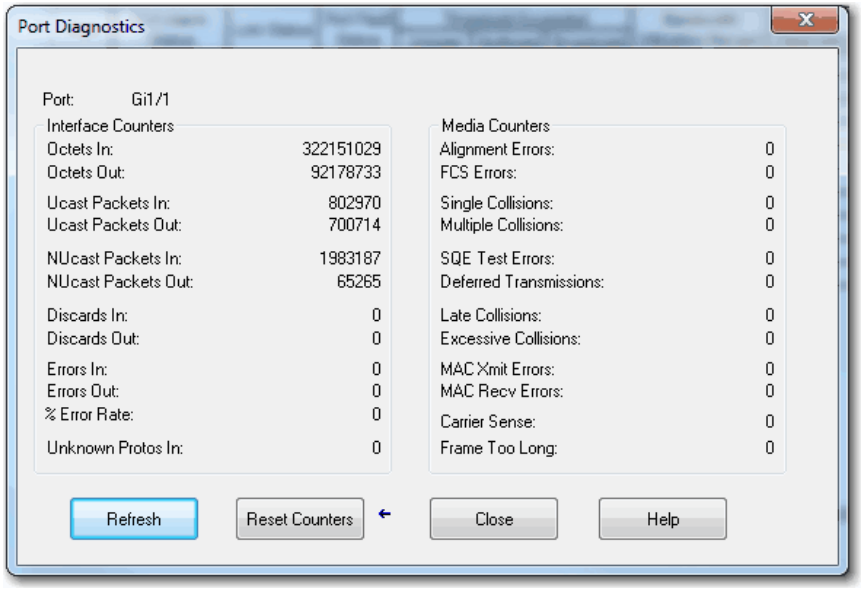


Table 156 - Port Diagnostics Fields

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.

Neighbors

Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) are neighbor discovery protocols. To enable, disable, and configure CDP and LLDP, use the command-line interface (CLI).

You can use the protocols together or separately:

- CDP is enabled by default.
- LLDP is disabled by default.

In Device Manager, you can view the neighbor information from each device to determine complete network topology. To view this information in Device Manager, the following is required:

- The neighboring device must support CDP or LLDP.
- CDP or LLDP must be enabled on a device to make the device discoverable.
- CDP or LLDP must be enabled on the switch.

When applied to a port, the following Smartport roles disable CDP:

- Automation Device
- Multiple Automation Device

From the Monitor menu, choose Neighbors. To display the neighbor information, click the CDP or LLDP tab.

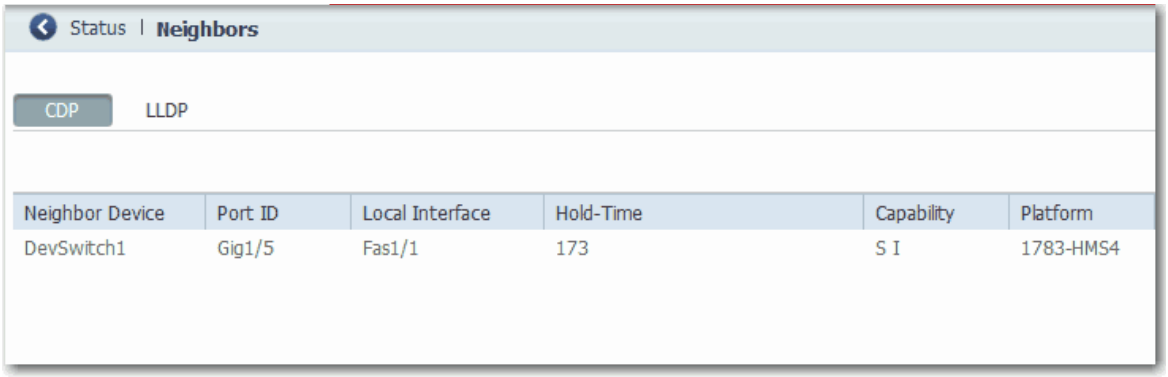


Table 157 - Neighbor Fields

Field	Description
Neighbor Device	The name of the neighboring device.
Port ID	The port type and port number of the neighboring device.
Local Interface	The local interface through which the neighbor is connected.
Hold-Time	The remaining amount of time in seconds that the current device holds the CDP or LLDP advertisement from a transmitting device before discarding it.
Capability	The device type of the neighbor, indicated by the capability code discovered on the device. A device can have multiple capability codes. Valid values: • R—Router • T—Transparent bridge • B—Source-routing bridge • S—Switch • H—Host • I—IGMP device • r—Repeater
Platform	(CDP only). The catalog number of the device.

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

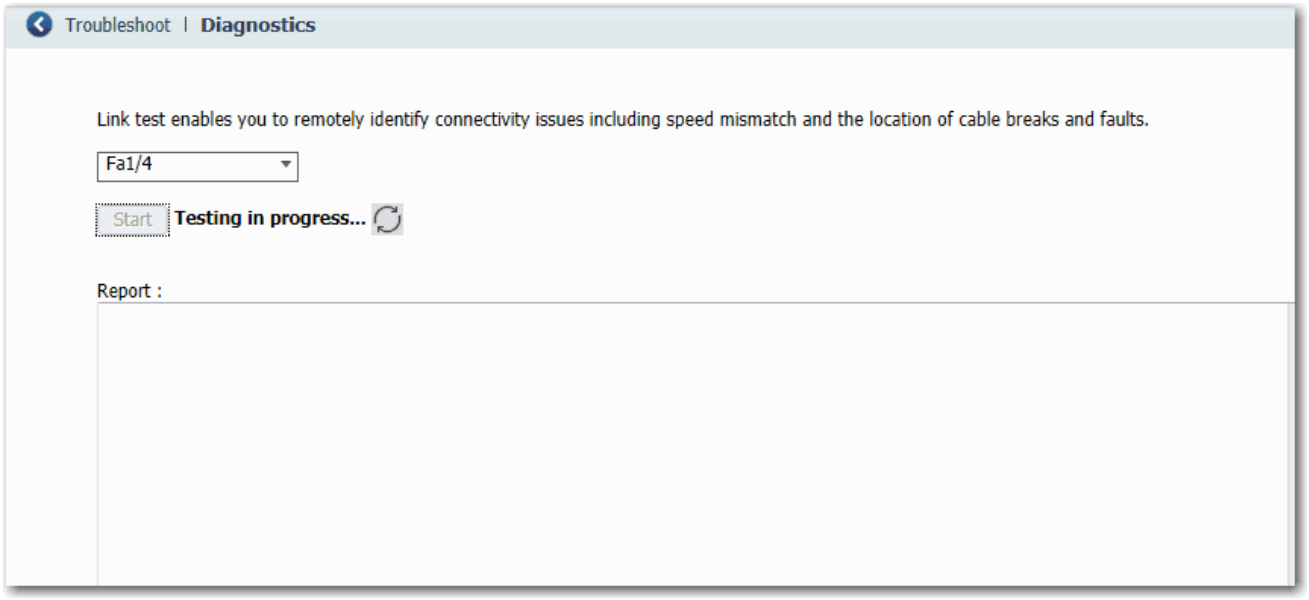
Use the Diagnostics page to run the Broken Wire Detection test, which uses Time Domain Reflectometry (TDR) detection to identify, diagnose, and resolve cable problems. TDR detection is supported on copper Ethernet 10/100 and 10/100/1000 ports. TDR is not supported on SFP module ports.

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 pages 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 45.

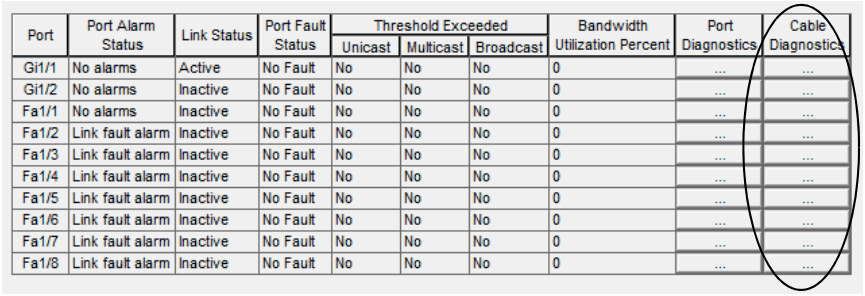
From the Monitor menu, choose Diagnostics.

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	...	...

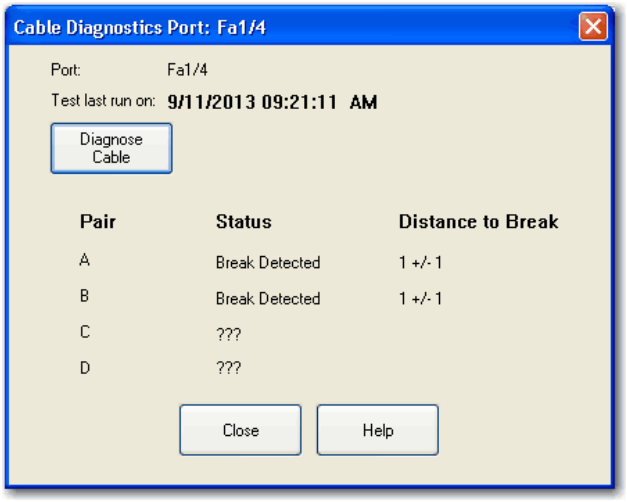


Table 158 - Cable Diagnostics Fields

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 page. **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 45. **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.

Notes:

Troubleshoot the Switch

Topic	Page
Troubleshoot the Installation	333
Verify Boot Fast	336
Troubleshoot IP Addresses	336
Troubleshoot Device Manager	336
Troubleshoot Switch Performance	337
Restart or Reset the Switch	337
Troubleshoot a Firmware Update	339
Collect System and Configuration Information for Technical Support	339

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:

- STP Status on page 325
- Neighbors on page 329
- System Log Messages on page 300

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.

SFP Module 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
The switch does not receive an IP address 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.
The switch has the 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 and update the switch IP address in Express Setup.

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.
Device Manager does not operate properly	Open Device Manager in a new browser window by using a private browsing mode: • In Internet Explorer, choose Safety > InPrivate Browsing. • In Firefox, choose New Private Window.

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.

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.

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 When you restart or reset the switch, connectivity of your devices to the network is interrupted.

Option	Method	Description
Restart	• Device Manager • Logix Designer application	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	• Device Manager • Express Setup button	This option resets the switch, deletes the current configuration settings, returns to the factory default settings, and then restarts the switch.

Restart or Reset the Switch from Device Manager

From the Admin menu, choose Restart/Reset.

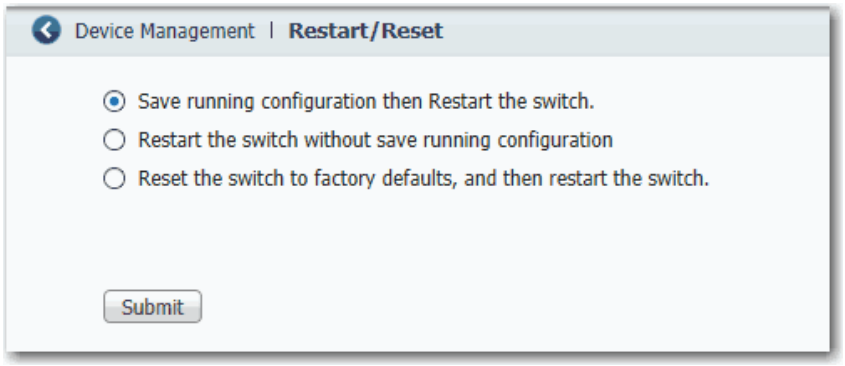


Table 159 - Restart/Reset Fields

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.

Reset the Switch via the Express Setup Button

IOS Release	Switch	Reset Procedure
15.2(4)EA3 or later	All	Press and hold the Express Setup button until the Setup status indicator flashes alternating green and red during seconds 16...20, and then release. See also Run Multimode Express Setup in Long Press Mode on page 29.
15.2(4)EA or earlier	Stratix 5400, 5410, 5700, or ArmorStratix™ 5700	Follow these steps. 1. Make sure that the switch is fully powered 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 status indicators turn red and the switch begins the power-on sequence. If this scenario occurs, power off and restart the switch to return to the factory default settings.
	Stratix 8000 or 8300	Follow these steps. 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.

Restart the Switch from the Logix Designer Application

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 restart the switch and maintain the current configurations, click Reset Module.

   A password prompt appears.
3. Enter your password and click Enter.

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.
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, Restart or Reset the Switch on page 337.

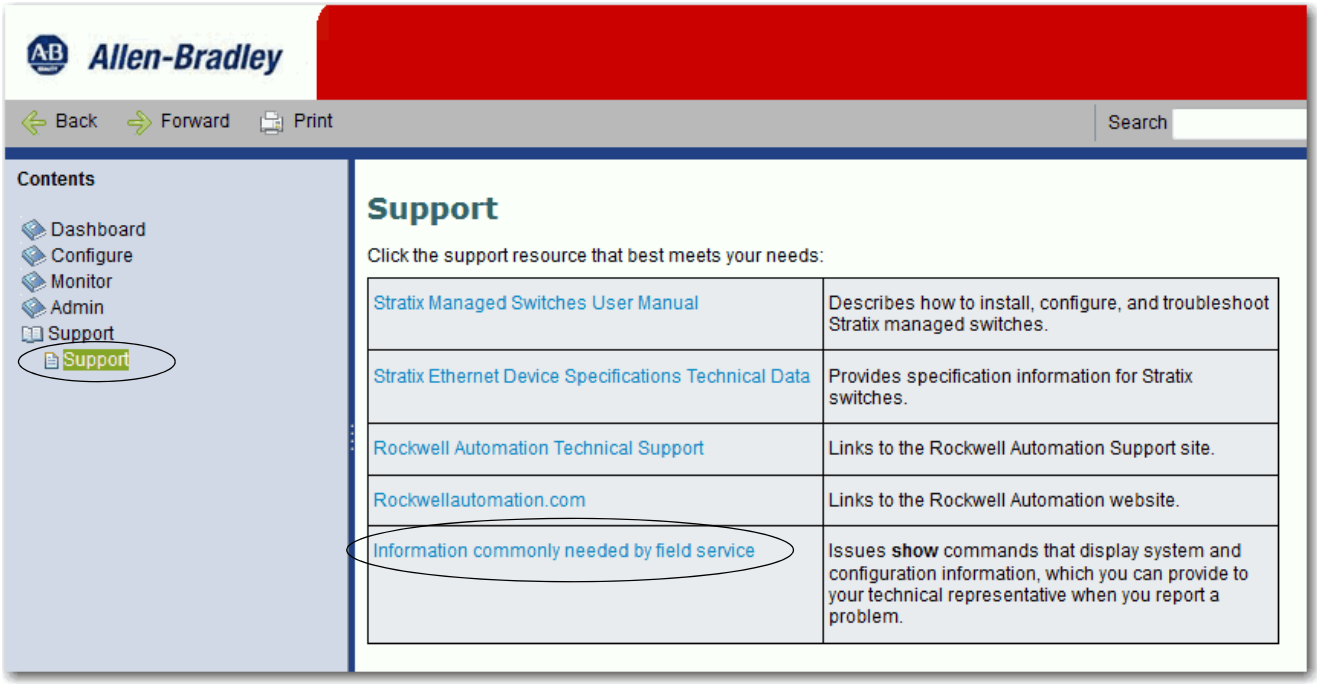
Collect System and Configuration Information for Technical Support

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	342
Stratix 5410 Data Types	356
Stratix 5700 and ArmorStratix 5700 Data Types	360
Stratix 8000 and 8300 Data Types	381

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 160 - 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	
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 161 - 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 162 - 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

Table 162 - Input Data Types (12-port switches) (Continued)

AB:STRATIX_5400_12PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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
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 163 - 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
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 164 - 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
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	

Table 164 - 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_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 165 - 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 166 - 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
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

Table 166 - Input Data Type (16-port switches) (Continued)

AB:STRATIX_5400_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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	
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 167 - 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
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 168 - 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
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

Table 168 - 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_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	
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 169 - 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 170 - 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
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

Table 170 - Input Data Type (20-port switches) (Continued)

AB:STRATIX_5400_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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	
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 171 - 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
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 172 - 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

Table 172 - 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_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
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
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	

Table 172 - 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_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 173 - 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
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 174 - 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
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

Table 174 - Input Data Type (Continued)

AB:STRATIX_5410_28PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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
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

Table 174 - Input Data Type (Continued)

AB:STRATIX_5410_28PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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	
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 175 - 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 176 - 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	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 177 - 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

Table 177 - Output Data Type (6-port Gb switches) (Continued)

AB:STRATIX_5700_6PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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 178 - 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
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 179 - 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 180 - 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	

Table 180 - Input Data Type (8-port switches) (Continued)

AB:STRATIX_5700_8PORT_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	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 181 - 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 182 - 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
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

Table 182 - Input Data Type (10-port Gb switches) (Continued)

AB:STRATIX_5700_10PORT_GB_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
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 183 - 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 184 - 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
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	

Table 184 - Input Data Type (10-port switches) (Continued)

AB:STRATIX_5700_10PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_10Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Table 185 - 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 186 - 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
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3

Table 186 - Input Data Type (16-port switches) (Continued)

AB:STRATIX_5700_16PORT_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
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	
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 187 - Output Data Type (16-port switches)

AB:STRATIX_5700_16PORT_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

20-port Gb Switches

Catalog numbers 1783-BMS20CGL, 1783-BMS20CGN, 1783-BMS20CGP, 1783-BMS20CGPK

Table 188 - 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

Table 188 - Input Data Type (20-port Gb switches) (Continued)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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
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	

Table 188 - 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_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	
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 189 - 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
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

Table 189 - 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_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
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	

Table 189 - 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_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 190 - 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
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 191 - 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
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

Table 191 - 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_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	
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 192 - 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
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 193 - 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

Table 193 - Input Data Type (20-port switches) (Continued)

AB:STRATIX_5700_20PORT_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
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
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
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	

Table 193 - Input Data Type (20-port switches) (Continued)

AB:STRATIX_5700_20PORT_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	
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 194 - 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
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 195 - 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
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

Table 195 - Input Data Type (24-port switches) (Continued)

AB:STRATIX_5700_24PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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
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	
PortFa1_18Utilization	SINT	Decimal	
PortFa1_19Utilization	SINT	Decimal	

Table 195 - Input Data Type (24-port switches) (Continued)

AB:STRATIX_5700_24PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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 196 - Output Data Type (24-port switches)

AB:STRATIX_5700_24PORT_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
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortFa1_19Disable	BOOL	Decimal	DisablePort:19
PortFa1_20Disable	BOOL	Decimal	DisablePort:20
PortFa1_21Disable	BOOL	Decimal	DisablePort:21
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 197 - 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	
AnyPortUnauthorizedDevice	BOOL	Indicates that an unauthorized MAC ID has attempted to communicate on any port.

Table 197 - Input Data Types (Continued)

Tag Name	Type	Description
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 197 - 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 197 - 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 198 - Output Data Types

Tag Name	Type	Description
AllPortsDisable	BOOL	Setting this bit disables all ports on the switch. 0 = Enable 1 = Disable

Table 198 - Output Data Types

Tag Name	Type	Description
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	387
Stratix 5410 Port Assignments	388
Stratix 5700 Port Assignments	389
ArmorStratix 5700 Port Assignments	390
Stratix 8000 and 8300 Port Assignments	390

The following tables identify the instance numbers of the Ethernet™ link objects that are associated with each port on Stratix® and ArmorStratix™ switches. Instance 0 does not apply to all ports as it does for bitmaps.

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 199 - 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 200 - 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

Bit	1783-IMS28NDC, 1783-IMS28NAC, 1783-IMS28GNDC, 1783-IMS28GNAC, 1783-IMS28RDC, 1783-IMS28RAC, 1783-IMS28GRDC, 1783-IMS28GRAC
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 201 - 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 202 - 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 202 - 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

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
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	393
Stratix 5410 Port Numbering	398
Stratix 5700 Port Numbering	399
ArmorStratix 5700 Port Numbering	404
Stratix 8000 and 8300 Port Numbering	406

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 203 - 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 2 3 4 5 6 7 8	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8
1783-HMS8T4CGN	12-port (4 combo Gigabit ports; 8 Ethernet ports) managed switch; Layer 2 firmware	1 2 3 4 5 6 7 8 9 10 11 12	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12
1783-HMS8S4CGN	12-port (4 combo Gigabit ports; 8 SFP ports) managed switch; Layer 2 firmware	1 2 3 4 5 6 7 8 9 10 11 12	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12

Table 203 - 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 2 3 4 5 6 7 8 9 10 11 12	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12
1783-HMS8TG4CGN	12-port (8 Gigabit ports; 4 Gigabit combo ports) managed switch; Layer 2 firmware	1 2 3 4 5 6 7 8 9 10 11 12	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12
1783-HMS8SG4CGN	12-port (4 Gigabit combo ports; 8 Gigabit SFP ports) managed switch; Layer 2 firmware	1 2 3 4 5 6 7 8 9 10 11 12	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12
1783-HMS4EG8CGN	12-port (4 Gigabit ports; 4 Gigabit combo ports; 4 Gigabit PoE/PoE+ ports) managed switch; Layer 2 firmware	1 2 3 4 5 6 7 8 9 10 11 12	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12
1783-HMS4S8E4CGN	16-port (4 combo Gigabit ports; 8 PoE/PoE+ ports; 4 SFP ports) managed switch; Layer 2 firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi1/1 Gi1/2 Gi1/3 Gi1/4 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 203 - Stratix® 5400 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-HMS4SG8EG4CGN	16-port (4 Gigabit combo ports; 8 Gigabit PoE/PoE+ ports; 4 Gigabit SFP ports) managed switch; Layer 2 firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12 Gi1/13 Gi1/14 Gi1/15 Gi1/16
1783-HMS16T4CGN	20-port (4 combo Gigabit ports; 16 Ethernet ports) managed switch; Layer 2 firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Fa1/17 Fa1/18 Fa1/19 Fa1/20
1783-HMS16TG4CGN	20-port (16 Gigabit ports; 4 Gigabit combo ports) managed switch; Layer 2 firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12 Gi1/13 Gi1/14 Gi1/15 Gi1/16 Gi1/17 Gi1/18 Gi1/19 Gi1/20

Table 203 - 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 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12 Gi1/13 Gi1/14 Gi1/15 Gi1/16 Gi1/17 Gi1/18 Gi1/19 Gi1/20
1783-HMS8TG4CGR	12-port (8 Ethernet ports; 4 Gigabit combo ports) managed switch; Layer 3 firmware	1 2 3 4 5 6 7 8 9 10 11 12	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12
1783-HMS8SG4CGR	12-port (4 Gigabit combo ports; 8 Gigabit SFP ports) managed switch; Layer 3 firmware	1 2 3 4 5 6 7 8 9 10 11 12	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12
1783-HMS4EG8CGR	12-port (4 Gigabit ports; 4 Gigabit combo ports; 4 Gigabit PoE/PoE+ ports) managed switch; Layer 3 firmware	1 2 3 4 5 6 7 8 9 10 11 12	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12

Table 203 - 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 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12 Gi1/13 Gi1/14 Gi1/15 Gi1/16
1783-HMS16TG4CGR	20-port (16 Gigabit ports; 4 Gigabit combo ports) managed switch; Layer 3 firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12 Gi1/13 Gi1/14 Gi1/15 Gi1/16 Gi1/17 Gi1/18 Gi1/19 Gi1/20
1783-HMS8TG8EG4CGR	20-port (8 Gigabit ports; 4 Gigabit combo ports; 8 Gigabit PoE/PoE+ ports) managed switch; Layer 3 firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10 Gi1/11 Gi1/12 Gi1/13 Gi1/14 Gi1/15 Gi1/16 Gi1/17 Gi1/18 Gi1/19 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 204 - 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 205 - 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
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

Table 205 - Stratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
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
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

Table 205 - Stratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
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
1783-BMS12T4E2CGP	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; full firmware; PTP	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
1783-BMS12T4E2CGL	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; lite firmware	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 205 - Stratix 5700 Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS20CL	20-port (16 Ethernet ports; 2 SFP slots; 2 combo ports) managed switch; lite firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	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 Fa1/17 Fa1/18 Fa1/19 Fa1/20
1783-BMS20CA	20-port (16 Ethernet ports; 2 SFP slots; 2 combo ports) managed switch; full firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	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 Fa1/17 Fa1/18 Fa1/19 Fa1/20
1783-BMS20CGL	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; lite firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 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 Fa1/17 Fa1/18 Gi1/1 Gi1/2

Table 205 - 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 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 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 Fa1/17 Fa1/18 Gi1/1 Gi1/2
1783-BMS20CGP	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; PTP	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 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 Fa1/17 Fa1/18 Gi1/1 Gi1/2
1783-BMS20CGPK	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; PTP; conformal coating	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 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 Fa1/17 Fa1/18 Gi1/1 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 206 - 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 206 - 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
1783-ZMS24TA	24-port (24 Ethernet ports) managed switch; full firmware	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24	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 Fa1/17 Fa1/18 Fa1/19 Fa1/20 Fa1/21 Fa1/22 Fa1/23 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 207 - 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
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

Table 207 - 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-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

Notes:

Cables and Connectors

Topic	Page
Stratix 5410 Cables and Connectors	409
Stratix 5400 and 5700 Cables and Connectors	415
ArmorStratix 5700 Cables and Connectors	422
Stratix 8000/8300 Cables and Connectors	427

For recommended cables and SFP modules, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Stratix 5410 Cables and Connectors

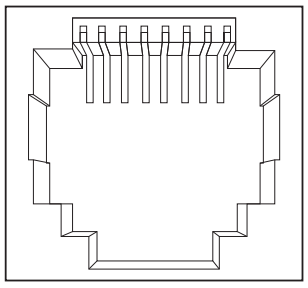
This section describes how to connect to ports on Stratix® 5410 switches.

10/100/1000 Ports

The 10/100/1000 Ethernet, PoE/PoE+ ports use standard RJ45 connectors and Ethernet™ pinouts with internal crossovers.

Figure 49 - 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 59 and Figure 60 show the cable schematics.

Figure 50 - Two Twisted-pair Straight-through Cable Schematics

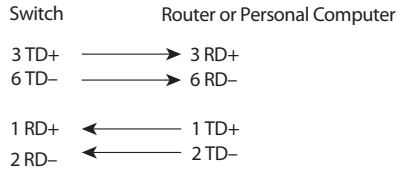
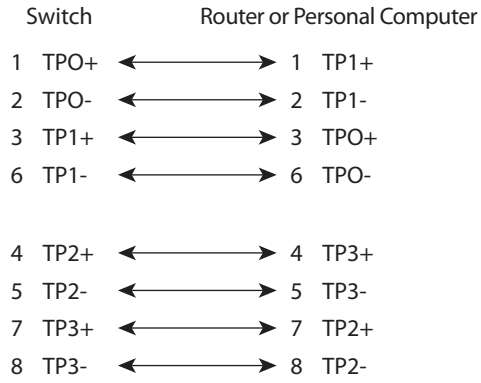


Figure 51 - Four Twisted-pair Straight-through Cable Schematics



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 61 and Figure 62 show the cable schematics.

Figure 52 - Two Twisted-pair Crossover Cable Schematics

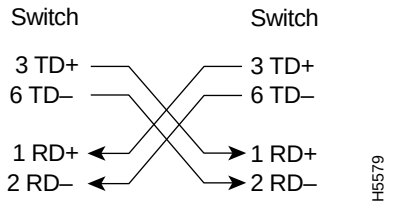
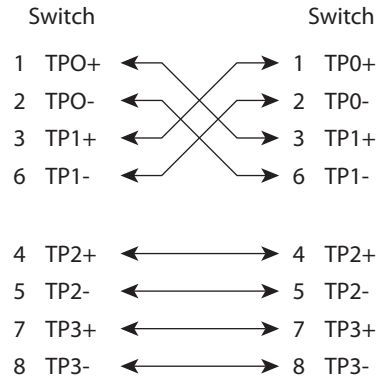


Figure 53 - Four Twisted-pair Crossover Cable Schematics

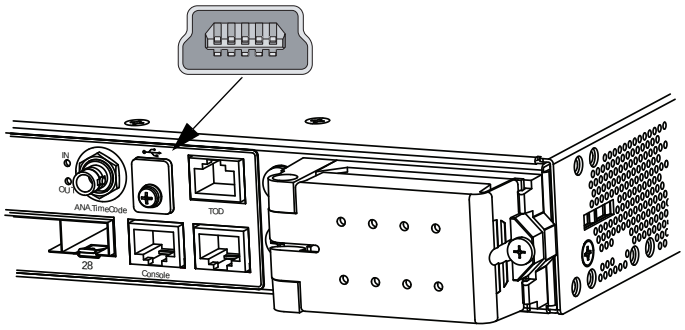


Console Ports

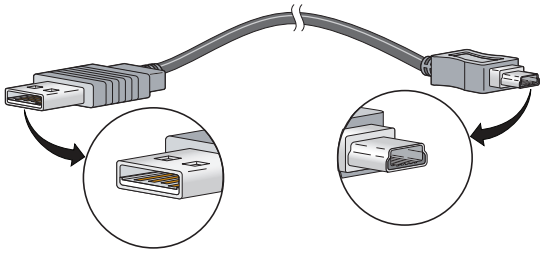
Console ports enable you to connect a switch to a computer if you use the Command-line interface (CLI) to configure and monitor a switch.

Stratix 5410 switches have these console ports:

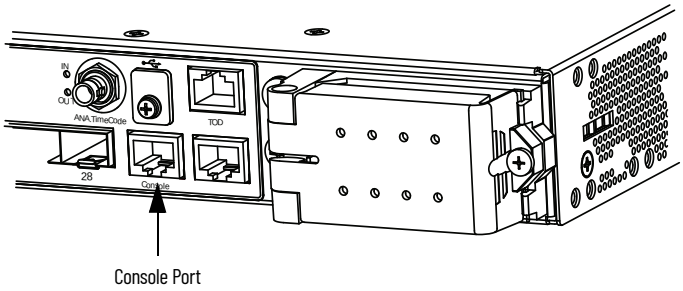
- A USB 5-pin mini-Type B port on the front panel



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 208 - 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 209 - 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 54 - Front Panel Alarm Connector

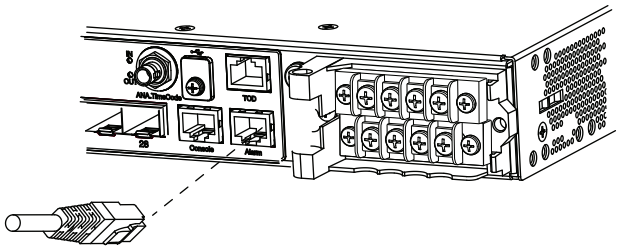
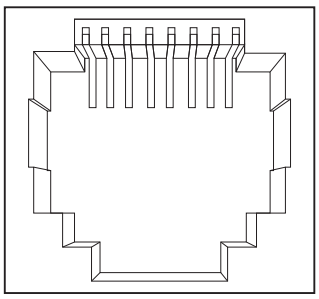


Figure 55 - Alarm Connector Pinout

Pin	Label	1 2 3 4 5 6 7 8
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 56 - 10/100 Connector Pinouts

Pin	Label
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

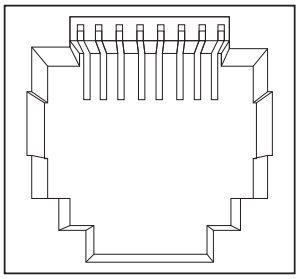
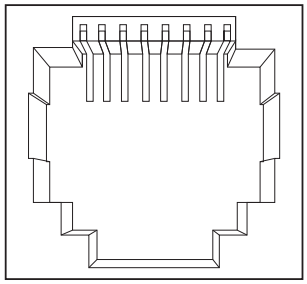


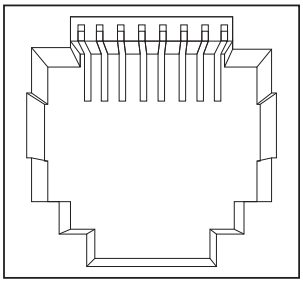
Figure 57 - 10/100/1000 Connector Pinouts

Pin	Label
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 58 - 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 59 and Figure 60 show the cable schematics.

Figure 59 - Two Twisted-pair Straight-through Cable Schematics

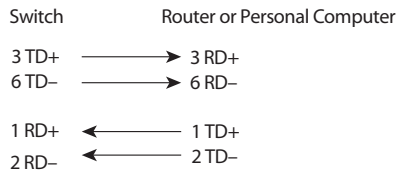
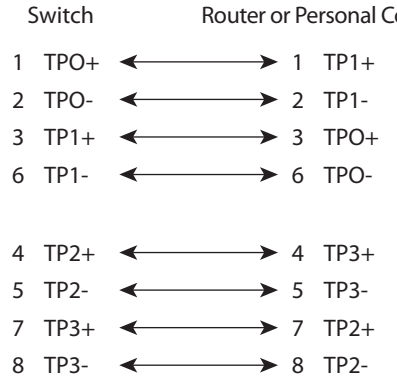


Figure 60 - Four Twisted-pair Straight-through Cable Schematics



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 61 and Figure 62 show the cable schematics.

Figure 61 - Two Twisted-pair Crossover Cable Schematics

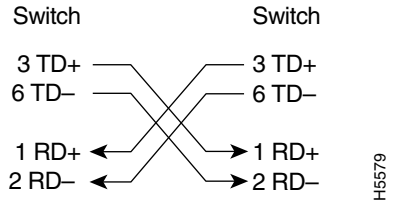
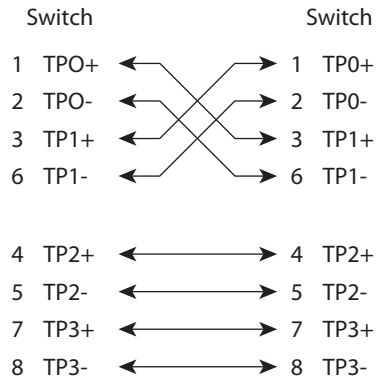


Figure 62 - Four Twisted-pair Crossover Cable Schematics

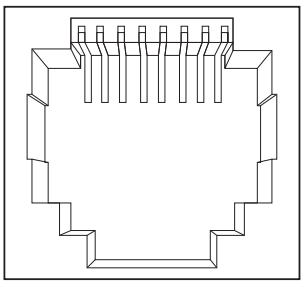


Dual-purpose Ports (combo ports)

The Ethernet port on a dual-purpose port uses standard RJ45 connectors. The following figure shows the pinouts.

Figure 63 - Ethernet Port RJ45 Connector

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



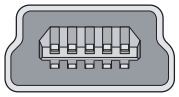
The SFP module slot on a dual-purpose port uses SFP modules for fiber-optic ports. The auto-MDIX feature is enabled by default.

Console Ports

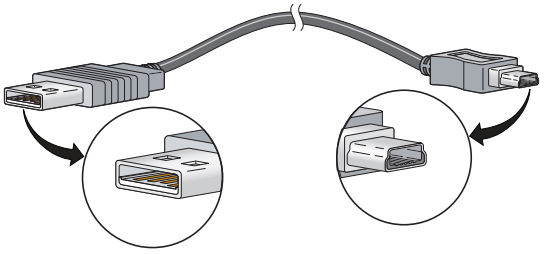
Console ports enable you to connect a switch to a computer if you use the Command-line interface (CLI) to configure and monitor a switch.

Stratix 5700 switches have these console ports:

- A USB 5-pin mini-Type B port on the front panel

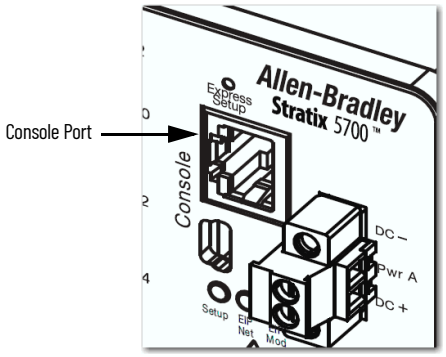


The USB console port uses a USB Type A to 5-pin mini-Type B cable. To use the USB cable, download the drivers for Microsoft Windows from http://www.rockwellautomation.com. The USB cable is not provided with the switch.



- 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 210 - 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.

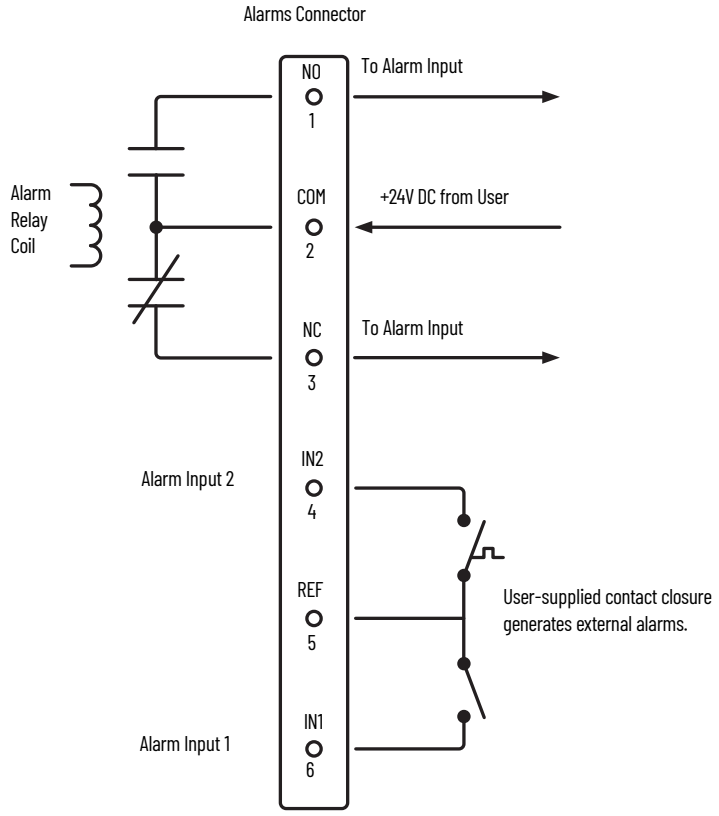
Table 211 - Pinouts with DB-25 Pin

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 64 - 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).

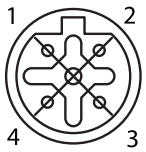
ArmorStratix 5700 Cables and Connectors

This section describes how to connect to ports on ArmorStratix™ 5700 switches.

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 65 - 10/100 Connector Pinouts

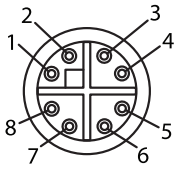


1	RD+
2	TD+
3	RD-
4	TD-

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 66 - 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 67 and Figure 68 show the cable schematics.

Figure 67 - Two Twisted-pair Straight-through Cable Schematics

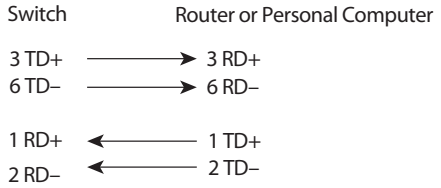
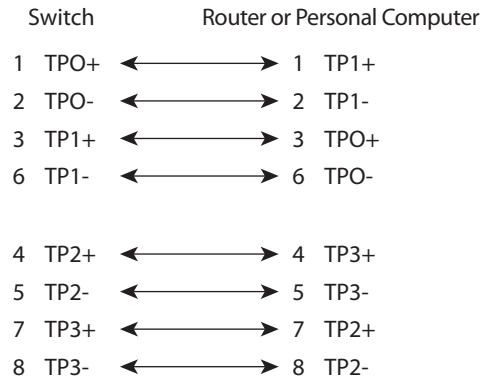


Figure 68 - Four Twisted-pair Straight-through Cable Schematics



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 69 and Figure 70 show the cable schematics.

Figure 69 - Two Twisted-pair Crossover Cable Schematics

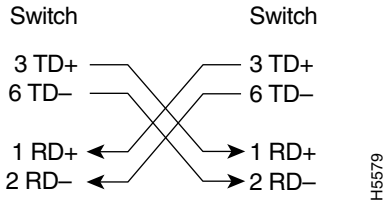
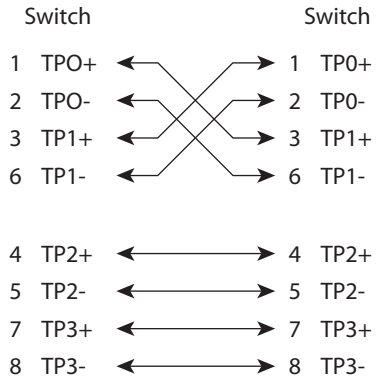


Figure 70 - Four Twisted-pair Crossover Cable Schematics



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 71):

- 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 71 - M12-to-DB-9 Cable

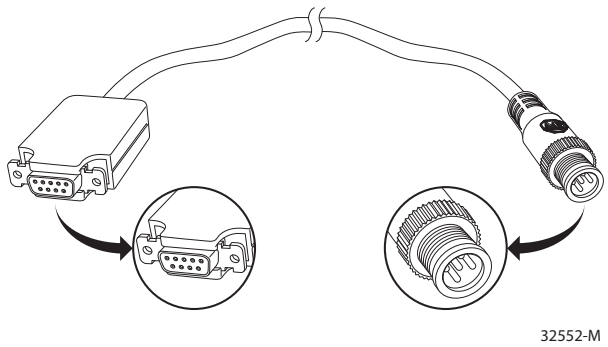
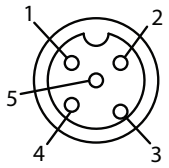
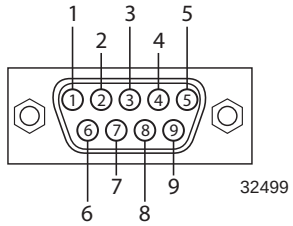


Figure 72 - Console Port Pinout



1	RTS
2	CTS
3	TXD
4	RXD
5	GND

Figure 73 - 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 74 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 74 - Alarm Connector Pinout

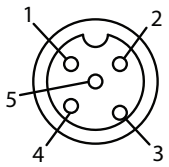
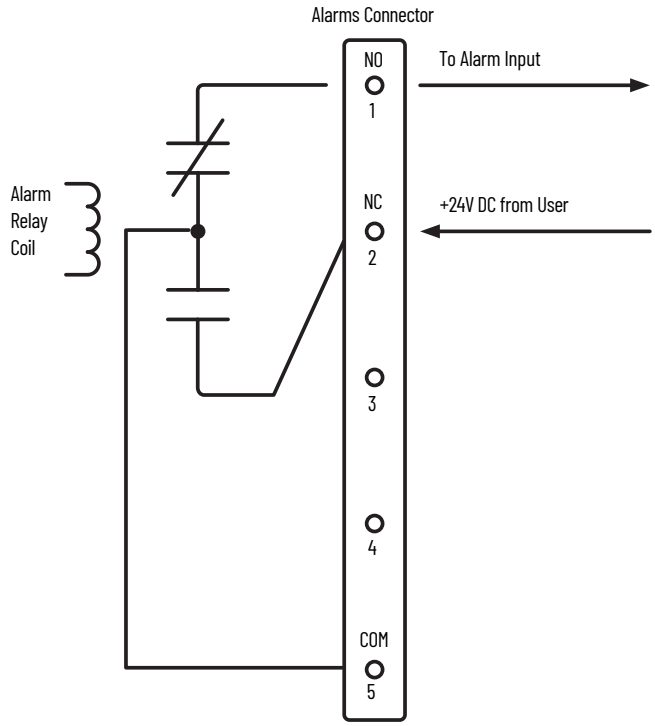


Table 212 -

1	NO
2	NC
3	Unconnected
4	Unconnected
5	Common

Figure 75 - 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.

The auto-MDIX feature is enabled by default.

Figure 76 - 10/100 Connector Pinouts

Pin	Label
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

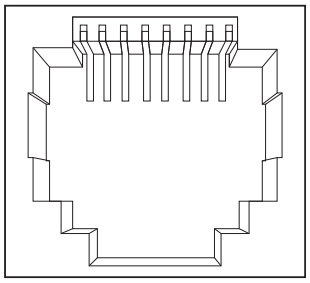
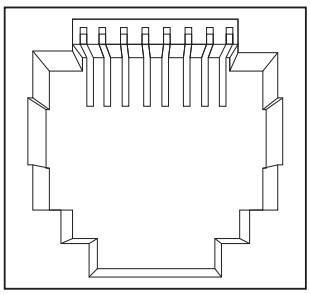


Figure 77 - 10/100/1000 Connector Pinouts

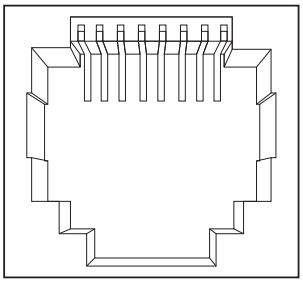
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



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 78 - 10/100 PoE Connector Pinouts and Power Sourcing Equipment (PSE) Voltage

Pin	Label	Alternative A (MDI)
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 79 and Figure 80 show the cable schematics.

Figure 79 - Two Twisted-pair Straight-through Cable Schematics

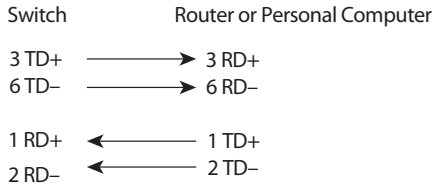
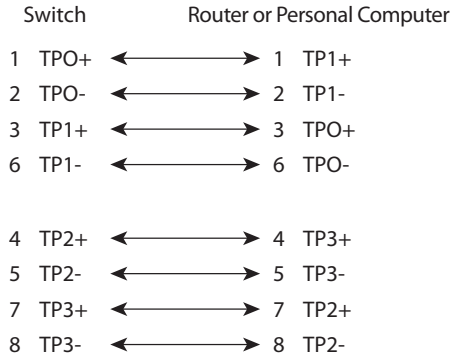


Figure 80 - Four Twisted-pair Straight-through Cable Schematics



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 81 and Figure 82 show the cable schematics.

Figure 81 - Two Twisted-pair Crossover Cable Schematics

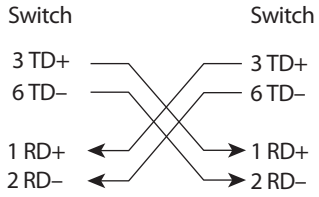
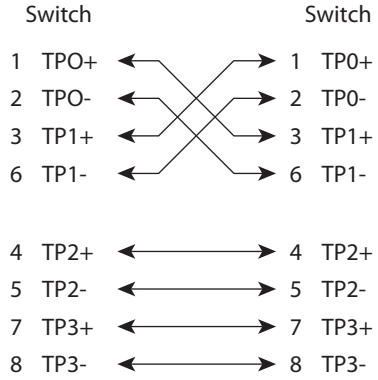


Figure 82 - Four Twisted-pair Crossover Cable Schematics

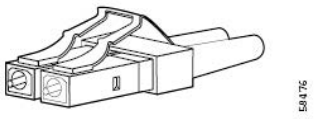


100Base-FX Ports

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 83 - 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.

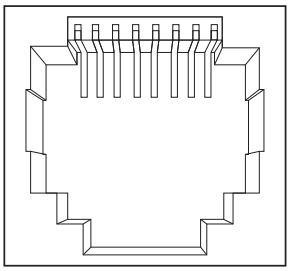
ATTENTION: Invisible laser radiation can be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

Dual-purpose Ports

The Ethernet port on a dual-purpose port uses standard RJ45 connectors. The following figure shows the pinouts.

Figure 84 - 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.

IMPORTANT Copper SFP modules cannot be used in dual-purpose (combo) ports.

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 213 lists the pinouts for the console port, the RJ45-to-DB-9 adapter cable, and the console device.

Table 213 - 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 214 - 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

68878
H1 Heading 1st Level
IEEE 1588 Power Profile 155

A

AAA 68
AAA Interface 83
AAA Methods 74
access Device Manager 41
access management 66
access port
choose 46
VLAN 0 priority tagging 242
ACLs 84 - 87
adapter pinouts
RJ45-to-DB-25 adapter 431
RJ45-to-DB-9 adapter 431
terminal
RJ45-to-DB-25 413, 420
RJ45-to-DB-9 413, 420
Add a Server Group 72
Add Accounting Methods 78
Add Authentication Method 74
Add Authorization Methods 75
address aliasing 156
address translation 167, 201
alert log 300
allocation, memory 23
announce interval 107
assign VLAN to NAT instance 173
Authentication, Authorization, and Accounting 68
Auto mode, PoE 233
auto-logout 41
auto-MDIX 430
autonegotiation
Duplex mode 46, 144
speed 46, 144
troubleshoot 337

B

Boundary mode 94, 99
BPDU Guard 275
broadcast storms 226

C

cable diagnostics 300
cables
connect to 10BASE-T and 100BASE-TX compatible devices 428
connect to console port 431
connect to dual-purpose ports 430
connect to fiber ports 429
crossover 410, 411, 416, 417, 418, 423, 424
damaged 334
Ethernet and fiber 334
identify 428
PoE module specifications 431
straight-through 410, 416, 417, 423
channel group, PRP 212, 302
CIP
data 39
enable for active ring DHCP server 117
enable on VLAN 34
CIP Sync Time Synchronization
compatible switches 16
overview 93
Cisco Discovery Protocol 329
CLI
access via console port 65
access via SSH 34, 65
access via Telnet 65
clock modes
Boundary 94, 106
End to End Transparent 96, 108
Forward 96, 108
NTP-PTP 96, 109
Configure AAA via Device Manager 68
Configure DLR VLAN Trunking via Device Manager 125
Configure IPDT via Device Manager 158
Configure REP Negotiated via Device Manager 251
connection faults 54
connectors and cables
10/100/1000 410, 416, 417, 423, 428
console 413, 420, 431
dual-purpose 418, 430
SC connectors 430
SFP module ports 430
console port
specifications 413, 420, 431
crossover cable 411, 418, 424, 429
cryptographic IOS software 111
customization
DHCP server 128, 131
IP address
DHCP IP address pool 130
switch port 130
IP address (for connected devices) 128
IP address for connected devices 131
Smartport roles 262

D

default gateway
NAT 167, 178, 188, 197
default router 130
delay request interval 107
Delete a Server Group 73
denial-of-service attack 226
Device Manager
access 41
auto-logout 41
hardware requirements 40
overview 40
software requirements 40
DHCP
clients 313
for ring devices 16
IP address pool 129, 131, 132
persistence 127, 130, 131
server 126
status 313
troubleshoot 336
DLR
active DHCP server IP address 117
compatible switches 16
enable CIP 117
features 113
overview 112
port choices 114
requirements and restrictions 113
ring nodes 112
status 313
switch as ring supervisor and DHCP server 124
via Device Manager 115
via Logix Designer application 118
DLR VLAN Trunking 125
DNS server1 and 2 130
domain name 130
DOT1Q standard 242
driver, Ethernet 201
dual-purpose ports
connectors and cables 418, 430
Duplex mode
default 46, 144
setting 46, 144
troubleshoot 337

E

Edit AAA Methods 83
Edit Radius Server Information 73
EIGRP 135 - 139
End to End Transparent mode 96, 101, 108
EtherChannels
configure via Device Manager 142
configure via Logix Designer application 145
example 140
overview 139
Ethernet drive 201
EtherNet/IP CIP interface 13
EtherNet/IP protocol 262, 311
Express Setup
button 24
global macro 38
Long Press mode 29
Medium Press mode 28
modes 26
Multi-mode 26
requirements 23
Short Press mode 27
Single-mode 30

F

factory default settings 29, 338
Fault/Program action 54
Feature mode 147
firmware upgrade, troubleshoot 339
Forward mode 96, 102
frame size 160
frequency bands 148
Full-duplex mode 46, 144

G

global macros
for CIP traffic 38
for motion traffic 38, 162
global navigation satellite system. See GNSS
GNSS 19, 148, 149, 150
GNSS status 290
GOOSE Messaging Support 277
GPS status indicator 290
GSD file 243, 245

H

Half-duplex mode 46, 144
hardware features 18
hardware requirements
Device Manager 40
high priority PoE ports 231
horizontal stacking 150
HSR
compatible switches 16
overview 150

I

IEEE 1588 Power Profile 93, 155, 277
IEEE 802.1Q standard 242
IEEE power classifications 232
IGMP snooping
and address aliasing 156
configure 157
definition 156
installation instructions 12
IOS software
cryptographic 111
non-cryptographic 111
IP address
active ring DHCP server 117
customization

connected devices 128, 131
DHCP IP address pool 130
switch port 130
DHCP IP address pool
ending range 130
starting range 130
switch port 130
assigning 130
deleting 130
modifying 130
translation 167
troubleshoot 336
DHCP 336
wrong IP address 336
IPDT 158

L

LC connector 429
lease length 130
link integrity, verify with REP 249
Link Layer Discovery Protocol 329
Linx-based software 38, 201
lite versus full firmware 15
locate switch
via Device Manager 285
via Logix Designer application 297
logout 41
Long Press mode Express Setup
overview 27
run 29
low priority PoE ports 231

M

macros
default global 162
Motion Prioritized QoS 162
QoS Priority Map 162
QoS Priority Queue 162
management interface
NAT 173
management VLAN 37, 278
Medium Press mode Express Setup
overview 27
requirements 23
run 28
memory 23
MIBs, supported 258
mismatch prevention, Smartport roles 263
mode
Access 262
Boundary 94, 99, 106
dual power 90
End to End Transparent 96, 101, 108
EtherChannel 141, 142
Express Setup 26
Feature 147
Forward 96, 102, 108
NTP-PTP Clock 96, 104, 109
Over-determined Clock 149
Plug-n-Play 31
PoE 233, 238, 240
Program 54
REP 250, 252
Restrict 222
Self-survey 149
STP 275, 276
Trunk 262
module-defined data types 341
monitor
alert log 300
CIP 311
DHCP clients 313
DLR 313
GNSS/GPS 290
NAT statistics 303
neighbors 329
port diagnostics 327
port mirroring 219
PROFINET 245
PRP 317
Motion Prioritized QoS macro 162
MTU 16, 160
multicast storm 226
Multi-mode Express Setup
overview 27
requirements 23
Multiple Spanning Tree Protocol (MSTP) 272

N

NAT
configuration considerations 174
configuration overview 167
configure via Device Manager Web interface 175 – 184
configure via Logix Designer application 185, 194, 195
definition 167
diagnostics 303, 306 – 308
management interface 173
traffic permits and fixups 174, 184, 194
translation entry types 172
native VLAN 281
NetFlow
compatible switches 17
configuration 165
overview 163
templates 164
network address translation. See NAT
network settings
configure via Device Manager 31, 33
configure via Logix Designer application 36
NTP
configure via Device Manager 203
overview 202

NTP-PTP Clock mode 96, 104, 109

O

OSPF 206 – 211
  compatible switches 17
Over-determined Clock mode, GNSS 149

P

Peer to Peer Transparent Mode 96
Per VLAN Spanning Tree Plus (PVST+) 272
pinouts
  10/100 ports 430
  crossover cables 429
    four twisted-pair, 1000BASE-T ports 411, 418, 424
  PoE 415, 427
  RJ45-to-DB-25 adapter 431
  RJ45-to-DB-25 terminal adapter 413, 420
  RJ45-to-DB-9
    adapter 431
    terminal adapter 413, 420
  SFP module 430
  straight-through cables
    two twisted-pair 410, 417, 423, 428
Plug-n-Play setup mode 31
PoE
  cable specifications 431
  compatible switches 17
  configure via Device Manager Web interface 231
  features 231 – 236
  initial power allocation 232
  pinouts 415, 427
  power management modes 233
  powered device detection 232
pool name 130
pop-up blockers 41
port
  assignments for CIP data 387, 393
  configuration 52
  numbering 46
  roles 264
  security 220, 222
  states 54
  status 299
  threshold 228
  thresholds 228
  type 250, 252
port mirroring
  configure via Device Manager 219
  overview 219
port settings
  auto-MDIX 46
  description 46, 144
  descriptions of 45
  Duplex mode 46, 144
  enable/disable 46
    default 46
  speed 46, 144
    default 46, 144
PortFast 275
power classifications 232
power priority 238
priority tagging 241, 281, 282
PROFINET
  compatible switches 17
  enable 244
  GSD file 243
  monitor 245
  overview 241
  Real-Time (RT) 241
  TCP/IP 241
  traffic forwarding 241
  VLAN 0 priority tagging 241
Program mode 54
proxy settings 41
PRP
  channel group 212
  configuration 214
  network components 211
  node and VDAN limitations 213
  overview 211
  port statistics 302
  RedBox 211, 214
  status 317
  traffic and supervisory frames 213
  troubleshoot via Device Manager 217
  via Device Manager 214
  via Logix Designer application 217
PTP
  compatible switches 16
  configure via Device Manager 97
  configure via Logix Designer application 105
  overview 93
PTP modes
  Boundary 94, 106
  End to End Transparent 96, 108
  Forward 96, 108
  NTP-PTP Clock 96, 109

Q

Qos Priority Map macro 162
QoS Priority Queue macro 162
QoS settings
  default 38, 162
  motion traffic 162

R

Rapid per VLAN Spanning Tree Plus (Rapid PVST+) 272
Real-Time (RT) PROFINET traffic 241
receiver, GNSS 148
recovery
  firmware upgrade 339
RedBox 211, 214
redundancy
  EtherChannel 141
redundant gateway 314, 316
remote connection 66
REP 246
  open segment 247
  ring segment 248
  segments 248
  verify link integrity 249
REP Admin VLAN 250

REP segments
configure 250
overview 246
reset factory defaults 338
reset, troubleshoot 338
Resilient Ethernet Protocol
see REP 246
restart with factory default settings 29
ring nodes
DLR 112
RJ45 connector, console port 431
RSWho 38

S

satellite constellation 148
SC connector 430
SD card
synchronize
configuration 58
synchronize IOS files 58
SD Flash Sync 62
SDM template 255
security
configure for ports 222
violations 222
segment ID 250
Self-survey mode, GNSS 149
Server Groups Sub-Tab 72
Server/Server Groups Tab 69
settings, factory default 29
SFP modules
connectors 430
Short Press mode Express Setup
overview 27
run 27
signaling, GNSS 149
Single-mode Express Setup
run 30
Smartport roles
applying 264
changing VLAN memberships 265
customization
optimize ports 262
mismatch prevention 263
Smartport roles and VLANs 270
SNMP
configuring 261
MIBs supported 258
snooping, IGMP 156
software features 16
customization
DHCP server settings 128, 131
Smartport roles 262
troubleshoot
firmware upgrade 63
software requirements
Device Manager 40
Spanning Tree Protocol 246, 272
See also Rapid Spanning Tree Protocol
specifications 12
speed
setting 46, 144
troubleshoot 337
SSH 65, 66
stacking, horizontal 150
Static mode, PoE 234
status indicators
Stratix 5400 288
Stratix 5410 290, 291
Stratix 8000/8300 292, 293
Stratix and ArmorStratix 5700 286
STCN interface 250, 252
STCN segment 250, 252
STCN STP 250, 252
storm control
described 226
thresholds 226
STP
BPDU Guard 275
configure via Device Manager 273
configure via Logix Designer application 276
MSTP 272
overview 272
PortFast 275
PVST+ 272
Rapid PVST+ 272
straight-through cable
pinout
two twisted-pair 10/100 ports 410, 411, 417, 418, 423, 424, 428, 429
subnet mask
DHCP IP address pool 130
subnet translation 172, 178, 182, 183, 187, 190
switch
configuration properties 51
installation
troubleshoot 333
installation instructions 12
manage via Device Manager 40
monitor
alert log 300
port mirroring 219
status 296
troubleshoot 333
Device Manager display 336
DHCP 336
firmware upgrade 339
IP address problems 336
reset switch 338
wrong IP address 336
sync interval 107
sync limit 107

T

tagging 281, 282
TCP/IP PROFINET traffic 241
Telnet 65, 66
threshold
port 228
traffic level 226
time synchronization
configure via Device Manager 97
configure via Logix Designer application 105
timing message settings 97, 105

traffic fixups and NAT 174, 184, 194
traffic permits and NAT 174, 184, 194
traffic suppression 226
translate IP addresses 167
translation entry types 172
troubleshoot
Device Manager display 336
DHCP 336
firmware upgrade 63, 339
IP address problems 336
PRP via Device Manager 217
reset switch 338
speed, duplex, and autonegotiation 337
switch 333
switch performance 337
wrong IP address 336
trunk port
choose 46
VLAN 0 priority tagging 242

U

unicast storm 226
upgrade firmware 63

V

VLAN 0 priority tagging
enable 46, 282
for PROFINET 241, 242
overview 281
priority values 281
VLAN memberships
changing 265
prerequisite 265
VLANs
access VLAN 46
allowed 46
assign to NAT instance 173, 177, 181, 186, 189
configure via Device Manager 279
configure via Logix Designer application 280
enable CIP 34
management VLAN 278
native VLAN 46, 281
overview 277
tagging 281

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)

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

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

Allen-Bradley, ArmorStratix expanding human possibility, FactoryTalk, Rockwell Automation, Rockwell Software, RSLogix 5000, RSNetWorx, Stratix, Studio 5000, and Studio 5000 Logix Designer are trademarks of Rockwell Automation, Inc.

CIP, CIP Sync, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, 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 EEE YÖnetmeliğine Uygundur

Connect with us.

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

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-UM007Q-EN-P - July 2022
Supersedes Publication 1783-UM007P-EN-P - November 2021

Copyright © 2022 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.