



Stratix 5200 and Stratix 5800 Managed Switches

Stratix 5200 Catalog Numbers 1783-CMS6B, 1783-CMS6P, 1783-CMS10B, 1783-CMS10P, 1783-CMS10DP, 1783-CMS10DN, 1783-CMS20DB, 1783-CMS20DP, 1783-CMS20DN

Stratix 5800 Catalog Numbers 1783-MMS10A, 1783-MMS10AR, 1783-MMS10B, 1783-MMS10BE, 1783-MMS10, 1783-MMS10E, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EA, 1783-MMS10EAR, 1783-MMX8T, 1783-MMX8E, 1783-MMX8S, 1783-MMX8SA, 1783-MMX8TA 1783-MMX6T2S, 1783-MMX16T, 1783-MMX16E, 1783-MMX14T2S, 1783-MMX8EA

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
Download Firmware, AOP, EDS, and Other Files 11
Additional Resources 11
Summary of Changes 12

Chapter 1

About the Switches

Stratix 5200 Switches 14
Stratix 5800 Switches and Expansion Modules 14
EtherNet/IP Interface 15
Software Features 15
Hardware Features 17
Front Panel Overview 17
Power Connectors 19
Alarm Connector 19
Console Ports 21
10/100/1000 BASE-T Downlink Ports 23
10/100/1000 PoE Ports (Stratix 5800 Switch Only) 25
100/1000 SFP Slots 26
Status Indicators 26

Chapter 2

Express Setup

Express Setup Modes 27
Express Setup Requirements and Recommendations 28
Express Setup Button 29
Run Express Setup in Short Press Mode 30
Run Express Setup in Medium Press Mode 31
Factory Default the Switch using Long Press Mode 32
Complete Express Setup via the WebUI 32
Complete Express Setup via the Logix Designer Application 37
Add the Switch to the Controller Project 37
Default Global Macro 41

Chapter 3

WebUI Basics

Requirements and Restrictions 43
Access the WebUI 44
Use the WebUI Toolbar 48
Set WebUI Preferences 49
Customize the Dashboard 50
Sort, Filter, and Customize Data in Columns 51

Configure the Switch

Chapter 4

Authentication, Authorization, and Accounting (AAA) . . . 54
- AAA Configuration . . . 54
- Configure AAA via the WebUI Wizard . . . 55
- Configure AAA Method Lists via the WebUI . . . 60
- Configure AAA Servers and Server Groups via the WebUI . . . 64
- Configure AAA Advanced Settings via the WebUI . . . 71

Access Control Lists (ACLs) . . . 75
- Configure ACLs via the WebUI . . . 75

Discovery Protocols . . . 78
- Cisco Discovery Protocol (CDP) . . . 78
- Link Layer Discovery Protocol (LLDP) . . . 78
- Configure Discovery Protocols via the WebUI . . . 79

Device Level Ring (DLR) Topology . . . 80
- Configure DLR Ring via WebUI . . . 80
- Configure DLR DHCP . . . 83
- DLR Port Choices . . . 85

Enhanced Interior Gateway Routing Protocol (EIGRP) (Stratix 5800 Switch Only) . . . 86
- Feature Summary . . . 86
- Network Operation . . . 86
- Configure EIGRP via the WebUI . . . 87

Ethernet Ports . . . 89
- Advanced Port Configuration . . . 89
- Configure Ethernet Interfaces via the WebUI . . . 89
- Configure VRF-Lite (Stratix 5800 Switch Only) . . . 97
- Configure Ethernet Ports via the Logix Designer Application . . . 98

Ethernet Ring G.8032 (Stratix 5200 Switch Only) . . . 100
- Add a Profile . . . 100
- Add a Ring . . . 101
- Edit or Delete Profile Rings . . . 102

Flow-based SPAN (FSPAN) . . . 103
- Configure FSPAN via the WebUI . . . 103

Logical Interfaces . . . 105
- Port Channels or EtherChannels . . . 105
- EtherChannel Modes . . . 105
- Configure Logical Interfaces via the WebUI . . . 107
- Loopback Interfaces . . . 108
- Configure EtherChannels via the Logix Designer Application . . . 109

High-availability Seamless Redundancy (HSR) (Stratix 5800 Switch Only) . . . 111
- Add an HSR Ring via the WebUI . . . 112
- Edit an HSR Ring Via WebUI . . . 114
- Configure Advanced HSR Settings via WebUI . . . 115

Hot Standby Router Protocol (HSRP) (Stratix 5800 Switch Only) . . . 117
- Configure HSRP via the WebUI . . . 117

Intermediate System-to-Intermediate System (IS-IS) (Stratix 5800 Switch Only) . . . 118
- Network Operation . . . 118
- Configure IS-IS via the WebUI . . . 119

IOx Services (Stratix 5800 Switch Only) . . . 120
Formatting Requirements for IOx via CLI . . . 120
Enable IOx via the CLI . . . 121
Enable IOx via the WebUI . . . 122
MACsec (Stratix 5800 Switch Only) . . . 123
MKA Policy . . . 124
Key Chain . . . 125
Media Redundancy Protocol (MRP) . . . 127
MRP Modes . . . 127
Protocol Operation . . . 127
Media Redundancy Automanager (MRA) . . . 129
Multiple MRP Rings . . . 129
MRP-STP Interoperability . . . 130
Requirements and Restrictions . . . 130
Configure MRP via the WebUI . . . 131
Multicast Services . . . 133
Configure Multicast Services via the WebUI . . . 133
NetFlow (Stratix 5800 Switch Only) . . . 134
Configure NetFlow via the WebUI . . . 135
Network Address Translation (NAT) . . . 137
Configuration Overview . . . 137
VLAN Assignments . . . 140
Traffic Permits and Fixups . . . 141
Configure NAT via the WebUI . . . 143
Configure NAT via the Logix Designer Application . . . 147
Open Shortest Path First (OSPF) Routing Protocol (Stratix 5800 Switch Only) . . . 153
Create an OSPF Route via the WebUI . . . 153
Parallel Redundancy Protocol (PRP) . . . 155
RedBox PRP Channel Groups . . . 156
Traffic and Supervisory Frames . . . 157
Node and VDAN Limitations . . . 157
Configuration Considerations . . . 157
Configure a Switch as a RedBox via the WebUI . . . 158
Port Security . . . 161
Configure Port Security via the WebUI . . . 161
Configure Port Security via the Logix Designer Application . . . 162
Quality of Service (QoS) . . . 163
Auto QoS Macros . . . 163
Configure QoS via the WebUI . . . 164
Remote Switch Port Analyzer (RSPAN) . . . 167
Configure RSPAN via the WebUI . . . 167
Resiliency Ethernet Protocol (REP) . . . 169
Default REP Configuration . . . 169
REP Over Port Channel . . . 169
Configuring the REP Administrative VLAN . . . 171
REP Port Types . . . 171
Configure REP via the WebUI . . . 172

Routing Information Protocol (RIP) 174
Configure RIP for Stratix 5800 Switch via WebUI 174
Smartports 175
Requirements and Restrictions 175
Avoid Smartport Mismatches 175
Smartport Roles 175
Assign Smartport Roles via the WebUI 176
Motion Prioritized QoS Macros 180
Assign Smartport Roles via the Logix Designer Application 181
Spanning Tree Protocol (STP) 182
Requirements and Restrictions 182
STP Modes 182
Multiple Spanning Tree (MST) 183
Configure STP via the WebUI 184
Configure STP via the Logix Designer Application 185
Static Routing 186
Configure Static Routing via the WebUI 186
Switched Port Analyzer (SPAN) 187
Requirements and Restrictions 187
Configure SPAN via the WebUI 187
TrustSec 190
TrustSec Security Groups 190
Security Group Tag Exchange Protocol 190
TrustSec Policies 191
CTS Interface Configuration 191
Configure TrustSec via the WebUI 192
Utility Features 199
GOOSE Messaging Support 199
Virtual Local Area Networks (VLANs) 200
Switch Virtual Interfaces (SVIs) 200
Supported VLANs 200
Management VLAN 200
Configure SVIs and VLANs via the WebUI 201
Configure VLANs via the Logix Designer Application 205
Virtual Router Redundancy Protocol (VRRP) (Stratix 5800 Switch Only) 206
Configure VRRP via the WebUI 206
Configure VRRP via WebUI 207
Virtual Routing and Forward (VRF) (Stratix 5800 Switch Only) 208
VLAN Trunk Protocol (VTP) 209
Requirements and Restrictions 209
VTP Modes 209
Configure VTP via the WebUI 210

Chapter 5

Administer the Switch

Alarm Profiles . . . 212
- Alarm Types . . . 212
- Alarm Actions . . . 212
- Default Alarm Profile . . . 212
- Create an Alarm Profile Via the WebUI . . . 213

Alarm Settings . . . 214
- External Alarm Devices . . . 214
- Global Alarm Types . . . 214
- Alarm Actions for Global Alarms . . . 215
- Configure Alarm Settings Via the WebUI . . . 215

Back Up and Restore Procedures . . . 218
- Back Up and Restore Configuration Files Via the WebUI . . . 218
- Back Up and Restore Sync Via the WebUI . . . 220
- Back Up, Restore, and Sync Configuration Files Via the Logix Designer Application . . . 221

Common Industrial Protocol (CIP) . . . 224
- Configure CIP Via the WebUI . . . 224

CIP Sync (PTP) . . . 224
- Configure Device Time Via the WebUI . . . 225
- Configure Device Time Via the Logix Designer Application . . . 232

Command-line Interface (CLI) . . . 238
- CLI Modes . . . 238
- Run CLI Commands Via the WebUI . . . 238

Device Settings . . . 239
- Configure Device Settings via the WebUI . . . 239
- Configure Device Settings Via the Logix Designer Application . . . 241

Device Time . . . 243
- Set Time Manually . . . 243
- Set Time Via NTP . . . 243

Domain Name System (DNS) . . . 244
- Add a DNS Server Via the WebUI . . . 244

Dynamic Host Configuration Protocol (DHCP) . . . 245
- DHCP Persistence . . . 245
- DHCP Snooping . . . 247
- Configure DHCP Via the WebUI . . . 247
- Configure DHCP Via the Logix Designer Application . . . 250

File Manager . . . 253

Field-programmable Gate Array (FPGA) Profiles (Stratix 5800 Switch Only) . . . 255
- Configure FPGA Profiles in WebUI . . . 255

HTTP/HTTPS/Netconf Access . . . 257
- Certificate Authority (CA) Trustpoints . . . 257
- Configure HTTP/HTTPS/Netconf/VTY Access Via the WebUI . . . 257

MODBUS . . . 258
- Requirements and Restrictions . . . 258
- Configure MODBUS Via the WebUI . . . 259

Power over Ethernet (PoE) (Stratix 5800 Switch Only) 260
Requirements and Restrictions 260
PoE Port Modes 260
Configure PoE via the WebUI 261
Configure PoE via the Logix Designer Application 263
PROFINET 264
Configure PROFINET via the WebUI 264
Reload the Switch Via the WebUI 266
SDM-Template 267
Secure Digital (SD) Card 268
Swap Drive 268
Procedure for Swap Drive 269
Simple Network Management Protocol (SNMP) 270
Supported SNMP Versions 270
SNMPv3 User Security Modes and Authentication 270
Configure SNMP Via the WebUI 271
Software Upgrade 275
Stratix 5200 Boot Order 276
Stratix 5800 Boot Order 276
User Administration 277
Privilege Levels 277
Password Policies 277
Create a User Account Via the WebUI 277

Chapter 6

Security Requirements (IEC-62443-4-2)

Switch Security Features 279
Telnet 280
Verify Telnet Settings 280
Disable Telnet 281
TLS 1.2 282
Verify TLS 1.2 Settings 282
Enable TLS 1.2 283
Additional Resources 283

Chapter 7

Monitor the Switch

Switch Status 286
Neighbors 287
CIP Sync (PTP) 289
PTP Details 289
PTP Clock Settings 290
PTP Parent Property 291
PTP Time Property 292
Common Industrial Protocol (CIP) 293
Device Level Ring (DLR) 295
Overview Tab 296
Faults Tab 296
Members Tab 297
Dynamic Host Configuration Protocol (DHCP) Clients 298
HSR (Stratix 5800 Switch Only) 299

VDAN . . . 299
Node . . . 299
HSRP (Stratix 5800 Switch Only) . . . 300
Network Address Translation (NAT) . . . 301
Monitor NAT Statistics via the WebUI . . . 301
Monitor NAT Statistics via the Logix Designer Application . . . 304
MODBUS (Modicon Communication Bus) . . . 307
Media Redundancy Protocol (MRP) . . . 309
Ports . . . 310
Monitor Ports via the WebUI . . . 310
Monitor Port Status via the Logix Designer Application . . . 312
PROFINET . . . 313
Parallel Redundancy Protocol (PRP) . . . 315
Monitor PRP via the WebUI . . . 315
Monitor PRP via the Logix Designer Application . . . 318
Resiliency Ethernet Protocol (REP) . . . 320
Spanning Tree Protocol (STP) . . . 322
Rapid Spanning Tree Protocol (RSTP) Mode . . . 322
System . . . 324
Inventory . . . 324
Memory Utilization . . . 325
CPU Utilization . . . 326
Time . . . 327
PTP . . . 327
PTP Serviceability . . . 330
VRRP (Stratix 5800 Switch Only) . . . 337
Monitor VRRP . . . 337

Chapter 8

Troubleshoot the Switch

Configure and View System Logs . . . 339
Message Severity Levels . . . 339
Download Core Files . . . 342
Download a Debug Bundle . . . 343
Troubleshoot with Ping and Trace Route . . . 344
Ping Destinations . . . 345
Discover Route Information . . . 345
Troubleshoot the Installation . . . 346
Bad or Damaged Cable . . . 346
Ethernet and Fiber Cables . . . 346
Port Status . . . 346
SFP Module Issues . . . 347
Port Settings . . . 347
Troubleshoot IP Addresses . . . 347
Troubleshoot the WebUI . . . 348
Troubleshoot Switch Performance . . . 348
Automatic Device Descriptive Analytics (ADDA) . . . 349
Considerations for Communication Loss Diagnostics . . . 349
Display Code Definitions . . . 350

Appendix A

Status Indicators

Stratix 5200 Status Indicators 351
Port Status Indicators 352
Stratix 5800 Status Indicators 352
Power Status Indicators 353
Power over Ethernet Status Indicator (Stratix 5800 Switch Only) 353
Setup Status Indicator 354
EIP Status Indicators 354
Alarm Status Indicators 355
Port Status Indicators 355

Appendix B

Data Types

Stratix 5200 Data Types 357
6-Port Data Types 358
10-Port Data Types 360
20-Port Data Types 363
Stratix 5800 Data Types 367
10-Port Data Types 367
18-Port Data Types 368
26-Port Data Types 370

Appendix C

Port Assignments for CIP Data

Port Assignments 375

Appendix D

Port Numbering

Switch Port Numbering 377
Expansion Module Port Numbering 382

Appendix E

MODBUS Register Lists

Stratix 5200 Register Files 385
Stratix 5200 6-port Register Files 385
Stratix 5200 10-port Register Files 386
Stratix 5200 20-port Register Files 387
Stratix 5800 Register Files 389
Stratix 5800 10-port Register Files 389
Stratix 5800 18-port Register Files 390
Stratix 5800 26-port Register Files 393
System Register File 396

Appendix F

History of Changes

Change Log 397

Index 401

About This Publication

This publication describes how to configure, manage, and troubleshoot Stratix® 5200 and Stratix 5800 managed Ethernet switches and expansion modules.

This manual assumes that you understand the following:

- Ethernet concepts and terminology
- Local area network (LAN) switch fundamentals

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.

Download Firmware, AOP, EDS, and Other Files

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

Additional Resources

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

Resource	Description
Stratix Ethernet Device Specifications Technical Data, publication 1783-TD002	Provides specifications for the switches and other devices.
Stratix 5800 Modular Managed Ethernet Switches Installation Instructions, publication 1783-IN013	Describes how to install Stratix 5800 switches and expansion modules.
Online Help within the Web user interface (WebUI) (provided with the switch)	Provides context-sensitive Help for pages within the WebUI.
EtherNet/IP Network Devices User Manual, ENET-UM006	Describes how to configure and use EtherNet/IP™ devices with a Logix 5000® controller and communicate with various devices on the Ethernet network.
Ethernet Reference Manual, publication ENET-RM002	Describes basic Ethernet concepts, infrastructure components, and infrastructure features.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001	Represents a collaborative development effort from Rockwell Automation® and Cisco Systems®. Adds to design guidelines from the Cisco® Ethernet-to-the-Factory (EttF) solution and the Rockwell Automation Integrated Architecture® system.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications	Provides declarations of conformity, certificates, and other certification details.

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

Summary of Changes

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

Topic	Page
Precision Time Protocol (PTP)	16
Wiring for the Alarm Connector	20
Complete Express Setup via the WebUI	32
Account Settings	33
Add an Access Control List	76
Device Level Ring (DLR) Topology	80
DLR Port Choices	85
Configure Interface Advanced	91
Ethernet Ring G.8032 (Stratix 5200 Switch Only)	100
Configure Port Channels	106
RedBox PRP Channel Groups	156
Resiliency Ethernet Protocol (REP)	169
Assign Smartport Roles via the WebUI	176
Multiple Spanning Tree (MST)	183
Configure SVIs	201
Create SVI	202
Configure VLANs	203
Configure Global Alarms	216
CIP Sync (PTP)	224
Device Settings	239
Add a DNS Server Via the WebUI	244
Configure HTTP/HTTPS/Netconf/VTY Access Via the WebUI	257
PROFINET	313
Spanning Tree Protocol (STP)	322
Download a Debug Bundle	343
Automatic Device Descriptive Analytics (ADDA)	349
Port Status Indicators	352
Power over Ethernet Status Indicator (Stratix 5800 Switch Only)	353

About the Switches

Topic	Page
Stratix 5200 Switches	14
Stratix 5800 Switches and Expansion Modules	14
EtherNet/IP Interface	15
Software Features	15
Hardware Features	17

The Stratix® 5200 have up to 20 gigabit Ethernet interfaces and deliver high-speed gigabit Ethernet connectivity. The switches support Layer 2 switching on all gigabit platforms.

The Stratix 5800 managed switches support Layer 2 and Layer 3 switching on an all gigabit platforms. The hybrid design includes both standalone and modular switches. The platform supports up to 26 ports with various copper, PoE, and fiber SFP options, providing flexibility for high-performance network applications.

Stratix 5200 Switches

The following table describes the types of Stratix 5200 modules. For details by catalog number, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD002.



Device	Description
Base switches	High-speed and Gigabit Ethernet, Layer 2, fixed switches. Available in 6, 10, and 20-port versions.

Stratix 5800 Switches and Expansion Modules

The following table describes the types of Stratix 5800 modules. Some switch and expansion modules support advanced Ethernet features and Power over Ethernet (PoE). For details by catalog number, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD002.

IMPORTANT Only one expansion module can be attached to a modular switch.



Stratix 5800 Switches and Expansion Modules

Devices	Description
Fixed switches	Gigabit Ethernet, Layer 2, fixed switches. Available in 10-port versions.
Modular switches	Gigabit Ethernet, Layer 2 or Layer 3, modular switches. Advanced feature support on some models. Available in 10-port versions.
Expansion modules	Gigabit Ethernet expansion modules. Advanced feature support on some models. Available in 8- and 16-port versions.

EtherNet/IP Interface

Stratix 5200 and 5800 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. CIP is a messaging protocol for devices in industrial automation control systems.

For more information about the EtherNet/IP protocol and CIP, see the Ethernet Reference Manual, publication ENET-RM002.

Software Features

Switch software features can be configured in the web user interface (WebUI) for the switch, the Studio 5000 Logix Designer® application, or both, as shown in Table 1.

All features, including additional features that are not described in this publication, are configurable via the Cisco® command-line interface (CLI). See CIP Sync (PTP) on page 224.

Table 1 - Supported Catalog Numbers and Software for Switch Features

Feature	Stratix 5200 Catalog Numbers	Stratix 5800 Catalog Numbers	WebUI	Logix Designer Application
Authentication, authorization, and accounting (AAA)	All	All	Yes	No
Access control lists (ACLs)	All	All	Yes	No
Alarm profiles	All	All	Yes	No
Cisco® Discovery Protocol (CDP)	All	All	Yes	No
Common Industrial Protocol (CIP) monitoring	All	All	Yes	No
Device Level Ring (DLR) Toplogy	1783-CMS10DP, 1783-CMS10DN, 1783-CMS20DB, 1783-CMS20DP, 1783-CMS20DN	1783-MMS10A, 1783-MMS10AR, 1783-MMS10EA, 1783-MMS10EAR, 1783-MMX8EA, 1783-MMX8TA, 1783-MMX8SA	Yes	No
Domain name system (DNS)	All	All	Yes	No
Dynamic Host Configuration Protocol (DHCP)	All	All	Yes	Yes
Enhanced Interior Gateway Routing Protocol (EIGRP)	–	1783-MMS10R, 1783-MMS10AR, 1783-MMS10ER, 1783-MMS10EAR(1)	Yes	No
Express Setup	All	All	Yes	Yes
Field-programmable Gate Array Profiles (FPGA)	–	1783-MMS10A, 1783-MMS10AR, 1783-MMS10EA, 1783-MMS10EAR, 1783-MMX8EA, 1783-MMX8TA, 1783-MMX8SA	Yes	No
Generic Object Oriented Substation Events (GOOSE) Messaging Support	1783-CMS6P, 1783-CMS10P, 1783-CMS10DP, 1783-CMS10DN, 1783-CMS20DP, 1783-CMS20DN	All	No	No
HSR	–	1783-MMS10A, 1783-MMS10AR, 1783-MMS10EA, 1783-MMS10EAR, 1783-MMX8EA, 1783-MMX8TA, 1783-MMX8SA	Yes	No
HTTP/HTTPS	All	All	Yes	No
Intermediate System-to-Intermediate System (IS-IS)	–	1783-MMS10AR, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No
IOx	–	1783-MMS10A, 1783-MMS10AR, 1783-MMS10EA, 1783-MMS10EAR	Yes	No
Link Layer Discovery Protocol (LLDP)	All	All	Yes	No
Logical interfaces (EtherChannel/Port Channel)	All	All	Yes	Yes
Media Redundancy Protocol (MRP)	All	All	Yes	No
Multicast services and Internet Group Management Protocol (IGMP)	All	All	Yes	No
NetFlow	–	1783-MMS10, 1783-MMS10A, 1783-MMS10AR, 1783-MMS10E, 1783-MS10EA, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No

Table 1 - Supported Catalog Numbers and Software for Switch Features (Continued)

Feature	Stratix 5200 Catalog Numbers	Stratix 5800 Catalog Numbers	WebUI	Logix Designer Application
Network Address Translation (NAT)	1783-CMS10DN, 1783-CMS20DN	1783-MMS10, 1783-MMS10A, 1783-MMS10AR, 1783-MMS10E, 1783-MMS10EA, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	Yes
Network Time Protocol (NTP)	All	All	Yes	Yes
Open Shortest Path First (OSPF)	—	1783-MMS10AR, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No
Parallel Redundancy Protocol (PRP)	1783-CMS10DN, 1783-CMS20DN	1783-MMS10A, 1783-MMS10AR, 1783-MMS10EA, 1783-MMS10EAR, 1783-MMX8EA, 1783-MMX8TA, 1783-MMX8SA	Yes	Yes
Port mirroring/Switch Port Analyzer (SPAN)	All	All	Yes	No
Port security (MAC ID-based)	All	All	Yes	Yes
Port thresholds	All	All	Yes	No
Power over Ethernet (PoE)	—	1783-MMS10BE, 1783-MMS10E, 1783-MMS10EA, 1783-MMS10ER, 1783-MMS10EAR, 1783-MMX8E, 1783-MMX8EA, 1783-MMX16E	Yes	Yes
Precision Time Protocol (PTP)	1783-CMS6P, 1783-CMS10DP, 1783-CMS10P, 1783-CMS10DN, 1783-CMS20DP, 1783-CMS20DN	All	Yes	Yes
Quality of Service (QoS)	All	All	Yes	No
Resilient Ethernet Protocol (REP)	All	All	Yes	No
Routing, Layer 3	—	1783-MMS10AR, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No
Routing, static and connected	All	All	Yes(2)	No
Simple Network Management Protocol (SNMP)	All	All	Yes	No
Smartports	All	All	Yes	Yes
Spanning Tree Protocol (STP)	All	All	Yes	Yes
Syslog	All	All	Yes	No
TrustSec	—	1783-MMS10AR, 1783-MMS10EAR, 1783-MMX8EA, 1783-MMX8TA, 1783-MMX8SA	Yes	No
Virtual local area networks (VLANs)	All	All	Yes	Yes
VLAN Trunk Protocol (VTP)	All	All	Yes	No
VRF-Lite	—	1783-MMS10AR, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No

(1) Expansion modules that are compatible with the listed layer 3 catalog numbers.

(2) Only static routing can be configured via the WebUI. Connected routing is enabled by default and cannot be disabled.

Hardware Features

For detailed hardware specifications, see the Ethernet Device Specifications Technical Data, publication 1783-TD002.

Front Panel Overview

Stratix 5200

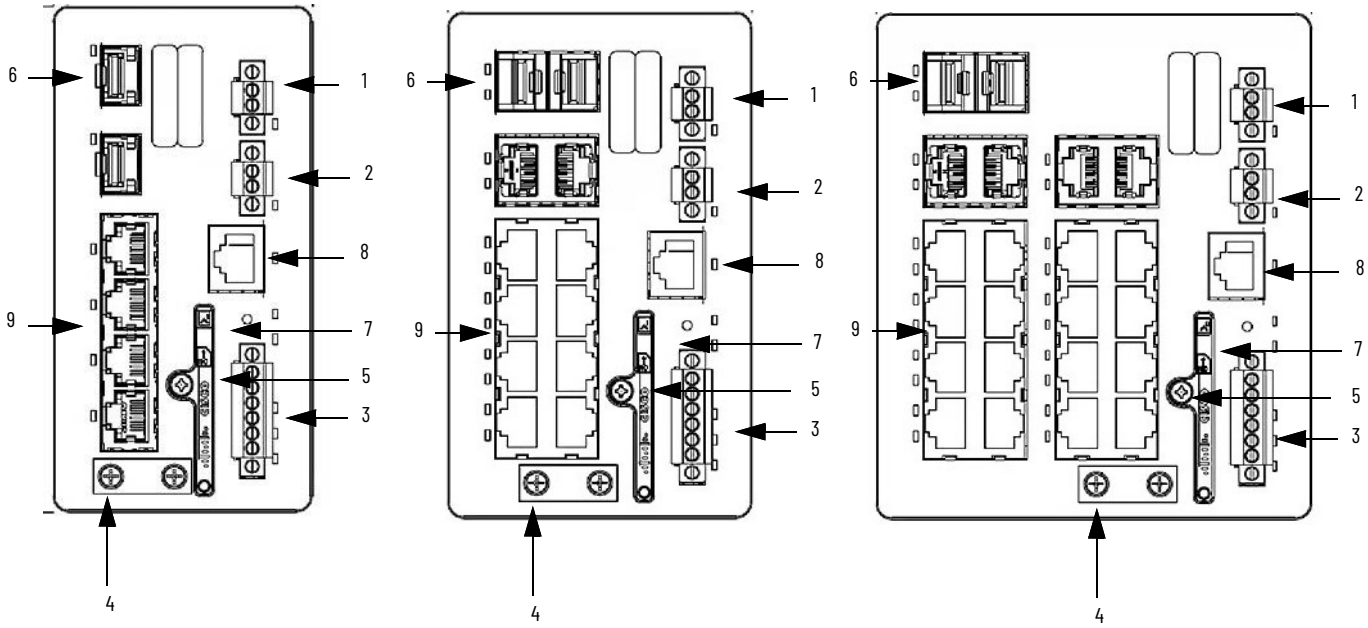


Table 2 - Stratix 5200 Front Panel

Item	Description
1	Power connector (Pwr A)
2	Power connector (Pwr B)
3	Alarm connector
4	Protective ground connection
5	SD card slot
6	SFP module slots (uplink ports)
7	USB micro console port
8	RJ45 console port
9	Ethernet ports (downlink ports)

Stratix 5800 Switch

For illustration purposes, the Stratix 5800 switch and expansion catalog numbers that are shown in the following example have PoE ports. Port types and combinations vary by catalog number, and not all models have PoE ports.

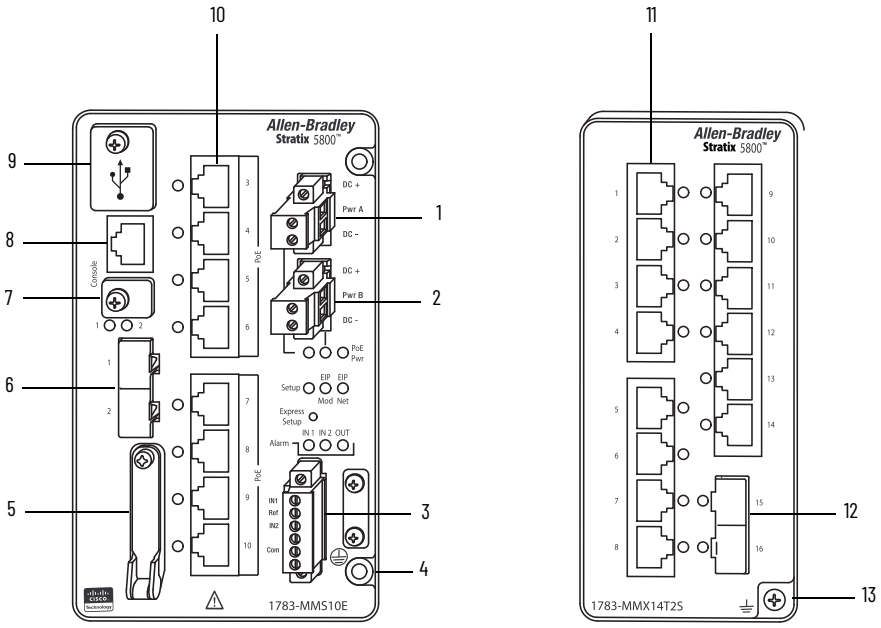


Table 3 - Stratix 5800 Front Panel

Item	Description
1	Power connector (Pwr A)
2	Power connector (Pwr B)
3	Alarm connector
4	Protective ground connection
5	SD card slot
6	SFP module slots (uplink ports)
7	USB mini-Type B console port
8	RJ45 console port
9	2 USB Type A ports
10	Ethernet PoE/PoE+ ports (downlink ports)
11	Ethernet ports (downlink ports)
12	SFP module slots (downlink ports)
13	Electromagnetic compatibility (EMC) ground connection(1)

(1) When an expansion module is connected, it must be grounded using the screw on the expansion module. This is an EMC ground, not a protective ground, unlike the one on the switch.

Power Connectors

You connect the DC power to the switch through the front panel connectors. The switch has a dual-feed DC power supply:

- One connector provides primary DC power.
- A second connector provides secondary DC power.

The two connectors are physically identical. On the Stratix 5800 switch, there is no separate power connector for PoE.

The switch can operate with one power source or with dual power sources. When both power sources are operational, the switch draws power from the DC source with the higher voltage. If one of the two power sources fail, the other continues to power the switch without interruption.

Alarm Connector

You connect the alarm signals to the switch through the alarm connector. The alarm connector is attached to the switch front panel with the provided captive screws.

The switch supports two alarm inputs and one alarm output relay.

- In the WebUI for the switch, you can configure each alarm input as an open or closed contact. See Configure Alarm Relays on page 215.
- The alarm output circuit is a relay with a normally open and a normally closed contact. Normally open contacts close. Normally closed contacts open. The alarm output relay can be used to control an external alarm device, such as a bell or a light.

For information about how to configure alarm settings, see page 214.

Figure 1 - Wiring for the Alarm Connector

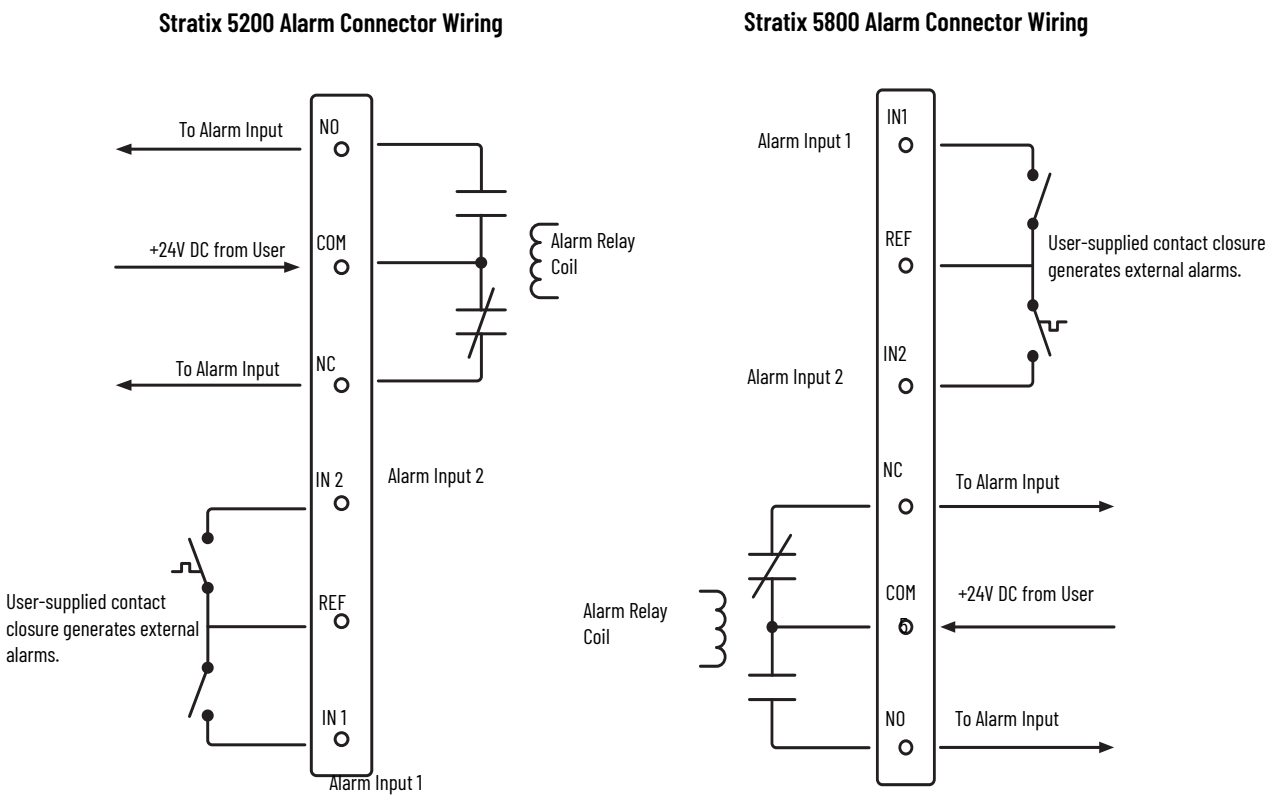


Table 4 - Alarm Connector Labels

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

Console Ports

The console ports on the switch enable you to configure, monitor, and manage the switch via the Cisco command-line interface (CLI). Use the console ports to connect to a workstation with terminal software on a Microsoft Windows® machine.

You can connect to either the RJ45 console port, the USB mini-Type B console port, also referred to as the USB-mini console port, or the USB-micro Type A console port (Stratix 5200 Switch Only). Only one console port can be active at one time.

The console ports use the following connectors:

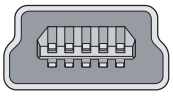
- RJ45 to DB-9 female cable for the RJ45 console port
- 5-pin mini-Type B to USB Type A cable for the USB-mini console port (Stratix 5800 Switch Only)
- USB Type A to 5-pin USB micro-Type B (Stratix 5200 Switch Only)
- RJ45 to USB Type A cable for the RJ45 console port (Allen-Bradley® catalog number 9300-USBCBL-CNSL)

The USB console interface speeds are the same as the RJ45 console interface speeds.

To use the USB-mini console port, you must install the USB device driver on the device that is connected to the USB-mini console port. For more information on how to download the mini USB driver, visit the Rockwell Knowledge base page https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/544134/loc/en_US#__highlight

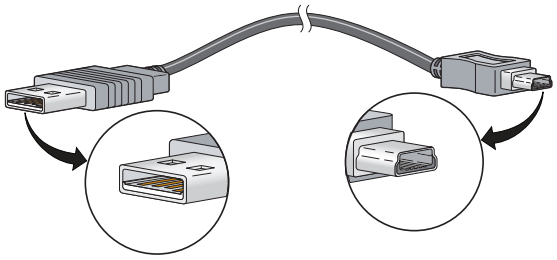
The 5-pin mini-Type B connectors resemble the 4-pin mini-Type B connectors, but they are not compatible. Use only the 5-pin mini-Type B as shown in Figure 2.

Figure 2 - USB Mini-Type B Port



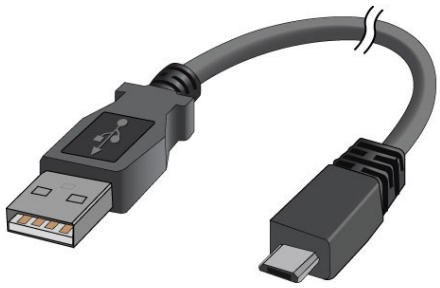
The USB console port on a Stratix 5800 switch uses a USB Type A to 5-pin mini-Type B cable as shown in Figure 3. The USB cable is not provided with the switch.

Figure 3 - USB Mini Cable



The USB console port on a Stratix 5200 uses a USB Type A to 5-pin USB micro-Type B as shown in Figure 4. The USB cable is not provided with the switch.

Figure 4 - USB Micro Cable



If the USB-mini or USB-micros console ports are activated, but no input activity occurs for a configured time period, the timeout reactivates the RJ45 console port. When the port deactivates due to a timeout, disconnect and reconnect the USB cable to restore its operation.

Table 5 lists the pinouts for the console port, the RJ45-to-DB-9 adapter cable, and the console device. The adapter cable is not supplied with the switch.

Table 5 - 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

Table 6 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 6 - 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

Table 6 - Pinouts with DB-25 Pin

Switch Console Port (DTE)	RJ45-to-DB-25 Terminal Adapter	Console Device
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

10/100/1000 BASE-T Downlink Ports

The copper Ethernet ports can operate at 10,100, or 1000 Mbps and full-duplex or half-duplex. You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3AB. The default setting is autonegotiated.

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.

When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. The auto-MDIX feature is enabled by default.

Follow these cabling guidelines when the auto-MDIX feature has been disabled:

- To connect two ports when only one port is designated with an X, use a straight-through cable. To connect two ports when both ports are designated with an X or when both ports do not have an X, use a crossover cable.
- To connect the ports to compatible devices, such as workstations, servers, and routers, use a two or four twisted-pair, straight-through cable that is wired for 10Base-T, 100Base-TX, 1000Base-T:
  - 10Base-T traffic can use Category 3 or Category 4 cables.
  - 100Base-TX traffic requires Category 5 cables.
  - 1000Base-T traffic requires four twisted-pair Category 5 cables.

Figure 5 and Figure 6 show the cable schematics.

Figure 5 - Two Twisted-pair Straight-through Cable Schematics

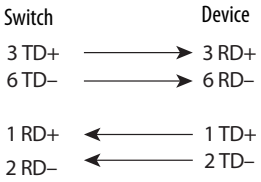
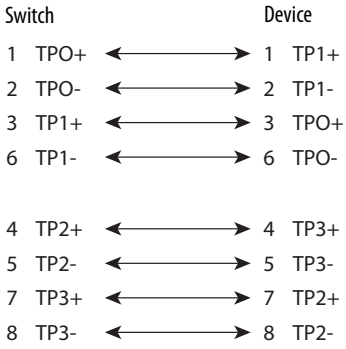


Figure 6 - Four Twisted-pair Straight-through Cable Schematics



To connect 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. 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. Be sure that the wires for the pins on the outside of the left plug and inside of the right plug are different colors.

Figure 7 and Figure 8 show the cable schematics.

Figure 7 - Two Twisted-pair Crossover Cable Schematics

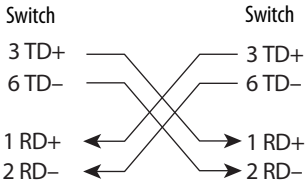
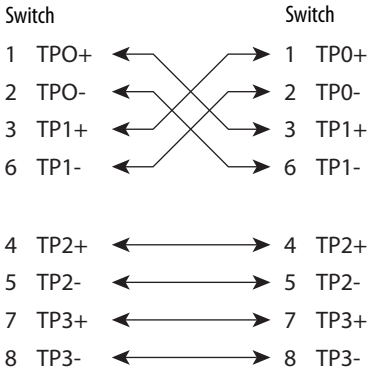


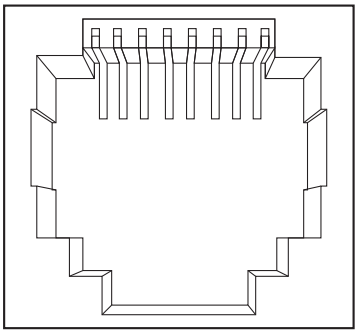
Figure 8 - Four Twisted-pair Crossover Cable Schematics



Copper Ethernet ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

Figure 9 - 10/100/100 Connector Pinouts

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



10/100/1000 PoE Ports (Stratix 5800 Switch Only)

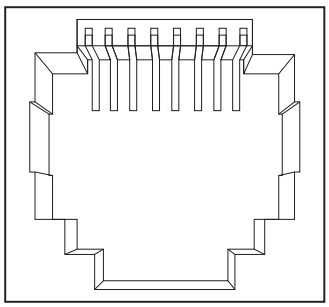
Gigabit Ethernet PoE/PoE+ ports are available on some switches and expansion modules. The ports provide full-duplex 10 Mbps, 100 Mbps, or 1000 Mbps connectivity. These ports can be configured for PoE (IEEE 802.3af) or PoE+ (IEEE 802.3at Type 2). You can configure PoE/PoE+ ports in any combination of PoE and PoE+.

PoE/PoE+ ports require four twisted-pair Category 5 cables.

PoE/PoE+ ports integrate power and data signals on the same wires. The ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

Figure 10 - 10/100/1000 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	



100/1000 SFP Slots

The IEEE 802.3u 1000 Mbps SFP slots provide full-duplex 1000 Mbps connectivity over multimode (MM) fiber cables or singlemode (SM) fiber cables. These ports use an SFP module that accepts a dual LC connector.



ATTENTION: Only use SFP modules from Rockwell Automation. For details about supported modules, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD002.
Stratix 5800 and 5200 switches do not support SFP catalog numbers 1783-SFP100T, 1783-SFP10GSRE, and 1783-SFP10GLRE.

Status Indicators

The status indicators on the front panel of the switch enable you to monitor the switch status, activity, and performance. For more information about status indicators, see Appendix A.

Express Setup

Topic	Page
Express Setup Modes	27
Express Setup Requirements and Recommendations	28
Express Setup Button	29
Run Express Setup in Short Press Mode	30
Run Express Setup in Medium Press Mode	31
Factory Default the Switch using Long Press Mode	32
Complete Express Setup via the WebUI	32
Complete Express Setup via the Logix Designer Application	37
Default Global Macro	41

Use the Express Setup process to perform these initial setup tasks:

- Assign the switch an IP address. You can then access the switch through the IP address for additional configuration.
- Run the global macro to set initial configuration parameters as described on page 41.

Express Setup Modes

Express Setup has three modes:

- Short Press mode—You want to use a directly connected computer to enter the initial IP address of the switch. You can then configure additional network settings via the WebUI. To run Short Press mode, see page 30.
- 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 the WebUI or the Studio 5000 Logix Designer® application. To run Medium Press mode, see page 31.
- Long Press mode—You want to reset the switch to use factory default settings. To run Long Press mode, see page 32.

IMPORTANT The Studio 5000 Logix Designer application supports only Medium Press mode.

Table 7 summarizes the function of each mode.

Table 7 - Express Setup Modes

Attribute	Short Press Mode	Medium Press Mode	Long Press Mode
Enable method	Press and hold the Express Setup button until the Setup status indicator flashes green during seconds 1...5, and then release.	Press and hold the Express Setup button until the Setup status indicator flashes red during seconds 6...10, and then release.	Press and hold the Express Setup button until the Setup status indicator flashes alternating green and red during seconds 16...20, and then release.
		Between seconds 11...15 and after 21 seconds, the Setup status indicator turns off. If you release the Express Setup button while the Setup status indicator is off, no Express Setup mode is enabled.	
Setup status indicator	Flashes green between seconds 1...5.	Flashes red between seconds 6...10.	Flashes green and red between seconds 16...20.
Function	The Express Setup management interface is selected. The switch acts as a DHCP server on VLAN 1000 with an address of 192.168.1.254. Once the DHCP session is successfully established, the switch assigns the computer an IP address of 192.168.1.1. The default login credentials are set to the following: User name: admin Password: switch	The switch sends a DHCP client request out of all ports on VLAN 1. DHCP assigns VLAN 1 an IP address. The default login credentials are set to the following: User name: admin Password: switch CIP™ (Common Industrial Protocol) is enabled on VLAN 1 with the CIP password set to **switch**.	All configuration settings (config.text, vlan.dat, and private-config.text files) in internal memory or on the SD card are reset to factory defaults. The switch restarts with factory default settings.
Software Tool for Express Setup Configuration	WebUI only	WebUI or Logix Designer application	Not applicable

Express Setup Requirements and Recommendations

All Express Setup modes require a small tool, such as a paper clip to press the Express Setup button.

In Short Press mode, you are required to complete Express Setup parameters via the WebUI. You need the following:

- A workstation with a supported operating system and browser. See Table 8.
- A straight-through or crossover Category 5 Ethernet cable to connect your workstation to the switch port.

In Medium Press mode, you can complete Express Setup parameters via the WebUI or the Logix Designer application. You need the following:

- For the WebUI, you need a supported operating system and browser. See Table 8.
- For the Logix Designer application, you need the Add-on Profile (AOP) for Stratix® switches, version 19.01.07 or later.
- A DHCP server and a Category 5 Ethernet cable to connect to the DHCP server.

Table 8 - Express Setup Recommendations

Component	Minimum Version
Operating System	
Microsoft® Windows	7 or higher
Apple Mac OS	10.9.5 or later
Browser	
Google Chrome	59 or later
Microsoft Edge	40 or later
Mozilla Firefox	60 or later
Screen Resolution	
1280 x 800 or higher	

Before you begin, do the following:

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

Express Setup Button

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

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

Figure 11 - Stratix 5200 Switch

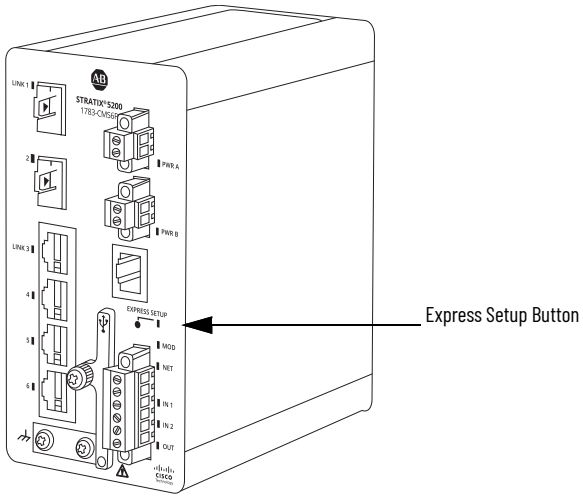
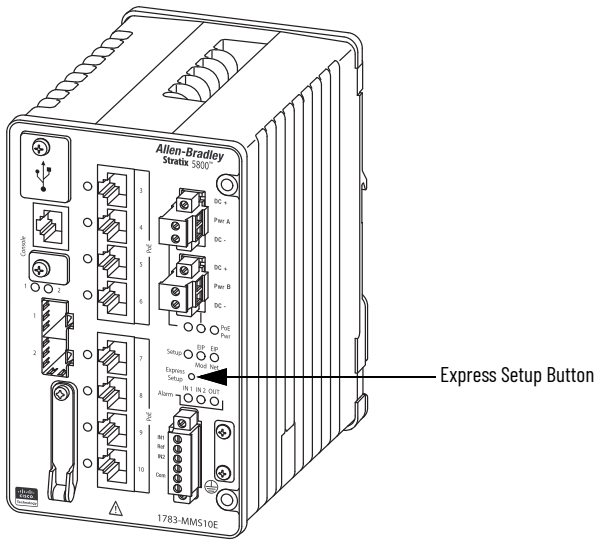


Figure 12 - Stratix 5800 Switch



Run Express Setup in Short Press Mode

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

Table 9 - Conditions in 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 60 minutes after an IP address is assigned to the computer.	The Setup status indicator turns off, but the connected port status indicator remains on.
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 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 long as 90 seconds (Stratix 5800 switch) and 140 seconds (Stratix 5200 switch) to complete.

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

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

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

3. Press and hold the Express Setup button until the Setup status indicator flashes green during seconds 1...5, and then release.

   The Stratix 5200 switch selects a port to use for Express Setup. Port Gi1/3 for DN, DP and P platforms and Port Fa1/3 on DB and B platforms blink green after a short press.

   The Stratix 5800 switch selects a port to use for Express Setup on Port Gi1/3.

4. Connect a Category 5 Ethernet cable from the flashing switch port to the Ethernet port on your workstation:
   - The status indicator for the port connected to the computer changes from flashing green to solid green.
   - The switch acts as a DHCP server on VLAN 1000 with an address of 192.168.1.254.
   - The switch assigns the computer an IP address of 192.168.1.1.
   - The Setup status indicator changes from flashing green to solid green.
5. Proceed to Complete Express Setup via the WebUI on page 32.

Run Express Setup in Medium Press Mode

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

Table 10 - Conditions in 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.	
No browser session is started for 60 minutes after an IP address is assigned to the computer.	The Setup status indicator turns off, but the connected port status indicator remains on.

IMPORTANT Before you begin, make sure that your system has a DHCP server that is configured to assign the switch an IP address.

To run 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 long as 90 seconds to complete.

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

- If the switch fails the sequence, the EIP Mod status indicator turns red**.**
- If you do not press the Express Setup button within 5 minutes after the sequence completes, the Setup status indicator turns off. 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 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 switch sends a DHCP request out of all ports on VLAN 1.
- DHCP assigns VLAN 1 an IP address.
- The default login credentials are set to the following:
  - User name: admin
  - Password: switch
  - CIP is enabled on VLAN 1 with CIP security password set to **switch**.

4. Complete the Express Setup configuration via the WebUI or the Logix Designer application:

- To use the WebUI, proceed to Complete Express Setup via the WebUI on page 32.
- To use the Logix Designer application, proceed to Complete Express Setup via the Logix Designer Application on page 37.

Factory Default the Switch using Long Press Mode

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.

IMPORTANT	Long Press mode overwrites all existing configuration files on both internal memory and external memory (SD card and USB Flash) and resets the switch back to factory default configuration.

Complete Express Setup via the WebUI

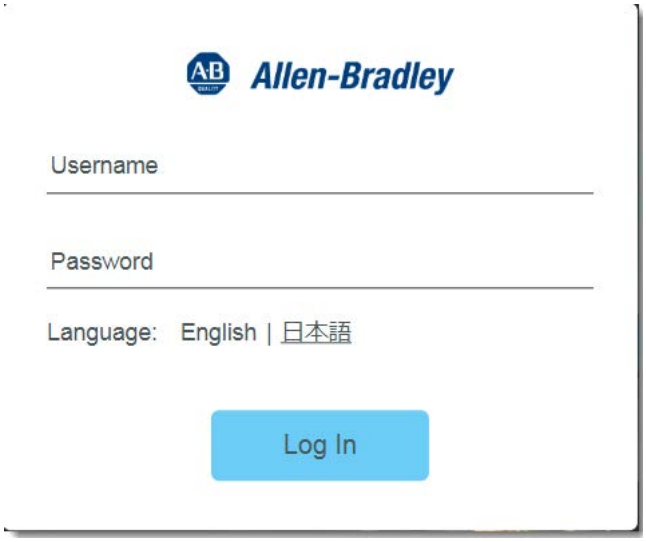
To complete the initial setup of the switch via the WebUI, follow these steps.

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

   For help with browser security options, see page 44.

   If the Login 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. On the Login page, enter the administrator user name and password, and click Login Now.
   - User name: admin
   - Password: switch



3. Configure account settings as described in Table 11, and then click Basic Settings.

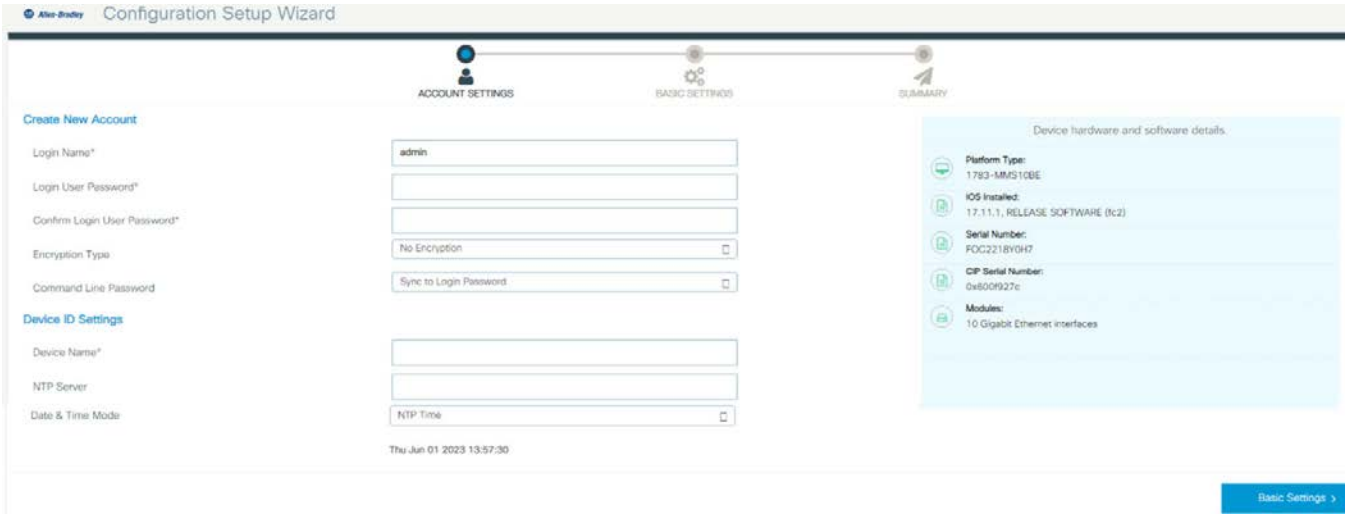
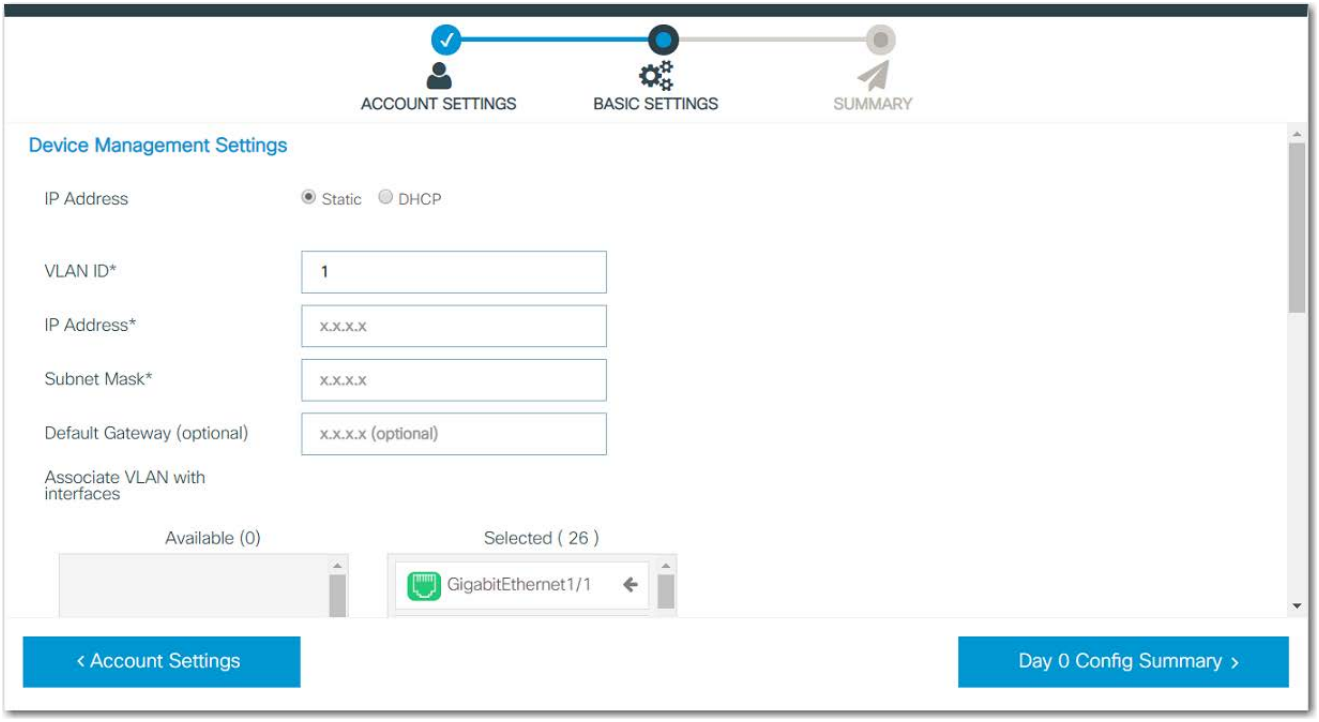


Table 11 - Account Settings

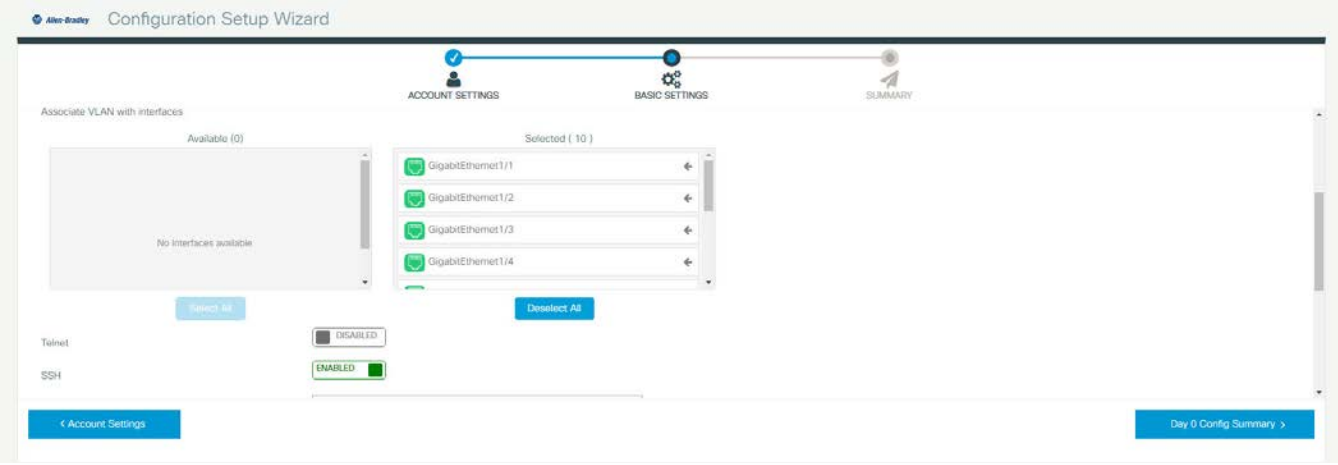
Field	Description
Create New Account	
Login Name	Enter a user name for the administrator.
Login User Password	Enter a password for the administrator.
Confirm Login User Password	Reenter the password for the administrator user.
Encryption Type (Stratix 5800 Switch Only)	The encryption types are: • No encryption • Type-6 and Type-7 encryption(1) - more secure - This is true encryption using 128 bit AES counter mode. The user defines a primary key which is used by IOS XE to encrypt the password. – **IMPORTANT** - The encrypted password that is visible in the running-config cannot be copied between devices unless the original primary Key is configured on the new device. • Type-7 encryption - less secure than type-6 - These use the Vigenerecipher, a simple algorithm. An attempt to use Type 7 in modern IOS XE throws an error.
Command Line Password	To set the password for entering commands in the Cisco® command-line interface (CLI), choose one of the following options: Sync to Login Password—Sets the password to the same password you specified for the current user login name. Set New Password—Sets a new password that you specify. No Password—Does not require a password to enter CLI commands.
Device ID Settings	
Device Name	Enter a unique name to identify the physical switch.
NTP Server	Enter the IP address of the Network Time Protocol (NTP) server.

(1) You can downgrade to firmware revision 17.10 If you select Type-6 and Type-7 passwords, but downgrading to firmware revision 17.9 and below is not supported.

4. Configure basic settings as described in Table 12, and then click Day 0 Config Summary.



To view all basic settings, scroll down the page.



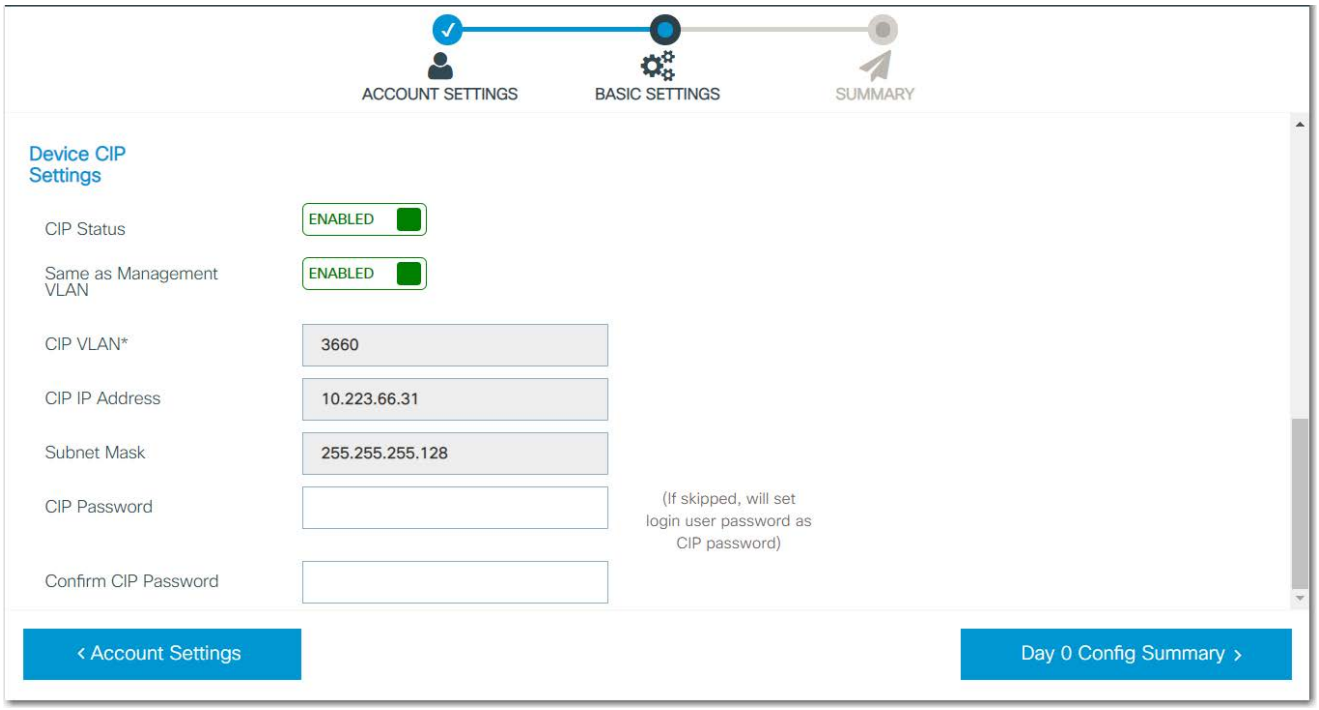


Table 12 - Basic Settings

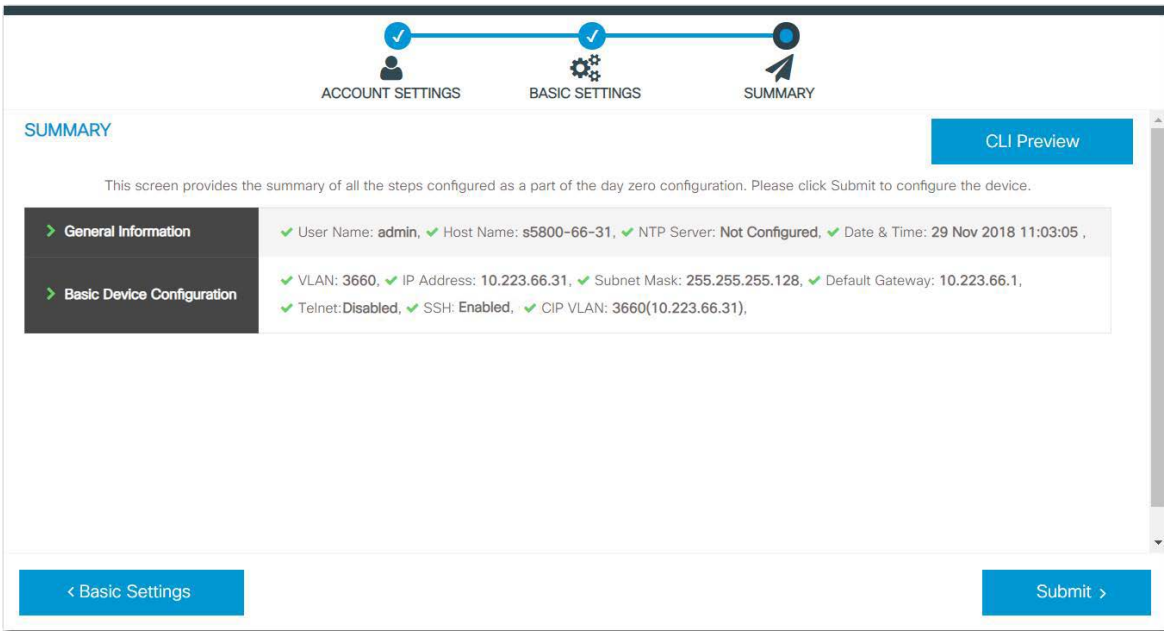
Field	Description
Device Management Settings	
IP Address	Click to determine how the IP information is assigned to the switch: Static—You manually assign IP information. We recommend that you manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the WebUI for the switch. DHCP—A DHCP server automatically assigns an IP address, subnet mask, default gateway, primary and secondary DNS server 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 the WebUI. The default mode is Static. **IMPORTANT:** For a manually assigned IP address in a network that uses a DHCP server, the IP address cannot be within the range of addresses that the DHCP server assigns. Otherwise, IP address conflicts can occur between the switch and another device.
VLAN ID	Enter an ID for 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 the following: Broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. Secure administrative access to all devices in the network. 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 can lose management connectivity to the switch.
IP Address	(Applies only to static IP addresses). Enter the IP address and associated subnet mask to assign to the switch: **IMPORTANT:** If you run Express Setup in Medium Press mode, the IP Address field displays the IP address from the DHCP server. If you change the address, the connection drops. To re-establish the connection with the new address, close your web browser and go to the address you specified. Make sure that the IP address that you assign to the switch is not assigned to another device in your network. The IP address and the default gateway cannot be the same.
Subnet Mask	Enter the subnet mask to assign to the switch. The default is 255.255.255.0.
Default Gateway (optional)	(Applies only to static IP addresses). Enter the IP address for the default gateway 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. 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.
Associate VLAN with interfaces	To assign switch interfaces to the management VLAN, click an interface in the Available column to move it into the Selected column.
Telnet	To use Telnet to access the switch via the command-line interface (CLI), click to Enable Telnet. 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 through strong encryption.

Table 12 - Basic Settings (Continued)

Field	Description
SSH	To allow Secure Shell (SSH) sessions on the switch, click to enable SSH. SSH uses the local account user name and password. SSH provides a secure, remote connection to the switch. SSH provides more security for remote connections than Telnet through strong encryption. Enabled by default
Domain Name for SSH	(Appears only if SSH is enabled). Enter the SSH domain name, such as server.company.com.
Device CIP Settings	
CIP Status	To provide application-level connections from the switch to other industrial automation and control systems for management and monitoring, click to enable CIP status.
Same as Management VLAN	To use the switch management VLAN as the CIP VLAN, click to enable this setting.
CIP VLAN	Enter 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.
CIP IP Address	If the CIP VLAN differs from the switch management VLAN, enter the IP address for the CIP VLAN. Make sure that the IP address is not used by another device in your network.
Subnet Mask	If the CIP VLAN differs from the switch management VLAN, enter the subnet mask for the CIP VLAN.
CIP Password	Enter the CIP password, or leave this field blank if you do not want to change the password.
Confirm CIP Password	If you entered a CIP password, reenter the password.

5. On the Summary page, review your configuration settings.
6. To view the CLI commands to execute once you submit the configuration, click CLI Preview.
7. Once you approve of the configuration, click Submit.

   The switch initializes its configuration for typical industrial EtherNet/IP™ applications by running the global macro as described on page 41. You can then log on to the WebUI for further configuration or exit the application.



8. Disconnect the cables to the switch.
9. To complete the Short Press Express setup, power cycle the switch.
10. If you ran 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 statically assigned IP address, verify the computer IP address is on the same subnet of the configured IP address of the switch.

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

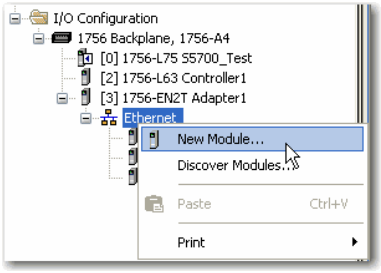
Complete Express Setup via the Logix Designer Application

To complete the initial setup of the switch via the Logix Designer application, follow these procedures. For details about how to use the Logix Designer application, refer to online Help.

Before you perform following procedures, you must run Express Setup on the switch in Medium Press mode, and the switch must receive its IP address from a DHCP server.

Add the Switch to the Controller Project

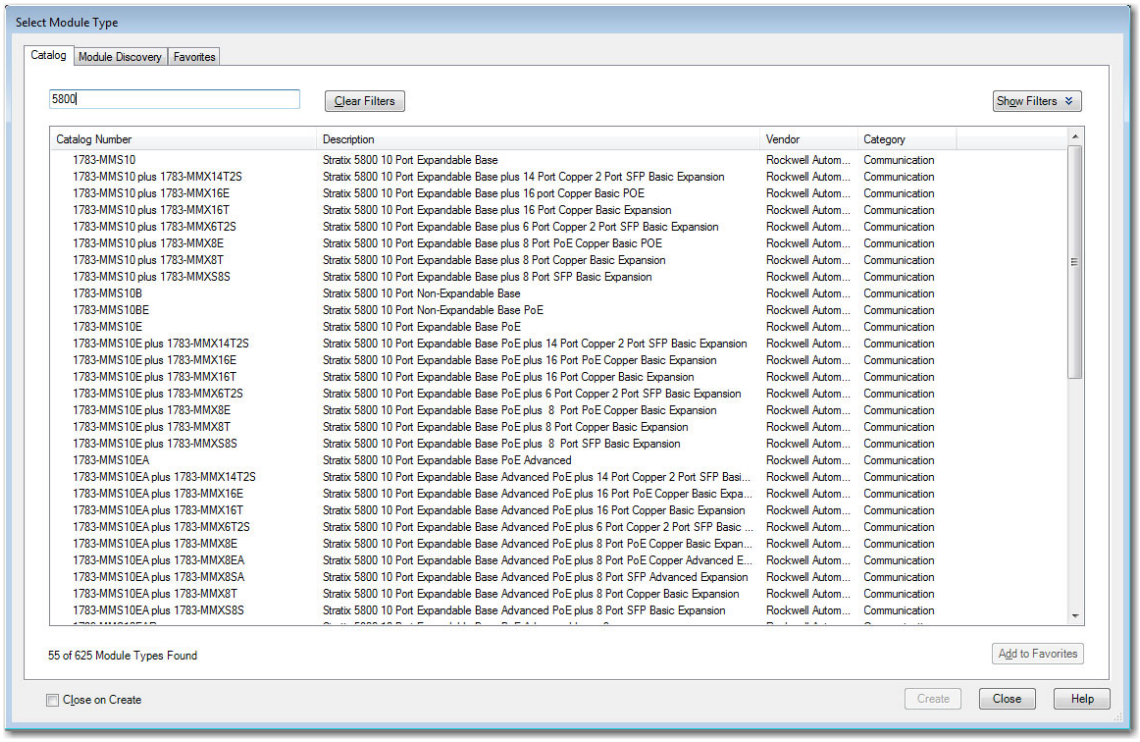
1. Open the project file for the controller to monitor the switch.
2. Right-click Ethernet and choose New Module.



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

   If you do not see the switch in the list of catalog numbers, obtain the AOP from the Rockwell Automation support site:

   https://www.rockwellautomation.com/en_NA/support/overview.page?



4. Complete the fields as described in Table 13.

   Be sure to specify the IP address that the DHCP server assigned.

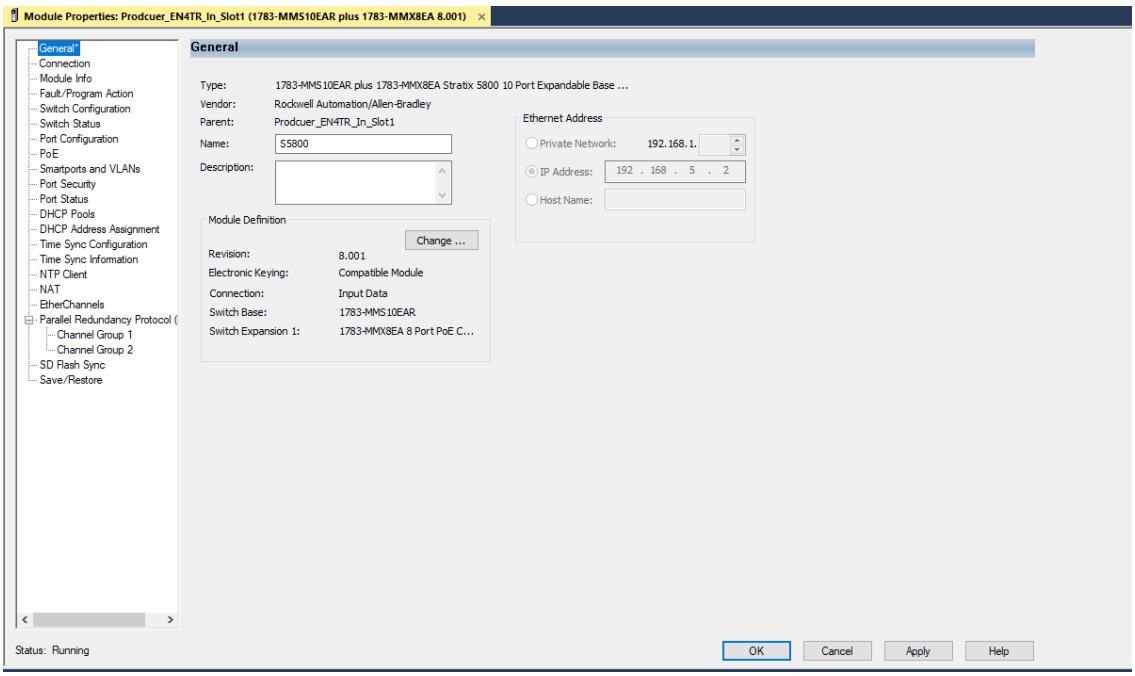


Table 13 - General View

Field	Description
Name	Enter a name to identify the switch.
Description	Enter a description of the switch.
Ethernet Address	Click IP Address, and then enter the IP address that the DHCP server assigned to the switch during Express Setup.

5. In the Module Definition area, click Change.
6. Complete the fields as described in Table 14, and then click OK.

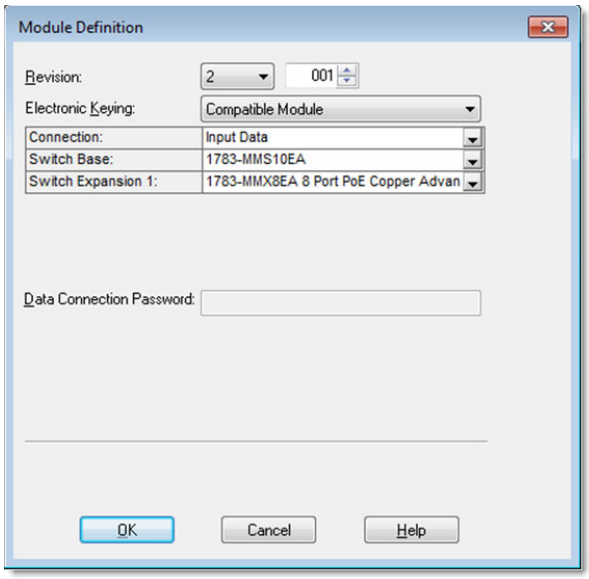
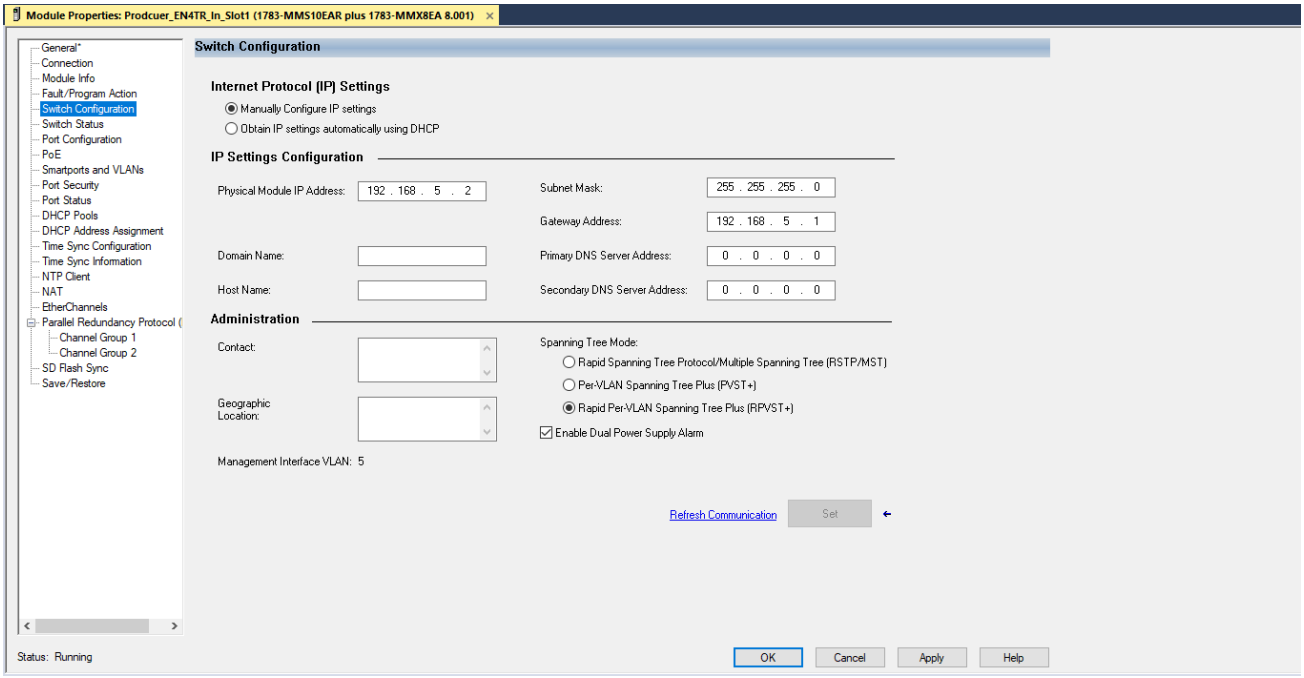


Table 14 - Module Definition

Field	Description
Revision	Choose the major and minor revision of the switch: Major revision: 1...128 Minor revision: 1...255
Electronic Keying	Choose one of the following: Compatible Module (default) Exact Match Disable Keying
Connection	Choose one of the following: Input Data (default): Enables only an input data connection. Data: Enables an input and output data connection. **ATTENTION:** This selection enables output tags, which can disable ports and interrupt connections to and through the switch. You can disable a switch port by setting the corresponding bit in the output tag. The output bits are applied every time that the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied. When the corresponding output bit is 0, the port is enabled. If you enable or disable a port via the WebUI or the CLI, the output bits from the controller can override the port setting on the next cyclic update of the I/O connection. The output bits always take precedence, regardless of whether the WebUI or the CLI was used to enable or disable the port.
Switch Base	Choose a base module from the pull-down menu.
Switch Expansion 1	Choose an expansion module from the pull-down menu.
Data Connection Password	(Data connections only). Enter the password for the switch.

7. On the General view, click Apply.
8. Go online with the controller, and then open the Module Properties page for the switch.

9. In the navigation pane, click Switch Configuration.



10. On the Express Setup page, complete the fields.

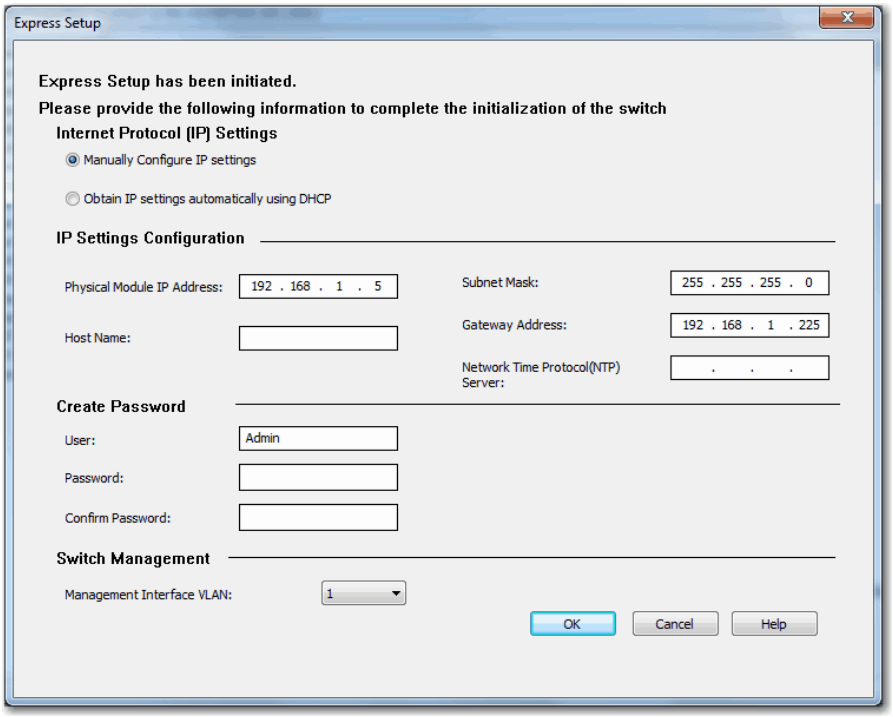


Table 15 - Express Setup Fields

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 the switch uses a static IP address and your network uses a DHCP server, make sure that the IP address is not within the range of addresses that the DHCP server assigns. Otherwise, IP address conflicts can occur between the switch and another device. Obtain IP settings automatically using DHCP—A Dynamic Host Configuration Protocol (DHCP) server automatically assigns the switch an IP address, subnet mask, and default gateway. Unless restarted, the switch continues to use the DHCP-assigned information.
Physical Module IP Address	Displays the IP address that the DHCP server assigned to the switch 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 OK. 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 subnet mask that the DHCP server assigned to the switch during Express Setup.
Host Name	Enter a name to identify the switch. The name can be up to 64 characters and can include alphanumeric and special characters (comma and dash).
Gateway Address	Displays the gateway address that the DHCP server assigned to the switch 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. If your network management station and the switch are in different networks or subnetworks, you must specify a default gateway. Otherwise, the switch and your network management station cannot communicate with each other. **IMPORTANT:** Communication is disrupted when you change the gateway (IP) address.
Network Time Protocol (NTP) Server	(Optional). Type the IP address of the NTP server. NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
User	Displays the default user name: **Admin**
Password, Confirm Password	Enter a password for the switch. The default password is **switch**. To complete initial setup, you must change the password from the default password. This password is also used as the Control Industrial Protocol (CIP) security password. You must provide a password to the switch to secure access to the WebUI.
Management Interface (VLAN)	Choose a management VLAN. The default management VLAN ID is 1. The management VLAN through which the switch is managed. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. It also provides secure administrative access to all devices in the network. **IMPORTANT:** Be sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch.

Default Global Macro

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

- Enable IGMP snooping and querier
- Enable CIP, if configured during Express Setup
- Enables alarms, SYSLOG, and SNMP notifications
- Enables Rapid Per VLAN Spanning Tree (RPVST) protocol, BPDU Guard, BPDU Filter, and loop guard
- Configure Quality of Service (QoS) settings and classify CIP, PTP, and other traffic

If you do not run Express Setup to initialize the switch, the global macro does not run. You can use the CLI to run the global macro. See CIP Sync (PTP) on page 224.

Notes:

WebUI Basics

Topic	Page
Requirements and Restrictions	43
Access the WebUI	44
Use the WebUI Toolbar	48
Set WebUI Preferences	49
Customize the Dashboard	50
Sort, Filter, and Customize Data in Columns	51

The web user interface (WebUI) provides a secure connection to the switch from anywhere in your network through a supported web browser.

Requirements and Restrictions

To make sure that the WebUI runs properly, disable any popup blockers or proxy settings in your browser. If directly connected to a network, consider disconnecting from any wireless networks on your workstation.

IMPORTANT The WebUI automatically logs you out if you are inactive for 20 minutes or longer.

To configure the inactivity timeout value for web sessions, from the Administration menu, choose HTTP/HTTPS/Netconf, and then enter a timeout value in the Session Idle Timeout field.

Be sure that the workstation you use to access the WebUI meets the requirements in Table 16.

Table 16 - WebUI Requirements

Component	Minimum Version
Operating System	
Microsoft® Windows	7 or higher
Apple Mac OS	10.9.5 or later
Browser	
Google Chrome	59 or later
Microsoft Edge	40 or later
Mozilla Firefox	60 or later
Screen Resolution	
1280 x 800 or higher	

Access the WebUI

Because the WebUI provides a secure connection, security messages from your browser can appear when you access the WebUI.

To access the WebUI, follow these steps.

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

   For information about setting the initial switch IP address, see Chapter 2, Express Setup.

2. If security messages from your browser appear, complete the procedures in the following table.

Browser	Procedure
Google Chrome	Click Advanced. Click Proceed to [IP address]. See Figure 13 on page 45.
Microsoft Edge	Click Details. Click Go on the webpage. See Figure 14 on page 46.
Mozilla Firefox	Click Advanced. Click Accept the Risk and Continue. See Figure 15 on page 47.

3. On the Login page, enter the switch Username and Password, and then click Log In.



Figure 13 - Security Messages—Chrome

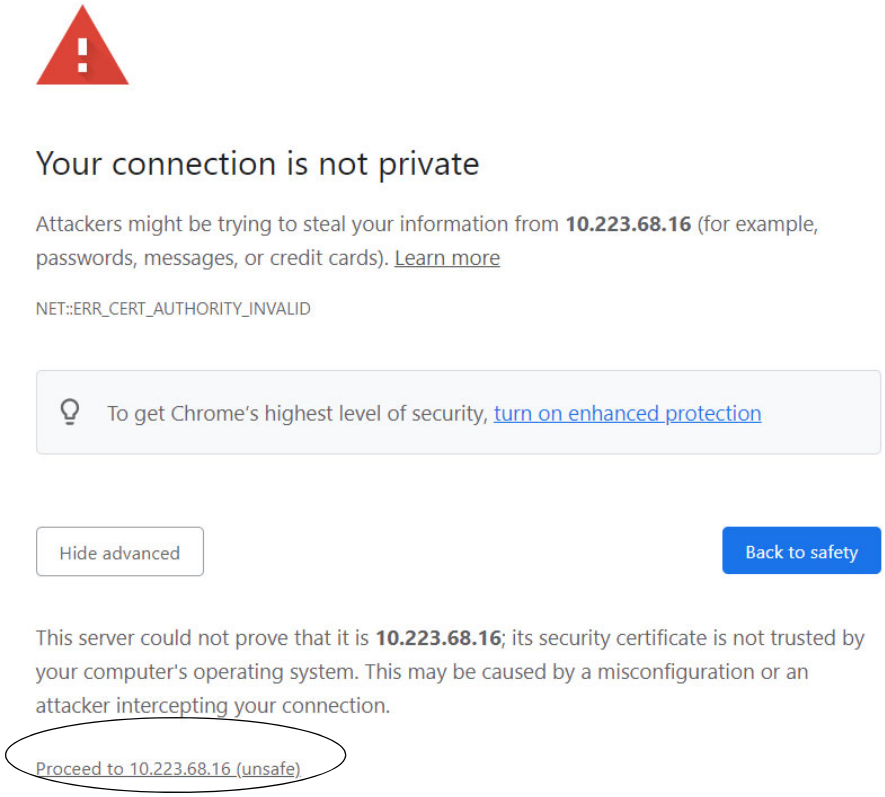


Figure 14 - Security Messages—Edge

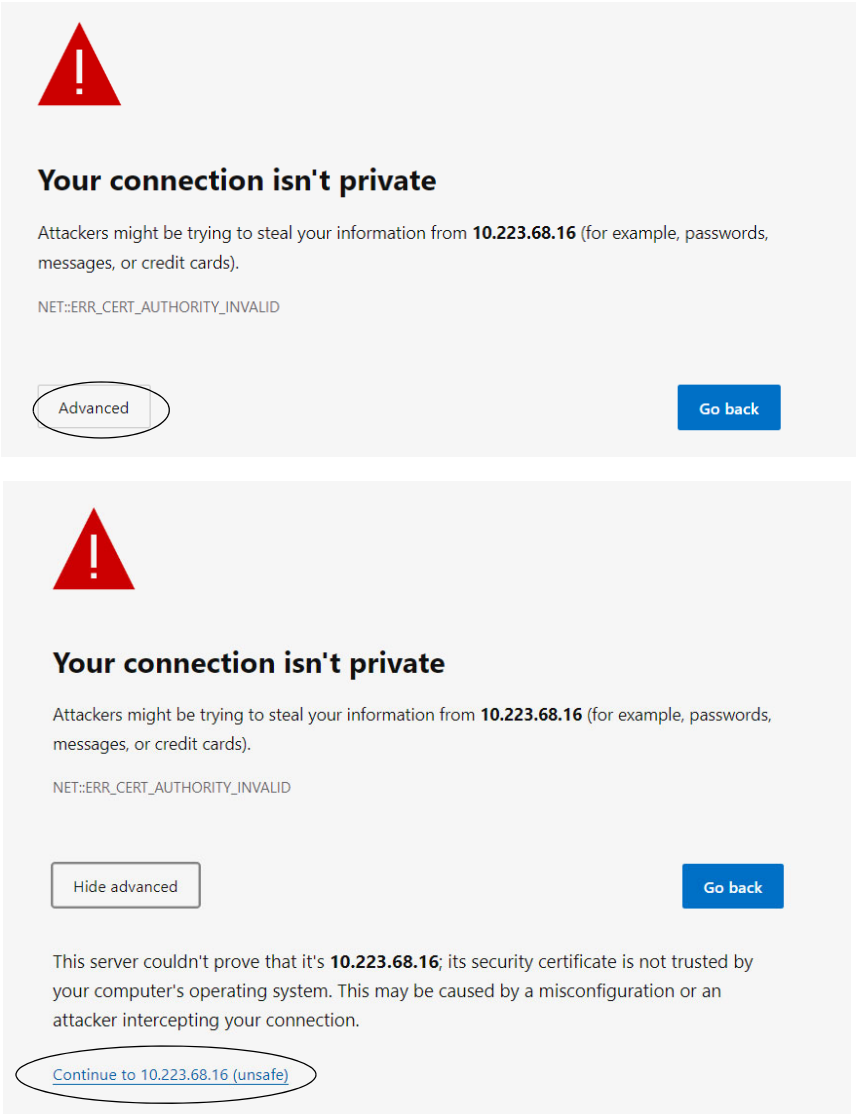
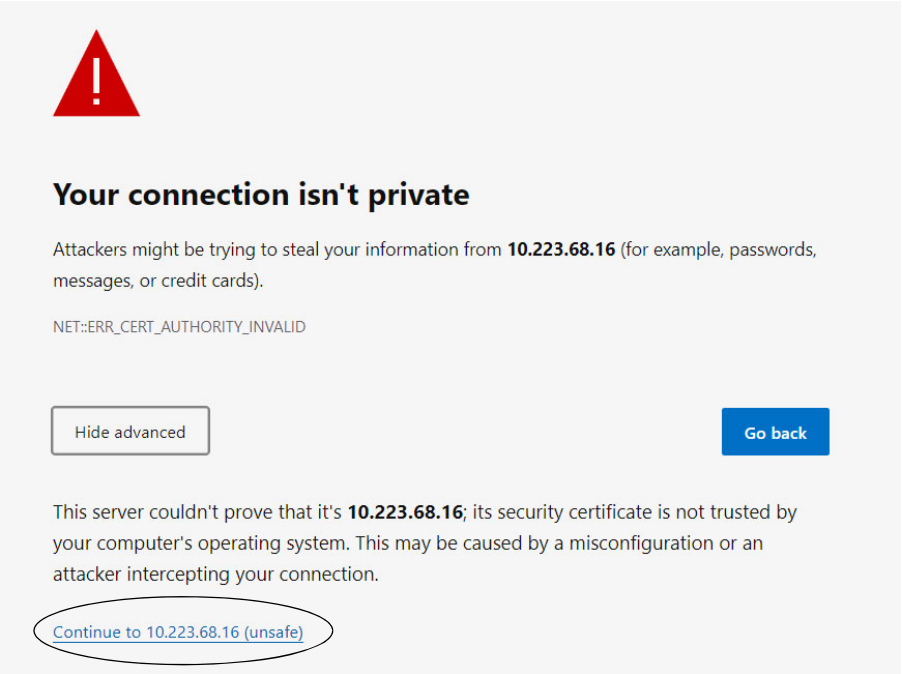


Figure 15 - Security Messages—Firefox



Use the WebUI Toolbar

The WebUI toolbar appears in the upper-right corner of the WebUI. The toolbar functions described in Table 17 enable you to make global changes to the WebUI.

Figure 16 - WebUI Toolbar

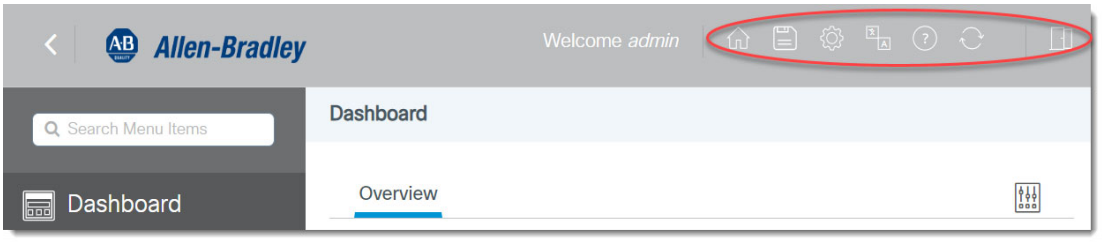


Table 17 - Global Toolbar

Icon	Description
Home	Takes you to the home page.
Save Configuration	Saves the Running configuration of the switch to the Startup configuration of the switch: Changes saved to the Running configuration are lost after you restart the switch unless you save them to the Startup configuration. Changes made to the switch via the WebUI pages are saved only to the Running configuration. Changes saved to the Startup configuration are stored in the internal memory of the switch and are retained after you restart the switch. **IMPORTANT:** You must click the Save Configuration button on the toolbar to save the Running configuration to the Startup configuration and retain the changes after a power cycle.
Preferences	Allows you to change the default home page, grid size, login tracking, and login tracking interval. See Set WebUI Preferences on page 49.
Language	Displays the language options available for the WebUI. The current options are English and Japanese.
Help	Launches the Help for the WebUI.
Refresh	Refreshes the current WebUI page.
Full Screen	Changes the current WebUI screen to full screen mode.
Log Out	Exits the WebUI.

Set WebUI Preferences

Each user with a WebUI account can set these preferences:

- Default page that appears when the user logs on to the WebUI.
- Default number of grid rows to display per page.
- Login activity for the user account.

In the upper-right corner of the WebUI, click the Preferences icon .

Figure 17 - WebUI Preferences

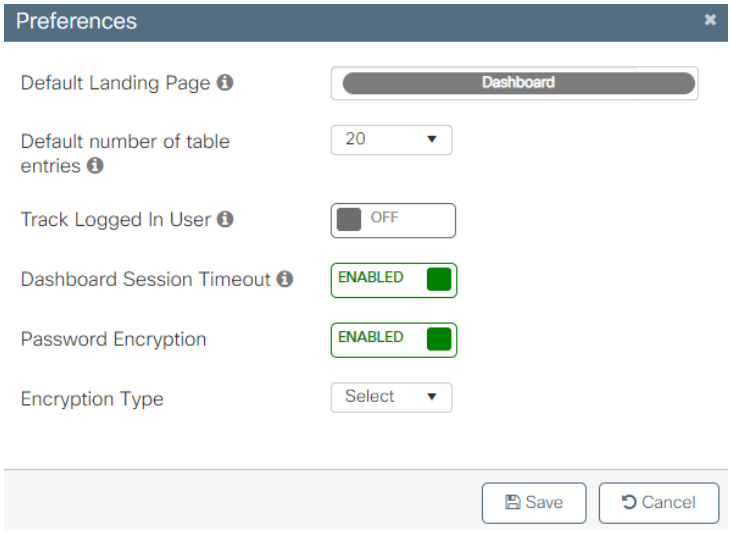


Table 18 - WebUI Preferences

Field	Description
Default Landing Page	Choose the setting from the list that is automatically generated. By default, the switch directs you to the dashboard.
Default number of table entries	Default value: 20
Track Logged In User	Click to enable the switch to track the following information for the user account: The time of the last failed login attempt by the user The number of failed login attempts by the user The number of times the user successfully logged into the WebUI If you enable tracking, the switch automatically configures AAA. For more information about AAA, see page 54. If you enable this preference, a message appears prompting you to confirm your choice. To enable tracking and AAA, click Yes.
Dashboard Session Timeout	Enabled by default Causes session timeout on inactivity when user is on the dashboard.
Password Encryption	Enabled by default Encrypts all passwords configured on the device.
Encryption Type	• Type 6 - More Secure - This is true encryption using 128 bit AES counter mode. The User defines a Primary key which is used by IOS XE to encrypt the password. • **IMPORTANT**: The encrypted password that is visible in the running-config cannot be copied between devices unless the original Primary Key is configured on the new device. • Type 7 - Less Secure (Not recommended) - These use the Vigenerecipher, a simple algorithm. An attempt to use Type 7 in modern IOS XE throws an error.
Primary Key	Primary Key is available with Encryption Type 6. The Primary Key contains at least 8 characters.

Customize the Dashboard

The Dashboard page has dashlets that display a snapshot of the overall status and statistics of the switch. Table 19 describes the dashlets.

Table 19 - Dashlets

Dashlet	Description
Switch View	This image shows the ports, status indicators, and other features on the front panel of the switch.
CPU & Memory Pressure Graph	Displays CPU usage on the processors on each core, every 5 minutes, every 1 minute, and every 5 seconds. The Memory Utilization section displays a chart of the device memory usage. To view the used space and free space percentage, hover over the chart.
Temperature	Displays the temperature of the device. If the temperature is yellow or red, your device needs attention.
System Information	Displays a snapshot of the specific details of the device.
Power over Ethernet Power Consumption (POE) (Stratix® 5800 Switch Only)	Displays Power over Ethernet (PoE) information for the switch, including the total power supported and the device power usage. To view the unused power and used power percentage, hover over the pie chart.

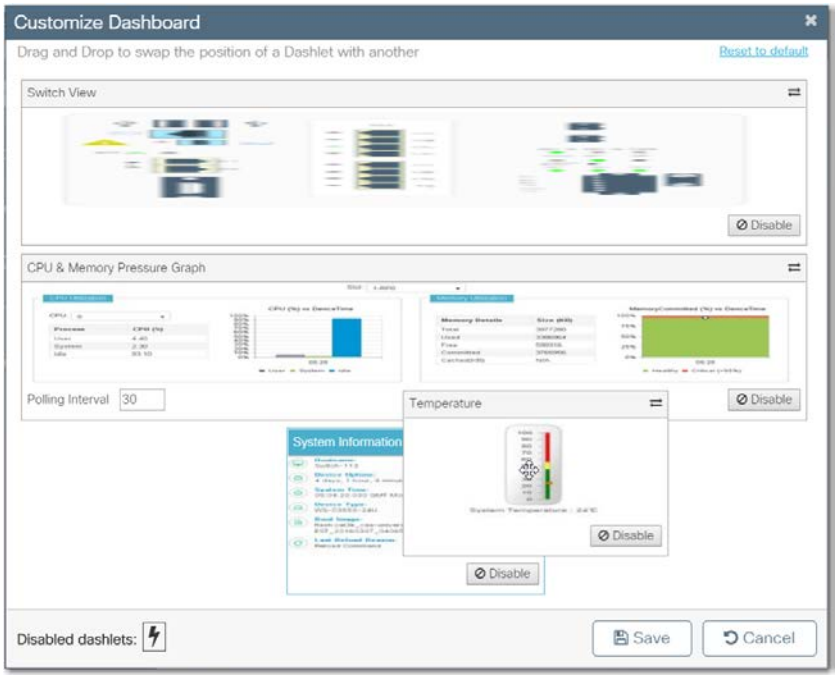
The time stamp that is associated with each dashlet indicates how recent the status information and statistics are.

Figure 18 - Dashlet Time Stamp



To customize the dashboard, click the Customize Dashboard icon  in the top-right corner of the page. On the Customize Dashboard page, you can set the order of appearance for each dashlet or disable specific dashlets to hide their appearance on the dashboard. Any disabled dashlets are available as icons on the dashboard and can be enabled at any time to be a part of the dashboard.

Figure 19 - Customize Dashboard



Sort, Filter, and Customize Data in Columns

The WebUI provides options to help view data in columns. For example, the Ethernet Ports page features a table of interfaces on the switch. To display options to view data, click the drop-down arrow in a column header, as shown in Figure 20.

Figure 20 - Column Header Options

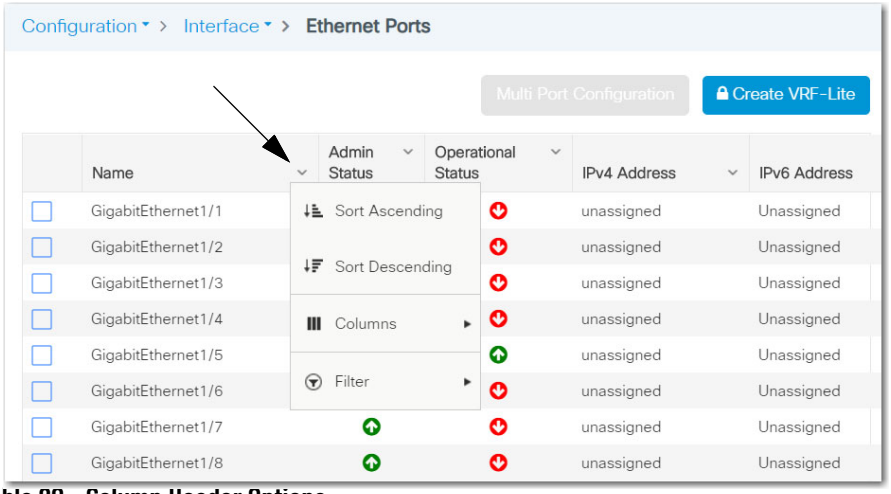
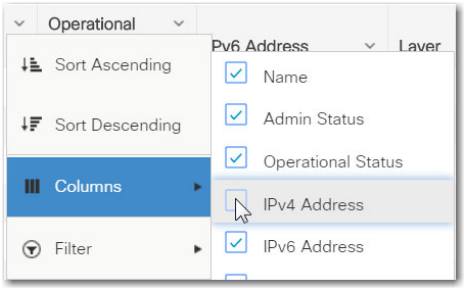
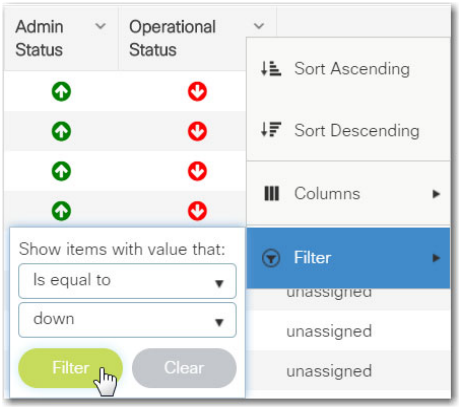


Table 20 - Column Header Options

Option	Description
Sort Ascending	Click to view column data in ascending order.
Sort Descending	Click to view column data in descending order.
Columns	Click to display a list of columns to show or hide on the page. For example, to hide the IPv4 Address column on the Ethernet Ports page, clear the IPv4 Address checkbox. 
Filter	Click to display filter options for data in the column. For example, to view only ports with a down state in the Operational Status column, choose Is equal to, and then choose down. 

Notes:

Configure the Switch

Topic	Page
Authentication, Authorization, and Accounting (AAA)	54
Access Control Lists (ACLs)	75
Discovery Protocols	78
Device Level Ring (DLR) Topology	80
Enhanced Interior Gateway Routing Protocol (EIGRP) (Stratix 5800 Switch Only)	86
Ethernet Ports	89
Ethernet Ring G.8032 (Stratix 5200 Switch Only)	100
Flow-based SPAN (FSPAN)	103
Logical Interfaces	105
High-availability Seamless Redundancy (HSR) (Stratix 5800 Switch Only)	111
Hot Standby Router Protocol (HSRP) (Stratix 5800 Switch Only)	117
Intermediate System-to-Intermediate System (IS-IS) (Stratix 5800 Switch Only)	118
IOx Services (Stratix 5800 Switch Only)	120
MACsec (Stratix 5800 Switch Only)	123
Media Redundancy Protocol (MRP)	127
Multicast Services	133
NetFlow (Stratix 5800 Switch Only)	134
Network Address Translation (NAT)	137
Open Shortest Path First (OSPF) Routing Protocol (Stratix 5800 Switch Only)	153
Parallel Redundancy Protocol (PRP)	155
Port Security	161
Quality of Service (QoS)	163
Remote Switch Port Analyzer (RSPAN)	167
Resiliency Ethernet Protocol (REP)	169
Routing Information Protocol (RIP)	174
Smartports	175
Spanning Tree Protocol (STP)	182
Static Routing	186
Switched Port Analyzer (SPAN)	187
TrustSec	190
Utility Features	199
Virtual Local Area Networks (VLANs)	200
Virtual Router Redundancy Protocol (VRRP) (Stratix 5800 Switch Only)	206
Virtual Routing and Forward (VRF) (Stratix 5800 Switch Only)	208
VLAN Trunk Protocol (VTP)	209

Authentication, Authorization, and Accounting (AAA)

AAA Network Security Services provide the primary framework for intelligently controlling access to resources, policy enforcement, and usage audits. For more information about AAA, see the Ethernet Reference Manual, publication ENET-RM002.

Terminal Access Controller Access-Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and Lightweight Directory Access Protocol (LDAP) are security protocols that control access to networks. You can configure the switch as a TACACS+, RADIUS, or LDAP client to authenticate and authorize users.

AAA Configuration

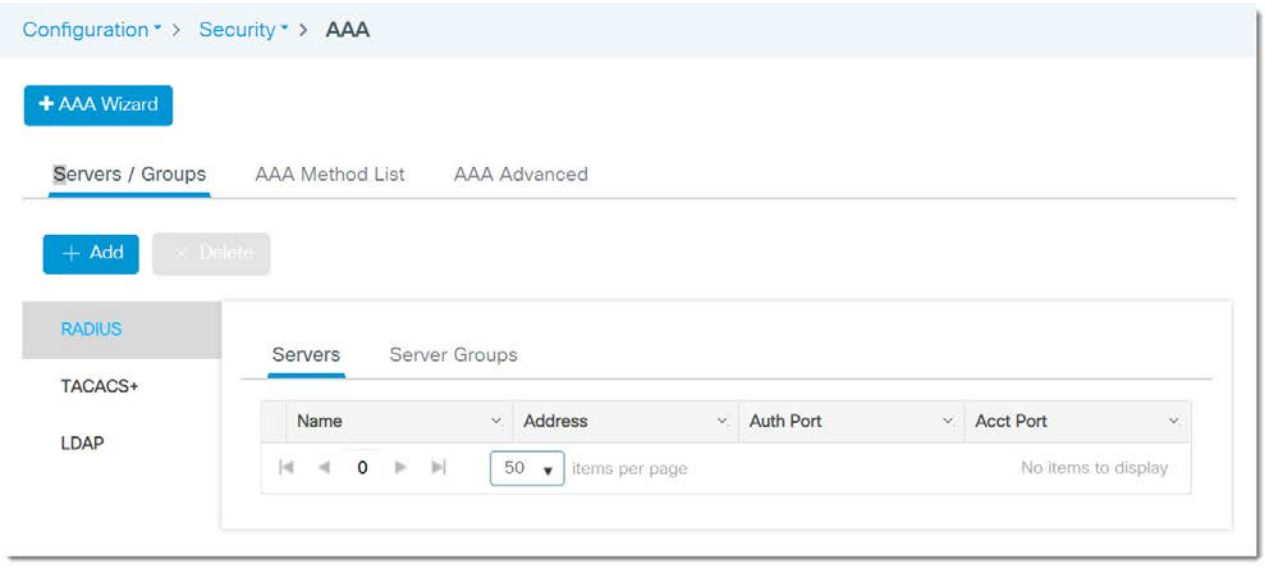
You can configure the AAA components in Table 21 by using the WebUI for the switch. The WebUI also provides a configuration wizard for these components. To use the wizard, see page 55.

Table 21 - AAA Configuration Components

Component	Page
Authentication Configuration	60
Authorization Configuration	62
Accounting Configuration	63
RADIUS Server Configuration	64
RADIUS Server Group Configuration	65
TACACS+ Server Configuration	67
TACACS+ Server Group Configuration	68
LDAP Server Configuration	69
LDAP Server Group Configuration	70
RADIUS Fallback Configuration	73
Policy Password Configuration	73

Configure AAA via the WebUI Wizard

From the Configuration menu, click AAA.



To use the AAA wizard, follow these steps.

1. Click AAA Wizard.
2. In the upper-right corner, click Basic or Advanced:
   - Basic—The wizard displays only basic configuration fields.
   - Advanced—The wizard displays both basic and advanced configuration fields.
3. Configure security servers as described in Table 22, and then click Next.

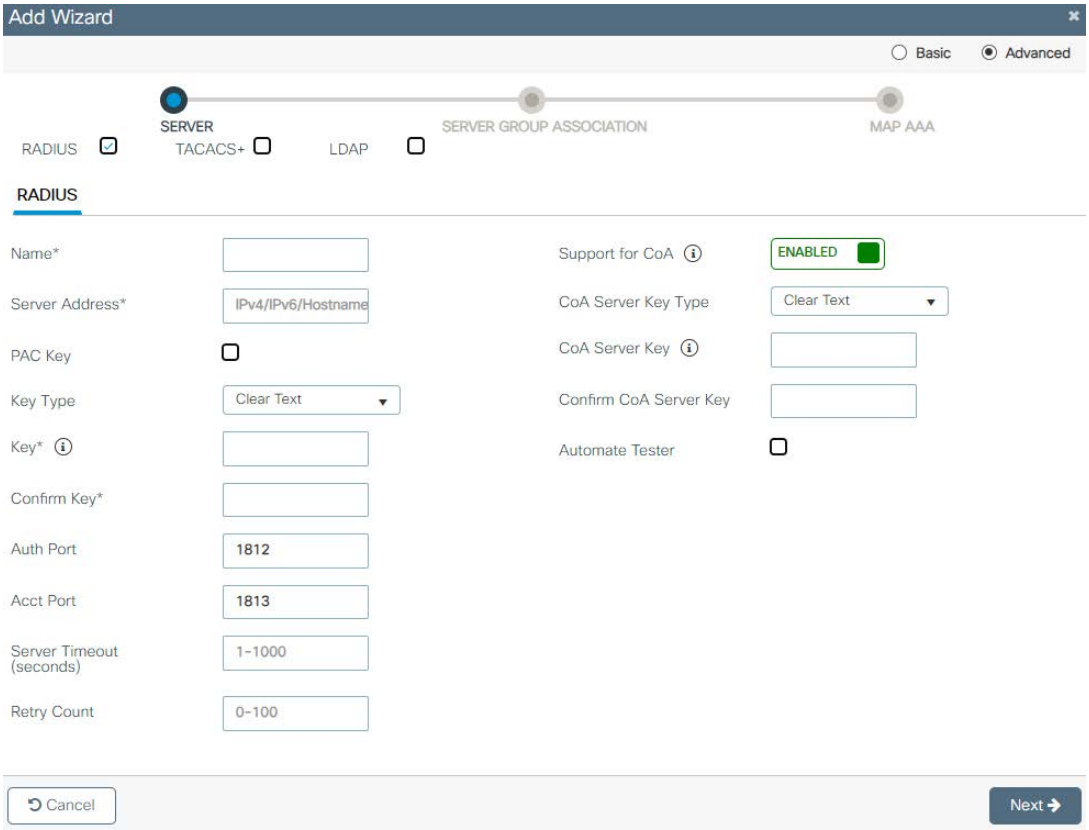


Table 22 - Server Configuration

Field	Description
RADIUS	To display the RADIUS tab in the configuration wizard, check RADIUS.
TACACS+	To display the TACACS+ tab in the configuration wizard, check TACACS+.
LDAP	To display the LDAP tab in the configuration wizard, check LDAP.
RADIUS Tab	
Name	Enter a name to identify the RADIUS server.
Server Address	Enter the IP address for the RADIUS server.
PAC Key	Check PAC Key to enter a Protected Access Credential (PAC).
PAC Key Type	(Appears only if you check PAC Key). Choose a PAC key type.
PAC Key	(Appears only if you check PAC Key). Enter the PAC to use to authentication between the server and your device.
Confirm PAC Key	(Appears only if you check PAC Key). Reenter the PAC key to confirm it.
Key Type	Choose a key type: 0—Requires you to enter an unencrypted key. LINE—Requires you to enter an unencrypted (cleartext) shared key. Default value: 0
Key	(Appears only if you clear the PAC Key checkbox). Enter the shared secret key to use for authentication between the server and your device.
Confirm Key	(Appears only if you clear the PAC Key checkbox). Reenter the key to confirm the value.
Auth Port	(Advanced configuration). Enter the UDP port number of the RADIUS server for authentication. Valid values: 1...65535 Default value: 1812
Acct Port	(Advanced configuration). Enter the UDP port number of the RADIUS server for accounting. Valid values: 1...65535 Default value: 1813
Server Timeout (seconds)	(Advanced configuration). Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Retry Count	(Advanced configuration). Enter the number of times the device can retry transmission. Valid values: 1...100 seconds
Support for CoA	To configure CoA, you must provide a valid IPv4/IPv6 address
CoA Server Key Type	• Clear Text • Encrypted • Hidden
Confirm CoA Server Key	(If global encryption is enabled, then all keys/passwords will be encrypted)
Automate Tester	(Appears only if you check Automate Tester)
Username	(Appears only if you check Automate Tester)
Ignore Auth Port	(Appears only if you check Automate Tester)
Ignore Acct Port	(Appears only if you check Automate Tester)
Enable Probe on	(Appears only if you check Automate Tester)
Idle Time (minutes)	(Appears only if you check Automate Tester)
TACACS+ Tab	
Name	Enter a name to identify the TACACS+ server.
Server Address	Enter the IP address of the TACACS+ server.
Key Type	Encrypted or Hidden
Key	Enter the shared secret key to be used for authentication between the server and your device.
Confirm Key	Reenter the key to confirm the value.
Port	(Advanced configuration). Enter the UDP port number of the TACACS server. Valid values: 1...65535 Default value: 9
Server Timeout (seconds)	(Advanced configuration). Enter the number of seconds between retransmissions. Valid values: 1...1000
LDAP Tab	
Server Name	Enter a name to identify the LDAP server.
IPv4/IPv6Server Address	Enter the IP address of the LDAP server.
Port Number	Enter the UDP port number of the LDAP server. Valid values: 1...65535 Default value: 389

Table 22 - Server Configuration (Continued)

Field	Description
Simple Bind	Choose the local authentication bind method for the LDAP server: Anonymous—Allows anonymous access to the LDAP server. Authenticated—Requires a user name and password to secure access. Default value: Anonymous
Bind User name	(Appears only if you choose Authenticated in the Simple Bind field). Enter a user name for local authentication to the LDAP server. The user name can contain a maximum of 80 characters. If the user name starts with "cn=", the controller does not append the user base distinguished name (DN). This designation allows the authenticated bind user to be outside the user base DN.
Bind Password	(Appears only if you choose Authenticated in the Simple Bind field). Enter a username to be used for local authentication to the LDAP server. The user name can contain a maximum of 80 characters.
Confirm Bind Password	(Appears only if you choose Authenticated in the Simple Bind field). Reenter the bind password to confirm the value.
User Base DN	Enter the distinguished name (DN) of the subtree in the LDAP server that contains a list of all users. **EXAMPLE:** ou=organizational unit, .ou=next organizational unit, and o=corporation.com. If the tree of users is the base DN, enter the following: . o=corporation.com, or dc=corporation, dc=com.
User Attribute	(Advanced configuration). Enter the name of the attribute in the user record that contains the user name. You can obtain this attribute from your directory server.
User Object Type	(Advanced configuration). Enter the value of the LDAP objectType attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user and some of which are shared with other object types.
Server Timeout (seconds)	(Advanced configuration). Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Secure Mode	(Advanced configuration). Check Secure Mode to configure a CA Trustpoint.
Trustpoint Name	(Advanced configuration). If you checked Secure mode, choose a Trustpoint name.

4. Configure server group associations as described in Table 23, and then click Next.

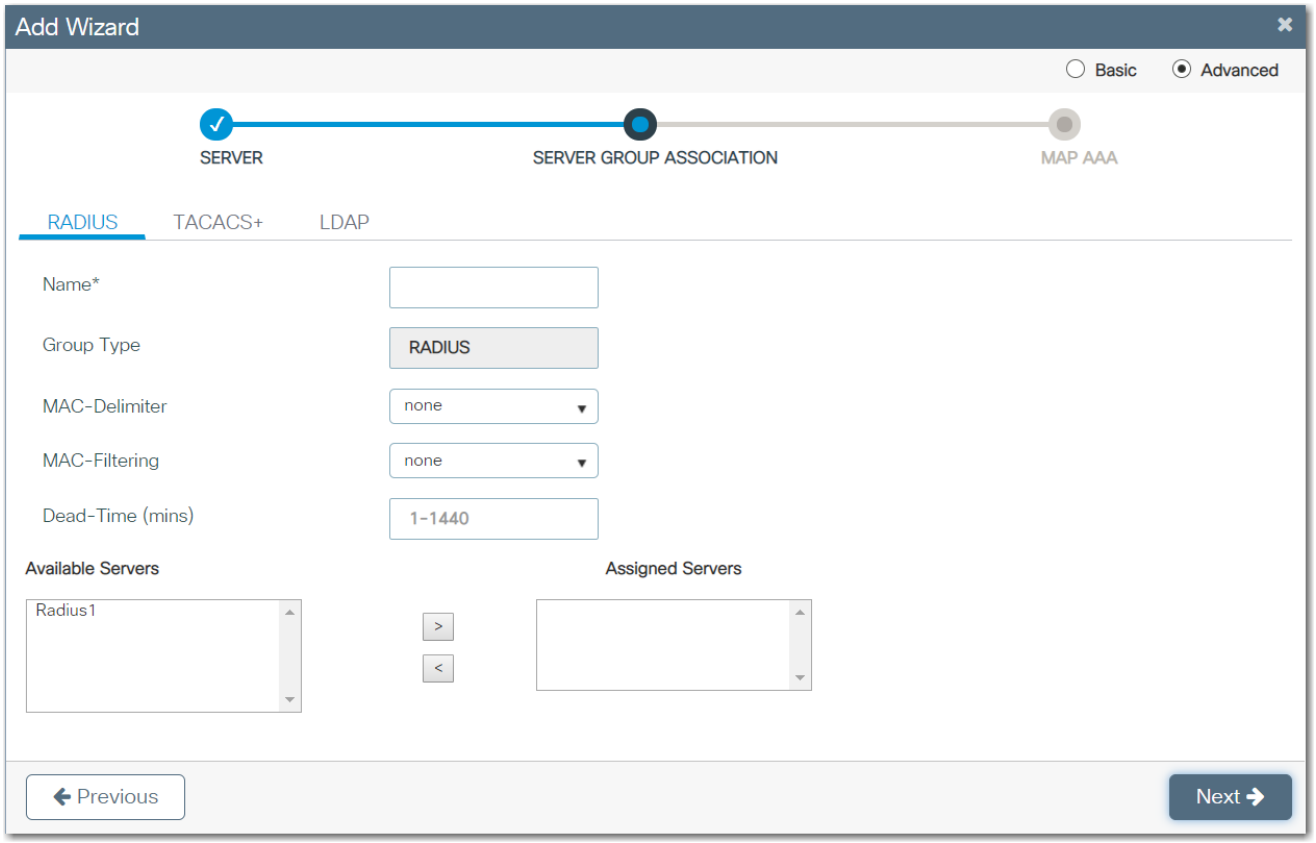


Table 23 - Server Group Association

Field	Description
RADIUS Tab	
Name	Enter a name to identify the RADIUS server group.
Group Type	(System-generated). Displays RADIUS.
MAC-Delimiter	Choose the delimiter to use in the MAC addresses that are sent to the RADIUS server: • none • colon • hyphen • single-hyphen
MAC-Filtering	Choose a value to use to filter MAC addresses: none MAC Key
Dead-Time (mins)	Enter the amount of time, in minutes, after which a server is assumed to be dead. After this time, AAA traffic for the server group is redirected to alternative groups of servers that have different operational characteristics. Valid values: 1...1440
Available Server Assigned Servers	In the Available Servers list, select the servers to include in the server group, and click to move them to the Assigned Servers list.
TACACS+ Tab	
Name	Enter a name to identify the TACACS+ server group.
Group Type	(System-generated). Displays TACACS.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the servers to include in the server group, and click to move them to the Assigned Server Groups list.
LDAP Tab	
Name	Enter a name to identify the LDAP server group.
Group Type	(System-generated). Displays LDAP.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the servers to include in the server group, and click to move them to the Assigned Servers Groups list.

5. Map the AAA as described in Table 24, and then click Save & Apply to Device.

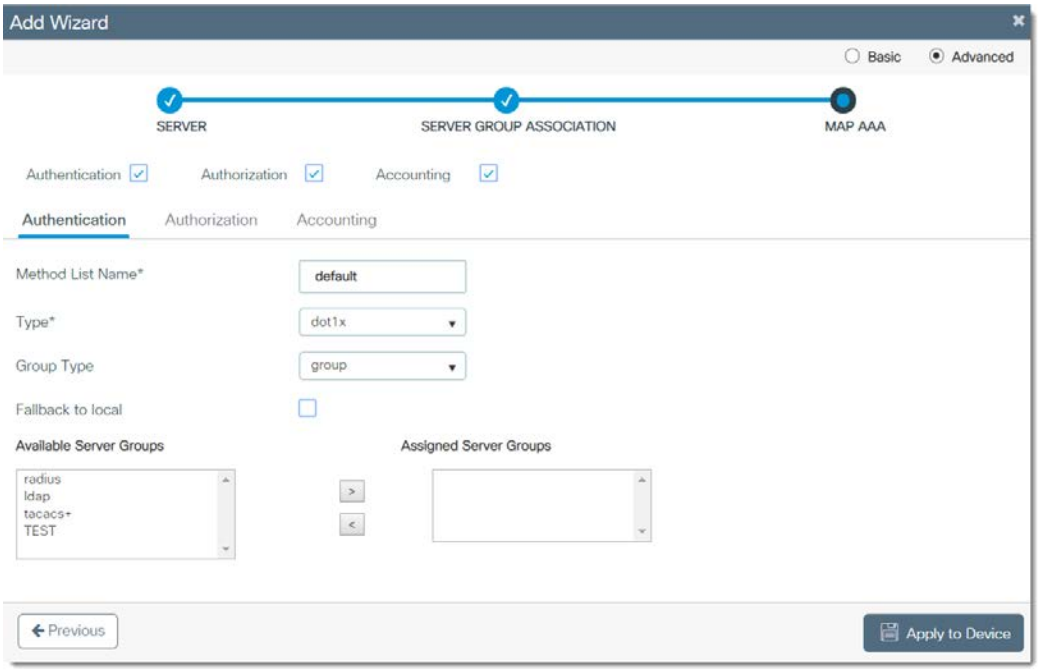


Table 24 - Map AAA

Field	Description
Authentication Tab	
Method List Name	Enter a name to identify the method list.
Type	Choose the type of authentication to perform before you allow access to the network: dot1x login
Group Type	Choose the type of server to authenticate access to the network: group local
Fallback to local	(Appears only if you choose group in the Group Type field). Check Fallback to local to configure a local server to act as a fallback method when servers in the group are unavailable.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to authenticate access to your network, and click to move them to the Assigned Server Groups list.
Authorization Tab	
Method List Name	Enter a name to identify the method list.
Type	Choose the type of authorization to perform before you allow access to the network: • network—Enables authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP. • exec—Enables authorization to determine if a user is allowed to run an EXEC shell. • credential-download—Enables authorization that is based on credentials.
Group Type	Choose the type of server to authorize access to the network: • group—Assigns a group of servers as your access server. • local—Uses a local server to authenticate access.
Fallback to local	(Appears only if you choose group in the Group Type field). Check Fallback to local to configure a local server to act as a fallback method when servers in the group are unavailable.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to authorize access to your network, and click to move them to the Assigned Server Groups list.
Accounting Tab	

Table 24 - Map AAA (Continued)

Field	Description
Method List Name	Enter a name to identify the method list.
Type	Choose the type of accounting to perform before you allow access to the network: • exec—Provides accounting records for user EXEC terminal sessions on the network access server, including user name, date, start and stop times. • identity • network—Enables authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP. • commands—Provides accounting information about specific, individual EXEC commands associated with a specific privilege level.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to track access to your network, and click to move them to the Assigned Server Groups list.

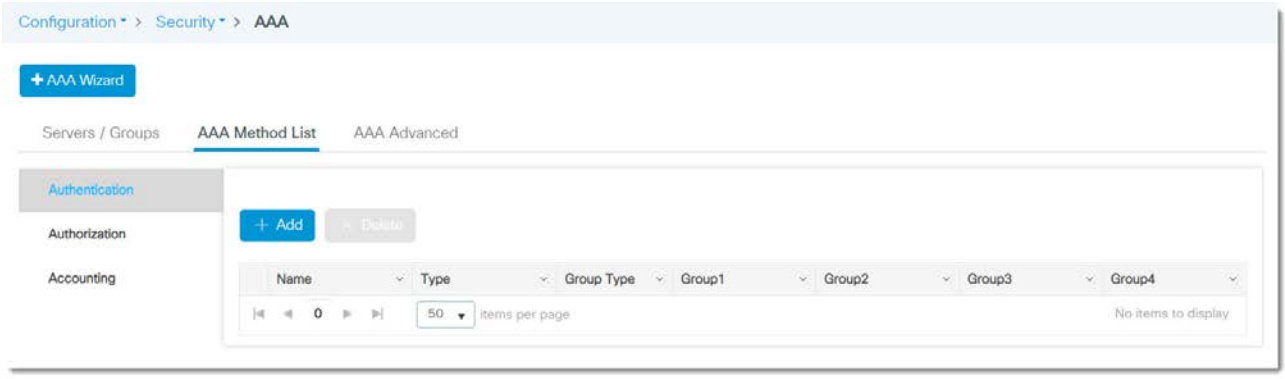
Configure AAA Method Lists via the WebUI

You can configure an AAA method list outside of the AAA wizard. To use the wizard, see page 55.

From the Configuration menu, click AAA.

Authentication Configuration

On the AAA Method List tab, click Authentication, and then click Add.



On the Quick Setup: AAA Authentication page, complete the fields as described in Table 25, and then click Apply to Device.

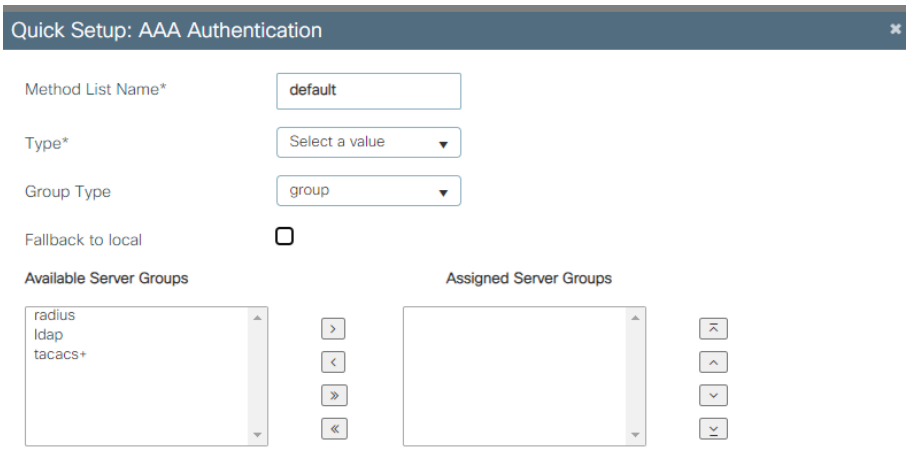
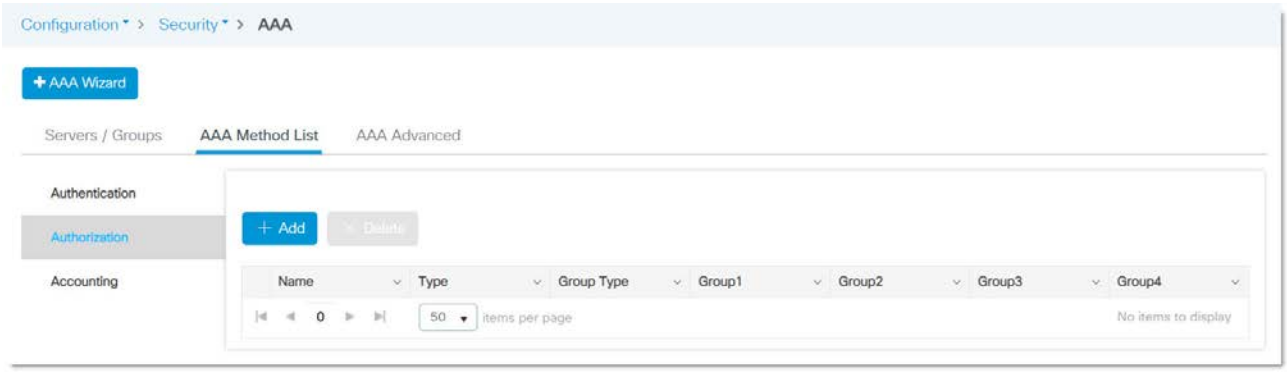


Table 25 - Quick Setup: AAA Authentication

Field	Description
Method List Name	Enter a name to identify the method list.
Type	Choose the type of authentication to perform before you allow access to the network: • dot1x • login
Group Type	Choose the type of server to authenticate access to the network: • group—Assigns a group of servers as your access server. • local—Uses a local server to authenticate access.
Fallback to local	Check Fallback to local to configure a local server to act as a fallback method when servers in the group are unavailable.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to authenticate access to your network, and click to move them to the Assigned Server Groups list.

Authorization Configuration

On the AAA Method List tab, click Authorization, and then click Add.



On the Quick Setup: AAA Authorization page, complete the fields as described in Table 26, and then click Apply to Device.

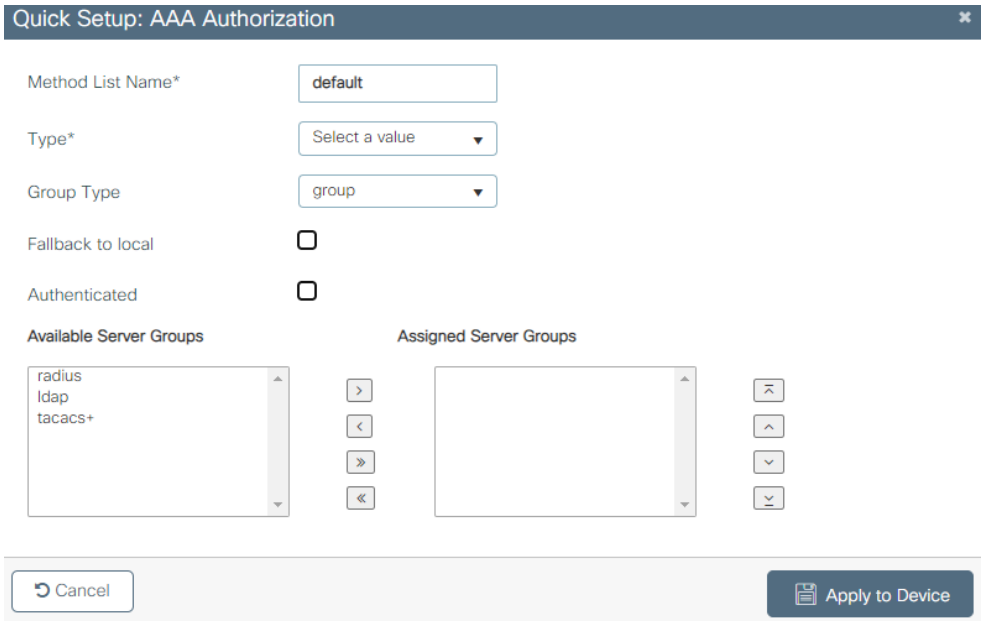
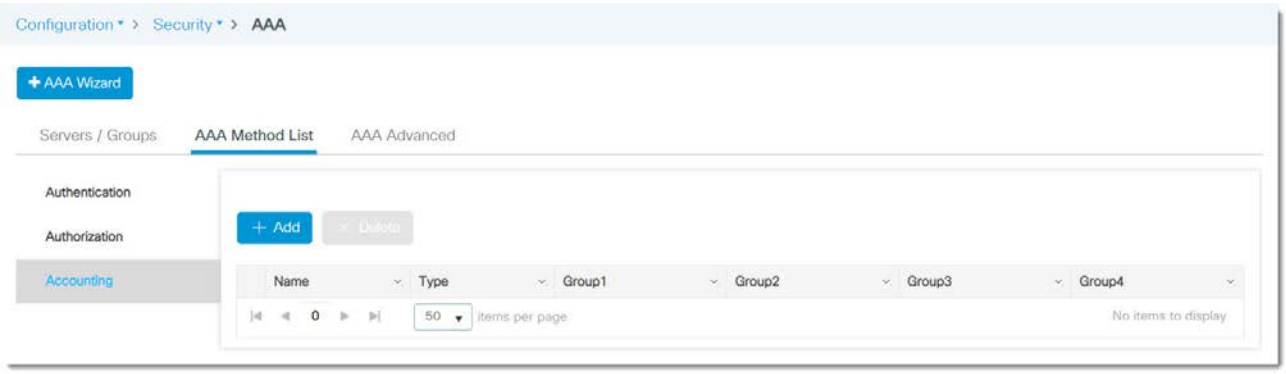


Table 26 - Quick Setup: AAA Authorization

Field	Description
Method List Name	Enter a name to identify the method list.
Type	Choose the type of authorization to perform before you allow access to the network: • network—Enables authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP. • exec—Enables authorization to determine if a user is allowed to run an EXEC shell. • credential-download—Enables authorization based on credentials.
Group Type	Choose the type of server to authorize access to the network: • group—Assigns a group of servers as your access server. • local—Uses a local server to authenticate access.
Fallback to local	Check Fallback to local to configure a local server to act as a fallback method when servers in the group are unavailable.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to authorize access to your network, and click to move them to the Assigned Server Groups list.

Accounting Configuration

On the AAA Method List tab, click Accounting, and then click Add.



On the Quick Setup: AAA Accounting page, complete the fields as described in Table 27, and then click Apply to Device.

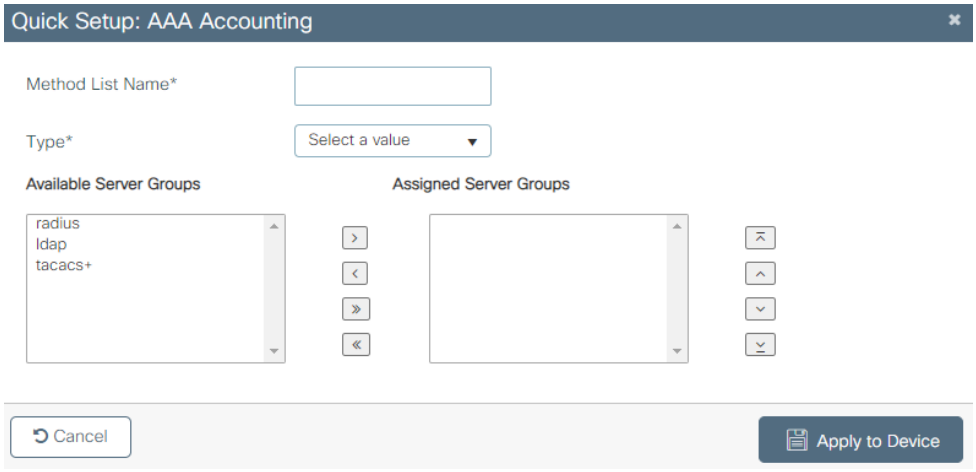


Table 27 - Quick Setup: AAA Accounting

Field	Description
Method List Name	Enter a name to identify the method list.
Type	Choose the type of accounting to perform before you allow access to the network: • exec—Provides accounting records for user EXEC terminal sessions on the network access server, including user name, date, start and stop times. • identity • network—Enables authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP. • commands—Provides accounting information about specific, individual EXEC commands associated with a specific privilege level.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to track access to your network, and click to move them to the Assigned Server Groups list.

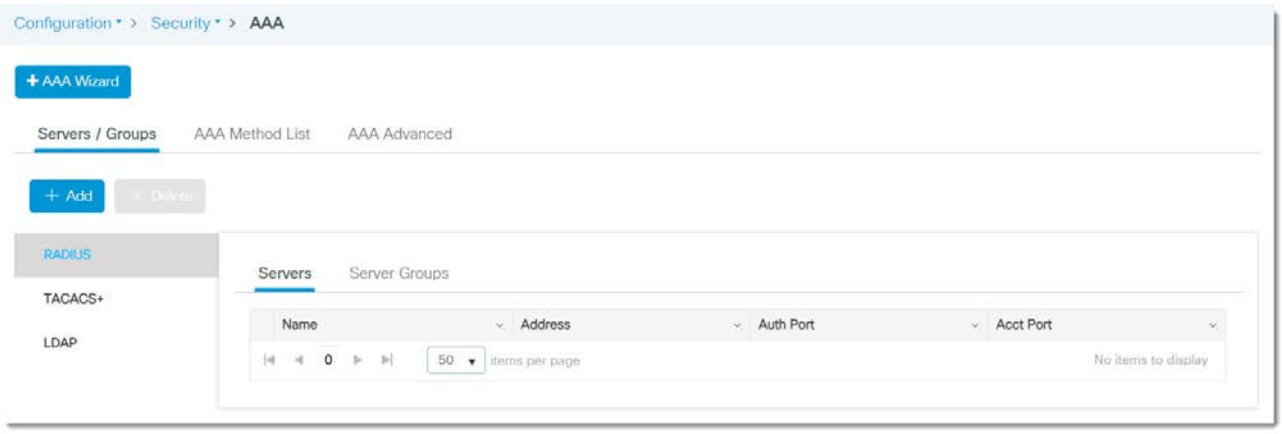
Configure AAA Servers and Server Groups via the WebUI

You can configure AAA servers and server groups outside of the AAA wizard. To use the wizard, see page 55.

From the Configuration menu, click AAA.

RADIUS Server Configuration

On the Servers/Groups tab, click RADIUS, Servers, and then click Add.



On the Quick Setup: AAA Radius Server page, complete the fields as described in Table 28, and then click Apply to Device.

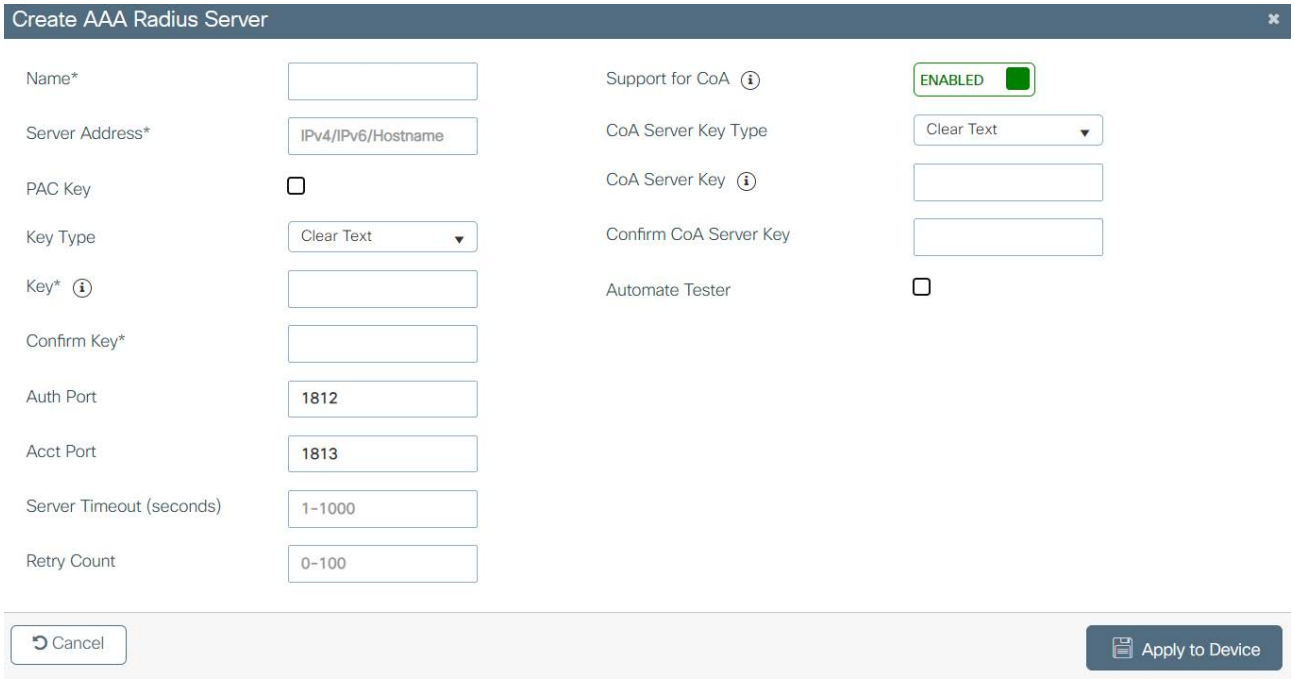
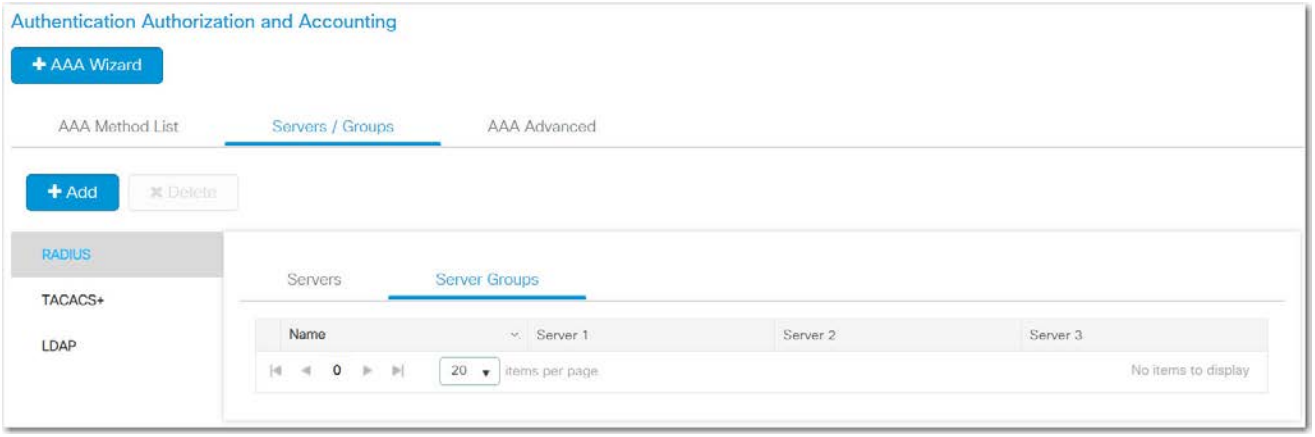


Table 28 - Create AAA RADIUS Server

Field	Description
Name	Enter a name to identify the RADIUS server.
IPv4 / IPv6 Server Address	Enter the IP address for the RADIUS server.
PAC Key	Check PAC Key to enter a Protected Access Credential (PAC).
PAC Key Type	(Appears only if you check PAC Key). Choose a PAC key type.
PAC Key	(Appears only if you check PAC Key). Enter the PAC to use to authentication between the server and your device.
Confirm PAC Key	(Appears only if you check PAC Key). Reenter the PAC key to confirm it.
Key	(Appears only if you clear PAC Key). Enter the shared secret key to use for authentication between the server and your device.
Confirm Key	(Appears only if you clear PAC Key). Reenter the key to confirm the value.
Auth Port	Enter the UDP port number of the RADIUS server for authentication. Valid values: 1...65535 Default value: 1812
Acct Port	Enter the UDP port number of the RADIUS server for accounting. Valid values: 1...65535 Default value: 1813
Server Timeout (seconds)	Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Retry Count	Enter the number of times the device can retry transmission. Valid values: 1...100 seconds
Support for CoA	Click to enable or disable support change-of-authorization (CoA) messages. CoA messages modify session authorization attributes such as data filters. Default value: Enabled
CoA Server Key Type	• Clear Text • Encrypted • Hidden
CoA Server Key	If global encryption is enabled, then all keys/passwords are encrypted.
Confirm CoA Server Key	Enter in the same key as the COA Server Key.
Automate Tester	Enable automatic testing on the RADIUS server accounting and authentication for RADIUS server load balancing.

RADIUS Server Group Configuration

On the Servers/Groups tab, click RADIUS, Server Groups, and then click Add.



On the Quick Setup: AAA RADIUS Server page, complete the fields as described in Table 29, and then click Apply to Device.

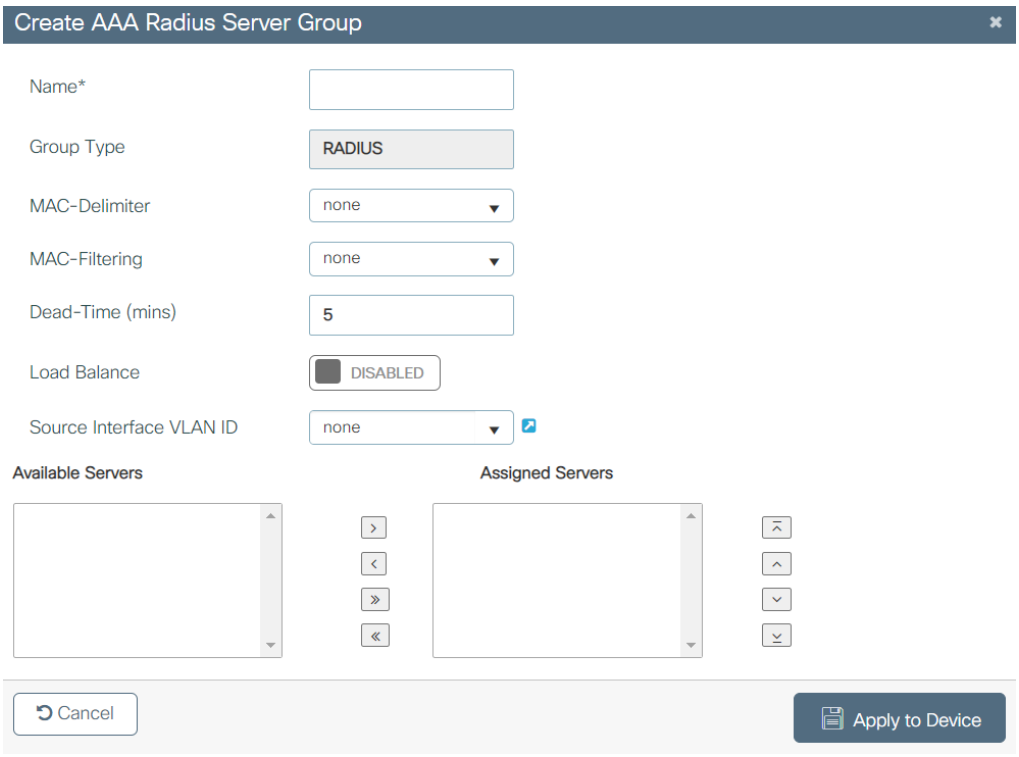
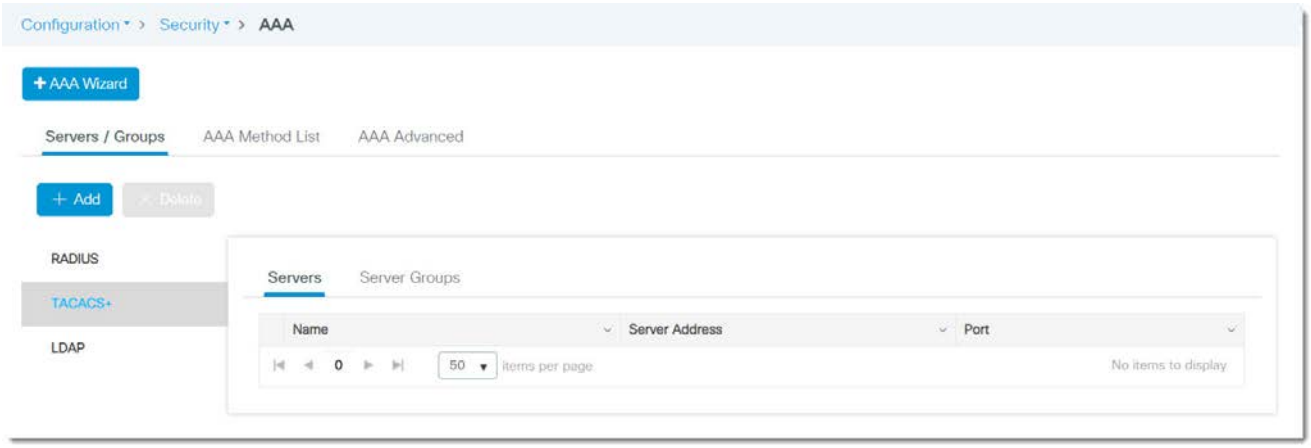


Table 29 - Create AAA RADIUS Server Group

Field	Description
Name	Enter a name to identify the RADIUS server group.
Group Type	(System-generated). Displays RADIUS.
MAC-Delimiter	Choose the delimiter to use in the MAC addresses that are sent to the RADIUS server: • none • colon • hyphen • single-hyphen
Load Balance	Disabled by default
Source Interface VLAN ID	Configured VLAN used for management communication to RADIUS server.
MAC-Filtering	Choose a value to use to filter MAC addresses: • none • MAC • Key
Dead-Time (mins)	Enter the amount of time, in minutes, after which a server is assumed to be dead. After this time, AAA traffic for the server group is redirected to alternative groups of servers that have different operational characteristics. Valid values: 1...1440
Available Servers Assigned Servers	In the Available Servers list, select the servers to include in the server group, and click to move them to the Assigned Servers list.

TACACS+ Server Configuration

On the Servers/Groups tab, click TACACS+, Servers, and then click Add.



On the Create AAA TACACS Server page, complete the fields as described in Table 30, and then click Apply to Device.

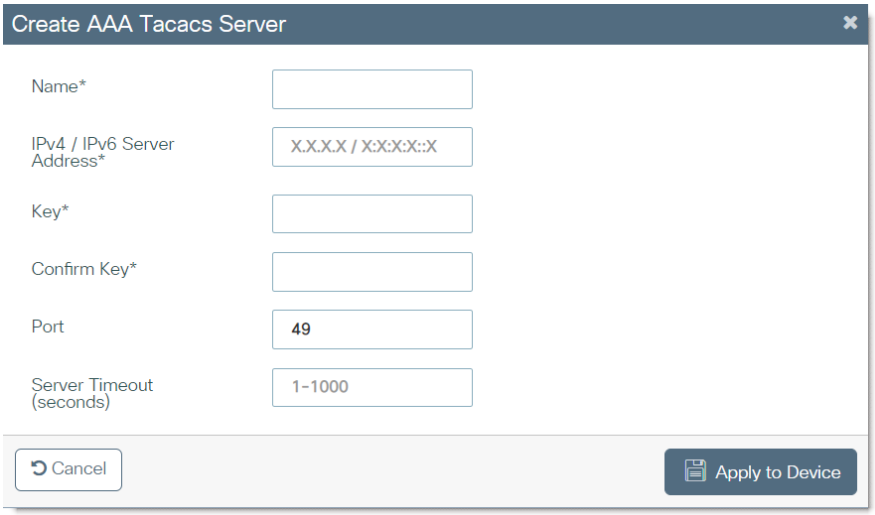
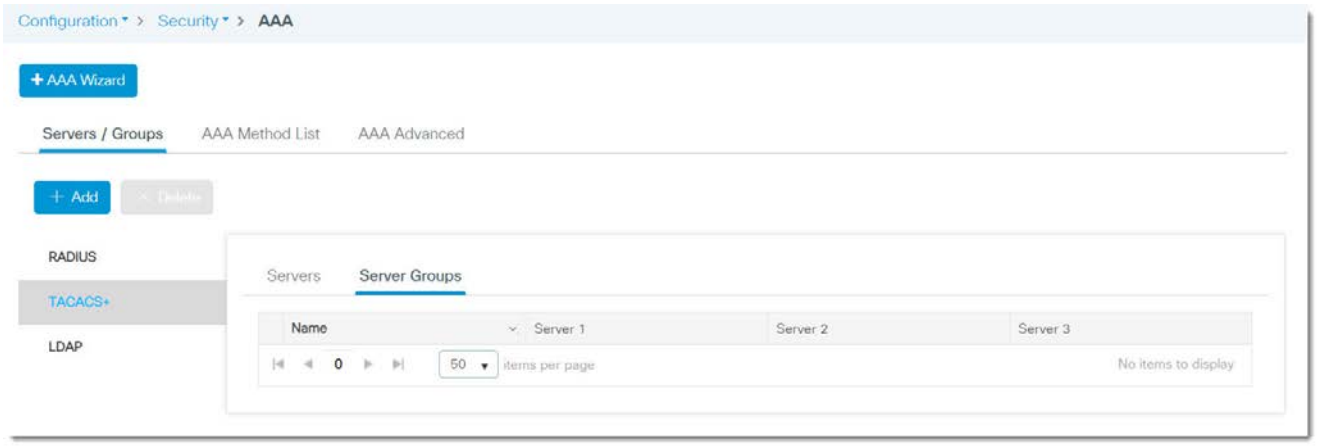


Table 30 - Create AAA TACACS Server

Field	Description
Name	Enter a name to identify the TACACS+ server.
IPv4 / IPv6 Server Address	Enter the IP address of the TACACS+ server.
Key	Enter the shared secret key to be used for authentication between the server and your device.
Confirm Key	Reenter the key to confirm the value.
Port	Enter the UDP port number of the TACACS server. Valid values: 1...65535 Default value: 49
Server Timeout (seconds)	Enter the number of seconds between retransmissions. Valid values: 1...1000

TACACS+ Server Group Configuration

On the Servers/Groups tab, click TACACS+, Server Groups, and then click Add.



On the Create AAA TACACS Server Group page, complete the fields as described in Table 31, and then click Apply to Device.

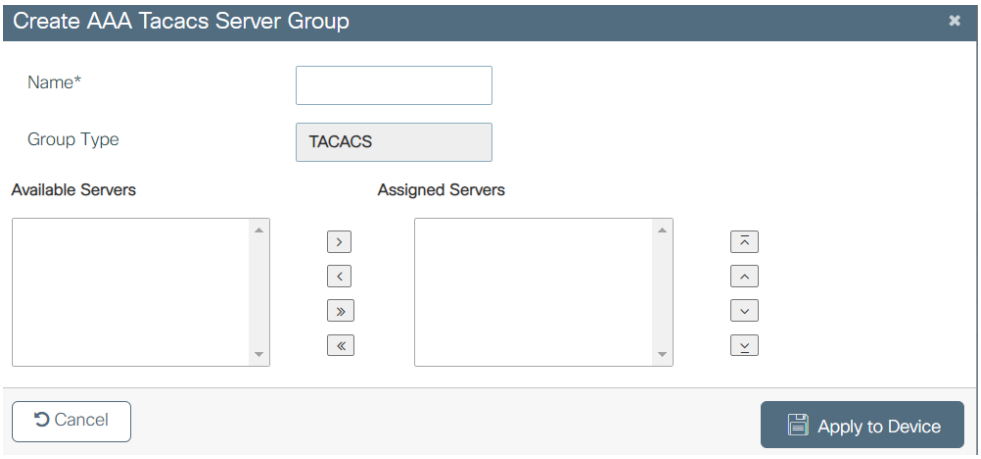
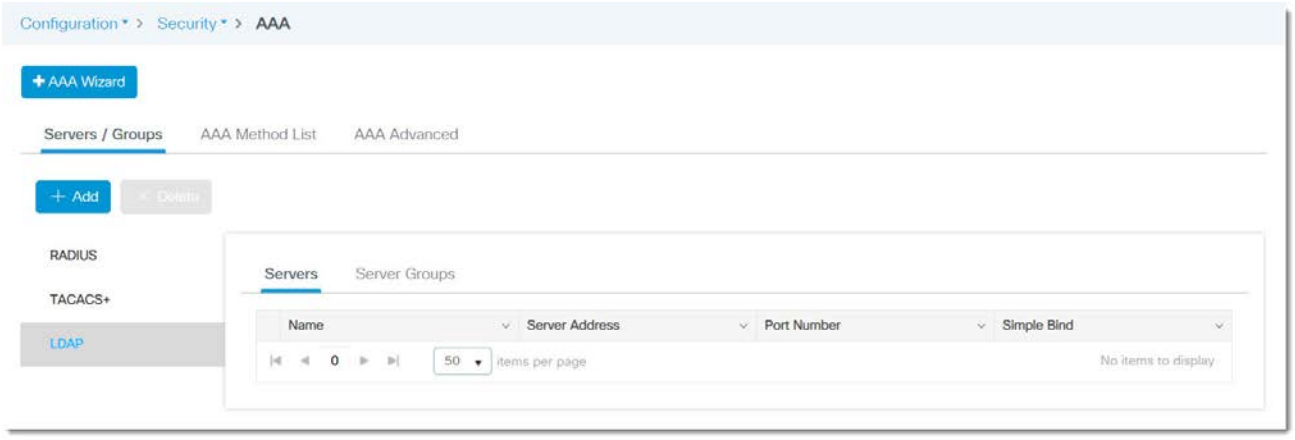


Table 31 - Create AAA TACACS Server Group

Field	Description
Name	Enter a name to identify the TACACS+ server group.
Group Type	(System-generated). Displays TACACS.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the servers to include in the server group, and click to move them to the Assigned Server Groups list.

LDAP Server Configuration

On the Servers/Groups tab, click LDAP, Servers, and then click Add.



On the Create AAA LDAP Server page, complete the fields as described in Table 32, and then click Apply to Device.

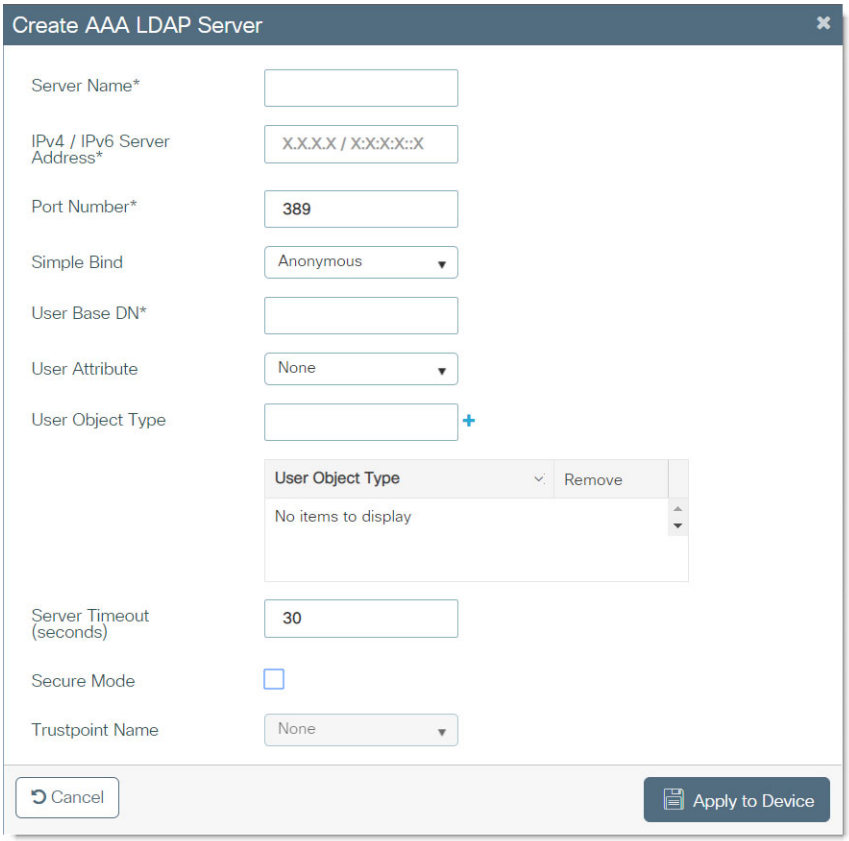
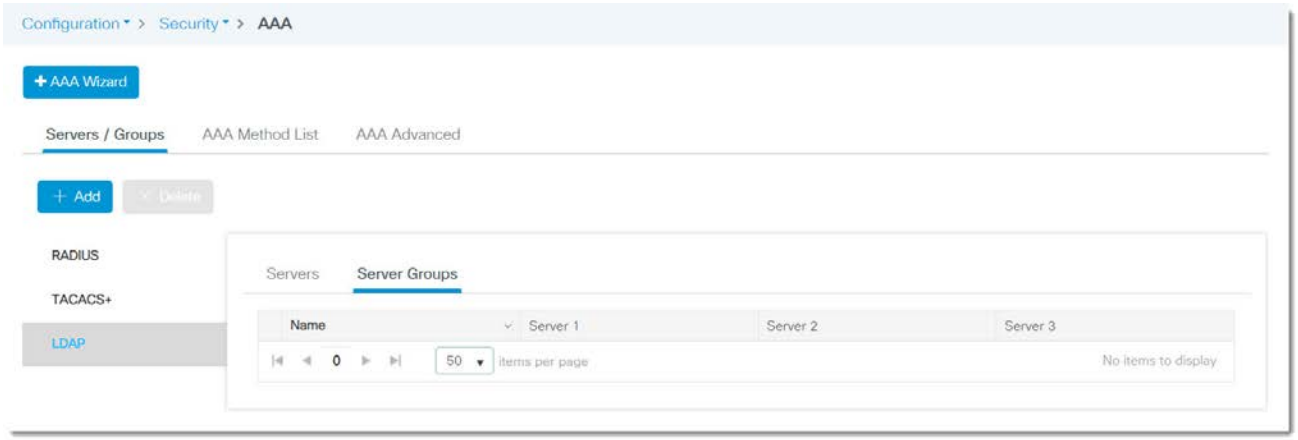


Table 32 - Create AAA LDAP Server

Field	Description
Server Name	Enter a name to identify the LDAP server.
IPv4/IPv6Server Address	Enter the IP address of the LDAP server.
Port Number	Enter the UDP port number of the LDAP server. Valid values: 1...65535 Default value: 389
Simple Bind	Choose the local authentication bind method for the LDAP server: • Anonymous—Allows anonymous access to the LDAP server. • Authenticated—Requires that a user name and password be entered to secure access. Default value: Anonymous
Bind User name	(Appears only if you choose Authenticated in the Simple Bind field). Enter a user name to be used for local authentication to the LDAP server. The user name can contain a maximum of 80 characters. If the user name starts with "cn=" (in lowercase letters), the controller assumes that the user name includes the entire LDAP database path and does not append the user base DN. This designation allows the authenticated bind user to be outside the user base DN.
Bind Password	(Appears only if you choose Authenticated in the Simple Bind field). Enter a username to be used for local authentication to the LDAP server. The user name can contain a maximum of 80 characters.
Confirm Bind Password	(Appears only if you choose Authenticated in the Simple Bind field). Reenter the bind password to confirm the value.
User Base DN	Enter the distinguished name (DN) of the subtree in the LDAP server that contains a list of all users. **EXAMPLE:** ou=organizational unit, .ou=next organizational unit, and o=corporation.com. If the tree containing users is the base DN, enter the following: . o=corporation.com, or dc=corporation, dc=com.
User Attribute	Enter the name of the attribute in the user record that contains the user name. You can obtain this attribute from your directory server.
User Object Type	Enter the value of the LDAP objectType attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user and some of which are shared with other object types.
Server Timeout (seconds)	Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Secure Mode	Check Secure Mode to configure a CA Trustpoint.
Trustpoint Name	If you checked Secure mode, choose a Trustpoint name.

LDAP Server Group Configuration

On the Servers/Groups tab, click LDAP, Server Groups, and then click Add.



On the Create AAA LDAP Server page, complete the fields as described in Table 32, and then click Apply to Device.

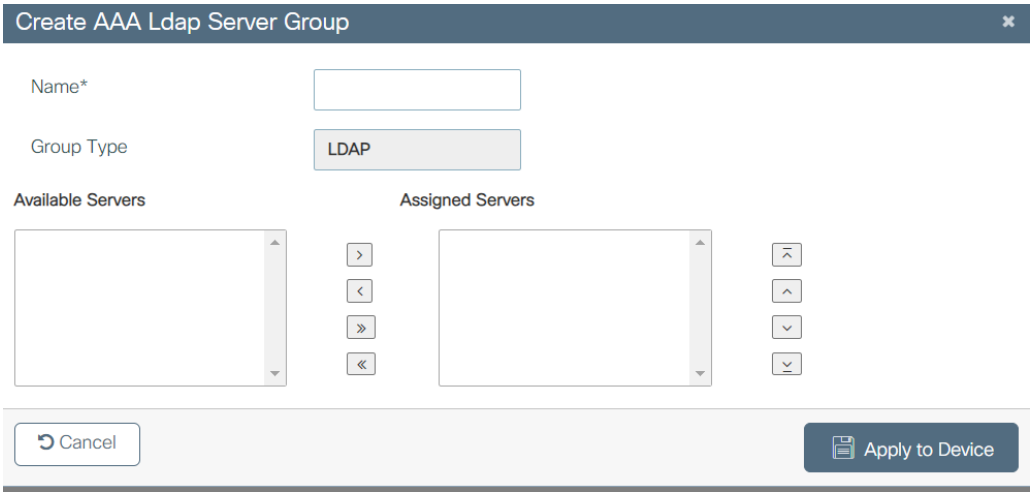


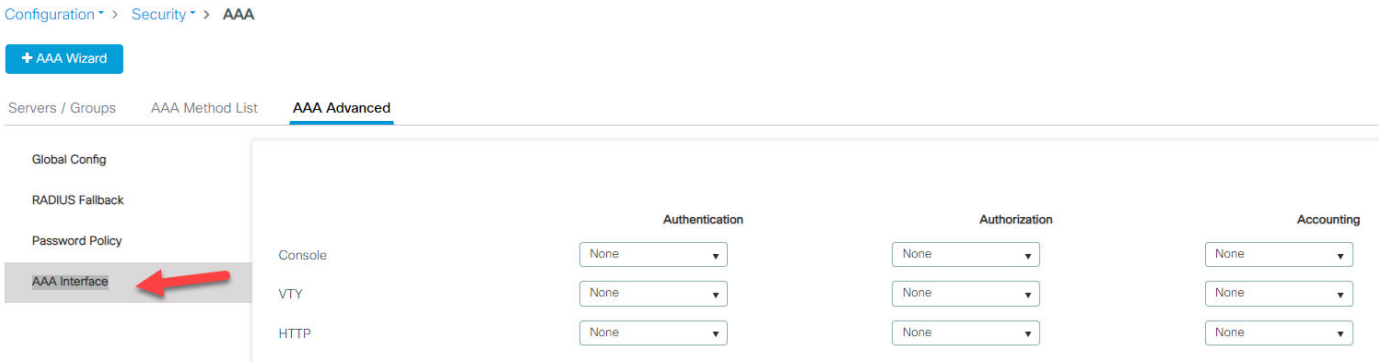
Table 33 - Create AAA LDAP Server Group

Field	Description
Name	Enter a name to identify the LDAP server group.
Group Type	(System-generated). Displays LDAP.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the servers to include in the server group, and click to move them to the Assigned Server Groups list.

Configure AAA Advanced Settings via the WebUI

You can configure AAA advanced settings outside of the AAA wizard. To use the wizard, see page 55.

From the Configuration menu, click AAA.



Global Configuration

On the AAA Advanced tab, click Global Config, complete the fields as described in Table 34, and then click Apply.

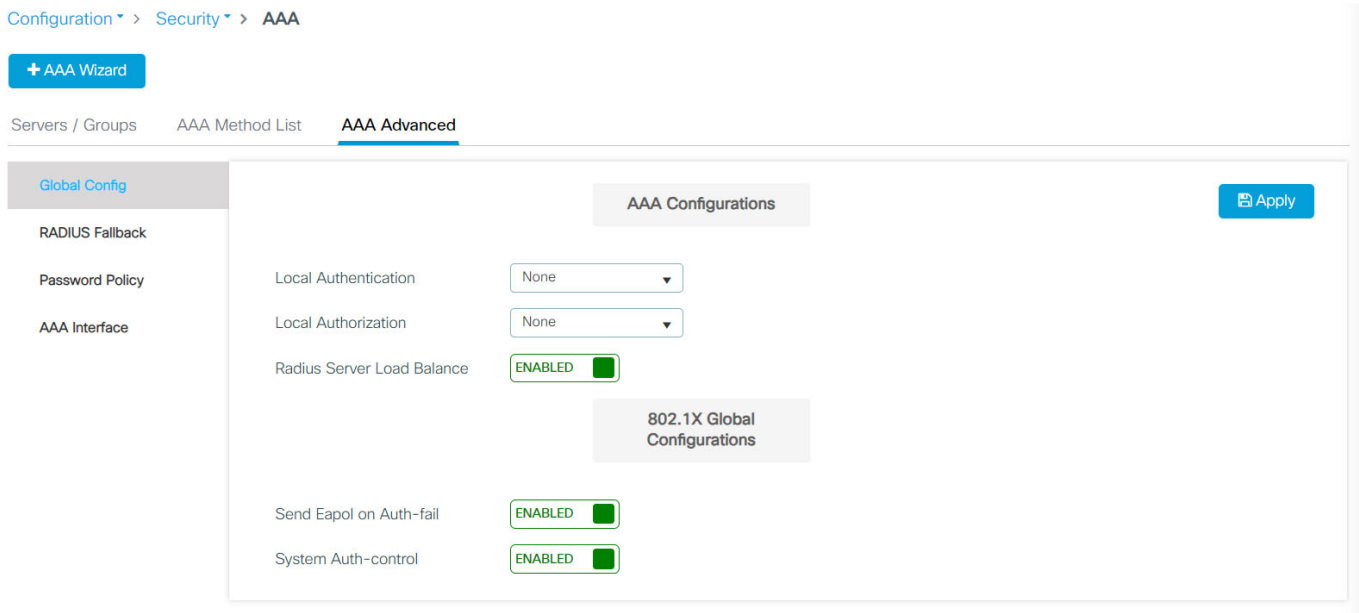


Table 34 - AAA Advanced—Global Config

Field	Description
AAA Configurations	
Local Authentication	Choose a local authentication method: • None—Do not use local authentication. If you choose None for local authentication, you must also choose None for local authorization. • Default—Use the default local authentication. • Method List—Choose a local authentication method list from the Authentication Method List field.
Local Authorization	• None—Do not use local authorization. If you choose None for local authorization, you must also choose None for local authentication. • Default—Use the default local authorization. • Method List—Choose a local authentication method list from the Authentication Method List field.
RADIUS Server Load Balance	Click to enable or disable load balancing for the global RADIUS server group.
802.1x Global Configurations	
Send Eapol on Auth-fail	Click to enable or disable Extensible Authentication Protocol over LAN (EAPOL) success messages. When enabled, the switch sends an EAPOL-Success message when it successfully authenticates a critical port.
System Auth-control	Click to globally enable or disable 802.1x authentication.

RADIUS Fallback Configuration

On the AAA Advanced tab, click RADIUS Fallback, complete the fields as described in Table 35, and then click Apply to Device.

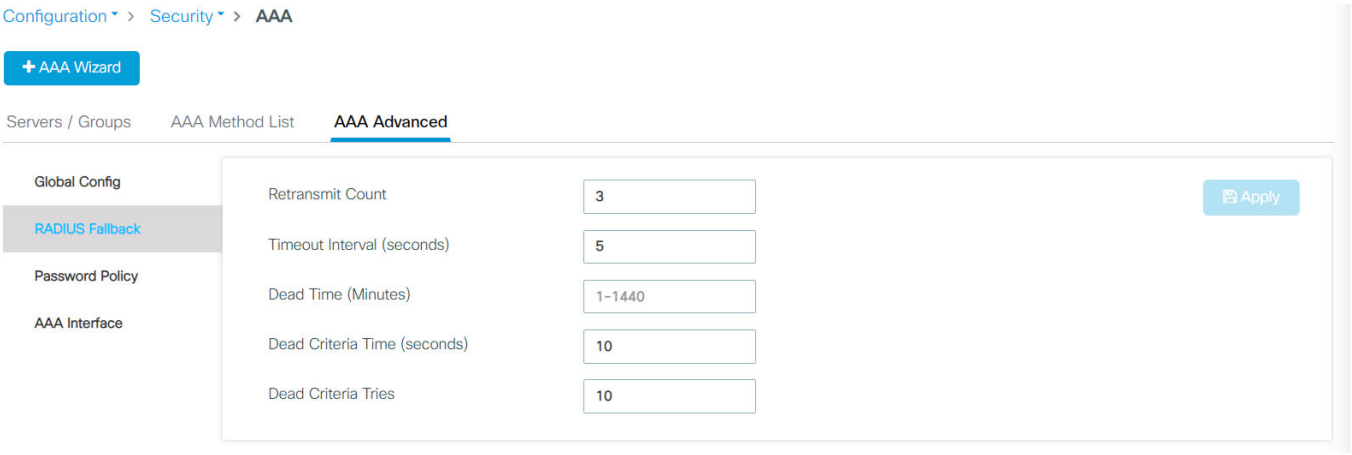
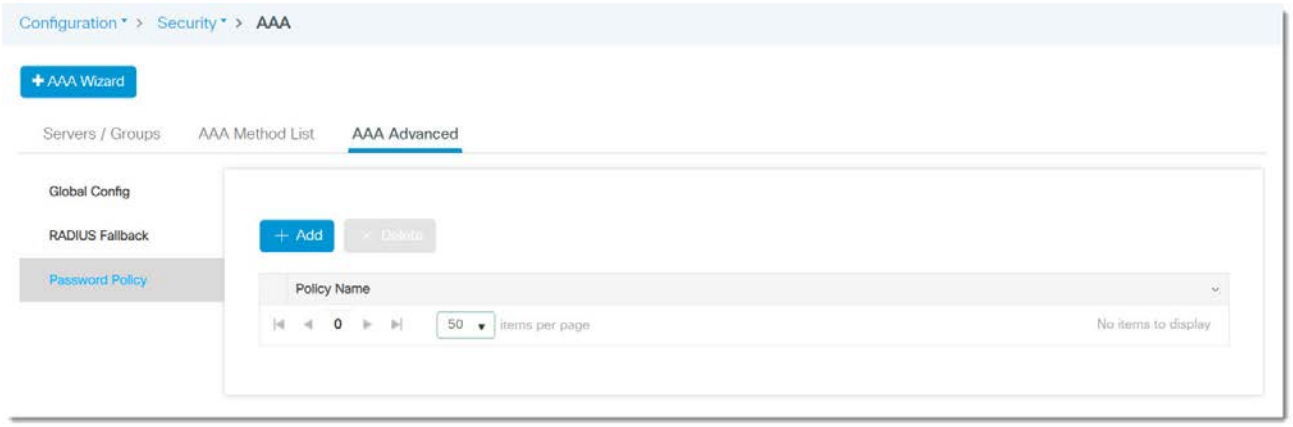


Table 35 - AAA Advanced—RADIUS Fallback

Field	Description
Retransmit Count	Enter the time after which the server should attempt retransmission.
Timeout Interval (Seconds)	Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Dead Time (Minutes)	Enter the amount of time, in minutes, after which a server is assumed to be dead.
Dead Criteria Time (Seconds)	Configure the minimum amount of time, in seconds, that must elapse from the time that the device last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the device booted, and there is a timeout, the time criterion will be treated as though it has been met.
Dead Criteria Tries	Enter the amount of tries, after which a RADIUS server is assumed to be dead.

Policy Password Configuration

On the AAA Advanced tab, click Policy Password, and then click Add.



On the Quick Setup: Password Policy page, complete the fields as described in Table 36, and then click Apply to Device.

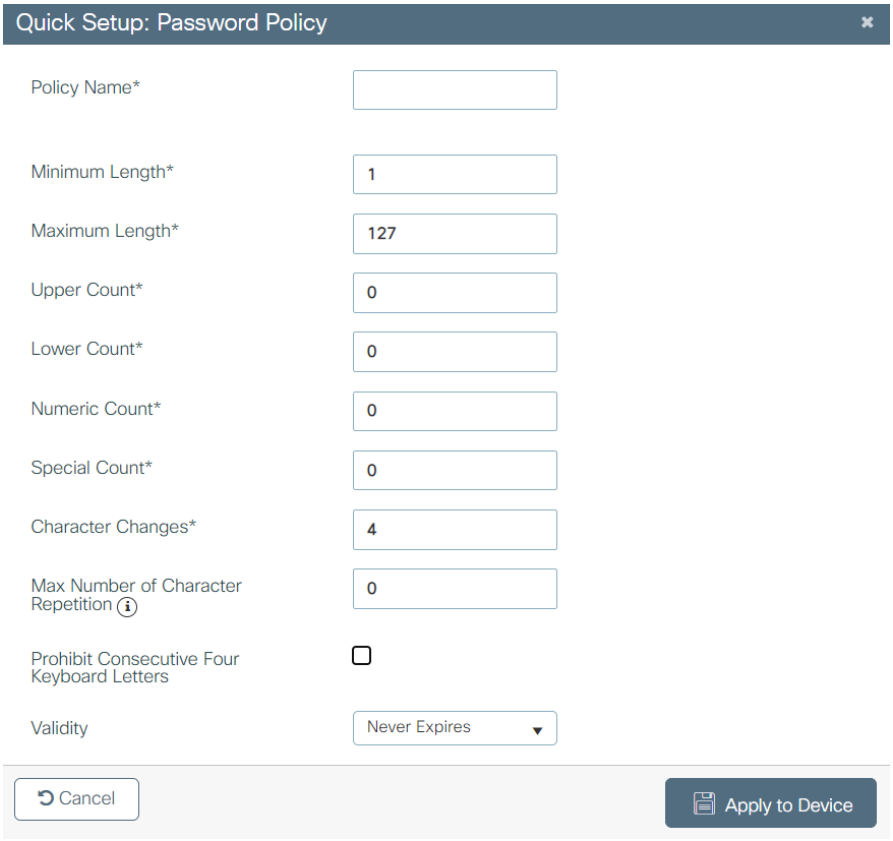


Table 36 - Quick Setup: Password Policy

Field	Description
Policy Name	Enter a name to identify the policy. The policy defines the criteria for the password.
Minimum Length	Enter the minimum length to require for the password. Default value: 1 Max Number of Character Repetition Prohibit Consecutive Four Keyboard Letters
Maximum Length	Enter the maximum length to require for the password. Default value: 127 Max Number of Character Repetition Prohibit Consecutive Four Keyboard Letters
Upper Count	Enter the number of uppercase letters to require for the password.
Lower Count	Enter the number of lowercase letters to require for the password.
Numeric Count	Enter how many numbers to require in the password.
Special Count	Enter how many special characters to require in the password.
Character Changes	Enter how many characters are required to differ from the previous password. Default value: 4
Validity	Choose the validity period for the password: • Never Expires • User Defined—Enter the number of years, months, days, hours, minutes, or seconds that the password remains valid.

Access Control Lists (ACLs)

ACLs provide basic security for a network by filtering traffic as it passes through a switch. ACLs permit or deny packets as they cross specified interfaces or VLANs. For more information about ACLs, see the Ethernet Reference Manual, publication ENET-RM002.

Configure ACLs via the WebUI

From the Configuration menu, choose ACL.



From the Access Control List page, you can add, edit, and delete ACLs:

- To add an ACL, see page 76. After you create an ACL, you must associate it with an interface to make it effective.
- To edit an access list, click the ACL in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an ACL, check its associated checkbox in the grid, and then click Delete.
- To associate ACLs to interfaces, see page 77.

Add an Access Control List

On the Access Control List page, click Add, complete the fields as described in Table 37, and then click Apply to Device.

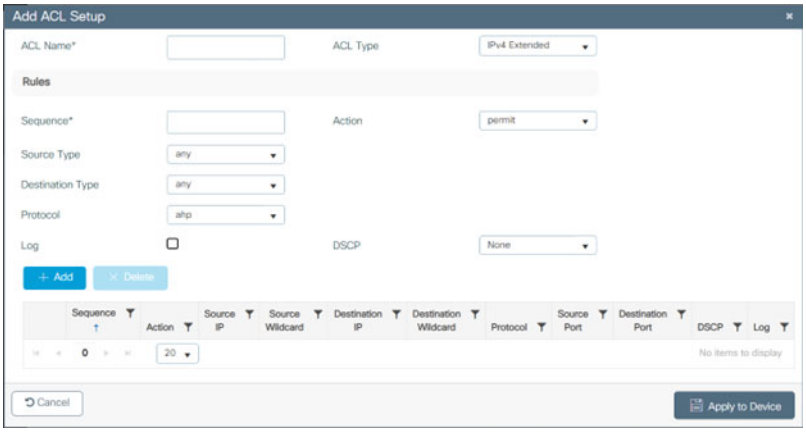


Table 37 - Add ACL Setup

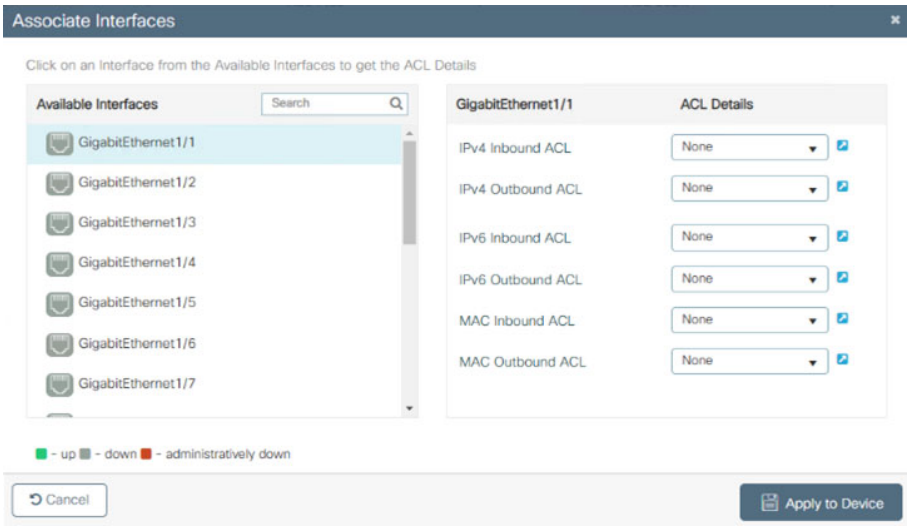
Field	Description
ACL Name	Enter a name to identify the ACL.
ACL Type	Choose the IP version to which the source or destination addresses belong: • IPv4 Standard • IPv4 Extended • IPv4 Role-based • IPv6 • MAC
Sequence	Enter a sequence number for the ACL.
Action	Choose if you want to deny or permit traffic using this ACL. The default action is permit.
Source Type	Choose the source type: • any • Host • IP
Host	(Appears only if the source type is Host). Enter the host name to indicate the source address.
Source IP	(Appears only if the source type is IP). Enter the source IP address. For IPv4 addresses, enter the subnet mask and for IPv6 addresses, enter the prefix length.
Source Wildcard/Prefix	(Appears only if the source type is IP). Enter the wildcard mask to identify the source addresses affected by the ACL: • For IPv4 addresses, enter the subnet mask. • For IPv6 addresses, enter the prefix length.
Destination Type	(Appears only if the ACL type is IPv4 Extended or IPv6). Choose the destination type: • any • Host • IP
Destination IP	(Appears only if the destination type is IP). Enter the destination IP address. For IPv4 addresses, enter the subnet mask and for IPv6 addresses, enter the prefix length.
Destination Wildcard/Prefix	(Appears only if the destination type is IP). Enter the wildcard mask to identify the destination addresses affected by the ACL: • For IPv4 Extended addresses, enter the subnet mask. • For IPv6 addresses, enter the prefix length.
Protocol	(Appears only if the ACL type is IPv4 Extended or IPv6). Choose the protocol to use for this ACL. The device can permit or deny only the IP packets in an ACL. Other types of packets, such as Address Resolution Protocol (ARP) packets, cannot be specified.
Source Port/Start Port/End Port	(Appears only if the protocol is TCP or UDP). Choose a source port or port range. The port or range is used by applications that send and receive data to and from the networking stack. Some ports are designated for specific applications such as Telnet, SSH, and HTTP.
Destination Port/Destination Port/End Port	(Appears only if the protocol is TCP or UDP). Choose a destination port or a port range. The port or range is used by applications that send and receive data to and from the networking stack. Some ports are designated for specific applications such as Telnet, SSH, and HTTP.
Log	Check Log to enable ACL logging.

Table 37 - Add ACL Setup (Continued)

Field	Description
DSCP	To use the ACL to mark associated packets with a DSCP value, choose a value.
Add	To add the sequence to the ACL, click Add. The sequence appears in the grid. To add an additional sequence, click Add and complete the fields in the Rules area.
Delete	To delete an ACL sequence and remove it from the grid, check its associated checkbox in the grid, and then click Delete.

Associate ACLs with Interfaces

1. On the Access Control List page, click Associate Interfaces.
2. In the list of available interfaces, select the interface to associate with ACLs.
3. From each ACL Details drop-down menu, choose an ACL name to associate with the corresponding traffic on the interface.
4. Click Apply to Device.



Discovery Protocols

The switch supports configuration of Layer 2 discovery protocols via the WebUI. You can use the protocols together or separately.

Cisco Discovery Protocol (CDP)

CDP is a Cisco® proprietary protocol that allows devices to communicate regardless of IP connectivity. The primary purpose of CDP is to communicate protocol addresses and device capabilities.

CDP allows network management applications, such as FactoryTalk® Network Manager™, to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

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 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 send and receive information from their neighbors. By using LLDP, devices can advertise details, such as configuration information, device capabilities, and device identity.

Table 38 describes the TLV structures.

Table 38 - 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 Discovery Protocols via the WebUI

From the Configuration menu, choose Discovery Protocols. On the Discovery Protocols page, you can configure CDP and LLDP.

Configure CDP

On the CDP tab, complete the fields in as described in Table 39, and then click Apply to Device.

CDP is enabled by default after completing express setup.

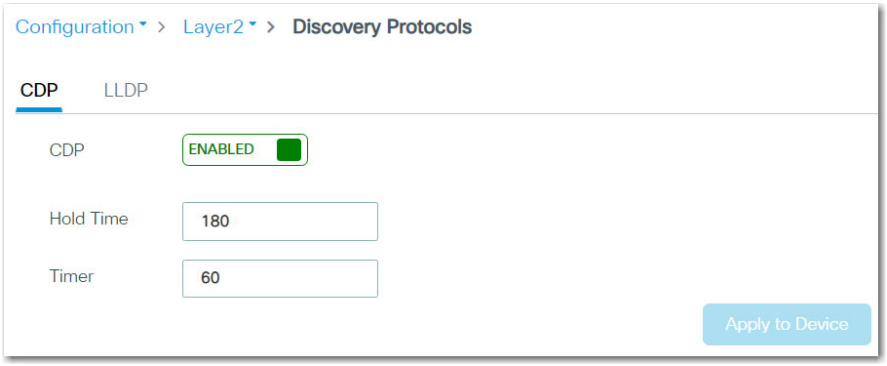


Table 39 - Discovery Protocols—CDP

Field	Description
CDP	Click to enable or disable CDP globally on the switch. CDP is enabled by default.
Hold Time	Enter the amount of time in seconds that the switch holds the CDP advertisement from a transmitting device before discarding it. Valid values: 10...255 Default value: 180
Timer	Enter the transmission frequency of CDP updates in seconds. Valid values: 5...254 Default value: 60

Configure LLDP

On the LLDP tab, complete the fields in as described in Table 40, and then click Apply to Device.

LLDP is enabled by default after completing express setup.

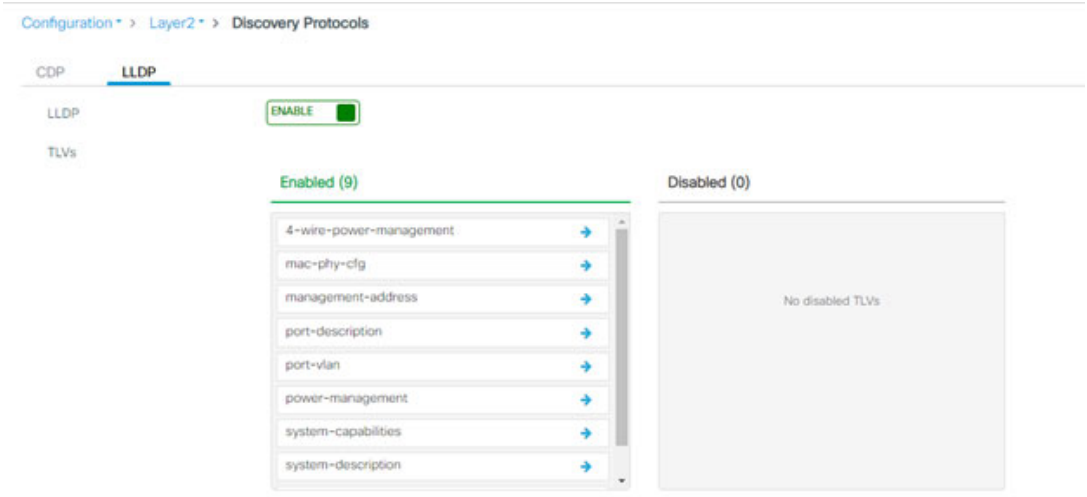


Table 40 - Discovery Protocols—LLDP

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 38 on page 78. By default, all TLV structures are enabled.

Device Level Ring (DLR) Topology

Device Level Ring (DLR) provides redundancy in a ring topology. The DLR protocol operates at Layer 2 and provides for fast network fault detection and reconfiguration for industrial networks. A DLR network includes at least one node that is configured as ring supervisor and up to 49 ring nodes. DLR also supports redundant gateways to allow a device on the DLR network to connect to the outside network.

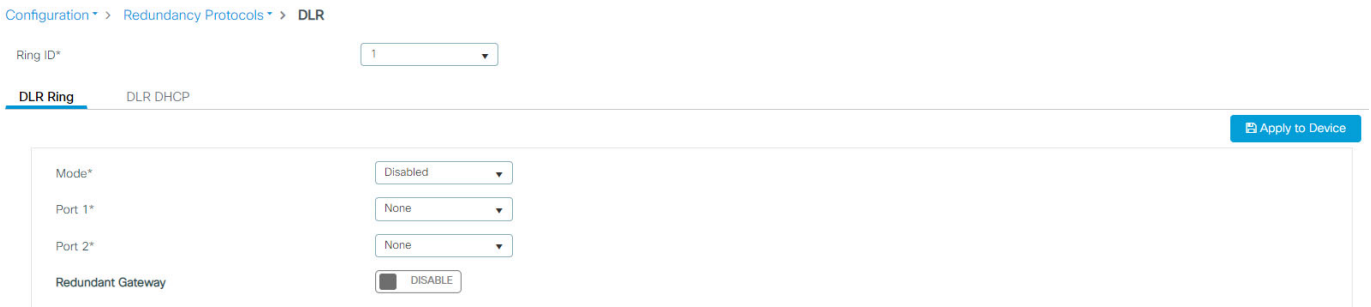
The switch supports multiple DLR rings (up to three on the Stratix 5800 switch and up to two on the Stratix 5200 switch), with the following limitations:

- DLR ring ports cannot be shared across multiple rings.
- To support multiple rings on Stratix 5800 switch, you must change the FPGA profile from "Default" to "Redundancy".
- WebUI restricts the ports that you can select for the DLR ring ports based on the switch device type.
- DLR ring access ports attached to the same ring instance must belong to the same access VLAN.
- If a switch is the active/backup gateway, it must be the active/backup gateway for all rings. A switch cannot act as the active gateway for one ring, and another switch act as active gateway for another ring.
- A DLR ring's active supervisor is also its Active DLR DHCP Server.
- The DLR ring number assignments do not have to match between switches. This is only a recommendation for clarity and has no effect on functionality.

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

Configure DLR Ring via WebUI

1. On the Configuration > Redundancy Protocols > DLR page, select the Ring ID number of the DLR ring. The Ring ID is 1 or 2 on a Stratix 5200 switch, and 1...3 on a Stratix 5800 switch.



2. On the DLR Ring tab, specify the Mode, Node or Supervisor, and select two consecutive ring ports.

Figure 21 - Supervisor Settings

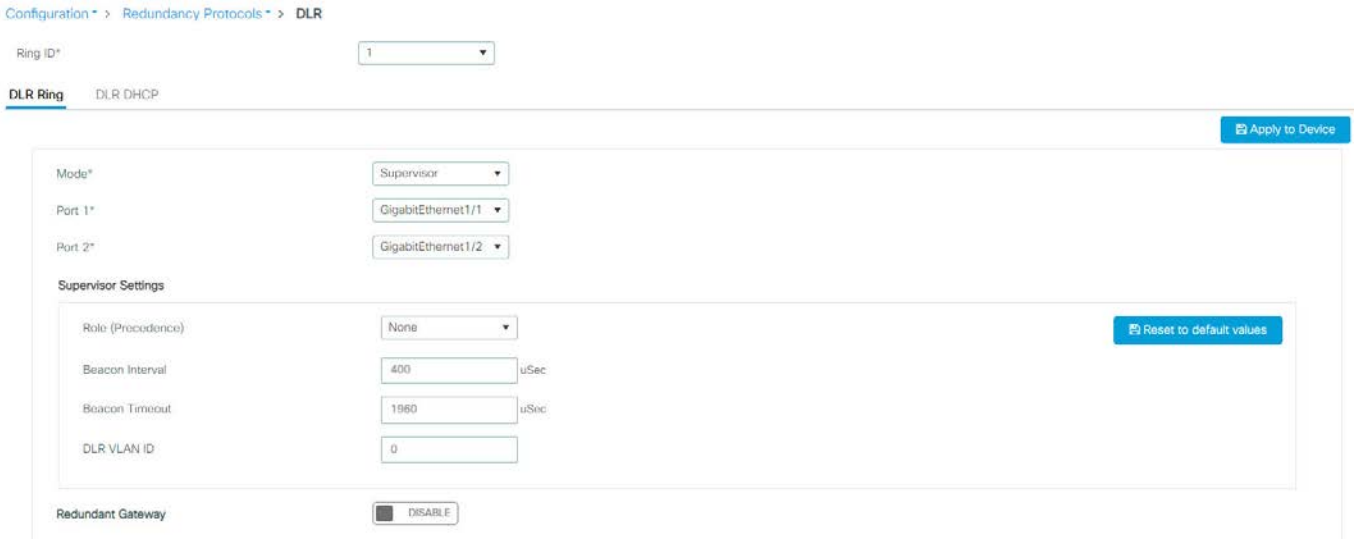


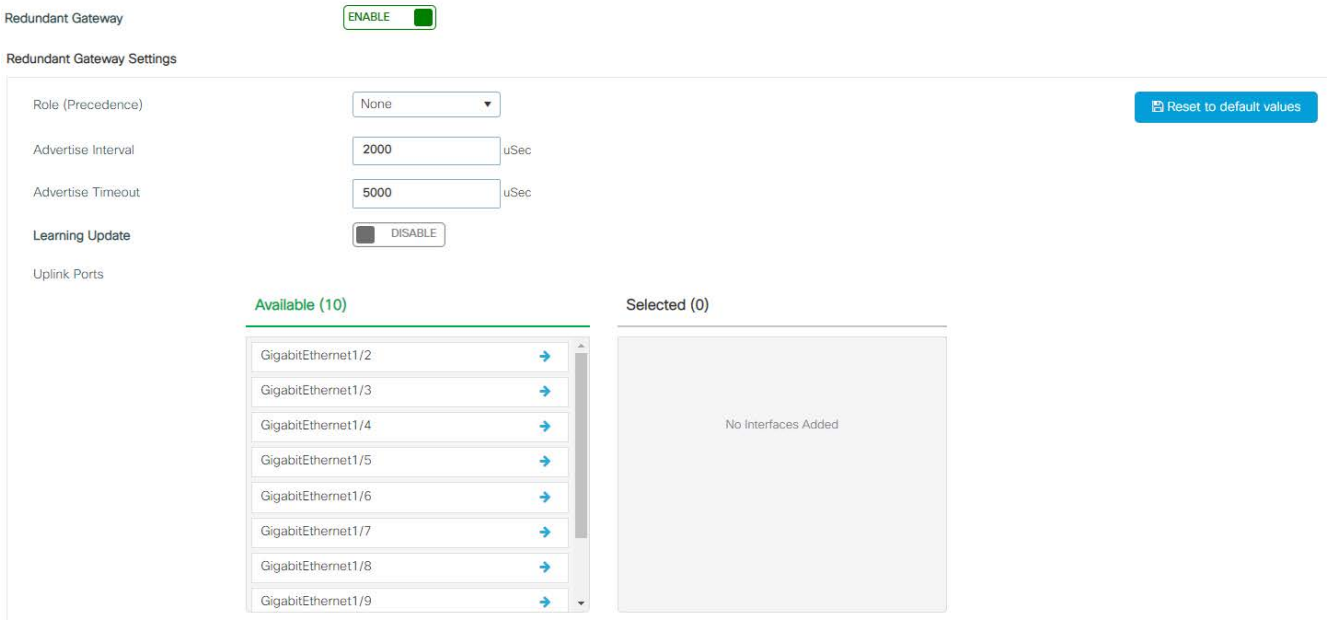
Table 41 - Supervisor Settings

Field	Description
Role (Precedence)	Assigned to the ring supervisor that corresponds to a pre-defined precedence value. A higher value means higher precedence. The options are as follows: • None - 0 • Primary - 255 • Backup - 1...100 • Backup - 2...90 • Backup - 3...80 • Custom - Enter a value from 0...255
Beacon Interval	Transmits beacon frames. The range is 200...100,000 microseconds. The default is 400 microseconds.
Beacon Timeout	The amount of time that ring nodes wait before timing out in the absence of received beacon messages. The range is 200...500,000 microseconds. The default is 1960 microseconds.
VLAN ID	The value 0 means that no VLAN ID is required in beacon messages. The default is 0.

3. To add a Redundant Gateway node, click the button to enable Redundant Gateway and configure Redundant Gateway Settings (or retain default values).

   Redundant Gateway requires all devices on the DLR ring to be Redundant Gateway capable.

Figure 22 - Redundant Gateway Settings

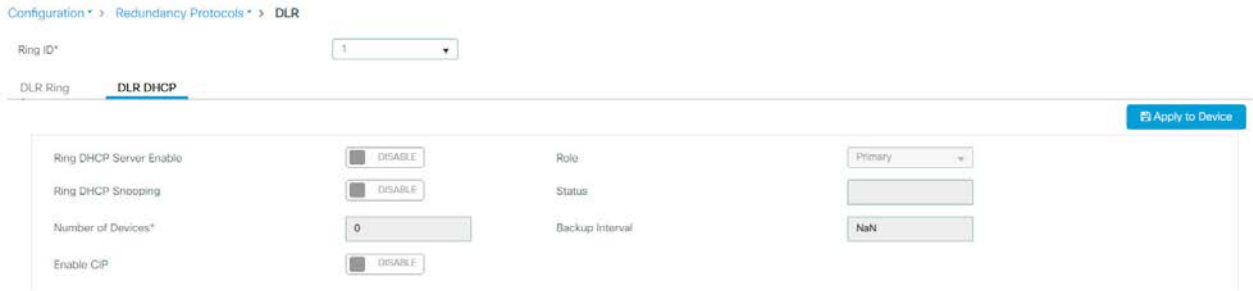


Field	Description
Role (Precedence)	Assigned to the ring supervisor that corresponds to a pre-defined precedence value. A higher value means higher precedence. The options are as follows: • None - 0 • Primary - 255 • Backup - 1...100 • Backup - 2...90 • Backup - 3...80 • Custom - Enter a value from 0...255
Advertise Interval	Interval where the gateway transmits advertise messages. The range is 1000 microseconds to 100,000 microseconds. The default is 2000 microseconds.
Advertise Timeout	the number of time nodes wait before timing out in the absence of received advertise messages. The range is 200 microseconds to 500,000 microseconds. The default is 5000 microseconds.
Learning Update	Specifies the use of learning update messages. The default is Enabled.

4. To save the DLR Ring settings, click Apply to Device.

Configure DLR DHCP

Use the DLR DHCP page to assign IP addresses to devices on the DLR ring using the active DLR supervisor and DHCP server running on the switch.

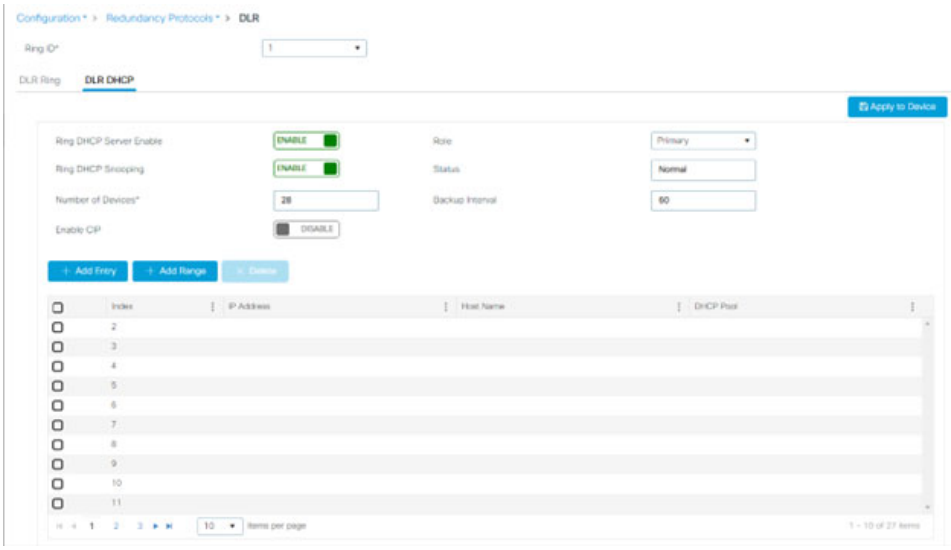


1. On the Configuration > Redundancy Protocols > DLR page, on the DLR DHCP tab, select the Ring ID number of the DLR ring. The ID is 1 or 2 on a Stratix 5200 switch, and 1 to 3 on a Stratix 5800 switch.

Table 42 - DLR DHCP Fields

Field	Description
Ring DHCP Server	Enables the Ring DHCP Server on the DLR supervisor device.
Ring DHCP Snooping	Enables Ring DHCP Snooping. When enabled, Ring DHCP Snooping restricts the broadcast of DHCP requests from going beyond the DLR ring. Only devices in the DLR ring receive address assignments from the DHCP server. DHCP snooping is enabled by default. If you are not using DLR DHCP, you can disable Ring DHCP Snooping to use DHCP server functionality outside of the ring.
Number of Devices	The number of devices in the DLR ring.
Enable CIP	Enable CIP on DLR DHCP.
Role	Select the role of the Ring DHCP Server: • None • Primary • Backup • Secondary
Status	The status is not an editable field. It displays the status of the DLR ring. The options for status are. • Normal • Ring Fault • Unexpected Loop Detected • Partial Network Fault • Rapid Fault/restore Cycle
Backup Interval	The interval, in seconds, at which the Backup Ring DHCP Server reads the reference table of the Active Ring DHCP Server. The range is 1...65535 seconds. The default is 60.

2. When the role of the Ring DHCP Server is Backup or Secondary (DLR Supervisor functions as Backup Ring DHCP Server), click the button to enable CIP and enter the Active Ring DHCP Server CIP IP address. This allows the Backup Ring DHCP Server to sync information with the Active Ring DHCP Server.



3. To add an entry to the DLR DHCP configuration table, click Add Entry and configure the following fields:
   a. Enter the Index value that indicates the ring member location. The range is 2...255.
   b. Enter the IP address for the entry.
   c. Enter the Host Name associated with the IP address for the entry.
   d. Select the DHCP Pool from the dropdown menu.

      The DHCP pool must be previously configured. See Configuring DHCP Pools.

   e. Click Apply to Device to save the entry.

4. Click Add Range to add a range of entries.
   a. Enter the Starting Index value that indicates the starting location of the ring members in the range. The range is 2...255.
   b. Enter the Starting IP address for the range of entries.
   c. Enter the Number of Entries in the range.
   d. Select the DHCP Pool from the drop-down menu.

      The DHCP pool must be previously configured. See Configuring DHCP Pools.

   e. Click Apply to Device to save the range of entries.
5. To save the DLR DHCP settings, click Apply to Device.

DLR Port Choices

Select switches allow you to configure DLR. DLR is supported on any adjacent port pair (N, and N+1) where N is an odd port number.

Stratix 5200 switches support up to two rings of DLR and are the following:

- SKUS that support one ring of DLR - 1783-CMS10DP, 1783-CMS20DB, 1783-CMS20DP
- SKUS that support two rings of DLR - 1783-CMS10DN and 1783-CMS20DN

Stratix 5800 switches support up to three rings of DLR on the following advanced feature catalog switches and expansion modules:

- 1783-MMS10A, 1783-MMS10AR, 1783-MMS10EA, 1783-MMS10EAR, 1783-MMX8EA, 1783-MMX8TA, 1783-MMX8SA. The Stratix 5800 switch supports up to three DLR rings on switches with an expansion module. When configuring multiple rings, the FPGA profile must be changed from Default to Redundancy.

Default FPGA Profile DLR Behavior

- A switch with no expansion supports one ring
- A switch with an expansion module supports two rings

Redundancy FPGA Profile DLR Behavior:

- A switch without and expansion module supports two rings.
- A switch with an expansion module supports three rings.
  - Two rings can be configured on the switch and one ring can be configured on the expansion module
  - One ring can be configured on the switch and two rings can be configured on the expansion module.

For more information on Redundancy, see High-availability Seamless Redundancy (HSR) (Stratix 5800 Switch Only) on page 111.

We recommend that you use the Multiport Automation Device Smartport role on ports you configure for DLR. See Smartports on page 175.

Enhanced Interior Gateway Routing Protocol (EIGRP) (Stratix 5800 Switch Only)

EIGRP is a Cisco proprietary, distance-vector-routing protocol. The following capabilities distinguish EIGRP from other routing protocols:

- Fast convergence
- Support for variable-length subnet mask
- Support for partial updates
- Support for multiple network layer protocols

IMPORTANT EIGRP is available only on Layer 3 switch models. For supported catalog numbers, see Table 1 on page 15.

Feature Summary

EIGRP features include the following:

- Hybrid Distance Vector/Link State algorithm
- Classless routing protocol
- Support for Variable Length Subnet Mask (VLSM) and Classless Interdomain Routing (CIDR)
- Support for summaries and discontinuous networks
- Performs partial updates as needed
- Consumes less bandwidth (no broadcasts, no periodic updates, updates contain only changes)
- Efficient neighbor discovery and fast convergence
- Best path selection via Diffusing Update Algorithm (DUAL)
- Support for IP, IPX, and AppleTalk via protocol-dependent modules

Network Operation

A device 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 continue until an alternate route is found. Variable-length subnet masks enable routes to be automatically summarized on a network number boundary. EIGRP can also 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. Partial updates are limited so that only routers that need the information are updated.

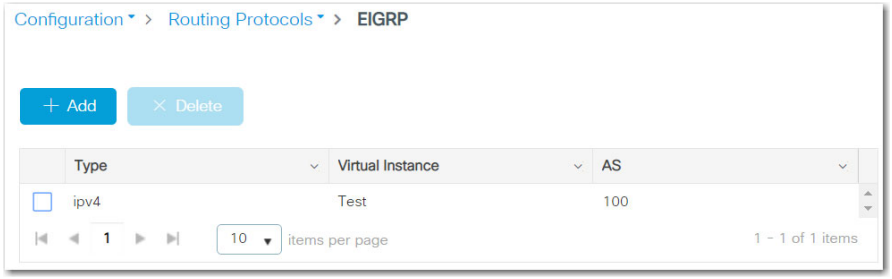
Neighbor discovery is the process that the EIGRP device uses to dynamically learn of other routers on directly attached networks. EIGRP devices send multicast hello packets to announce their presence on the network. You can also define static neighbors, which receive unicast packets. When the device 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 device. Once this neighbor relationship is established, routing updates are not exchanged unless there is a change in the network topology.

EIGRP uses the Diffusing Update Algorithm (DUAL), which provides loop-free operation at every instance throughout a route computation. DUAL allows all devices that are involved in a topology change to synchronize simultaneously. Routers that are 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 the WebUI

From the Configuration menu, choose EIGRP.



From the EIGRP page, you can add, edit, and delete EIGRP instances:

- To add an EIGRP instance, click Add, complete the fields as described in Table 43, and then click Apply to device
- To edit an EIGRP instance, click the EIGRP instance in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an EIGRP instance, check its associated checkbox in the grid, and then click Delete.

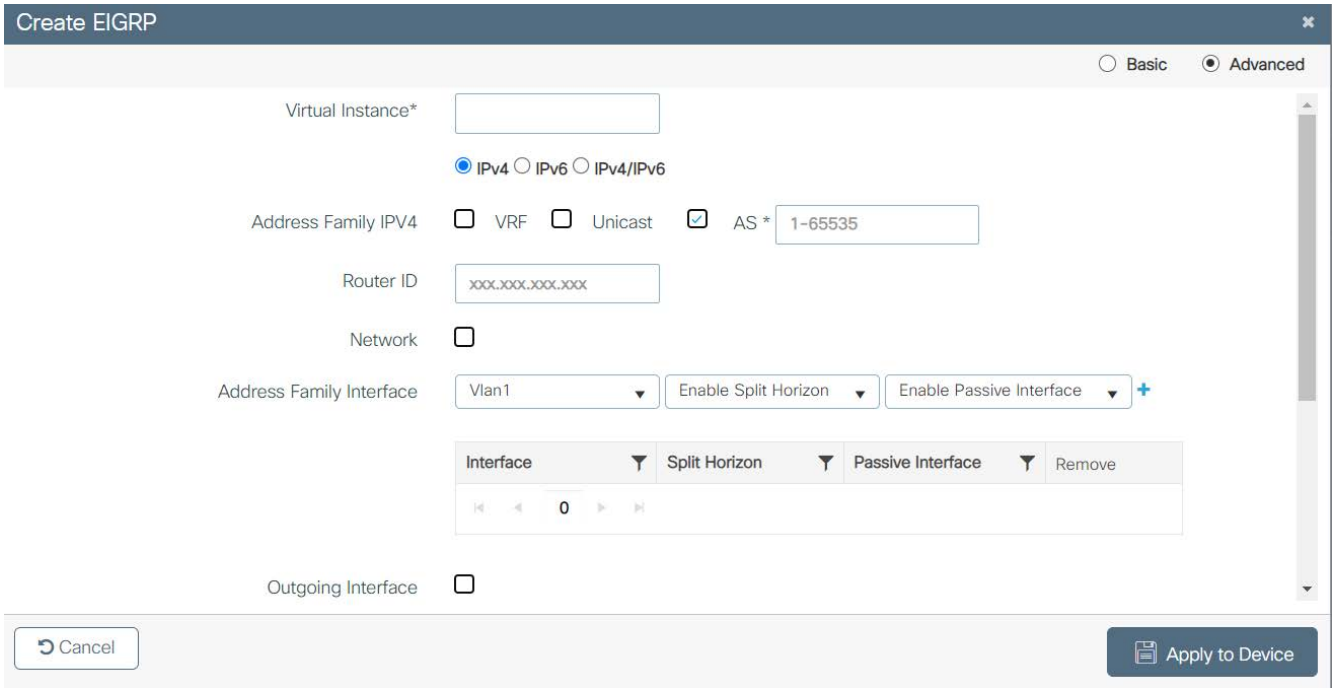


Table 43 - Create EIGRP

Field	Description
Basic or Advanced	Click to determine the level of configuration: • Basic—The page displays only basic configuration fields. Basic is the default value. • Advanced—The page displays both basic and advanced configuration fields.
Basic Settings	
Virtual Instance	Enter a name to identify the EIGRP route in the network.
IPV4, IPV6, IPV4/IPV6	Click the IP version for which to configure EIGRP.
Address Family IPV4	Specify the following information for IPv4, IPv6, or both: 1. Check VRF, and then choose the VRF name. 2. To enable unicast transmission, check Unicast. 3. Check AS, and then enter the AS number. Valid values: 1...65535
Advanced Settings	
Router ID	Enter a router ID to manually configure the router for EIGRP. The router ID identifies the originating router for external routes. If an external route is received with the local router ID, the route is discarded. EIGRP automatically selects an IP address to use as the router ID when an EIGRP process is started. The highest IP address assigned to a loopback interface is selected as the router ID. If there are not any loopback addresses configured, the highest IP address assigned to any other interface is chosen as the router ID. The highest local IP address is selected and loopback interfaces are preferred. The router ID can be configured with any IP address with two exceptions: 0.0.0.0 and 255.255.255.255 are not valid values. Configure a unique value for each router.
Network	(IPv4 only). Check Network, and then enter the network IP address and the wildcard mask. To list the network IP address and wildcard details, click the plus sign (+).
Address Family Interface	In Address Family Interface you can enable or disable Split Horizon and Passive interface on the switch interfaces. • 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. In general, we recommend that you keep split horizon enabled unless you are certain that your application requires the change in order to properly advertise routes. • Passive Interface suppresses the exchange of hello packets between two routers. This results in the loss of their neighbor relationship. It stops not only routing updates from being advertised, but it also suppresses incoming routing updates.
Outgoing Interface Stub	This static configuration must be performed on both neighbors, and the specified IP address must belong to the same subnet as the specified outgoing interface. To configure the outgoing interface, do the following: 1. Check Outgoing Interface. 2. From the drop-down menu, choose an interface. 3. Click the plus sign (+) to add the interface to the grid.
Stub	The EIGRP stub routing feature improves network stability, reduces resource utilization, and simplifies the stub device configuration. To enable the stub routing feature, do the following: 1. Check Stub. 2. To set the device as a receive-only neighbor, check Receive only. 3. To advertise redistributed routes from other protocols and autonomous systems, check Redistribute. 4. To advertise static routes, check Static. 5. To advertise summary routes, check Summary.
Variance	The variance number is used to load balance over unequal cost paths. The variance number is multiplied by the local best metric then includes the routes with the lesser or equal metric. Enter the variance number. Valid values: 1...128 Default value: 1 (equal-cost load balancing)
Redistribute	Redistribution is the use of a routing protocol to advertise routes that are learned by some other means, such as by another routing protocol, static routes, or directly connected routes. Check each protocol or routing type to redistribute, and then enter the metrics for each type.
Auth Key	Enter an authentication key.
Enable Best Practices	To enable the default features, check Enable Best Practices. To view the list of default features, hover your mouse over the information icon .

Ethernet Ports

Configure Ethernet ports, or interfaces, on the switch to 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.

Advanced Port Configuration

Advanced port configuration includes these features:

- 802.1X Configurations
- Access Lists
- DHCP relay
- DHCP snooping
- IP Device Tracking
- Quality of Service (QoS) policy management
- Port security
- Port thresholds and storm control

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

Configure Ethernet Interfaces via the WebUI

From the Configure menu, choose Ethernet Ports.

Figure 23 - Stratix 5200 Ethernet Ports

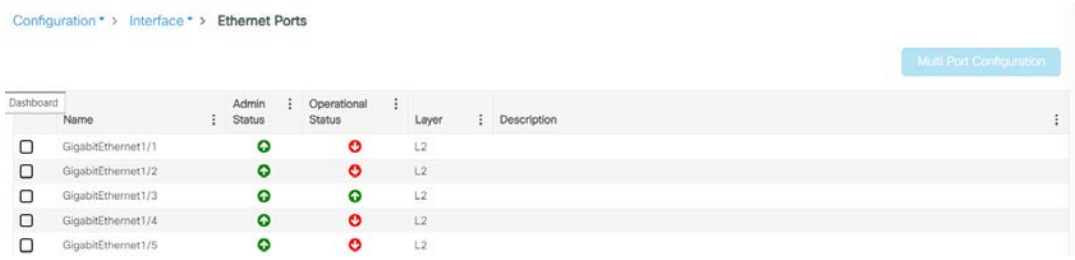
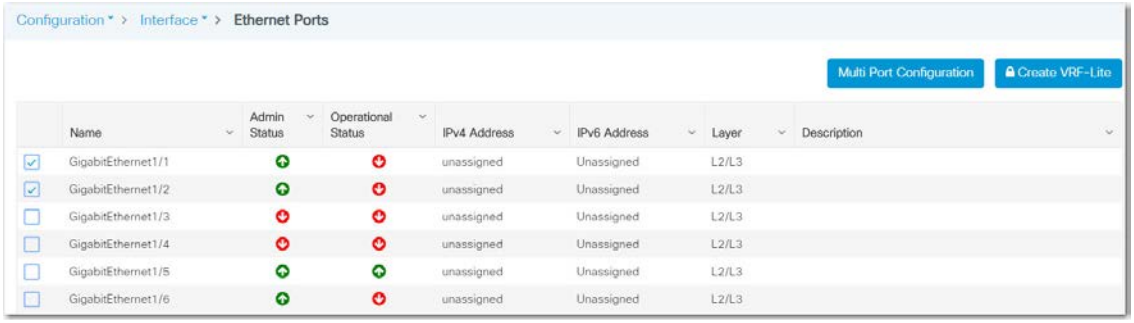


Figure 24 - Stratix 5800 Ethernet Ports



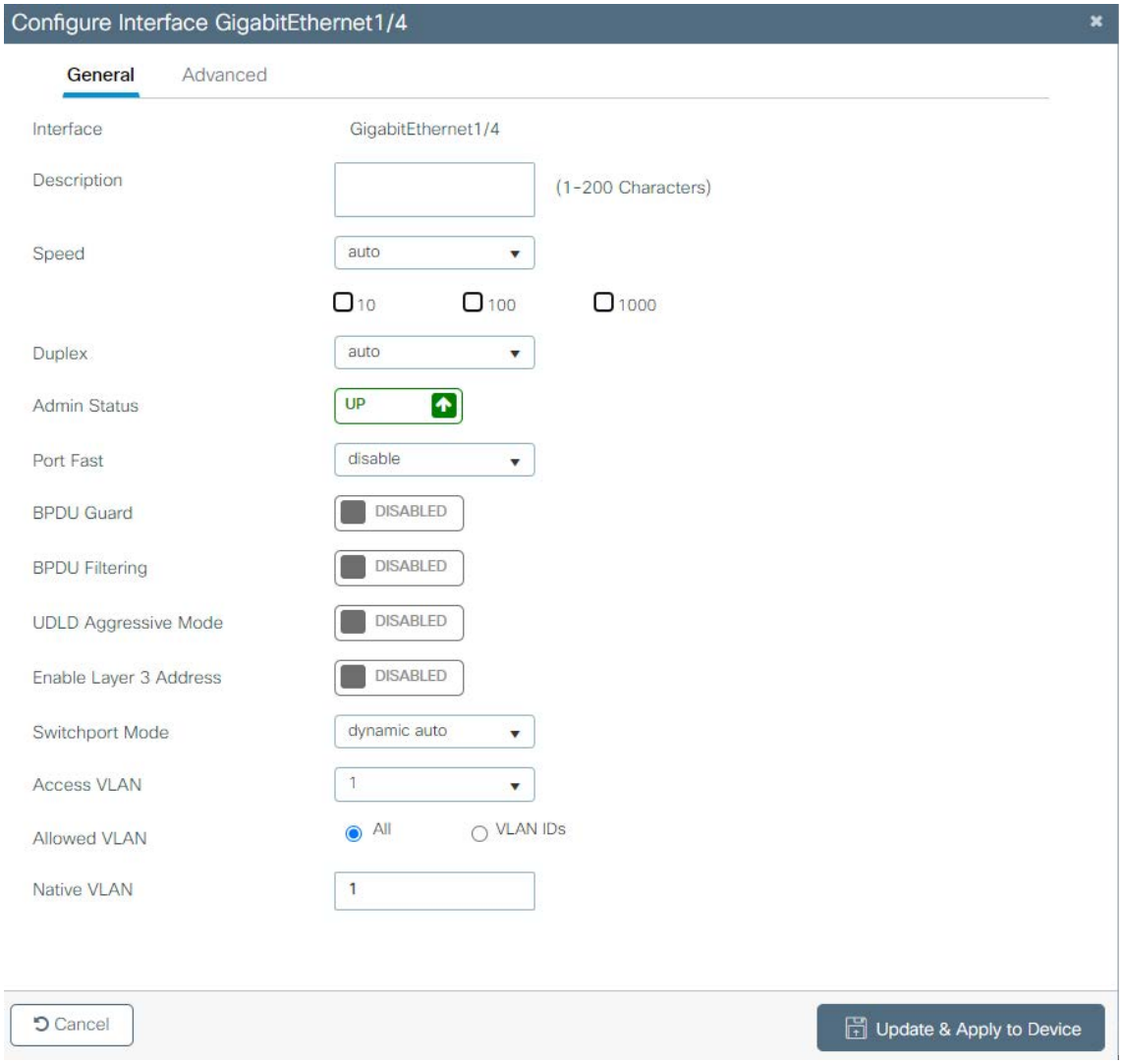
From the Ethernet Ports page, you can do the following:

- Configure individual ports as described on page 90.
- Configure multiple ports simultaneously as described on page 92.
- Configure VRF-Lite as described on page 97.

Configure Individual Ports

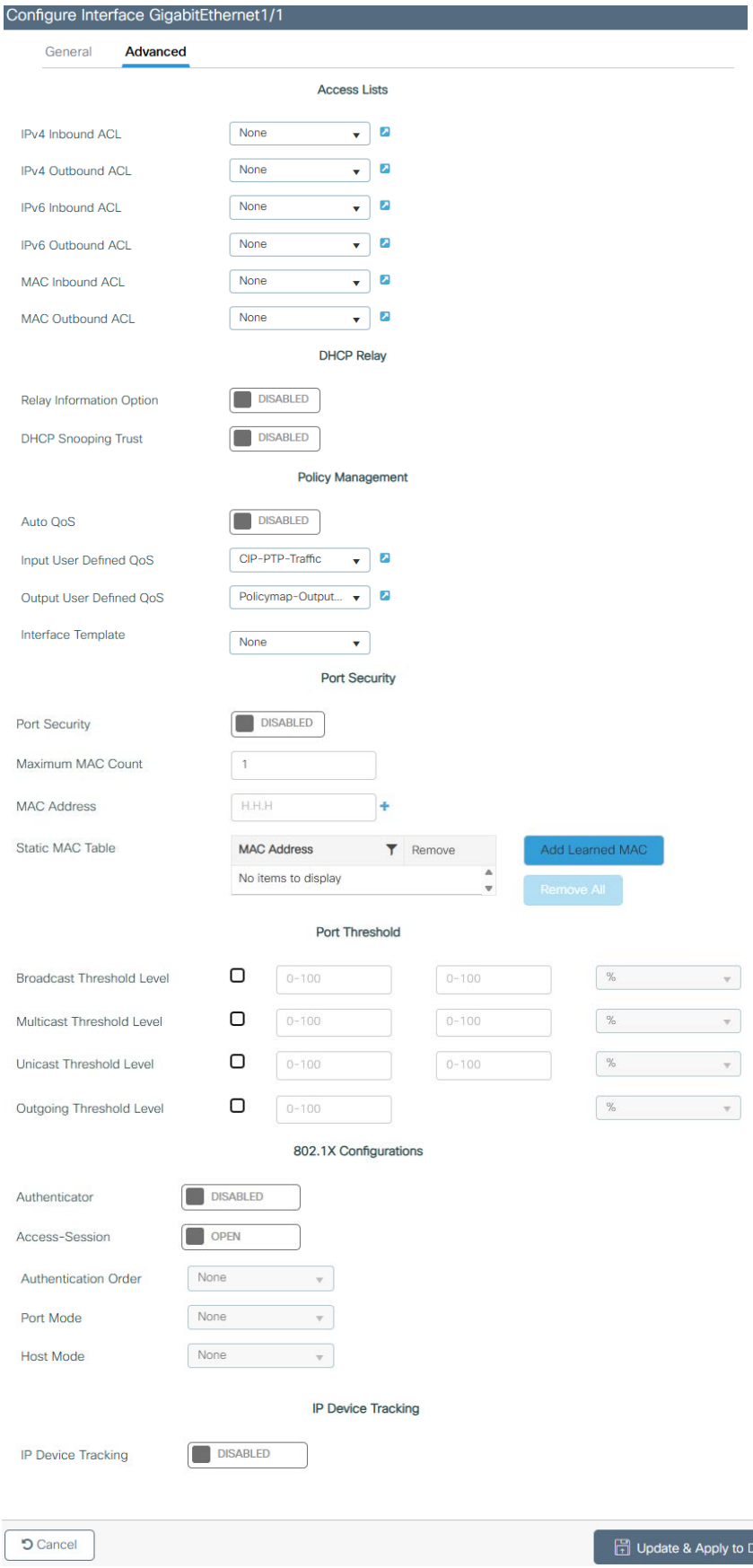
1. In the grid, click the port to configure.
2. On the General tab, complete the fields as described in Table 44 on page 94.

Figure 25 - Configure Interface General



3. On the Advanced tab, complete the fields as described in Table 45 on page 95.

Figure 26 - Configure Interface Advanced



4. Click Update & Apply to Device.

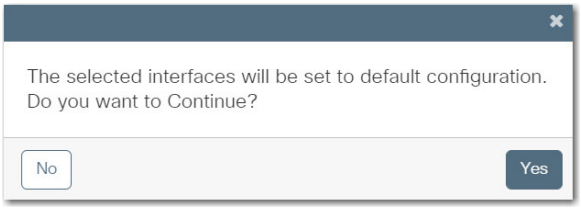
Configure Multiple Ports Simultaneously

WARNING: Multiport configuration resets the current settings for the selected ports to the default settings. You must reconfigure all settings for the selected ports. Upon completion, the selected ports configurations are identical.

1. In the grid, click the checkbox next to each port to configure.
2. Click Multi Port Configuration.

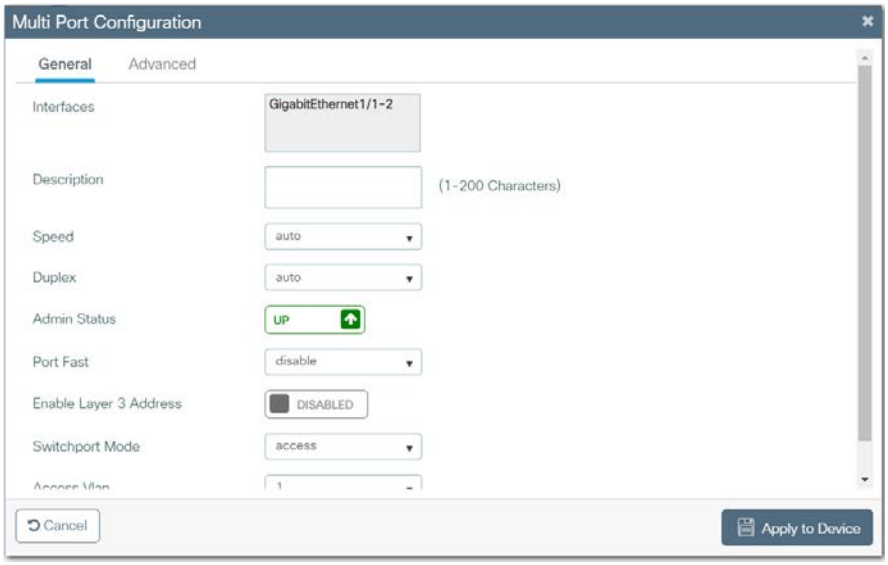


A warning appears.

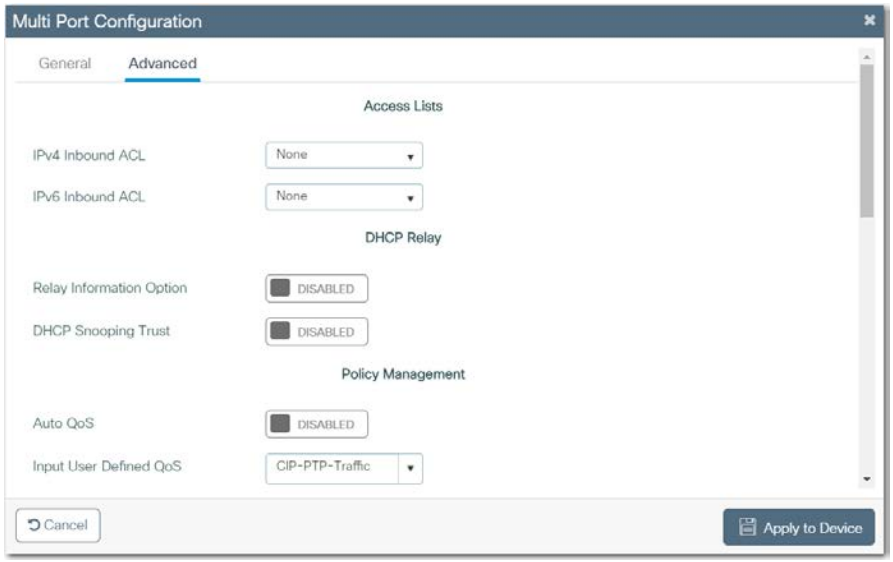


3. To reset the current settings for the selected ports and proceed with the reconfiguration of the selected ports, click Yes.

4. On the General tab, complete the fields as described in Table 44.



5. On the Advanced tab, complete the fields as described in Table 45.



6. Click Apply to Device.

Table 44 - Configure Interface—General Tab

Field	Description
Interface	Displays the port types and numbers.
Description	Enter a description for the interface. We recommend that you provide a port description to help identify the port during monitoring and troubleshooting. The description can be the location of the connected device or the name of the person using the connected device.
Speed	Choose the operating speed of the switch port in Mbps: • 10 • 100 • 1000 • auto If the connected device can negotiate the link speed with the switch port, choose auto (autonegotiation). The default speed is auto. We recommend that you use autonegotiation 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.
Duplex	Choose the duplex mode of the switch port: • full— (Full-duplex mode). Both devices can send and receive data simultaneously. • half— (Half-duplex mode). The connected device must alternate sending or receiving data. • auto—(Autonegotiation). The connected device can negotiate the duplex mode with the switch. Default value: auto We recommend that you use autonegotiation 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.
Admin Status	Click to enable or disable the operational status of the interface: • Up—The interface is operational. • Down—The interface is not operational. Default value: Up
Port Fast	Choose whether to enable PortFast on the port: • disable—Does not enable PortFast. • access—Enables PortFast when the port is operating as an access port. • trunk—Enables PortFast when the port is operating as a trunk port. Devices that connect to ports that are enabled for PortFast can connect to the network immediately. Otherwise, the devices wait for the port to transition from the listening and learning states to the forwarding state. If the switch port connects to endpoints (for example, to computers and not to other switches or routers), enable PortFast on the port.
BPDU Guard	BPDU guard prevents loops by moving a nontrunking port into an err-disable state when a BPDU is received on that port.
BPDU Filtering	BPDU filtering allows you to avoid transmitting BPDUs on PortFast-enabled ports that are connected to an end system.
UDLD-Aggressive Mode	Detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected ports on fiber-optic links.
Media Type (Stratix 5200 Switch Only)	(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 the 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
Enable Layer 3 Address (Stratix 5800 Switch Only)	Click to enable or disable Layer 3 functionality on the port. When enabled, this elevates the interface from a switch port (Layer 2) to a routed port (Layer 3). Default value: Disabled
IP Options (Stratix 5800 Switch Only)	(Appears when a Layer 3 address is enabled.) Choose one of the following IP address types: • IPV4 • IPV6

Table 44 - Configure Interface—General Tab (Continued)

Field	Description
Switchport Mode	Choose one of the following administrative port modes: • access—The port operates permanently as an access port and negotiates to convert a neighbor port into an access port even if the neighbor 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. • trunk—The port operates permanently as a trunk port and negotiates to convert a neighbor port into a trunk port even if the neighbor port is not a trunk port. If you choose Trunk mode, be sure to also choose a native VLAN and allowed VLANs. • dynamic auto—The port converts to a trunk port if the neighbor port is set to Trunk mode or Dynamic Desirable mode. If you choose Dynamic Auto mode, be sure to also specify these VLANs: – Choose an access VLAN to use when the port is in Access mode. – Choose a native VLAN and allowed VLANs to use when the port is in Trunk mode. • dynamic desirable—If the neighbor port is set to Trunk, Dynamic Desirable, or Auto mode, the port converts to a trunk port. If you choose Dynamic Desirable mode, be sure to also specify these VLANs: – Choose an access VLAN to use when the port is in Access mode. – Choose a native VLAN and allowed VLANs to use when the port is in Trunk mode. Default value: dynamic auto
Access Vlan	Choose the VLAN to assign to the port when the port operates as an access port. The port carries traffic for only its assigned VLAN.
Allowed Vlan	Click to specify the VLANs to assign to the port when the port operates as a trunk port: • All— The port carries traffic for all available VLANs. • Vlan IDs—The port carries traffic for only the VLANs you specify.
VLAN IDs	(Appears only when you click VLAN IDs in the Allowed VLAN field). Enter the VLAN IDs to allow on the port. You can enter a series of IDs or a range of IDs, such as 2, 4, 6-10.
Native Vlan	Choose the VLAN to transport untagged packets on the switch when the port operates as a trunk port.

Table 45 - Configure Interface—Advanced Tab

Field	Description
Access Lists	
IPv4 Inbound ACL	Choose the inbound IPv4 access control list (ACL) to apply to ingress traffic on the port.
IPv6 Inbound ACL	Choose the inbound IPv6 access control list (ACL) to apply to ingress traffic on the port.
IPv4 Outbound ACL	Choose the outbound IPv4 access control list (ACL) to apply to egress traffic on the port.
IPv6 Outbound ACL	Choose the outbound IPv6 access control list (ACL) to apply to egress traffic on the port.
MAC Inbound ACL	Choose the inbound MAC address access control list (ACL) to apply to ingress traffic on the port.
MAC Outbound ACL	Choose the outbound MAC address access control list (ACL) to apply to ingress traffic on the port.
DHCP Relay	
Relay Information	Click to enable or disable a DHCP server from forwarding relay information. Default value: Disabled
DHCP Snooping Trust	Click to enable or disable DHCP snooping. DHCP snooping configures the port as a trusted source of DHCP messages. Default value: Disabled
Policy Management	
Auto QoS	Click to enable or disable Auto QoS on the port. Auto QoS deploys QoS features by determining the network design and enabling the configurations that allow the switch to prioritize different traffic flows. Default value: Disabled
Input User Defined QoS	Choose an QoS policy for ingress traffic on the port.
Output User Defined	Choose an QoS policy for egress traffic on the port.
Interface Template	Choose a QoS template for the port.
Port Security (This section is not included in the Multi Port Configuration page.)	
Port Security	Click to enable or disable port security. Port security restricts access to a port. A security violation occurs in the following scenarios: • When a device with a MAC address that differs from any identified, secure MAC address attempts to access the switch port • When the number of MAC addresses on a port exceeds the maximum number that is allowed on that port. MAC addresses for allowed devices are manually configured or learned by the switch. Default value: Disabled
Maximum MAC Count	Enter the maximum number of static MAC addresses to allow on the port.
MAC Address	To add the MAC address of a device that is not currently connected to the Static MAC Table, enter the address in the MAC Address field and click +.
Static MAC Table	To remove a MAC address from the Static MAC Table, click the x in the table row for that MAC address. To add the MAC addresses of all devices that are connected to this port to the Static MAC Table, click Add Learned MAC.
Port Threshold	

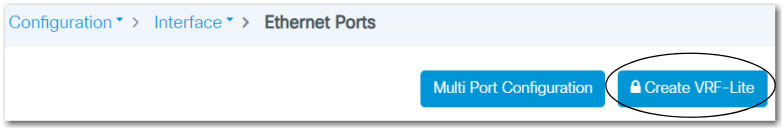
Table 45 - Configure Interface—Advanced Tab (Continued)

Field	Description
Broadcast Threshold Level	To enable broadcast storm control on the port, check Broadcast Threshold Level. Choose one of the following units, and then type values in each of the two fields in the correct range: • % (0...100) • bps (bits per second, 0...10 billion) • pps (packets per second, 0...10 billion) When the threshold value is reached, the port blocks traffic until the traffic rate drops below the threshold.
Multicast Threshold Level	To enable multicast storm control on the port, check Multicast Threshold Level. Choose one of the following units, and then type values in each of the two fields in the correct range: • % (0...100) • bps (bits per second, 0...10 billion) • pps (packets per second, 0...10 billion) When the threshold value is reached, the port blocks traffic until the traffic rate drops below the threshold.
Unicast Threshold Level	To enable unicast storm control on the port, check Unicast Threshold Level. Choose one of the following units, and then type values in each of the two fields in the correct range: • % (0...100) • bps (bits per second, 0...10 billion) • pps (packets per second, 0...10 billion) When the threshold value is reached, the port blocks traffic until the traffic rate drops below the threshold. By default, unicast storm control is disabled.
Outgoing Threshold Level	To enable outgoing thresholds on the port, check Outgoing Threshold Level. Enter a percentage value in the range of 0...100.
802.1x Configurations	
Authenticator	Click to enable or disable Authenticator on 802.1x configurations.
Access-Session	Click to open or close Access-Session on the 802.1x configurations. The default is Open when the Authenticator setting is disabled, and Closed when enabled.
Authentication Order	Choose an Authentication Order for the 802.1x configuration on the port. • None • dot1x • Mab • dot1x->Mab • Mab->dot1x dot1x is the default when the Authenticator setting is enabled.
Port Mode	Choose a Port Mode for the 802.1x configuration on the port. • None • Auto • Force Authorized • Force UnAuthorized Force Authorized is the default when the Authenticator setting is enabled.
Host Mode	Choose a Host Mode for the 802.1x configuration on the port. • None • Single Host • Multiple Host • Multiple Domain • Multiple Authentication Multiple Authentication is the default when the Authenticator setting is enabled.
IP Device Tracking	
IP Device Tracking	Click to enable or disable IP device tracking on the port. IP device tracking maintains a list of devices that are connected to the port via an IP address.

Configure VRF-Lite (Stratix 5800 Switch Only)

Virtual Routing and Forwarding (VRF) is a feature that supports two or more Virtual Private networks (VPNs), where IP addresses can be overlapped among the VPNs. VRF-lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF.

1. On the Ethernet Ports page, click Create VRF-Lite.



2. On the Create VRF Lite page, complete the fields as described in Table 46, and click Apply to Device.

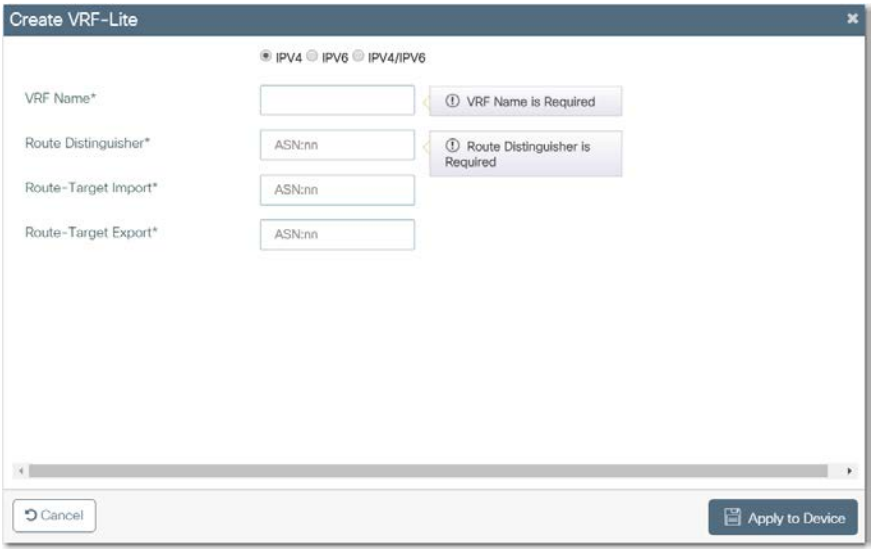


Table 46 - Create VRF-Lite Fields

Field	Description
IPV4, IPV6, IPV4/IPV6	Click the address type.
VRF Name	Enter a name for the VRF.
Route Distinguisher	Create a VRF table by specifying a route distinguisher. Enter either an Autonomous System (AS) number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y).
Route-Target Import	Create a list of import route target communities for the VRF. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y).
Route-Target Export	Create a list of export route target communities for the VRF. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y).

Configure Ethernet Ports via the Logix Designer Application

1. In the navigation pane, click Port Configuration.
2. Complete the fields as described in Table 47, and then click Set.

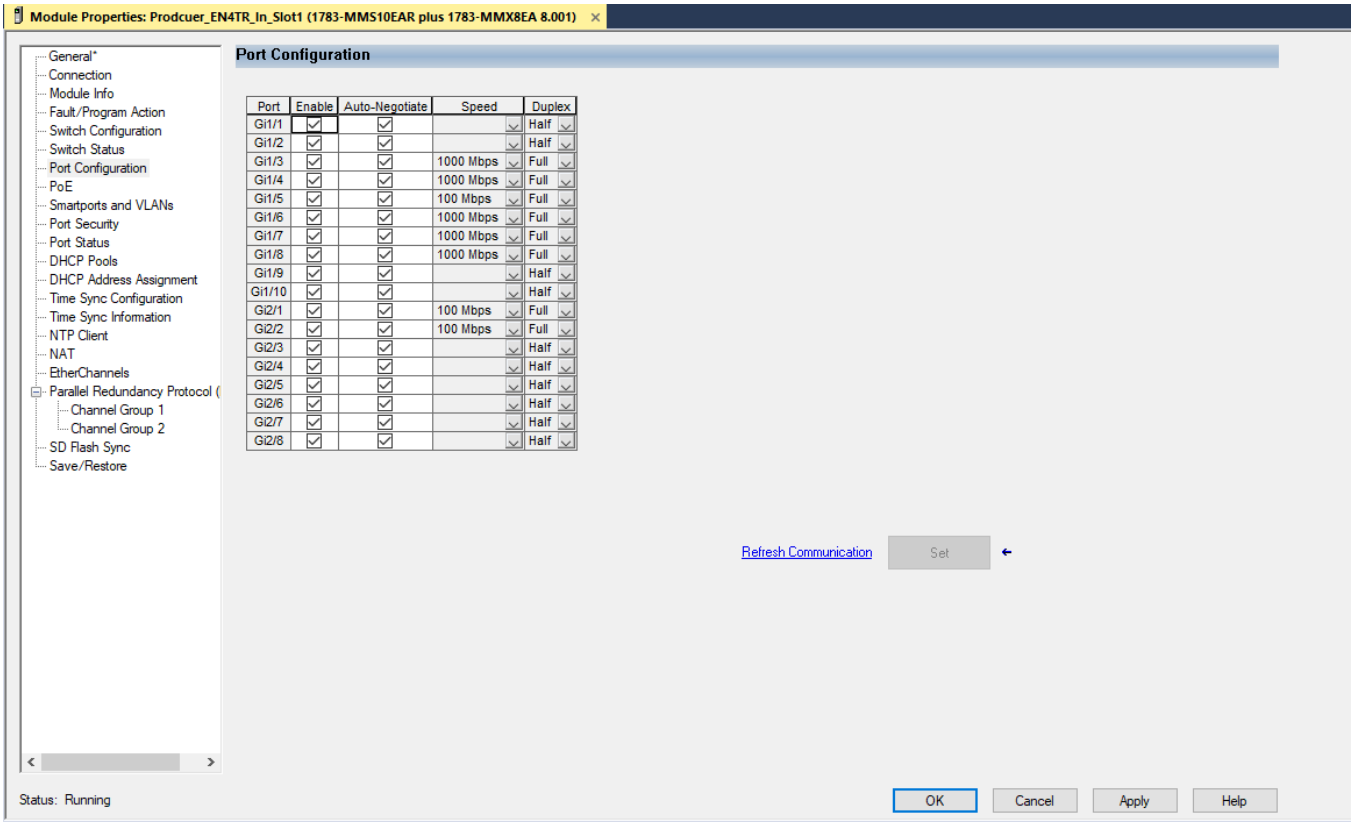


Table 47 - Port Configuration

Field	Description
Port	The port that is selected for configuration.
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.
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: • 10 Mbps • 100 Mbps • 1 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.

Configure 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

1. In the navigation pane, click Fault/Program Action.
2. Complete the fields as described in Table 48, and then click Apply.

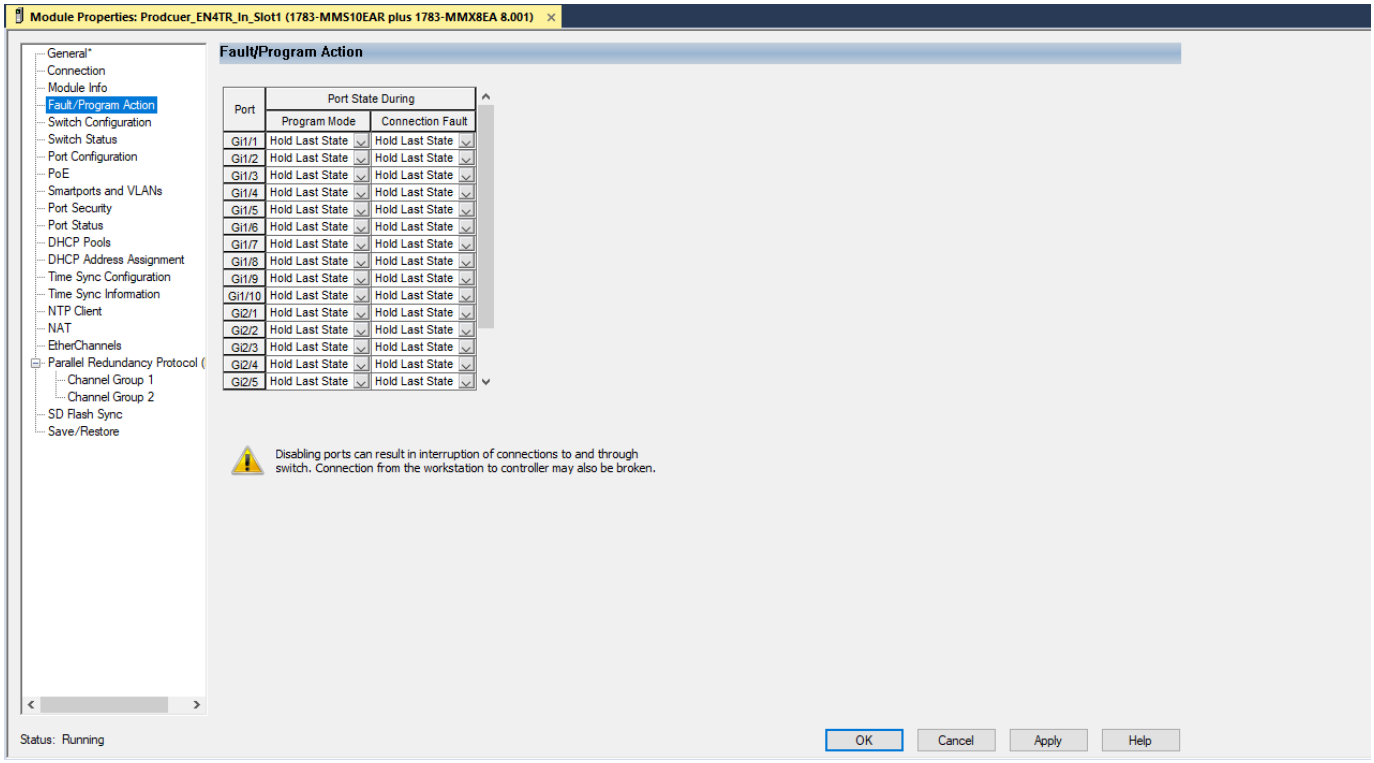


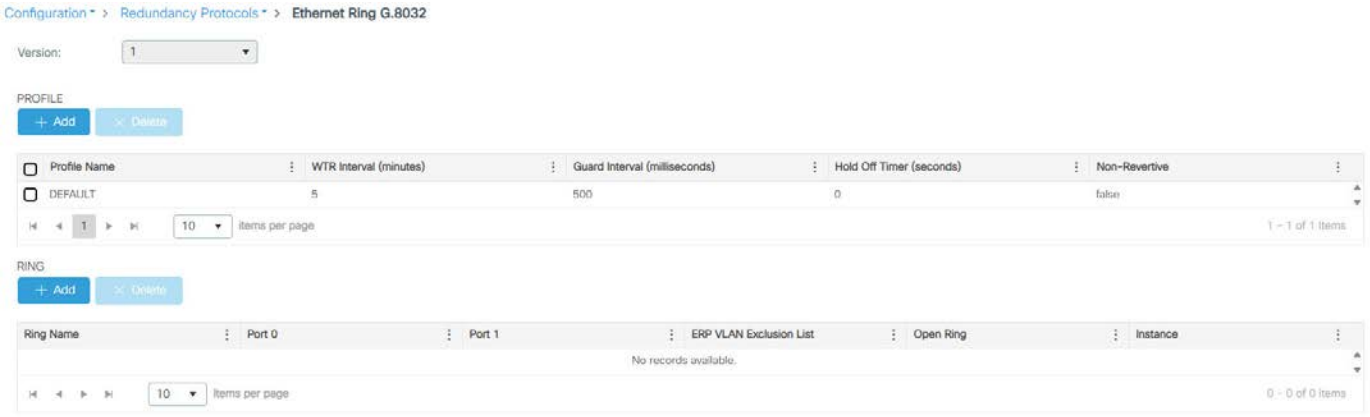
Table 48 - Fault/Program Action

Field	Description
Port	Displays the port type and number.
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. Default value: 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.

Ethernet Ring G.8032 (Stratix 5200 Switch Only)

The G.8032 Ethernet Ring Protocol (ERP) provides protection to Ethernet traffic in a ring topology while ensuring that there are no loops within a ring at the Ethernet layer. Loop formation is prevented by blocking traffic on either a predetermined link, or a failed link.

You can configure the Ethernet Ring G.8032 protocol in the Configuration > Redundancy Protocols > Ethernet Ring G.8032 page.



Add a Profile

In the Profile area, click Add. The following screen appears.

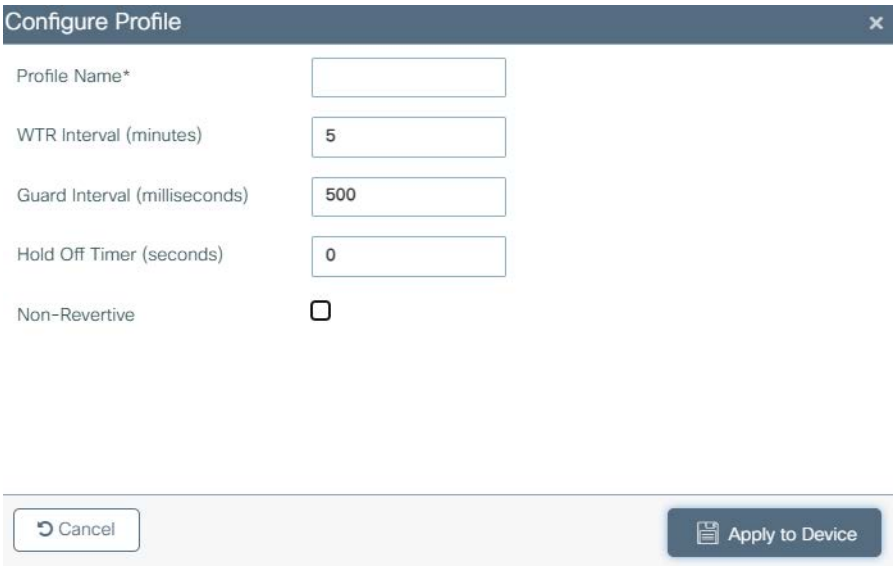


Table 49 - Configure Profile for Ethernet Ring G.8032

Field	Description
Profile Name	Enter a profile name.
WTR Interval (minutes)	The (Wait-to-Restore) WTR interval is used to verify that signal failure is not intermittent
Guard Interval (milliseconds)	Ensures that there are no overlaps in transmissions.
Hold Off Timer (seconds)	Filters out intermittent link faults. Faults are reported only if this timer expires.
Non-Revertive	To enable non-revertive switching, check the Non-Revertive checkbox.

Add a Ring

In the Ring area, click Add. The following screen appears.

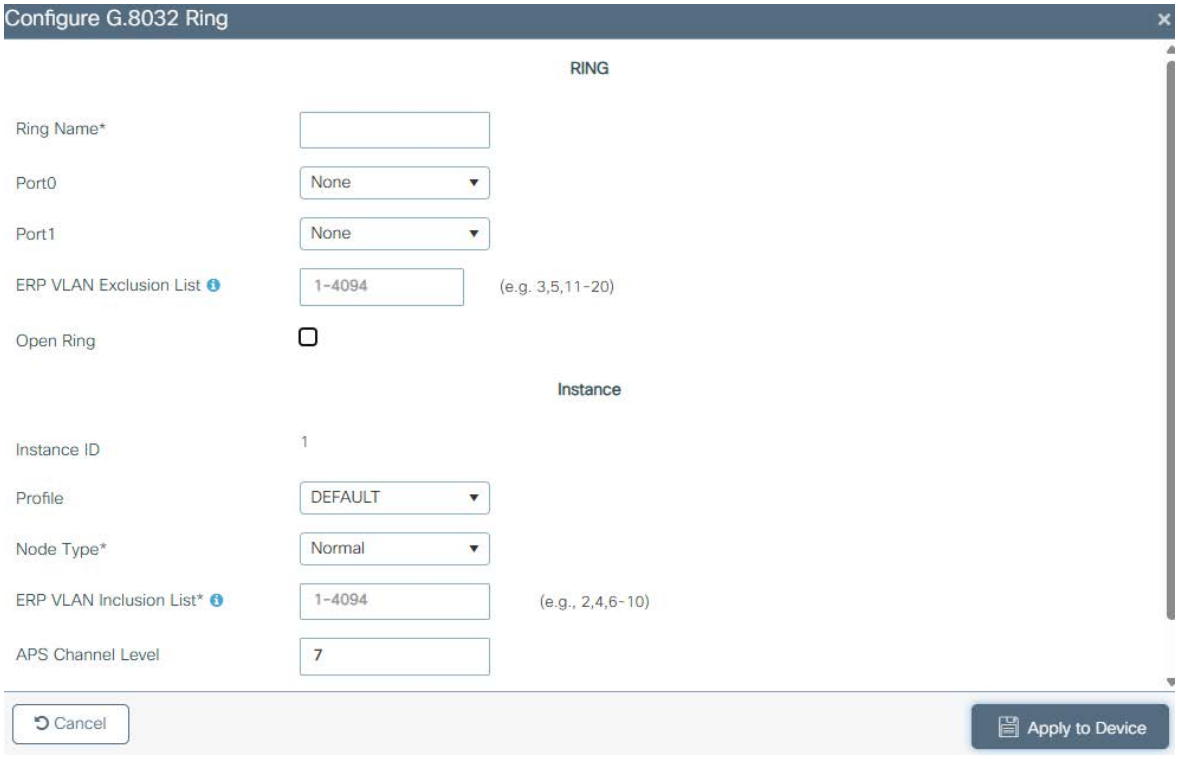


Table 50 - Configure Ring for Ethernet Ring G.8032

Field	Description
RING	
Ring Name	Enter a ring name.
Port0	From the drop-down menu, choose an interface for Port 0 and Port 1. This allows you to choose if all VLANs are allowed on the switchport, or configure specific allowed VLANs.
Port1	
ERP VLAN Exclusion List(1)	Define an ERP VLAN exclusion list.
Open Ring	To configure an open ring, check the Open Ring checkbox.
INSTANCE	
Instance ID	
Profile	Choose the profile to apply the ring to.
Node Type	Choose a node type.
ERP VLAN Inclusion List(2)	Define an ERP VLAN inclusion list. The inclusion list must be a subset of the switchport-allowed VLANs on Port 0 or Port 1.
APS Channel Level	Enter an APS channel level, and the APS channel control VLAN.
APS Channel Control VLAN	Enter an APS channel level, and the APS channel control VLAN.

(1) The VLAN ID list is not protected by ERP.

(2) The VLAN ID list is protected by ERP.

Edit or Delete Profile Rings

To edit a profile or a link use the following steps.

1. Check the check-box for the required entry from the displayed list.
2. Click Edit.

   A slide-in pane displays the configured information for you to edit.
3. After you make your edits, click Update and Apply to Device.
4. To delete a profile or a link, check the checkbox for the required entry and click Delete.

Flow-based SPAN (FSPAN)

FSPAN is used to mirror traffic based on filter criteria. FSPAN supports three types of access control lists (ACLs) to the SPAN session and filtering based on VLAN.

You can control the type of network traffic to be monitored in SPAN or RSPAN sessions by using flow-based SPAN (FSPAN) or flow-based RSPAN (FRSPAN), which apply ACLs to the monitored traffic on the source ports. The FSPAN ACLs can be configured to filter IPv4, IPv6, and VLAN monitored traffic. You can use SPAN for troubleshooting connectivity issues and calculating network utilization and performance.

Configure FSPAN via the WebUI

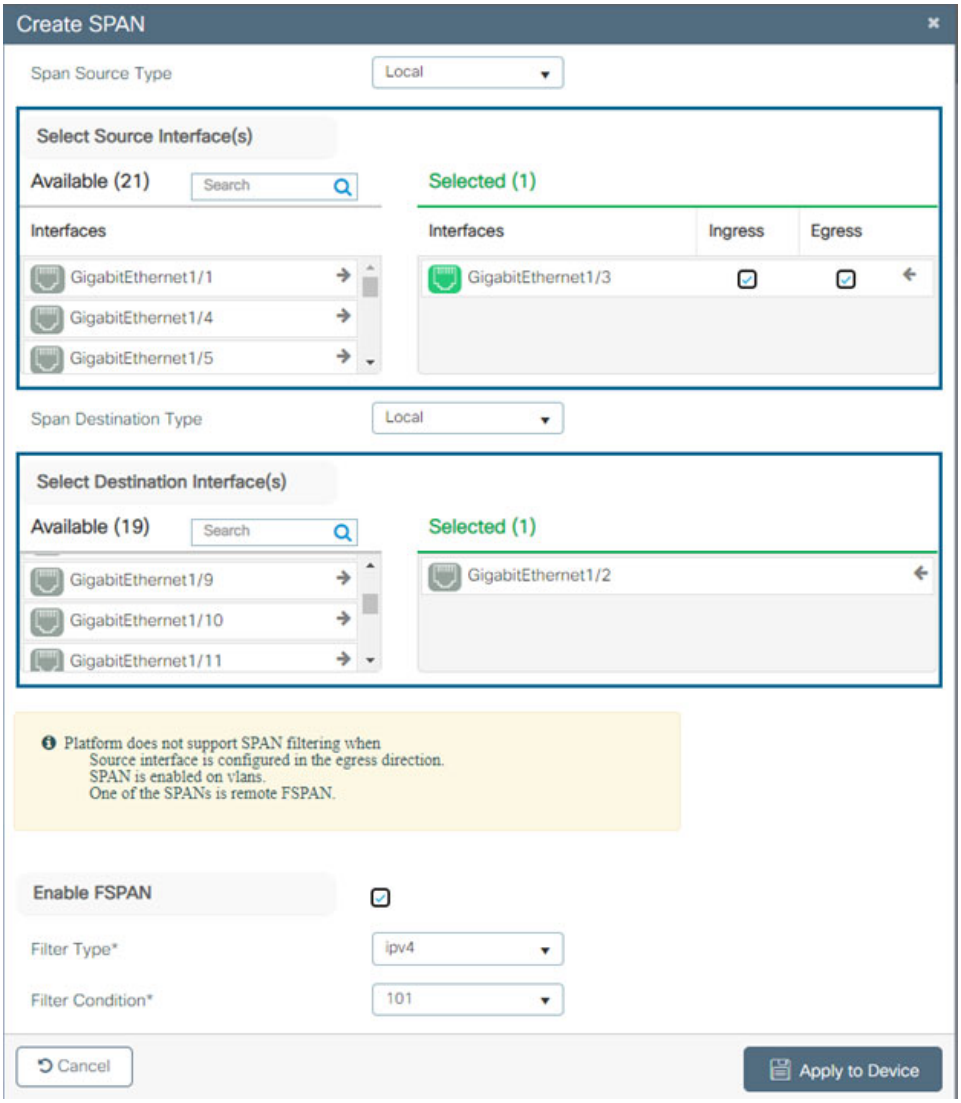
From the Configuration Menu, choose SPAN.



To configure FSPAN, use the following steps:

1. Select one or more source interfaces from the list of available interfaces on the left and click the arrow to add them to the Selected list on the right.
2. Check or uncheck the Ingress checkboxes to specify the direction of source packets to be monitored.
3. Select Enable FSPAN for local source, and then select the Filter Type and Filter Condition from the drop-down lists.

4. When you are finished, Click Apply to Device.



IMPORTANT This platform does not support SPAN filtering when:

- Source interface is configured in the egress direction.
- SPAN is enabled on VLANs.
- One of the SPANs is remote FSPAN.

Logical Interfaces

A logical interface is a virtual interface, rather than a physical interface You can configure these logical interfaces on the switch:

- Port channels, also known as EtherChannels
- Loopback interfaces

Port Channels or EtherChannels

A port channel, or EtherChannel, is a group of switch ports that are bundled into one logical link to create a higher bandwidth between two switches. For example, four switch ports that are all configured to operate at 100 Mbps can be assigned to an EtherChannel to provide full-duplex bandwidth of up to 400 Mbps. If one of the ports in the EtherChannel becomes unavailable, traffic is carried over the remaining ports within the EtherChannel. For more information about port channels, see the Ethernet Reference Manual, publication ENET-RM002.

EtherChannel Modes

In the Logix Designer application, you can assign the EtherChannel modes as described in Table 51.

Table 51 - 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.
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.

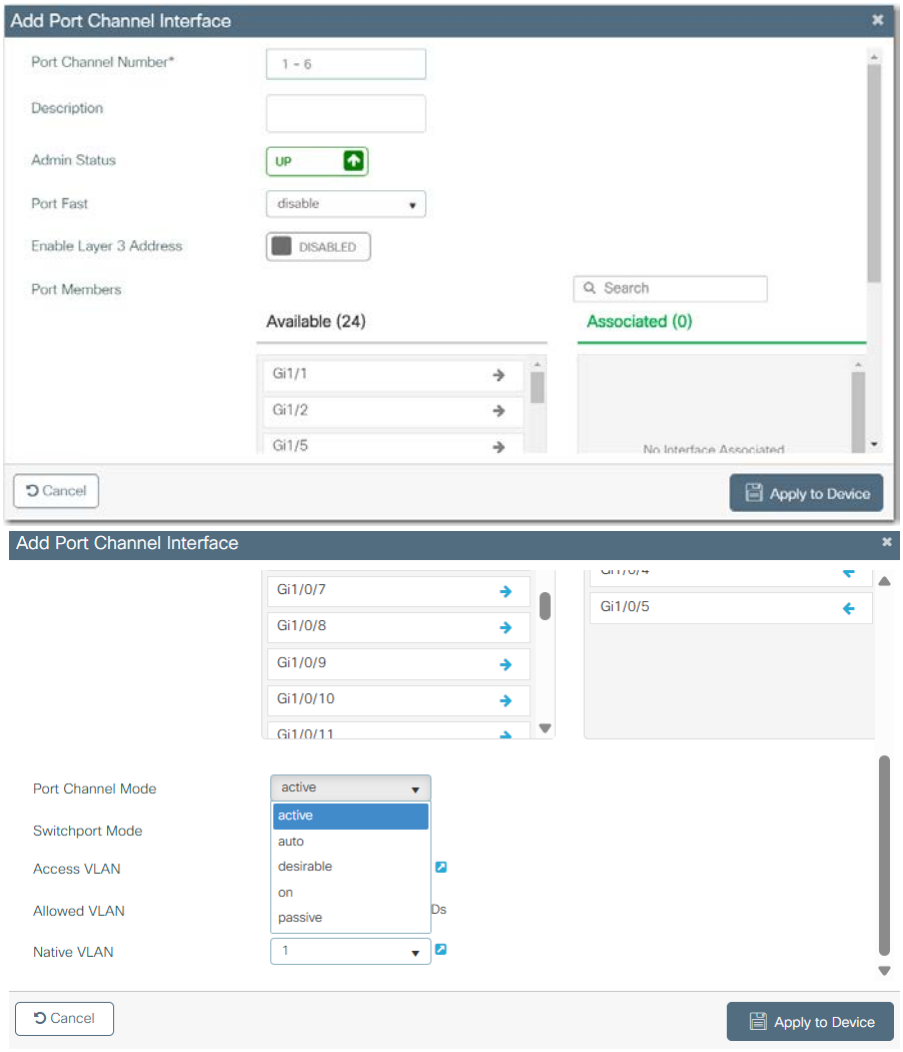
Configure Port Channels

From the Port Channels tab, you can add, edit, and delete port channels.

- To add a port channel, click Add, complete the fields as described in Table 53, and then click Apply to Device.
- To edit a port channel, check the checkbox for the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a port channel, check its associated checkbox in the grid, and then click Delete.

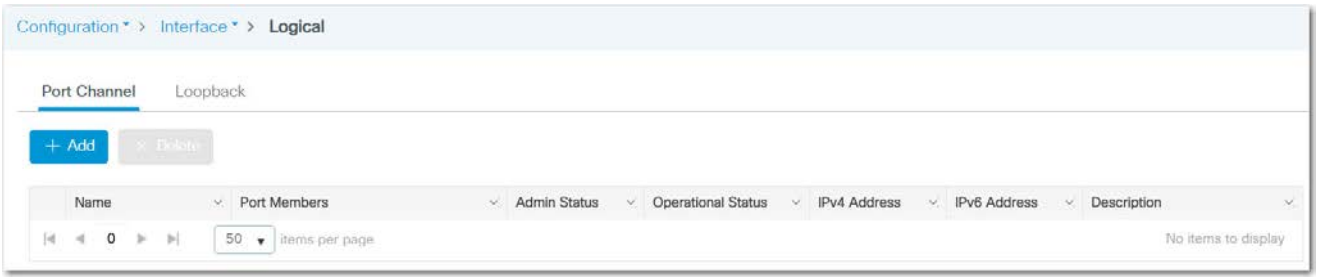
Table 52 - Port Channel Modes

Port Channel Mode	Descriptions
Active (Recommended)	Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.
Auto	Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation.
Desirable	Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.
On	Forces the port to channel without PAgP or LACP. In the on mode, an EtherChannel exists only when a port group in the on mode is connected to another port group in the on mode.
Passive	Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.



Configure Logical Interfaces via the WebUI

From the Configure menu, choose Logical.



From the Logical page, you can configure logical interfaces. Logical interfaces include port channels and loopback interfaces:

- To configure port channels, see the following instructions.
- To configure loopback interfaces, see page 108.

Table 53 - Add Port Channel Interface

Field	Description
Port Channel Number	Enter a number to identify the port channel. Valid values: 1...6
Description	Enter a description for the port channel.
Admin Status	Click to enable or disable the operational status of the interface: • Up—The interface is operational. • Down—The interface is not operational. Default value: Up
PortFast	Choose whether to enable PortFast on the port channel: • disable—Does not enable PortFast. • access—Enables PortFast when the port channel is operating as an access interface. • trunk—Enables PortFast when the port channel is operating as a trunk interface. Devices that connect to port channels that are enabled for PortFast can connect to the network immediately. Otherwise, the devices wait for the interface to transition from the listening and learning states to the forwarding state. If the port channel connects to endpoints (for example, to computers and not to other switches or routers), enable PortFast on the port channel.
Enable Layer 3 Address (Stratix 5800 Switch Only)	Click to enable or disable Layer 3 functionality on the port. When enabled, this elevates the interface from a switch port (Layer 2) to a routed port (Layer 3). Default value: Disabled
Port Members	In the Available list, click to move interfaces to the Associated list and make them members of the port channel.
Switchport Mode	• Access - Layer 2 Access • Trunk - Layer 2 Trunk Mode
Access VLAN	Select the VLAN that the interface belongs to and carries traffic for. For Trunk mode, select the list of allowed VLANs that transmit traffic from this interface in tagged format. Also in trunk mode, select the VLAN that is sending and receiving untagged traffic on the trunk port.
Allowed VLAN	Click to specify the VLANs to assign to the port when the port operates as a trunk port: • All— The port carries traffic for all available VLANs. • Vlan IDs—The port carries traffic for only the VLANs you specify.
Native VLAN	Choose the VLAN to transport untagged packets on the switch when the port operates as a trunk port.

Loopback Interfaces

A loopback interface is a virtual interface that remains in an up (operational) state. A loopback interface can provide a stable interface on which you can assign a Layer 3 address. This address can be configured as the source address when the networking device must send data for protocols, such as Cisco Discovery Protocol (CDP), to another device in your network and you always want the receiving device to see the same source IP address from the networking device. This is an issue in networks with multiple equal-cost paths because of the following:

- Under normal circumstances the packets that are generated by a networking device use the IP address from the outbound interface as the source address for the packets
- From the networking device to the receiving host, each packet can use another outbound interface.

Configure Loopback Interfaces

From the Loopback tab, you can add, edit, and delete loopback interfaces:

- To add a loopback interface, click Add, complete the fields as described in Table 54, and then click Apply to Device.
- To edit a loopback interface, click the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a loopback interface, check its associated checkbox in the grid, and then click Delete.

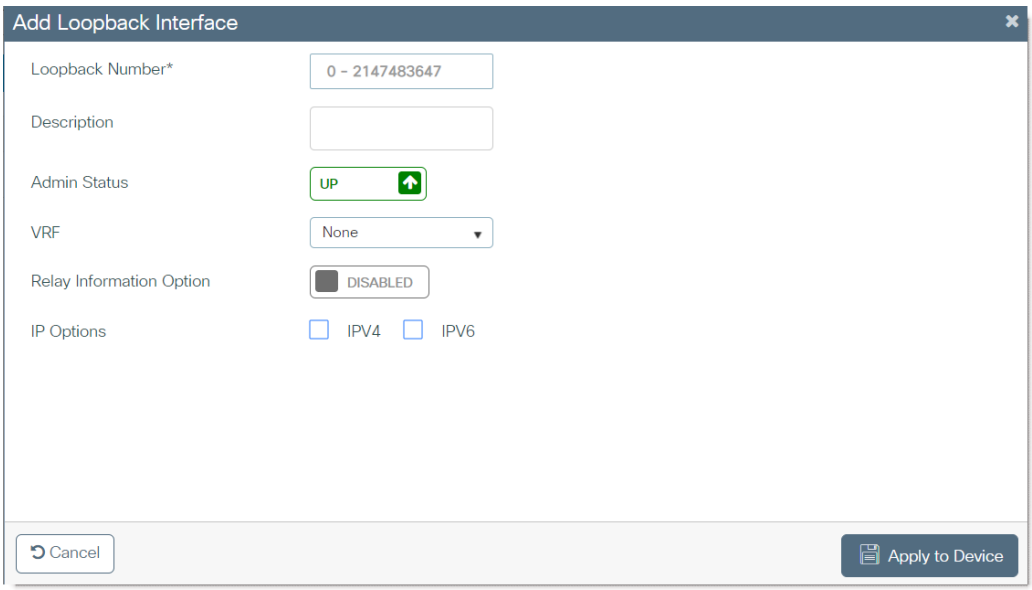
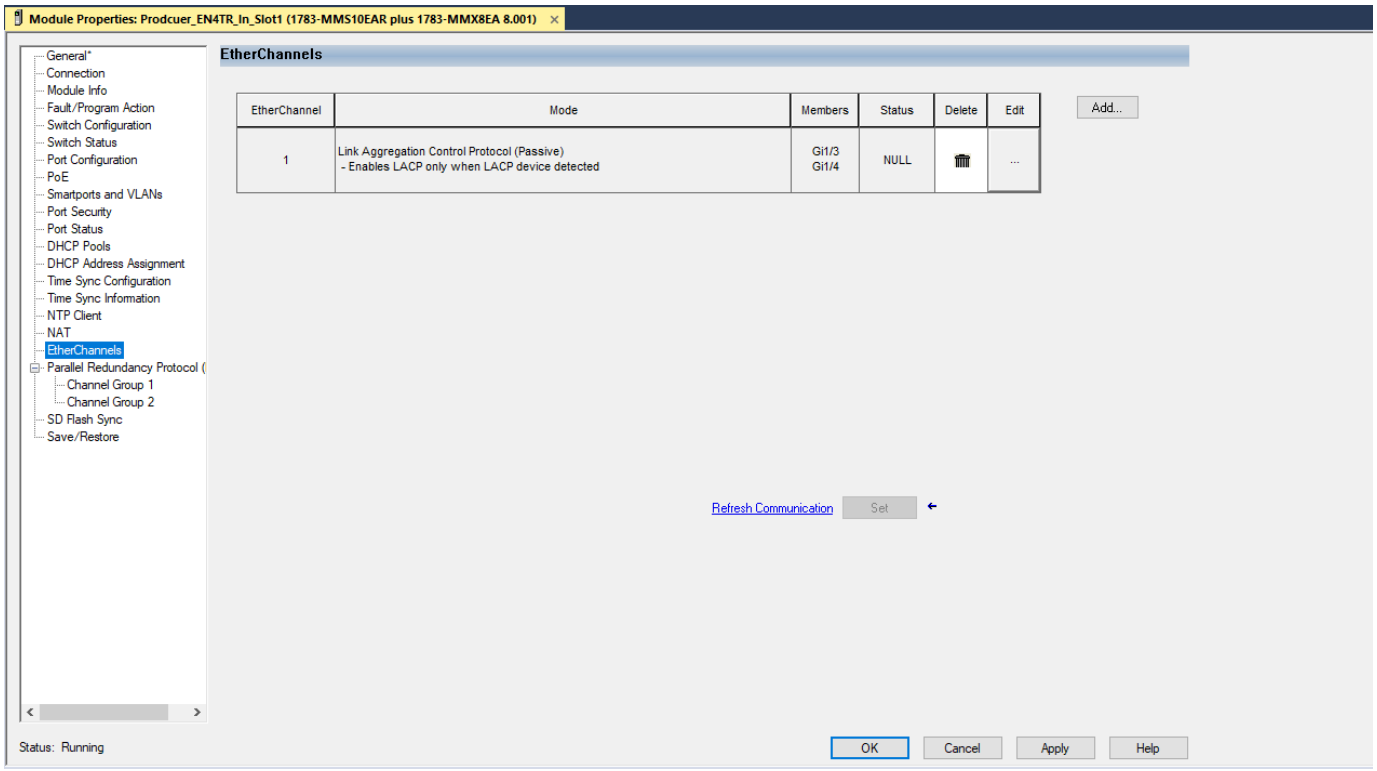


Table 54 - Add Loopback Interface

Field	Description
Loopback Number	Enter a number to identify the loopback interface. Valid values: 0...2147483647
Description	Enter a description for the loopback interface.
Admin Status	Click to enable or disable the operational status of the interface: • Up—The interface is operational. • Down—The interface is not operational. Default value: Up
VRF (Stratix 5800 Switch Only)	Choose a Virtual Routing and Forwarding (VRF) instance to assign to the loopback interface.
Relay Information	Click to enable or disable a DHCP server from forwarding relay information. Default value: Disabled
IP Options	To configure an IPv4 interface, check IPV4, and then specify the IPv4 address information. To configure an IPv6 interface, check IPV6, and then specify the IPv6 address information.

Configure EtherChannels via the Logix Designer Application

In the navigation pane, click EtherChannels.



On the EtherChannels view, you can add, edit, and delete EtherChannels:

- To add an EtherChannel, click Add, complete the fields as described in Table 55, click Set, and then click Close.
- To edit an EtherChannel, click the Ellipses icon in the Edit column, modify the fields, click Set, and then click Close.
- To delete an EtherChannel, click the Trash icon in the Delete column.

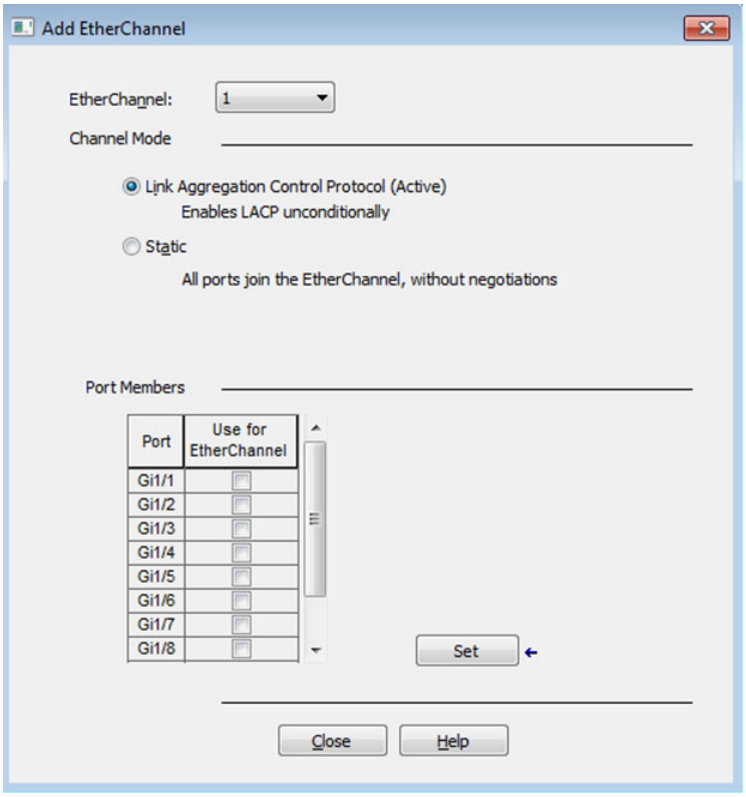


Table 55 - Add EtherChannel

Field	Description
EtherChannel	Choose a number to identify the EtherChannel.
Channel Mode	Choose a mode to determine how ports become active. With Link Aggregation Control Protocol, 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. For a description of each mode, see Table 51 on page 105.
Port Members	To make a port a member of this EtherChannel, check its associated checkbox in the grid.

High-availability Seamless Redundancy (HSR) (Stratix 5800 Switch Only)

High-availability Seamless Redundancy (HSR) is similar to Parallel Redundancy Protocol (PRP), but is designed to work in a ring topology. Instead of two parallel independent networks of any topology (LAN-A and LAN-B), HSR defines a ring with traffic in opposite directions. Port-A sends traffic counter clockwise in the ring, and Port-B sends traffic clockwise.



The HSR feature is only available on hardware systems that support advanced features.

The HSR packet format is also different from PRP. To allow the switch to determine and discard duplicate packets, additional protocol-specific information is sent with the data frame.

For PRP, this information is sent as part of a trailer called the redundancy control trailer (RCT), whereas for HSR this is sent as part of the header called the HSR header. Both the RCT and HSR header contain a sequence number, which is the primary data that is used to determine if the received frame is the first instance or a duplicate instance.

The non-switching nodes with two interfaces attached to the HSR ring are Doubly Attached Nodes implementing HSR (DANHs). Singly Attached Nodes (SANs) are attached to the HSR ring through a RedBox. The RedBox acts as a DANH for all traffic that it is the source or destination for. Since the RedBox emulates these as DANH, they are called Virtual Doubly Attached Nodes (VDAN).

The switch implements RedBox functionality using Gigabit Ethernet port connections to the HSR ring. In HSR-SAN mode, the RedBox inserts the HSR tag on behalf of the host and forwards the ring traffic, except for frames that are sent by the node itself, duplicate frames, and frames for which the node is the unique destination.

Add an HSR Ring via the WebUI

From the Configuration tab, you can find the HSR page. You can view, add, edit, and delete an HSR ring.

- Only one HSR instance is supported. The switch supports only one HSR or one PRP instance, so if a PRP instance has been created, you cannot create the HSR instance.
- HSR ring 1 can only be configured as a pair of ports: G1/1 and G1/2 or G1/3 and G1/4. Using these port pairs, you can configure one HSR ring.

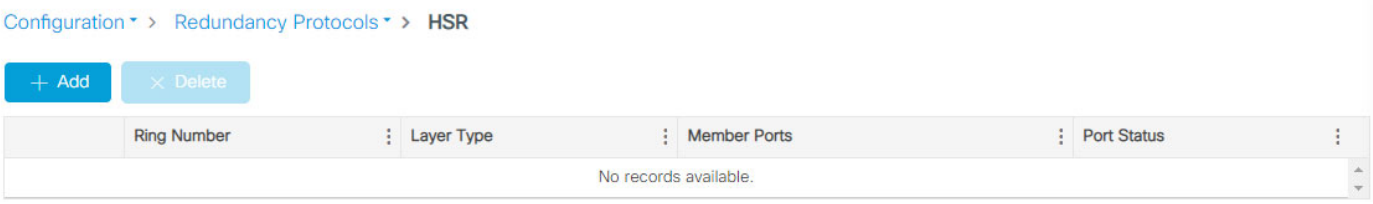


Table 56 - HSR

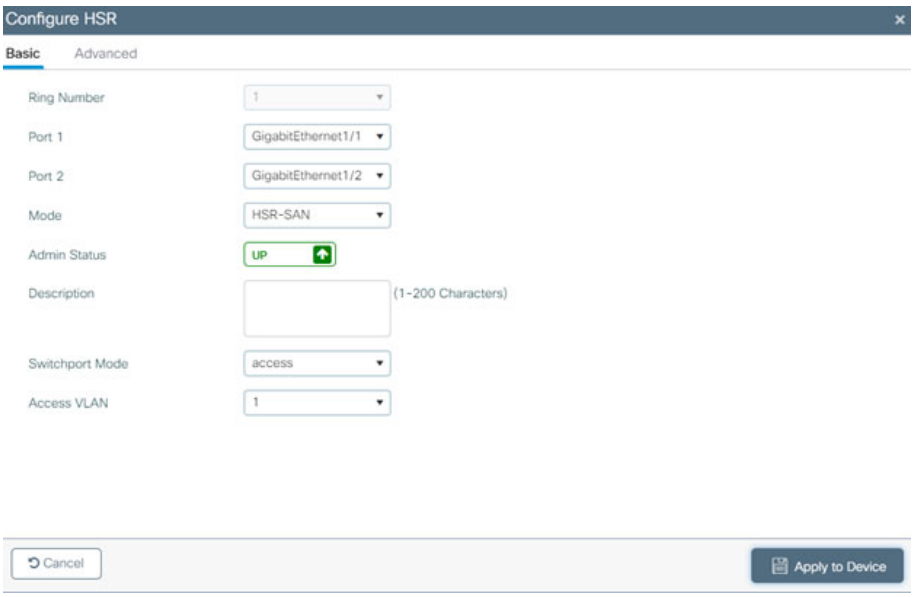
Parameter	Description
Ring Number	1
Layer Type	Network type of the ports in the HSR ring - Layer2 or Layer3. Both interfaces within an HSR ring must have the same configuration.
Member Ports	Ports in the HSR ring: • G1/1 and G1/2 or G1/3 and G1/4
Port Status	The status of the group: • InUse • Not-InUse • Not-InUse (Admin Down)

Table 57 displays the following information for a configured HSR ring.

HSR-SAN Mode

In HSR-SAN mode, the RedBox inserts the HSR tag on behalf of the host and forwards the ring traffic, except for frames sent by the node itself, duplicate frames, and frames for which the node is the unique destination.

To add an HSR-SAN ring, click Add on the HSR page.



HSR-PRP Mode

HSR-PRP mode, also called Dual RedBox mode, is used to bridge HSR and PRP networks.

In this mode, two different RedBoxes connect to LAN A and LAN B of the PRP network. Two ports connect to the HSR ring and one port connects to one of the two PRP LANs. The traffic on the upstream interlink port connecting the RedBox to the PRP network is PRP-tagged. In HSR-PRP mode, the RedBox extracts data from the PRP frame and generates the HSR frame using this data, and performs the reverse in the opposite direction.

To add an HSR ring for PRP-LAN-A/B, click Add on the HSR page.

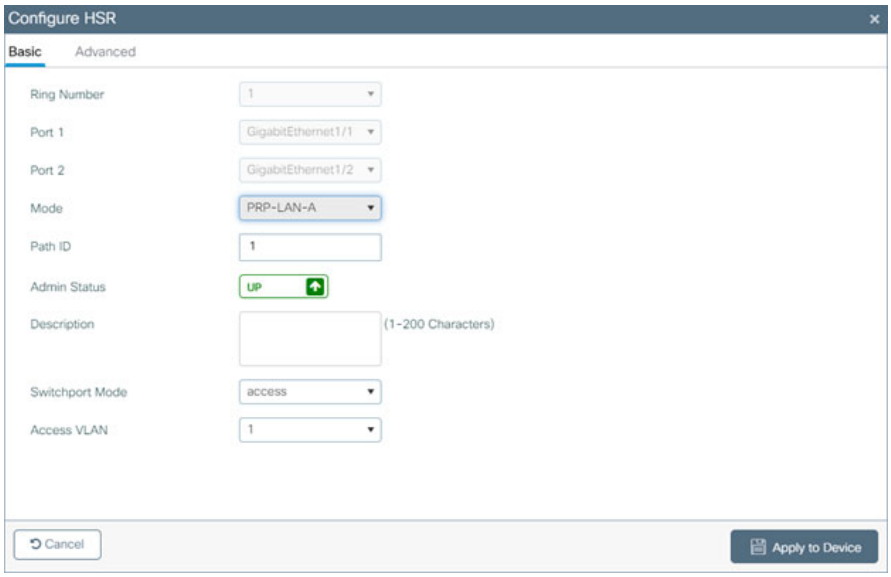


Table 57 - HSR Ring Configuration

Parameter	Description
Ring Number	The ring number that was selected on the Configuration Page. This cannot be changed.
Port 1	GigabitEthernet1/1 or GigabitEthernet1/3
Port 2	GigabitEthernet1/2 or GigabitEthernet1/4
Mode	• HSR-SAN • PRP-LAN-A • PRP-LAN-B
Path ID	The 3-bit NetID (1...6), which identifies a PRP network and the two RedBoxes that connect the PRP network to an HSR ring. Both RedBoxes must have same NetID (Path ID) Default Value: 1
Admin Status	Click the button to change the Admin Status of the ports in the HSR ring to Up or Down. The Admin Status is Up by default.
Description	Optional description entry for the HSR ring.
Switchport Mode	• Access—Layer 2 access mode • Trunk—Layer 2 trunk mode
Access VLAN	For Access mode, select the VLAN that the HSR ring interface belongs to and carries traffic for. For Trunk mode, select the list of allowed VLANs that transmit traffic from this interface in tagged format. Also in trunk mode, select the VLAN that is sending and receiving untagged traffic on the trunk port.

Click Save and Apply to Device.

To delete an existing HSR ring, select that row in the HSR ring table and click Delete.

Edit an HSR Ring Via WebUI

You can only modify the Admin Status and VLANs or IP Assignment Mode for an existing HSR ring. To change the port numbers, you must delete the ring configuration and reconfigure it.

To edit an existing HSR ring configuration, navigate to the HSR page under the Configurations tab and click the row in the HSR ring table to bring up the Configure HSR window.

Click the Admin status button of the ports in the HSR ring to Up or Down. The Admin Status is Up by default. For Access mode, select the VLAN that the HSR ring interface belongs to and carries traffic for.

For Trunk mode, select the list of allowed VLANs that transmit traffic from this interface in tagged format and also select the VLAN that is sending and receiving untagged traffic on the trunk port.

Click Save and Apply to Device.

Configure Advanced HSR Settings via WebUI

To configure additional HSR settings, including Supervision Frame Options, click the Advanced tab. Modify the settings as needed, and then click Save and Apply to Device.

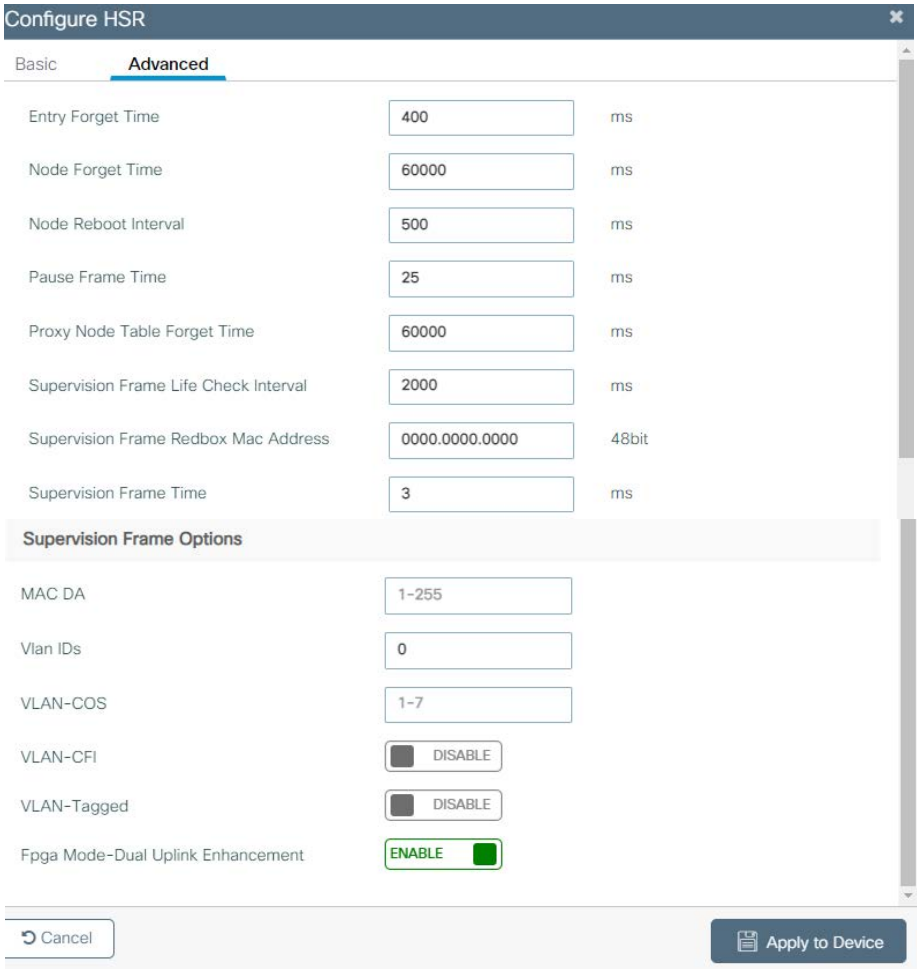


Table 58 - HSR Advanced Ring Configuration

Parameter	Description
Entry Forget Time	Time for clearing the inactive entry from the duplicate discard table. Range: 0...65535 ms. Default: 400 ms.
Node Forget Time	Time to clear an inactive entry from the node table. Range: 0...65535 ms. Default: 60,000 ms.
Node Reboot Time	Time after which the RedBox must start sending supervision frames after bootup. Range: 0...65535 ms. Default: 500 ms.
Pause Frame Time	If there is congestion, the receiving station sends pause requests using pause frames. The pause frame contains the pause time, which is the length of time for which the station that received the pause request is requested to stop transmitting data. Range: 0...65535 ms. Default: 25 ms.
Proxy Node Table Forget Time	Time to clear an inactive entry from the proxy node table or vdan table. Range: 0...65535 ms. Default: 60,000 ms.
Supervision Frame Life Check Interval	Life check interval value for supervision frames. Range: 0...65535 ms. Default: 1600 ms.
Supervision Frame RedBox MAC address	The RedBox MAC address in the supervision frames. Range: 48-bit MAC address. The default is the interface HSR ring MAC address.
Supervision Frame Time	Time interval between supervision frames. Range: 0...65535 ms. Default: 3 ms.
Supervision Frame Options	

Table 58 - HSR Advanced Ring Configuration

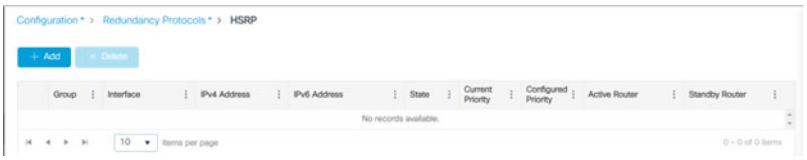
Parameter	Description
MAC DA	The last bytes of the destination MAC address of the supervision frames (01:15:4E:00:01:00). The last 00 is replaced by the value depending on this parameter. Range: 1...255 MAC DA last 8-bits option value. Default: 1.
VLAN IDs	The VLAN tag of supervision frame (valid only if the Supervision Frame VLAN Tag option is Enabled). Range: 0...4095. Default: 0.
VLAN-COS	COS value to be set in the VLAN tag of the Supervision frame (valid only if the Supervision Frame VLAN Tag option is Enabled). Range: 1...7. Default: 1.
VLAN-CFI	Enables CFI value to be set in the VLAN tag of the Supervision frame The settings are either Enabled or Disabled. Default is Disabled.
VLAN-Tagged	Enables the VLAN tagging of supervision frames. The settings are either Enabled or Disabled. Default is Disabled.
Fpga Mode-Dual Uplink Enhancement	Enables HSR dual uplink redundancy handling. This feature allows two separate interfaces to connect upstream from the HSR ring through two separate HSR RedBoxes. This makes sure that there is no single point of failure exiting the HSR ring. Examples of protocols that can leverage this feature to improve high availability include HSRP, VRRP, and REP. The settings are either Enabled or Disabled. Default is Enabled.

Hot Standby Router Protocol (HSRP) (Stratix 5800 Switch Only)

HSRP (Hot Standby Router Protocol) is a redundancy protocol to provide gateway redundancy without any additional configuration on the end devices in the subnet. With HSRP configured between a set of routers (treated as HSRP group or a standby group), they work together to present the appearance of one virtual router to the hosts on the LAN.

Configure HSRP via the WebUI

From the Configuration menu, choose Redundancy Protocols. From there, find the HSRP page and click Add.



From the Redundancy Protocol page, you can find the HSRP page. To configure the HSRP, click Add.

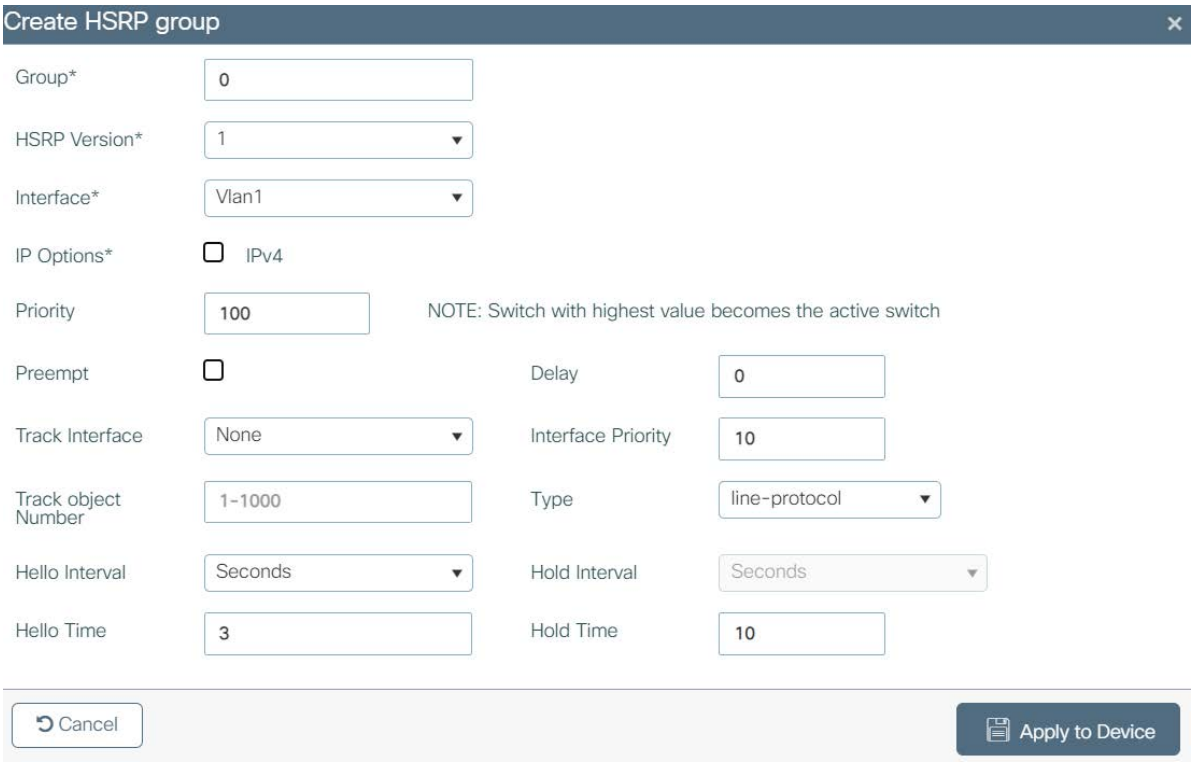


Table 59 - HSRP Configuration Options

Field	Description
Group	0…255
HSRP Version	• v1 (default) • v2
Interface	Layer 3 interface on which to enable HSRP.
IP Options	The IP address of the hot standby router interface and an optional secondary IP address.
Priority(1)	1…255 (default of 100)
Delay	0s…3600 s (default of 0)
Preempt	Choose a value to cause the local router to postpone taking over the active role for the configured number of seconds.
Track Interface(2)	Choose an interface for Track Interface.
Interface Priority	1…255 (default of 10)
Track Object Number	1…1000
Type	• line-protocol • IP routing • ipv6 routing
Hello Time	1…254 s (default of 3) 15…999 ms (default of 15)
Hold Time	4…255 s (default of 10) 50…3000 ms (default of 50)

(1) The switch with the highest value becomes the active switch.

(2) 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.

Intermediate System-to-Intermediate System (IS-IS) (Stratix 5800 Switch Only)

IS-IS is a link-state Interior Gateway Protocol (IGP). Link-state protocols create the information that is required to build a complete network connectivity map on each participating device. That map is then used to calculate the shortest path to destinations. IS-IS provides fast convergence, scalability, and efficient use of network bandwidth.

Network Operation

IS-IS operates by reliably flooding link state information throughout a network of routers. Each IS-IS router independently builds a database of the network topology to aggregate the flooded network information. Like the Open Shortest Path First (OSPF) protocol, IS-IS uses an algorithm for computing the best path through the network. Packets (datagra10 ms) are then forwarded based on the computed ideal path through the network to the destination.

Unlike other IP routing protocols, IS-IS runs directly on the datalink layer (Layer 2). On Stratix 5800 switches, IS-IS supports route redistribution and load balancing.

To configure ISIS, you create an ISIS route and associate an interface.

Configure IS-IS via the WebUI

From the Configuration menu, choose ISIS.



From the ISIS page, you can add, edit, and delete ISIS routes:

- To add an ISIS route, click Add, complete the fields as described in Table 60, and then click Apply to device
- To edit an ISIS route, click the ISIS route in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an ISIS route, check its associated checkbox in the grid, and then click Delete.

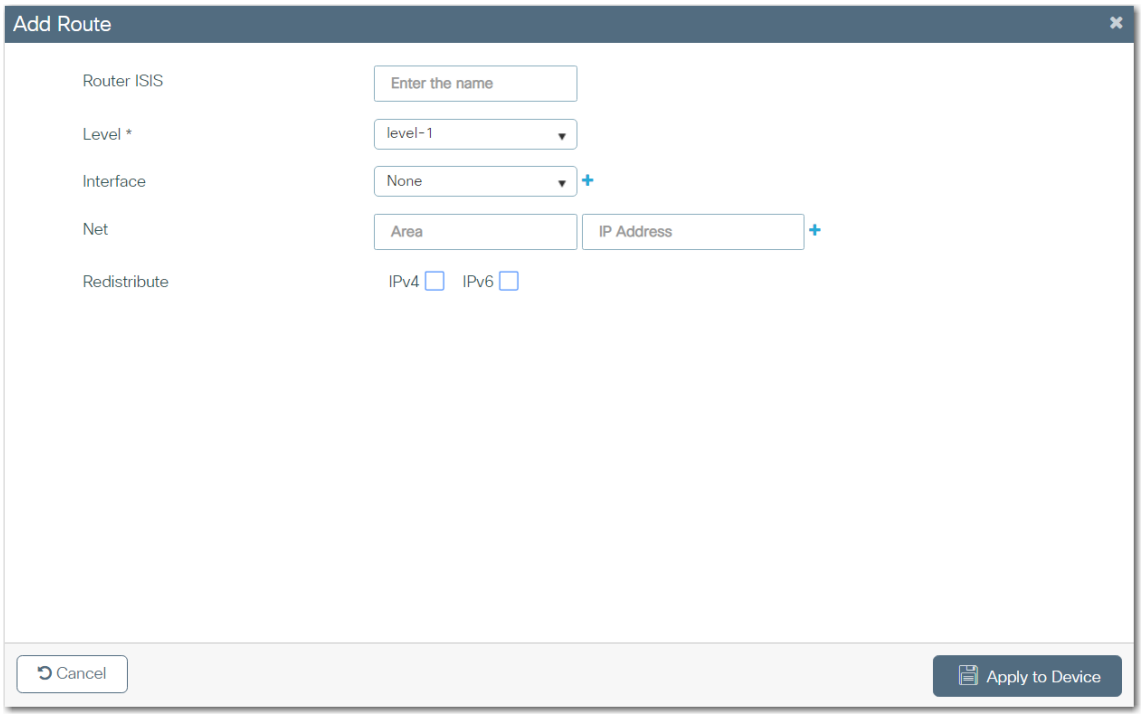


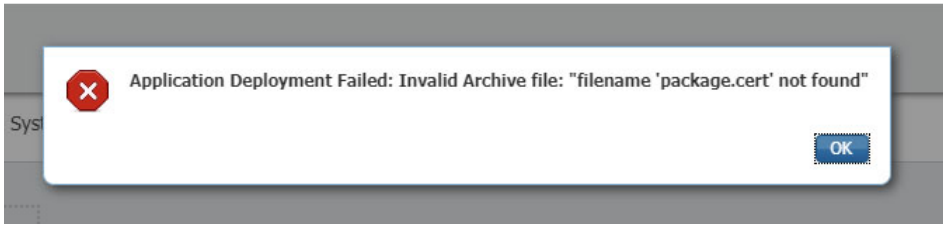
Table 60 - Add Route

Field	Description
Router ISIS	Enter a name for the ISIS process.
Level	Choose a configuration for the ISIS router: • level-1—The router acts as only a station router. • level-1-2—The router acts as both a station router and an area router. • level-2-only—The router acts as only an area router.
Interface	Choose an interface to route ISIS.
Net	The NET is the address of a Network Service Access Point (NSAP), which identifies an instance of the ISIS routing protocol running on an IS. Enter the Network Entity Title (NET) area and IP address for the routing process. Click the plus + sign to add the information to the grid.
Redistribute	Check each IP protocol to use for route redistribution.

IOx Services (Stratix 5800 Switch Only)

IOx provides an infrastructure to host applications on the device. On a device with IOx enabled, you can use the WebUI IOx tab to launch an application. IOx is only available on hardware systems that support advanced features.

Only Rockwell approved applications can run on IOx. Attempting to run any other applications will result in an error message similar to the following image.



There are two ways to enable IoX:

- Via CLI
- Via WebUI

Formatting Requirements for IOx via CLI

To configure IOx and a Stratix 5800 device, you need IOS release 17.06.01 or later, with a Rockwell Automation 8 GB High Capacity SD card. The SD card must be in an ext4 format.

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

There are two ways to format the SD card.

1. The entire SD card can be formatted to ext4 format. In this case, the SD card is used for IoX purposes only.

   format sdflash: ext4

```
Petra1.7#format sdflash: ext4
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "sdflash:".  Continue? [confirm]
Format operation reloads, if partitions are there. Continue? [confirm]
```

2. The second formatting method is to create partitions on the SD card so that one partition is used for configuration backup and the other is used for IOx. A percentage size of IoX partition can be provided. If it is not provided, a default percentage of 66% is used.

   partition sdflash: iox

```
Petra1.7#partition sdflash: iox ?
  <67-99>  Percentage Size of iox partition (67% to 99%)
  <cr>     <cr>
```



Partitioning an SD card reloads the switch.
While formatting an SD card, if partitions exist, the switch reloads and the partitions are removed.

3. To verify the sdflash filesystem, use the command "show sdflash: filesys".
4. To verify that the internal clock is synchronized, check the date and time using the "show clock" command.

Enable IOx via the CLI

To enable IOx using CLI, the command "iox" must be executed in the global configuration mode. After executing the command, save the configuration.

```
Petr1.7#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Petr1.7(config)#iox
Warning: Do not remove SD flash card when IOx is enabled or errors on SD device
could occur.

Petr1.7(config)#exit
Petr1.7#wr
Building configuration...
[OK]
```

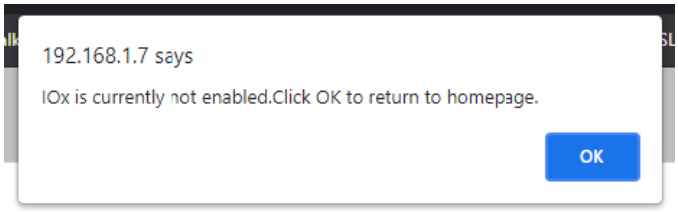
Verify that IOx is running by using the "show iox" command.

```
Petra1.7#sh Iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
Dockerd 18.03.0                : Running
```

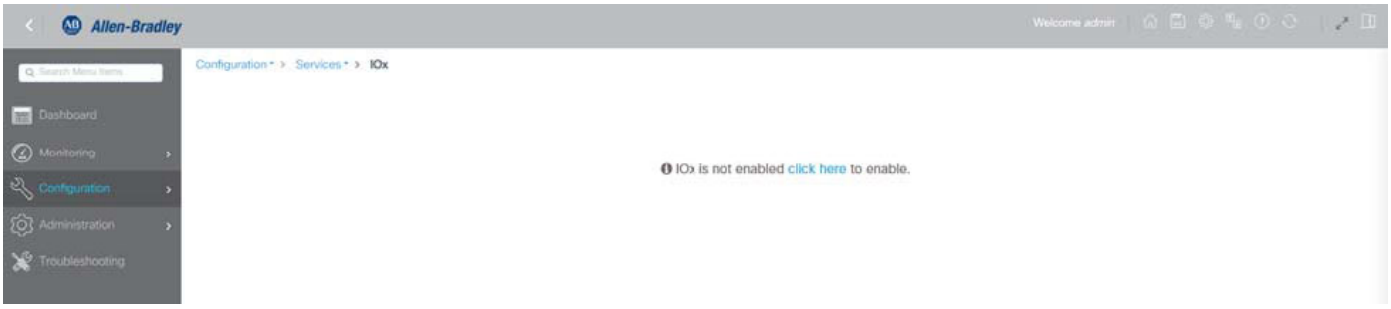
Enable IOx via the WebUI

1. Navigate to the IOx page under the Configuration tab, and click enable IoX. The following message appears.



2. Click OK.
3. Enable IOx using the “click here to enable” option on the webpage.

   It can take a couple of minutes to enable IOx.



The SD card cannot be formatted while IoX running. If you attempt to format the SD card while IoX is running, the switch will not format the SD card.

```
Petra1.9#sh iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
Dockerd 18.03.0                : Running

Petra1.9#
Petra1.9#
Petra1.9#
Petra1.9#format sdf
Petra1.9#format sdflash:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "sdflash:".  Continue? [confirm]
Format operation reloads, if partitions are there. Continue? [confirm]
Warning: IOx is running, stop IOx to run format command

%Error formatting sdflash: (Unknown error 0)
Petra1.9#
```

ATTENTION: To avoid errors, do not remove the SD card when IOx is enabled.

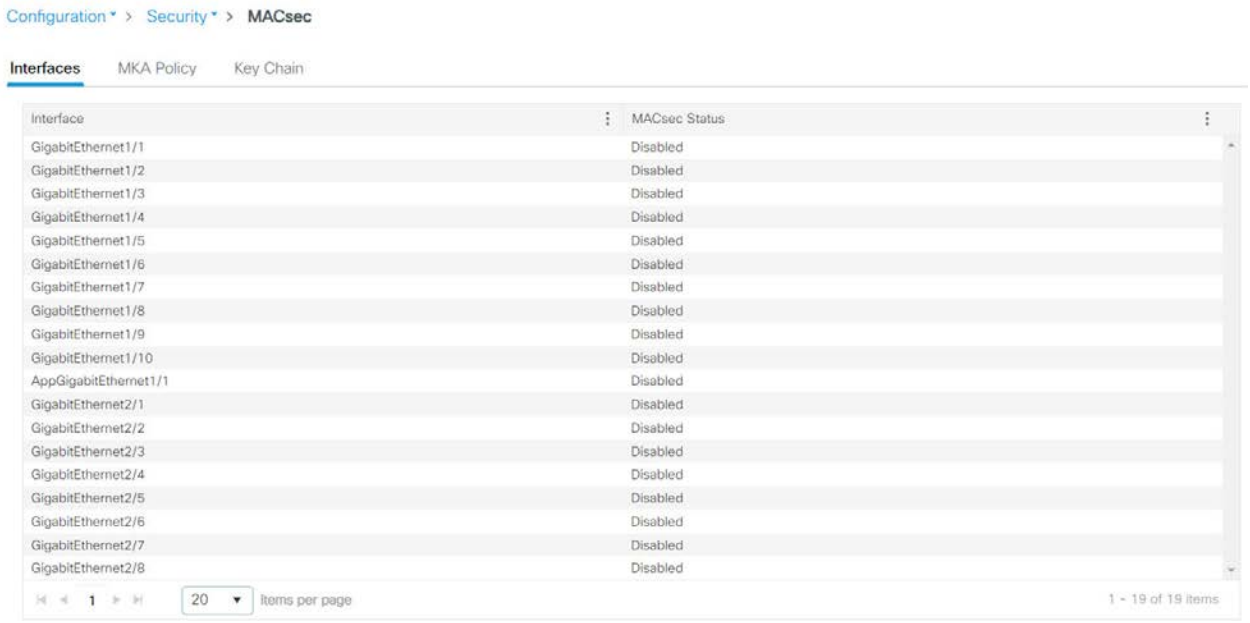
MACsec (Stratix 5800 Switch Only)

MACsec is the standard for authenticating and encrypting packets between two MACsec-capable devices. The switch supports encryption with MACsec Key Agreement (MKA) on downlink ports for encryption between the switch and host devices. The MKA protocol provides the required session keys and manages the required encryption keys.

Only switch-to-switch MACsec configuration is supported with WebUI.

To configure MACsec, define an MKA policy and apply it to an interface. You also must create a key chain that contains the Connectivity Key Name (CKN) and the Connectivity Association Key (CAK).

When MACsec is enabled on an interface, the entire interface traffic is secured by default. MACsec does not allow any unencrypted packets to be transmitted or received from the same physical interface. However, to enable MACsec on selected interfaces, you can choose to allow unencrypted packets to be transmitted or received from the same physical interface.



MKA Policy

Complete the following steps to configure an MKA Policy on the device.

On the Configuration > Security > MACsec > MKA Policy page, click Add to display the Add MKA Policy window.

To make changes to an existing policy, click the policy in the list.

To delete an MKA policy, select the check box for the policy and click X Delete.

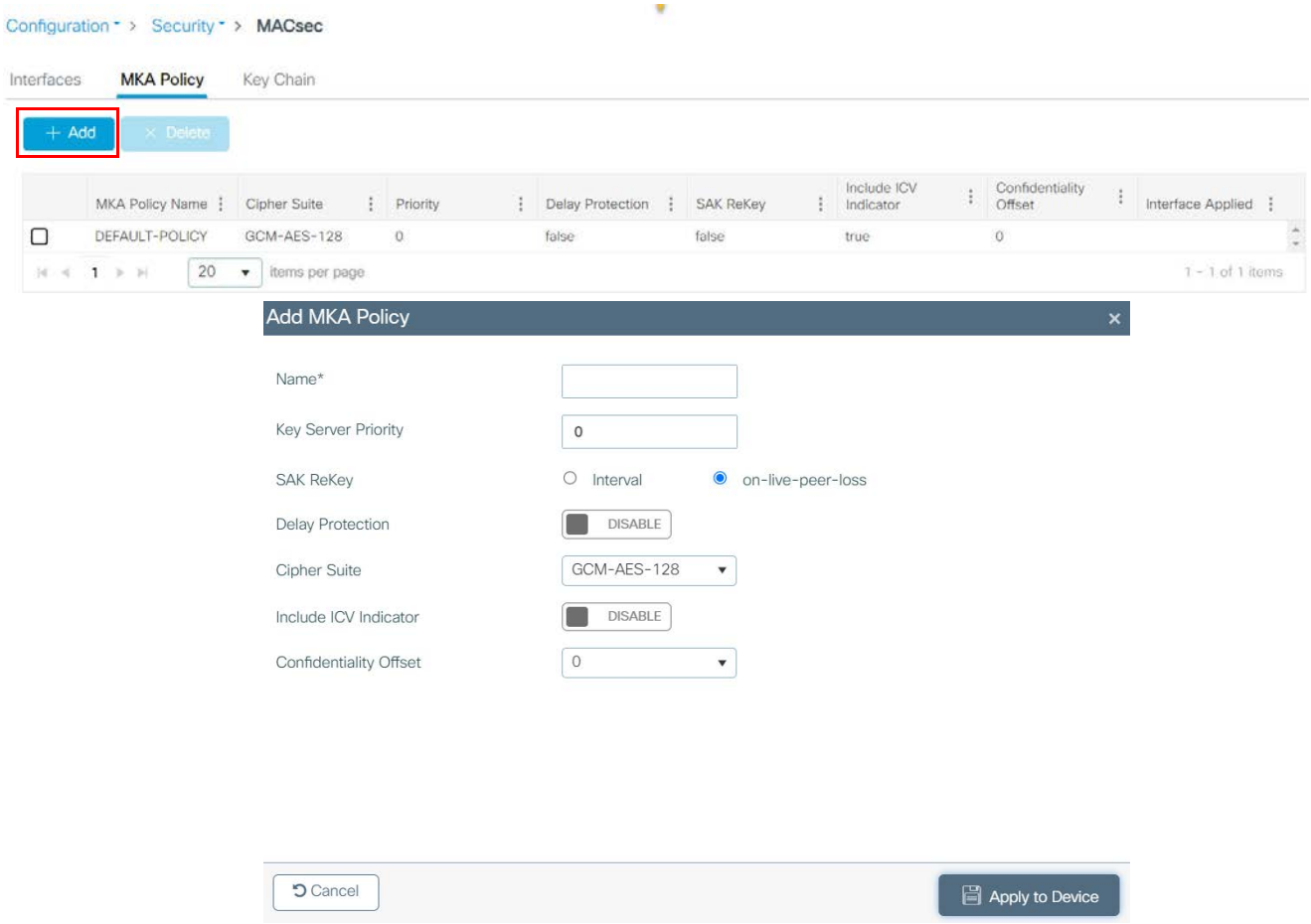


Table 61 - Add MKA Policy

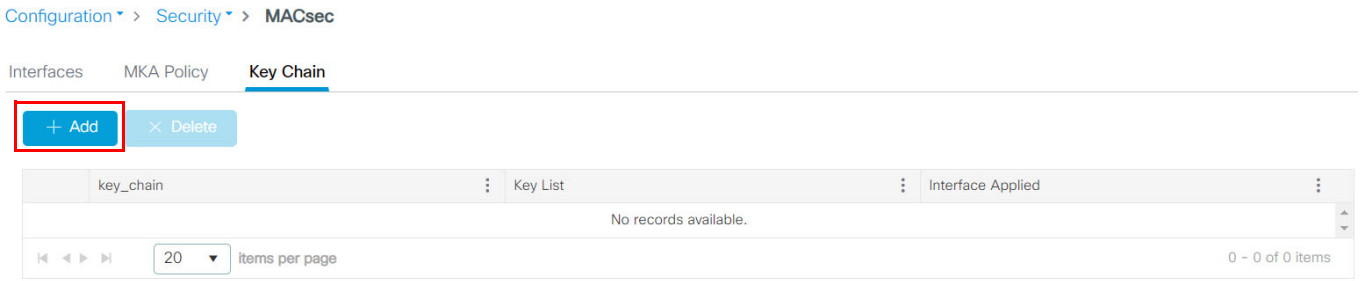
Field	Description
Name	Enter a name for the MKA Policy.
Key Server Priority	Key server priority (0...255). When the key server priority value is set to 255, the peer cannot become the key server.
SAK Rekey	Select whether to set a timer to rekey the MACsec secure association key (SAK) at a specified interval or when the link to the peer is lost during the session. If you select to perform the SAK Rekey at an interval, enter the rekey interval (in seconds). The range is from 30...65535, and the default value is 30.
Delay Protection	Allows MKA participants to ensure that the data frames protected by MACsec are not delayed by more than 2 seconds.

Table 61 - Add MKA Policy

Field	Description
Cipher Suite	You can configure the cipher suite for deriving SAK with 128-bit encryption. The default MACsec cipher suite is GCM-AES-128. If the device supports both GCM-AES-128 and GCM-AES-256 ciphers, it is highly recommended to define and use a user defined MKA policy to include both 128 and 256 bits ciphers or only 256 bits cipher, as may be required.
Include ICV Indicator	If you want to include the optional Integrity check value (ICV) Indicator as part of the transmitted MACsec Key Agreement PDU (MKPDU), Enable Include ICV Indicator. The ICV is sent with the protected data unit and is recalculated and compared by the receiver to detect data modification.
Confidentiality Offset	Confidentiality offset specifies the number of bytes starting from the frame header. MACsec encrypts only the bytes after the offset in a frame. An offset of 0 causes the entire packet (after the MACsec header) to be encrypted.

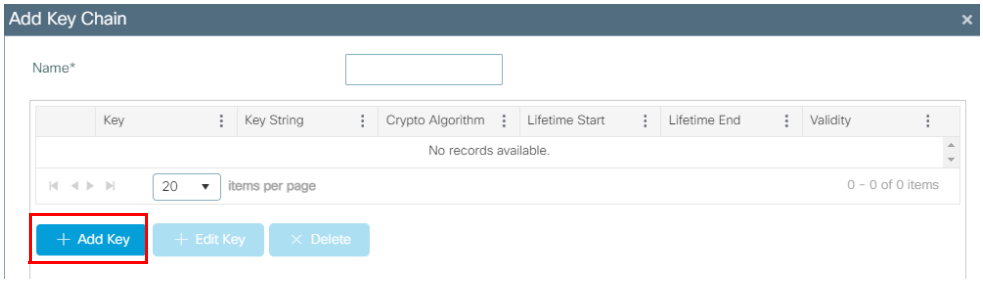
Key Chain

1. On the Configuration > Security > MACsec > Key Chain page, click Add to display the Add Key Chain window.



2. Enter a name for the key chain.
3. Click + Add Key.

   Click +Edit Key to make changes to an existing key. Click X Delete to remove a key.



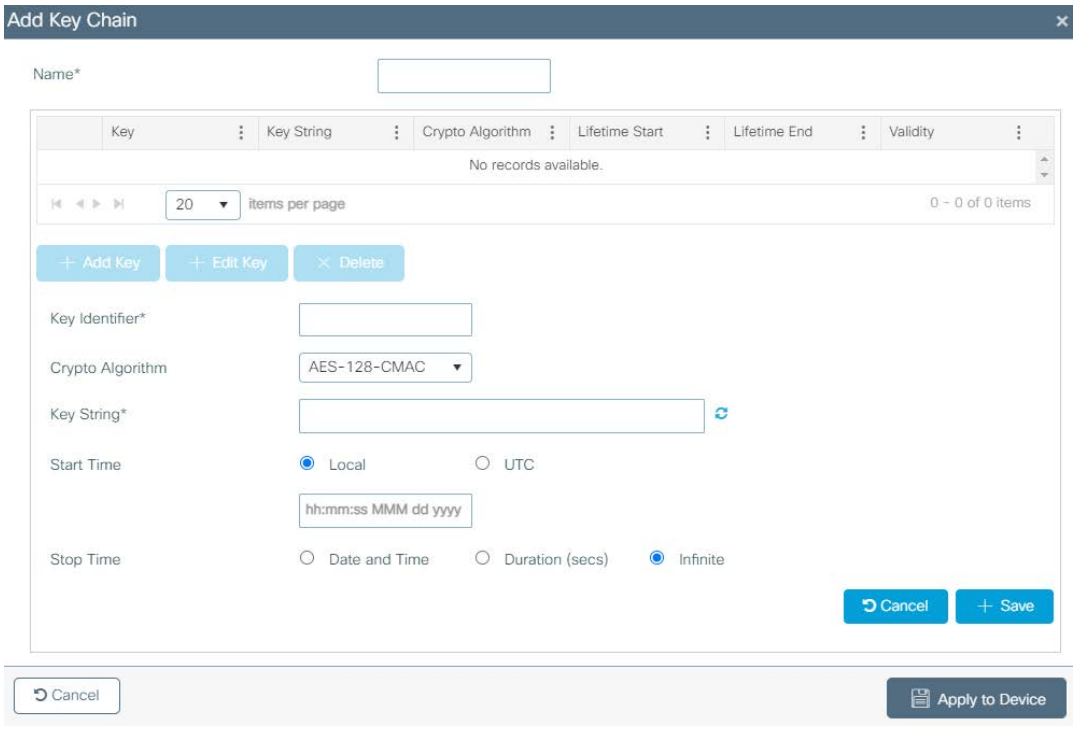


Table 62 - Add Key Chain

Field	Description
Key Identifier	Enter a unique identifier for the key. For 128-bit encryption, use 32 hex digit key-string. For 256-bit encryption, use 64 hex digit key-string.
Crypto Algorithm	Set the cryptographic authentication algorithm with 128-bit or 256-bit encryption.
Key String	Enter hex characters for the key string. Click to generate a key string. Set the lifetime of the pre-shared key.
Start Time	Choose Local or UTC and enter the time in the format {hh:mm:ss MMM dd yyyy}.
Stop Time	Choose one of the following: • Date and Time: Enter the date and time in the format {hh:mm:ss MMM dd yyyy}. • Duration (secs): Enter the number of seconds. • Infinite

4. Click Save to add the key.

Media Redundancy Protocol (MRP)

MRP, defined in International Electrotechnical Commission (IEC) standard 62439-2, provides fast convergence in a ring network topology for industrial automation networks. MRP operates at the MAC layer and is commonly used in conjunction with the PROFINET standard for industrial networking in manufacturing.

MRP Modes

The switch can operate in one of two MRP modes:

- PROFINET MRP mode—Deployed in a PROFINET environment, the switch is added and managed by Siemens Totally Integrated Automation (TIA) Framework. This is the default mode of the MRP manager or client.

  IMPORTANT When managing the switch via TIA, do not use the CLI or WebUI to configure MRP.

- MRP Ring mode—This mode is managed via the WebUI to configure as many as three MRP rings.

Protocol Operation

An MRP ring contains the following nodes, each with a pair of ports that participate in the ring:

- Media Redundancy Manager (MRM)—The ring manager initiates and controls the ring topology to react to network faults by sending control frames on one ring port over the ring and receiving them from the ring over its other ring port and conversely in the other direction.The MRM defines its maximum recovery times for a ring in the following range: 30 ms, 200 ms, and 500 ms.
- Media Redundancy Clients (MRCs)—Member ring nodes. An MRC reacts to received reconfiguration frames from the MRM and can detect and signal link changes on its ring ports.

All MRM and MRC ring ports support these states:

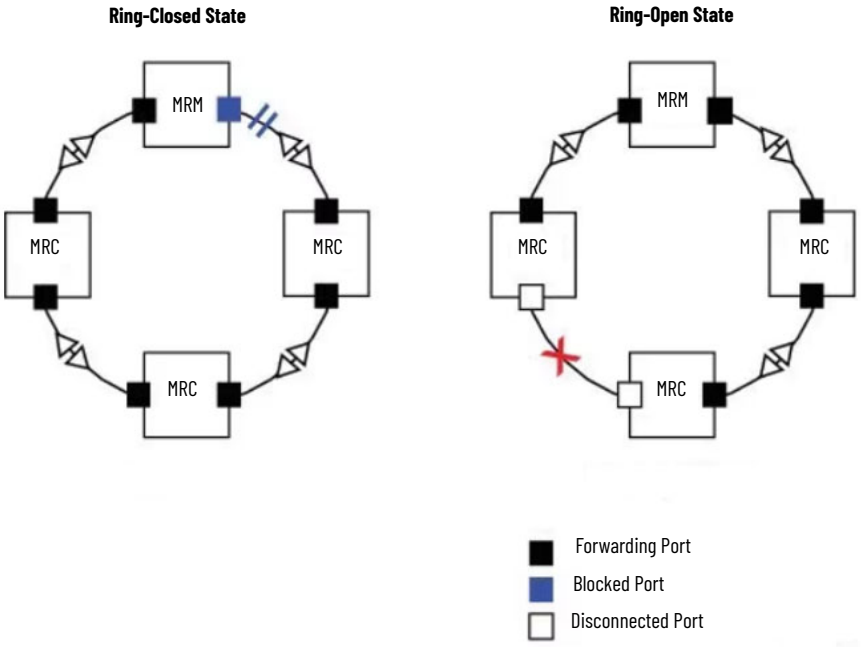
- Disabled—Ring ports drop all received frames.
- Blocked—Ring ports drop all received frames except MRP control frames and some standard frames, such as LLDP.
- Forwarding—Ring ports forward all received frames.
- Not Connected—The link is physically down or disconnected. This state differs from the Disabled state in which the MRP port is manually disabled via the WebUI.

During normal operation, the ring network operates in the Ring-Closed state (Figure 27). To prevent a loop, one of the MRM ring ports is blocked while the other port is forwarding. Most of the time, both ring ports of all MRCs are in the Forwarding state. With this loop avoidance, the physical ring topology becomes a logical stub topology.

Note the following details about the network shown in Figure 27:

- Ring-Closed State—The connection represented by the blue square on the MRM is in a Blocked state (two parallel lines) because no ports are disconnected.
- Ring-Open State—The two MRC connections represented by the white squares are in the Disabled state because the link between them is broken, as marked by a red "x".

Figure 27 - MRP Ring States



If a failure occurs, the network shifts into the Ring-Open state.

A connection failure between two MRCs causes the following port changes:

- On the MRM, both ring ports change to the Forwarding state.
- On each MRC adjacent to the failure, one ring port changes to a Disabled state and the other port changes to the Forwarding state.
- On the other MRCs, both ring ports change to the Forwarding state.

In the Ring-Open state, the network logical topology becomes a stub.

Layer 2 Ethernet frames are lost during the time required for the transition between these two ring states. The MRP protocol defines the procedures to automatically manage the switchover to minimize the switchover time. A recovery time profile, composed of various parameters, drives the MRP topology convergence performance. The 200 ms profile supports a maximum recovery time of 200 ms. 200_ms is the default profile setting.

MRP uses three types of control frames:

- To monitor the ring status, MRM regularly sends test frames on both ring ports.
- When MRM detects failure or recovery, it sends TopoChange frames on both ring ports.
- When MRC detects failure or recovery on a local port, it sends LinkChange subtype frames, Linkdown and Linkup, to the MRM.

Media Redundancy Automanager (MRA)

A Stratix 5200 switch or a Stratix 5800 switch can configure certain nodes or all nodes in the ring to start as a Media Redundancy Automanager (MRA). If configured to start as a Media Redundancy Automanager (MRA), a node selects an MRM by using a voting protocol and a configurable priority value. The remaining MRAs transition to the MRC role. All nodes must be configured as MRA or MRC. A manually configured MRM and MRA in the same ring is not supported.

The MRA role is not an operational MRP role like MRM or MRC. It is only an administrative, temporary role at device startup. A node must transition to the MRM role or the MRC role after startup and the MRM is selected through the manager voting process.

MRA functions as follows:

1. At startup, all MRAs begin the manager voting process. Each MRA begins to send MRP_Test frames on both ring ports. The MRP_Test frame contains the MRA priority value. The remote manager's priority value contained in the received MRP_Test frames are compared with the MRA's own priority. If its own priority is higher than the received priority, the MRA sends a negative test manager acknowledgment (MRP_TestMgrNAck) frame, along with the remote manager's MAC address.
2. If the receiving MRA receives an MRP_TestMgrNAck with its own MAC address, the receiving MRA initiates the transition into the client (MRC) role.
3. The MRP_TestPropagate frame informs other MRA devices in the client role about the role change and the new higher priority manager. The clients receiving this frame update their higher priority manager information accordingly. This makes sure that clients remain in the client role if the monitored higher priority manager role changes.

Multiple MRP Rings

In an Industrial Ethernet network, an MRP ring in a cell/area is a subring of the access layer. Depending on the MRP license and platform, you can connect multiple MRP rings, which you can then aggregate into the distribution layer.

On a Stratix 5200 switch or a Stratix 5800 switch, you can configure as many as three rings with MRP.

MRP-STP Interoperability

MRP works with Spanning Tree Protocol (STP) to help prevent unwanted broadcast loops if someone connects a device that does not participate in the MRP ring. In a network operating with MRP and STP, spanning tree BPDUs are not sent on MRP-enabled ports. If ports are unconfigured from an MRP ring, then the ports are added to the spanning tree.

MRP-STP interoperability is supported for both PROFINET MRP mode and MRP Ring mode and functions without additional CLI or WebUI configuration.

Requirements and Restrictions

Before you configure MRP, do the following:

- Verify that the switches have IOS release:
  - 17.11.01 or later for the Stratix 5200 switch
  - 17.10.01 or later for the Stratix 5800 switch
- Because MRP is deployed in a physical ring topology, leave one physical connection between two nodes in each ring open by using one of these methods:
  - Issue a shut command on the connecting interfaces.
  - Physically remove the cable to avoid any network storms.

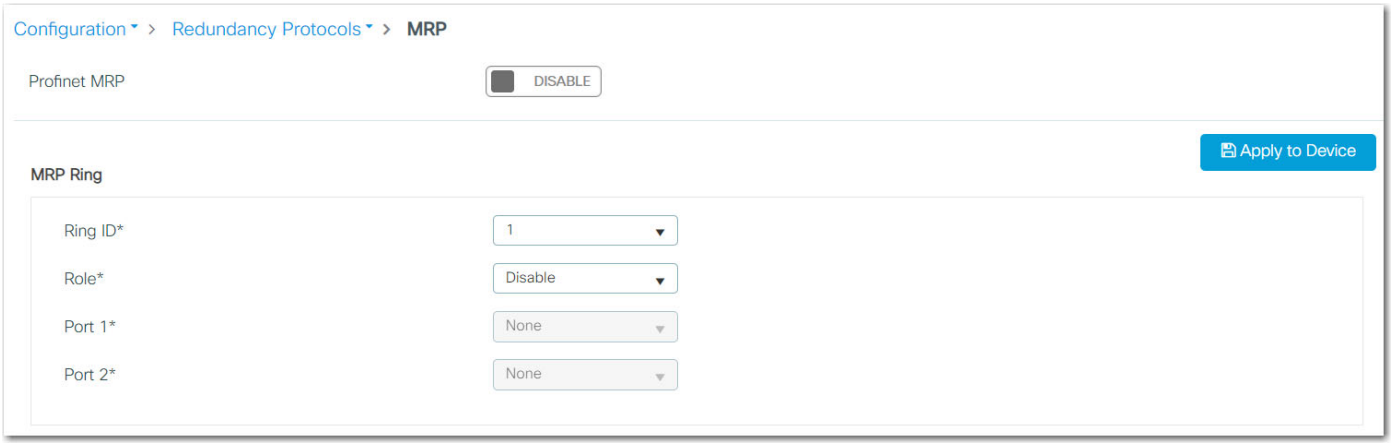
  After you have properly configured all MRCs and MRMs, issue a no shut command on the port or reconnect the cable between the nodes.
- Determine the MRP configuration on the switch: MRA or MRC.
- To use a non-default VLAN, configure the PROFINET VLAN ID before assigning it to the MRP configuration. The MRP default VLAN is 1.

Observe these guidelines:

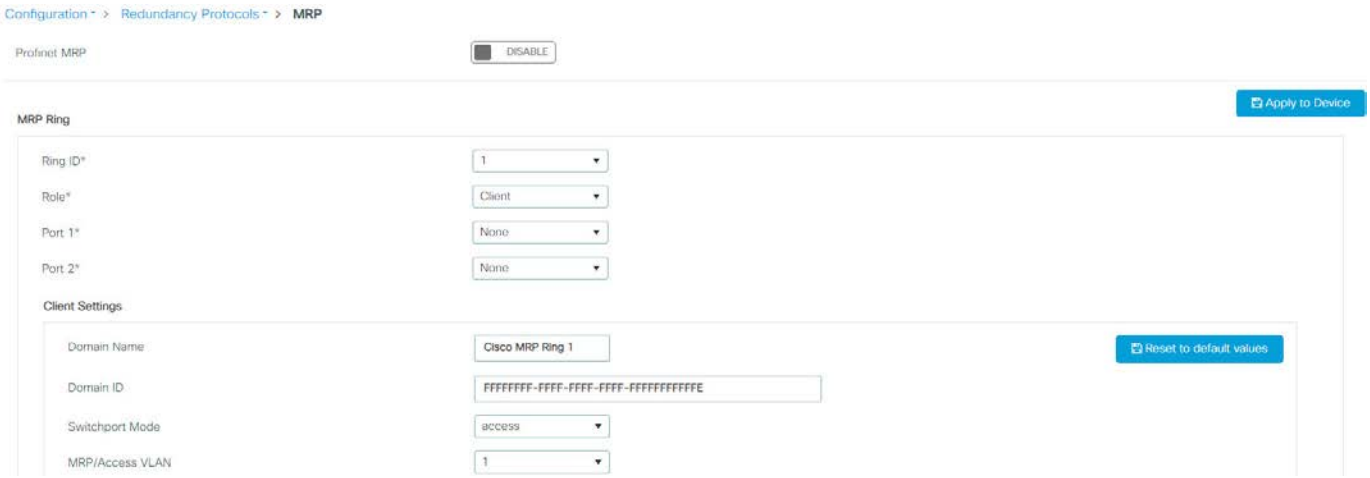
- The switch supports up to 50 MRCs per ring.
- MRP cannot run on the same interface as Resilient Ethernet Protocol (REP), Spanning Tree Protocol (STP), macsec, or Dot1x.
- STP does not run on MRP segments. MRP interfaces drop all STP BPDUs.
- For access ports, you must specifically configure **switchport mode access** and **switchport access vlan** *x* commands in the MRP interface.
- MRP interfaces come up in a forwarding state and remain in a forwarding state until notified that it is safe to block. The MRP ring changes to a Ring-Closed state.
- MRP ports cannot be configured as any of these port types: SPAN destination port, Private VLAN port, or Tunnel port. When operating PROFINET mode, you cannot configure MRP ports as trunk ports.
- MRP is not supported on EtherChannels or on an individual port that belongs to an EtherChannel.
- Each MRP ring can have one MRP VLAN. The VLAN must be different for each ring in a device to avoid traffic flooding.

Configure MRP via the WebUI

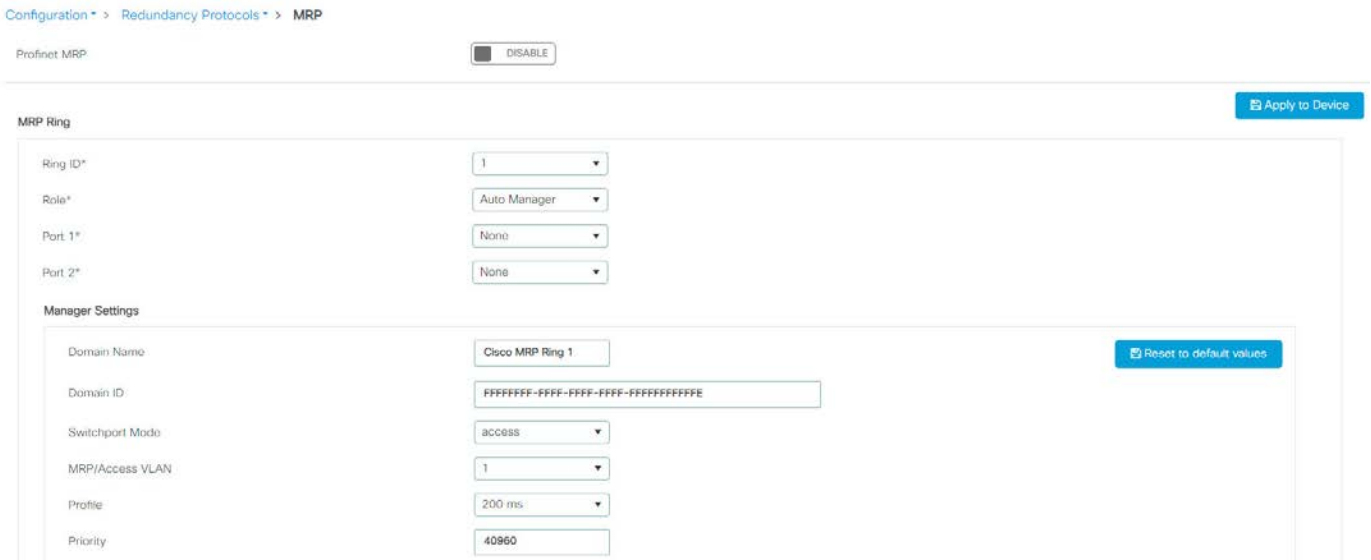
From the Configuration > Redundancy Protocols menu, choose MRP.



To see the Client Settings, set the Role field to Client.



To see the Manager Settings, set the Role field to Auto Manager.



Complete the fields as described in Table 63, and then click Apply to Device.

If you plan to use TIA to configure and manage MRP on the switch in a PROFINET environment, on the Administration > Industrial Protocols > PROFINET page, click the button to enable PROFINET. PROFINET is only available on the Stratix 5800 switch.

If you enable PROFINET, the MRP ring configuration disappears and the following warning appears.



WARNING: Enabling PROFINET MRP disables MRP and does not allow you to configure MRP ring. Are you sure you want to continue?

Table 63 - MRP

Field	Description
PROFINET MRP	Click to enable or disable PROFINET MRP. Default value: Disabled **IMPORTANT:** MRP mode and PROFINET MRP mode are mutually exclusive. You cannot use WebUI to configure the MRP ring when PROFINET MRP mode is enabled.
MRP Ring	
Ring ID	Select the ID number of the MRP ring: 1, 2, or 3. There is a one-to-one association between the MRP ring ID and the Domain ID.
Role	Select an MRP role: • Disable (default) • Auto Manager • Client
Port 1	Select a switch port to designate as MRP ring port 1.
Port 2	Select a switch port to designate as MRP ring port 2.
Client Settings	
Domain Name	Enter a logical name of the configured MRP domain ID.
Domain ID	Enter a unique ID (UUID) that represents the MRP ring. The Domain ID references different rings when multiple rings are configured. The UUID is a string of 32 hexadecimal digits in five groups that are separated by hyphens, for example 550e8400-e29b-41d4-a716.
Switchport Mode	Select a Switchport mode for the MRP ports. Both MRP ports must have the same interface mode (access or trunk). When both MRP ports are in access mode, the access VLANs must match. Valid values: • access • trunk
Allowed Vlan	(Appears only for trunk Switchport mode). Select all VLANs or a range of VLANs.
MRP/Native Vlan	(Appears only for trunk Switchport mode). Select a VLAN for sending MRP frames. The default VLAN is 1. To use a non-default VLAN, you must create it before assigning it to MRP.
MRP/Access Vlan	(Appears only for access Switchport mode). Select a VLAN for sending MRP frames. The default VLAN is 1. To use a non-default VLAN, you must create it before assigning it to MRP.
Manager Settings	
Profile	(Appears only for Auto Manager MRP role). Select a ring recovery time profile: • 30 ms— Maximum recovery time 30 milliseconds • 200 ms— Maximum recovery time 200 milliseconds • 500 ms— Maximum recovery time 500 milliseconds
Priority	(Appears only for Auto Manager MRP role). Enter the manager priority for multiple MRMs. Valid values: 36864...65535 Default value: 40960

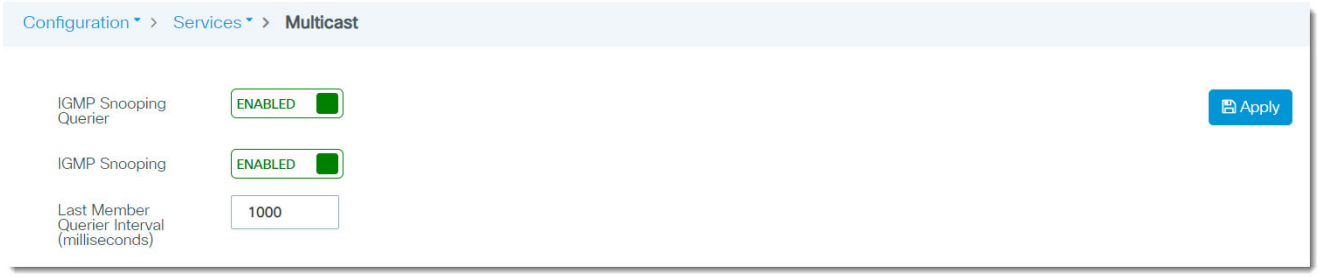
Multicast Services

Multicast services include Internet Group Management Protocol (IGMP) snooping settings. Switches can use IGMP snooping to constrain the flooding of multicast traffic. IGMP snooping dynamically configures interfaces so that multicast traffic is forwarded to only those interfaces that are associated with IP multicast devices. For more information about IGMP snooping, see the Ethernet Reference Manual, publication ENET-RM002.

Multicast services are supported on both Layer 2 and Layer 3 interfaces.

Configure Multicast Services via the WebUI

From the Configuration menu, choose Multicast.



Complete the fields as described in Table 64, and then click Apply to Device.

Table 64 - Multicast

Field	Description
IGMP Snooping Querier	Click to enable or disable IGMP snooping with querier. Default value: Enabled
IGMP Snooping	Click to enable or disable IGMP snooping. Default value: Enabled
Last Member Querier Interval (milliseconds)	To configure a last member query interval for IGMP snooping, enter a value in milliseconds. The query interval is the length of time after which a group record is deleted if no reports are received. Default value: 1000 ms

NetFlow (Stratix 5800 Switch Only)

NetFlow is an application that provides statistics on packets that flow through the switch. NetFlow applications include network traffic accounting, usage-based network billing, network planning, security, denial-of-service, and network monitoring.

IMPORTANT NetFlow is available only on select modular switch models. For supported catalog numbers, see Table 1 on page 15.

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 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.

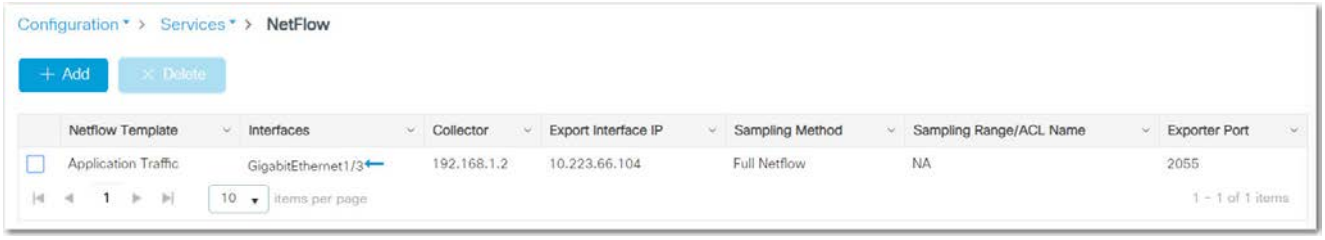
There are two primary methods to access NetFlow data:

- 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.

Configure NetFlow via the WebUI

From the Configuration menu, choose NetFlow.



From the NetFlow page, you can add, edit, and delete NetFlow templates:

- To add a NetFlow template, click Add, complete the fields as described in Table 65, and then click Apply to device
- To edit a NetFlow template, click the NetFlow template in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a NetFlow template, check its associated checkbox in the grid, and then click Delete.

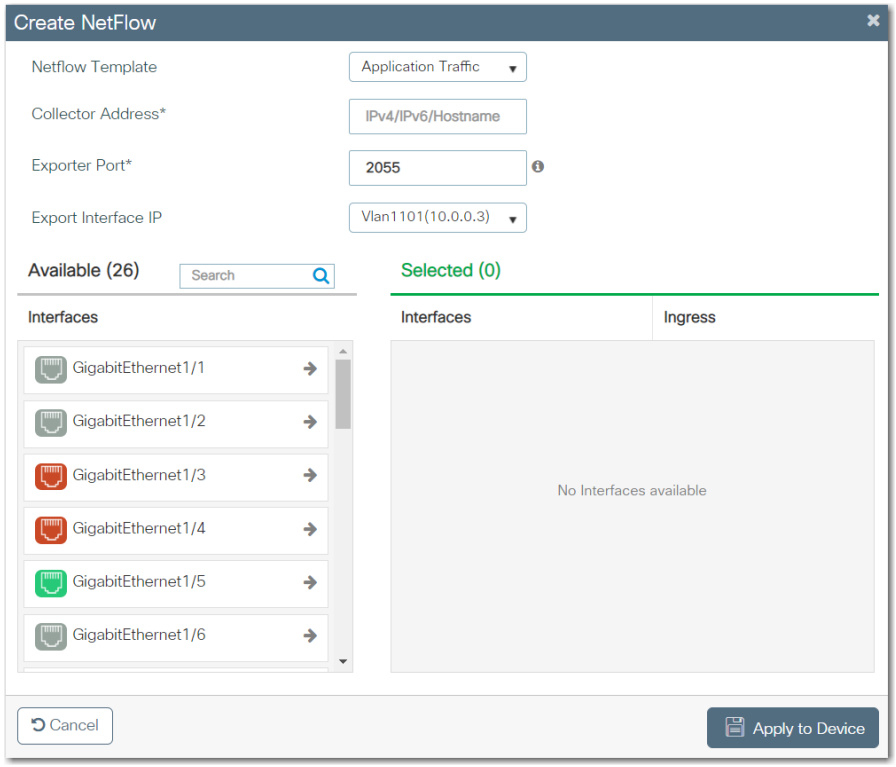


Table 65 - Create NetFlow

Field	Description
Netflow Template	Choose a NetFlow template: • Application Traffic—Monitors application traffic. • Server Utilization—Monitors packets to analyze server usage in the network. • Security—Monitors packets for network security. • Capacity Planning—Monitors packets to analyze network capacity and usage. • StealthWatch—Monitors packets to detect threats and security vulnerabilities.
Collector Address	Enter the collector IP address of where to send the NetFlow data.

Table 65 - Create NetFlow

Field	Description
Exporter Port	Enter the port number on which your NetFlow collector is listening.
Export Interface IP	Choose e export address to use when sending the NetFlow data.
Interfaces	In the Available list, click the arrows to move interfaces to the Selected list to associate them with the NetFlow template.

Network Address Translation (NAT)

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.

IMPORTANT NAT is available only on select modular switch models. For supported catalog numbers, see Table 1 on page 15.

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 (inside) subnets while maintaining unique identities on the public (outside) 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 NAT Whitepaper, publication ENET-WP032.

Configuration Overview

To configure NAT, create one or more unique NAT instances. A NAT instance contains entries that define each address translation and other configuration parameters.

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 that you route traffic through a Layer 3 switch or router.

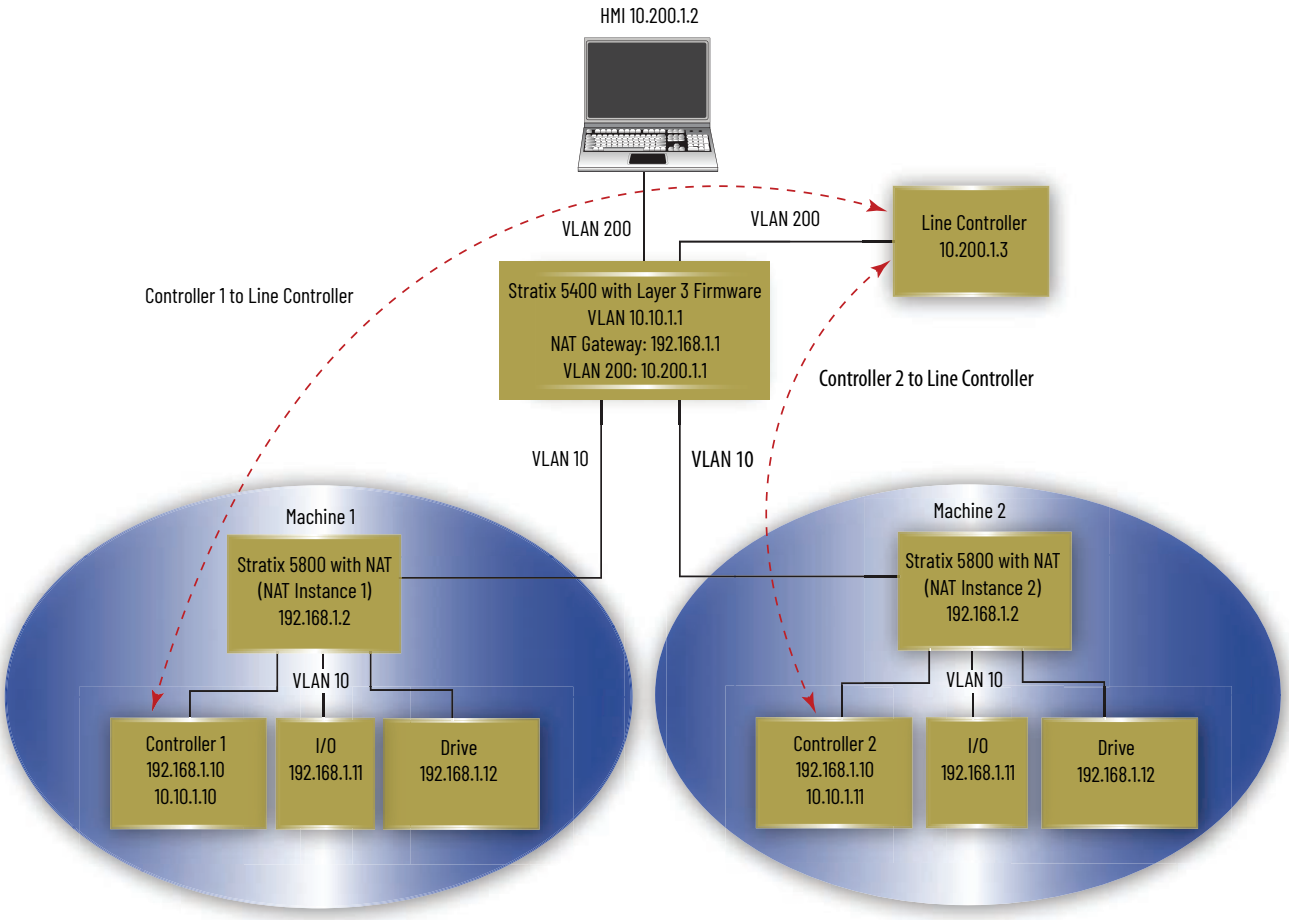
If traffic is routed through a Layer 3 switch or router (Figure 28), you define the following:

- 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.

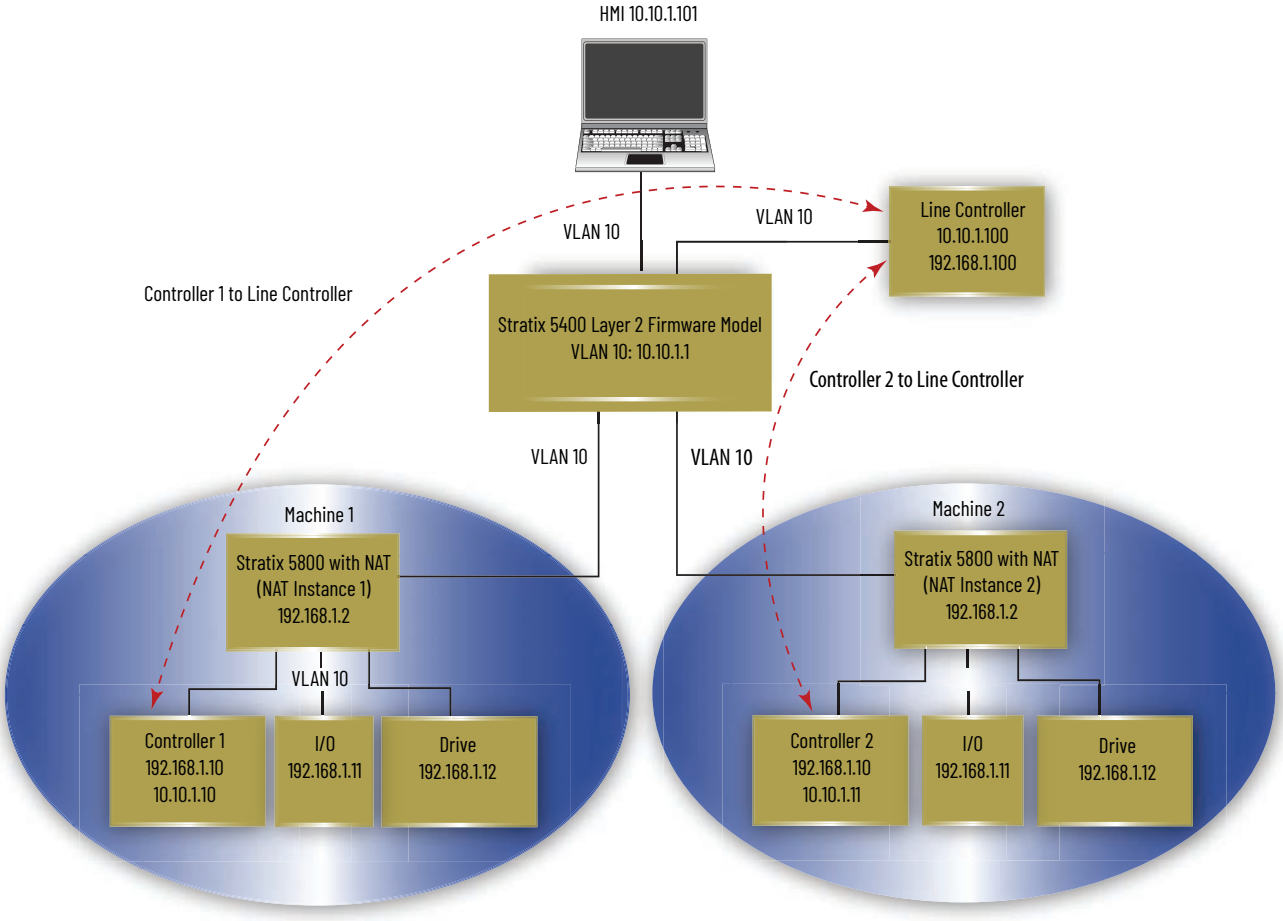
Figure 28 - Layer 3 Example with NAT in Stratix 5800 Switch



If traffic is routed through a Layer 2 switch (Figure 29), you define the following.

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

Figure 29 - Layer 2 Example with NAT in Stratix 5800 Switch



An address translation can be one of three types. The type of translation determines the number of translation entries as shown in Table 66.

Table 66 - 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
Network	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 combination counts 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 translation allows you to save translation-entries by having one translation-entry for many addresses.

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.

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

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

Requirements and Restrictions

Before configuring NAT, know the following requirements and restrictions:

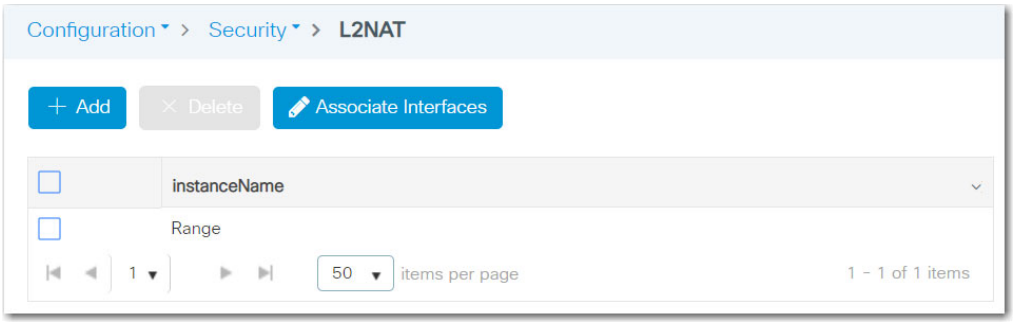
- Available interfaces for NAT instances are Gi1/1 and Gi1/2. For the Stratix 5800 switch, both interfaces are SFP slots, and for the Stratix 5200 switch they are Combo ports.
- Some NAT configurations can result in greater-than-expected traffic loads on both private and public subnets. Also, unintended 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.
- 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.
- 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.
- The switch can translate only IPv4 addresses.
- The switch can have a maximum of 128 NAT instances and 128 translation entries across all NAT ports. Note that a subnet translation counts as only one translation entry, but includes translations for many devices.

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

Configure NAT via the WebUI

From the Configuration menu, choose L2NAT.



From the L2NAT page, you can add, edit, and delete NAT instances and associate NAT instances with interfaces and VLANs:

- To add a NAT instance, proceed to page 143.
- To edit a NAT instance, click the instance in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a NAT instance, check its associated checkbox in the grid, and then click Delete.
- To associate a NAT instance with an interface and VLANs, proceed to page 146.

Add NAT Instances

1. From the L2 NAT page, click Add.
2. In the Name field, enter a unique name to identify the instance.

   When editing a NAT instance, you cannot change this field.
3. On the Translations tab, define translations based on your application, and then click Apply to Device.

   For information about how to complete the Inside and Outside fields, refer to the corresponding descriptions in Table 67 on page 144.

Application	Required Translations
Traffic is routed through a Layer 3 switch or router, as shown in Figure 28 on page 138	A private-to-public (inside) translation for each device in the private subnet that communicates on the public subnet. a. From the Inside drop-down menu, choose a translation type, and then complete the fields to the right. b. Click the plus sign (+) to add the translation to the grid. c. Repeat these steps for each device that requires a translation entry. One gateway (outside) translation for the Layer 3 switch or router. a. From the Outside drop-down menu, choose a translation type, and then complete the fields to the right. b. Check Gateway. c. Click the plus sign (+) to add the translation to the grid. d. Repeat these steps for to add the gateway translation to the grid.
Traffic is routed through a Layer 2 switch, as shown in Figure 29 on page 139	A private-to-public (inside) translation for each device in the private subnet that communicates on the public subnet. a. From the Inside drop-down menu, choose a translation type, and then complete the fields to the right. b. Click the plus sign (+) to add the translation to the grid. c. Repeat these steps to add the translation to the grid. d. Repeat these steps for each device that requires a translation entry. A public-to-private (outside) translation for each device on the public subnet that communicates on the private subnet. a. From the Outside drop-down menu, choose a translation type, and then complete the fields to the right. b. Make sure that the Gateway checkbox is cleared, and then click the plus sign (+) to add the translation to the grid. c. Repeat these steps to add the translation to the grid. d. Repeat these steps for each device that requires a translation entry.

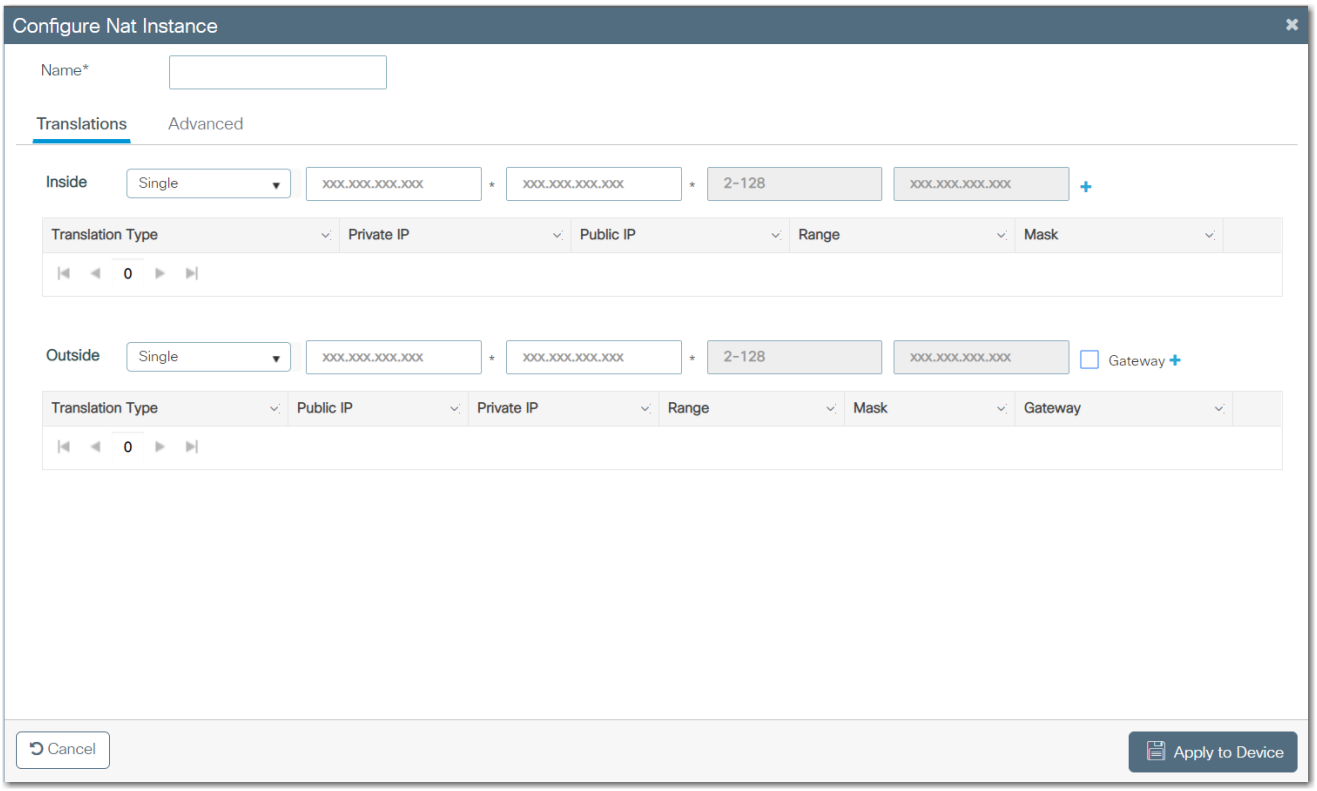


Table 67 - Configure NAT Instance Grids—Translations Tab

Field	Description
Inside (private-to-public translations)	
Translation Type	The type of translation: • Single—Translates one private address to one public address. • Network—Translates all or a portion of the addresses in the private subnet to addresses on the public subnet. • Range—Translates many sequential private addresses to many sequential public addresses.
Private IP	For single translation types, this is the existing address for the device on the private subnet. For network translation types, this is the network address for the private subnet. This address must correspond to the size of the subnet mask to translate. See Table 68. For range translation types, this is the first address in the range of sequential addresses.
Public IP	For single translation types, this is the unique public address to represent the device. For network translation types, this is the network address for the public subnet. This address must correspond to the size of the subnet mask to translate. See Table 68. For range translation types, this is the first address in the range of sequential addresses.
Range	(Applies only to Range translation types). The number of addresses to translate. **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Mask	(Applies only to Network translation types). The subnet mask for the addresses to translate.
Outside (public-to-private translations)	
Translation Type	The type of translation: • Single—Translates one public address to one private address. • Network—Translates all or a portion of the addresses in the public subnet to addresses on the private subnet. • Range—Translates many sequential public addresses to many sequential private addresses.
Public IP	For single translation types, this is the unique public address to represent the device. For network translation types, this is the network address for the public subnet. This address must correspond to the size of the subnet mask to translate. See Table 68. For range translation types, this is the first address in the range of sequential addresses.
Private IP	For single translation types, this is the existing address for the device on the private subnet. For network translation types, this is the network address for the private subnet. This address must correspond to the size of the subnet mask to translate. See Table 68. For range translation types, this is the first address in the range of sequential addresses.

Table 67 - Configure NAT Instance Grids—Translations Tab (Continued)

Field	Description
Range	(Applies only to Range translation types). The number of addresses to translate. **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Mask	(Applies only to Network translation types). The subnet mask for the addresses to translate.
Gateway	Indicates whether the translation is a gateway translation. A gateway translation enables devices on the public subnet to communicate with devices on different VLANs on the private subnet. Valid values: • true • false

Table 68 - Subnet Mask Starting Address

Subnet Mask	Subnet Address
255.255.0.0	The last two octets must end in 0. **EXAMPLES:** 192.168.0.0 or 10.200.0.0
255.255.255.0	The last octet must end in 0. **EXAMPLES:** 192.168.1.0 or 10.200.1.0.
255.255.255.128	The last octet must end in 0 or 128. **EXAMPLES:** 192.168.1.0 or 192.168.1.128; 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. **EXAMPLES:** 192.168.1.64 or 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. **EXAMPLES:** 192.168.1.32 or 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. **EXAMPLES:** 192.168.1.16 or 10.200.1.16

4. To configure traffic permits and packet fixups, click the Advanced tab, configure the fields as described in Table 69, and then click Apply to Device.

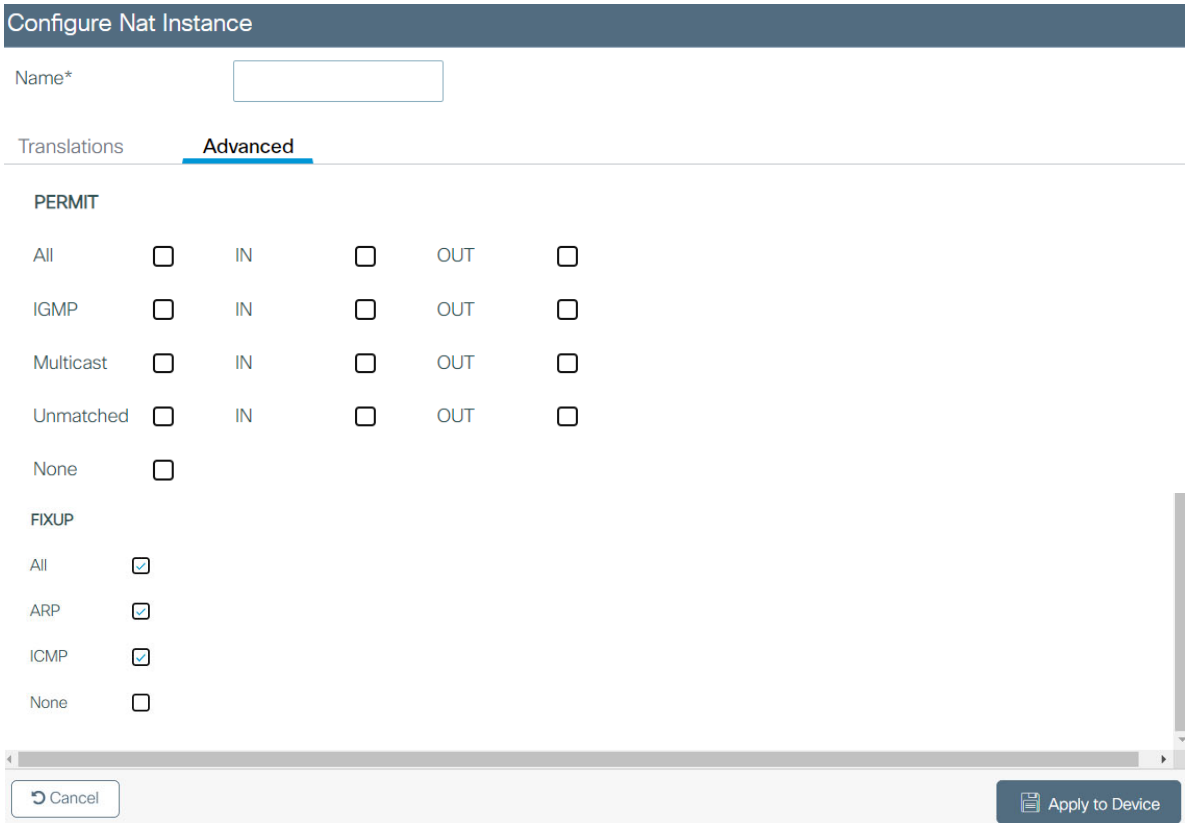


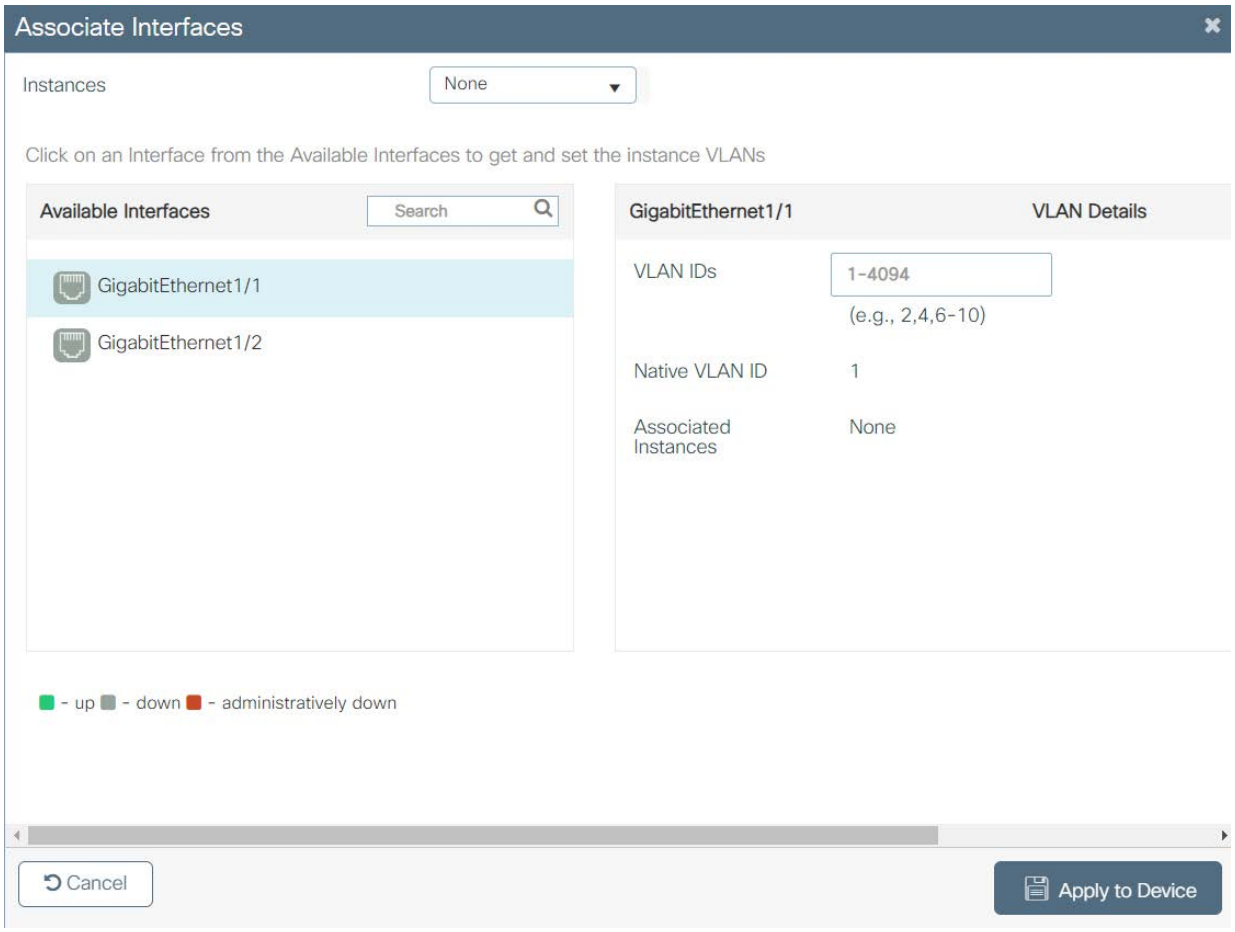
Table 69 - Configure NAT Instance—Advanced Tab

Field	Description
PERMIT	• Only unicast traffic is subject to translation. All unmatched, multicast, and IGMP packets are dropped by default. Check the All check box to permit unmatched traffic and traffic types that are not configured to be translated. Check the None check box to drop unmatched, multicast, and IGMP packets.
FIXUP	Protocols, such as ARP and ICMP, do not work transparently across the NAT boundary. By default, these protocols are fixed up to support translations. Specify whether to enable or disable fixups for protocol packets: • All—Check to enable fixups for all protocol packets. • ARP - The number of packets handled with ARP Fixup to change dynamic ARP entries into static entries in the NAT instance. • ICMP - The number of packets handled with the ICMP Fixup to change dynamic ICMP entries into static entries in the NAT instance. • None—Check to disable fixups for all protocol packets.

Associate NAT Instances with Interfaces and VLANs

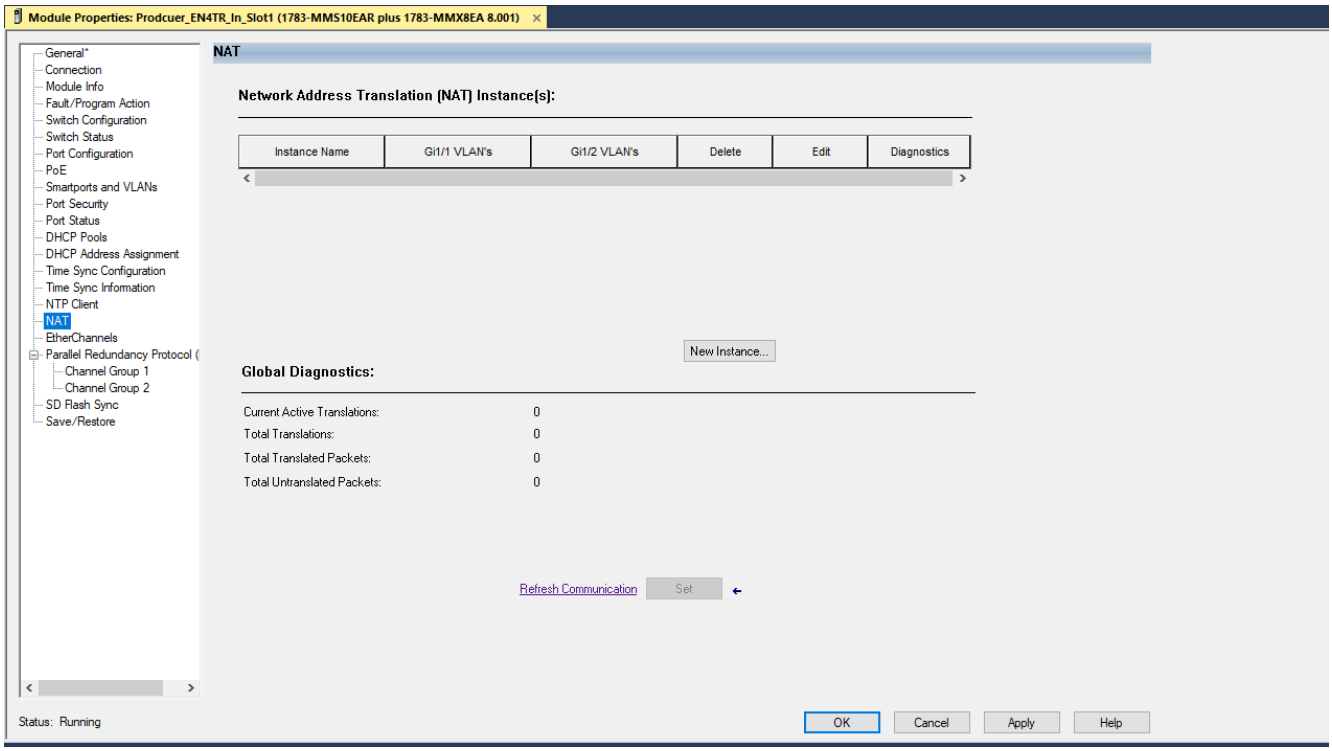
1. From the L2 NAT page, click Associate Interfaces.
2. From the Interfaces drop-down menu, choose the NAT instance to associate with interfaces and VLANs.
3. In the list of available interfaces, select GigabitEthernet1/1 or GigabitEthernet1/2.
4. On the right, specify the VLANs to associate with the NAT instance, and then click Apply to Device.

Field	Description
VLAN IDs	Enter one VLAN ID or a range of VLAN IDs, such as 2, 4, or 6...10.
Native VLAN ID	Displays the native VLAN for the selected interface.
Associated Instances	Instances that specify the address translations.



Configure NAT via the Logix Designer Application

In the navigation pane, click NAT.

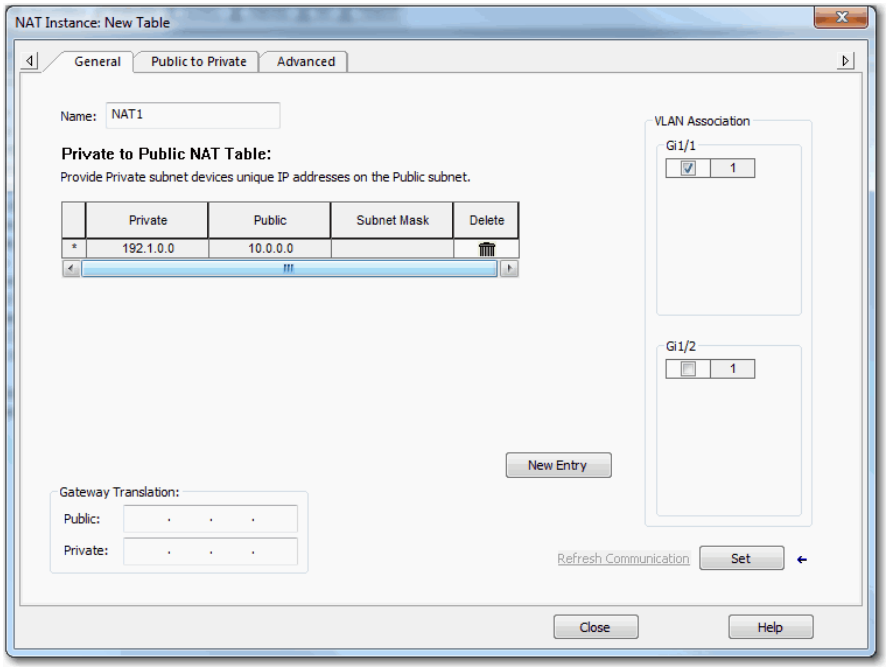


On the NAT view, you can add, edit, delete, and monitor NAT instances:

- To add a NAT instance, click New Instance, and then proceed to page 148.
- To edit a NAT instance, click the Ellipses icon in the Edit column, modify the fields, and then click Close.
- To delete a NAT instance, click the Trash icon in the Delete column.
- To monitor NAT statistics, see page 304.

Add NAT Instances

1. From the NAT view, click New Instance to display the New Instance dialog box.



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

   The instance name cannot include spaces or exceed 32 characters.

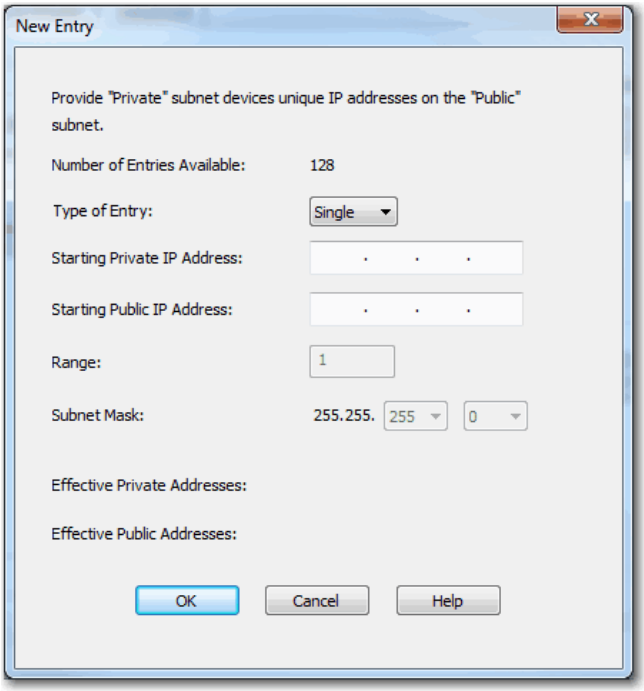
3. In the VLAN Association area, check the checkbox next to each VLAN to assign to the instance.

   For more information about VLAN assignments, see page 140.

4. Define translations based on your application as described in Table 70.
5. To configure traffic permits and packet fixups for the instance, see page 152.

6. Click Set.

New Entry—Private to Public Translation



New Entry—Public to Private Translation

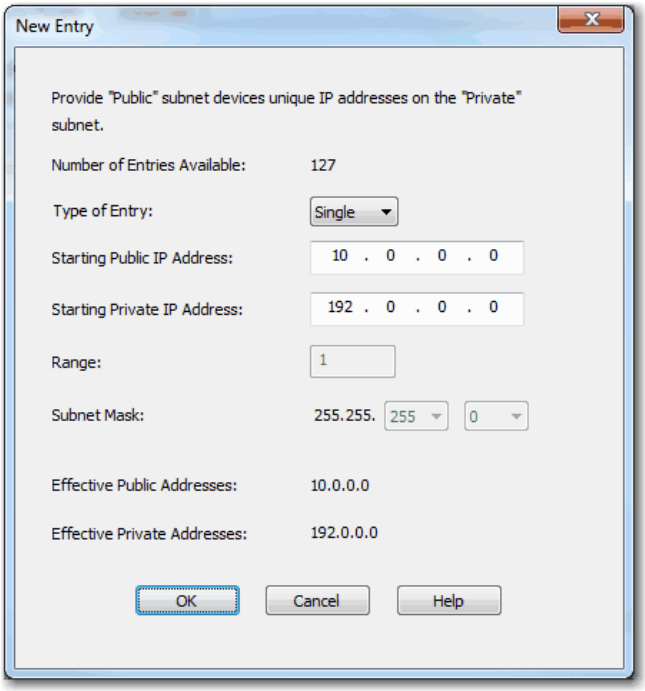


Table 70 - Translations Required by Application

Application	Required Translations
Traffic is routed through a Layer 3 switch or router, as shown in Figure 28 on page 138	A private-to-public (inside) translation for each device in the private subnet that communicates on the public subnet. a. On the General tab, click New Entry. b. Do one of the following: – To translate one address for a device on the private subnet that communicates on the public subnet, see Table 71. – To translate a range of addresses for devices on the private subnet that communicates on the public subnet, see Table 72. – To translate all addresses in the private subnet or a portion of the private subnet, see Table 73. c. Click OK. One gateway (outside) translation for the Layer 3 switch or router. a. In the Gateway Translations Public field, enter the default gateway address of the Layer 3 switch or router that is connected to the uplink port of the switch. b. In the Gateway Translations Private field, enter a unique IP address to represent the Layer 3 switch or router on the private network. c. Click OK.
Traffic is routed through a Layer 2 switch, as shown in Figure 29 on page 139	A private-to-public (inside) translation for each device in the private subnet that communicates on the public subnet. a. On the General tab, click New Entry. b. Do one of the following: – To translate one address for a device on the private subnet that communicates on the public subnet, see Table 71. – To translate a range of addresses for devices on the private subnet that communicates on the public subnet, see Table 72. – To translate all addresses in the private subnet or a portion of the private subnet, see Table 73. A public-to-private (outside) translation for each device on the public subnet that communicates on the private subnet. a. Click the Public to Private tab. b. Click New Entry. c. Do one of the following: – To translate one address for a device on the public subnet that communicates on the private subnet, see Table 74. – To translate a range of addresses for devices on the public subnet that communicates on the private subnet, see Table 75. – To translate all addresses on the public subnet or a portion of the public subnet that communicates on the private subnet, see Table 76. d. Click OK.

Table 71 - Single Translation–Private to Public 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 72 - Range Translation–Private to Public 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 73 - Network Translation–Private to Public 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. See Table 77.
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. See Table 77.
Subnet Mask	Choose the subnet mask for the addresses to translate. Valid values: • 255.255.0.0 • 255.255.255.0 • 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.

Table 74 - Single Translation—Public to Private 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 75 - Range Translation—Public to Private 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 76 - Network Translation—Public to Private Translation

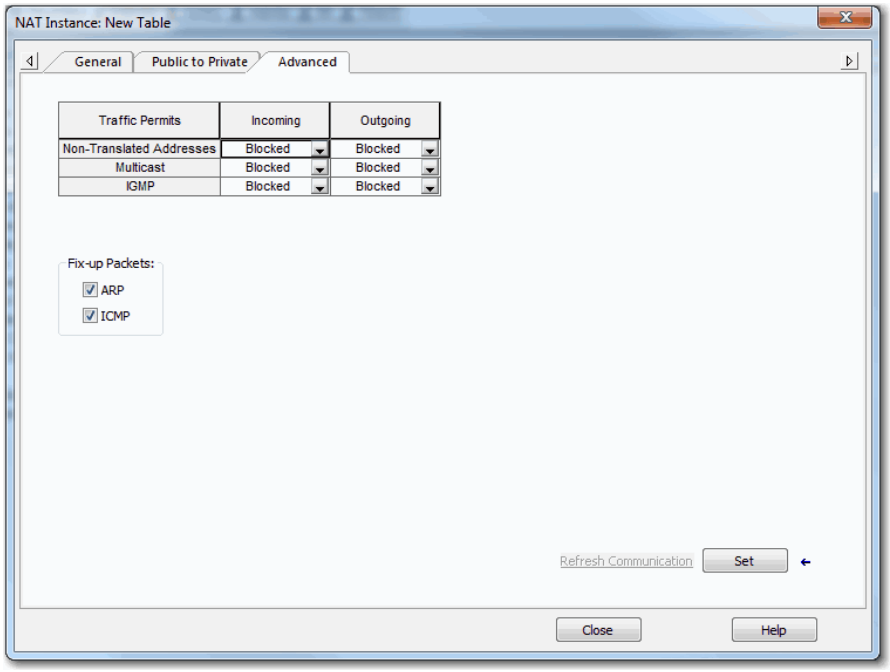
Field	Description
Type of Entry	Choose Subnet.
Starting Public IP Address	Type the existing starting address for a device on the public subnet. This address must correspond to the size of the subnet mask to translate. See Table 77.
Starting Private IP Address	Type a unique, starting private address to represent the devices. This address must correspond to the size of the subnet mask to translate. See Table 77.
Subnet Mask	Choose the subnet mask for the addresses to translate. Valid values: • 255.255.0.0 • 255.255.255.0 • 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.

Table 77 - Subnet Mask Starting Address

Subnet Mask	Subnet Address
255.255.0.0	The last two octets must end in 0. **EXAMPLES:** 192.168.0.0 or 10.200.0.0
255.255.255.0	The last octet must end in 0. **EXAMPLES:** 192.168.1.0 or 10.200.1.0.
255.255.255.128	The last octet must end in 0 or 128. **EXAMPLES:** 192.168.1.0 or 192.168.1.128; 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. **EXAMPLES:** 192.168.1.64 or 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. **EXAMPLES:** 192.168.1.32 or 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. **EXAMPLES:** 192.168.1.16 or 10.200.1.16

Configure Traffic Permits and Fixups

1. From the NAT Instance view, 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.
4. Click Set.

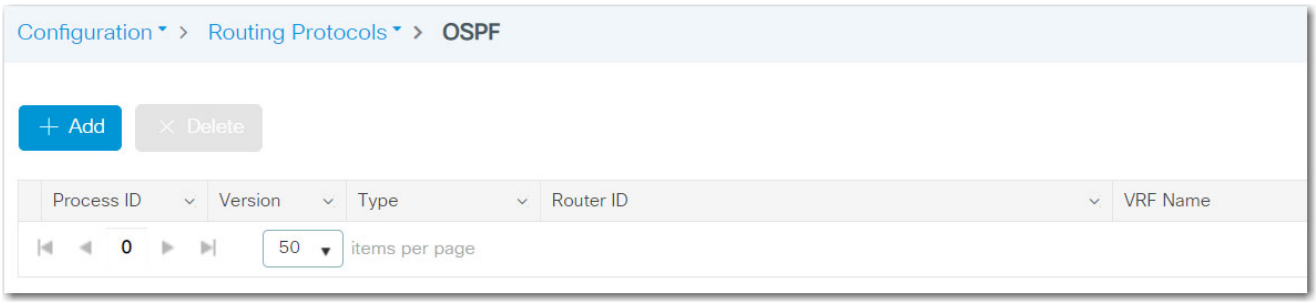
Open Shortest Path First (OSPF) Routing Protocol (Stratix 5800 Switch Only)

OSPF is a standards-based routing protocol that uses the Shortest Path First (SPF) algorithm to determine the best route to its destination. 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.

IMPORTANT OSPF is available only on select modular switch models. For supported catalog numbers, see Table 1 on page 15.

Create an OSPF Route via the WebUI

From the Configuration menu, choose OSPF.



From the OSPF page, you can add, edit, and delete OSPF routes:

- To add a route, click Add, complete the fields as described in Table 78 for OSPF or Table 79 for OSPFv3, and then click Apply to Device.
- To edit a route, click the route in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a route, check its associated checkbox in the grid, and then click Delete.

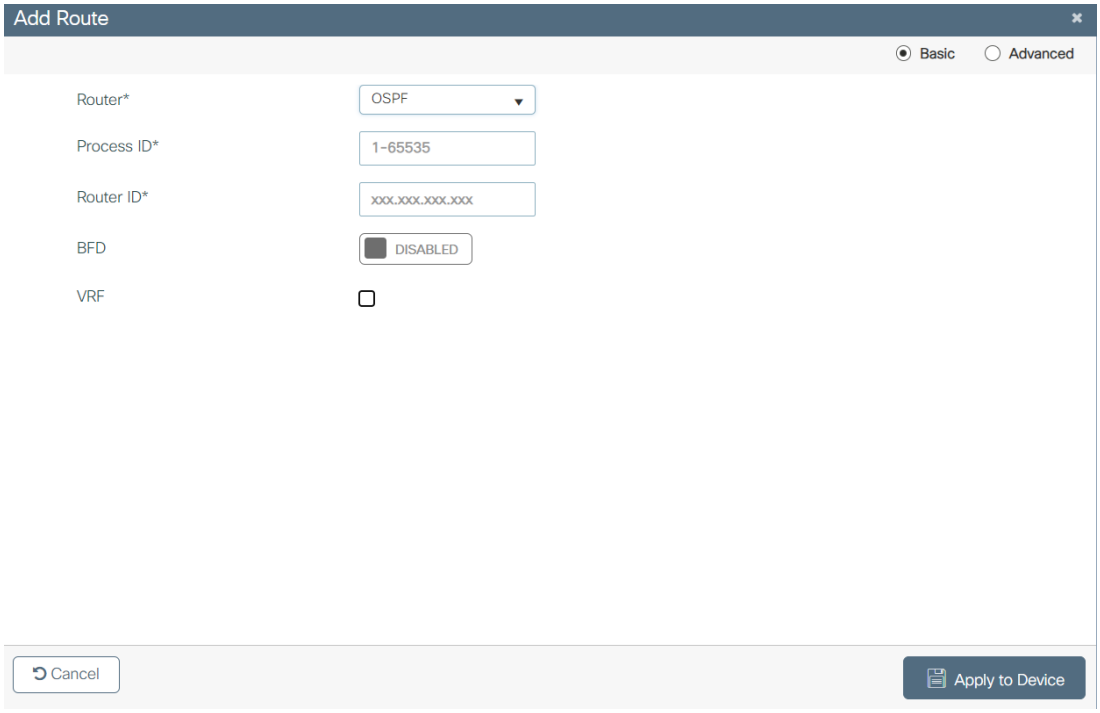


Table 78 - Add Route—OSPF

Field	Description
Basic or Advanced	Click to determine the level of configuration: • Basic—The page displays only basic configuration fields. Basic is the default value. • Advanced—The page displays both basic and advanced configuration fields.
Basic Settings	
Router	Choose OSPF.
Process ID	Enter a unique process ID to enable other routers to identify the OSPF routing process of this router.
Router ID	Enter a unique router ID for the OSPF process.
BFD	Disabled by default.
VRF ((Stratix 5800 Switch Only)	To create a virtual routing and forwarding (VRF) interface for the OSPF process, check the VRF checkbox, and then enter a name to identify the VRF interface.
Advanced Settings	
Network	1. In the IP Address field, enter the IP address of the destination network for this route. 2. In the Wildcard field, enter the subnet mask that is used on that network. 3. In the Area field, enter the OSPF area number for the network. Each router in a particular OSPF area maintains a topological database for that area. 4. Click + to add the network information to the grid.

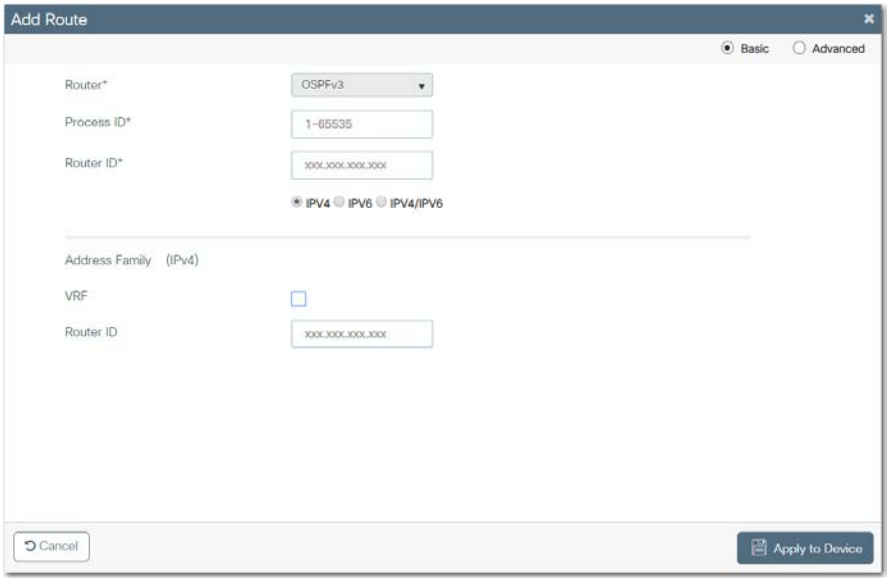


Table 79 - Add Route—OSPFv3

Field	Description
Basic or Advanced	Click to determine the level of configuration: • Basic—The page displays only basic configuration fields. Basic is the default value. • Advanced—The page displays both basic and advanced configuration fields.
Basic Settings	
Router	Enter a unique process ID to enable other routers to identify the OSPFv3 routing process of this router.
Process ID	Enter a unique router ID for the OSPFv3 process.
Router ID	1. Enter a unique router ID for the OSPFv3 process. 2. Choose IPV4, IPV6, or IPV4/IPV6.
Address Family	
VRF (Stratix 5800 Switch Only)	A VRF must be created based on type (IPv4, IPv6, and IPv4/IPv6) if none is available in the device. Otherwise, the VRF option is not selectable. Check VRF to specify an OSPF VPN routing and forwarding (VRF) instance, and then enter the VRF name.

Table 79 - Add Route—OSPFv3

Field	Description
Router ID	Enter the IP address of the router associated with the OSPFv3 route.
Advanced Settings	
Area	1. In the Area field, enter the OSPF area number for the network. Each router in a particular OSPF area maintains a topological database for that area. 2. Choose Stub. Stub areas are areas into which information on external routes is not sent. 3. Click + to add the area information to the table.

Parallel Redundancy Protocol (PRP)

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 interfaces (Gi1/1 & Gi1/3)	Redundant, active Ethernet networks that operate in parallel.
LAN-B interfaces (Gi1/2 & Gi1/4)	
Double attached node (DAN)	An end device with PRP technology that connects to both LAN A and LAN B.
Single attached node (SAN)	An end device without PRP technology that connects to either LAN A or LAN B. A SAN does not have PRP redundancy.
Redundancy box (RedBox)	A switch with PRP technology that connects devices without PRP technology to both LAN A and LAN B.
Virtual double attached node (VDAN)	An end device without PRP technology that connects to both LAN A and LAN B through a RedBox. A VDAN has PRP redundancy and appears to other nodes in the network as a DAN.
Infrastructure switch	A switch that connects to either LAN A or LAN B and is not configured as a RedBox.

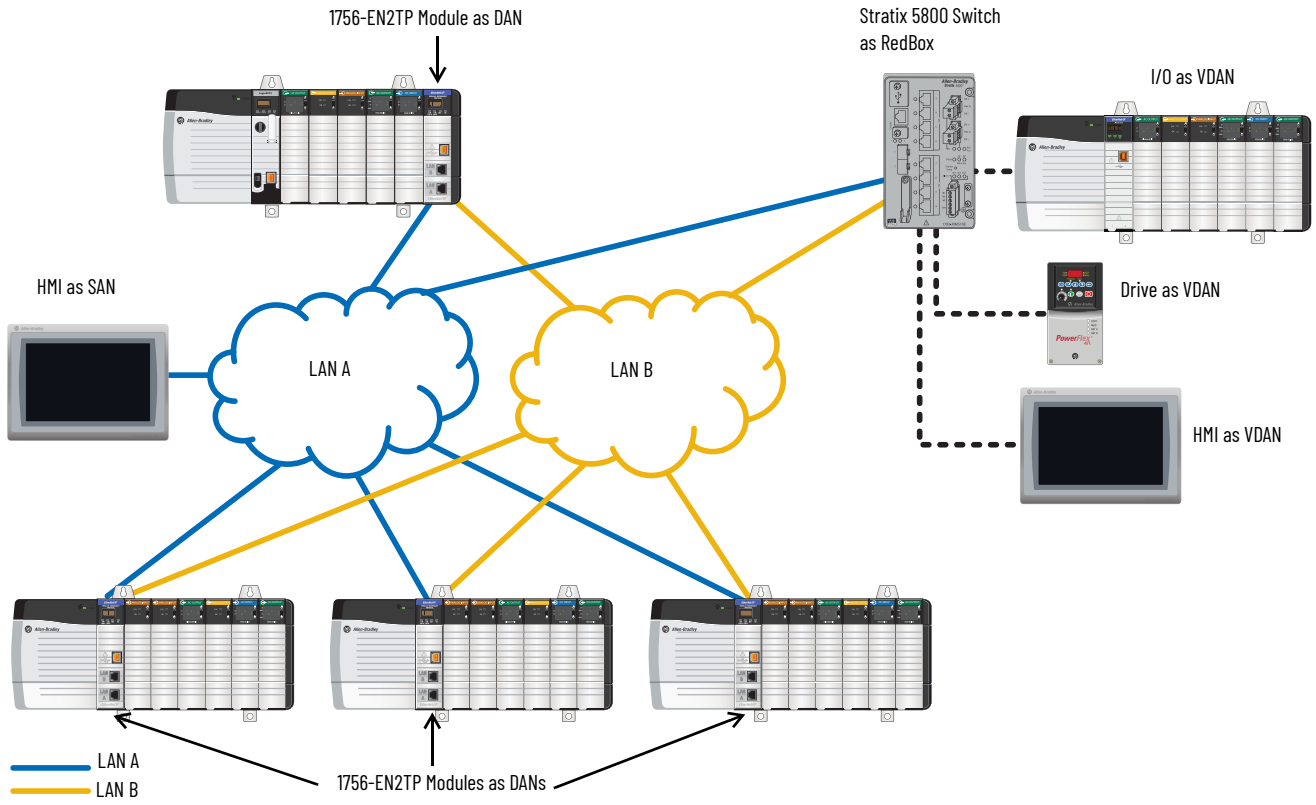
For more information about PRP, see the EtherNet/IP Parallel Redundancy Protocol Application Technique, publication ENET-AT006.

IMPORTANT PRP is available only on select modular switch models. For supported catalog numbers, see Table 1 on page 15.

Figure 30 illustrates the Stratix 5800 switch as RedBox.

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

Figure 30 - PRP Topology with Stratix 5800 Switch as RedBox



RedBox PRP Channel Groups

For RedBox functionality, Stratix 5200 (Advanced 5200 PIDs) and 5800 switches have designated ports for PRP channel groups. A PRP channel or channel group is a logical interface that aggregates two Gigabit Ethernet interfaces (access, trunk, or routed) into one link. In the channel group, the lower numbered Gigabit Ethernet member port is the primary port and connects to LAN A. The higher numbered port is the secondary port and 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 total number of supported PRP channel groups is 1 per switch for the Stratix 5200 switch and 2 per switch for the Stratix 5800 switch.

There are two pairs of port that can be used for channel group 1:

- Gi1/1 LAN A and Gi1/2 LAN B
- Gi1/3 LAN A and Gi1/4 LAN B (Stratix 5800 Switch Only)

Channel 2 can only be configured on a 1783-MMX8EA, 1783-MMX8SA, or 1783-MMX8TA expansion module. The only two ports that can be used are Gi2/1 LAN A and Gi2/2 LAN B.

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

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

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

Configure a Switch as a RedBox via the WebUI

From the Configuration menu, choose PRP.

Figure 31 - Stratix 5200 PRP Configuration

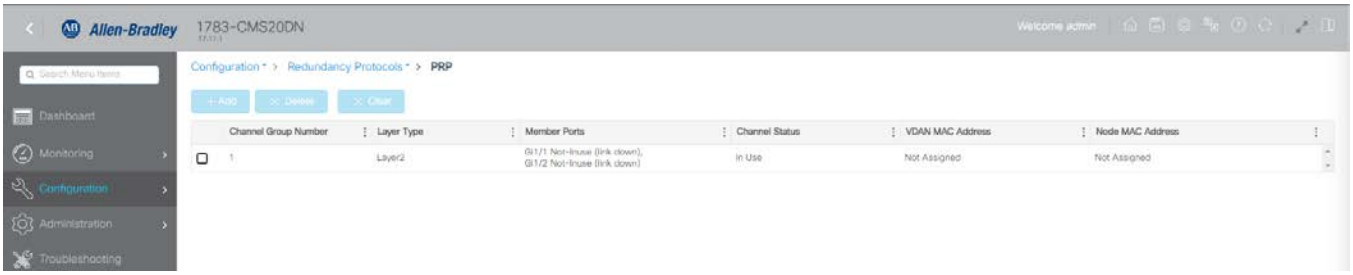
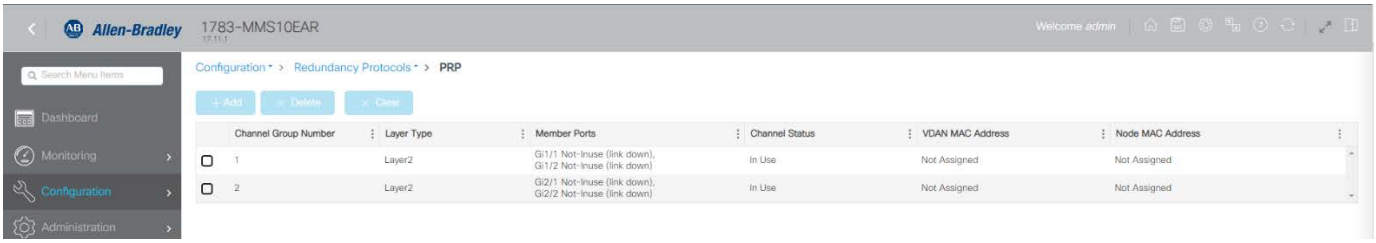


Figure 32 - Stratix 5800 PRP Configuration



From the PRP page, you can add, edit, and delete channel groups and clear dynamic VDAN and Node table entries:

- To add a channel group, click Add, complete the fields as described in Table 80, and then click Apply to Device.
- To edit a channel group, click the channel in the grid, modify the fields, and then click Update & Apply to Device.
- If you have an advanced expansion module, you can add a second channel group (Stratix 5800 Switch Only).
- To delete a channel group, check its associated checkbox in the grid, and then click Delete.
- To clear all dynamic entries from the VDAN and Node tables, check the associated checkbox for one or both channels in the grid, and then click Clear. On the dialog box that appears, select whether to clear entries from the VDAN table, Node table, or to clear all entries, and then click Save & Apply to Device.

Figure 33 - PRP Configuration

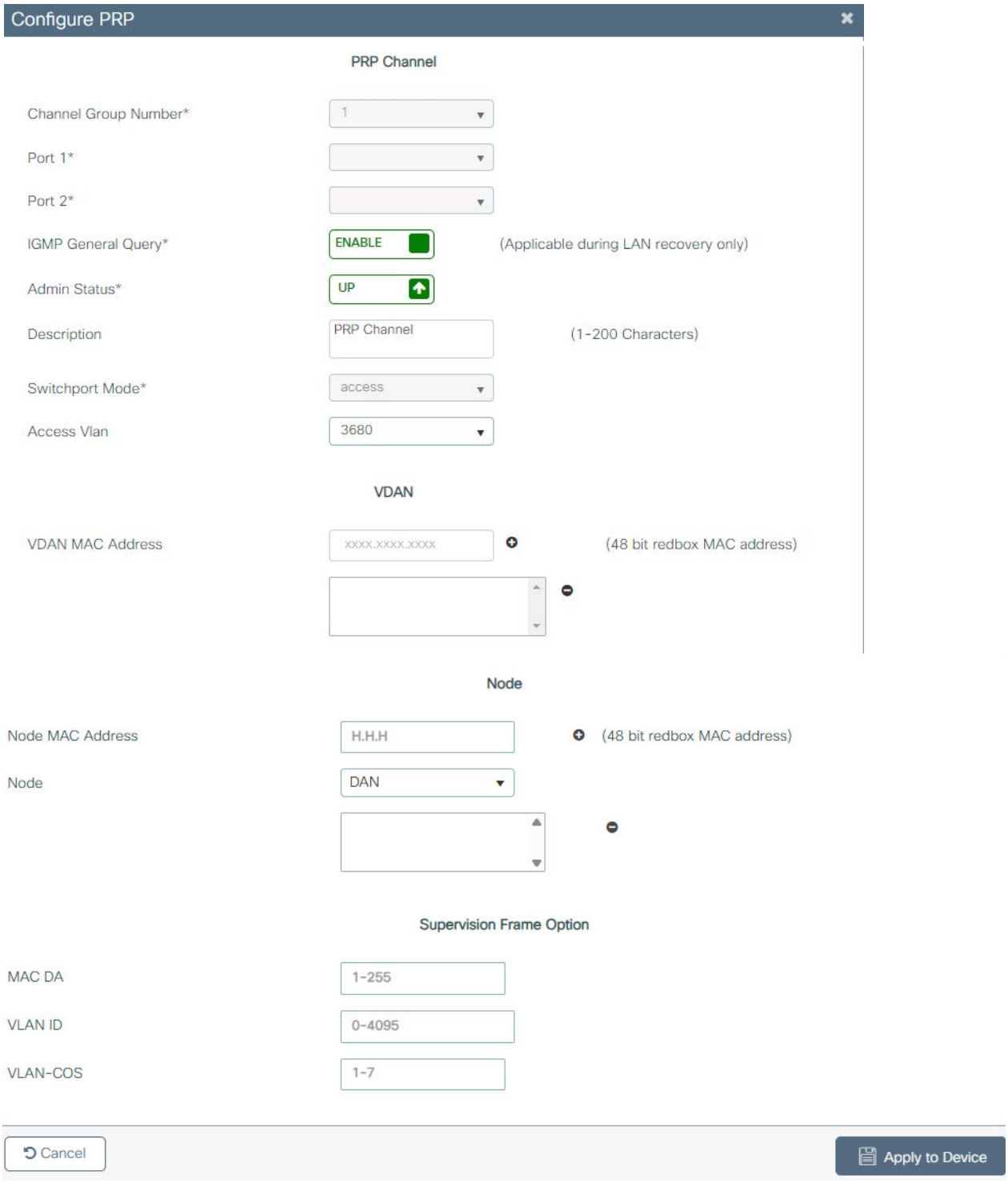


Figure 34 - PRP Configuration (Stratix 5800 Only)



Table 80 - Configure PRP

Field	Description
PRP Channel	
Channel Group Number(1)	Choose an available channel group number. Valid values: 1 or 2 (Channel group 2 can only be configured on a 1783-MMX8EA or 1783-MMX8SA expansion module.
Port 1	There are two pairs of port than can be used for channel group 1: • Option 1: Gi1/1 • Option 2: Gi1/3 (Stratix 5800 Switch Only) Channel 2 can only be configured on a 1783-MMX8EA or 1783-MMX8SA expansion module. The fixed port is Gi2/1
Port 2	(System-generated). Displays the port assignment for LAN B: • Channel Group 1 – Option 1: Gi1/2 – Option 2: Gi1/4 (Stratix 5800 Switch Only) • Channel 2 can only be configured on a 1783-MMX8EA or 1783-MMX8SA expansion module. The fixed port is Gi2/2.
IGMP General Query	Click whether to enable or disable the RedBox from sending 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. By default, general queries are disabled.
Admin Status	Click whether to activate the switch ports in the channel group: • Up—The ports are active. • Down—The ports are inactive.
Description	Enter a description for the channel group. The description can contain a maximum of 200 characters.
Administrative Mode	Choose one of the following modes for the PRP channel group: • access—The channel group carries traffic for one VLAN. • trunk—The channel group carries traffic for multiple VLANs. • routed—Layer 3(2)
Access VLAN	(Access mode only). Choose the VLAN to which the PRP channel group belongs. Default value: 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—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. Enter 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. Default value: 1
IP Assignment Mode(2)	(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. Enter the IP address and the subnet mask. • DHCP—Allow a DHCP server to assign an IP address automatically.
VDAN—Add static entries to the VDAN table.	
VDAN MAC Address	Enter the MAC ID of the VDAN to add, and then click the plus (+) sign. To delete a VDAN, click the minus (-) sign.
Node—Add static entries to the Node table.	
Node MAC Address	Enter the MAC ID of the DAN or SAD to add, and then click the plus (+) sign. To delete a DAN or SAN, click the minus (-) sign.
Node	Choose the type of PRP node: • DAN—Double attached node. • LAN-A (SAN-A)—Single attached node on LAN A. • LAN-B (SAN-B)—Single attached node on LAN B.
Supervision Frame Option	
MAC DA	• Specify the last 8 bits of the supervision frame MAC DA. • Value: 1...255

Table 80 - Configure PRP (Continued)

Field	Description
VLAN ID	• Set the VLAN ID to be used in VLAN tags for supervision frames. • Value 0...4095
VLAN-COS	• Enter the Class of Service (COS) value to be set in the VLAN tag of the supervision frames. • Value: 1...7
VLAN-Tagged(2)	• Enable the toggle button to allow supervision frames to be tagged with VLAN IDs.
VLAN-Aware(2)	• Enable the toggle button to turn on the VLAN awareness feature which ensures supervision frames are sent with tags matching the VLAN of the associated VDAN.
VLAN Aware Reject Untagged(2)	• Enable the toggle button to reject untagged supervision frames from being displayed in the node table.
VLAN Aware Allowed VLAN(2)	• Specify the VLANs to be recorded in the node table.

(1) Only 1 channel for the Stratix 5200 switch.
(2) Only for the Stratix 5800 switch.

Port Security

You can configure port security based on the MAC ID of the switch. 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.

Configure Port Security via the WebUI

In the WebUI, you can configure port security in the advanced settings for Ethernet ports. See Advanced Port Configuration on page 89.

Configure Port Security via the Logix Designer Application

In the navigation pane, click Port Security.

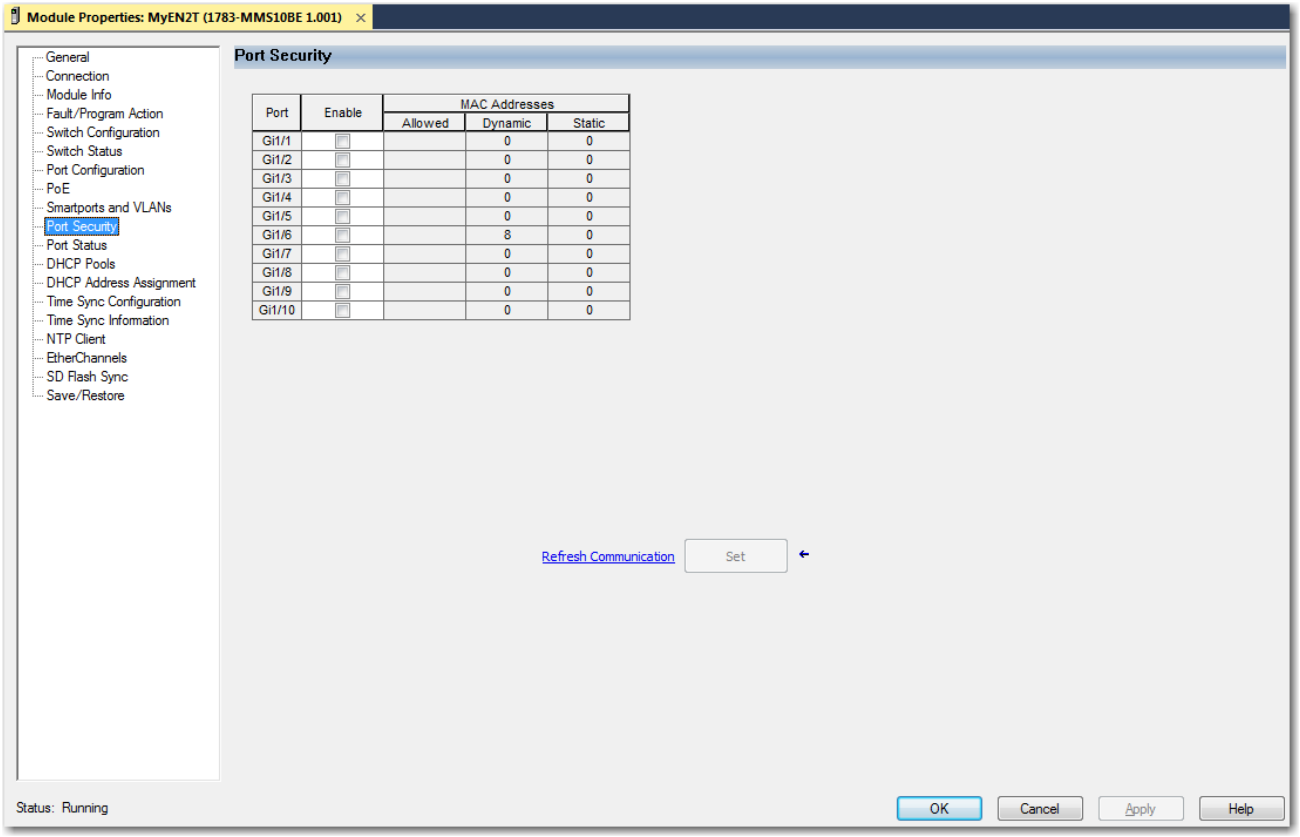


Table 81 - Port Security

Field	Description
Port	Displays the port type and number.
Enable	To enable or disable port security on a port, check or clear its associated checkbox on the grid.
MAC Addresses	The number of supported dynamic or static MAC IDs. • Allowed—1...80. • Dynamic—The number of dynamically defined MAC IDs (devices) currently connected to the port. • Static—The number of statically defined MAC IDs (devices). This number must be greater than the sum of the numbers in the Dynamic and Static fields for a port. To set the number to less, disconnect the devices and let their entries in the port security table time out.

Quality of Service (QoS)

QoS determines how packets are marked, classified, and treated. Allen-Bradley EtherNet/IP™ devices prioritize traffic internally. QoS implementations at the switch level add another level of prioritization. QoS does not increase bandwidth—QoS gives preferential treatment to some network traffic at the expense of others. For more information about QoS, see the Ethernet Reference Manual, publication ENET-RM002.

QoS is supported on both Layer 2 and Layer 3 interfaces.

Auto QoS Macros

Table 82 describes QoS macros available on the switch. You can apply a QoS macro when you enable the Auto QoS feature via the WebUI for the switch.

Table 82 - QoS Macros

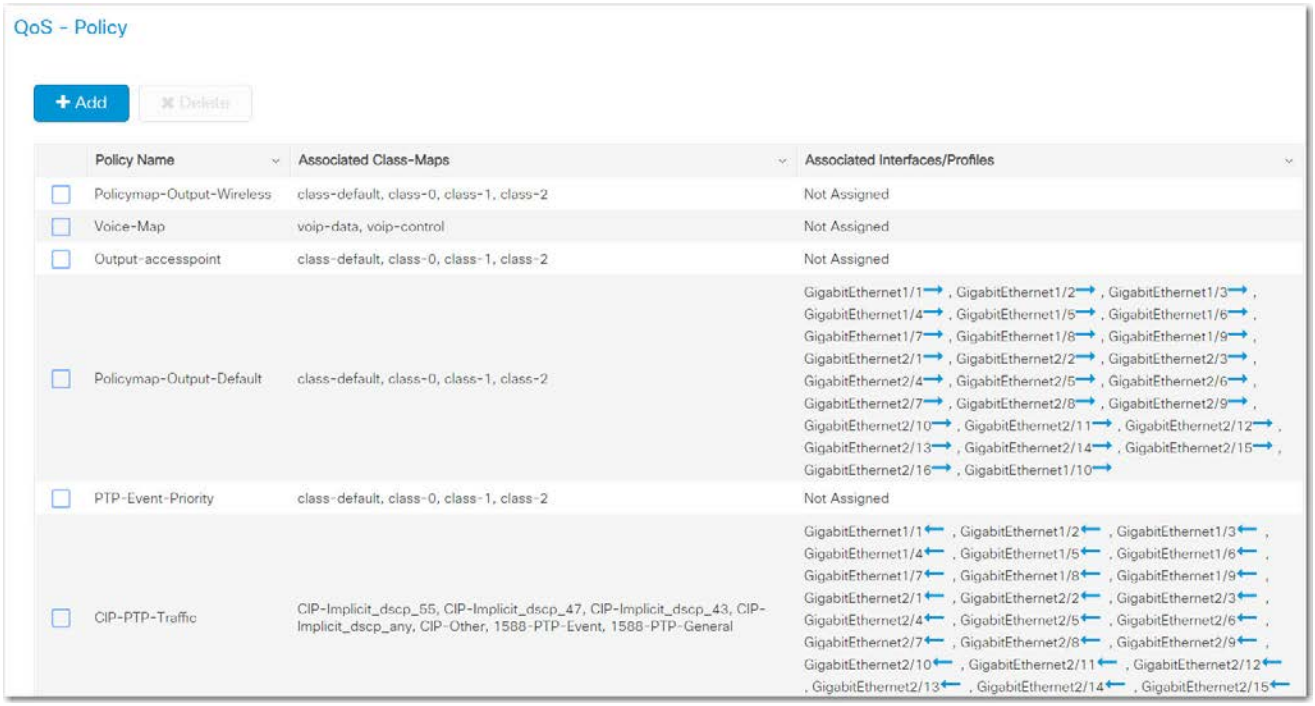
Macro	Description
classify police	Automatically configures QoS policing for untrusted devices within a QoS domain.
classify	Automatically configures QoS classification for untrusted devices within a QoS domain.
trust cos	Trusts the CoS packet classification.
trust dscp	Trusts the Differentiated Services Code Point (DSCP) packet classification.
trust	Automatically configures QoS classification for trusted devices within a QoS domain.
video cts	Specifies a port that is connected to a TelePresence System and automatically configures QoS for video.
video ip-camera	Specifies a port that is connected to an IP camera and automatically configures QoS for video.
video media-player	Specifies a port that is connected to a CDP-capable digital media player and automatically configures QoS for video.
voip phone	Specifies a port that is connected to an IP phone, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted only when the telephone is detected.
voip softphone	Specifies a port that is connected to a device running SoftPhone, and automatically configures QoS for VoIP.
voip trust	Specifies a port that is connected to a trusted device, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

Configure QoS via the WebUI

You can use standard QoS, or you can use Auto QoS to simplify the deployment of QoS features. Auto QoS determines the network design and enables QoS configurations so that the switch can prioritize different traffic flows.

You can enable or disable Auto QoS on a per-port basis in the advanced settings for Ethernet ports. See Advanced Port Configuration on page 89.

From the Configuration menu, choose QoS.



From the QoS page, you can add, edit, and delete QoS policies:

- To add a policy, click Add, complete the fields as described in Table 83, and then click Save & Apply to Device.
- To edit a policy, click the policy in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a policy, check its associated checkbox in the grid, and then click Delete.

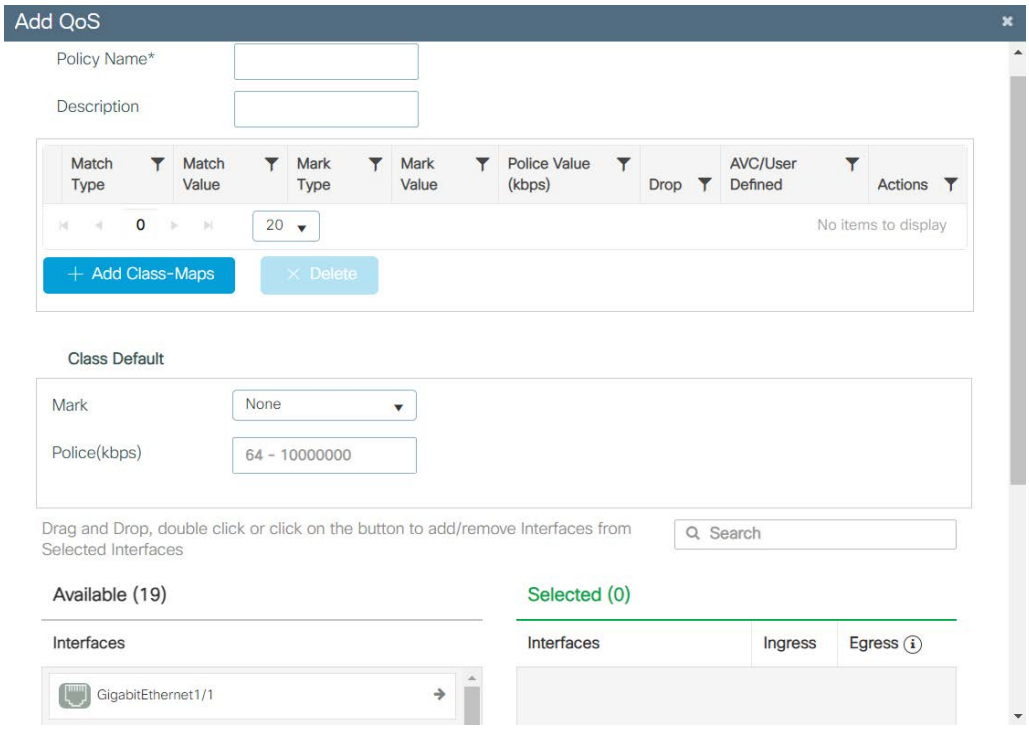


Table 83 - Add QoS

Field	Description
Auto QoS	Click to enable or disable Auto QoS. Default value: Disabled
Auto QoS Macro	(Appears only if Auto QoS is enabled). Choose a policy to apply to interfaces on the switch. For a description of each policy, see Table 82 on page 163.
Policy Name	Enter a name to identify the QoS policy.
Description	Enter a description for the QoS policy.
+ Add Class-Maps—Click to name a specific traffic flow (or class) and isolate it from all other traffic. The class map defines the criteria that are used to match against a specific traffic flow to classify it. Configure the following fields, and then click Save to save the class map.	
AVC/User Defined	Choose
Match	If any one of the match criteria must be met to classify traffic as part of the traffic class, click Any. If all match criteria must be met to classify traffic as part of the traffic class, click All.
Match Type	Choose the type of protocol to match: • DSCP • ACL
Match Value	Enter a value to specify the differentiated services code point value. Valid values: 0...63
Mark Type	Choose the type of marking label for packets: • None • DSCP
Police (kbps)	Enter the policing rate. Valid values: 64...10000000

Table 83 - Add QoS (Continued)

Field	Description
Class Default—The class default is used to match all unclassified packets.	
Mark	Choose • None • DSCP
Police (kbps)	Enter a Valid values: 64...10000000
Available Selected	To attach the policy to interfaces, click to move the interfaces from the Available list to the Selected list. To specify the direction in which the policy is applied, check the checkboxes for Ingress or Egress.

Remote Switch Port Analyzer (RSPAN)

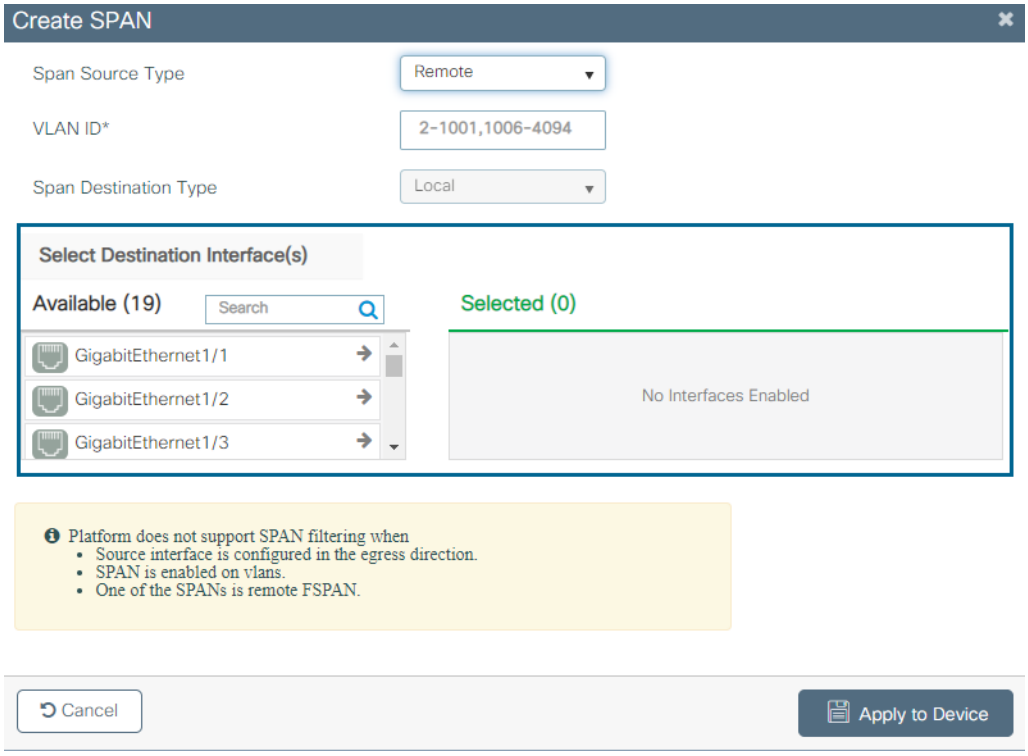
You can analyze network traffic passing through ports or VLANs by using Switched Port Analyzer (SPAN) or Remote SPAN (RSPAN) to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. You can use SPAN for troubleshooting connectivity issues and calculating network utilization and performance.

Configure RSPAN via the WebUI

From the configuration menu, choose SPAN.



In the Create SPAN window, select the Span Source Type, Remote.



To configure the RSPAN, use the following steps:

1. For remote source, enter the VLAN ID of the remote source interface.
2. From the list of available interfaces on the left, select a destination interface and click the arrow to add it to the selected list on the right.
3. When you are finished, Click Apply to Device.

Resiliency 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 also provides a basis for constructing more complex networks and supports VLAN load balancing. For more information about REP, see the Ethernet Reference Manual, publication ENET-RM002.

Default REP Configuration

REP is disabled on all interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.

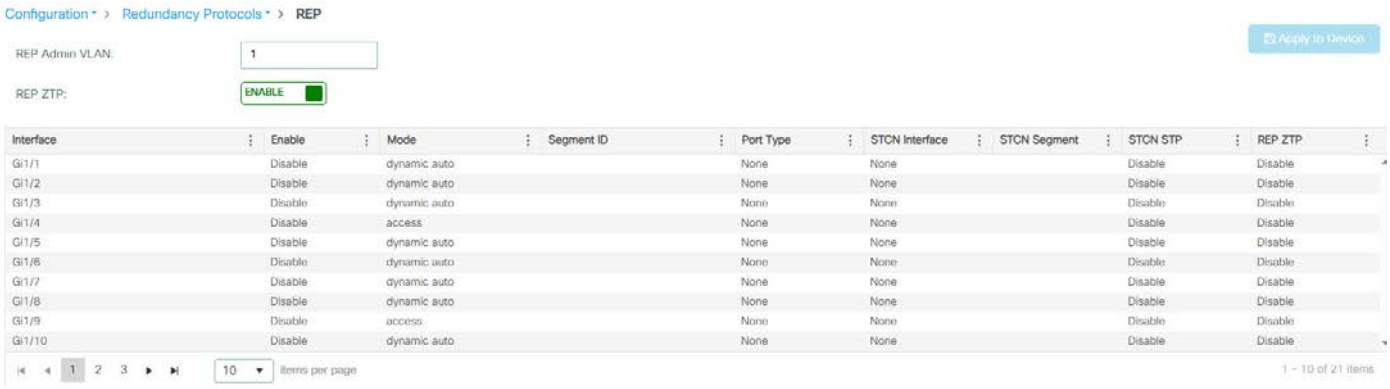
When REP is enabled, the task of sending a segment topology change notice (STCN) is disabled, all VLANs are blocked, and the administrative VLAN is VLAN 1.

When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all VLANs in the primary edge port.

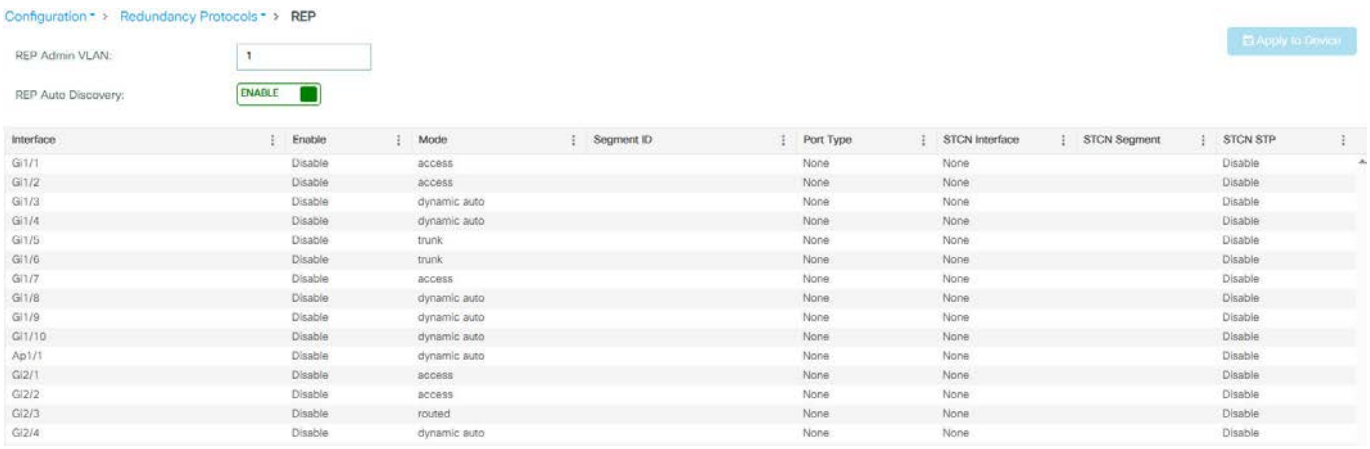
REP Over Port Channel

REP controls a group of ports connected in a segment, makes sure that the segment does not create any bridging loops, and responds to link failures in the segment.

Stratix 5200 Switch



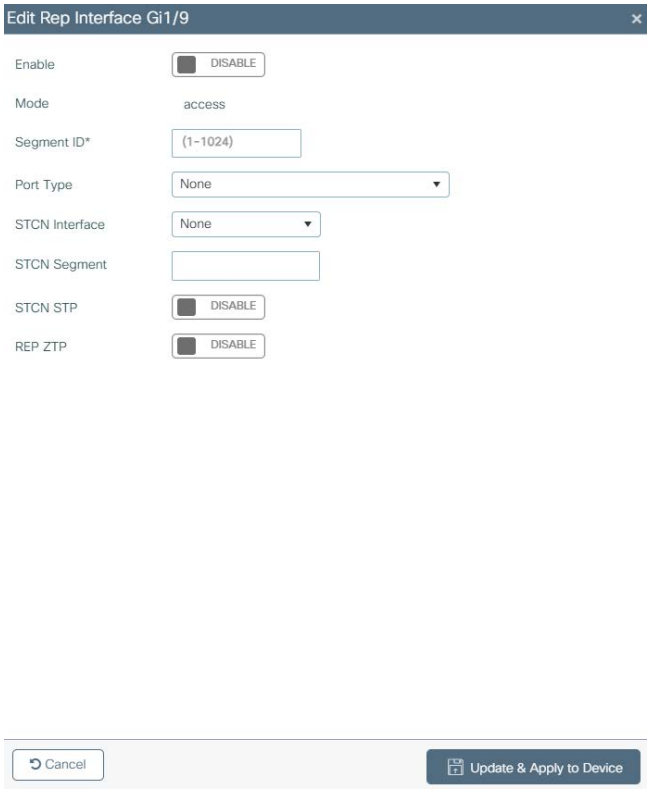
Stratix 5800 Switch



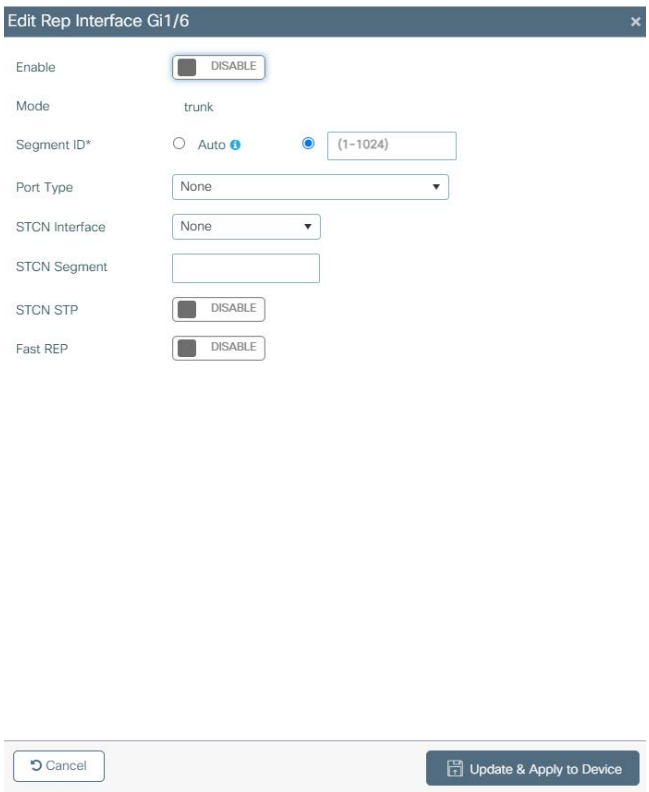
The REP configuration screen is shown under the Configuration tab in Redundancy Protocols.

From there, you can reach the REP screen. This screen currently shows physical interfaces and port channels.

Stratix 5200 Switch



Stratix 5800 Switch



Configuring the REP Administrative VLAN

To avoid the delay created by link-failure messages, and VLAN-blocking notifications during load balancing, REP floods packets to a regular multicast address at the hardware flood layer. These messages are flooded to the whole network, and not just the REP segment. You can control the flooding of these messages by configuring an administrative VLAN for the whole domain or for a particular segment.

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default is VLAN 1.
- You can configure one admin VLAN on the switch for all segments or configure an admin VLAN per segment.
- The administrative VLAN cannot be the RSPAN VLAN.

REP Port Types

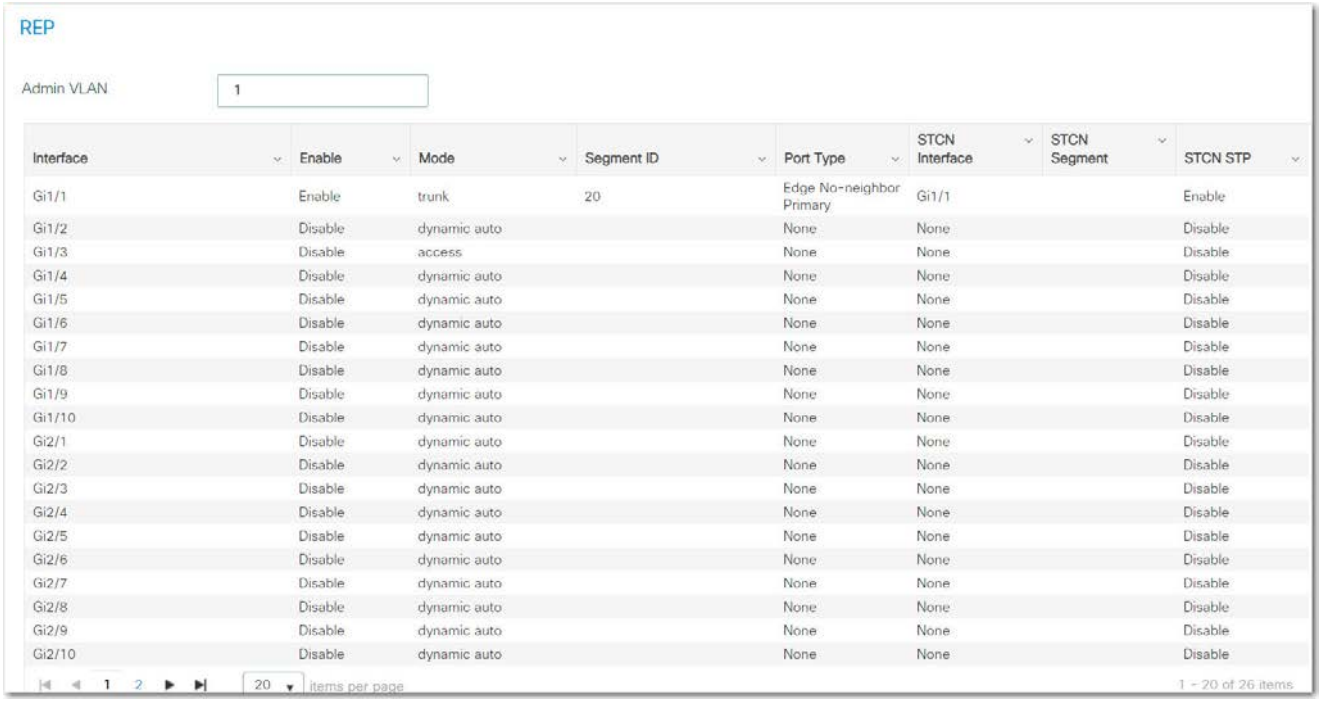
Table 84 describes the types of REP ports available for configuration.

Table 84 - REP Port Types

REP Port Type	Description
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.
Preferred	A secondary edge port that is the preferred alternate port for VLAN load balancing.
Edge No-neighbor Preferred	A secondary edge port that is connected to a non-REP switch and is the preferred 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	A non-edge port in the REP segment. The default port type is None.

Configure REP via the WebUI

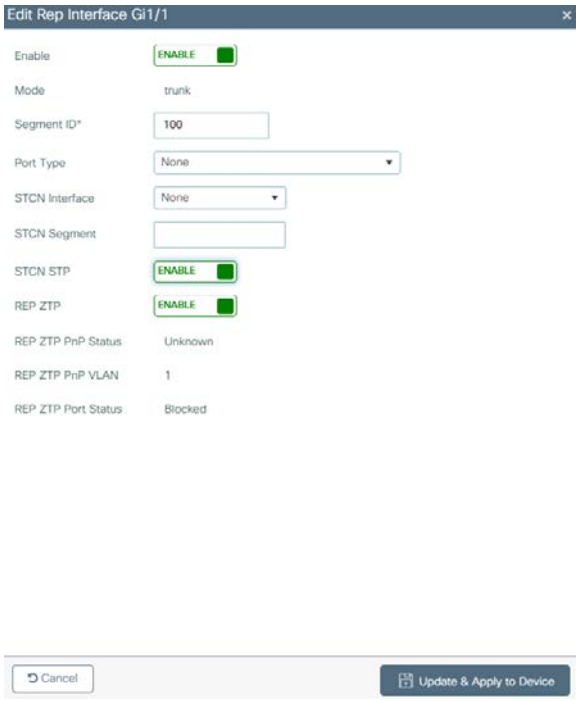
From the Configuration menu, choose REP.



From the REP page, you can specify the administrative VLAN for all REP segments or edit the REP configuration for an interface:

- To change the administrative VLAN, enter a VLAN ID in the Admin VLAN field:
  - The default administrative VLAN is 1.
  - Valid values are 2...4094.
- To edit the REP configuration for an interface, click the interface, modify the fields as described in Table 85, and then click Update & Apply to Device.

Stratix 5200 Switch



Stratix 5800 Switch

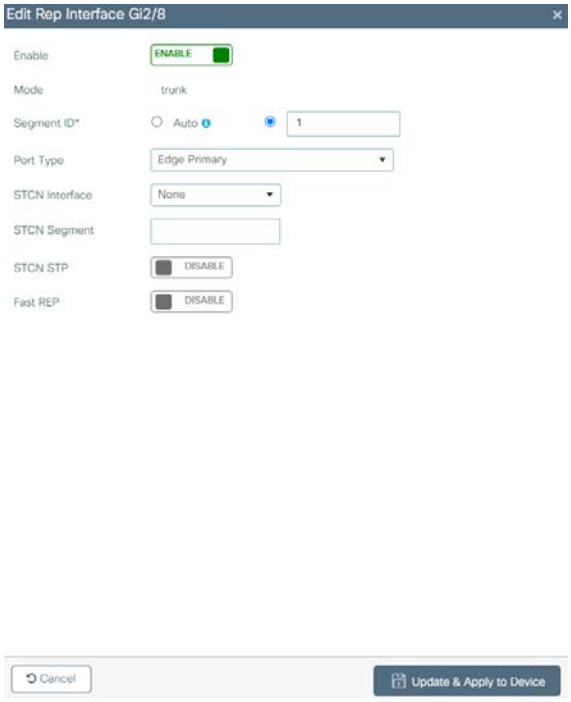


Table 85 - Edit REP Interface

Field	Description
Enable	Click to enable or disable REP on the interface. When enabled, the interface is a regular segment port unless it is configured as an edge port. Default value: Disabled
Mode	(System-generated). Displays the Switchport mode that is configured for the interface. You can configure the Switchport mode in the basic settings for Ethernet ports. See Ethernet Ports on page 89.
Segment ID	Enter the segment ID. Valid values: 1...1024
Port Type	Choose a REP port type. For a description of REP port types, see Table 84 on page 171.
STCN Interface	(Optional) Choose a physical interface to receive segment topology change notices (STCNs).
STCN Segment	(Optional) Enter one or more segments to receive STCNs. Valid values: 1...1024
STCN STP	Click to enable or disable STCNs on STP networks. Spanning Tree (MST) mode is required on edge no-neighbor nodes to send STCNs to STP networks.
Fast REP (Stratix 5800 Switch Only)	REP Fast works on a per link basis. It does not impact the REP Protocol. REP Fast requires both ends of the link to support REP Fast to work.
REP ZTP(1)	REP ZTP automates bringing up network devices into a functional state with minimal to no manual configuration.
REP ZTP PnP Status	• Unknown • In-Progress
REP ZTP PnP VLAN	
REP ZTP Port Status	• Blocked • Unblocked

(1) REP ZTP works on both the Stratix 5200 switch and the Stratix 5800 switch, but can only be configured with WebUI on the Stratix 5200 switch.

Routing Information Protocol (RIP)

RIP is a commonly used routing protocol in small to medium TCP/IP networks. It is a stable protocol that uses a distance-vector algorithm to calculate the best route to a destination based on the number of hops in the path.

Configure RIP for Stratix 5800 Switch via WebUI

On the Configuration > Routing Protocols > RIP page, configure the device to receive and send only RIP Version 1 or RIP Version 2 packets. By default, the device receives Version 1 and 2 but sends only Version 1.

Figure 35 - Basic RIP Configuration IPv4

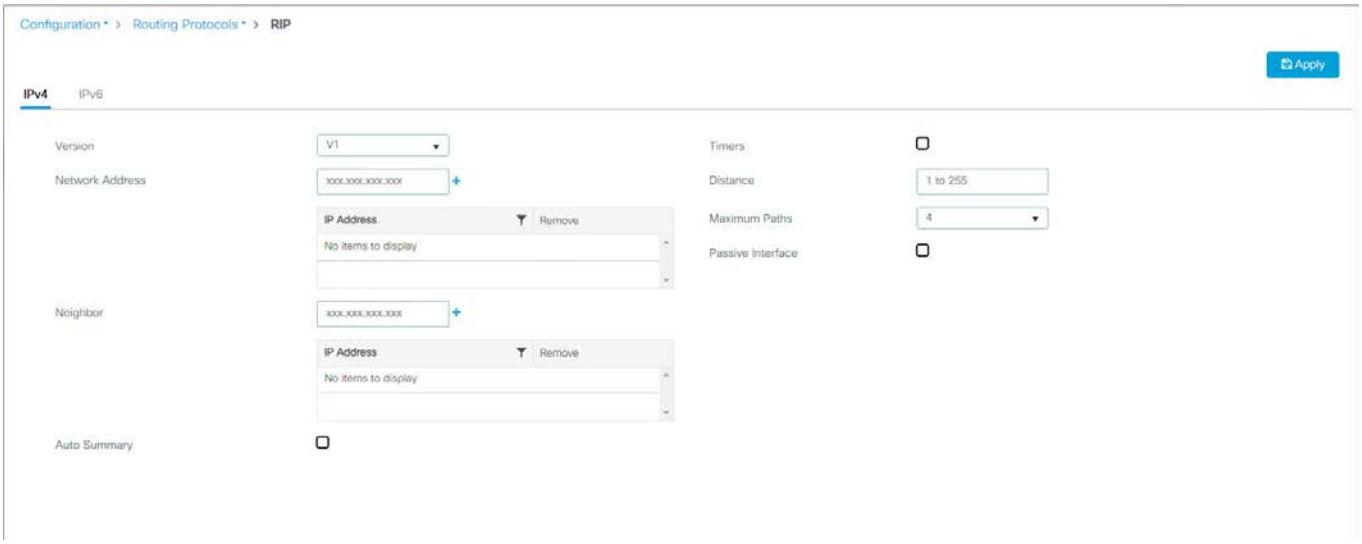


Figure 36 - Basic RIP Configuration IPv6



Table 86 - Basic RIP Configuration Fields

Field	Description
Version	Choose one of the following firmware revisions for your RIP configuration: • V1 - Does not support authentication of update messages (plain-text or MD5). • V2 - Supports plain text and message digest algorithm 5 (MD5) authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).
Network Address	Enter the network address to associate a network with a RIP routing process, and click + to add the address.(1)
Neighbor	Enter the IP address of a neighboring device to exchange routing information, and click + to add the address.
Disable RIP	Completely removes RIP configurations.

(1) You can specify multiple network addresses. RIP routing updates are sent and received through interfaces only on these networks.

Smartports

Smartports are recommended configurations for switch ports. These configurations, called Smartport roles, optimize the switch connections and provide security, transmission quality, and reliability for traffic from the switch ports. Smartport roles also help prevent port misconfigurations.

Requirements and Restrictions

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

Observe these guidelines:

- We recommend that you do not change port settings after assigning a Smartport role. Any port setting changes can alter the effectiveness of the Smartport role.
- Before assigning Smartport roles, decide which switch port is connected to which device type.
- Before attaching a device to the port or reconnecting any devices that have been moved, verify which Smartport role is assigned to a port.
- You cannot assign Smartport roles to routed ports.

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 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

Before you attach a device to a port, verify which Smartport role is assigned to the port.

Smartport Roles

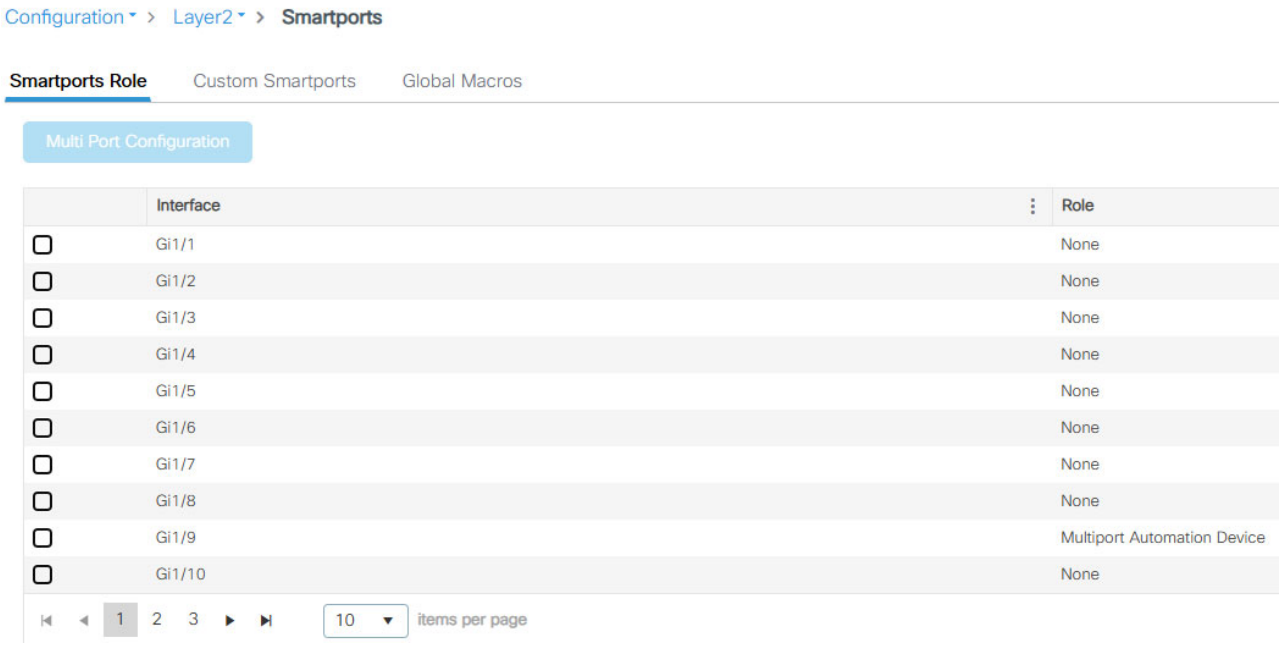
Table 88 describes the Smartport roles that you can assign to switch port. The port roles are based on the type of devices that connect to the switch ports. For example, the Desktop for Automation port role is specifically for switch ports to be connected to desktop and laptop computers.

You can create a maximum of 10 custom Smartport roles for various custom applications.

The default Smartport role is None.

Assign Smartport Roles via the WebUI

From the Configuration menu, choose Smartports.



From the Smartports page, you can assign Smartports roles and configure Custom Smartports roles:

- To assign a Smartports role, see page 177.
- To configure Custom Smartports roles, see page 179.
- To configure Multiple Port Configuration, see page 92.

VLAN Type

When you assign a Smartport role to one or more ports, you must also assign a VLAN. Table 87 describes the types of VLANs you can assign depending on the type of Smartport role. For example, if you choose the Phone for Automation role, you can assign an access VLAN and a voice VLAN.

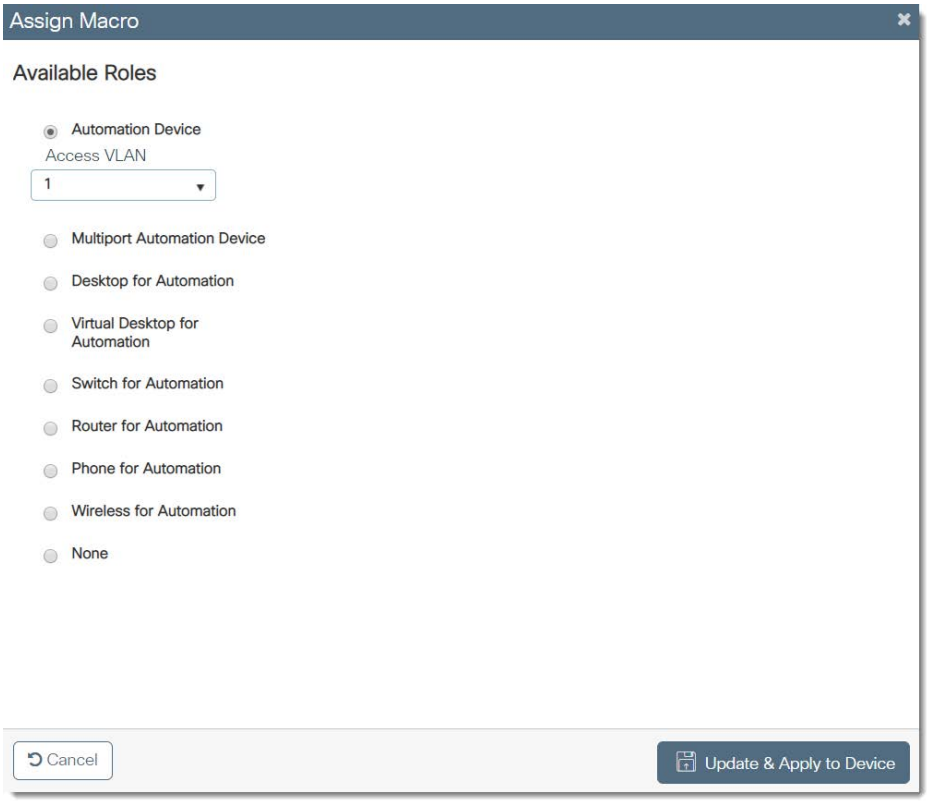
Table 87 - VLAN Type

VLAN Type	Description
Native	A native VLAN is for ports that can belong to a VLAN trunk (a port belonging to multiple VLANs). The native VLAN for ports that are assigned to these Smartport roles: • Switch for Automation • Router for Automation • Wireless for Automation
Access	An access VLAN is for ports that can belong to only one VLAN. The access VLAN ID for ports that are assigned to these Smartport roles: • Automation Device • Multiport Automation Device • Desktop for Automation • Virtual Desktop for Automation • Phone for Automation
Voice	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 ID for ports that are assigned to the Phone for Automation Smartport role.

Assign Smartports Roles

On the Smartport Role tab, you can assign a Smartport role to one interface or multiple interfaces simultaneously. For Smartport role descriptions, see Table 88.

To assign a role to one interface, select an interface in the grid. On the Assign Macro page, select a Smartport role and VLAN, and then click Update & Apply to Device.



To assign a role to multiple interfaces simultaneously, select multiple interfaces in the grid, and then click Multi Port Configuration. On the Assign Macro page, select a Smartport role and VLAN, and then click Apply to Device.

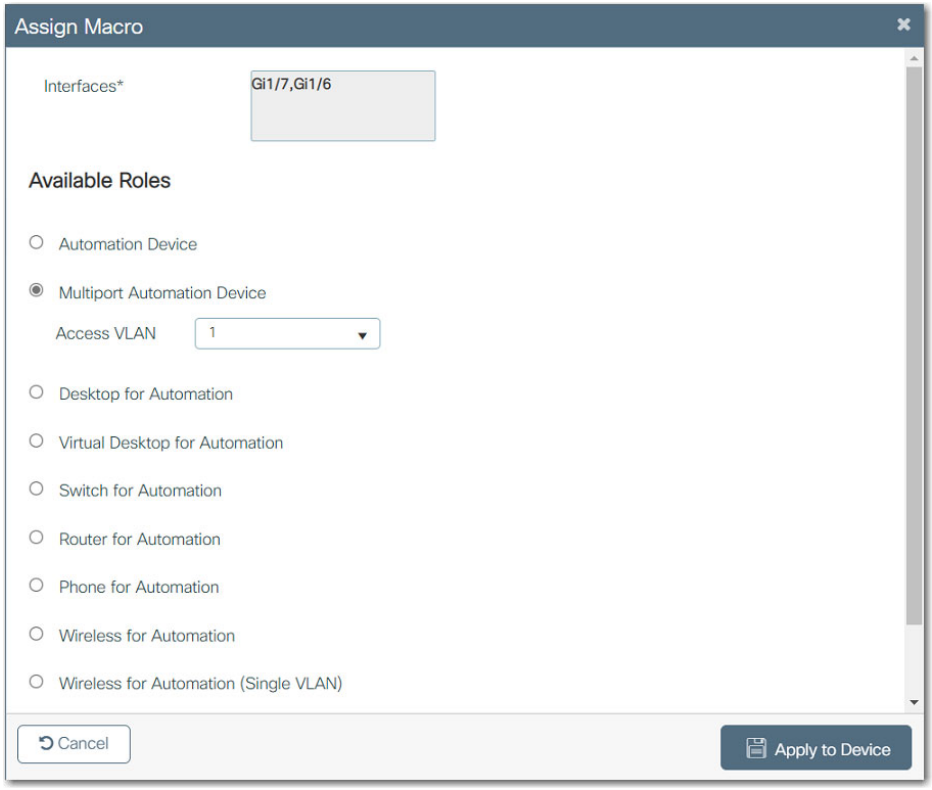


Table 88 - Assign Macro

Field	Description
Smartports Role	
Automation Device	Apply this role to ports that connect to EtherNet/IP (Ethernet Industrial Protocol) devices, such as logic controllers and I/O: • Port is set to Access mode. • Port security supports only one MAC ID. • Optimized queue management for CIP traffic.
Multiport Automation Device	Apply this role to DLR-enabled ports and ports that connect to multiport EtherNet/IP devices. For example, devices can 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: • Port is set to Access mode. • No port security. • Optimized queue management for CIP traffic.
Desktop for Automation	Apply this role to ports that connect 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. **IMPORTANT:** Do not apply the Desktop for Automation role to ports that connect to switches, routers, or access points.
Virtual Desktop for Automation	Apply this role to ports that connect to a computer with virtualization software. You can use this role 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 connect to switches, routers, or access points.
Switch for Automation	Apply this role to ports that connect to other switches. Port is set to Trunk mode.
Router for Automation	Apply this role to ports that connect to routers or Layer 3 switches with routing services enabled. Port is set to Trunk mode.

Table 88 - Assign Macro (Continued)

Field	Description
Phone for Automation	Apply this role to ports that connect to IP phones. A desktop device, such as a computer, can connect 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 that connect to wireless access points. The access point can provide network access to as many as 30 wireless users.
None	Apply this role to ports if you do not want a specialized Smartport role on the port. You can apply this role to ports that connect to any device, including a device with another Smartport role.
CS1...CS10	Custom Smartport roles. You can create a customized port role with a user-defined name.

Configure Custom Smartport Roles

On the Custom Smartports tab, you can add, delete, import, and export custom Smartport roles:

- To add a custom Smartports role, click Add, complete the fields as described in Table 89, and then click Apply to Device.
- To delete a Custom Smartports role, click the role in the grid, and then click Delete.
- To import a Custom Smartports role, click Import and then Select File to browse to the location of the file to upload from your computer or network drive. Click Apply to Device.
- To export a Custom Smartports Macro, click the role in the grid, and then click Export. Select the directory where you want to export the file.

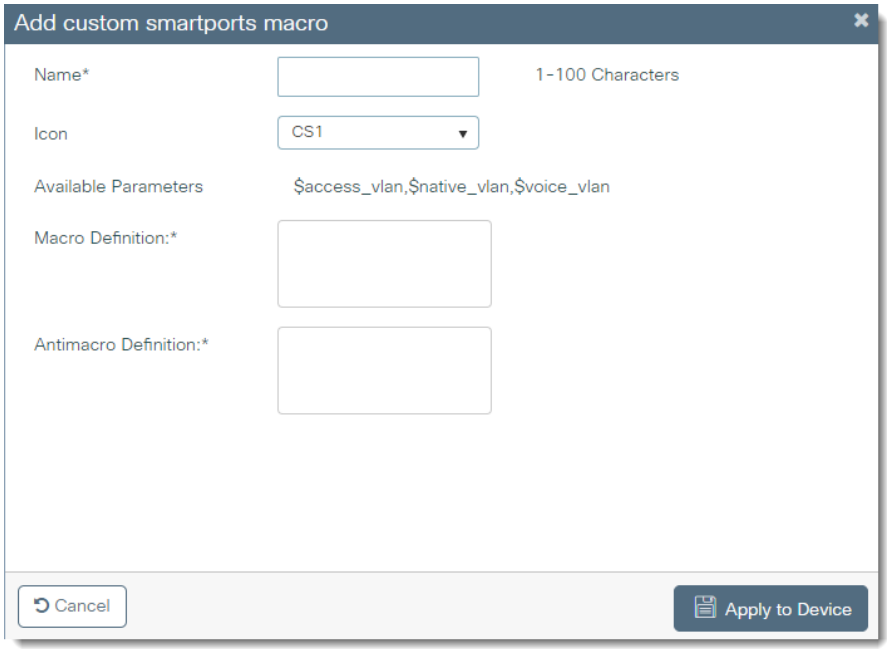


Table 89 - Add Custom Smartports Macro

Field	Description
Name	Enter a name to identify the custom Smartport role.
Icon	Choose an icon to identify the custom Smartport role. Valid values: CS1...CS10
Available Parameters	Displays the available parameters: $native_vlan, $access_vlan, and $voice_vlan You can use these parameters to achieve proper VLAN configuration in your custom Smartport roles.
Macro Definition	Enter the commands to define the custom role with one command per line. A macro definition can have up to 3000 characters. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro. We recommend that you do not use the exit or end commands or change the command mode by using interface interface-id in a macro. This can cause any commands following exit, end, or interface interface-id to execute in another command mode. For best results, all commands in a macro must be in the same configuration mode.
Antimacro Definition	Enter the commands to remove the custom role with one command per line. The antimacro is the portion of the applied macro that removes the macro when you replace it or remove it. Before you can apply the macro definition to the port, you must first define the antimacro with the proper commands to set the port back to its original state. An antimacro definition can have a maximum of 3000 characters. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro.

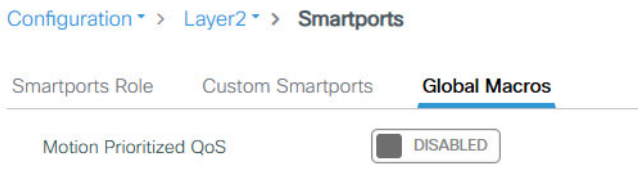
Motion Prioritized QoS Macros

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 the WebUI interface.

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 WebUI

From the Configure menu, choose Layer2 > Smartports > Global Macros and enable the switch for Motion Prioritized QoS.



Assign Smartport Roles via the Logix Designer Application

In the navigation pane, click Smartports and VLANs.

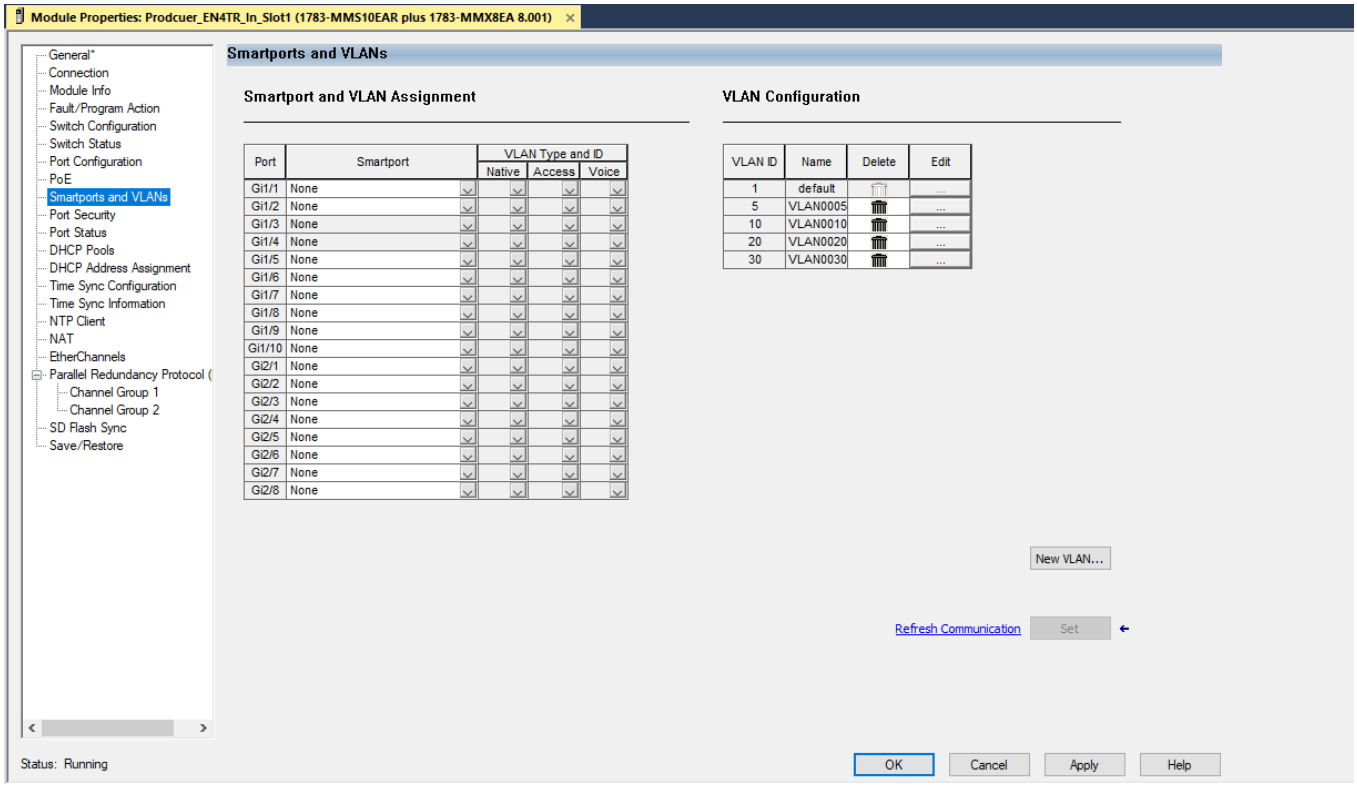


Table 90 - Smartports and VLANs

Field	Description
Port	Displays the port type and number.
Smartport	Choose the role that corresponds to the type of device to be connected to the port. For a description of each role, see Table 88 on page 178.
VLAN Type and ID	Choose the VLANs to assign to the port. The types of VLANs you can assign depend on the type of Smartport role. For a description of each VLAN type, see Table 87 on page 176.

Spanning Tree Protocol (STP)

STP is a Layer 2 link management protocol that provides path redundancy and helps to prevent loops in the network. A spanning-tree algorithm selects one switch in a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a Layer 2 network. For more information about STP, see the Ethernet Reference Manual, publication ENET-RM002.

Requirements and Restrictions

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

IMPORTANT Disabling STP can affect connectivity to the network.

STP Modes

Table 91 describes the STP modes that you can assign to the switch. The default mode is RPVST.

Table 91 - STP Modes

STP Mode	Description
MST	Multiple Spanning Tree (MST) is based on the IEEE 802.1s standard. MST uses Rapid Spanning Tree Protocol (RSTP) for rapid convergence. This mode maps a group of VLANs into one 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 that are required to support many VLANs.
PVST	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 one 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.
RPVST	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 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.

Multiple Spanning Tree (MST)

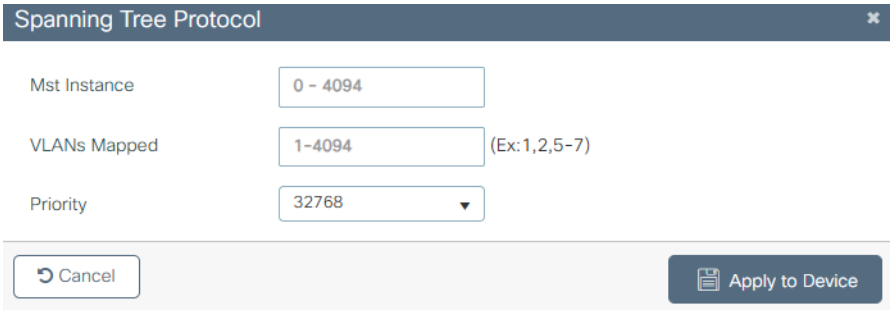


Table 92 - MST Mode

Parameter	Description
MST Instance	The number assigned to this spanning tree instance.
VLANs Mapped	VLANs mapped to this MST instance.
ROOT	
Priority	Priority Indicator.
Address	MAC address of the port.
Port	Identifier of the named port.
Cost	Cost associated with the port.
Remaining (Rem) Hops	Number of hops remaining of the maximum hop count (configured value of MaxHops) after each downstream switch decrements the hop count field on reception of Internal Spanning Tree (IST) BPDU.
BRIDGE	
Priority	Priority Indicator.
Address	MAC address of the port.
Remaining (Rem) Hops	Number of hops remaining of the maximum hop count (configured value of MaxHops) after each downstream switch decrements the hop count field on reception of Internal Spanning Tree (IST) BPDU.
Interface	Interface type and number of the port.
Role	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 receives 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	Cost associated with the port.
Prio.Nbr	The local port priority and port ID.
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.

Configure STP via the WebUI

1. From the Configuration menu, choose Spanning Tree.
2. Complete the fields as described in Table 93.
3. To enable or disable STP on a VLAN or change the bridge priority, click the VLAN in the grid, modify the fields, and then click Update & Apply to Device.



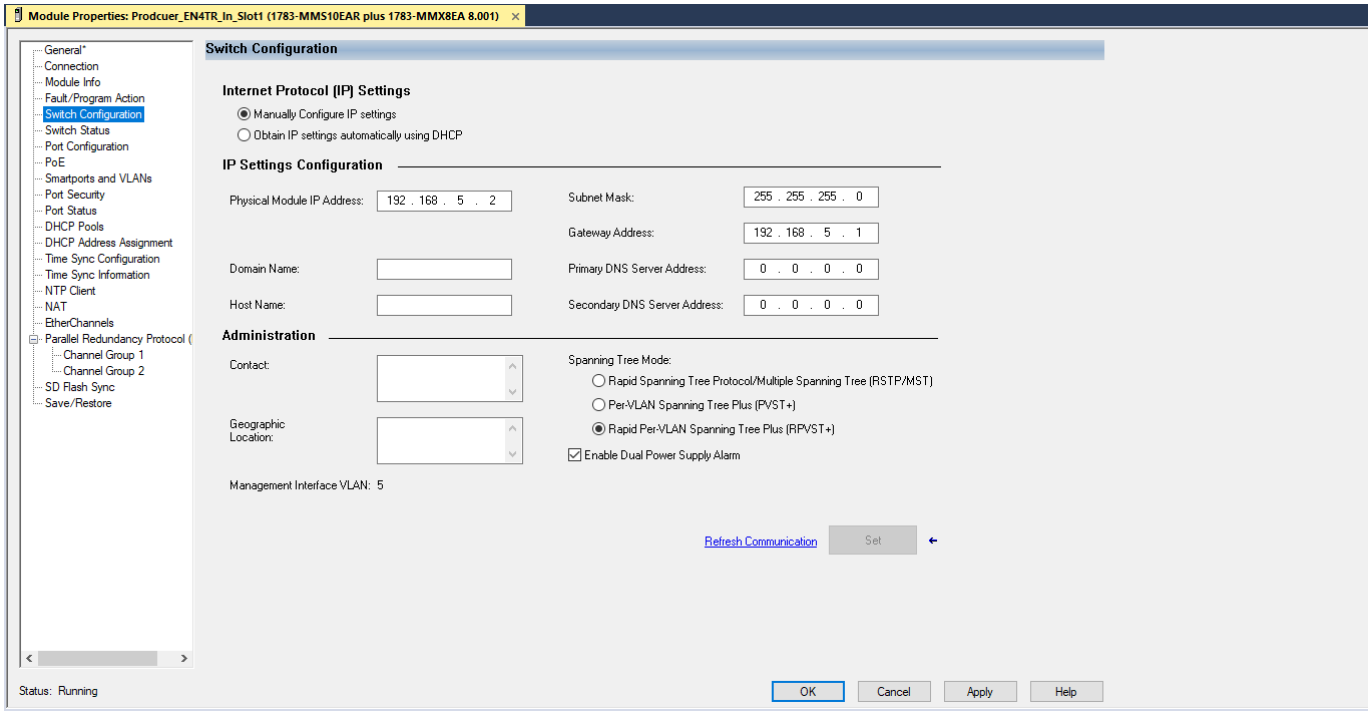
Table 93 - Spanning Tree Protocol

Field	Description
STP Mode	Choose the STP mode to apply to the switch. For a description of each mode, see Table 91 on page 182. The default mode is RPVST.
BPDU Filtering	Click to enable or disable BPDU filtering. BPDU filtering avoids transmitting bridge protocol data units (BPDUs) on PortFast-enabled ports that are connected to an end system. When you enable PortFast on the device, STP places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states first.
BPDU Guard	Click to enable or disable BPDU guard. BPDU guard helps to prevent loops by moving a nontrunk port into an err-disable state when a BPDU is received on that port. When you enable BPDU guard on the switch, STP shuts down PortFast-configured interfaces that receive BPDUs instead of putting them into the STP blocking state. In a valid configuration, PortFast-configured interfaces do not receive BPDUs. If a PortFast-configured interface receives a BPDU, an invalid configuration exists. BPDU guard provides a secure response to invalid configurations because the administrator must manually put the interface back in service.

Configure STP via the Logix Designer Application

1. In the navigation pane, click Switch Configuration.
2. In the Spanning Tree Mode field, click to specify an STP mode, and then click Apply.

   For a description of each mode, see Table on page 182.



Static Routing

The switch provides two types of routing:

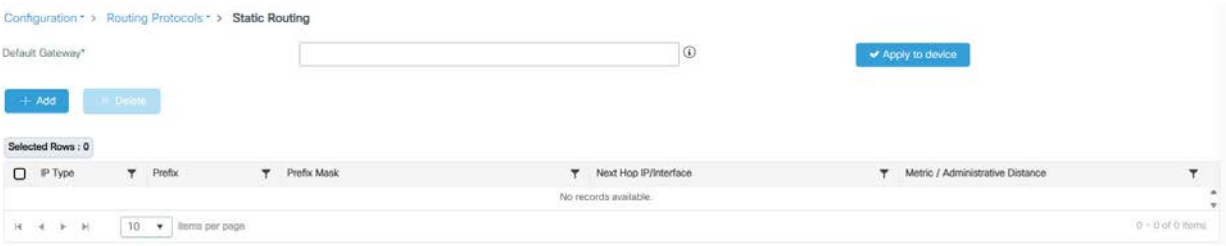
- Connected routing—Enables all devices on any VLAN that use the switch to communicate with each other if they use the switch as their default gateway.

IMPORTANT Connected routing is enabled by default and cannot be disabled.

- 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.

Configure Static Routing via the WebUI

From the Configuration menu, choose Static Routing.



From the Static Routing page, you can add, edit, and delete IP routes:

- To add an IP route, click Add, complete the fields as described in Table 94, and then click Save & Apply to Device.
- To edit a route, click the route in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a route, check its associated checkbox in the grid, and then click Delete.

You can also specify a default gateway to direct packets addressed to networks not explicitly listed in the routing table. When the default gateway is configured, the switch has connectivity to the remote networks with which a host must communicate. To configure a default gateway, enter the IP address of the default gateway and click Apply to Device.

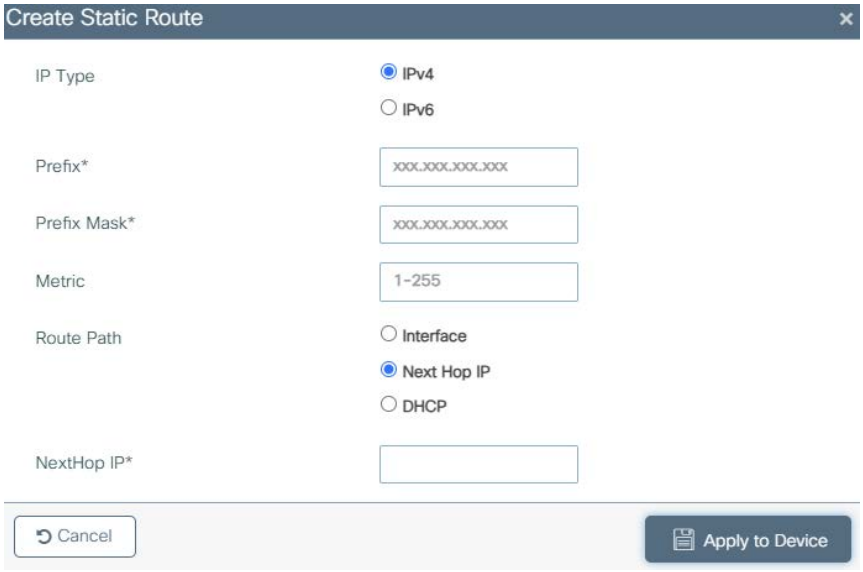


Table 94 - Create Static Route

Field	Description
IP Type	Click the type of static route.
Prefix	Enter the prefix for your IPv4 or IPv6 address.
Prefix Mask	(Appears only for IPv4). Enter the prefix for your IPv4 address.
Metric	(Appears only for IPv4). Enter the metric for your IPv4 address. (1) Valid values: 1...55
Prefix Length	(Appears only for IPv6). Enter the prefix length for your IPv6 address. Valid values: 0...128
Administrative Distance	(Appears only for IPv6). Enter the metric to choose the best path when there are two or more routes to the same destination from two different routing protocols.(1) Valid values: 1...254
VRF (Stratix 5800 Switch Only)	If you want the static route to support Virtual Routing and Forwarding (VRF) instances, check VRF.
VRF Name	(Appears only if VRF is checked). Choose the VRF name.
Route Path	Click to specify a route path: • Interface • Next Hop IP • DHCP (IPv4 only)
Interface	(Appears only if the route path is Interface). Choose the forwarding interface.
NextHop IP	If the route path is an interface or next hop IP, enter the IPv4 or IPv6 IP address.

(1) A router prefers a static route over a dynamic route because the router considers a route with a low number to be the shortest. If you want a dynamic route to override a static route, specify an administrative distance for the static route. For example, if there are two dynamic routes with an administrative distance of 120, specify an administrative distance that is greater than 120 for the static route.

Switched Port Analyzer (SPAN)

SPAN, also known as port mirroring, copies traffic from one port to a monitoring port where a network analyzer tool can capture the traffic. You can use SPAN to troubleshoot network issues and calculate network utilization and performance. For more information about SPAN, see the Ethernet Reference Manual, publication ENET-RM002.

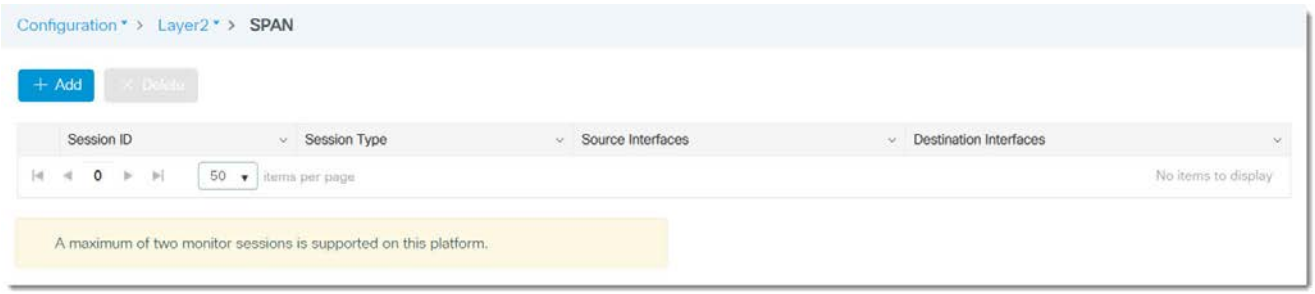
Requirements and Restrictions

Observe these guidelines:

- You can configure a maximum of two monitor sessions on the switch. Session IDs are 1 and 2.
- There can be multiple source interfaces and only one destination interface.
- Source interfaces cannot be a combination of VLAN and physical interfaces.
- If using multiple source ports, you can lose traffic if the combined source throughput is more than the output port is capable of.

Configure SPAN via the WebUI

From the Configuration menu, choose SPAN.


Configuration > Layer2 > SPAN
+ Add
Session ID
Session Type
Source Interfaces
Destination Interfaces
0
50
items per page
No items to display
A maximum of two monitor sessions is supported on this platform.

From the SPAN page, you can add, edit, and delete SPAN monitor sessions:

- To add a SPAN session, click Add, complete the fields as described in Table 95, and then click Apply to Device.
- To edit a SPAN session, click the session in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a session, check its associated checkbox in the grid, and then click Delete.

Figure 37 - SPAN Page



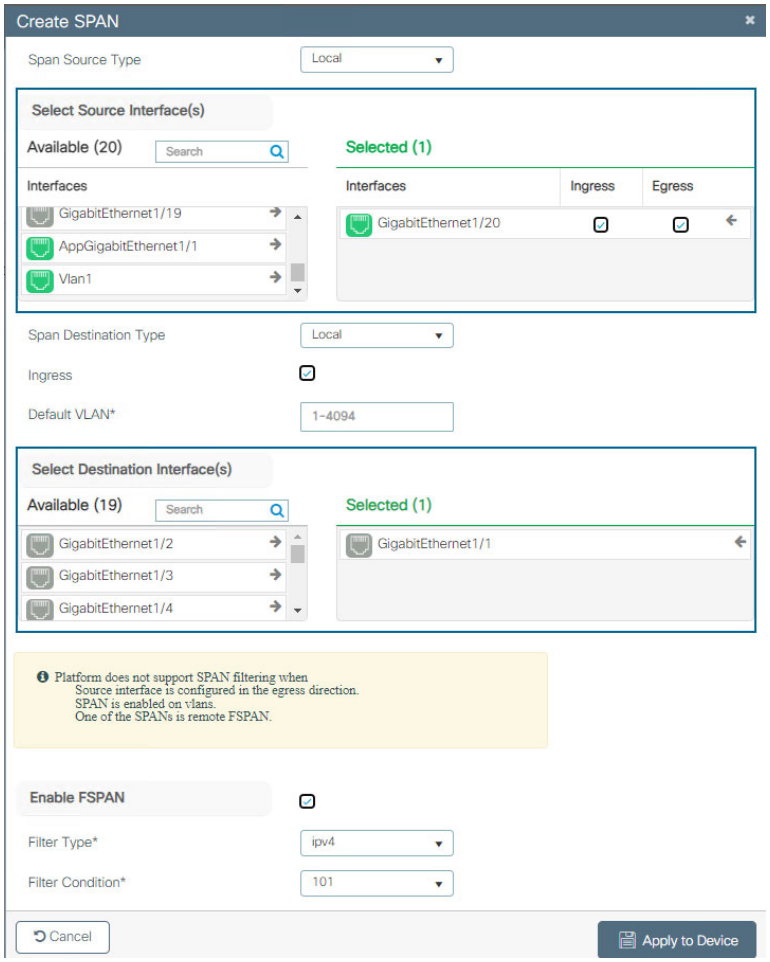


Table 95 - Create SPAN

Field	Description
Select Source Interfaces	In the Available list, click to move one or more source interfaces to the Selected list on the right. To specify the direction of source packets to be monitored, check the Ingress and Egress checkboxes.
Select Destination Interfaces	In the Available list, click to move a destination interface to the Selected list on the right. Stratix 5800 switches support only one destination interface.

TrustSec

Cisco TrustSec builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

- TrustSec is only supported on catalog numbers 1783-MMS10AR, 1783-MMS10EAR, 1783-MMX8EA, 1783-MMX8TA, 1783-MMX8SA.
- Trustsec not supported with redundancy FPGA profile.

TrustSec Security Groups

TrustSec uses the device and user credentials that are acquired during authentication for classifying the packets by security groups as they enter the network. A security group is a grouping of users, endpoint devices, and resources that share access control policies. Once a device is authenticated, TrustSec tags any packet that originates from that device with a security group tag (SGT) that contains the security group number of the device. The packet carries this SGT throughout the network within the TrustSec header. The SGT is a single label that determines the privileges of the source within the entire enterprise.

You can map an SGT to a subnet, VLAN, or interface as described in Table 96.

Table 96 - SGT Mappings

Mapping Type	Description
IPv4 subnet-to-SGT	Binds an SGT to all host addresses of a specified subnet. TrustSec imposes the SGT on an incoming packet when the source IP address in the packet belongs to the specified subnet.
VLAN-to-SGT	Binds an SGT to packets from a specified VLAN. This type of mapping is useful in networks with these characteristics: • Do not have authentication enabled • Use third-party switches • Have devices that do not support Cisco TrustSec
L3IF-SGT	Directly maps SGTs to traffic of any of the following Layer 3 interfaces regardless of the underlying physical interface: • Routed port • SVI (VLAN interface) • Layer 3 subinterface of a Layer 2 port • Tunnel interface

Security Group Tag Exchange Protocol

The Security Group Tag (SGT) Exchange Protocol (SXP) is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. This helps propagate the SGTs across network devices that do not have hardware support for TrustSec.

TrustSec Policies

To control the operations performed by a user, you can use Cisco TrustSec (CTS) policies. CTS policies include a selection of security group access control lists (SGACLs). A list specifies the permissions to be applied to packets from an IP address belonging to a source security group and having a destination IP address that belongs to the destination security group.

You must enable SGACL policy enforcement on specific VLANs to apply access control to switched traffic within a VLAN, or to traffic that is forwarded to an SVI associated with a VLAN.

You can enable Monitor mode on a global or per-policy basis to test security policies without enforcing them to make sure that the policies function as intended.

CTS Interface Configuration

By enabling CTS Manual Configuration mode on an interface, you can configure a physical port so that one SGT is imposed on all traffic that enters the port. This SGT is applied on all IP traffic exiting the port until a new binding is learned.

CTS configuration is available for the following ports:

- Routed ports
- Ports in Access mode
- Ports in Trunk mode

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no Security Association Protocol (SAP) parameters are defined, MACsec encapsulation or encryption is not performed.
- If the selected SAP mode allows SGT insertion and an incoming packet carries no SGT, the packet is tagged with the SGT configured for the interface.
- If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:
  - If the policy is configured without the trusted keyword, the SGT is replaced with the SGT configured for the interface.
  - If the policy is configured with the trusted keyword, no change is made to the SGT.

Configure TrustSec via the WebUI

From the Configuration menu, choose TrustSec. From the Trustsec page, you can configure the following:

- Global settings as described on page 192. (Stratix 5800 Switch Only)
- SGT mappings as described on page 192.
- SGT Exchange Protocol (SXP) as described on page 194.
- CTS policies as described on page 196. (Stratix 5800 Switch Only)
- CTS link configuration as described on page 197. (Stratix 5800 Switch Only)

IMPORTANT To configure global settings, CTS policies, and CTS interfaces, you must have one of the following:

- A switch with advanced features with no expansion module attached
- A switch with advanced features attached to an expansion module with advanced features

Configure TrustSec Global Settings (Stratix 5800 Switch Only)

On the General tab, complete the fields as described in Table 97, and then click Apply.

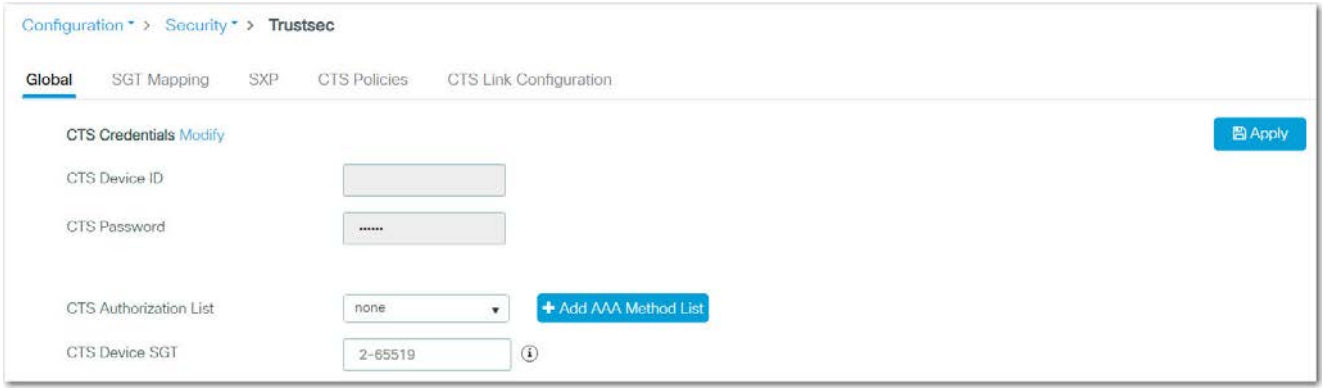


Table 97 - Trustsec—Global Tab (Stratix 5800 Switch Only)

Field	Description
CTS Credentials	Click Modify, and then enter the Cisco TrustSec device ID and password.
CTS Device ID	Displays the CTS device ID.
CTS Password	Displays the CTS device password.
CTS Authorization List	Choose the Cisco TrustSec global authorization list to configure on the switch. To add a new method list, click + Add AA Method List.
CTS Device SGT	Enter the ID of the security group tag to configure on the switch. Valid values: 2...65519.

Configure SGT Mappings



On the SGT Mapping tab, you can add, edit, and delete SGT mappings:

- To add an SGT mapping, click Add, complete the fields as described in Table 96, and then click Apply to Device.
- To edit an SGT mapping, click the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an SGT mapping, check its associated checkbox in the grid, and then click Delete.

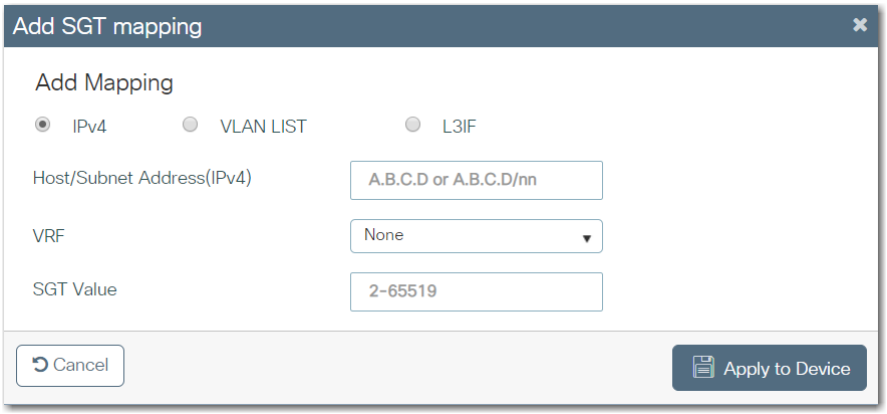


Table 98 - Add SGT Mapping

Field	Description
Mapping	Click the type of SGT mapping to add. For a description of each type of mapping, see Table 96.
Host/Subnet Address(IPv4)	(Appears only for IPv4 mappings). Enter an IPv4 network address in dotted decimal notation.
VRF (Stratix 5800 Switch Only)	(Appears only for IPv4 mappings). Choose a VRF interface. For information about creating a VRF interface, see page 97.
VLAN List	(Appears only for VLAN LIST mappings). Enter the VLAN IDs to apply to the SGT mapping.
Layer-3 Interface	(Appears only for L3IF mappings). Choose an interface configured for Layer 3. For information about configuring a Layer 3 interface, see page 90.
SGT Value	Enter a number to identify the mapping. Valid values: 0...65519

Configure SXP

To configure SXP, follow these steps.

1. Click the SXP tab.
2. In the SXP Parameters area, complete the fields as described in Table 99, and then click Apply.

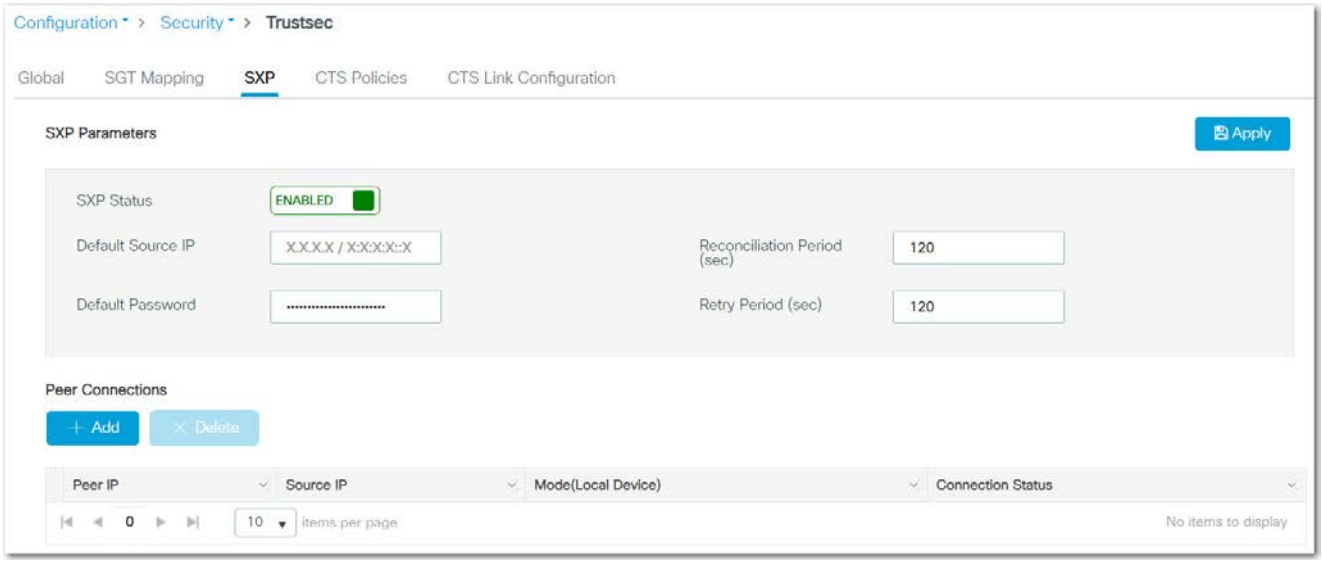


Table 99 - SXP Parameters

Field	Description
SXP Status	Click to enable or disable TrustSec SXP. You must enable SXP before you can configure peer connections.
Default Source IP	Enter an SXP default source IP address. SXP uses the default source IP address for all new TCP connections where a source IP address is not specified. There is no effect on existing TCP connections when you configure the default SXP source IP address.
Reconciliation Period (sec)	Enter a reconciliation period in seconds. After a peer ends an SXP connection, an internal timer starts. If the peer reconnects before the internal timer expires, the SXP reconciliation period timer starts. While the SXP reconciliation period timer is active, TrustSec retains the SGT mapping entries learned from the previous connection and removes invalid entries. Setting the reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed. Default value: 120 seconds (2 minutes)
Default Password	Enter an SXP default password. By default, SXP uses no password when setting up connections. Spaces and special characters are not allowed.
Retry Period (sec)	Enter a retry period in seconds. The SXP retry period determines how often TrustSec retries an SXP connection. When an SXP connection is not successful, TrustSec makes a new attempt to connect after the SXP retry period timer expires. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted. Default value: 120 seconds (2 minutes)

3. In the Peer Connections area, you can add, edit, and delete peer connections:
   - To add a peer connection, click Add, complete the fields as described in Table 100, and then click Apply to Device.
   - You must configure the SXP peer connection on both of the devices. One device is the speaker and the other is the listener. When using password protection, make sure to use the same password on both ends.
   - To edit a peer connection, click the connection in the grid, modify the fields, and then click Update & Apply to Device.
   - To delete a peer connection, check its associated checkbox in the grid, and then click Delete.

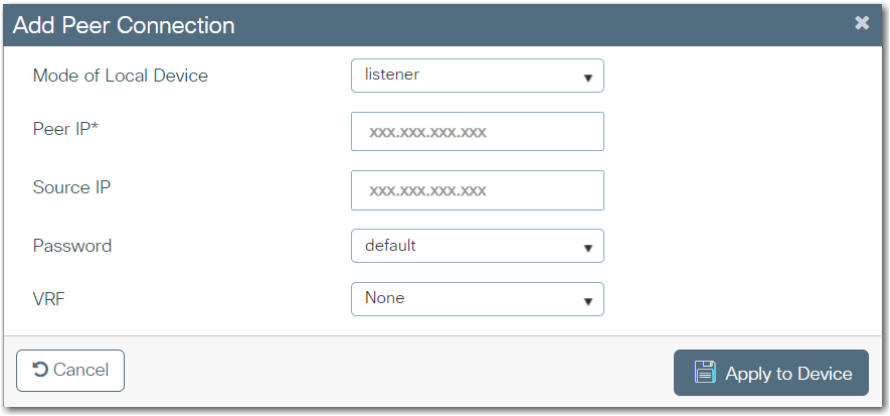


Table 100 - Add Peer Connection

Field	Description
Mode of Local Device	Choose one of the following modes for the remote peer device: • listener—The device is the listener in the connection. • speaker—The device is the speaker in the connection. • both—The device is both the listener and the speaker in the connection. Default value: listener
Peer IP	Enter the IPv4 address of the peer device.
Source IP	Enter the IPv4 address of the source device. If you do not specify an address, the connection uses the default source address, if configured, or the address of the port.
Password	Choose one of the following options to specify the password that SXP uses for the connection: • default—Uses the default SXP password. • none—Does not use a password. Default value: default
VRF (Stratix 5800 Switch Only)	Choose one of the following to specify the VRF to the peer: • None • [VRF name] Default value: None

Configure CTS Policies

To configure CTS policies, follow these steps.

1. Click the CTS Policies tab.
2. In the Policy Enforcement area, complete the fields as described in Table 101, and then click Apply.



Table 101 - Policy Enforcement

Field	Description
VLAN List	Enter the VLAN IDs on which to enforce Cisco TrustSec policies. Valid values: 1...4094
Global	Click to enable or disable global CTS role-based enforcement. **IMPORTANT:** You must enable policy enforcement globally for TrustSec-enabled routed interfaces. Default value: Disabled

3. In the Manage Policies area, you can add, edit, and delete policies:
   - To add a policy, click Add, complete the fields as described in Table 102, and then click Apply to Device.
   - To edit a policy, click the connection in the grid, modify the fields, and then click Update & Apply to Device.
   - To delete a policy, check its associated checkbox in the grid, and then click Delete.
4. In the Monitor mode for all field, click to enable or disable the Monitor mode for all policies.

   For more information about Monitor mode, see TrustSec Policies on page 191.

5. To force an immediate refresh of TrustSec policies, click Refresh.

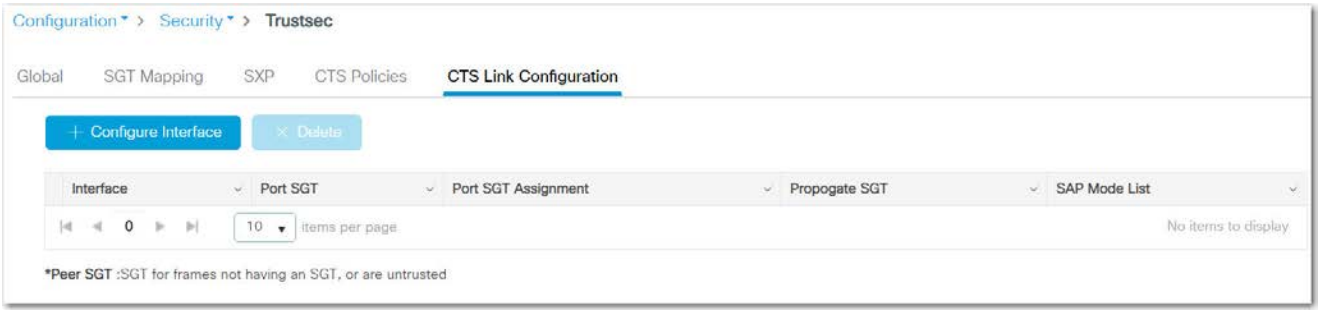


Table 102 - Manage Policies

Field	Description
Default Policy	Check to make this policy the default policy.
Monitor Mode	Click to enable or disable Monitor mode for this policy. Default value: Disabled For more information about Monitor mode, see TrustSec Policies on page 191.
From SGT	Enter the source security number for this policy.
To SGT	Enter the destination security group number for this policy.
SGACL Type	Click the type of IP addresses that belong to the security groups for this policy: • IPv4 • IPv6
Available SGACLs	To select the SGACLs to include in this policy, click an SGACL in the Available SGACLs column to move it into the Selected SGACLs column. To create a SGACL, click Add SGACL. See Add an Access Control List on page 76.

Configuring CTS Link Configuration

To configure CTS interfaces, click the CTS Link Configuration tab.



On the CTS Link Configuration tab, you can configure, edit, and delete STC interfaces:

- To configure an interface, click Configure Interface, complete the fields as described in Table 103, and then click Apply to Device.
- To edit an interface, click the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an interface, check its associated checkbox in the grid, and then click Delete.

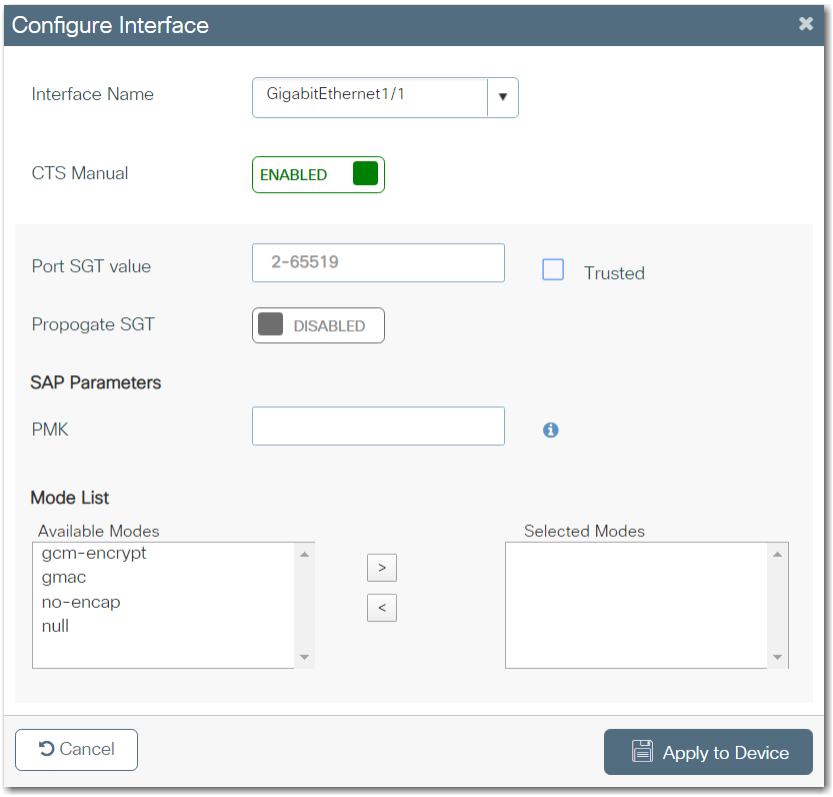

Configure Interface
Interface Name
GigabitEthernet1/1
CTS Manual
ENABLED
Port SGT value
2-65519
Trusted
Propogate SGT
DISABLED
SAP Parameters
PMK
Mode List
Available Modes
gcm-encrypt
gmac
no-encap
null
>
<
Selected Modes
Cancel
Apply to Device

Table 103 - Configure Interface

Field	Description
Interface Name	Choose the interface to configure.
CTS Manual	To remove the ability to manually configure Cisco TrustSec on the interface, click to disable Manual Configuration mode. The remaining fields on the page become unavailable for configuration. Default value: Enabled
Port SGT value	To configure a static authorization policy on this interface, enter an SGT tag value. Valid values: 2...65519
Trusted	Check to indicate that ingress traffic on the interface with this SGT should not have its tag overwritten.
Propogate SGT	To allow the interface to transmit the SGT to the peer, click to enable the Propogate SGT function. To help prevent the interface from transmitting the SGT to the peer, click to disable the Propogate SGT function. Disable the function when the peer is incapable of processing an SGT.
PMK	To enable Security Association Protocol (SAP), enter the pairwise-master key. The key is a hexadecimal value with an even number of characters and a maximum length of 32 characters. In Manual Configuration mode, SAP is disabled by default.
Mode List	To select SAP operation modes, click a mode in the Available Modes column to move it into the Selected Modes column. SAP operations modes: • gcm encrypt—Authentication and encryption • gmac—Authentication, no encryption • no-encap—No encapsulation • null—Encapsulation, no authentication or encryption

Utility Features

GOOSE Messaging Support

GOOSE (Generic Object Oriented Substation Events) messaging 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.

Virtual Local Area Networks (VLANs)

A VLAN is a switched network segmented on a functional application rather than a physical or geographical basis. The isolation of different types of traffic helps to preserve the quality of the transmission and to minimize excess traffic among the logical segments. A VLAN also gives you the ability to control access and security to a group of devices independent of their physical location. For more information about VLANs, see the Ethernet Reference Manual, publication ENET-RM002.

Switch Virtual Interfaces (SVIs)

An SVI is a virtual interface in the switch that allows a VLAN to have an IP address and additional configuration. An SVI allows traffic to be routed out of a Layer 2 domain without requiring a physical interface.

You can configure SVIs via the WebUI with these restrictions:

- 32 SVIs total
- 1 SVI per VLAN
- 1 SVI per subnet

Supported VLANs

The switch supports VLANs in VTP client, server, and transparent modes. VLANs are identified by a number from 1...4094:

- VLAN 1 is the default VLAN and is created during system initialization.
- VLAN IDs 1002...1005 are reserved for token rings and Fiber Distributed Data Interface (FDDI) switching.

All VLANs except 1002...1005 are available for configuration. All VLAN Trunking Protocol (VTP) versions support both normal and extended range VLANs, but the switch only propagates extended range VLAN configuration information with VTP version 3. When extended range VLANs are created in VTP versions 1 and 2, their configuration information is not propagated. Even the local VTP database entries on the switch are not updated, but the extended range configuration information is created and stored in the running configuration file.

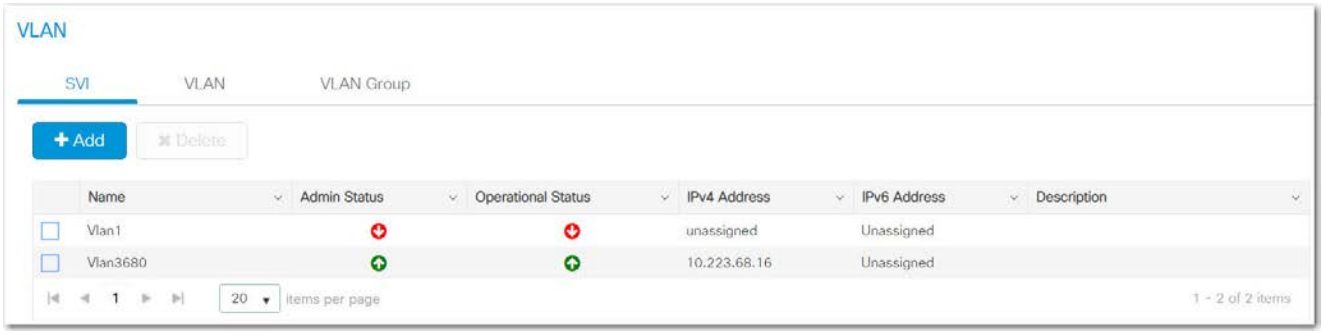
You can configure a maximum of 256 VLANs on the switch.

Management VLAN

The management VLAN provides administrative access to the switch. VLAN 1 is the default VLAN and also the default management VLAN. During Express Setup, you can change the default VLAN ID for the management VLAN. To have administrative access to the switch, you must assign one of the switch ports to the management VLAN.

Configure SVIs and VLANs via the WebUI

From the Configuration menu, choose VLAN.



From the VLAN page, you can configure SVIs, VLANs, and VLAN groups:

- To configure SVIs, see page 201.
- To configure VLANs, see page 203.
- To configure VLAN groups, see page 204.

Configure SVIs

From the SVI tab, you can add, edit, and delete SVIs:

- To add an SVI, click Add, complete the fields as described in Table 104, and then click Apply to Device.
- To edit an SVI, click the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an SVI, check its associated checkbox in the grid, and then click Delete.

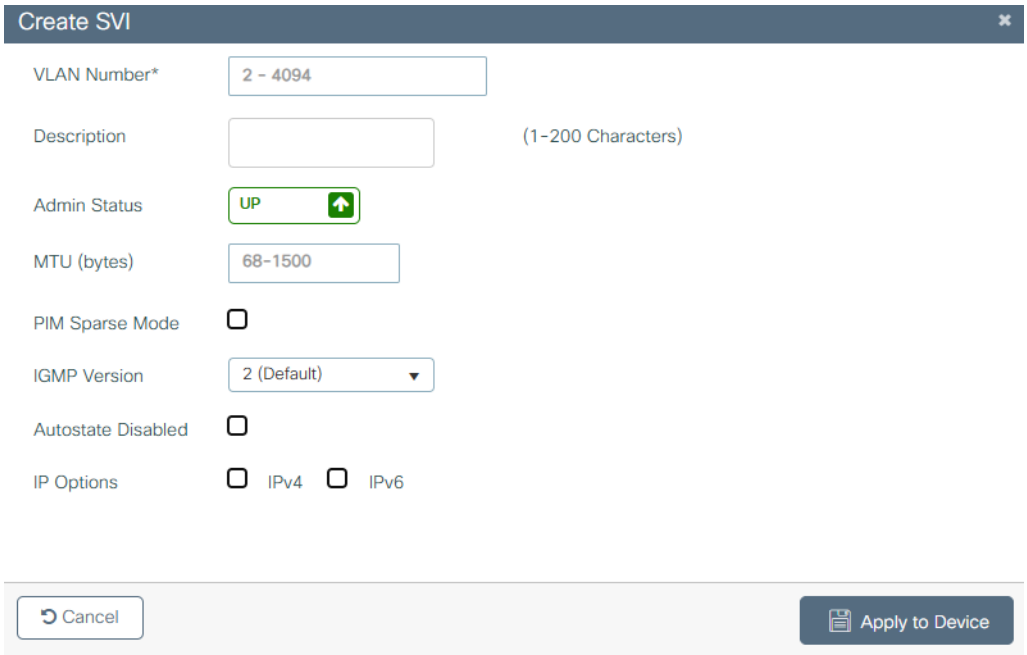


Table 104 - Create SVI

Field	Description
VLAN Number	Enter a unique number to identify the VLAN. If you enter a VLAN number that does not exist, the switch creates a VLAN. Be sure to assign ports to newly created VLANs. Valid values: 1…4094
Description	Enter a description for the VLAN.
Admin Status	Click to enable or disable the operational status of the interface: • Up—The interface is operational. • Down—The interface is not operational. Default value: Up
MTU (bytes)	Only populate this field if you specifically want to limit MTU on the associated VLAN. If this field is left blank, the SVI defaults to the global MTU, which is set in the System MTU (Bytes) field on General tab of the Administration | Device page. Enter the maximum transmission unit (MTU) for the VLAN. Valid values: 68…1500
PIM Sparse Mode (Stratix 5800 Switch Only)	Forwards multicast traffic only to the routers that request it.
IGMP Version (Stratix 5800 Switch Only)	Choose the IGMP version to be applied Default: Version 2
Autostate Disabled	To keep the SVI active even when there are no active VLAN interfaces, check the Autostate Disabled checkbox.
IP Options	To configure an IPv4 SVI, check IPV4. To configure an IPv6 SVI, check IPV6. You can configure multiple IPv6 addresses on the same interface.
IPv4 Type	(Appears only for IPv4). Choose the IP address type: • Static • DHCP • Local Pool
Host Name	(Appears only DHCP IPv4 types). (Optional) Enter the DHCP server address.
DHCP Pool List	(Appears only for Local Pool IPv4 types). Choose a DHCP pool from which to assign addresses.
IP Address	(Appears only Static IPv4 types). Enter the IP address for the SVI.
Subnet Mask	(Appears only for Static IPv4 types). Enter the subnet mask for the SVI.
Secondary IP	(Appears only for Static IPv4). Check Secondary IP
Static	(Appears only for IPv6). Choose an IPv6 address type, and then enter an IPv6 address or prefix. To add an address or prefix, click +.
DHCP	(Appears only for IPv6). Check DHCP to use the Rapid Commit feature.
Rapid Commit	(Appears only for DHCP IPv6 types). To allow a two-message exchange method for address assignment, check Rapid Commit.
AutoConfig	(Appears only for IPv6). To simplify the configuration, check AutoConfig, and then choose from the following: • None • Default—If a default device is selected on this interface, a default route is installed.
Act as an IPv6 DHCP Client	(Appears only for IPv6). To make the interface act as a DHCPv6 client, check the checkbox, and then enter a prefix name.

Configure VLANs

From the VLAN tab, you can add, edit, and delete VLANs:

- To add a VLAN, click Add, complete the fields as described in Table 105, and then click Apply to Device.
- To edit a VLAN, click the VLAN in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a VLAN, check its associated checkbox in the grid, and then click Delete.

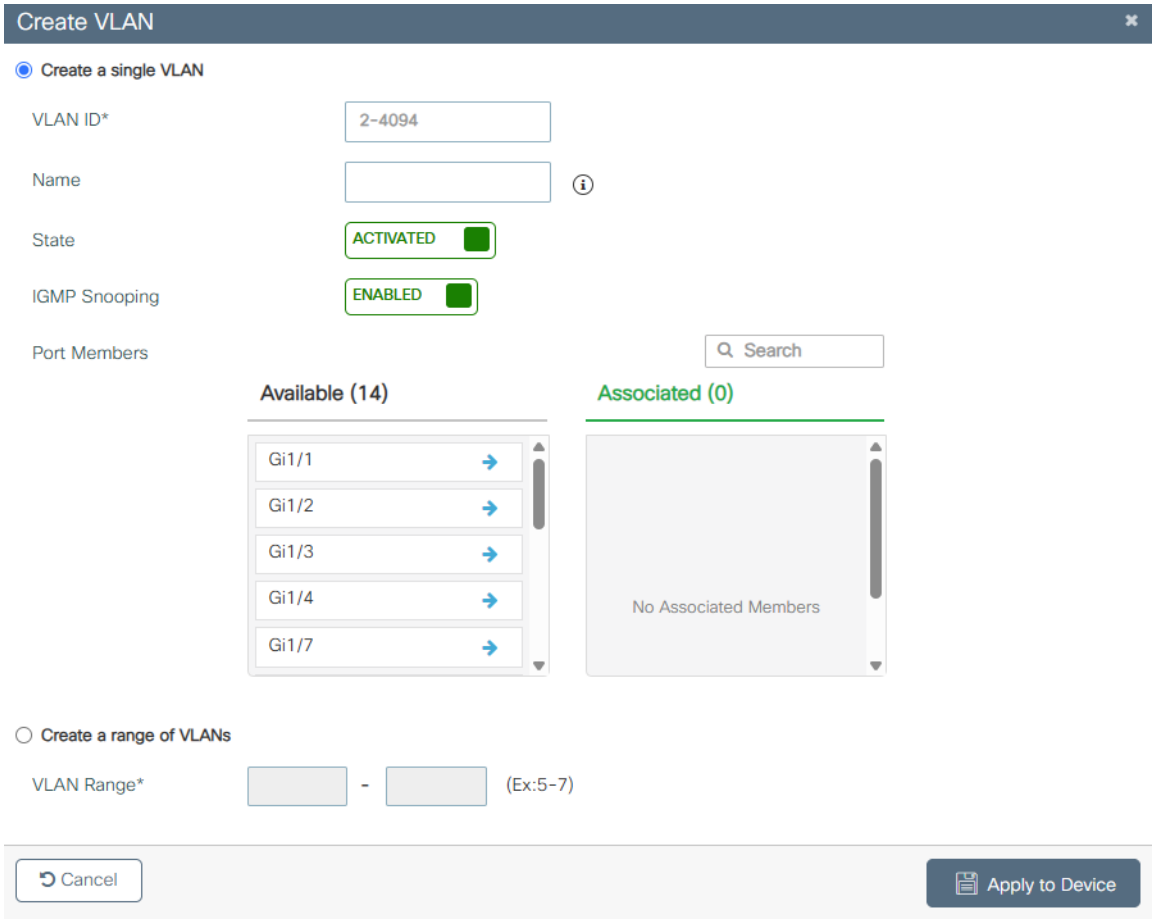


Table 105 - Create VLAN

Field	Description
VLAN ID	Enter a VLAN ID. Valid values: 2...4094
Name	Enter a name to identify the VLAN.
State	Click to activate or deactivate the VLAN.
IGMP Snooping	Click to enable or disable IGMP snooping on the VLAN. Default: Enabled
Port Members	In the Available list, click one or more ports to move them to the Associated list and make them members of the VLAN.
Create a range of VLANs	A VLAN range can be added to the parameters.

Configure VLAN Groups

From the VLAN Group tab, you can add, edit, and delete VLAN groups:

- To add a VLAN group, click Add, complete the fields as described in Table 106, and then click Apply to Device.
- To edit a VLAN group, click the group in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a VLAN group, check its associated checkbox in the grid, and then click Delete.

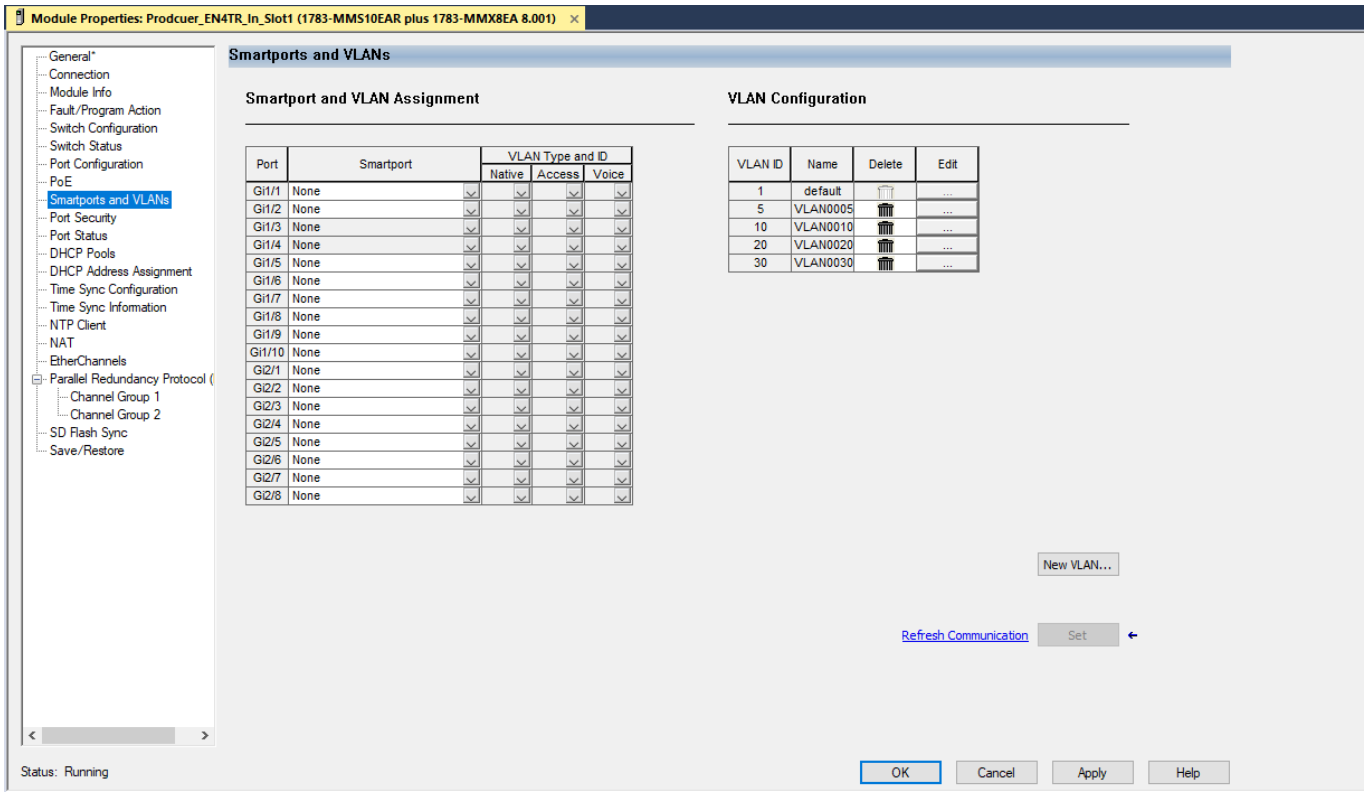


Table 106 - Create VLAN Group

Field	Description
VLAN Group Name	Enter a name to identify the VLAN group.
VLAN List	To map one VLAN or a range of VLANs to the group, enter VLAN IDs. For example, you can enter 1, 2, 5-7. Valid values: 1...4094

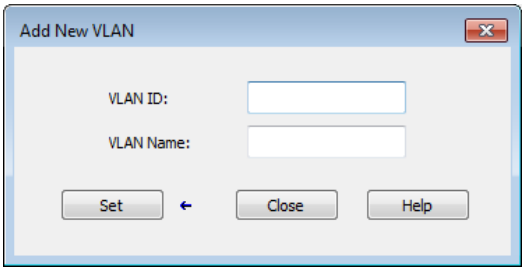
Configure VLANs via the Logix Designer Application

In the navigation pane, choose Smartports and VLANs.



In the VLAN Configuration area, you can add, edit, and delete VLANs:

- To add a VLAN, click New VLAN, enter a VLAN ID and description, click Set, and then click Close.



- To edit a VLAN, click the Ellipses icon in the Edit column, modify the fields, click Set, and then click Close.
- To delete a VLAN, click the Trash icon in the Delete column.

Virtual Router Redundancy Protocol (VRRP) (Stratix 5800 Switch Only)

The VRRP specifies an election protocol that assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address associated with a virtual router is called the Master and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility should the Master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

Configure VRRP via the WebUI

There are multiple ways a LAN client can determine which router is the first to go to a remote destination. The client can use a dynamic process or static configuration.

The following are examples of dynamic router discovery.

- Proxy ARP - The client uses ARP to get the destination it wants to reach, and a router responds to the ARP request with its own MAC address.
- Routing protocol - The client listens to dynamic routing protocol updates, for example, from Routing Information Protocol (RIP). After the client listens, it forms its own routing table.
- ICMP Router Discovery Protocol (IRDP) client - The client runs an Internet Control Message Protocol (ICMP) router discovery client.



Dynamic discovery protocols can incur some configuration and processing overhead on the LAN client. In the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This method simplifies client configuration and processing, but also creates a one point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

VRRP can solve the issues that are related to static configuration. VRRP enables a group of routers to form a one virtual router. This allows for the configuration of the LAN clients with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group. VRRP is supported on Ethernet, Fast Ethernet, BVI, Gigabit Ethernet interfaces, MPLS VPNs, VRF-aware MPLS VPNs, and VLANs.

The IP address of the virtual router is the same as the address configured for the Ethernet interface of the router.

Configure VRRP via WebUI

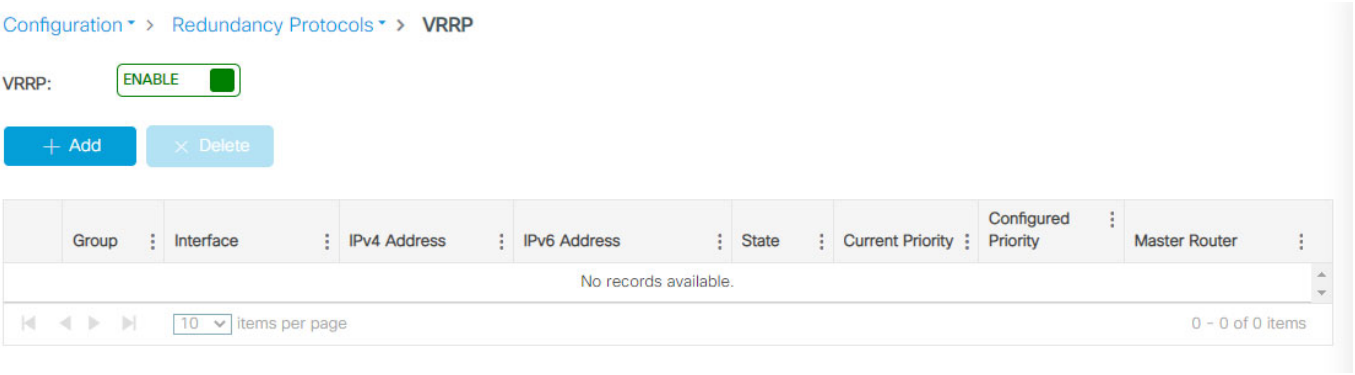
To configure the VRRP from Configuration, choose VRRP under the Redundancy Protocols category.

To enable VRRP, click “enable” next to the VRRP status.

To edit and existing group, click the row in the VRRP Group table.

Create a VRRP Group

To create a VRRP group, click Add.



The following window appears to create the VRRP group.

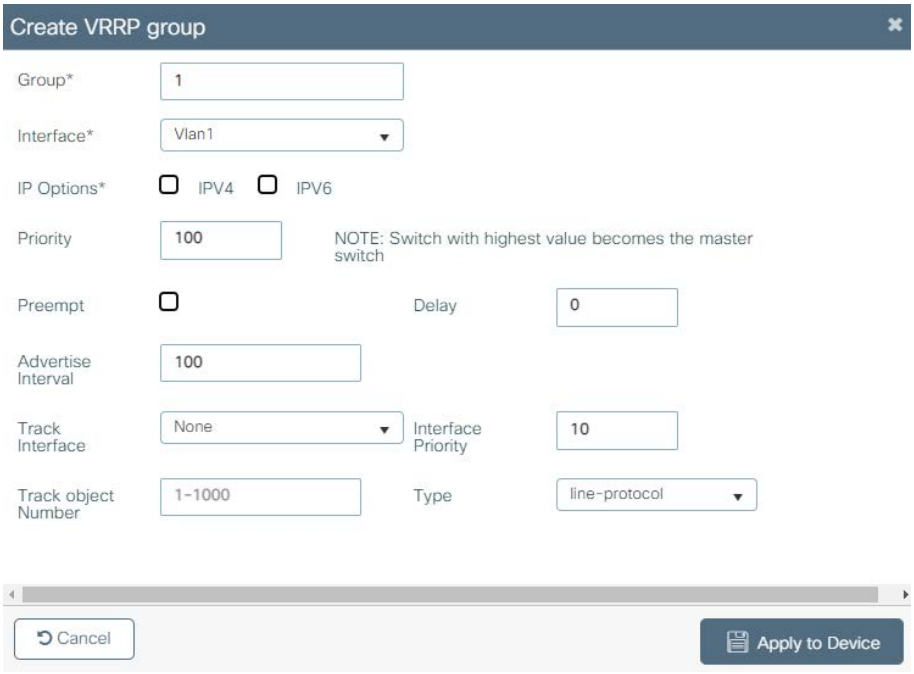


Table 107 - VRRP Group

Parameter	Description
Group	Enter the group number on the VRRP interface that is being enabled.
Interface	Choose the interface to enable the VRRP.
IP Options	To enter the virtual IP address information of the VRRP interface, check the IP Options box. • IPv4: Select the IPv4 type and enter the IP address of the VRRP interface and optional secondary IP address. • IPv6: Assign an IPv6 address or prefix to the interface. To add an address or prefix to the list, Click the "+." To remove them, click the "x."
Priority	Set a priority value that is used in choosing the virtual device master. The VRRP interface with the highest priority value becomes the virtual device master.
Preempt	Select Preempt so that when the VRRP interface has a higher priority than the virtual device master, it assumes control as the virtual device master.
Delay	To cause the VRRP interface to postpone taking over the virtual device master role for the configured number of seconds, enter a delay value. The range is 0…3600 (1 hour). The default is 0, or no delay before taking over.
Advertise Interval	Set the advertisement timer. The range is 100…40950 with a default of 100.
Track Interface	If you want to specify another VRRP interface for the VRRP process to monitor to alter the VRRP priority for a given group, select a Track Interface. If the line protocol of the specified interface goes down, the VRRP priority is reduced. This means that another VRRP interface with higher priority can become the virtual device master if that interface has standby preempt enabled.
Interface Priority	To specify the decrease of the VRRP priority when the tracked interface goes down, enter a priority value. When the tracked interface comes back up, the priority increases by the same amount. The range is 1…255 with a default of 10.
Track Object Number	Enter an object number for the tracked interface from 1…1000.
Type	Select the type of interface to be tracked.

Click Apply to Device.

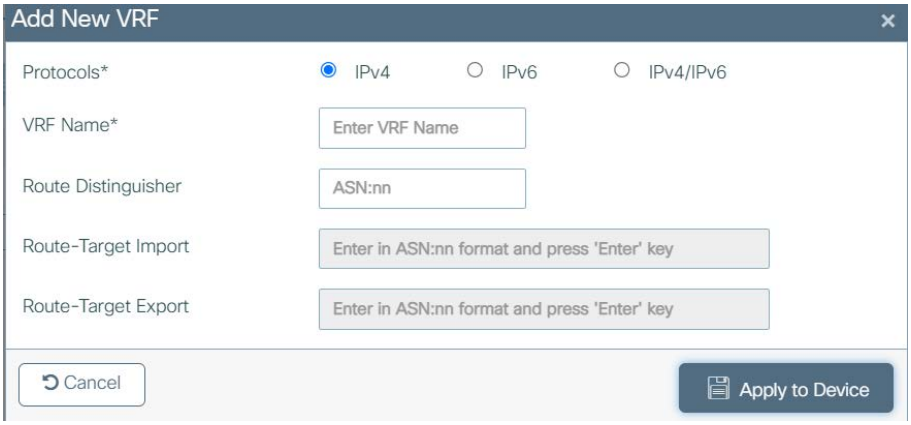
Virtual Routing and Forward (VRF) (Stratix 5800 Switch Only)

Virtual Routing and Forwarding (VRF) is a logical representation or grouping of Layer 3 entities, such as IP address, and routes. The VRF Support feature provides the controller with the capability to split the control plane and data plane into multiple segregated logical instances within the same controller platform and make the planes VRF aware.

VRF can enable flexible routing in infrastructure services and facilitate support for overlapping IP addresses.

Use the following steps to configure the VRF.

1. On the Configuration > Interface > VRF page, click Add to add a new VRF interface.



2. In the Add New VRF window, select the IPv4, IPv6 or IPv4/IPv6 protocol to enable the address family for the defined VRF.
3. Add a VRF name.
4. In the Route Distinguisher field, enter the route distinguisher Autonomous System (AS) number.
5. In the Route-Target Import and Route-Target Export field, enter the import and export route target number. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y).
6. Click Apply to Device to save the configuration.

VLAN Trunk Protocol (VTP)

VTP reduces administration and minimizes misconfiguration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. VTP avoids the need to configure the same VLAN on multiple switches in a network. For more information about VTP, see the Ethernet Reference Manual, publication ENET-RM002.

Requirements and Restrictions

Observe these guidelines:

- VTP has three versions. Only version 3 provides enhanced authentication, support for extended range VLAN (VLANs 1006...4094) database propagation, and support for any database in a domain. For example, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. If extended VLANs are configured in the domain, you cannot convert from VTP version 3 to VTP version 2.
- Before configuring VTP, configure a trunk port so that the switch can send and receive VTP advertisements to and from other switches in the domain.

VTP Modes

You can configure a switch to operate in the VTP modes described in Table 108.

Table 108 - VTP Modes

Mode	Description
Server	You can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain. The servers also synchronize their VLAN configurations with other switches based on advertisements that are received over trunk links.
Off	The switch functions in the same manner as a VTP transparent switch, except that it does not forward VTP advertisements on trunks.
Client	A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode. Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.
Transparent	A VTP transparent switch does not participate in VTP. It does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode. In VTP versions 1 and 2, the switch must be in VTP transparent mode when you create extended-range VLANs. VTP version 3 also supports creating extended-range VLANs in server mode only.

Configure VTP via the WebUI

1. From the Configuration menu, choose VTP.
2. Complete the fields as described in Table 109, and then click Apply to Device.

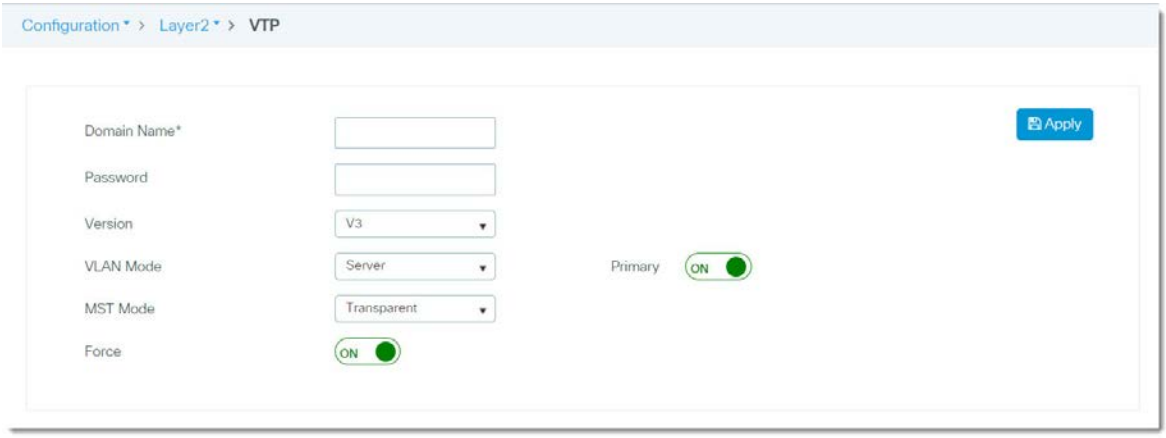


Table 109 - VTP

Field	Description
Domain Name	Enter a VTP domain name. The domain name is an ASCII string from 1...32 characters that identifies the VTP administrative domain for the device. The domain name is case sensitive.
Password	(Optional) Enter the administrative domain password. This password is for the generation of the 16-byte secret value that is used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case-sensitive.
Version	Choose the VTP version: • V1—Supports only normal-range VLANs (VLAN IDs 1...1005). • V2—Supports only normal-range VLANs (VLAN IDs 1...1005). • V3—Supports the entire VLAN range (VLANs 1...4096). The default version 1.
VLAN Mode	Choose the VLAN mode. For a description of each mode, see Table 108 on page 209. The default mode is Server. For Server mode, click the Primary field to indicate the operational state of the primary server: • ON—Changes the operational state of a switch from a secondary server (the default) to a primary server and advertises the configuration to the domain. • OFF—Does not change the operational state of a switch from a secondary server (the default) to a primary server.
MST Mode	(Optional, VTP version 3 only). Choose a VTP mode for the MST database. For a description of each mode, see Table 108 on page 209. The default mode is Server. For Server mode, click the Primary field to indicate the operational state of the primary server: • ON—Changes the operational state of a switch from a secondary server (the default) to a primary server and advertises the configuration to the domain. • OFF—Does not change the operational state of a switch from a secondary server (the default) to a primary server.
Force	(Optional, VTP Version 3 only, and VLAN Server mode and MST Server mode only). Click to indicate whether to overwrite the configuration of any conflicting servers: • ON—Overwrite configurations that conflict. • OFF—Do not overwrite configurations that conflict.

Administer the Switch

Topic	Page
Alarm Profiles	212
Alarm Settings	214
Back Up and Restore Procedures	218
Common Industrial Protocol (CIP)	224
CIP Sync (PTP)	224
Command-line Interface (CLI)	238
Device Settings	239
Device Time	243
Domain Name System (DNS)	244
Dynamic Host Configuration Protocol (DHCP)	245
File Manager	253
Field-programmable Gate Array (FPGA) Profiles (Stratix 5800 Switch Only)	255
HTTP/HTTPS/Netconf Access	257
MODBUS	258
Power over Ethernet (PoE) (Stratix 5800 Switch Only)	260
PROFINET	264
Reload the Switch Via the WebUI	266
SDM-Template	267
Secure Digital (SD) Card	268
Simple Network Management Protocol (SNMP)	270
Software Upgrade	275
Stratix 5200 Boot Order	276
Stratix 5800 Boot Order	276
User Administration	277

Alarm Profiles

Alarm profiles enable you to apply a group of alarm settings to multiple interfaces. These port-specific alarm settings specify the type of alarms and actions to trigger for the ports.

Alarm Types

An alarm profile can include the following alarm types.

Table 110 - Alarm Types for Alarm Profiles

Alarm	Description
Link Fault	The switch triggers the alarm when problems with a port physical layer cause unreliable data transmission. A typical link fault condition is loss of signal or clock. The link fault alarm clears automatically when the link fault condition is clear. The severity for this alarm is error condition, level 3.
Port Not Forwarding	The switch triggers the alarm when a port is not forwarding packets. This alarm clears automatically when the port begins to forward packets. The severity for this alarm is warning, level 4.
Port Not Operating	The switch triggers the alarm when the port fails during the startup self-test. When triggered, the port not-operating alarm is only clear when the switch restarts and the port is operational. The severity for this alarm is error condition, level 3.
Fcs Bit Error Rate	The switch triggers the alarm when the actual frame check sequence (FCS) bit error-rate is close to the configured rate. You can set the FCS Threshold on the Port page under Administration > Alarm Settings in the WebUI. The severity for this alarm is error condition, level 3.

Alarm Actions

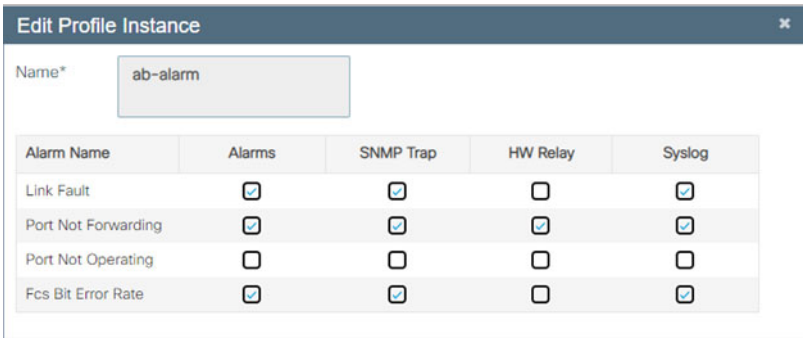
For each port-specific alarm, you can trigger the following actions.

Table 111 - Alarm Actions

Alarm Action	Description
Alarms	Enable the alarm.
SNMP trap	Alarm traps are sent to an SNMP server. SNMP is enabled on the SNMP page under Administration > Management in the WebUI.
HW relay	The alarm relay is triggered for the switch, and the switch sends a fault signal to a connected external alarm device, such as a bell, light, or other signal device.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Syslog page under Troubleshooting in the WebUI.

Default Alarm Profile

Express Setup configures all ports to use the default alarm profile called ab-alarm.



Create an Alarm Profile Via the WebUI

From the Administration menu, choose Alarm Profiles.



From the Alarm Profiles page, you can add, edit, and delete alarm profiles:

- To add an alarm profile, click Add, complete the fields as described in Table 112, and then click Apply to Device.
- To edit an alarm profile, click the profile in the grid, modify the fields, and then click Update and Apply to Device.
- To delete an alarm profile, check its associated checkbox in the grid, and then click Delete.

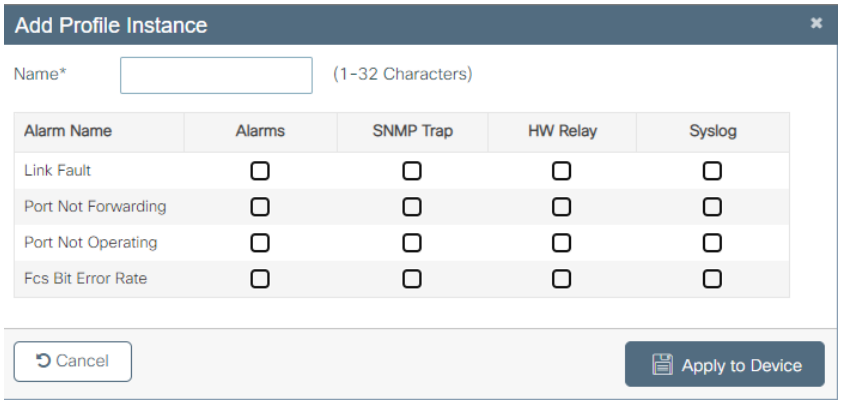


Table 112 - Add Profile Instance

Field	Description
Name	Enter a unique profile name.
Alarm Name	See Alarm Types on page 212.
Alarms	Check each type of action to trigger for the associated alarm type. See Alarm Actions on page 212.
SNMP Trap	
HW Relay	
Syslog	

Alarm Settings

The switch monitors alarm conditions on a per-port or a global basis. If conditions on the switch or on a port do not match the parameters that you configure for an alarm, the switch triggers an alarm or a system message.

External Alarm Devices

You can configure the switch to trigger an external alarm device by using the alarm relay. The switch supports one alarm output with both a normally closed and a normally open contact. The switch software is configured to detect faults, which are used to energize the relay coil and, change the state on both of the relay contacts. You can wire the external alarm to be triggered when the circuit is open or closed.

Global Alarm Types

You can configure the following types of global alarms on the switch.

Table 113 - Global Alarm Types

Alarm	Description
Power Supply	The switch triggers the alarm if a power supply fails or is missing. The alarm clears when the power supply is present or working.
Temperature—Primary	The switch triggers the primary alarm when the system temperature is higher or lower than the configured thresholds. By default, this alarm cannot be disabled. You can change the default temperature thresholds by entering new values. Default high threshold value: +90 °C (+194 °F) Default low threshold value: -40°C (-40°F) Valid threshold range: -55...+125°C (-67...+257°F)
Input—Alarm 1	The switch triggers the two input alarms based on the alarm relay configuration.
Input—Alarm 2	
SD card	The switch triggers the alarm when the SD Card is removed and it is cleared when it is inserted.(1)
Temperature—Secondary	The switch triggers the secondary alarm when the system temperature is higher or lower than the configured thresholds. By default, this alarm is disabled. You can change the default temperature thresholds by entering new values. Default high threshold value: +90 °C (+194 °F) Default low threshold value: 0 °C (+32 °F) Valid threshold range: -55...+125°C (-67...+257°F)
DLR	The Device Level Ring (DLR) alarm is triggered by any of the following Major DLR Alarm events: • The ring goes from Normal to Fault state. • Redundant gateway status changes from Active Normal or Backup. • Supervisor goes into Rapid_Fault state/partial fault. • Redundant Gateway goes to Partial_Network_Fault state.
HSR (Stratix 5800 Switch Only)	An HSR ring can generate the following two alarms: • Partial Ring Fault: This minor fault is generated by an HSR RedBox when one of its physical ring ports/links is down. Because the packets can be sent using the redundant path, this is considered as a partial fault. However, this fault still requires user intervention to restore the ring. • Full Ring Fault: This major fault is generated by an HSR RedBox when both of its physical ring ports/links are down. This is a catastrophic failure and needs immediate attention.

(1) To enable the HW Relay alarm for SD card, the alarms also must be enabled.

Alarm Actions for Global Alarms

For each global alarm, you can trigger the following actions.

Alarm Action	Description
Alarm	Enable the alarm.
SNMP trap	Alarm traps are sent to an SNMP server. SNMP is enabled on the SNMP page under Administration > SNMP in the WebUI.
HW relay	The alarm relay is triggered for the switch, the switch sends a fault signal to a connected external alarm device, such as a bell, light, or other signal device.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Syslog page under Troubleshooting in the WebUI.

Configure Alarm Settings Via the WebUI

To configure alarm settings, from the Administration menu, choose Alarm Settings.

From the Alarm Settings page, you can configure alarm relays, global alarms, and port alarms:

- To configure alarm relays, see page 215.
- Configure global alarms, see page 216.
- Configure port alarms, see page 217.

Configure Alarm Relays

On the Alarm Relay Setup tab, complete the fields as described in Table 114. When you make changes, a message appears in the lower-right corner of the WebUI to confirm that the configuration was successfully applied.

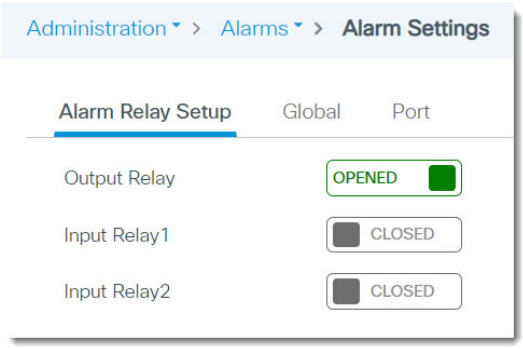


Table 114 - Alarm Settings—Alarm Relay Setup

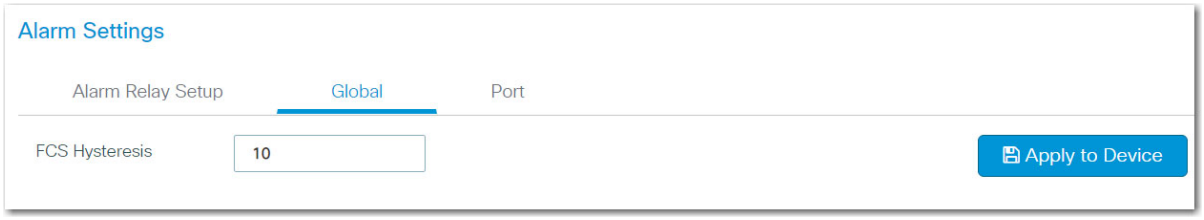
Field	Description
Output Relay	Click to determine the normal state of the output relay circuit: • Opened—When an alarm state occurs, the output relay circuit closes. • Closed—When an alarm state occurs, the output relay circuit opens.
Input Relay 1	Click to determine the normal state of input relay 1: • Opened—An alarm triggers when the input relay circuit closes. • Closed—An alarm triggers when the input relay circuit opens.
Input Relay 2	Click to determine the normal state of input relay 2: • Opened—An alarm triggers when the input relay circuit closes. • Closed—An alarm triggers when the input relay circuit opens.

Configure Global Alarms

On the Global tab, you can change the frame check sequence (FCS) error hysteresis threshold and edit global alarms:

- To change the (FCS) error hysteresis threshold, enter a percentage value from 1...10 and click Apply to Device. The default value is 10 percent.

  The frame check sequence (FCS) error hysteresis threshold is used to determine when an alarm condition is cleared. This value is expressed as a percentage of fluctuation from the FCS bit error rate. 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. You can also configure this setting for individual ports.



- To edit a global alarm, click the alarm in the grid, complete the fields as described in Table 115, and then click Update & Apply to Device.

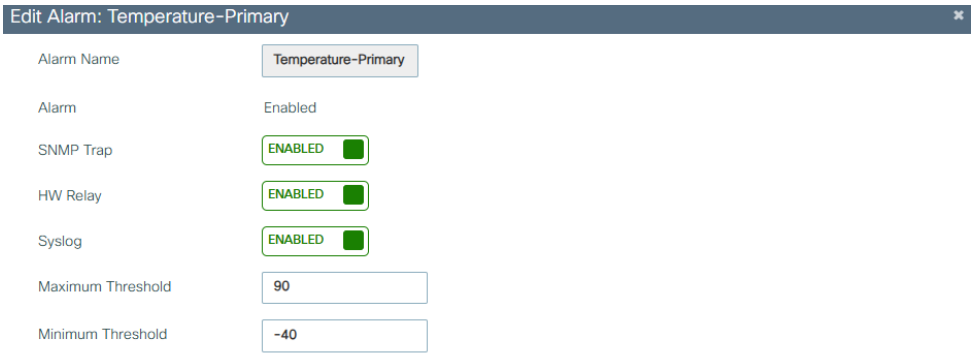
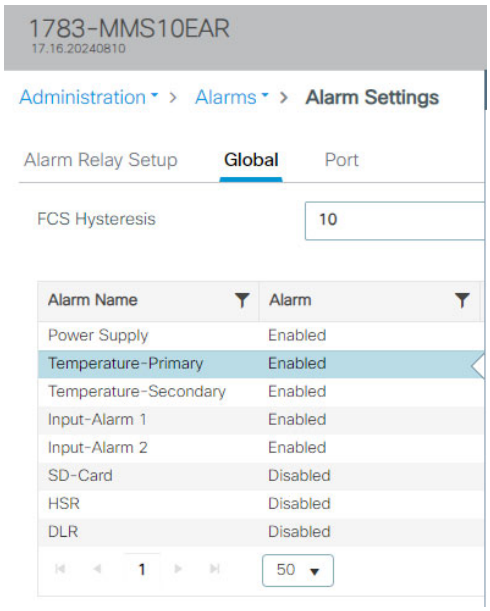


Table 115 - Alarm Settings—Global

Field	Description
Alarm Name	(System-generated). Displays the name of the global alarm. See Global Alarm Types on page 214.
Alarm	Click to enable or disable the action from being triggered by the associated alarm type. See Alarm Actions for Global Alarms on page 215.
SNMP Trap	
HW Relay	
Syslog	
Max Threshold in °C	Enter a maximum temperature in degrees Celsius. Valid threshold range: -55...+125°C
Min Threshold in °C	Enter a minimum temperature in degrees Celsius. Valid threshold range: -55...+125°C

Configure Port Alarms

On the Port tab, you can view and edit port alarms.



To edit a port alarm, on the Port tab, click the alarm in the grid, complete the fields as described in Table 116, and click Update & Save to Device.

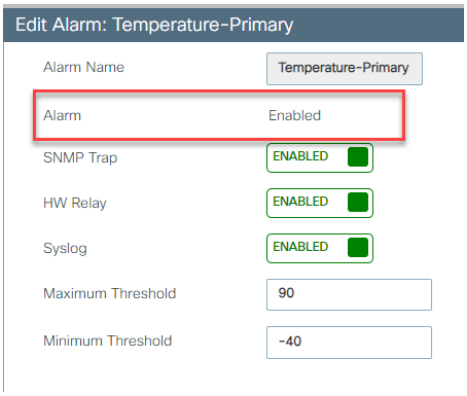


Table 116 - Alarm Settings—Port

Field	Description
Port Name	Displays the port type and number.
Alarm Profile	Choose an alarm profile. The default profile that is configured via Express Setup is ab-alarm.
FCS Threshold	Enter a percentage value from 6...8. This value is expressed as a percentage of fluctuation from the FCS bit error rate. 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. You can also configure this setting at the global level. Default value: 8

Back Up and Restore Procedures

You can perform these procedures on the switch:

- Back up and restore configuration files.
- Sync the SD card with the internal memory of the switch.

Back Up and Restore Configuration Files Via the WebUI

Configuration files contain the IOS software commands that are used to customize the functionality of your switch. The WebUI uses these configuration files:

- The Startup configuration file (startup-config) is used during system startup to configure the software.
- The Running configuration file (running-config) contains the current configuration of the software.

The two configuration files can be different. For example, you can change the configuration for a short time period rather than permanently.

IMPORTANT	Changes made to the Running configuration are lost after you restart the switch. The switch uses its Startup configuration after a power cycle.

1. From the Administration menu, choose Backup & Restore.

   On the Config File Management tab, you can copy configuration files to the switch or from the switch.
2. Complete the fields as described in Table 117.
3. If you are copying a file to the switch, click Upload File.

   or

   If you are copying a file from the switch, click Download File.
4. To reload the switch, click Reload.

IMPORTANT	A downloaded configuration does not take effect until after a reload.

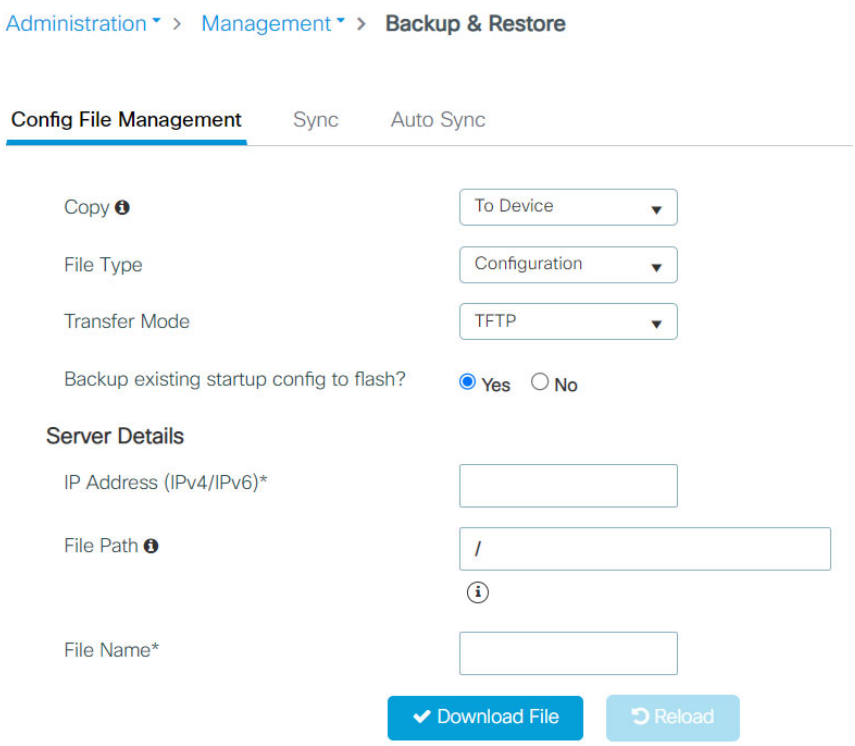


Table 117 - Backup & Restore—Config File Management

Field	Description
Copy	Choose whether to copy the configuration file to the device or from the device: • To Device (default) • From Device
File Type	Choose Configuration.
Transfer Mode	Choose the protocol to use for the file transfer: • TFTP (default) • SFTP • FTP • HTTP
Back up existing start up config to flash	If you chose to transfer a file to the device, click whether to back up the existing startup config to flash: • Yes—The switch saves the current startup configuration in its internal memory as a backup. • No—The switch does not save the current startup configuration.
Server Details	
IP Address (IPv4/IPv6)	(Appears only for TFTP, SFTP, and FTP transfers.) Enter the IP address of the TFTP or FTP server.
File Path	(Appears only for TFTP, SFTP, and FTP transfers.) Enter the file location for the configuration file on the TFTP, FTP server.
File Name	(Appears only for TFTP, SFTP, and FTP transfers.) Enter the name of the configuration file to transfer.
Server Login UserName	(Appears only for SFTP transfers.) Type the user name of the server to be accessed.
Server Login Password	(Appears only for SFTP transfers.) Type the password of the server to be accessed.
Logon Type	(Appears only for FTP transfers). Choose the type of logon required to access the FTP site: • Anonymous (default) • Authenticated
Source File Path	(Appears only for HTTP transfers). Click Select File and then browse to the .config file.

Back Up and Restore Sync Via the WebUI

Synchronization copies the firmware image or device configuration or both, from internal flash to SD card.

A configured Switch (not in a factory default state) always uses the startup configuration on the internal memory during start up. Changes to the running configuration are not immediately saved to the startup Configuration and must be saved explicitly. Once changes are saved, it is highly recommended to synchronize the configuration from internal flash to SD card.

You can use manual sync or enable automated sync. The SD card must be inserted to use Sync.

Use the Administration > Management > Backup & Restore > Sync page to display the SD card, device flash, and synchronization status and to manually synchronize files. Use the Administration > Management > Backup & Restore > Auto Sync page to configure the switch to synchronize automatically when the configuration is changed.

IMPORTANT Sync between usbflash and sdflash is not supported. Also, syncing from sdflash or usbflash to internal flash is not supported.

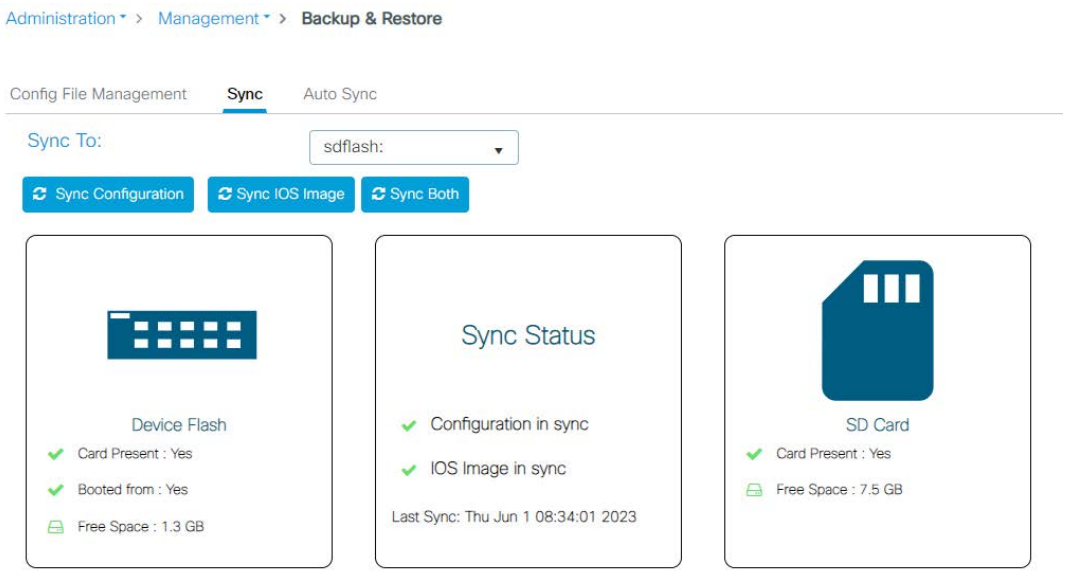


Table 118 - Backup & Restore—Sync

Sync Option	Description
Sync Configuration	Synchronizes the device configuration file.
Sync IOS Image	Synchronizes the image file.
Sync Both	Synchronizes both the device configuration file and the image file.

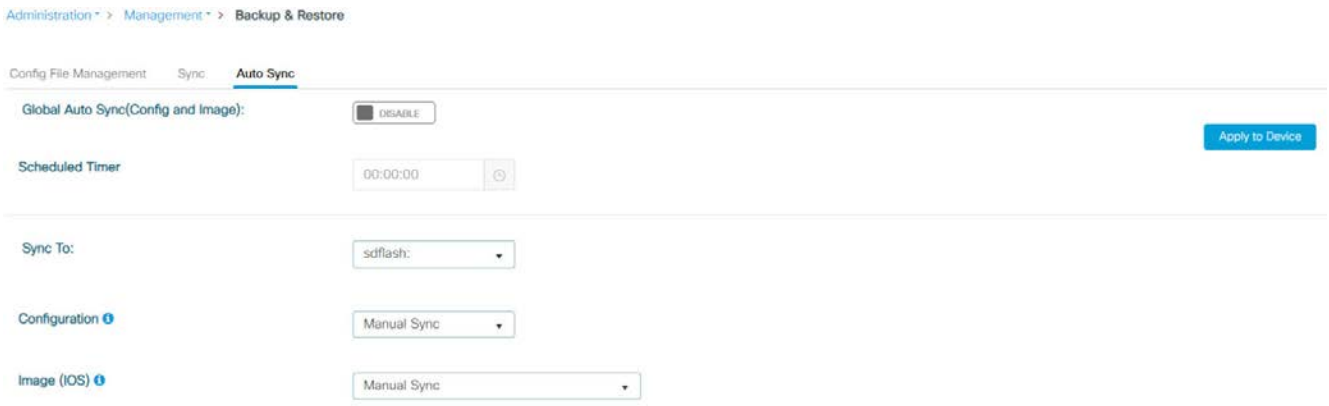


Table 119 - Backup & Restore—Auto Sync

Field	Description
Global Auto Sync (Config and Image)	Select this option to copy the IOS files from the internal flash memory to the SD card at a given specific time every day.
Schedule Timer	Select the time at which Auto Sync will be initiated every day.
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)	
Auto Sync	After firmware update, use this feature for the switch to synchronize automatically.
Prompt to Sync	After firmware update, use this feature for synchronization between the SD Card and an onboard flash.
Manual Sync	Use this feature for the synchronization to occur manually.

For more information on SD Cards as well as Swap Drive, see page 268.

Back Up, Restore, and Sync Configuration Files Via the Logix Designer Application

The Logix Designer application uses these configuration file:

- Text file with configuration parameters (config.text)
- Binary file with VLAN information (vlan.dat)

You can sync the configuration files between the switch and an SD card or save and restore the configuration files.

Sync Configuration Files with an SD Card

1. In the navigation pane, click SD Flash Sync.
2. Complete the fields as described in Table 120, and then click Apply.

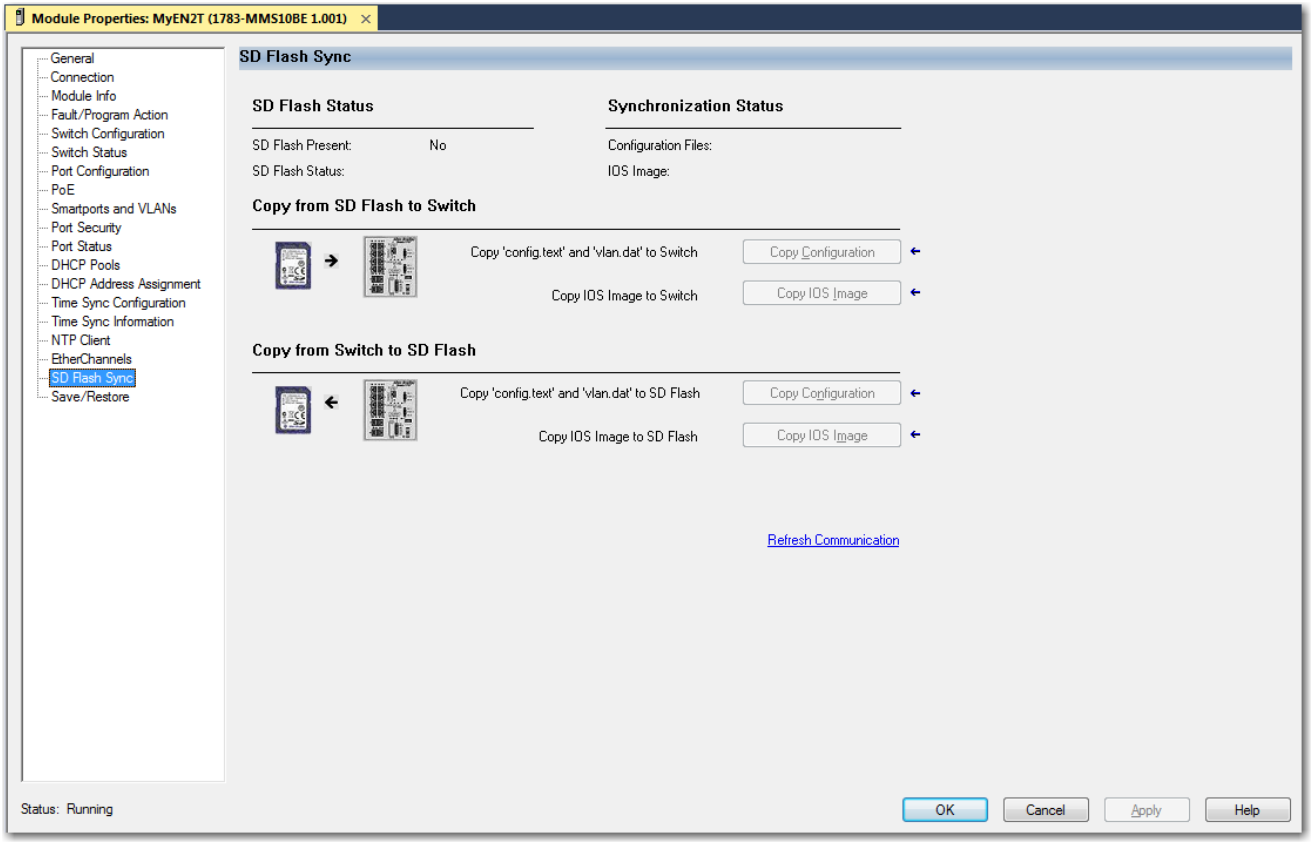
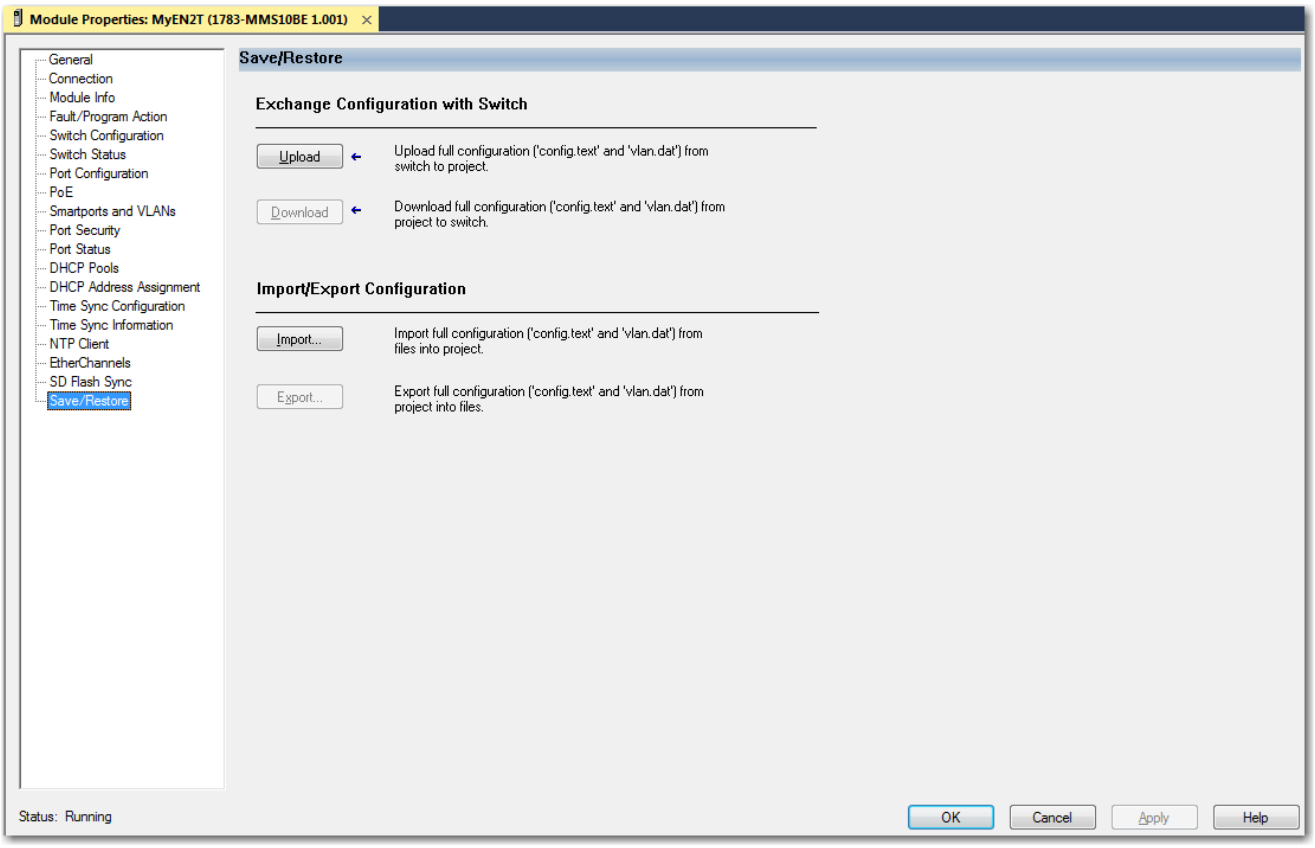


Table 120 - SD Flash Sync

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	Click to sync one of the following from the SD card to the switch: • Copy Configuration • Copy IOS Image
Copy from Switch to SD Flash	Click to sync one of the following from the switch to the SD card: • Copy Configuration • Copy IOS Image

Save and Restore Configuration Files

1. In the navigation pane, click Save/Restore.
2. Perform the following save and restore actions as needed, and then click Apply:
   - To restore a configuration that is stored on your local computer to the controller project, click Import.
   - To save the configuration that is stored in the controller project to your computer, click Export.
   - To copy the configuration from the switch to the controller project, click Upload.
   - To download the configuration from the controller project to the switch, click Download.



Common Industrial Protocol (CIP)

CIP™ is a messaging protocol for devices in industrial automation control systems. CIP is the application layer for the EtherNet/IP™ network. For more information about CIP, see the Ethernet Reference Manual, publication ENET-RM002.

Configure CIP Via the WebUI

IMPORTANT To manage the switch via the Logix Designer application, CIP must be enabled on the switch.

To configure CIP on the switch, from the Administration menu, choose CIP.

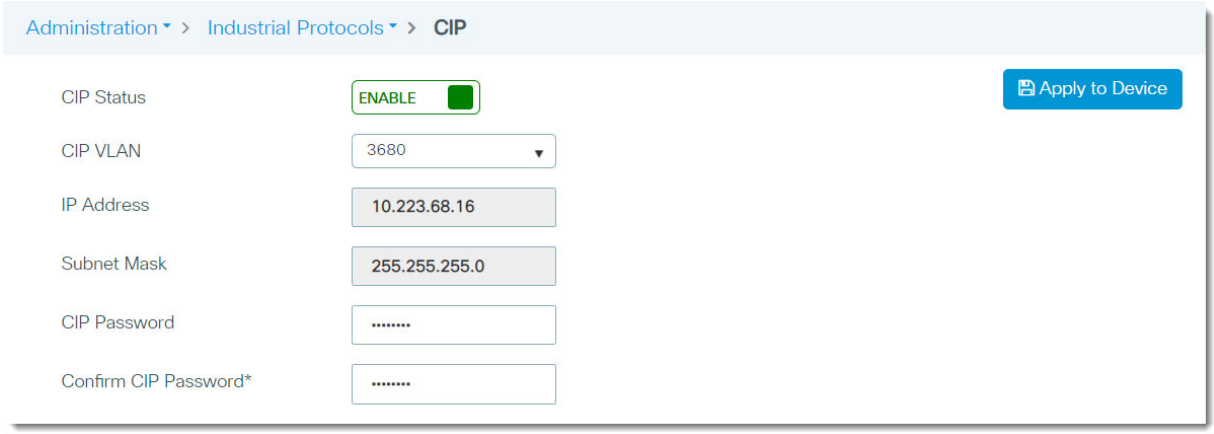


Table 121 - CIP

Field	Description
CIP Status	Click to enable or disable CIP messaging.
CIP VLAN	Choose a CIP VLAN. CIP can be enabled on only one VLAN.
IP Address	Displays the IP address and subnet mask for the CIP connection on the VLAN that you chose in the CIP VLAN field. To change these values, modify the SVI on the Configure > VLAN page.
Subnet Mask	
CIP Password	Enter a CIP password.
Confirm CIP Password	Reenter the CIP password to confirm it.

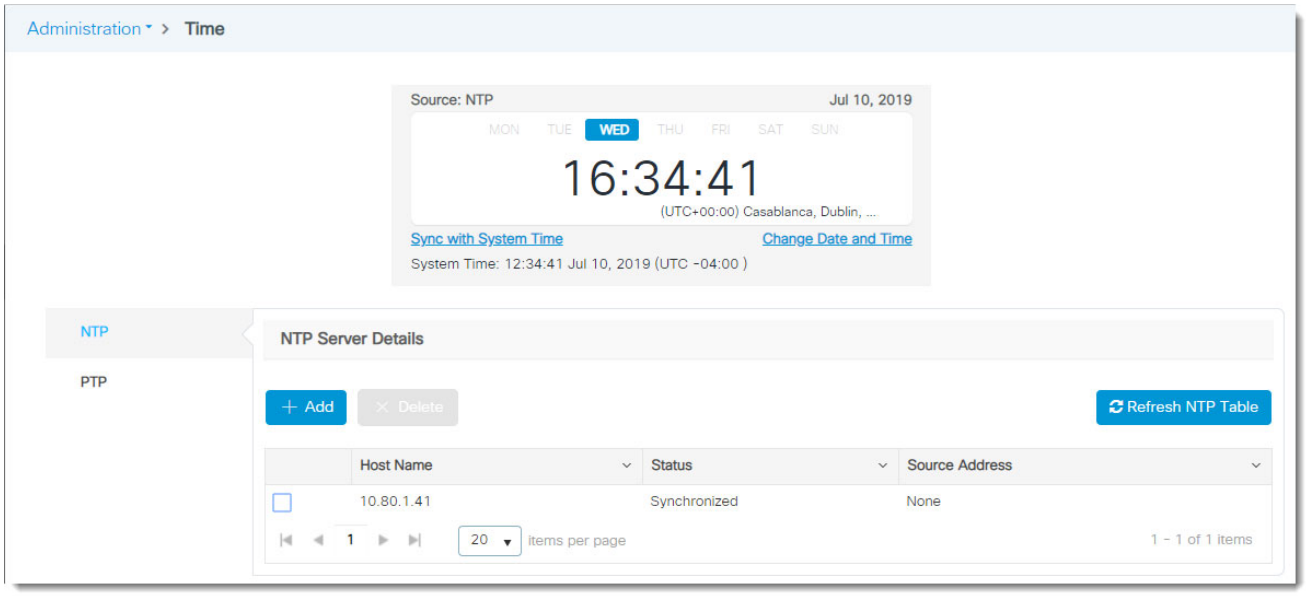
CIP Sync (PTP)

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 primary-secondary relationship among the clocks in the system. All clocks ultimately derive their time from a clock that is selected as the Grandmaster clock. For more information about PTP and CIP Sync, see the Ethernet Reference Manual, publication ENET-RM002.

Table 124 describes the PTP modes that you can apply to a Stratix 5200 or Stratix 5800 switch.

Configure Device Time Via the WebUI

From the Administration menu, choose Time.



From the Time page, you can set time manually or via NTP:

- To set time manually, see page 225.
- To set time via NTP, see page 226.

Set Time Manually

- To synchronize the time on the switch with the time on your computer, click Sync with System Time.

  The WebUI session is re-established and you are redirected to the sign in page.
- To enter date and time settings manually, click Change Date and Time, complete the fields as described in Table 122, and then click Apply to Device.

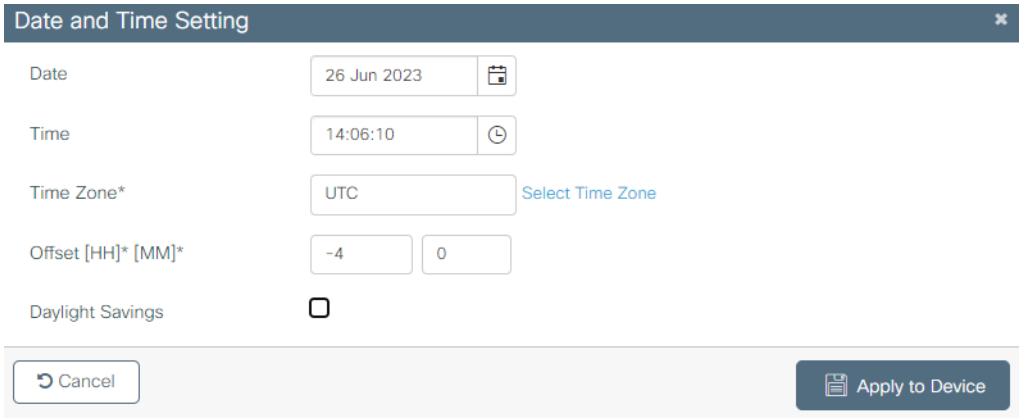
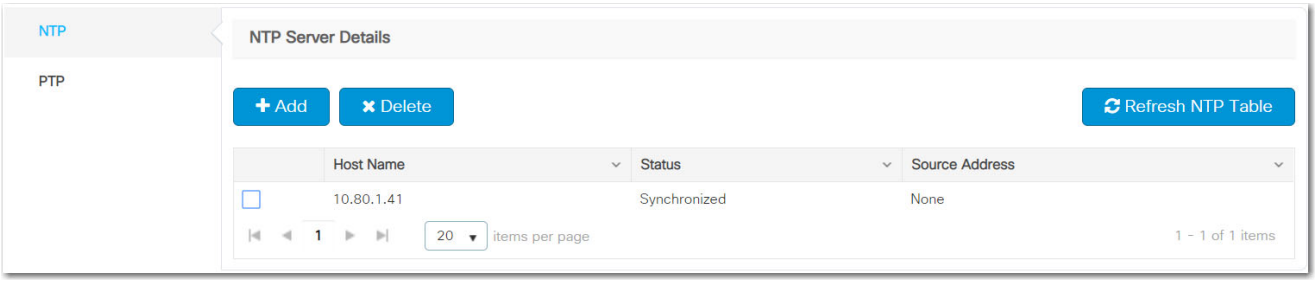


Table 122 - Date and Time Setting

Field	Description
Date	Enter the date and time to set on the device.
Time	
Time Zone	From the drop-down menu, choose a time zone. Default value: Coordinated Universal Time (UTC)
Offset [HH]* [MM]*	• HH - Hours offset from Coordinated Universal Time (UTC). Range is from –23...+23. • MM - (Optional) Minutes offset from UTC.
Daylight Saving	Check to set the Daylight Saving observance period.

Set Time Via NTP

On the Time page, click NTP.



Under NTP Server Details, you can add, edit, and delete NTP servers.

- To add an NTP server, click Add, complete the fields as described in Table 123, and then click Apply to Device.
- To edit an NTP server, click the server in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an NTP server, check its associated checkbox in the grid, and then click Delete.
- To reload the NTP server details, click Refresh NTP Table.

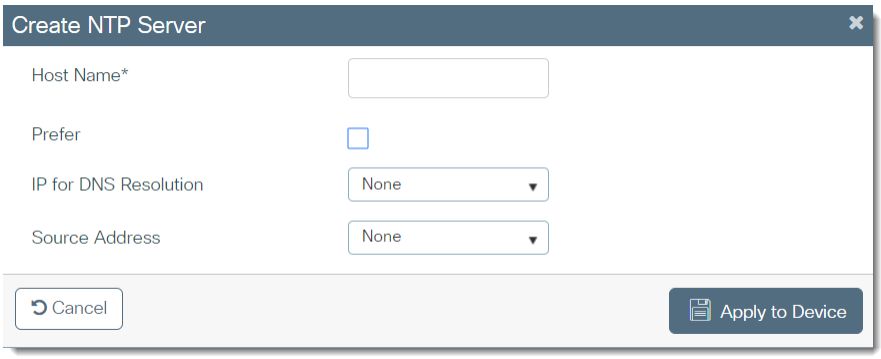


Table 123 - Create NTP Server

Field	Description
Host Name	Enter the host name or IP address to identify the NTP server.
Prefer	Check Prefer to make this server the preferred server if multiple servers are synchronized.
IP for DNS Resolution	Choose an IP protocol to resolve the DNS server name: • None (default) • IP—Uses an IPv4 address. • IPv6—Uses an IPv6 server address.
Source Address	Choose the source to use for establishing a connection to the NTP server. • None (default)—The switch automatically chooses a source. • VLAN • Interface
Vlan	If you chose VLAN in the Source Address field, choose a VLAN ID from the list.
Interface	If you chose Interface in the Source Address field, choose an interface from the list.

CIP Sync PTP

Table 124 - PTP Modes

PTP Mode	Description
Boundary	Allows the switch to participate in selecting the best master clock. If the switch does not detect a better clock, it becomes the Grandmaster clock and parent clock to all connected devices. If the best master is to be a clock that is connected to the switch, the switch becomes a child to that clock, and acts as a parent clock to devices connected to other ports. The clock selection process is determined in part by the relative priority of the switches in the network.
End to End Transparent	The switch transparently synchronizes all clocks with the master clock that is connected to it. All ports are enabled by default. The switch corrects the delay that is incurred by every packet passing through it (referred to as residence time). This mode causes less jitter and error accumulation than Boundary mode.
Forward	The switch passes PTP packets as normal multicast traffic. All switch ports are enabled by default.
NTP/PTP	This mode is also known as NTP-PTP Clock mode. Allows the switch to act as a Grandmaster. Derives PTP clock time from an NTP time source, it adds the TOD reference from NTP to PTP. If not the Grandmaster, the switch operates in Boundary mode.
End to End Transparent with Multiple VLAN	This PTP mode is only supported with Device Level Ring (DLR) for DLR's Supervisor, Gateway and Beacon nodes. For PTP over DLR, configure the DLR supervisor node in transparent clock mode with multiple VLAN support. This allows the use of multiple VLANs while maintaining a single time source on the ring.

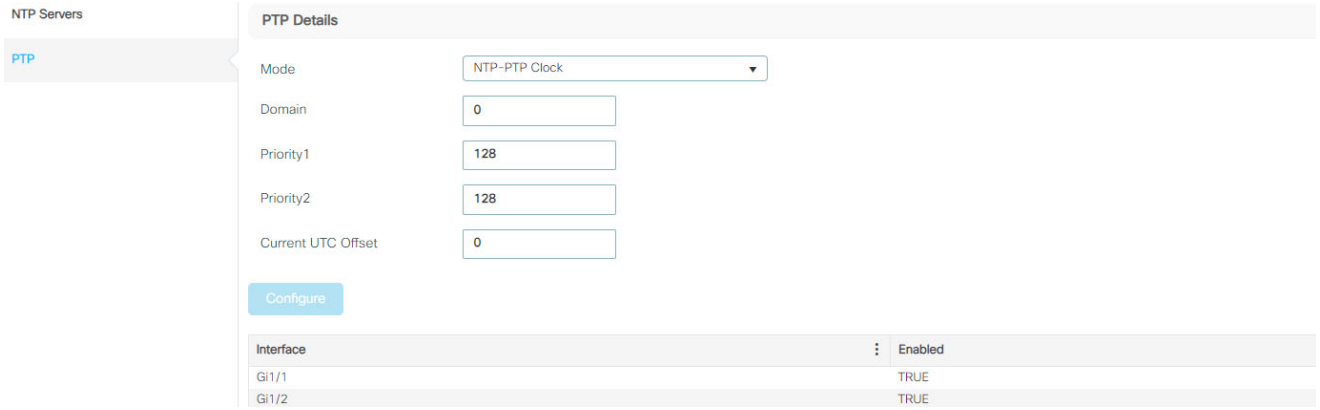
Table 125 - PTP Details

Boundary Mode	
Domain	The participating grandmaster clock, switches, and slave devices should be in the same domain. (Optional) Range: 0...255
Priority 1	First priority to override the default criteria (clock quality, clock class, and so on) for best master clock selection. Range: 0...255
Priority 2	Second priority to use as a tie-breaker between two devices that are otherwise equally matched in the default criteria. Range: 0...255
Current 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. Supported range is from 0...100.
End to End Transparent	
Domain	The participating grandmaster clock, switches, and slave devices should be in the same domain. (Optional) Range: 0...255
Forward - N/A	
NTP-PTP Clock	
Domain	The participating grandmaster clock, switches, and slave devices should be in the same domain. (Optional) Range: 0...255
Priority 1	First priority to override the default criteria (clock quality, clock class, and so on) for best master clock selection. Range: 0...255
Priority 2	Second priority to use as a tie-breaker between two devices that are otherwise equally matched in the default criteria. Range: 0...255

Table 125 - PTP Details

Current 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. Supported range is from 0...100.
End to End Transparent with Multiple VLAN	
Domain	The participating grandmaster clock, switches, and slave devices should be in the same domain. (Optional) Range: 0...255

On the Time page, click the PTP tab.



To configure PTP in NTP-PTP Clock mode, follow these steps.

1. Be sure that you have an NTP server configured as described in Set Time Via NTP on page 226.
2. From the Mode drop-down menu, choose NTP-PTP Clock.
3. Domain (Optional) - domain-number - A number from 0...255.

   The participating grandmaster clock, switches, and slave devices should be in the same domain.
4. In the Priority1 field, enter a priority value in the range of 0...255 to override the default criteria (clock quality, clock class, and so on) for best master clock selection.

   A lower value takes precedence. The default value is 128.
5. In the Priority2 field, enter a second priority in the range of 0...255 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.
6. Current UTC Offset (Optional) - A number from 0...100.
7. Click Apply to Device.

To configure PTP in Boundary mode, follow these steps.

1. From the Mode dropdown menu, choose Boundary.
2. Domain (Optional) - domain-number - A number from 0...255.

   The participating grandmaster clock, switches, and slave devices should be in the same domain.
3. In the Priority1 field, enter a priority value in the range of 0...255 to override the default criteria (clock quality, clock class, and so on) for best master clock selection.

   A lower value takes precedence. The default value is 128.
4. In the Priority2 field, enter a second priority in the range of 0...255 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.
5. Current UTC Offset (Optional) - A number from 0...100.
6. Click Apply to Device.
7. Click Configure.

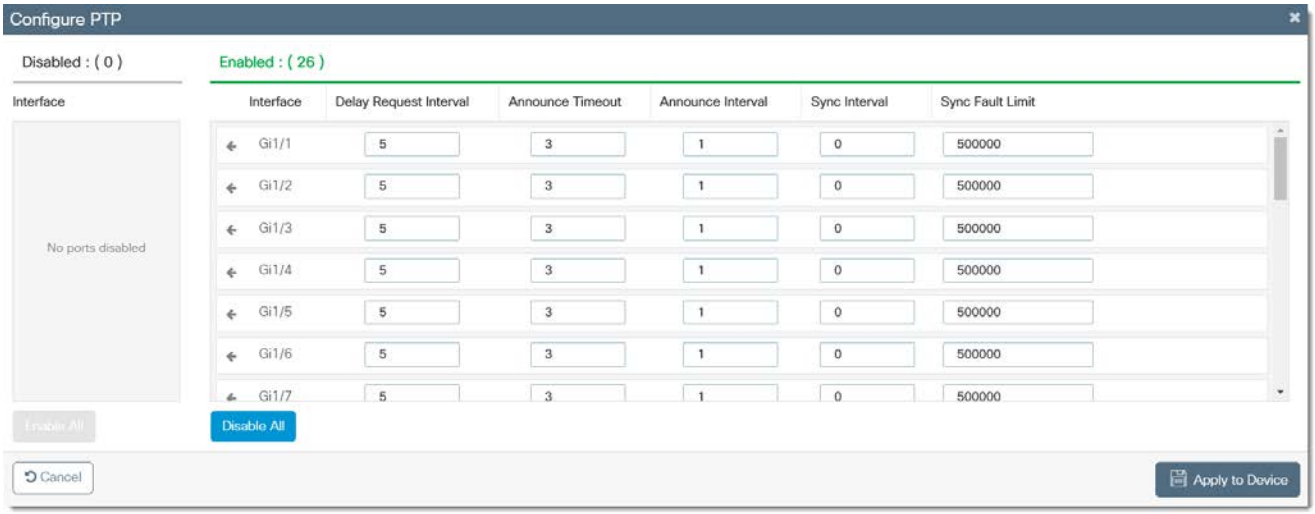


Table 126 - Configure PTP

Field	Description
Delay Request Interval	Enter the time for the member devices to send delay request messages when the port is in the master state. Valid values: -1...+6 seconds Default value: 5
Announce Timeout	Enter the time for announcing timeout messages. Valid values: 2...10 seconds Default value: 3
Announce Interval	Enter the time for sending announce messages. Valid values: 0...4 seconds Default value: 1
Sync Interval	Enter the time for sending synchronization messages. Valid values: -1...+1 seconds Default value: 1
Sync Fault Limit	Enter the maximum clock offset value before PTP attempts to resynchronize. The range is 50...500000000 nanoseconds. The default is 50,000 nanoseconds. Valid values: 50... 50000000 nanoseconds Default value: 50000

8. To disable PTP on specific interfaces, click each interface to move it from the Enabled list to the Disabled list.

   or

   To disable all interfaces, click Disable All.

9. To enable PTP on specific interfaces, click each interface to move it from the Disabled list to the Enabled list.

   or

   To enable all interfaces, click Enable All.

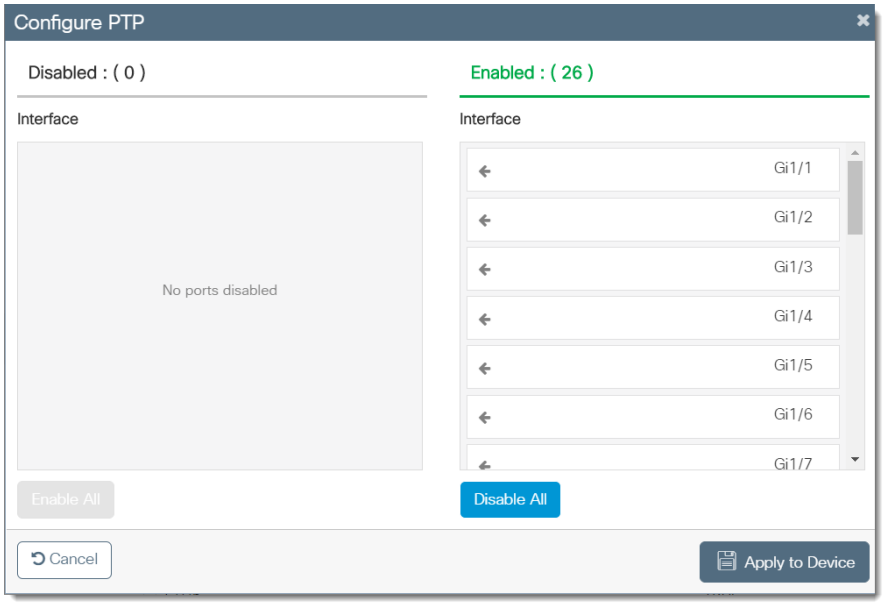
10. To change the PTP values for each interface, modify the fields as described in Table 126.
11. Click Apply to Device.

To configure PTP in End to End Transparent mode, follow these steps.

1. From the Mode dropdown menu, choose End to End Transparent.
2. Domain (Optional) - domain-number - A number from 0 to 255.

   The participating grandmaster clock, switches, and slave devices should be in the same domain.

3. Click Apply to Device.
4. Click Configure.



5. To disable PTP on specific interfaces, click each interface to move it from the Enabled list to the Disabled list.

   or

   To disable all interfaces, click Disable All.

6. To enable PTP on specific interfaces, click each interface to move it from the Disabled list to the Enabled list.

   or

   To enable all interfaces, click Enable All.
7. Click Apply to Device.

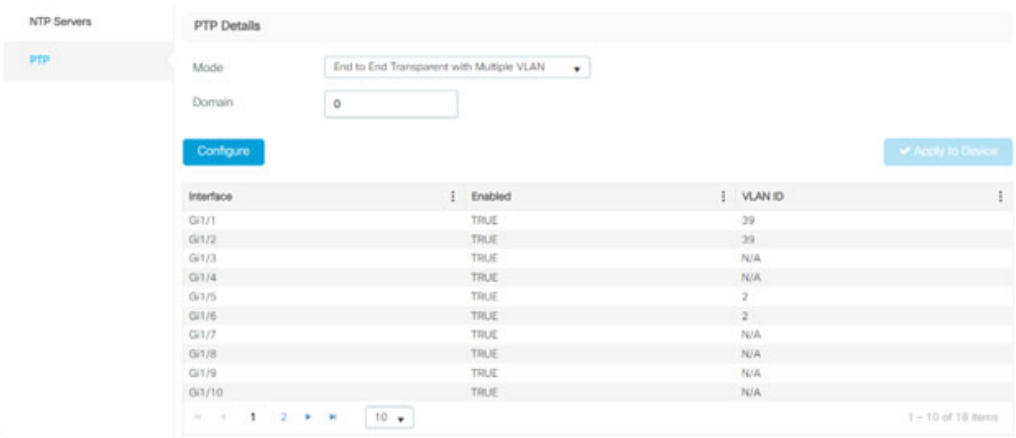
To configure PTP in Forward mode, follow these steps.

1. From the Mode dropdown menu, choose Forward.
2. Click Apply to Device.

To configure PTP in End to End Transparent with Multiple VLAN mode, follow these steps.

1. From the Mode dropdown menu, choose End to End Transparent with Multiple VLAN.
2. Domain (Optional) - domain-number - A number from 0 to 255.

   The participating grandmaster clock, switches, and slave devices should be in the same domain.
3. Click Apply to Device.
4. Click Configure.



5. To disable PTP on specific interfaces, click each interface to move it from the Enabled list to the Disabled list.

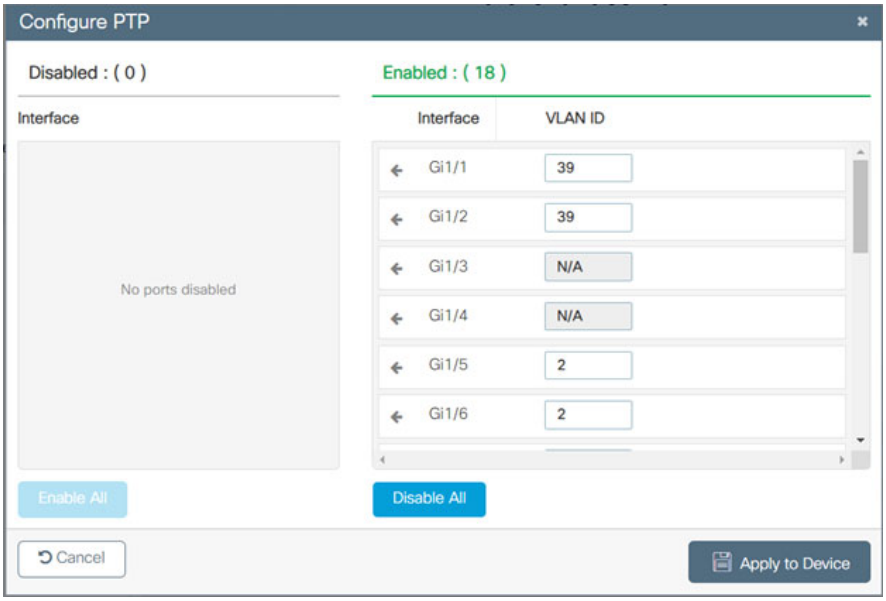
   or

   To disable all interfaces, click Disable All.
6. To enable PTP on specific interfaces, click each interface to move it from the Disabled list to the Enabled list.

   or

   To enable all interfaces, click Enable All.
7. To change the VLAN number for each interface, modify the fields under VLAN ID

8. Click Apply to Device.



Configure Device Time Via the Logix Designer Application

In the Logix Designer application, you can manage device time in these ways:

- To configure CIP Sync Time (PTP), see page 232
- To view CIP Sync Time information, page 235
- To manage NTP servers, see page 236

Configure CIP Sync Time (PTP)

1. In the navigation pane, click Time Sync Configuration.
2. From the Clock Type dropdown menu, choose a mode.

   For a description of each mode, see Table 121 on page 224.
3. Complete the fields, and then click Set:
   - To configure Boundary mode, see page 233.
   - To configure End to End Transparent mode, see page 234.

   There is no configuration for Forward mode.

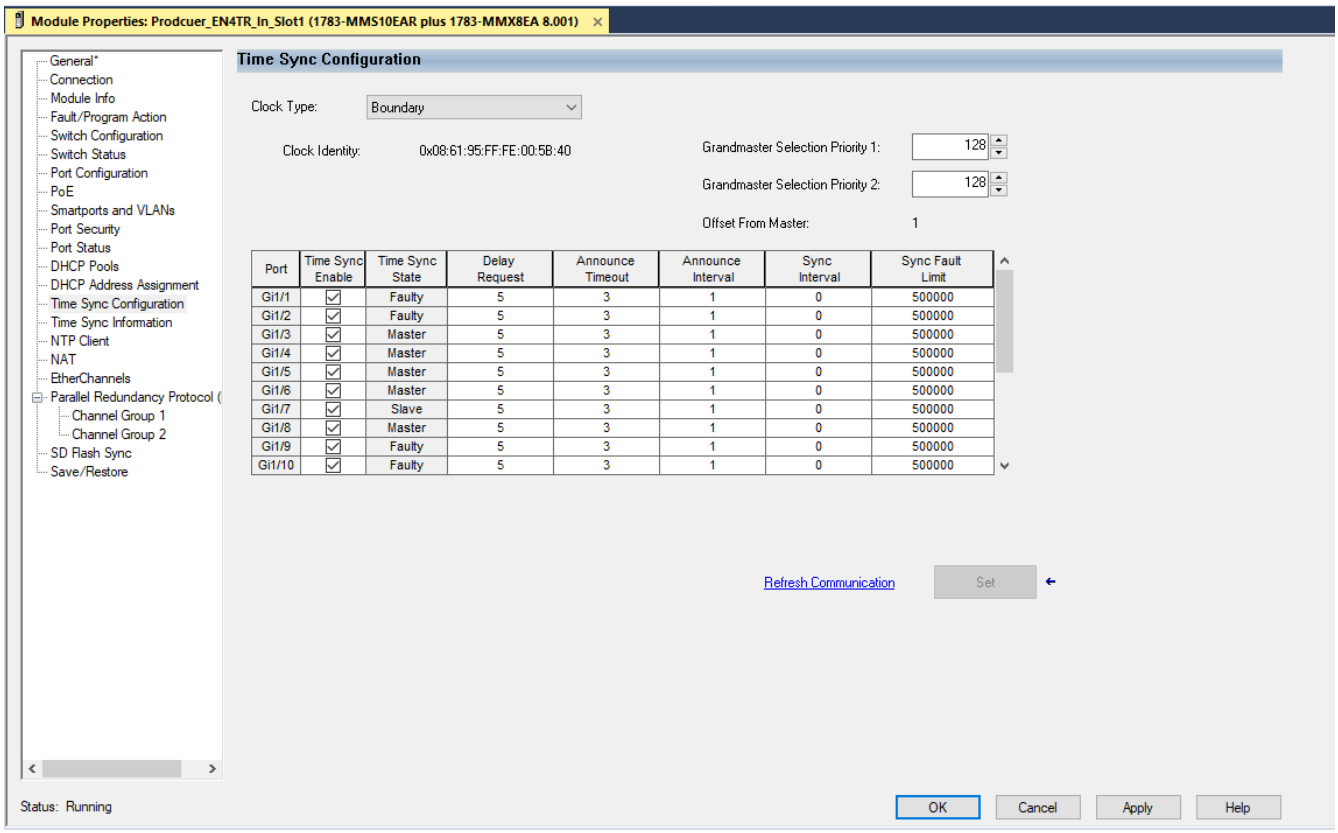


Table 127 - Boundary Mode

Field	Description
Clock Identity	Displays a unique identifier for the clock.
Grandmaster Selection Priority1	Type a value to override the default criteria (clock quality, clock class, and so on) for the best master clock selection. A lower value takes precedence. Valid values: 0...255 Default: 128
Grandmaster Selection Priority 2	Type a value to use as a tie-breaker between two devices that are otherwise equally matched in the default criteria. For example, you can give a specific switch priority over other identical switches. A lower value takes precedence. Valid values: 0...255 Default: 128
Offset from Master	Displays the time offset in nanoseconds between the slave and master clocks.
Port	Displays the port type and number.
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 ports.
State	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 synchronizing with the parent or Grandmaster clock. • Faulty—Either PTP is not operating properly on the switch port or nothing is connected to the port. • Disabled—PTP is not enabled on the switch port.
Delay Request	The logarithmic mean interval in seconds for connected devices to send delay request messages when the switch port is in the master state. Default value: 5 (32 seconds)
Announce Timeout	The number of announce intervals 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 value: 3 (8 seconds)

Table 127 - Boundary Mode (Continued)

Field	Description
Announce Interval	The logarithmic mean time interval in seconds for sending announce messages. Valid values: • 0…1 second • 1…2 seconds • 2…4 seconds • 3…8 seconds • 4…16 seconds Default value: 1 (2 seconds)
Sync Interval	The logarithmic mean time interval in seconds for sending synchronization messages. Valid values: • -1…half second • 0…1 second • 1…2 seconds Default value: 0 (1 second)
Sync Fault Limit	Type the maximum clock offset before PTP attempts to reacquire synchronization. Valid values: 50…500000000 nanoseconds Default value: 50,000 nanoseconds **IMPORTANT:** We recommend against setting the sync limit below the default (50,000 nanoseconds). Use values below 50,000 nanoseconds only in networks with a very high-precision Grandmaster clock. These networks have a critical need to keep sensitive devices synchronized.

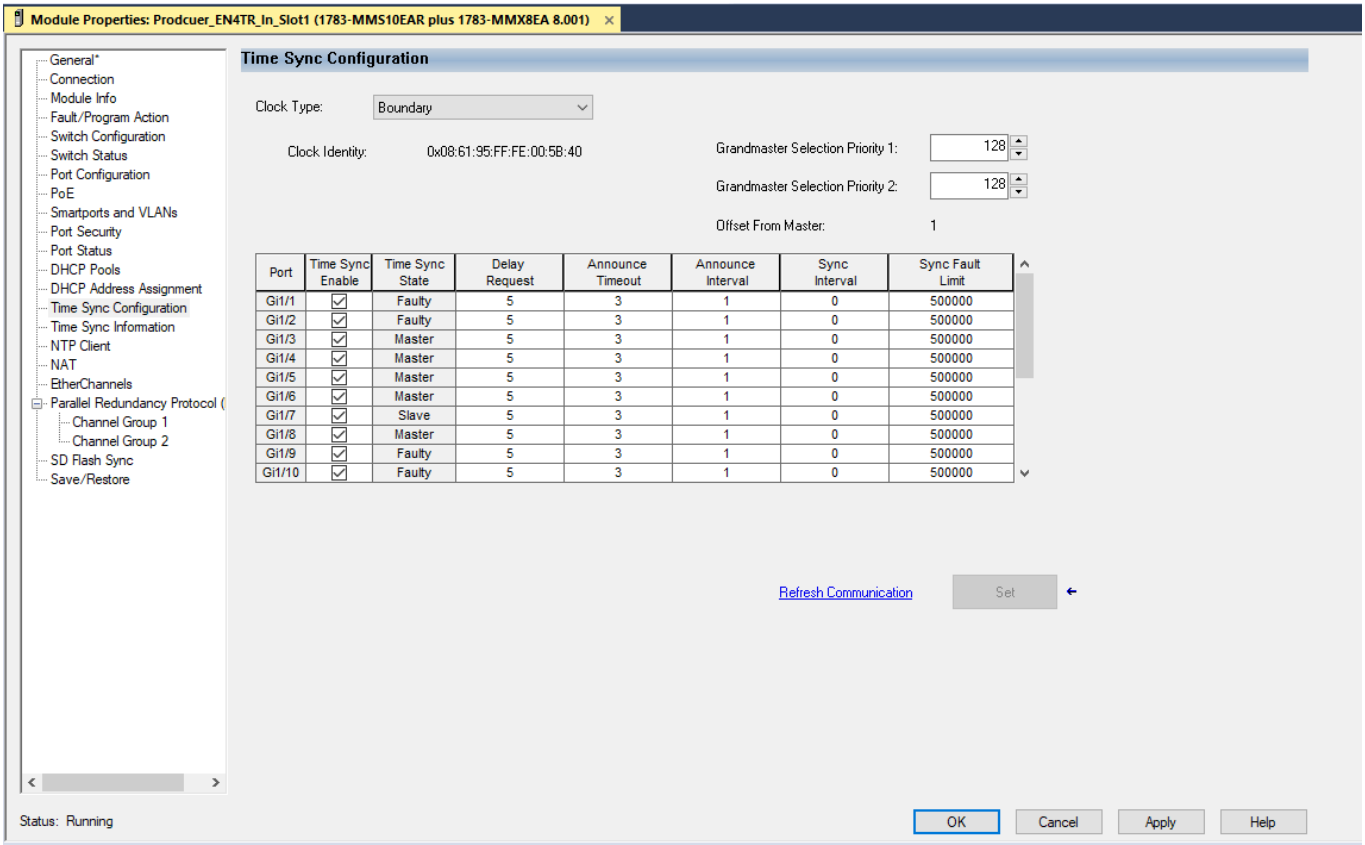


Table 128 - End to End Transparent Mode

Field	Description
Port	Displays the port type and number.
Time Sync Enable	To enable or disable time synchronization on a port, check or clear its associated Time Sync Enable checkbox.

View Time Sync Information

The Time Sync Information view shows current information about the real-time clocks in the network.

In the navigation pane, click Time Sync Information.

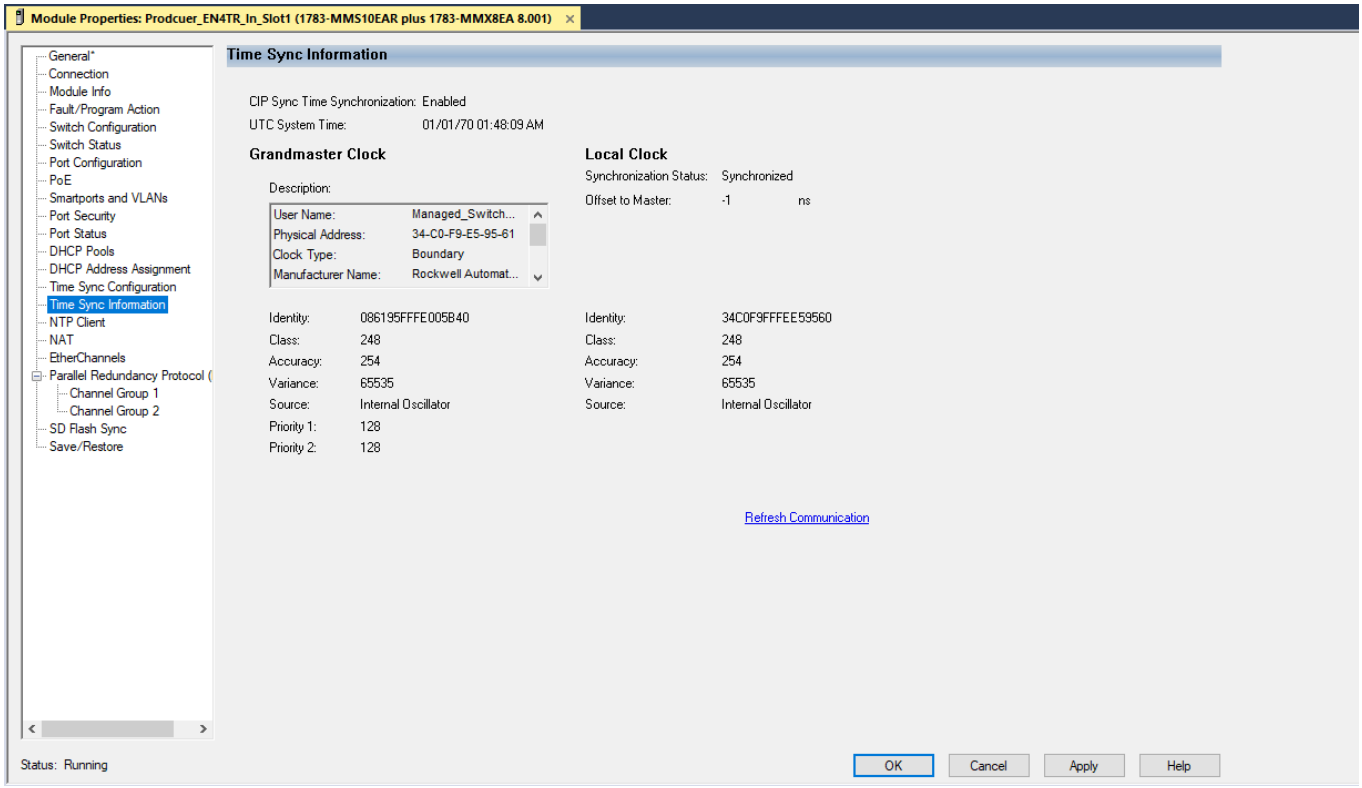


Table 129 - Time Sync Information

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 clock type.
Identity	Displays the unique identifier for the Grandmaster clock. The format depends on the network protocol.
Class	Displays a measure of the quality of the Grandmaster clock. Values are defined from 0...255 with 0 as the best clock.
Accuracy	Indicates the expected absolute accuracy of the Grandmaster clock relative to CIP Sync time synchronization epoch (31 December 1969 23:59:51.99918 UTC). The accuracy is specified as a graduated scale starting at 25 ns and ending at greater than 10 seconds or unknown. For example, a GPS time source has an accuracy of approximately 250 ns. A hand-set clock typically has an accuracy less than 10 seconds. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the Grandmaster clock. The value is in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the clock time source: • Atomic Clock • GPS • Terrestrial Radio • CIP Time Synchronization • NTP • HAND Set • Other • Internal Oscillator
Priority 1 Priority 2	Displays the relative priority of the Grandmaster clock to other clocks in the system. The value is between 0...255. The highest priority is 0.

Table 129 - Time Sync Information (Continued)

Field	Description
Local Clock	
Synchronization Status	Displays whether the local clock is synchronized or asynchronized with the Grandmaster clock.
Offset to Master	Displays the offset value between the local clock and the master clock.
Identity	Displays the unique identifier for the local clock. The format depends on the network protocol. • The Ethernet protocol encodes the MAC 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 starting at 25 ns and ending at greater than 10 seconds or unknown. For example, a GPS time source has an accuracy of approximately 250 ns. A hand-set clock typically has an accuracy less than 10 seconds. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the local clock. The value is in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the clock time source: • Atomic Clock • GPS • Terrestrial Radio • CIP Time Synchronization • NTP • HAND Set • Other • Internal Oscillator

Manage NTP Servers

In the navigation pane, click the NTP Client.

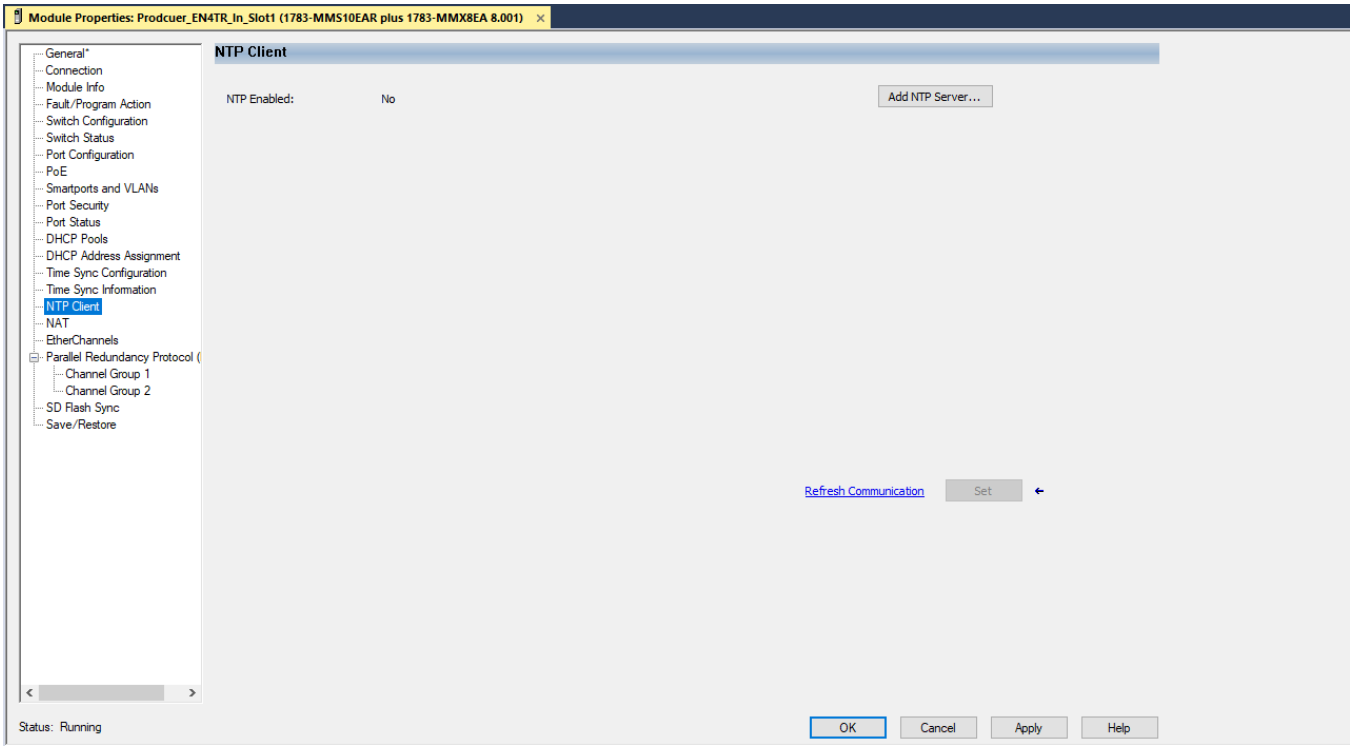


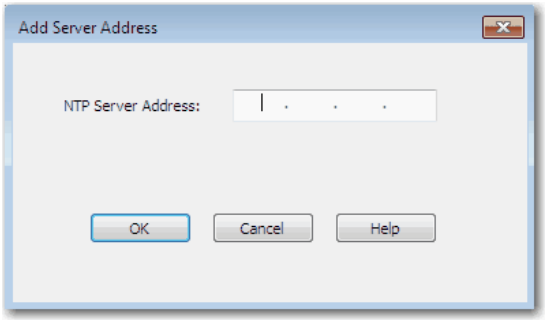
Table 130 - NTP Client

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 Servers	
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.

On the NTP Client view, you can add and delete NTP servers:

- To add an NTP server, see the following procedure.
- To delete an NTP server, click the Trash icon in the Delete column.
- To reload the NTP server details, click Refresh Communication.

1. Click Add NTP Server.



2. In the NTP Server Address field, enter one of the following, and then click OK:
   - For a peer association, enter the IP address of the peer providing, or being provided, the clock synchronization.
   - For a server association, enter the IP address of the time server providing the clock synchronization.

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

Command-line Interface (CLI)

Apart from software and web-based applications, you can manage the switch via the Cisco® command-line interface (CLI). The CLI enables you to execute Cisco IOS commands. Technical Support representatives from Rockwell Automation can also use the CLI to troubleshoot the switch. For more information about the CLI, refer to www.cisco.com.

For other Stratix® switches, the CLI is accessible only via a console port, Telnet session, or Secure Shell (SSH) session. The CLI is available via the same methods as other switches, but they also provide access to the CLI via the WebUI.

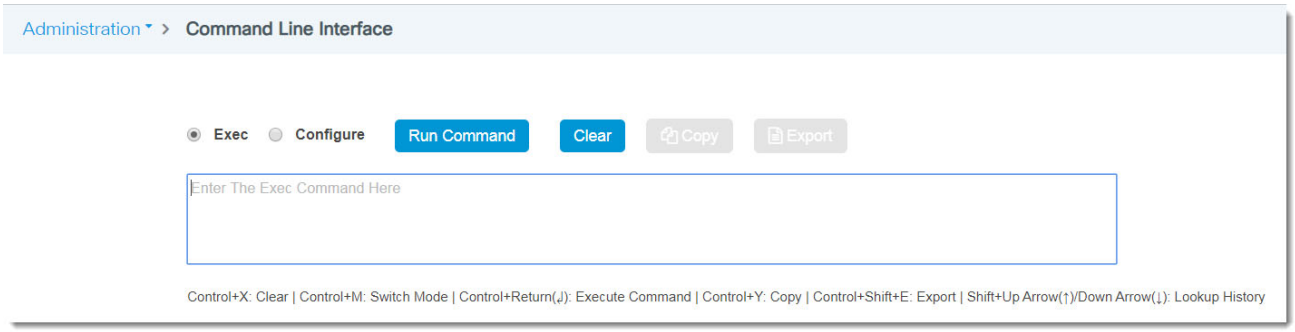
CLI Modes

Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode you are currently in. The WebUI provides two command modes:

- Exec mode—Most commands in Exec mode are one-time commands. For example, show commands provide important status information, and clear commands clear counters or interfaces.
- Configure mode—Configure mode enables you to make changes to the running configuration.

Run CLI Commands Via the WebUI

From the Administration menu, choose Command Line Interface.



From the Command Line Interface page, you execute and manage commands:

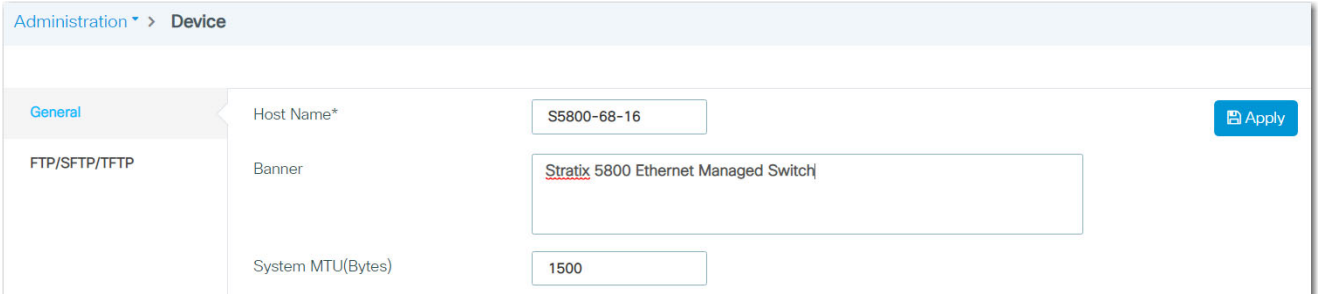
- To run a command, click a CLI mode, enter the command in the text box, and then click Run Command. The command output appears in the bottom area of the page.
- To delete commands or output, click Clear.
- To copy the command output to your clipboard, click Copy.
- To export the command output to a text file on your local computer, click Export.

Device Settings

Device settings are system-wide values for the switch.

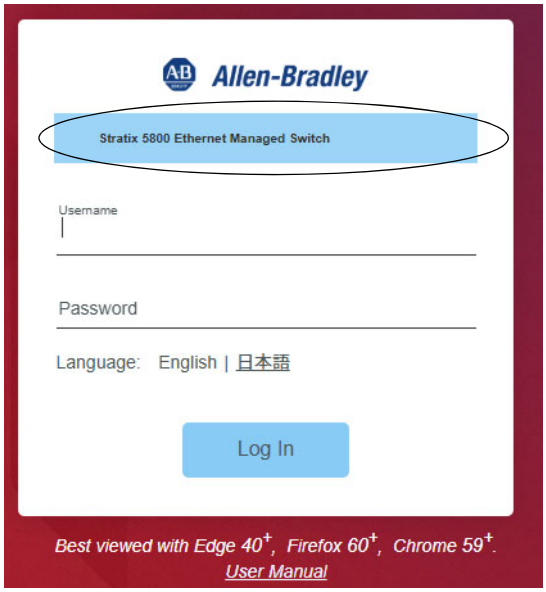
Configure Device Settings via the WebUI

From the Administration menu, choose Device.



On the General tab, complete the fields as described in Table 131, and then click Apply to Device.

Table 131 - Device Settings—General

Field	Description
Host Name	Enter a unique name to identify the switch.
Banner	To display a message on the Login page of the WebUI, enter the text to appear in the banner area, as shown in the following example. 
System MTU (Bytes)	Enter the maximum transmission unit (MTU) value in bytes for all interfaces on the switch that operate at 10 Mbps or 100 Mbps or 1000 Mbps (1 Gbps). Valid values: 1500...1998 Advanced SKU valid values: 1500...2000 Non-advanced SKU valid values: 1500...8996 Default value: 1500 **NOTE**: If you set an odd number for the System MTU size, an error appears.

On the FTP/TFTP tab, complete the fields in Table 132, and then click Apply.

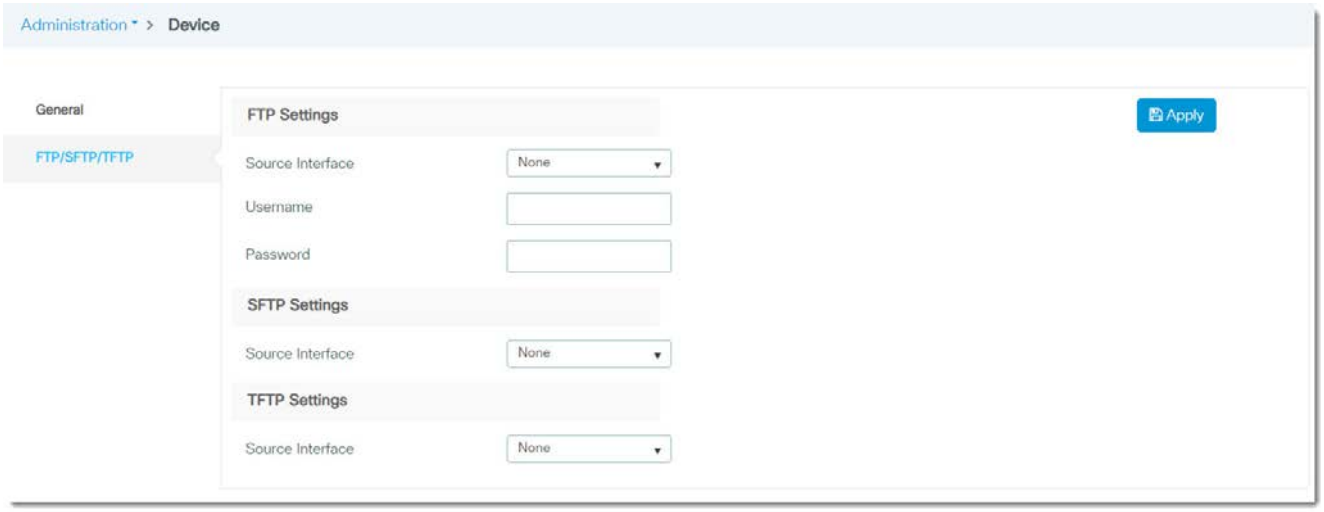


Table 132 - Device Settings—FTP/SFTP/TFTP

Field	Description
FTP Settings	
Source Interface	Choose the interface on the switch to use during any FTP session.
User name	Enter the user name.
Password	Enter the password.
SFTP Settings	
Source Interface	Choose the interface on the switch to use during any SFTP session.
TFTP Settings	
Source Interface	Choose the interface on the switch to use during any TFTP session.
User name	Enter the user name.
Password	Enter the password.

Configure Device Settings Via the Logix Designer Application

Configure Connection Properties

1. In the navigation pane, click Connection.
2. Complete the fields as described in Table 133, and then click Apply.

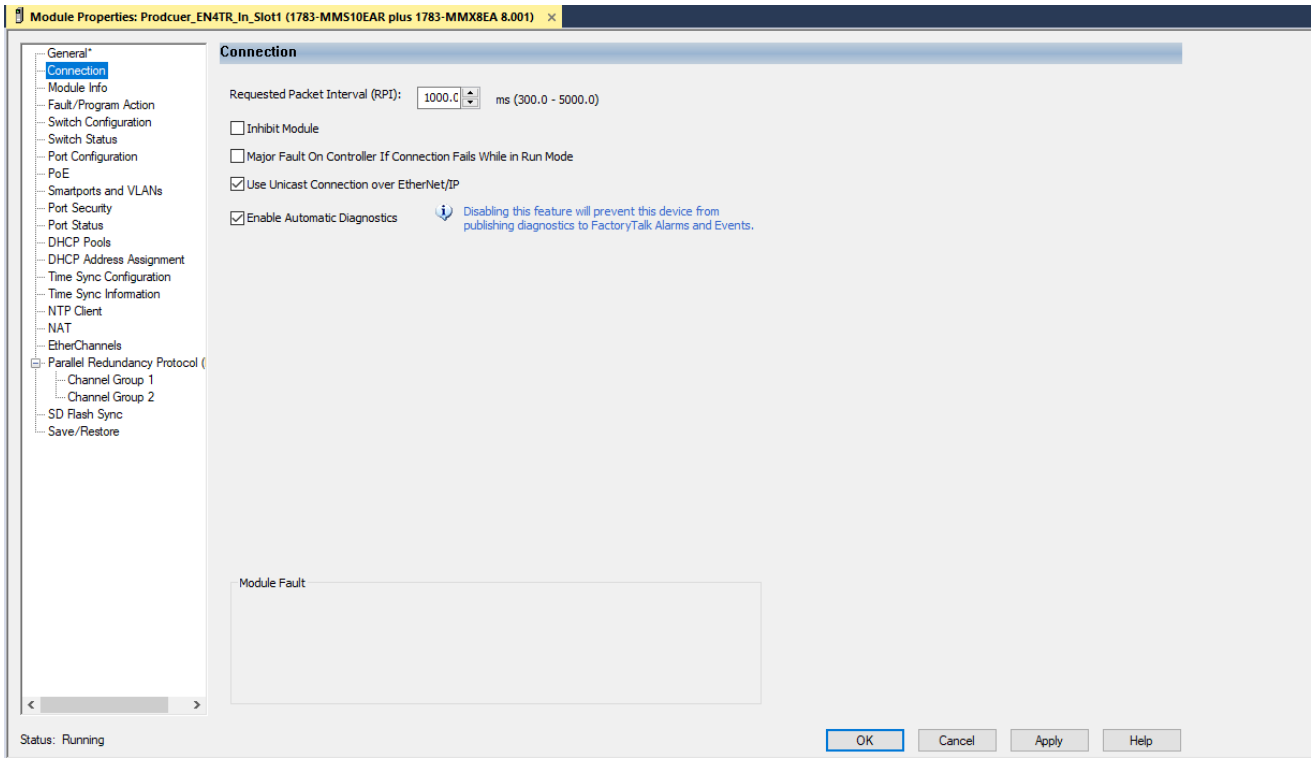


Table 133 - Connection Fields

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.

Configure Switch Information

In the navigation pane, click Switch Configuration.

3. Complete the fields as described in Table 133, and then click Apply.

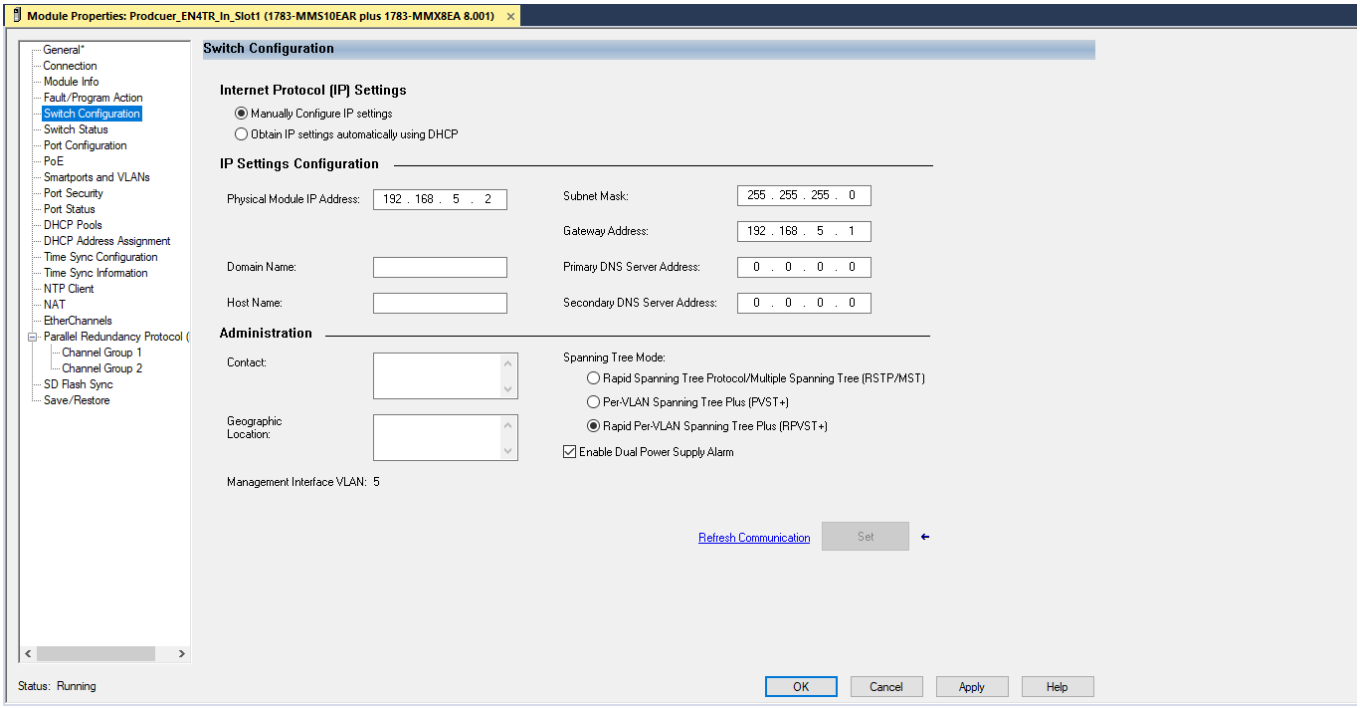


Table 134 - Switch Configuration

Field	Description
Internet Protocol (IP) Settings	
Manually configure IP settings or Obtain IP settings automatically using DHCP	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 the switch has a static IP address and your network uses a DHCP server, make sure that the IP address is not within the range of DHCP address pool. Otherwise, IP address conflicts can occur between the switch and another device. • Obtain IP settings automatically using DHCP—A Dynamic Host Configuration Protocol (DHCP) server automatically assigns the switch an IP address, subnet mask, and default gateway. • Unless restarted, the switch continues to use the DHCP-assigned information. We recommend that you manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the switch.
IP Settings Configuration—Applies to manually assigned IP addresses.	
Physical Module IP Address	Enter the IP address for the switch. 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 Apply. 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	Enter the subnetwork (subnet) for the switch. 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.
Gateway Address	Enter the gateway address for the switch. 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. 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.
Primary DNS Server Address	Enter the IP addresses of the primary domain name system (DNS) IP server available to a DHCP client.
Secondary DNS Server Address	Enter the secondary domain name system (DNS) IP server available to a DHCP client.
Host Name	Enter a name to identify the switch. The name can be up to 64 characters and can include alphanumeric and special characters (comma and dash).
Administration	

Table 134 - Switch Configuration (Continued)

Field	Description
Contact	(Optional). Enter contact information for the switch. The contact information can include a maximum of 200 characters, alphanumeric and special characters (dash and comma), and a carriage return.
Geographic Location	(Optional). Enter a geographic location of the switch. The geographic location can include a maximum of 200 characters, alphanumeric and special characters (dash and comma), and a carriage return.
Management Interface VLAN	Displays the VLAN through which the switch is managed. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. It also provides secure administrative access to all devices in the network. **IMPORTANT:** Be sure that the switch and your network management station are in the same VLAN. Otherwise, you can lose management connectivity to the switch.
Spanning Tree Mode	See Configure STP via the Logix Designer Application on page 185.
Enable Dual-Power Supply Alarm	To enable dual-power supply alarms, check the checkbox.

Device Time

You can set the time on the switch by using the following methods:

- Set the time manually
- Set the time via a Network Time Protocol (NTP) server

Set Time Manually

If you do not use a network-based method of synchronizing time, such as NTP or PTP, you can set the time of the switch by using these methods:

- Sync the switch time with the time on your computer
- Manually complete the fields in the WebUI

IMPORTANT	Manual time settings override time and date settings from the NTP server.

Set Time Via NTP

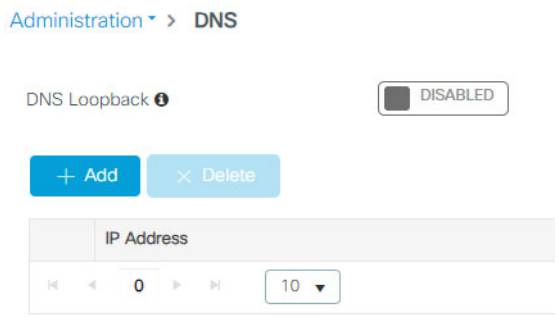
Network Time Protocol (NTP), defined in RFC 1305, synchronizes clocks across packet-based networks. NTP uses a two-way time transfer mechanism between a master and a slave. For more information about NTP, see the Ethernet Reference Manual, publication ENET-RM002.

Domain Name System (DNS)

DNS is a name resolution protocol that enables you to identify devices by names rather than IP addresses. For DNS to work, a DNS server is configured to hold a table of names and the associated IP addresses. When a device attempts to send a message to a device with an unknown name, it requests the IP address of the named device from the DNS server. For more information about DNS, see the Ethernet Reference Manual, publication ENET-RM002.

Add a DNS Server Via the WebUI

From the Administration menu, choose DNS.



From the DNS page, you can add, edit, and delete DNS servers:

- To add a DNS server, click Add, complete the fields as described in Table 135, and then click Apply to Device.
- To edit a DNS server, click the server in the grid, modify the fields, and then click
- To delete a DNS server, click its associated checkbox in the grid, and then click Delete.

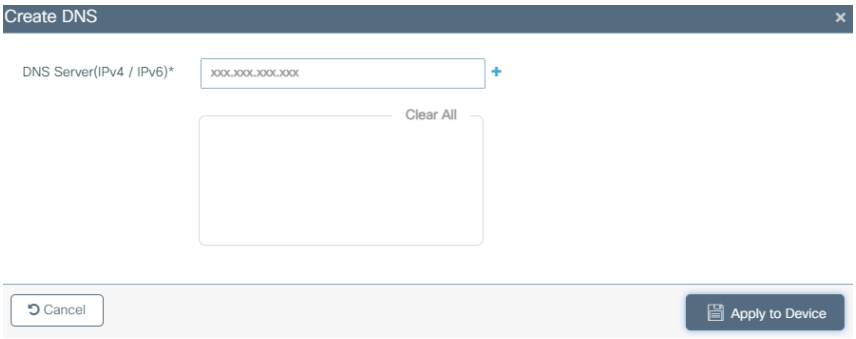


Table 135 - Create DNS

Field	Description
DNS Server (IPv4/IPv6)	Enter the IP address of a DNS server and click + to add it to the list. You can add multiple DNS servers for backup.
[DNS server list]	To change the order of DNS servers in the list, click a server in the list, and then click the up and down arrows.
	IMPORTANT: The first server in the list is the primary server. The device sends DNS queries to the primary server first. If that query fails, the device queries the backup servers.

Dynamic Host Configuration Protocol (DHCP)

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. The switch can operate as a DHCP server by automatically assigning IP addresses to connected devices. If a device leaves and then rejoins the network, the device receives the next available IP address. For more information about DHCP, see the Ethernet Reference Manual, publication ENET-RM002.

DHCP Persistence

DHCP persistence, or port-based address allocation, is a feature that enables DHCP to maintain the same IP address on an Ethernet switch port. The device that is connected to that port always receives the same IP address regardless of the MAC address of the connected device. You can assign an IP address from an IP address pool.

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, a 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.

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 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.

Figure 38 - DHCP Persistence

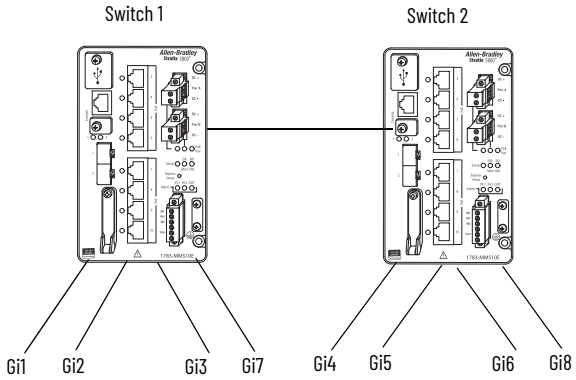


Table 136 - DHCP Persistence Behavior

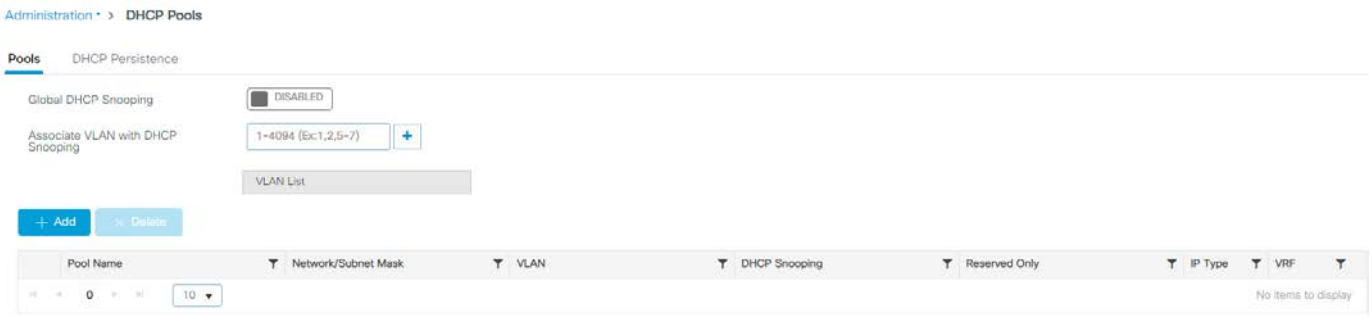
If	Then
• Switch 1 has ports Gi1...Gi3 in its persistence table • Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table • Reserved Only is disabled and DHCP snooping is disabled	A new device that is connected to switch 1 Gi1 receives an IP address from the switch 1 persistence table. A broadcast 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 Gi1...Gi3 in its persistence table • Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table • Reserved Only is enabled in both switches and DHCP snooping is disabled	A new device that is connected to switch 1 Gi1 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 Gi7 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 Gi1...Gi3 in its persistence table • Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table • Reserved Only is enabled in switch 1 and DHCP snooping is disabled • Reserved Only is disabled in switch 2	A new device is connected to Gi1 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 Gi4 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 Gi1...Gi3 in its persistence table • Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table • DHCP Snooping is enabled • Reserved Only is enabled	A new device that is connected to switch 1 Gi1 receives an IP address from the persistence table in switch 1. A broadcast request is not sent across the network, so switch 2 does not respond. If a device is connected to Gi7 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 Gi1...Gi3 in its persistence table • Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table • DHCP Snooping is enabled • Reserved Only is enabled	A new device that is connected to switch 1 Gi1 receives an IP address from the persistence table in switch 1. A broadcast request is not sent across the network, therefore switch 2 does not respond. If a device is connected to Gi7 (not defined in the DHCP persistence table) of switch 1, it receives an unassigned IP address from the switch 1 pool.

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.

Configure DHCP Via the WebUI

From the Administration menu, choose DHCP Pools.

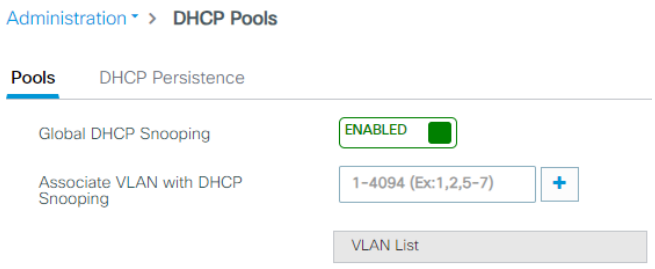


From the DHCP page, you can enable or disable DHCP snooping and configure DHCP pools and DHCP persistence:

- To enable or disable DHCP snooping, see page 247.
- To configure DHCP pools, see page 248.
- To configure DHCP persistence, see page 249.

Enable or Disable DHCP Snooping

On the Pools tab, click to enable or disable Global DHCP snooping. By default, DHCP snooping is enabled. A message appears in the lower-right corner of the WebUI to confirm that the configuration was successfully applied.



Configure DHCP Pools

On the Pools tab, you can add, edit, and delete DHCP pools:

- To add a pool, click Add, complete the fields as described in Table 137, and then click Apply to Device.
- To edit a pool, click the pool in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a pool, check its associated checkbox in the grid, and then click Delete.

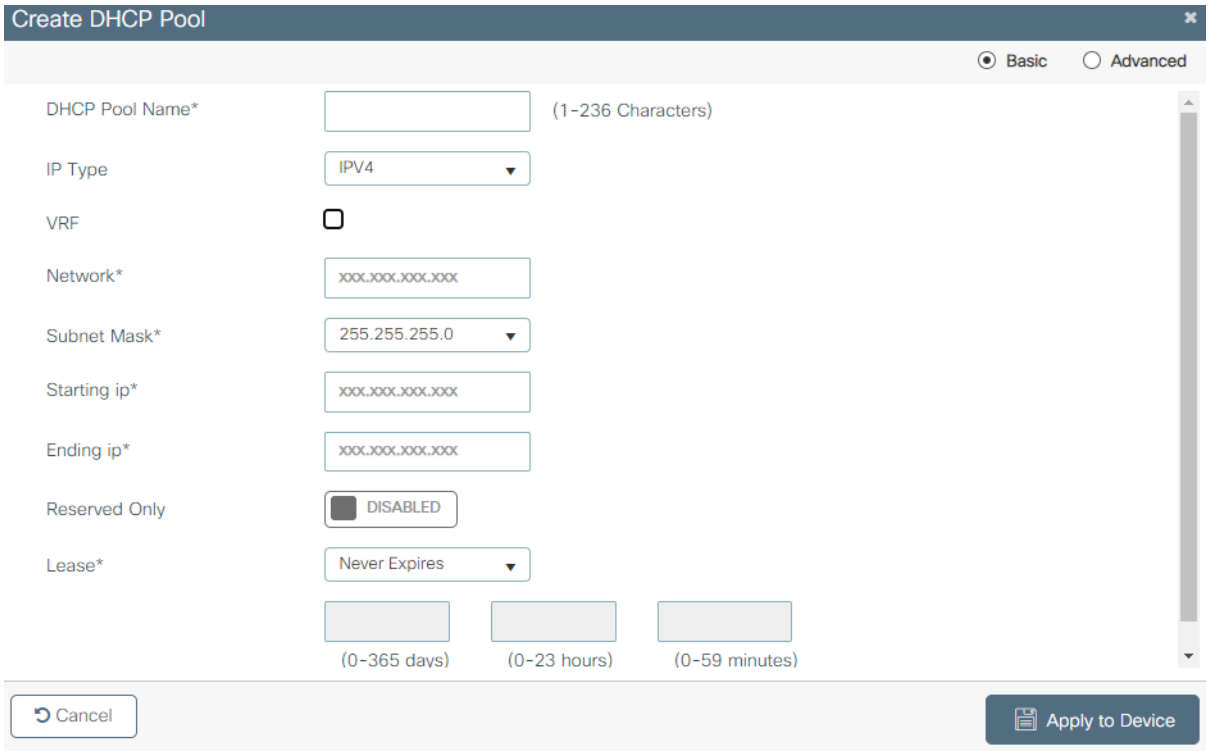


Table 137 - Create DHCP Pool

Field	Description
Basic or Advanced	Click to determine the fields that appear on the Create DHCP Pool page: • Basic (default)—Only basic fields on appear on the page. • Advanced—Both basic and advanced fields appear on the page. Advanced fields include configuration of Domain Name System (DNS) or • NetBIOS™ servers for IPv4 address types.
Basic	
DHCP Pool Name	Enter a unique name for the DHCP address pool.
IP Type	Choose the IP protocol to use for this DHCP address pool. • IPV4 (default) • IPV6
IPV4	
VRF (Stratix 5800 Switch Only)	Choose a Virtual Routing and Forwarding (VRF) instance to assign to the DHCP Pool.
Network	Enter the IP address of the network served by this DHCP address pool. This IP address is used by the management interface with Netmask applied, as configured on the Interface page.
Subnet Mask	Choose the subnet mask to assign to the DHCP clients.
Starting IP	Enter the first of the contiguous addresses in the DHCP address pool. Any new DHCP client joining the LAN receives an IP address between this starting address and the ending address.
Ending IP	Enter the last contiguous address in the address pool.
Reserved Only	To limit address assignments to only ports that are defined in the DHCP persistence table, click to enable Reserved Only.

Table 137 - Create DHCP Pool (Continued)

Field	Description
Lease	Choose the duration of the lease for an IP address that is assigned to a DHCP client: • Never Expires (default)—The DHCP client can use the assigned IP address indefinitely. • User Defined—The DHCP client can use the assigned IP address for a limited time. If you choose User Defined, enter the duration of the lease in the numbers of days, hours, and minutes.
IPV6	
DNS Server(s)	Enter the IP addresses of a DNS server for a DHCP client, and then click the plus sign to add the translation to the grid. Repeat for each address.
DNS Domain Name	Enter the domain name for the DHCP client, and then click the plus sign to add the name to the grid. Repeat for each domain name. The name can have a maximum of 31 alphanumeric characters. The name cannot contain a ? or a tab.
IPV6 Address Allocation	Enter an IP addresses allocated to IPV6 protocol, and then click the plus sign to add the address to the grid. Repeat for each address.
Advanced	
Enable DNS Proxy	(Appears only for IPv4 address types). Check Enable DNS Proxy to add default routers to DNS servers.
DHCP Options List—DHCP provides an internal framework for passing configuration parameters and other control information to clients on your network. DHCP options carry parameters as tagged data stored within protocol messages that are exchanged between the DHCP server and its clients.	
DHCP Options	Enter a DHCP option value from 2...251 and click Add. You can also enter a range of options, such as 7...11.
Options Value	Enter a string value for the DHCP option.

Configure DHCP Persistence

On the DHCP Persistence tab, click an interface in the grid, modify the fields as described in Table 138, and then click Update & Apply to Device.

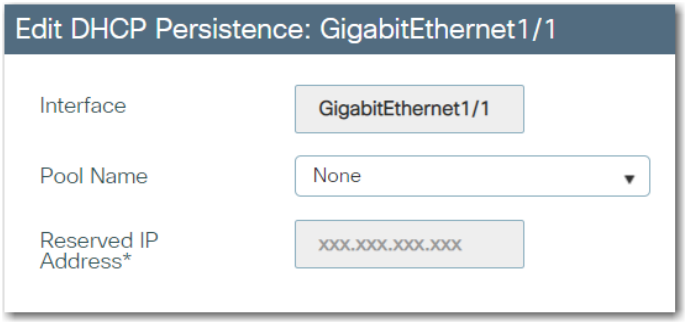
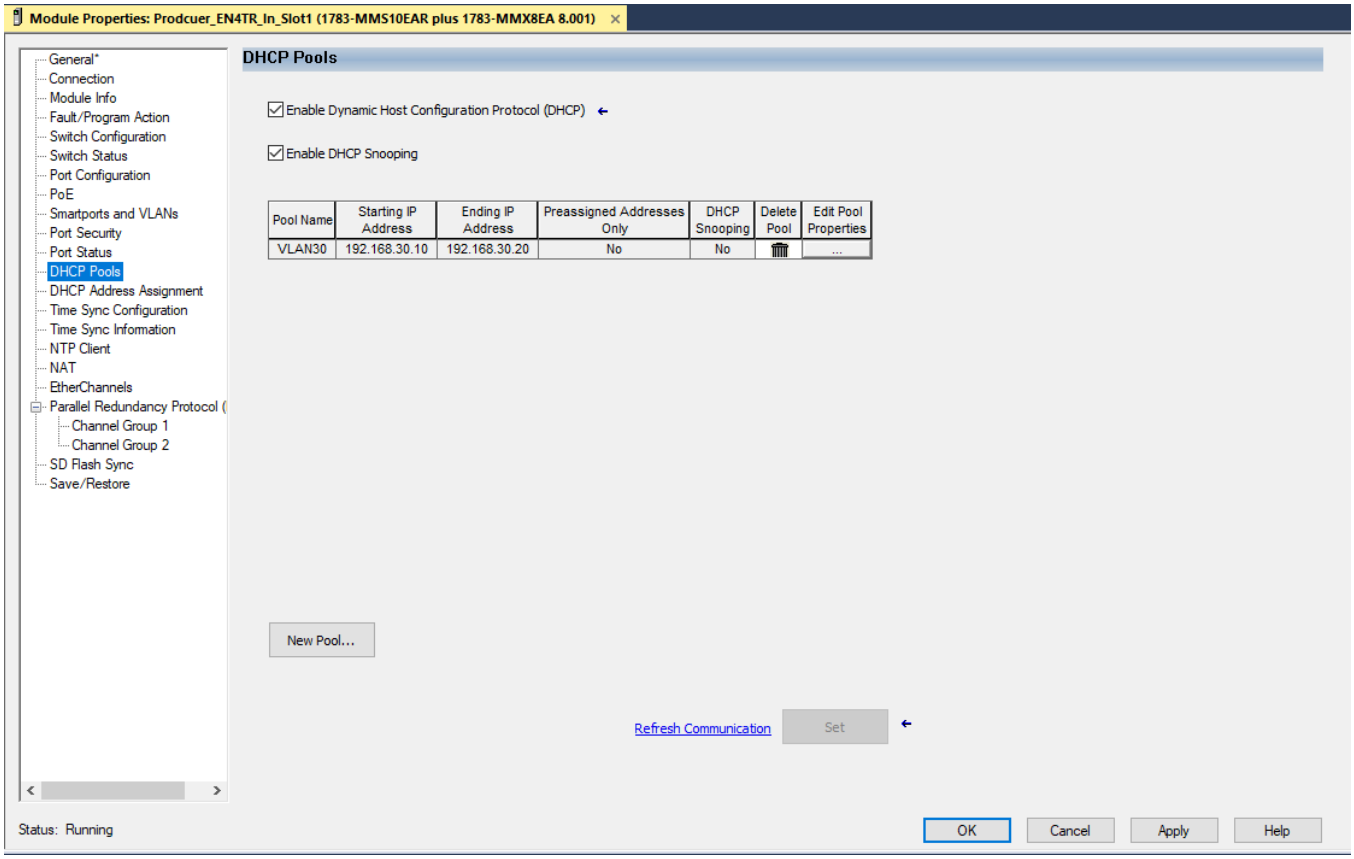


Table 138 - DHCP Persistence

Field	Description
Interface	Displays the interface type and number.
Pool Name	Choose the DHCP address pool that includes the IP address to assign to this interface.
Reserved IP Address	Enter the IP address reserved for the device that connects to this interface. The IP address that you assign is reserved for only this port and is not available for normal DHCP dynamic assignment. The IP address must be in the range of the assigned DHCP address pool.

Configure DHCP Via the Logix Designer Application

In the navigation pane, click DHCP Pools.



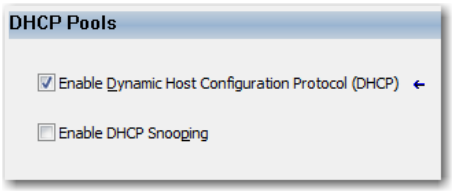
From the DHCP Pools view, you can enable or disable DHCP and DHCP snooping and configure DHCP pools:

- To enable or disable DHCP and DHCP snooping, see page 251.
- To add a DHCP pool, see page 251.
- To edit a DHCP pool, click the Ellipses icon in the Edit Pool Properties column, modify the fields, and then click Close.
- To delete a DHCP pool, click the Trash icon in the Delete Pool column.
- To configure DHCP persistence, see page 252.

Enable or Disable DHCP or DHCP Snooping

On the DHCP Pools view, check the checkboxes to enable DHCP and DHCP snooping. Clear the checkboxes to disable the features.

By default, DHCP is enabled, and DHCP snooping is disabled.



Add a DHCP Pool

1. Click New Pool.
2. Complete the fields as described in Table 139, click Set, and then click Close.
3. Click Apply.

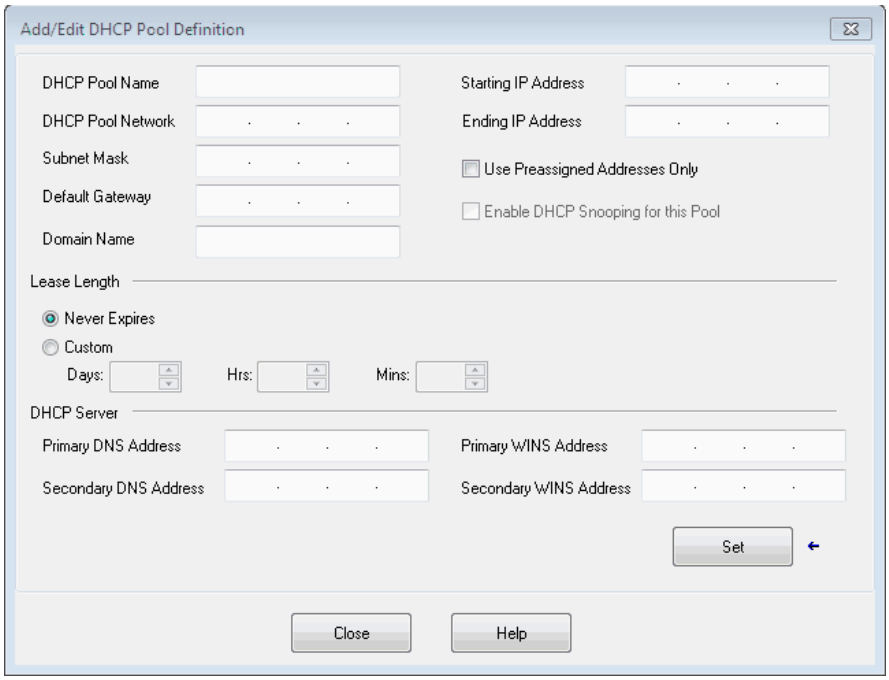


Table 139 - Add/Edit DCHP Pool Definition

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.
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.
Default Gateway	The default gateway IP address for the DHCP client.
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 that you assign are being used by other devices in your network. This field is required.

Table 139 - Add/Edit DCHP Pool Definition (Continued)

Field	Description
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.

Configure DHCP Persistence

To make sure that a device that is connected to a specific port receives the same IP address, assign a specific IP address to the port.

1. In the navigation pane, click DHCP Address Assignment.
2. Complete the fields as described in Table 140, and then click Set.
3. Click Apply.

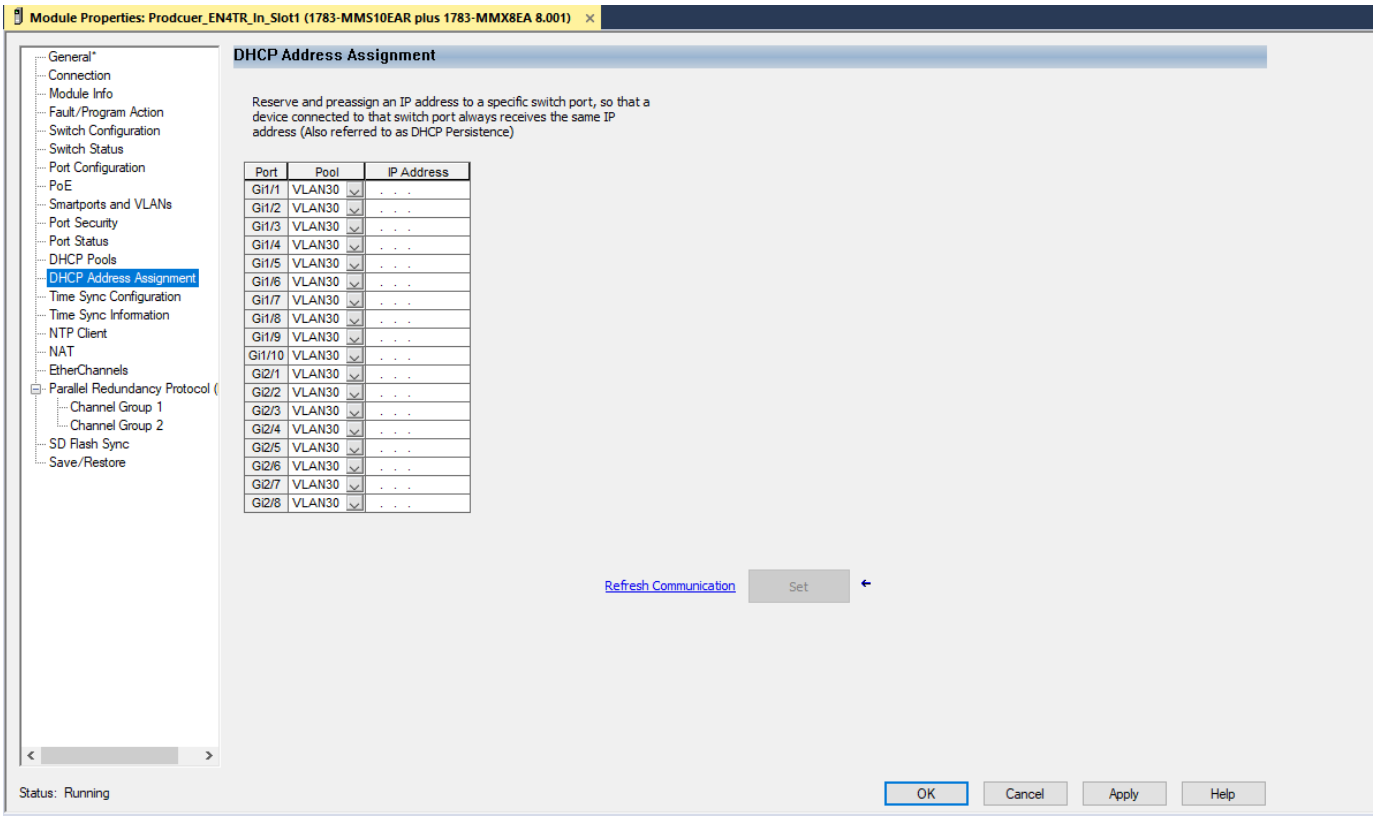


Table 140 - DHCP Address Assignment

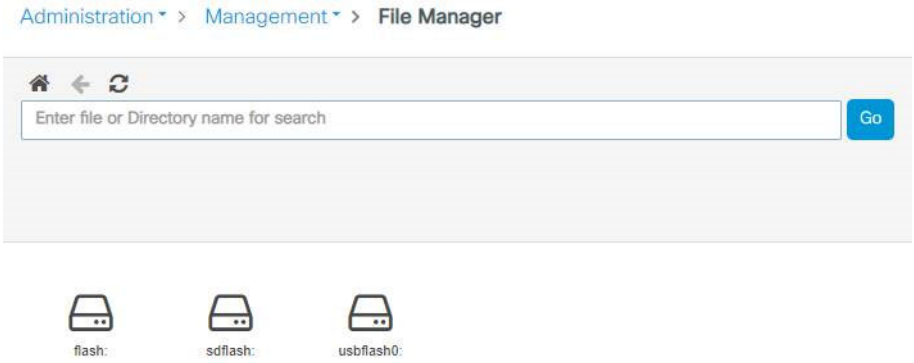
Field	Description
Port	Displays the port type and number.
Pool	Choose the DHCP address pool that includes the IP address to assign to this port.
IP Address	Enter the IP address reserved for the port that connects to this interface. The IP address that you assign is reserved for only this port and is not available for normal DHCP dynamic assignment. The IP address must be in the range of the assigned DHCP address pool.

File Manager

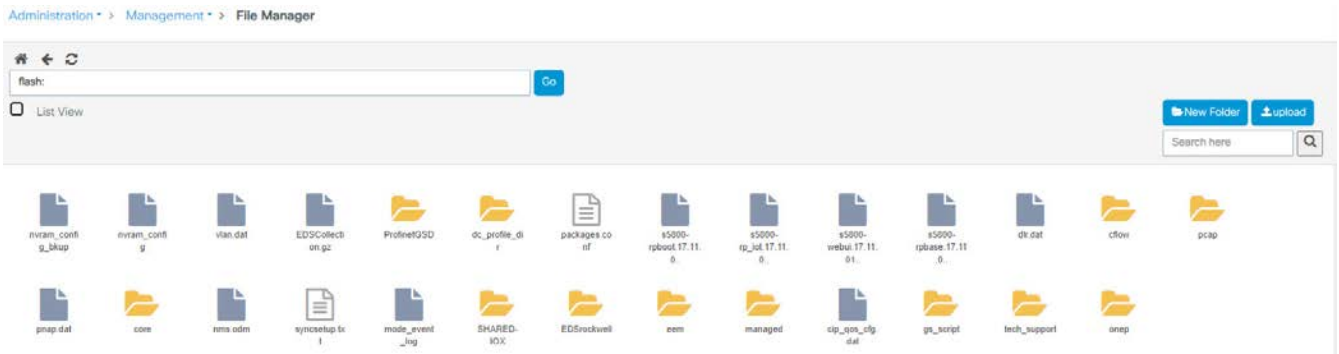
In the WebUI, you can manage files in the flash and sdflash file systems on the device. You can upload and download files such as logs, scripts, data files, and so on. Also, you can create folders, display folder contents, and search for files.

From the Administration menu, choose File Manager.

To display the files and directories in the file system, double-click flash or sdflash. You can also type the path to a file in the directory search field, or you can search for a file name from within a directory or folder.



The contents of the file system appears.



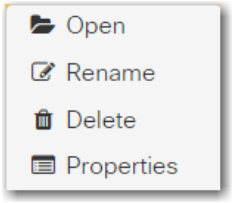
Within a file system, you can do the following:

- To return to a previous level in the file system, click the left arrow, or click the Home icon to return to the top level.
- To create a folder, click New Folder, enter a folder name, and then click OK.

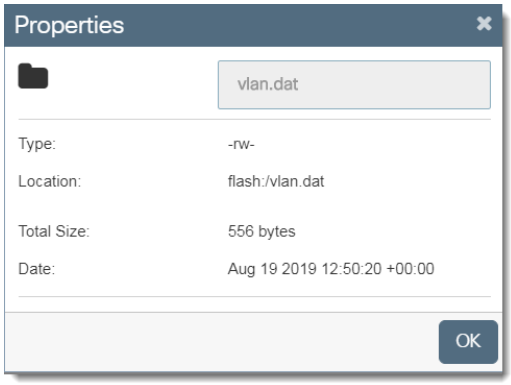


- To upload a file, click upload, browse to the file to upload, and then click Open.

- To open, rename, delete, or view file properties, right-click a folder.



- To view folder or file details, click Properties.



Field	Description
Type	The permissions file types: • d = directory • r = read • w = write • x = execute • - (dash)= used when a particular permission is not granted
Location	The path to the folder or file.
Total Size	The size of the folder contents or file size.
Date	The date and time stamp of folder or file.

Field-programmable Gate Array (FPGA) Profiles (Stratix 5800 Switch Only)

The Field-programmable Gate Array (FPGA) feature turns certain software features assisted by field-programmable gate array on or off. Some switch features such as PRP, HSR, and TrustSec rely on FPGA implementation.

FPGA Profiles allow for efficient allocation of platform resources for the operation of multiple time sensitive, resilient industrial protocols without changes to hardware.

Configure FPGA Profiles in WebUI

From the Administration Menu, choose FPGA.



The switch supports three FPGA profiles with different combinations of features that are supported in each profile, as shown in the following table.

FPGA Profile Name	Description
Default	Supports 1 instance of PRP/HSR, and CTS IPv4 Security Group Tag (SGT) with VRF and Security Group Access Control List (SGACL) Logging.
CTS-IPv6	Supports CTS IPv4 and IPv6 SGT with VRF and SGACL Logging.
Redundancy(1)	• Supports 1 instance of PRP/HSR. The expansion module can increase the capacity of the instances that are supported on the system. • Supports up to 3 DLR rings: 2 rings can be configured on the switch and 1 ring configured on the expansion module, or 1 ring configured on the switch and 2 rings configured on the expansion module. • The same profile that is configured for the switch is used for the expansion module.(2)

(1) TrustSec is not supported when using the Redundancy FPGA profile on the Stratix 5800 switch.

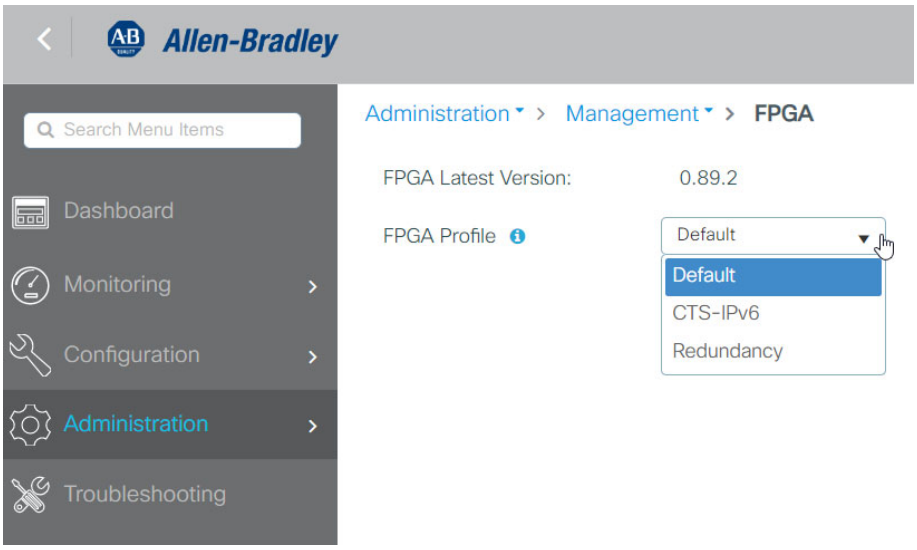
(2) An advanced expansion module is required.

IMPORTANT You must reload the switch after changing the configured FPGA Profile to activate the profile.

An FPGA Profile is configured globally on the switch. All base systems and expansion modules load the same FPGA Profile that is configured for the switch. If an expansion module is present, the FPGA Profile that is configured for the switch also applies to the expansion module.

An FPGA Profile is supported in firmware release 17.8 and later. In any previous release that does not support FPGA Profile, for example, an upgrade from firmware release 17.7 to 17.8, the default FPGA Profile is installed.

Any features controlled by FPGA Profile that are configured in the switch running the earlier release and are not included in the default profile are rejected. For example, an IPv6 address is not supported in the default profile, so IPv6 configurations are rejected during startup after the upgrade. Similarly, after an upgrade where the IPv6 profile is loaded, existing PRP and DLR configurations are rejected upon startup.



HTTP/HTTPS/Netconf Access

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent. HTTP with SSL encryption provides a secure connection between two devices, such as a switch and your web browser.

With Personal Identity Verification (PIV), the identity of a user is verified using a certificate and the login user name and password. Prerequisites to enable PIV include configuring a PKI trust store and installing the root CA certificate, and then enabling PKI from HTTP.

Certificate Authority (CA) Trustpoints

CA Trustpoints manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are known as trustpoints. For more information about CA Trustpoints, see the Ethernet Reference Manual, publication ENET-RM002.

IMPORTANT CA trustpoints must be configured on each device individually. Copying them from other devices makes them invalid on the device.

Configure HTTP/HTTPS/Netconf/VTY Access Via the WebUI

1. From the Administration menu, choose HTTP/HTTPS/Netconf/VTY.
2. Complete the fields as described in Table 141, and then click Apply.

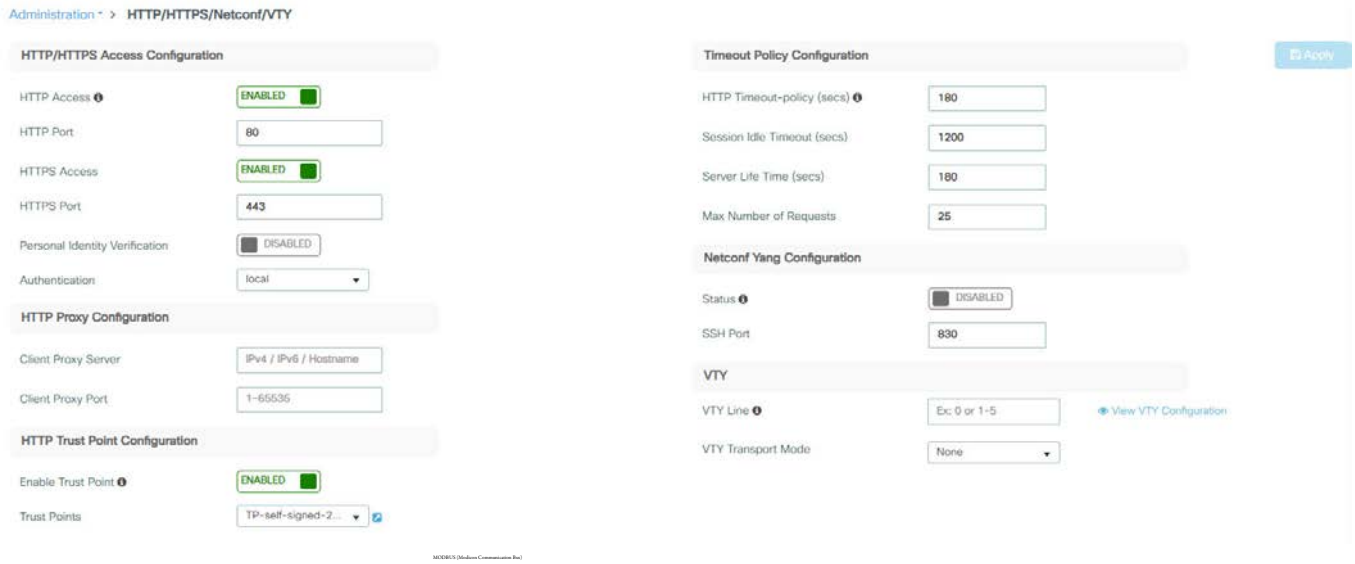


Table 141 - HTTP/HTTPS/Netconf

Field	Description
HTTP/HTTPS Access Configuration	
HTTP Access	Click to enable or disable HTTP connections. By default, HTTP access is enabled. IMPORTANT: If both HTTP and HTTPS are enabled, HTTP redirects to HTTPS.
HTTPS Access	Click to enable or disable HTTPS connections. By default, HTTPS access is enabled.
Personal Identity Verification	Click to enable or disable PIV. **IMPORTANT:** If you enable PIV before setting it up, you are not able to access the switch.
HTTP Trust Point Configuration	
Enable Trust Point	Click to enable or disable certificate authority (CA) trustpoints. See Certificate Authority (CA) Trustpoints on page 257.
Trust Points	If trustpoints are enabled, choose a trustpoint from the list.

Table 141 - HTTP/HTTPS/Netconf (Continued)

Field	Description
Netconf Yang Configuration	
Status	Click to enable or disable Netconf on the device.
SSH Port	Enter the port number for Netconf-over-SSH sessions. Valid values: 1...65535 Default value: 830
Timeout Policy Configuration	
HTTP Timeout-policy (secs)	Enter the number of seconds to determine how long a connection to the HTTP server remains open.
Session Idle Timeout (secs)	Enter the number of seconds of inactivity allowed before the session times out.
Server Life (secs)	Enter the server life time in seconds. Valid values: 1...86400
Max Number of Requests	Enter the maximum number of concurrent requests the device can accept. Valid values: 1...86400
VTY Line	Enter the virtual terminal line (VTY) line number or a range.
VTY Transport Mode	Choose a transport mode for the VTY: • Telnet & SSH • Telnet • SSH • None

MODBUS

MODBUS is an application layer protocol for client-server communication between two devices on the network, where the Stratix 5800 switch acts as the server, and a device with MODBUS client software can query the switch for information. This MODBUS implementation is read-only and only provides data.

Requirements and Restrictions

Before you configure MODBUS, know the following:

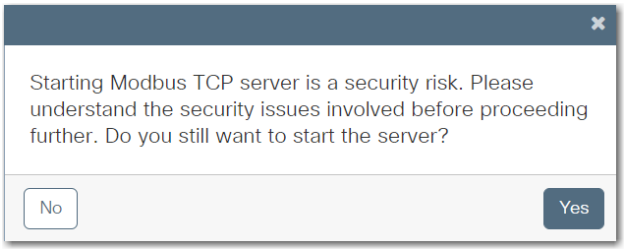
- If a firewall or other security services are enabled, the switch TCP port can be blocked, and the switch and the client cannot communicate.
- If a firewall and other security services are disabled, a denial-of-service attack can occur on the switch.
- To add security when using MODBUS TCP, configure an ACL to permit traffic from specific clients or configure QoS to rate-limit traffic.

Configure MODBUS Via the WebUI

To configure MODBUS, follow these steps.

1. From the Administration menu, choose MODBUS.
2. In the Status field, click to enable or disable MODBUS.

   By default, MODBUS is disabled. If you enable MODBUS, a security warning appears.



IMPORTANT Before proceeding, observe and understand the security risk that is involved in starting the MODBUS TCP server.

3. To proceed through the security warning, click Yes.
4. Complete the fields as described in Table 142, and then click Apply to Device.

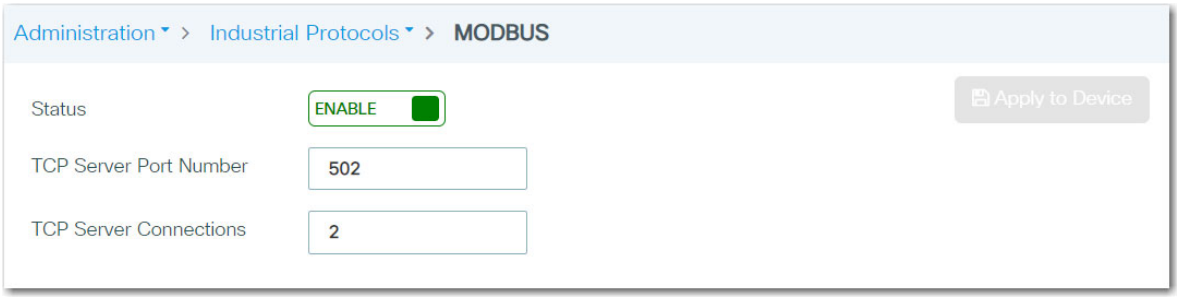


Table 142 - MODBUS

Field	Description
Status	Click to enable or disable MODBUS. By default, MODBUS is disabled.
TCP Server Port Number	Enter the port number of the MODBUS TCP server. Valid values: 1...65535 Default value: 502
TCP Server Connections	Enter the number of simultaneous connection requests sent to the switch. Valid values: 1...5 Default value: 2

For a list of MODBUS register addresses, see Appendix E.

Power over Ethernet (PoE) (Stratix 5800 Switch Only)

Power over Ethernet (PoE) provides power to end devices over a copper Ethernet cable. Switches and expansion modules with PoE ports are software-configurable and provide automatic detection and power budgeting. PoE is implemented following the specifications in IEEE 802.3af (2003) and IEEE 802.3at (2009), which accommodate different power levels. For more information about PoE, see the Ethernet Reference Manual, publication ENET-RM002.

IMPORTANT A mismatch between the total power that is supported and the power supply can damage the switch. Do not oversubscribe the power supply. If you intend to connect the switch to a power supply that allows more wattage than configured, first change the power supply and then enter the total power supported. If you intend to connect the switch to a power supply that allows less wattage than configured, first change the total power that is supported to an appropriate value and then change the power supply.

Requirements and Restrictions

There is a power budget of 360 W shared across PoE/PoE+ ports.

PoE Port Modes

You can assign the following modes to PoE ports.

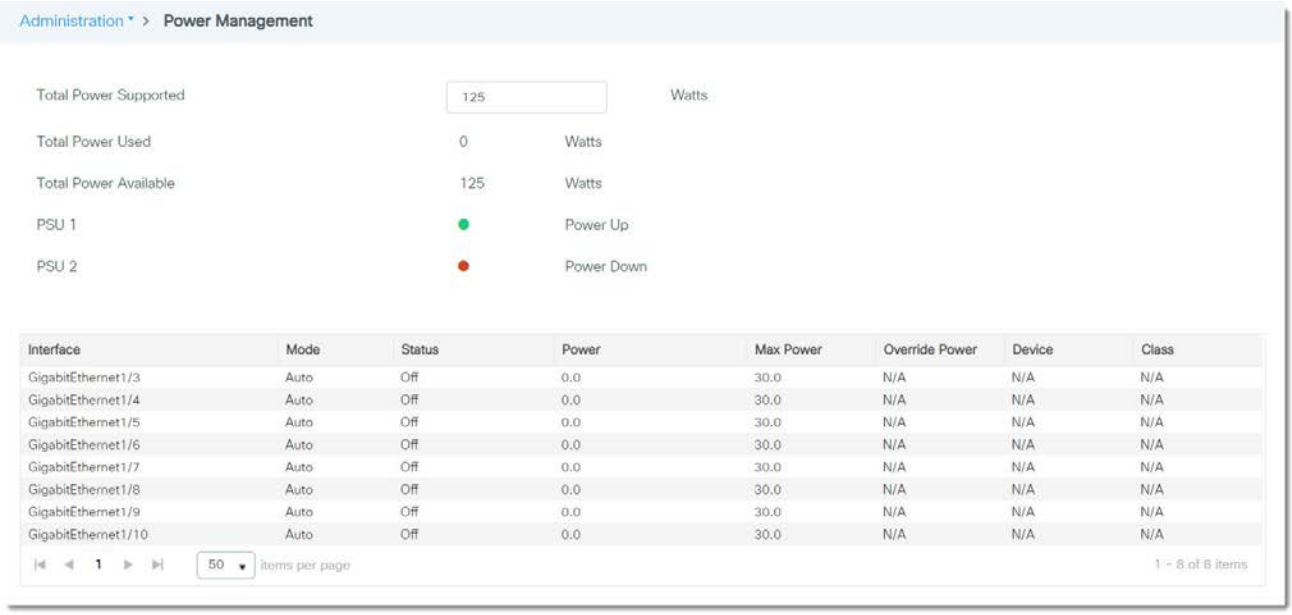
Table 143 - PoE Modes

Mode	Description
Disabled	The switch disables powered-device detection and never powers the PoE port even if an unpowered device is connected.
Auto (default)	The switch automatically detects if the connected device requires power and automatically assigns the required capacity.
Static	The switch preallocates power to the port, even when a non-PoE device is connected, and makes sure that power is available to the port.

Configure PoE via the WebUI

The Power Management page is available for devices that have PoE support.

From the Administration menu, choose Power Management.



From the Power Management page, you can view and configure PoE information:

- The fields at the top of the page show information about the total power on the switch See Table 144.

  To configure the total power supported, modify the value in the Total Power Supported field. A warning appears. Misconfiguration of this setting can result in damage to the switch. Click Yes to apply the configuration, which power cycles any PoE devices currently connected.

Table 144 - Power Management

Field	Description
Total Power Supported	The total amount of power that the switch can support for external devices. To limit the total PoE power budget, enter a value based on the power source. Valid values: 4...480 watts
Total Power Used	The amount of power used on the switch for PoE.
Total Power Available	The amount of power available on the switch for PoE.
PSU1	The status of the power supply connected to the Pwr A power connector.
PSU2	The status of the power supply connected to the Pwr B power connector.

- To configure PoE for an individual switch interface, click the interface in the grid, complete the fields as described in Table 145, and then click Update & Apply to Device.

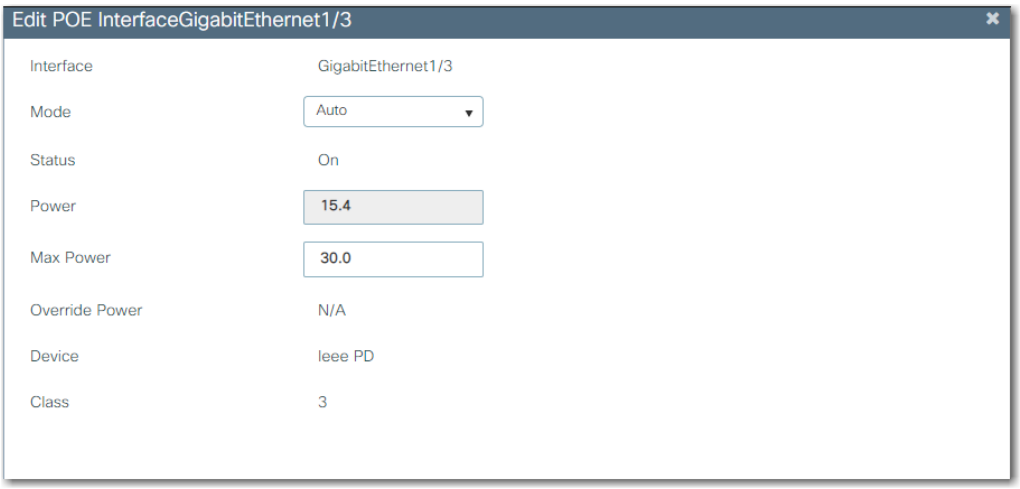
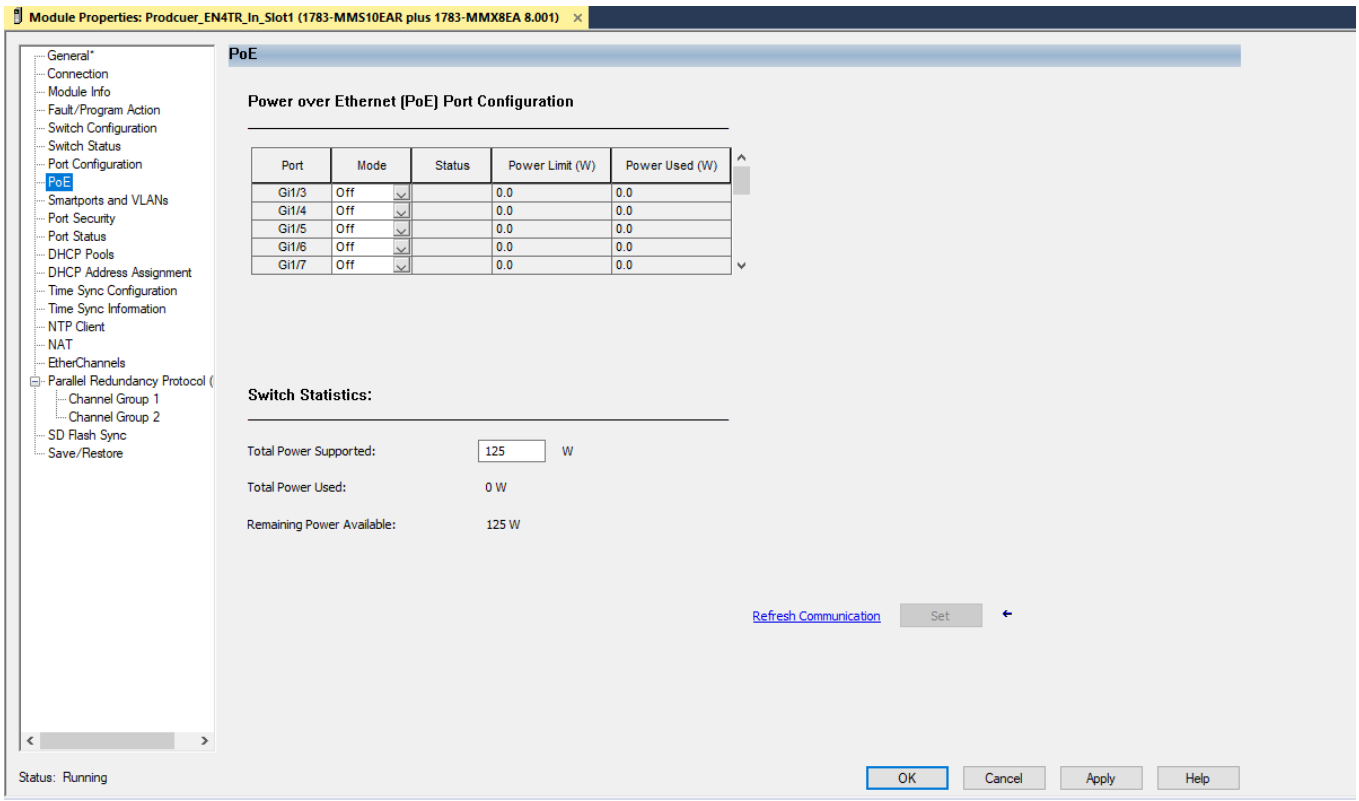


Table 145 - Edit PoE Interface

Field	Description
Interface	The interface type and number.
Mode	Choose a PoE mode to apply to the interface. For a description of each mode, see Table 143 on page 260.
Status	Displays whether PoE is in use on the interface. The status turns to On once a PoE device is connected to the interface.
Power	Enter the amount of power in watts to allocate to the interface.
Max Power	Enter the maximum power that can be allocated to the interface. Valid values: 4...30 watts
Override Power	Displays either N/A or the power that is configured for the interface. To configure this parameter, enter the following command in command-line interface (CLI) where X is the wattage value: power inline consumption default wattage X
Device	The device that is connected to the interface.
Class	Displays the power classification of the powered device.

Configure PoE via the Logix Designer Application

1. In the navigation pane, click PoE.
2. Complete the fields as described in Table , and then click Set.



Field	Description
Power over Ethernet (PoE) Port Configuration	
Port	Displays the port type and number.
Mode	Choose a PoE mode to apply to the port. For a description of each mode, see Table 143 on page 260.
Status	Displays whether PoE is enabled (On) or disabled (Off) on the port.
Power Limit (W)	Enter the maximum power in that can be allocated to the interface. If the port is in Auto mode, you can enter a value. Valid values: 4...30 watts
Power Used (W)	Displays the amount of power in watts currently in use by the port.
Switch Statistics	
Total Power Supported	The total amount of power that the switch can support for external devices. To limit the total PoE power budget, enter a value based on the power source. Valid values: 4...720 watts
Total Power Used	The amount of power used on the switch for PoE.
Remaining Power Available	The amount of power available on the switch for PoE.

PROFINET

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

The Stratix 5800 switch supports the forwarding of these PROFINET traffic types:

- TCP/IP
- Real-Time (RT)

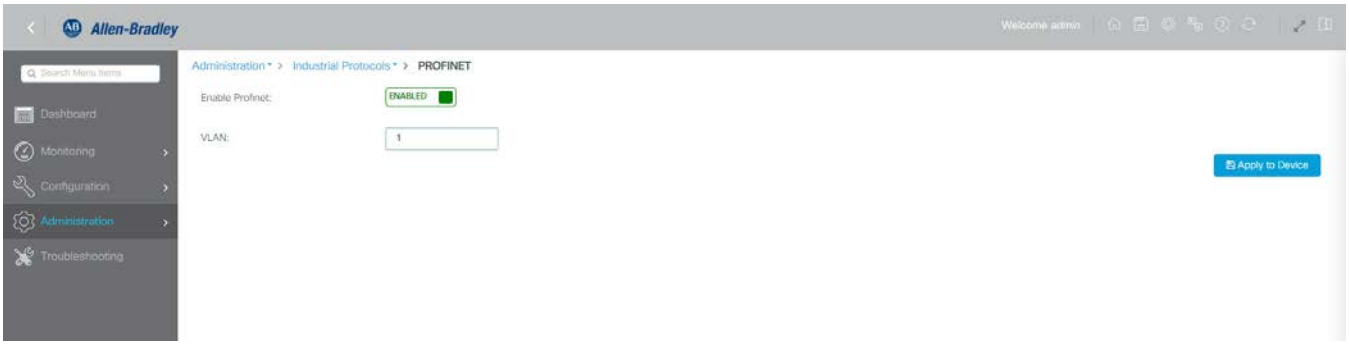
  Stratix switches do not support the forwarding of Isochronous Real-Time (IRT) traffic.

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

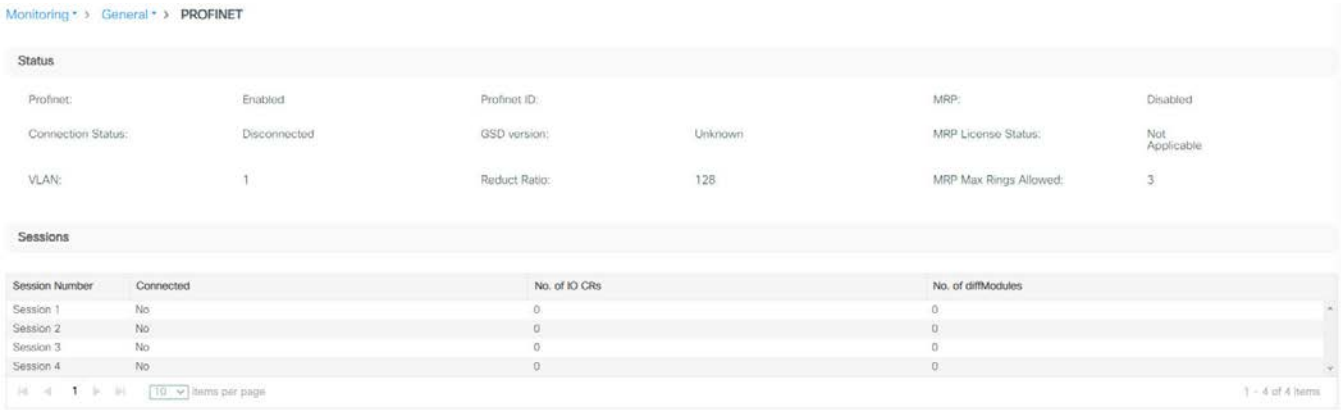
Configure PROFINET via the WebUI

To configure PROFINET, from the Administration Menu, choose Industrial Protocols. An option for PROFINET is present.

From the following screen, you are able to choose to enable PROFINET.



After you enable PROFINET, it is available in the Monitoring tab.



From the PROFINET Monitoring screen, you can choose the status and session parameters.

Table 146 - PROFINET Status Parameters

Parameter	Description
Profinet	Shows whether PROFINET is enabled or disabled on the switch.
Connection Status	Shows whether the switch is connected to the PROFINET PLC (I/O Controller).
VLAN	The VLAN number for PROFINET traffic.
Profinet ID	PROFINET device identifier.
GSD version	Shows whether the General Station Description (GSD) file for the switch matches the GSD file in the controller configuration software.
Reduct Ratio	Reduction Ratio denotes the rate at which the real time (RT) packets are exchanged between controller and the IO devices. By default, the value is set to 128 ms. This denotes that the transmit and receive occurs at every 128th send clock. Other values like 256 and 512 can also be configured from the TIA tool.
MRP(1)	Shows whether MRP is enabled or disabled.
MRP License Status(1)	Shows whether the MRP license is active.
MRP Max Rings Allowed(1)	The maximum number of MRP rings that can be configured based on the license.

(1) Stratix 5800 Switch Only

Table 147 - PROFINET Session Parameters

Parameter	Description
Session Number	Number of the PROFINET session.
Connected	Shows whether the session is connected.
Number of I/O Communication Relationships	Number of IO Communication Relationships (CRs) for the session.
Number of diffModules	A value greater than zero means that there is a difference in expected (configured from TIA) and the actual submodules in the device. This number denotes the count of the differences. The presence of diffmodule blocks in the response shows the details of missing or additional submodules in the device from the ones configured.

Reload the Switch Via the WebUI

You can reload the switch with or without saving the Running configuration to the Startup configuration. You can also reset the switch to its factory default state.

1. From the Administration menu, choose Reload.
2. Click an option as described in Table 148, and then click Apply to Device.

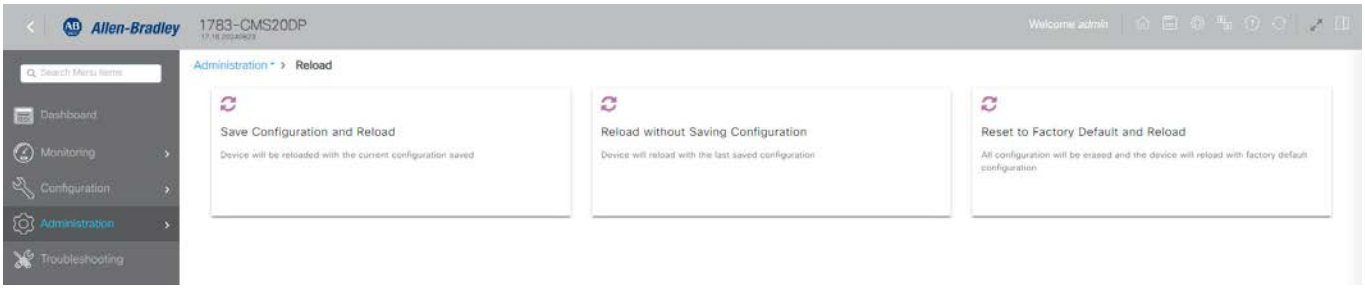


Table 148 - Reload

Field	Description
Save Configuration and Reload	Click to restart the switch and save the Running configuration to the Startup configuration. The current Running configuration is retained when the switch restarts.
Reload without Saving Configuration	Click to restart the switch without saving the Running configuration. The switch restarts with the Startup configuration stored in its internal memory.
Reset to Factory Default and Reload(1)	Click to restart the switch and overwrite all applied and saved configuration parameters and return to the factory default. You are prompted for confirmation to reset the configuration. All configuration data files are deleted, and the device is restored to its factory default state when the switch restarts. To restore the base configuration, you can run Express Setup on the switch.

(1) Using the Reset to Factory Default and Reload overwrites all existing configuration files on both internal memory and external memory (SD card and USB Flash) and resets the switch back to factory default configuration

SDM-Template

Switch Management Database (SDM) templates optimize how system resources are allocated to support specific features, depending on how the switch is used in the network. In the WebUI, you can apply an SDM template to the switch.

To apply an SDM template to the switch, follow these steps.

1. From the Administration menu, choose SDM-Template.

   The only SDM-Template available is the 'Default' template.

2. To select a template to apply to the switch, click a template in the List of Resources column, and then click Apply to Device.

Figure 39 - Stratix 5200 SDM Template

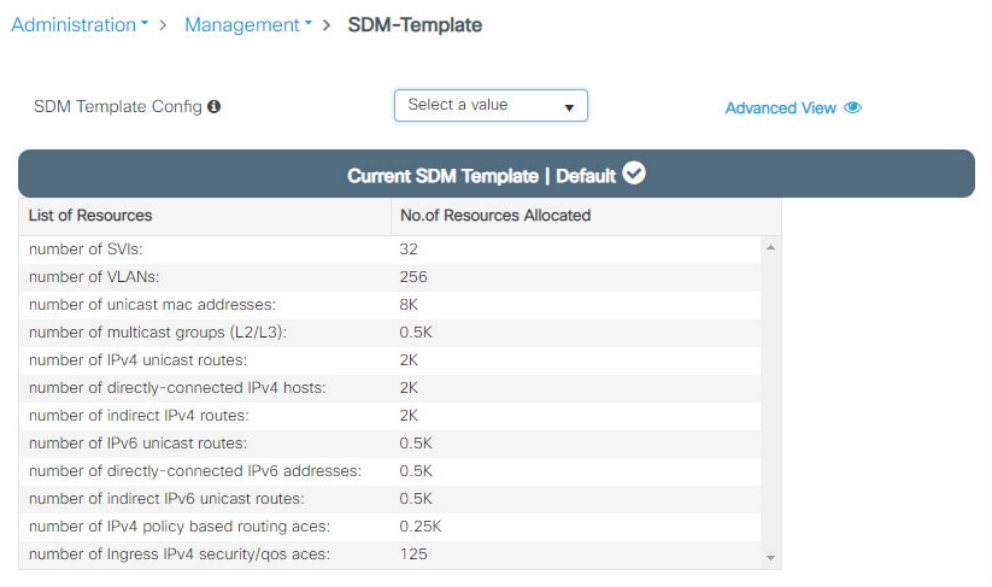
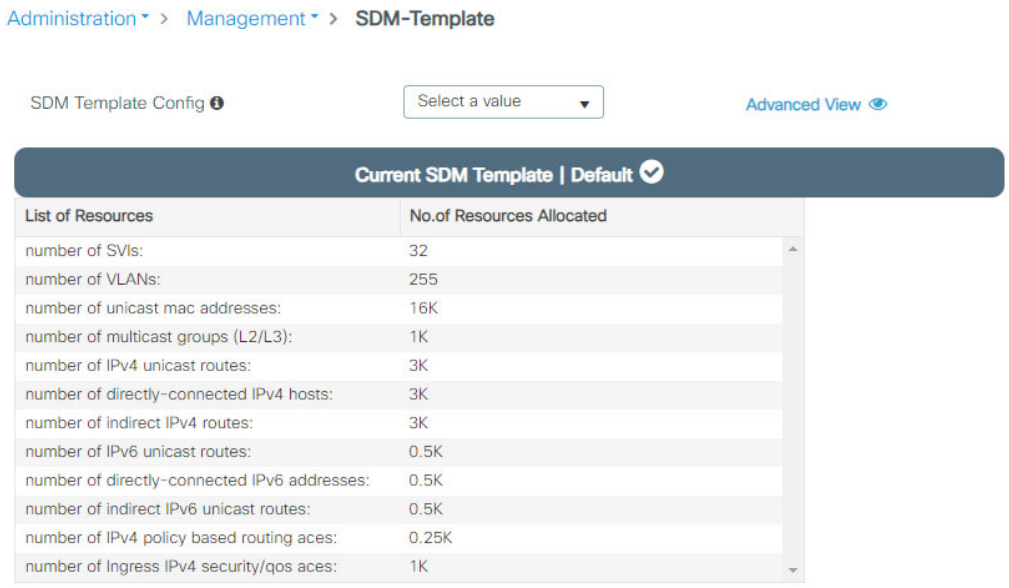


Figure 40 - Stratix 5800 Switch SDM Template



Secure Digital (SD) Card

The following switches can store their configuration in an SD card, USB device (Stratix 5800 Switch Only), or internal memory:

- The Stratix switch has a slot for an optional SD card. You must use the 1784-SDHC8 card available from Rockwell Automation with the switches.

The switches can store their configuration in an SD card, USB device (Stratix 5800 Switch Only), or internal memory: The Stratix switch has a slot for an optional SD card. You must use the 1784-SDHC8 card available from
Rockwell Automation with 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 to do the following:

- Synchronize the configuration and software from the internal memory to the SD card.
- Restore a switch configuration if it fails (using the Swap-Drive feature).
- Store versions of software files or store copies of configurations on the SD card.

You can use WebUI or the Logix Designer application to synchronize configuration and IOS from the internal flash to the SD card.



ATTENTION: SD cards commonly have a physical read-only lock switch. If the lock switch is engaged, Syncing from the internal memory to SD Card is not possible.

Swap Drive

Swap drive is a switch recovery feature. The swap drive feature enables you to replace a failed switch quickly and easily. You move an SD card or USB drive (Stratix 5800 Switch Only) with a backup of the original switch to a new, factory defaulted switch. After you turn on the new switch, the same image and configuration as the original switch appears.

To restore the settings to the new switch, you must have previously synchronized the original switch with the SD card or USB drive.

Restore occurs automatically, when you insert the SD card or USB drive into the new switch and power the switch. The new switch looks for an SD card and scans it to see if an image and configuration are present. If the image and configuration are present, the switch then copies them to internal flash and comes up with the image and configuration of the original switch.

On a Stratix 5800 switch, if an SD card is not present or doesn't have the original switch's image and configuration, the switch then looks for and scans the USB drive. If they are present on the USB drive, the switch comes up with the original switch's image and configuration.

If the image and configuration are not present on any external media, the system asks if you want to continue with the initial configuration on the new switch, in which express setup has to be performed.

Procedure for Swap Drive

Cable the new switch correctly and make sure that it is powered off before you transfer the SD card or USB drive.

Use the following steps to utilize the swap drive feature:

1. On the failed switch, remove the SD card or USB drive.

   The SD card and USB drive are hot-swappable, but do not remove it from the switch while SD flash write is in progress.
2. On the new switch, verify that the SD card or USB drive is oriented properly, and then press it into the slot on the switch until it is seated.
3. Power on the new switch.

   The image and configuration of the failed switch are transferred to the new one.

Simple Network Management Protocol (SNMP)

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

Supported SNMP Versions

Stratix 5800 switches support SNMP versions 1, 2c, and 3. Your configuration requirements depend on the SNMP version that you use. You can choose an SNMP version on the Hosts tab of the SNMP page of the WebUI for the switch.

SNMP Version	Required Configuration Components
SNMPv1	• A community string to authenticate access to the device. • A host defined to be the recipient of SNMP notifications.
SNMPv2C	• A community string to authenticate access to the device. • A host defined to be the recipient of SNMP notifications.
SNMPv3	• User security modes and authentication. • A host defined to be the recipient of SNMP notifications.

SNMPv3 User Security Modes and Authentication

SNMPv3 enables you to configure an authentication strategy for a user. A combination of security modes and authentication protocols determines the security mechanism that is applied to an SNMP packet.

The following table describes the combinations of security modes and authentication that you can configure for each user.

Table 149 - User Security Modes and Authentication

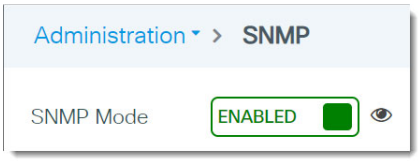
Security Mode	Authentication	Encryption	Result
AuthPriv (default)	Message digest algorithm 5 (MD5) or Secure Hash Algorithm (SHA)	Data Encryption Standard (DES)	Provides authentication based on the hashed message authentication code (HMAC)-MD5 or HMAC-SHA algorithms. In addition to authentication, provides DES 56-bit encryption based on the cipher block chaining (CBC)-DES (DES-56) standard.
AuthNoPriv	Message digest algorithm 5 (MD5) or Secure hash algorithm (SHA)	No	Provides authentication based on the hashed message authentication code (HMAC)-MD5 or HMAC-SHA algorithms.
NoAuthNoPriv	User name	No	Uses a user name match for authentication.

Configure SNMP Via the WebUI

From the Administration menu, choose SNMP.

From the SNMP page, you can configure these aspects of SNMP:

- To enable or disable SNMP mode, click the SNMP Mode field. To see all SNMP views that are included and excluded, click the eye icon.



- To configure system information and enable or disable traps, see page 271.
- To configure community strings, see page 272. Community strings to provide a remote manager read-only or read/write access to the switch. Community strings are required for SNMP versions 1 and 2c.
- To configure SNMPv3 users and authentication, see page 273. This feature requires that you choose SNMPv3 on the Hosts tab.
- To configure SNMP hosts, see page 274.

Configure System Information and SNMP Traps

On the General tab, complete the fields as described in Table 150, and then click Apply.

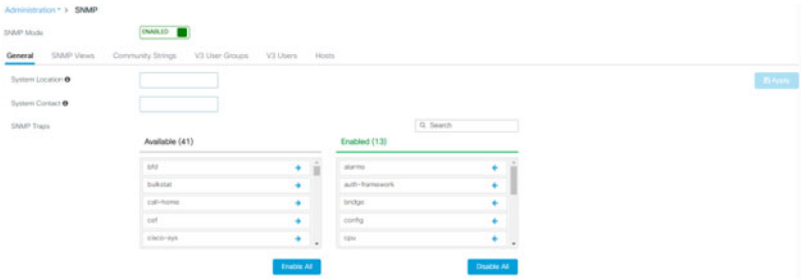


Table 150 - SNMP—General

Field	Description
SNMP Mode	Click to enable or disable SNMP. By default, SNMP is enabled. To see all SNMP views that are included and excluded, click the eye icon.
System Location	Enter the location of the device.
System Contact	Enter the contact details of the device administrator.
SNMP Traps	To enable one or more traps: • Click each trap to move it from the Available list to the Enabled list. or • Click Enable All. To disable one or more traps: • Click each trap to move it from the Enabled list to the Available list. or • Click Disable All.

Configure Community Strings

On the Community Strings tab, you can add, edit, and delete community strings:

- To add a community string, click Add, complete the fields as described in Table 151, and then click Apply to Device.
- To edit a community string, click the community name in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a community string, check its associated checkbox in the grid, and then click Delete.

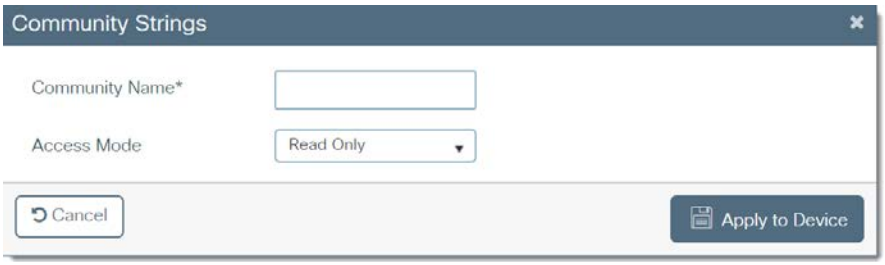


Table 151 - SNMP—Community Strings

Field	Description
Community Name	Enter a name to identify the community. The name must be a unique, case-sensitive, alphanumeric string of up to 16 characters.
Access Mode	Choose the level of access to grant to this community: • Read-only (default) • Read/Write

Configure V3 User Groups

On the V3 User Groups tab, you can add, edit, and delete SNMP V3 user groups and their authentication methods.

- To add a user group, click Add, complete the fields as described in Table , and then click Apply to Device.
- To edit a user group, click the user group name in the grid, modify the fields, and then click Apply to Device.
- To delete a user, check its associated checkbox in the grid, and then click Delete.

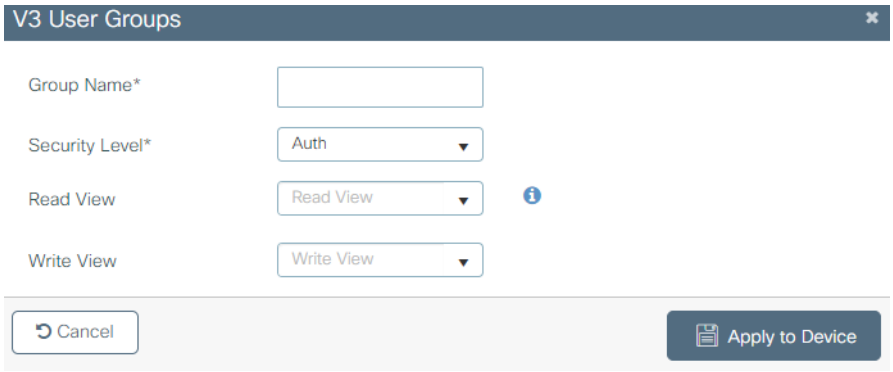


Table 152 - V3 User Groups

Field	Descriptions
Group Name	Enter a name for the user group.
Security Level	Choose a security level: • Auth • No Auth • Priv

Configure SNMP Users and Authentication

On the V3 Users tab, you can add, edit, and delete SNMPv3 users and their authentication methods:

- To add a user, click Add, complete the fields as described in Table 153, and then click Apply to Device.
- To edit a user, click the user name in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a user, check its associated checkbox in the grid, and then click Delete.

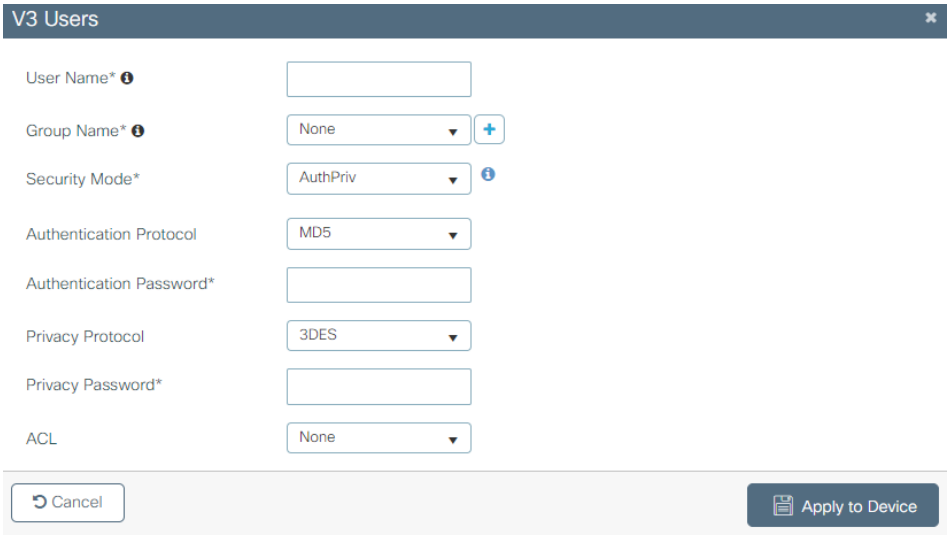


Table 153 - SNMP—V3 Users

Field	Description
User Name	Enter a name for the user.
Group Name	Choose an existing group name, or to create a new group name, click the plus sign (+).
Security Mode	Choose a security mode. See SNMPv3 User Security Modes and Authentication on page 270.
Authentication Protocol	(Applies only to AuthPriv and AuthNoPriv security modes). Choose an algorithm to configure authentication based on the Hashed message authentication code (HMAC)-MD5 or HMAC-SHA algorithms: • MD5 (default) • SHA
Authentication Password	(Applies only to AuthPriv and AuthNoPriv security modes). Enter a password to authenticate user access.
Privacy Protocol	(Applies only to AuthPriv security mode). Choose an encryption method: • 3DES (default) • AES128 • AES192 • AES256 • DES AES 128, AES 192, and AES 256 use Cipher Feedback (CFB) mode with encryption key sizes of 128 bits, 192 bits, or 256 bits respectively. 3DES uses the cipher block chaining (CBC)-DES (DES-56) standard with a 168-bit key size for encryption.
Privacy Password	(Applies only to AuthPriv security mode). Enter a password for the user.
ACL	Select an Access Control List (ACL) to be associated with this SNMP user from the ACL drop-down menu.

Add SNMP Hosts

On the Hosts tab, you can add, edit, and delete SNMP hosts, or recipients of SNMP notifications:

- To add a host, click Add, complete the fields as described in Table 154, and then click Apply to Device.
- To edit a host, click the user name in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a host, check its associated checkbox in the grid, and then click Delete.

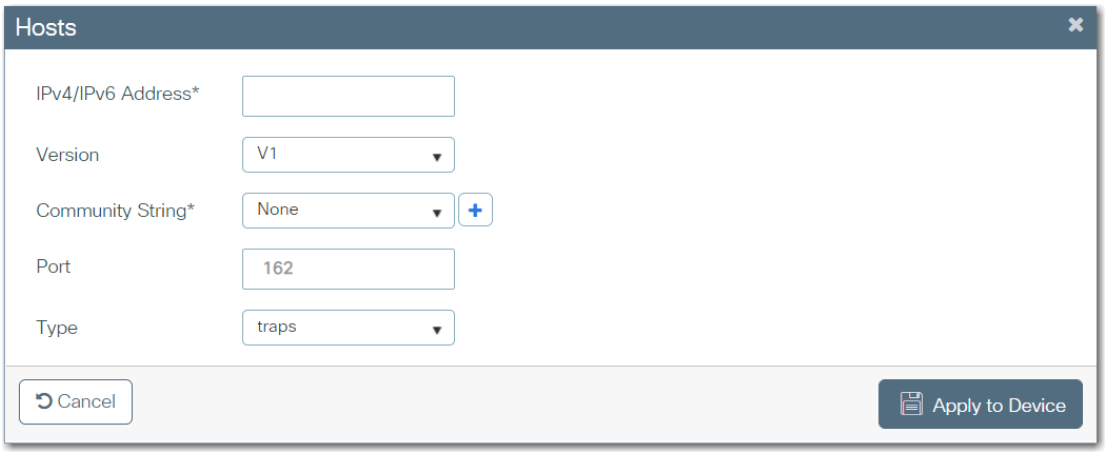


Table 154 - SNMP—Hosts

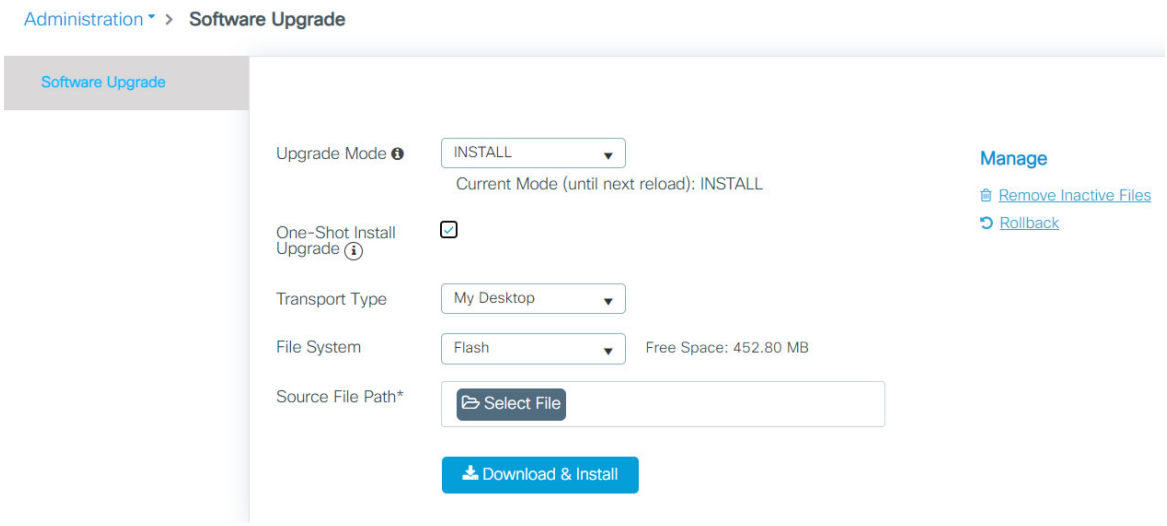
Field	Description
IPv4/IPv6 Address	Enter the IP address for the device to accept and use to send SNMP packets. An AND operation is performed between the requesting entity IP address and the subnet mask before being compared to the IP address. If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. Default value: 0.0.0.0
Version	Choose the SNMP version. See See Supported SNMP Versions on page 270.
Community String	For SNMP versions 1 and 2c, enter the SNMP community that you want to use.
Port	Enter the UDP port number for the remote SNMP agent of the device where the user resides. Valid values: 0...65535 Default value: 162
Type	Choose traps to enable the device to send SNMP traps to this host.

Software Upgrade

In WebUI, you can upgrade the software image on your switch using the following steps.

1. From the Administration menu, choose Software Upgrade.
2. Deleting unused software files using "Remove Inactive Files" link on the "Software Upgrade" page or manually removes them from the File Manager page to ensure there is enough space (~1.3GB) to upgrade successfully.
3. In Upgrade Mode, choose Install Mode.

   Install Mode - In this mode, a single .BIN file is copied to the switch. Then, multiple files (packages) are extracted from the .BIN file and installed on the on-board flash memory. After transferring and installing the files, the switch must be rebooted to apply the new software version.



4. Complete the fields as described in Table 155, and then click Download.
5. To restart the switch with the new software, click Save Configuration & Reload.

   If “One-Shot Install Updgrade” is selected, this occurs automatically. Without this selection, you will need to manually reload the switch to apply the new firmware.

Table 155 - Software Upgrade

Field	Description
Upgrade Mode	There are two modes: • INSTALL • BUNDLE (Not Supported)
One Shot Install Upgrade	The new image/package would be installed and activated as a part of One-Shot upgrade. In case of an image upgrade, the device will be reloaded post activation to bring it up with new software.
Transport Type	Choose the method to use for sending the software image to your device: • TFTP • SFTP • FTP • Device • Desktop (HTTPS)
Source File Path	(Applies only for Desktop transport types.) Click to select the .bin file from your local device. If you inadvertently select a file that is not a .bin file, an error message appears.
Server IP Address (IPv4/IPv6)[1]	Enter the IP address of the FTP or TFTP server to use.
(SFTP/FTP) Username[2]	Enter the SFTP or FTP user name.
(SFTP/FTP) Password[2]	Enter the SFTP or FTP password.

Table 155 - Software Upgrade

Field	Description
File System[3]	Due to limited space on the Internal flash, it is highly recommended to "Remove Inactive Files." before upgrading. Choose a file system for the file: • Flash • SD Flash – When using the SD Flash as a File System on an Install mode, the SD Flash acts as an intermediate location where the .bin file is copied to before extracting the Install files to the internal flash. • USB Flash (Available when USB is inserted on the Stratix 5800 switch only)
Source File Path	Specify the complete path from where you want to download the software image file, including the name of the file. **EXAMPLE:** FolderOnFTP/s5800-universalk9.16.10.01i.SPA.bin
Destination[4]	(Applies to all transport types except Device.) Choose a destination for the file: • SD Flash • Flash • USB Flash (Available when USB is inserted on the Stratix 5800 switch only)

(1) Applies only to TFTP, SFTP, or FTP transport types
(2) Applies only to SFTP or FTP transport types.
(3) Only available on Install Mode. Applies only to Device transport type.
(4) Located in Bundle Mode, which is not supported.

Stratix 5200 Boot Order

The boot order for the Stratix 5200 switch is as follows:

- flash:
- sdflash: (for Swap-drive on a factory defaulted switch)

For more information on SD Cards as well as Swap Drive, see page 268.

The configuration file is always stored and booted from flash: (Firmware revision 17.11.1 and later.)

Stratix 5800 Boot Order

The boot order for the Stratix 5800 switch is as follows:

Boot sequence comes only when we don't have boot variable set. If the device is set with a boot variable, then the boot flow follows the same sequence.

If no boot variable set, then boot media priority is as follows:

- sdflash:
- usbflash: (0 and 1)
- flash:

The configuration file is always stored and booted from flash: (Firmware revision 17.10.1 and later.)

User Administration

You can maintain user accounts with specified privilege levels and password policies to help prevent unauthorized users from reconfiguring the switch and viewing its configuration.

Privilege Levels

A privilege level defines what commands that a user can enter by using the CLI after logging on to the switch. There are two methods of configuring a privilege level:

- Basic—Allows admin, read-only, or no access privileges.

  Users with read-only privileges are restricted from viewing the configuration, administration, and troubleshooting pages in the WebUI.
- Advanced—Allows privilege level between 0…15. Privilege 1 allows access in User Exec mode. Privilege 15 allows access in Privileged Exec mode.

Password Policies

A password policy is a security mechanism for defining rules, constraints, and restrictions to specify user passwords. You can create a password policy via the CLI, and then apply the policy to users when creating accounts.

Create a User Account Via the WebUI

From the Administration menu, choose User Administration.



From the User Administration page, you can add, edit, and delete users:

- To add a user, click Add, complete the fields as described in Table 156, and then click Apply to Device.
- To edit a user, click the name in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a user, check its associated checkbox in the grid, and then click Delete.

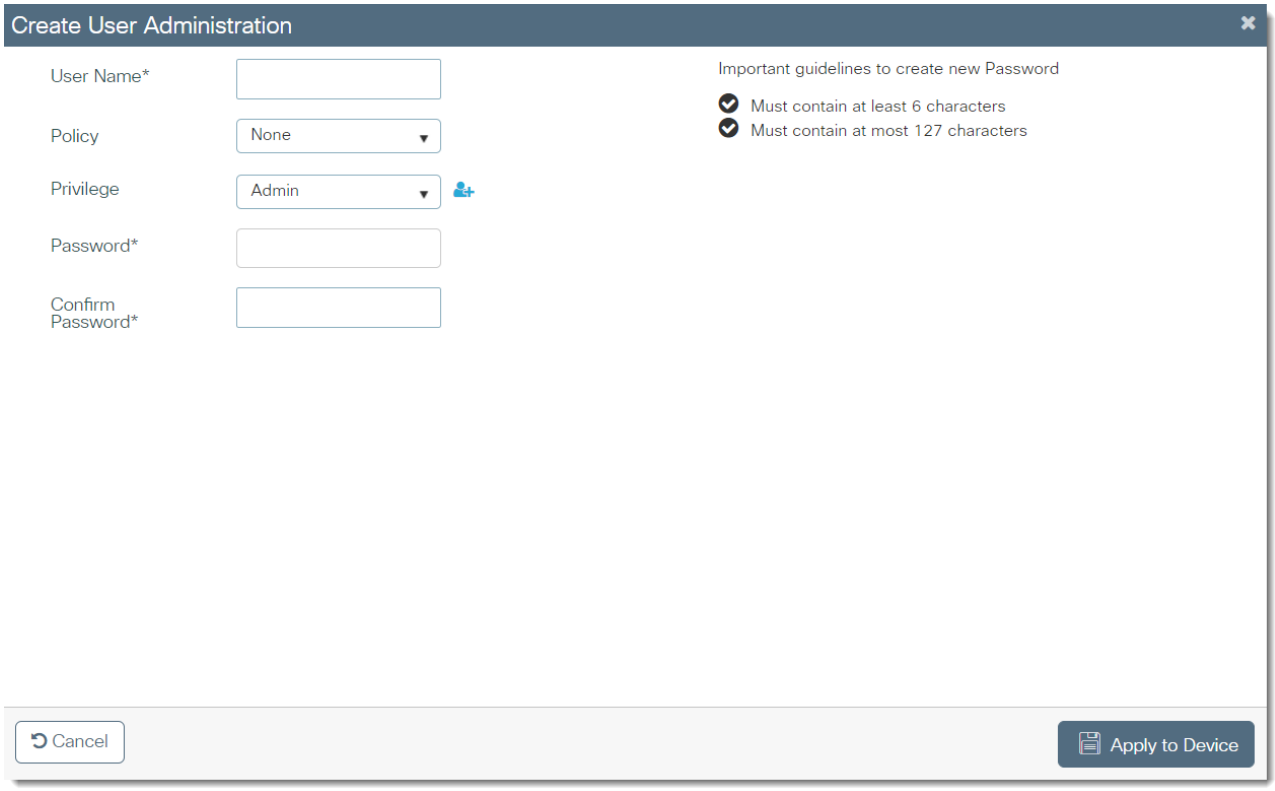


Table 156 - Create User Administration

Field	Description
User Name	Enter a unique user name.
Policy	(Optional). Choose a password policy. See Password Policies on page 277.
Privilege	To assign a basic privilege level, choose Admin, Read Only, or No Access. To assign an advanced privilege level, click the icon, and then choose a numeric value. See Privilege Levels on page 277.
Password	Enter the password to authenticate the user when they log on to the switch. See the guidelines in the upper-right corner of the page. The password must meet these requirements: • Minimum length: 6 characters • Maximum length: 27 characters • If you specified a password policy, the password must meet all criteria in the policy.
Confirm Password	Reenter the password.

Security Requirements (IEC-62443-4-2)

Topic	Page
Switch Security Features	279
Telnet	280
TLS 1.2	282
Additional Resources	283

Switch Security Features

To comply with the certification requirements, implement the security features in the following table in the order listed.

✓	Switch Security Feature	Required to Meet IEC-62443-4-2	Details
	IOS Release is certified for IEC-62443-4-2	Yes	To verify if your IOS release is certified for IEC-62443-4-2, access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc.
	Configure Certificate Authority (CA)	Yes	A CA provides a chain of trusts for devices in the network. This mechanism provides the ability for a user or process to trust the connection to one of these devices on the network by validating its identity. For more information, see the Security Configuration Guide available at https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg.html.
	Configure Authentication, Authorization, and Accounting (AAA)	Yes	AAA services provide flexible administrative control and accounting for network access. For more information, see Authentication, Authorization, and Accounting (AAA) on page 54 and the Security Configuration Guide available at https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg.html.
	Disable Telnet(1)	Yes	Telnet is disabled by default during Express Setup. Keep Telnet disabled to secure remote access to the switch, such as when you are using the command-line interface (CLI) to manage the switch from a computer. To verify that Telnet is disabled or disable Telnet if needed, see Telnet on page 280.
	Transport Layer Security (TLS) 1.2	Yes	TLS 1.2 is enabled by default during Express Setup. Keep this feature enabled to secure the exchange of data through encryption. To verify that TLS 1.2 is enabled or to enable TLS 1.2 if needed, see TLS 1.2 on page 282.
	Configure Type 9 password hashing	Yes	Hashing makes password storage more secure by transforming a password into data that cannot be converted back to the original password. For more information, see the User Security Configuration Guide at https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xe-16-12/sec-usr-cfg-xe-16-12-book.html.

(1) When both Telnet and Secure Shell (SSH) are disabled, the only way to access the switch is via console cable or HTTPS.



Secure web access to the switch is enforced via HTTPS. Attempts to access the switch via HTTP automatically redirect to secure access via HTTPS.

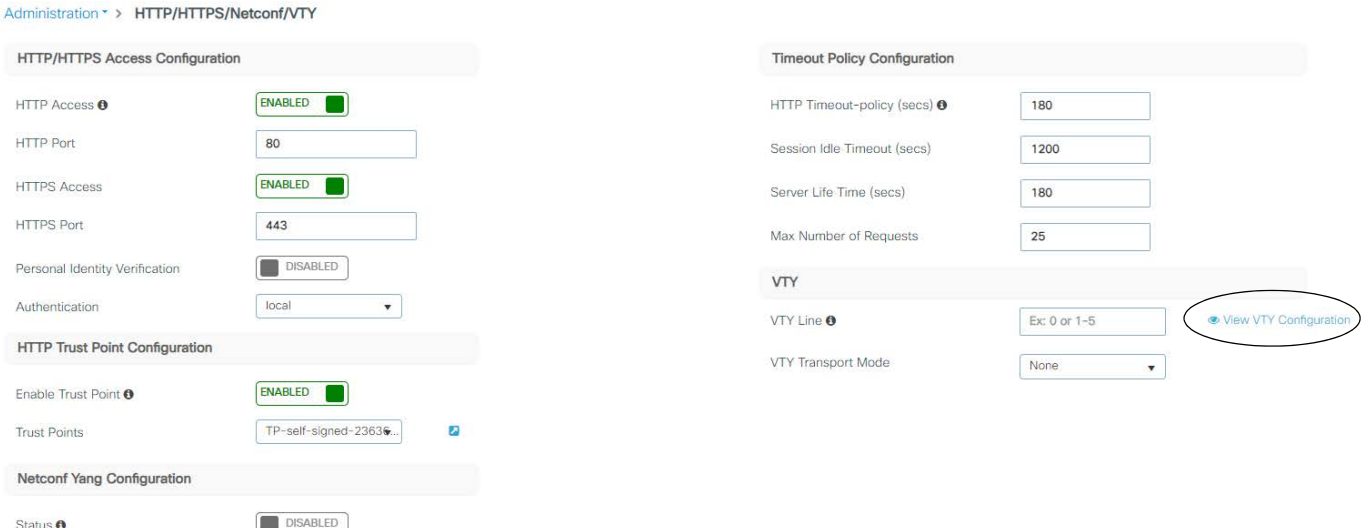
Telnet

Telnet must be disabled to comply with IEC-62443-4-2 requirements. By default, Telnet is disabled during Express Setup. The following procedures describe how you can verify that Telnet is disabled and disable it if needed.

Verify Telnet Settings

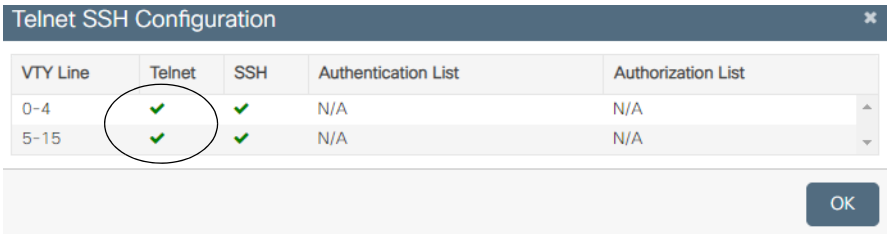
To verify that Telnet is disabled, follow these steps.

1. From the Administration menu, choose Device to Admin.
2. On the General tab, click View VTY options.



3. On the Telnet SSH Configuration dialog box, note which lines must be disabled, and then click OK.

   Telnet is currently enabled on any single lines or range with acheckbox in the Telnet column.

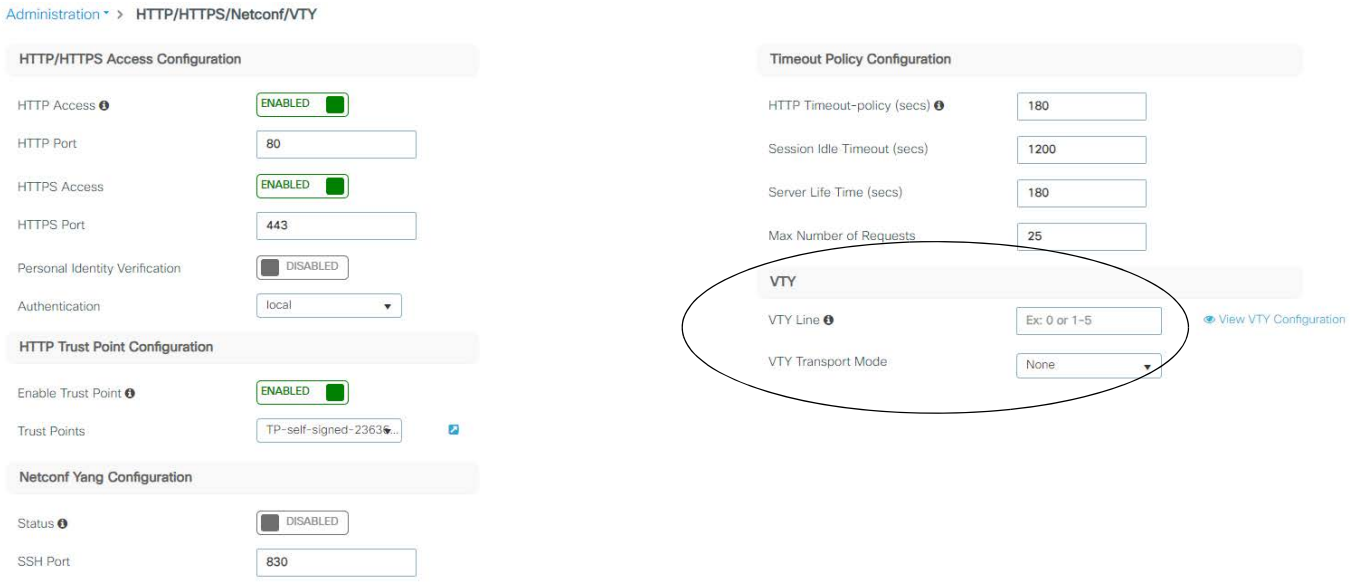


4. If Telnet is enabled on any lines to the switch, proceed to Disable Telnet on page 281.

Disable Telnet

To disable Telnet on lines to the switch, follow these steps.

1. From the Administration menu, choose Device to Admin.
2. In the VTY Line field, enter a single line or range of lines on which to disable Telnet.
3. In the VTY Transport Mode field, choose one of these values, and then click Apply:
   - SSH—SSH is enabled, and Telnet is disabled.
   - None—Both SSH and Telnet are disabled.



TLS 1.2

TLS 1.2 must be enabled and all other TLS versions must be disabled to comply with IEC-62443-4-2 requirements. By default, TLS 1.2 is enabled during Express Setup and all other versions are disabled. The following procedures describe how you can verify that TLS 1.2 is enabled and then enable it if needed.

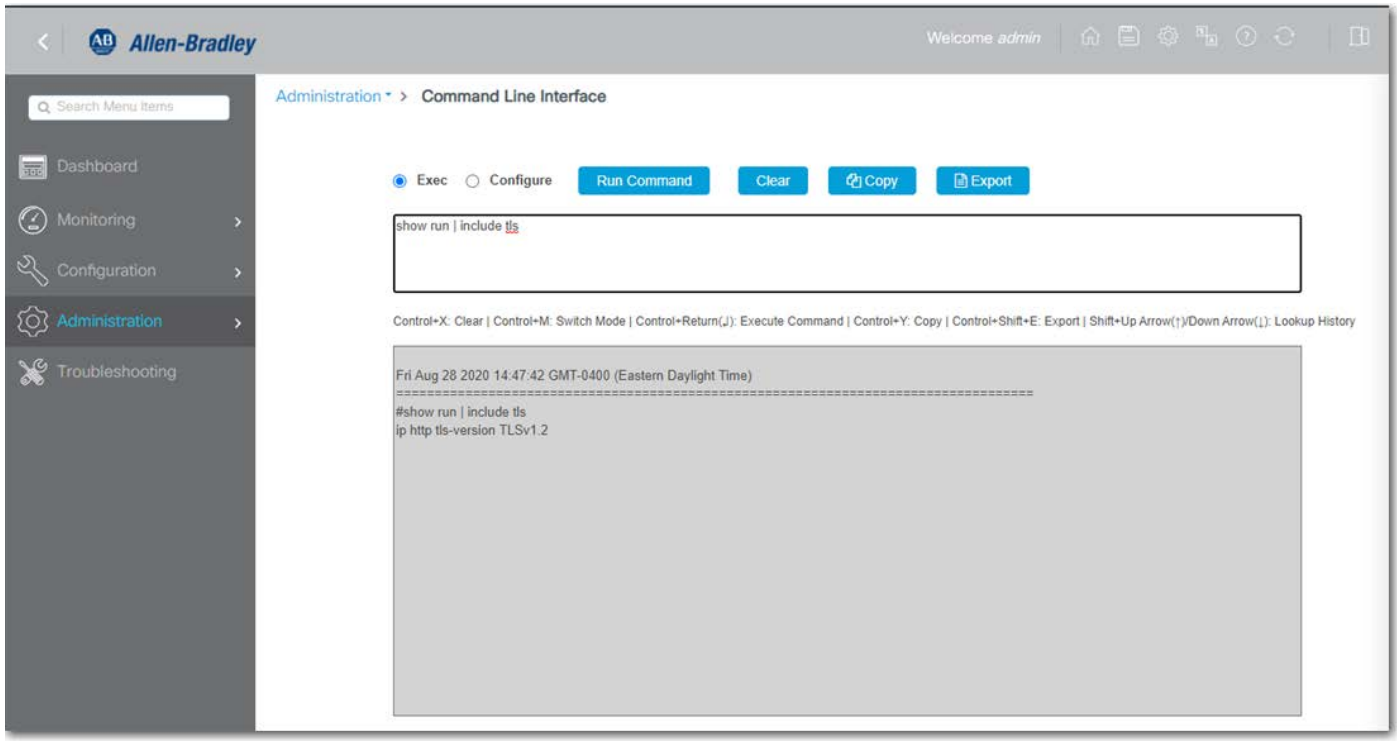
Verify TLS 1.2 Settings

To verify that TLS 1.2 is enabled, follow these steps.

1. From the Administration menu, choose Command Line Interface.
2. Click Exec to run the command in Executive mode.
3. In the text box, type the following command, and then click Run Command:

   show run | include tls

4. If the result is **ip http tls-version TLSv1.2**, then TLS 1.2 is enabled and only that version of TLS is allowed.
5. If any version other than 1.2 shows, proceed to Enable TLS 1.2 on page 283.



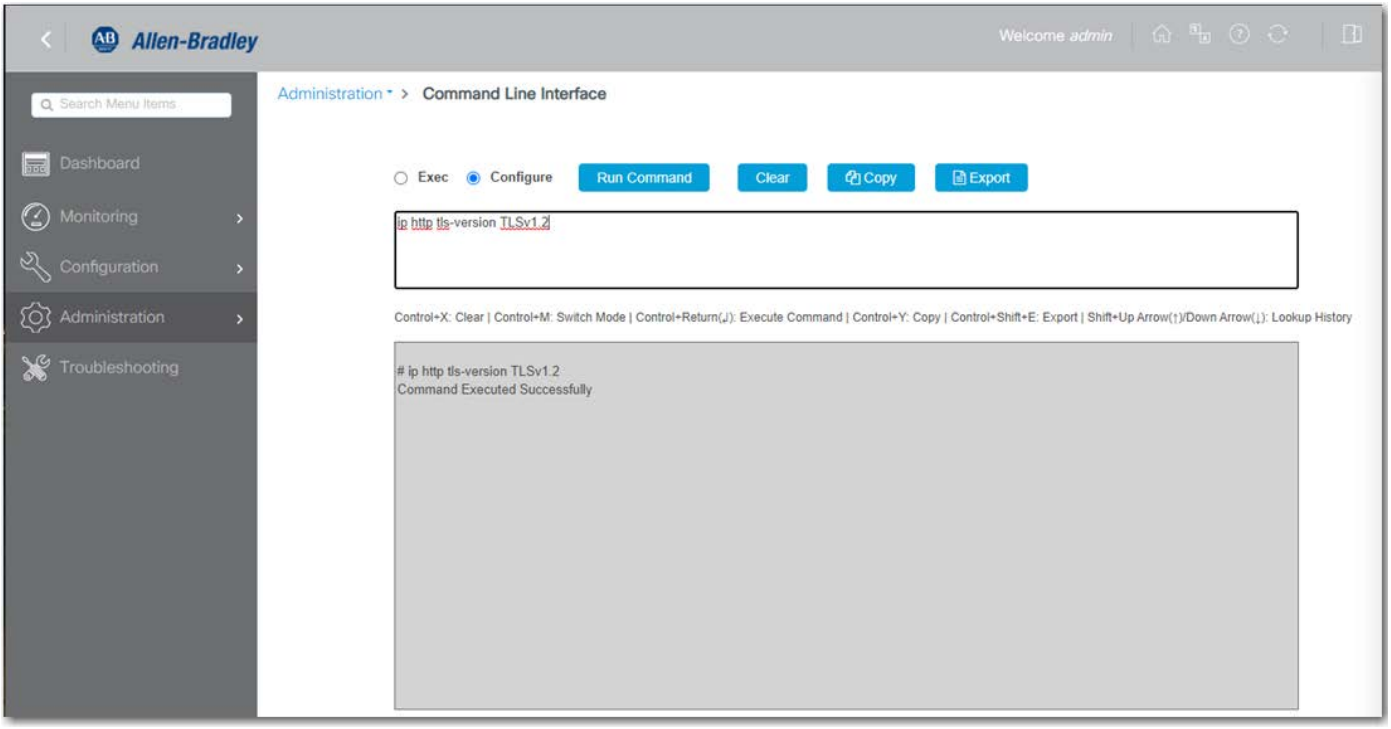
Enable TLS 1.2

To enable TLS 1.2, follow these steps.

1. From the Administration menu, choose Command Line Interface.
2. Click Configure to run the command in Configure mode.
3. In the text box, type the following command, and then click Run Command:

   ip http tls-version TLSv1.2

   The command enables TLS 1.2 and disallows any other version of TLS.



Additional Resources

For more information about how to implement security requirements, see the following resources.

Resource	Description
User Security Configuration Guide available at https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xe-16-12/sec-usr-cfg-xe-16-12-book.html	Cisco® publication that provides details about how to secure user access to the switch. For the User Security Configuration Guide that corresponds to the current IOS version on your switch, search www.cisco.com.
Security Configuration Guide available at https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg.html	Cisco publication that provides details about how to secure the switch on your network. For the Security Configuration Guide that corresponds to the current IOS version on your switch, search www.cisco.com.
Security Configuration User Manual, publication SECURE-UM001	Describes how to configure and use Rockwell Automation products to improve the security of your industrial automation system.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001.	Defines manufacturing-focused reference architectures to help accelerate the successful deployment of standard networking technologies and convergence of manufacturing and enterprise/business networks.

Notes:

Monitor the Switch

Topic	Page
Switch Status	286
Neighbors	287
CIP Sync (PTP)	289
Common Industrial Protocol (CIP)	293
Device Level Ring (DLR)	295
Dynamic Host Configuration Protocol (DHCP) Clients	298
HSR (Stratix 5800 Switch Only)	299
HSRP (Stratix 5800 Switch Only)	300
Network Address Translation (NAT)	301
MODBUS (Modicon Communication Bus)	307
Media Redundancy Protocol (MRP)	309
Ports	310
PROFINET	313
Parallel Redundancy Protocol (PRP)	315
Resiliency Ethernet Protocol (REP)	320
Spanning Tree Protocol (STP)	322
System	324
Time	327
VRRP (Stratix 5800 Switch Only)	337

Switch Status

In the Logix Designer application, you can view overall switch status information as shown in the following figure.

In the navigation pane, click Switch Status.

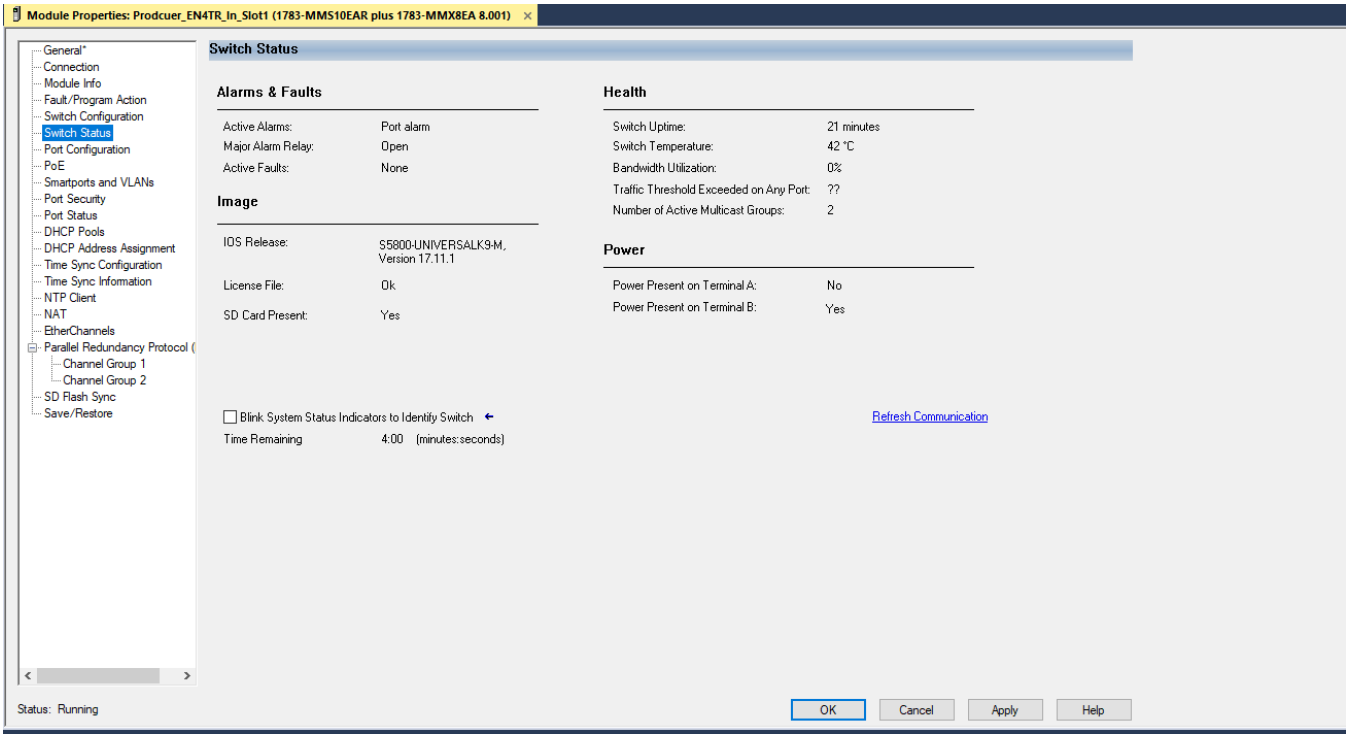


Table 157 - Switch Status

Field	Description
Alarms & Faults	
Active Alarms	The current active alarm: • None • Port alarm • Dual Mode Power Supply alarm • Primary Temperature alarm
Major Alarm Relay	The status of the alarm relay: • Open • Closed
Active Faults	The current active fault: • None • Port fault • Hardware fault If the port and hardware faults are active, the Hardware fault status appears.
Health	
Switch Uptime	The days, hours, and minutes that the switch has been functioning since the last restart.
Switch Temperature	The current internal temperature (in degree Celsius) of the switch.
Bandwidth Utilization	The total percentage of the switch bandwidth being used.
Traffic Threshold Exceeded on Any Port	Indicates whether the current unicast, multicast, and broadcast thresholds have been exceeded on any port.
Number of Active Multicast Groups	The number of active multicast groups.
Image	
IOS Release	The current version of the switch operating system.
License File	Indicates whether the license file is valid.
SD Card Present	Indicates whether the SD card is installed.
Power	
Power Present on Terminal A	Indicates whether power is present on terminal A.
Power Present on Terminal B	Indicates whether power is present on terminal B.

Neighbors

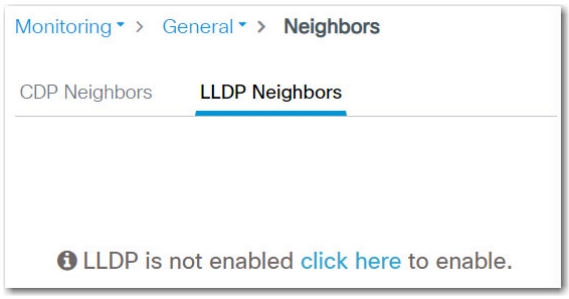
In the WebUI, you can view neighbor information that uses Cisco® Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).

When CDP or LLDP is enabled, you can use the neighbor information from each node to determine complete network topology.

From the Monitoring menu, choose Neighbors:

- To view CDP neighbor information, see the information on the CDP Neighbors tab as described in Table 158. For more information about CDP, see page 78.
- To view LLDP neighbor information, see the information on the LLDP Neighbors tab as described in Table 159. For more information about LLDP, see page 78.

  If LLDP is not enabled on the switch, a message appears. To enable LLDP, click the link in the message.



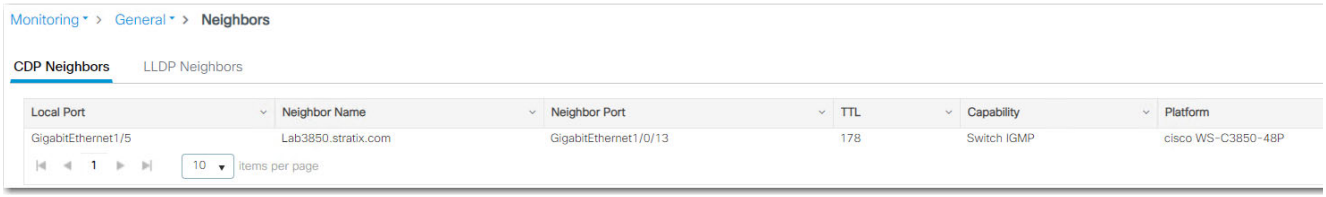


Table 158 - Monitor CDP Neighbors

Field	Description
Local Port	The port number on the local switch.
Neighbor Name	The name of the CDP neighbor device.
Neighbor Port	The port number on the CDP neighbor device.
TTL	The time left in seconds before each CDP neighbor entry expires.
Capability	The functional capability of the neighbor device: • Router • Trans Bridge • Source Route Bridge • Switch • Host • IGMP • Repeater • Remotely Managed Device
Platform	The platform of the CDP neighbor device.



Table 159 - Monitor LLDP Neighbors

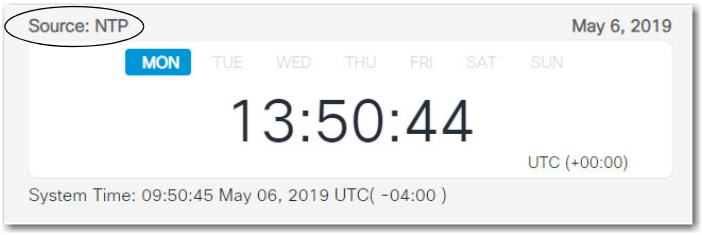
Field	Description
Local Interface	The local interface through which this neighbor is connected.
Device ID	The ID of the neighboring device.
Port ID	The interface and port number of the neighboring device.
Capability	The device type of the neighbor, indicated by the capability code discovered on the device: • Router • Trans Bridge • Source Route Bridge • Switch • Host • IGMP • Repeater • Remotely Managed Device

CIP Sync (PTP)

In the WebUI, you can monitor time details for the time source that is configured on the switch.

From the Monitor menu, choose Time.

The clock at the top of the page shows the local time and the time source. The time source indicates where the switch is receiving its time, such as from an NTP server, PTP, or the local computer.



PTP Details

PTP Details shows the properties of the local PTP clock and the clock identity.

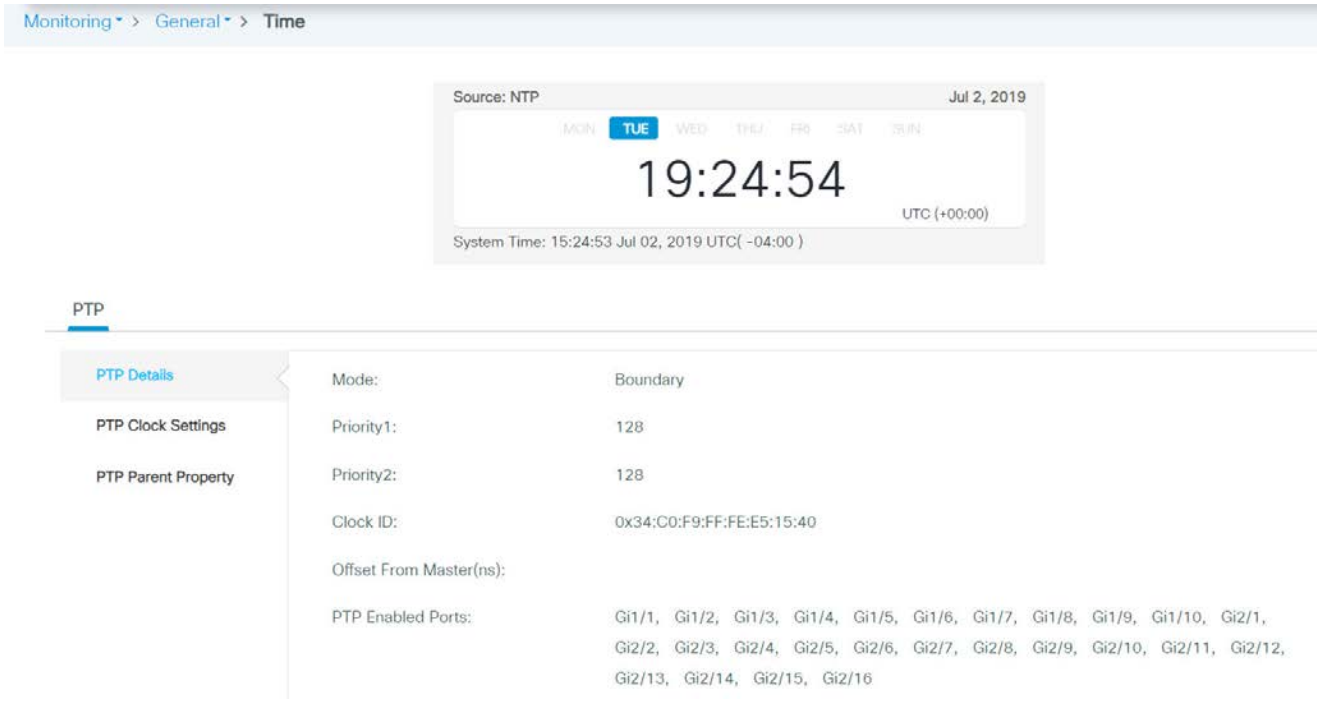


Table 160 - Monitor Time—PTP Details

Field	Description
Mode	The PTP mode configured for the switch: • Forward • Boundary • End to End Transparent • GMC-BC (NTP-PTP Clock)
Priority 1	(Appears only for Boundary and NTP-PTP mode). Priority 1 preference value of the PTP clock. The priority1 clock is considered first during clock selection.
Priority 2	(Appears only for Boundary and NTP-PTP mode). Priority 2 preference value of the PTP clock. The priority2 clock is considered after all other clock sources during clock selection.

Table 160 - Monitor Time—PTP Details (Continued)

Field	Description
Clock ID	(Appears only for Boundary and NTP-PTP mode). The unique clock identity.
Offset From Master (ns)	(Appears only for Boundary and NTP-PTP mode). The time offset between the slave and master clocks.
PTP Enabled Ports	(Appears only for Boundary and End to End Transparent modes).The list of ports that are assigned to the PTP clock.

PTP Clock Settings

PTP Clock Settings shows the settings of the local PTP clock when PTP is in Boundary and End to End Transparent mode.

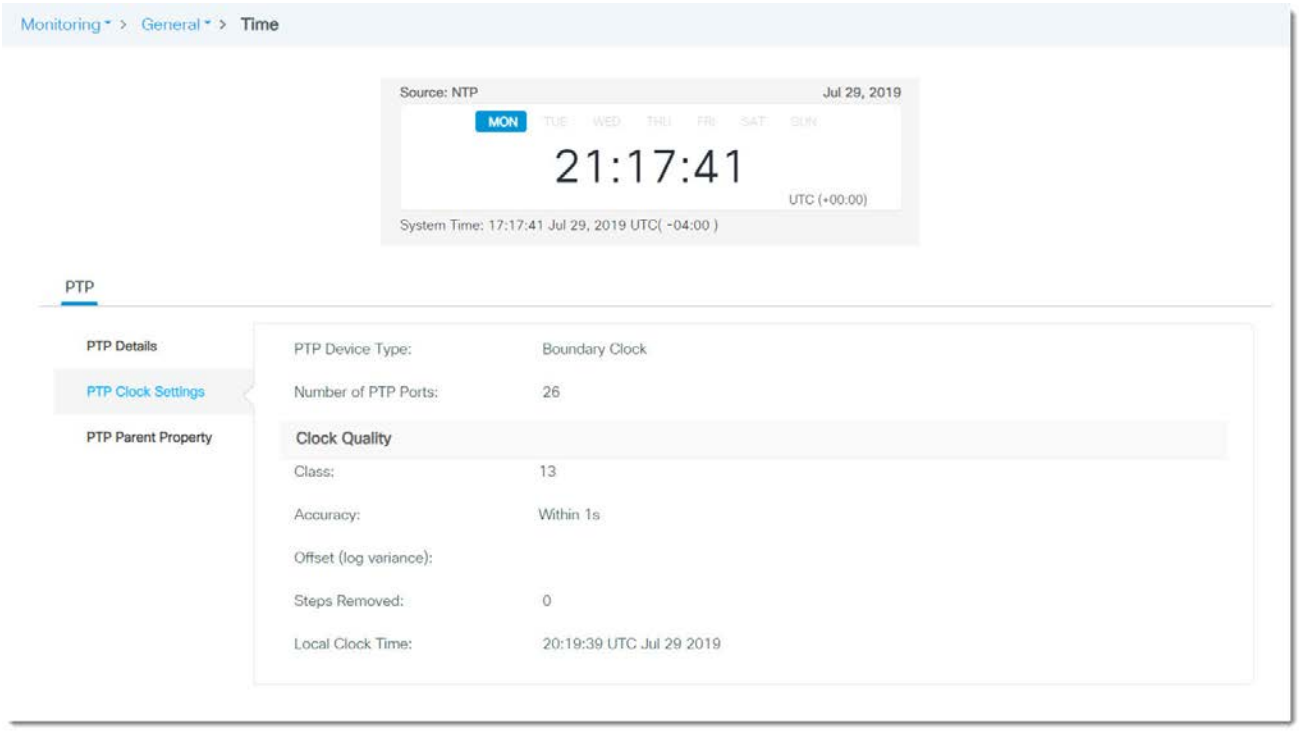


Table 161 - Monitor Time—PTP Clock Settings

Field	Description
PTP Device Type	The PTP clock type as determined by the PTP mode configured on the switch. • Forward Clock • Boundary Clock • End to End Transparent Clock • GMC-BC (NTP-PTP Clock)
Number of PTP Ports	The number of ports that are assigned to the PTP clock.
Class	(Appears only for Boundary and NTP-PTP clock type). The time and frequency traceability of the Grandmaster clock.
Accuracy	(Appears only for Boundary and NTP-PTP clock type. Applies only when the Best Master Clock algorithm is in use.) This is an enumerated list of ranges of accuracy to UTC.
Offset (log variance)	(Appears only for Boundary and NTP-PTP clock type). The offset between the Grandmaster clock and the parent clock.
Steps Removed	The number of hops from the local clock to the Grandmaster clock.
Local Clock Time	The time of the local PTP clock.

PTP Parent Property

PTP Parent Property shows the properties of the PTP parent clock when PTP is in Boundary and NTP-PTP mode.

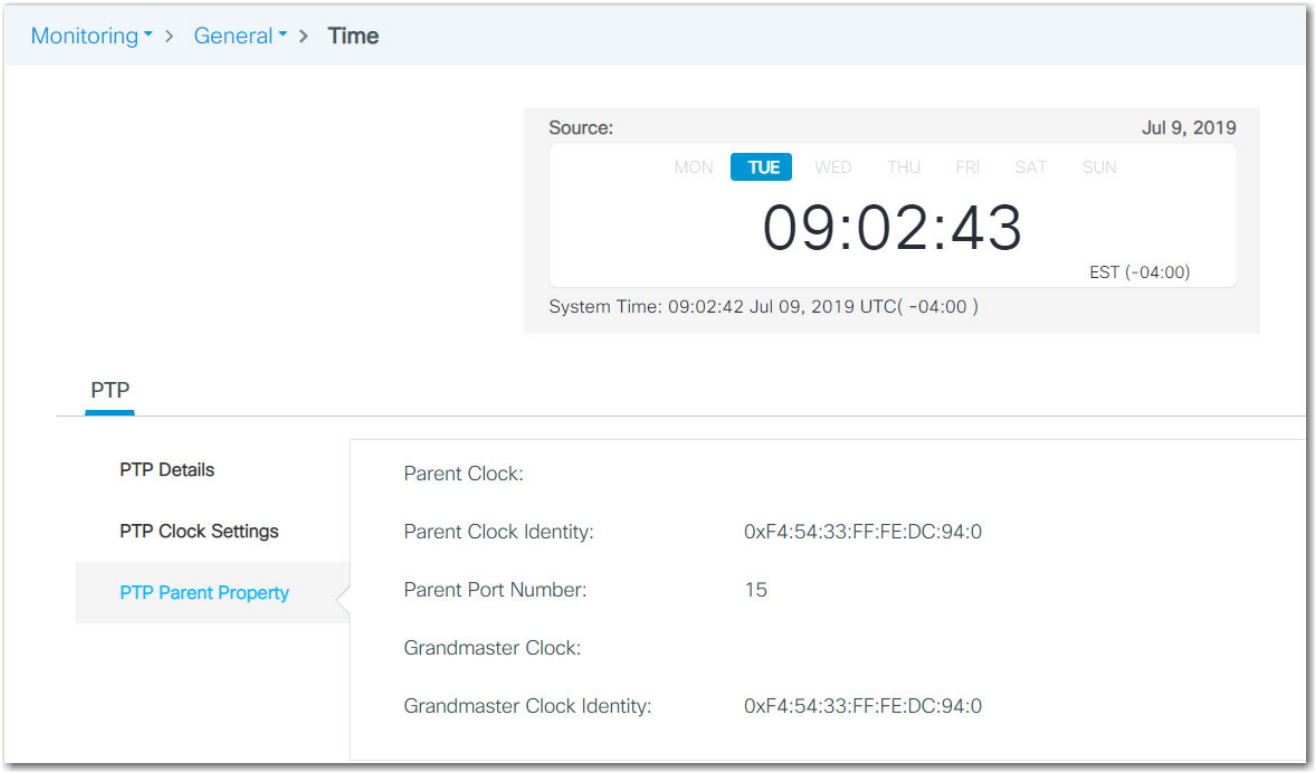
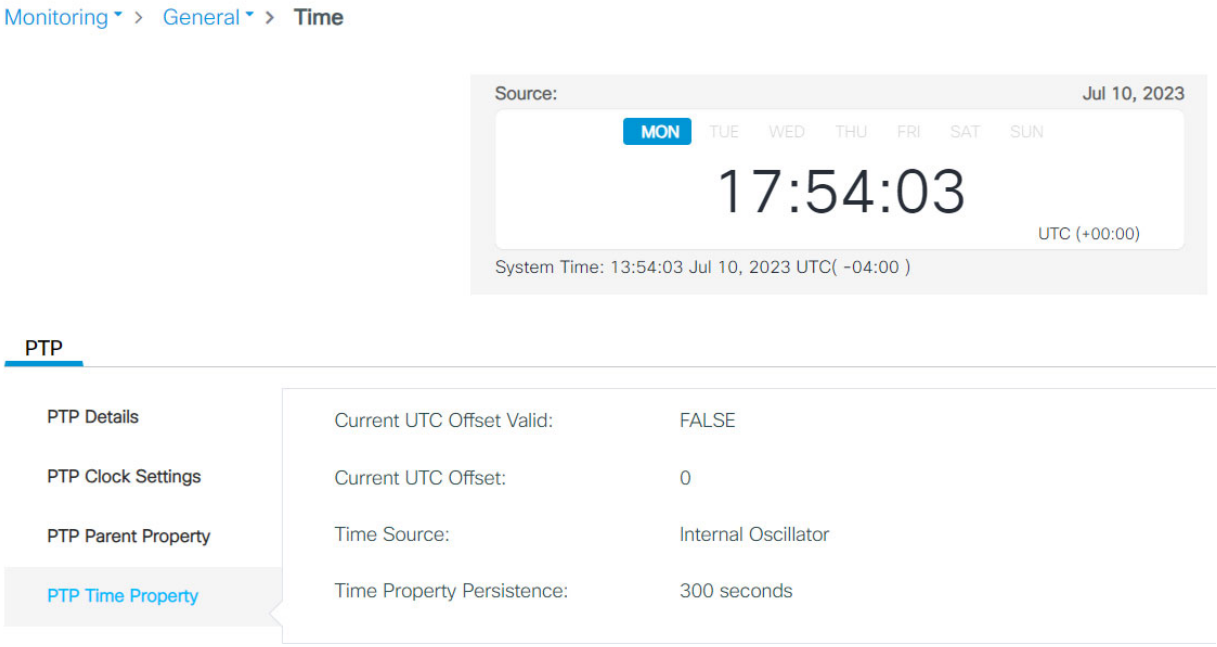


Table 162 - Monitor Time—PTP Parent Property

Field	Description
Parent Clock	The clock to which the member-slave clocks synchronize.
Parent Clock Identity	The unique parent clock identity.
Parent Port Number	The clock port ID of the parent port.
Grandmaster Clock	The root of the master-slave clock hierarchy.
Grandmaster Clock Identity	The unique Grandmaster clock identity.

PTP Time Property

Display the PTP time properties.



Common Industrial Protocol (CIP)

In the WebUI, you can monitor information about CIP™ status and statistics since the switch was last powered on, was restarted, or the counters were last reset.

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 Monitoring menu, choose CIP:

- To view general CIP information, such as status, VLAN, and total number of connections, see the information on the Overview tab as described in Table 163.
- To view connection details, see the information on the Connection Details tab as described in Table 164.

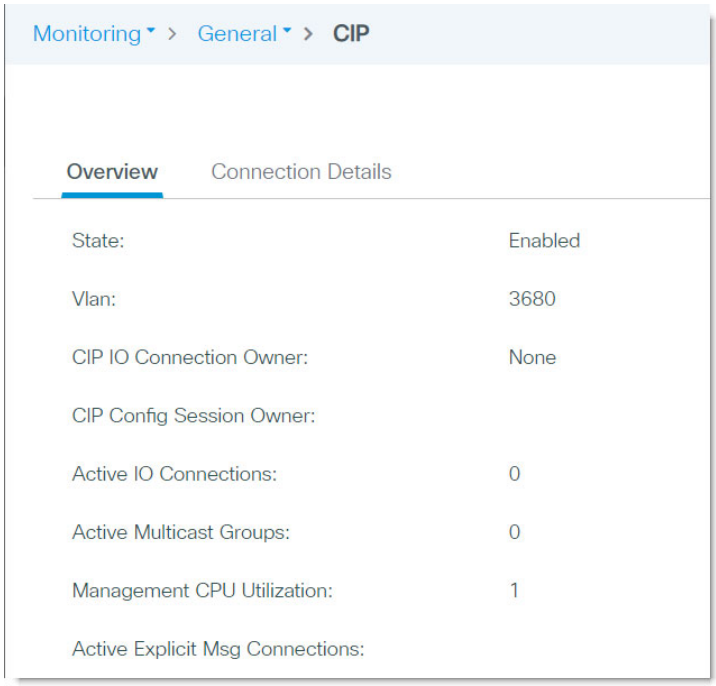


Table 163 - Monitor CIP—Overview Tab

Field	Description
State	The state of the CIP protocol: • Enabled • Disabled
Vlan	The CIP VLAN ID.
CIP IO Connection Owner	The IP address of the device to and from which application-specific I/O output data is sent.
CIP Config Session Owner	The IP address of the device controlling the CIP configuration session.
Active IO Connections	The number of active application-specific connections between a producing application and one or more consuming applications.
Active Multicast Groups	The number of multicast groups, including the CIP multicast group, configured on the device.
Management CPU Utilization	The CPU usage (%) for the CIP configuration session owner.
Active Explicit Msg Connections	The number of active explicit message connections (generic, multipurpose communication) between devices.

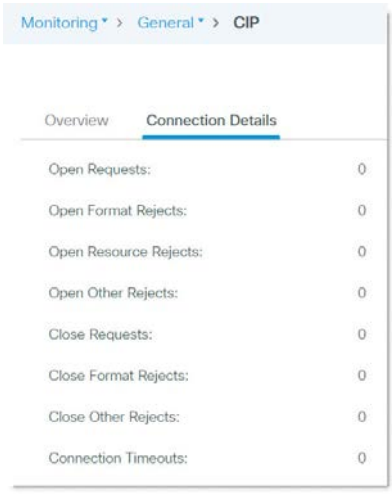


Table 164 - Monitor CIP—Connection Details Tab

Field	Description
Open Requests	The number of Forward Open requests to establish a connection with an industrial device in the network.
Open Format Rejects	The number of Forward Open requests that failed because the request was 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.
Open Other Rejects	The number of Forward Open requests that failed for reasons such as incompatible electronic keying.
Close Requests	The number of Forward Close requests received after a connection is successfully established with an industrial device in the network.
Close Format Rejects	The number of Forward Close requests that failed because the request was not in the proper format.
Close Other Rejects	The number of Forward Close requests that failed for reasons such as incompatible electronic keying.
Connection Timeouts	The number of connection timeouts that have occurred.

Device Level Ring (DLR)

Use the Monitoring > General > DLR page to view information and status of the Device Level Ring (DLR) rings configured on the system. Select the ring number from the drop-down menu to see the status for that ring.

A diagram of each configured ring displays the status of the switch as a DLR member and shows which ports are configured for DLR. The diagram provides the ring port status shown in Table 165.

Table 165 - DLR Ring Status Port

Status	Description
Green	Forwarding Port: Ring ports forward all received frames.
Red	Not Connected Port: The link is physically down or disconnected. (This state differs from the Disabled state, in which the DLR Port is manually disabled through software.)
Gray	Disabled Port: Ring ports drop all received frames.

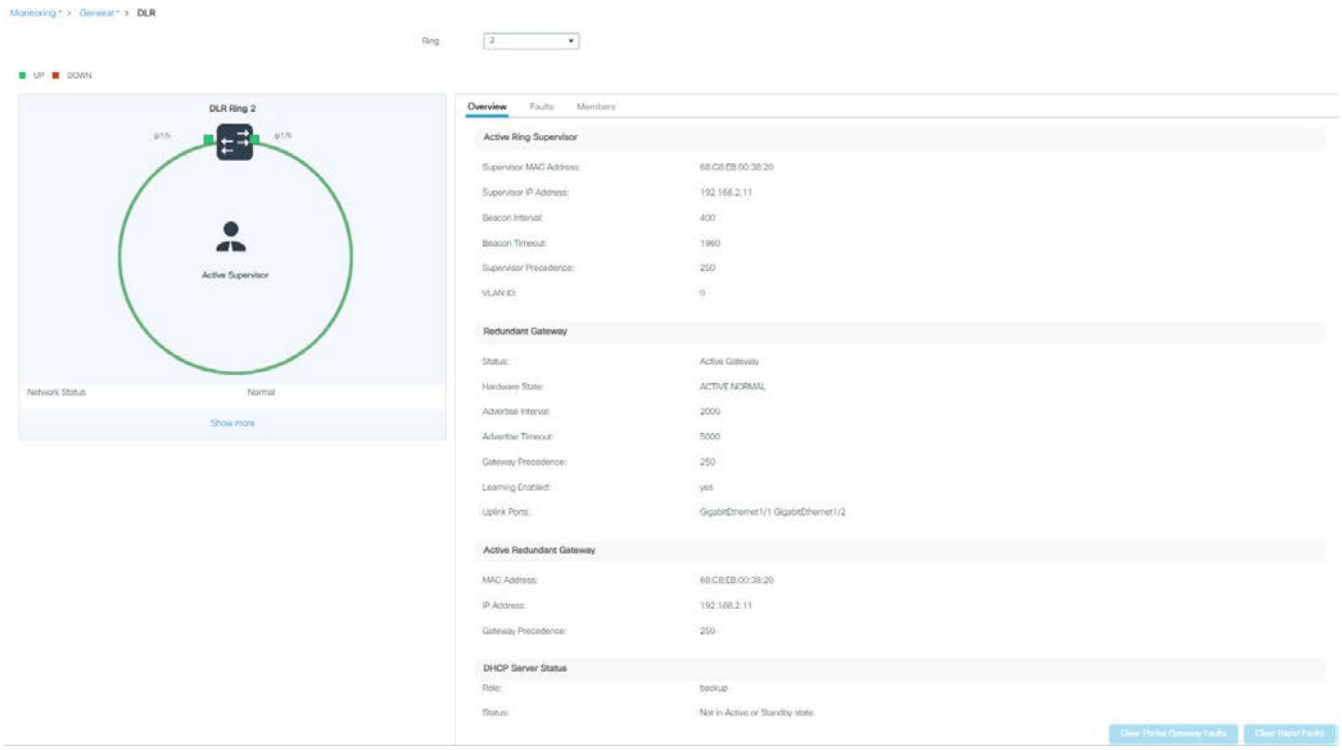
The ring states, indicated by the ring colors, are shown in table Table 166

Table 166 - DLR Ring States

Status	Description
Black dashed line	Represents beacon node ring.
Green solid line	Supervisor ring in normal operation.
Red open line	Supervisor ring in error condition due to link failure or power loss in any other device in the ring.

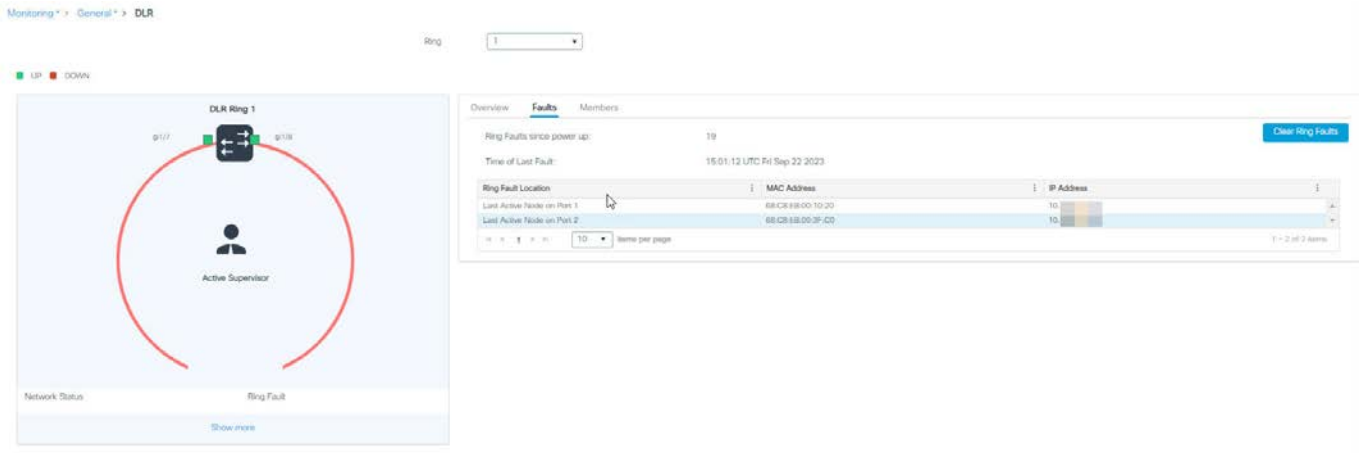
Overview Tab

The Overview tab displays the settings of the Active Supervisor. The Overview tab also displays status and settings for the Backup Supervisor and Redundant Gateway, if configured.



Faults Tab

The Faults tab displays fault statistics for the ring, including the number of faults since power-up, time of last fault, and the MAC and IP addresses of the node where the fault occurred. Click Clear Ring Faults to clear the supervisor's ring fault count.



Members Tab

The Members tab displays the node number, MAC address, and IP address for each node in the ring.

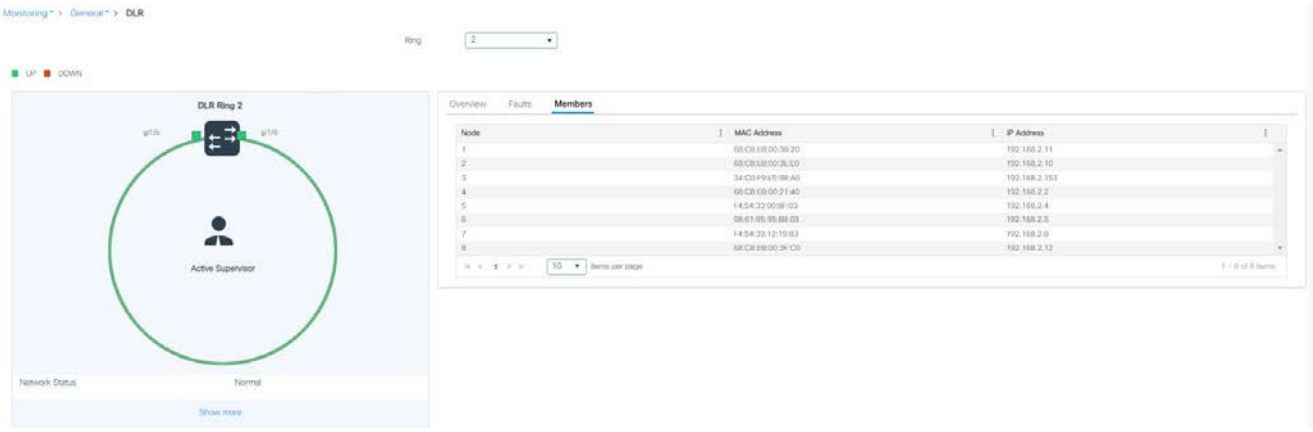


Table 167 - Switch DLR Status

Parameter	Description
Network Status	Current network status based on the device's view of the network. Possible values are: • Normal—Operation is normal. • Ring Fault— A ring fault has been detected. • Unexpected Loop Detected— A loop has been detected in the network. • Partial Network Fault— A network fault has been detected in one direction only. This fault occurs only when the node is the active ring supervisor. • Rapid Fault/restore Cycle— A series of rapid ring fault/restore cycles has been detected. Similar to the Partial Network Fault status, the supervisor remains in a state with forwarding blocked on its ring ports. Clear this condition by clicking Clear Rapid Faults.
Ring Type	Physical media type.
Network Topology	Ring.
IP Address	IP address of the ring node.
MAC Address	MAC address of the ring node.
VLAN ID	VLAN ID used when sending DLR protocol frames.

Table 168 - Active Supervisor

Parameter	Description
Supervisor MAC Address	MAC address of the active supervisor.
Supervisor IP Address	IP address of the active supervisor.
Beacon Interval	Interval for active supervisor to transmit beacon frames.
Beacon Timeout	Amount of time ring nodes wait before timing out in the absence of received beacon messages.
Precedence	Precedence value assigned to ring supervisor and transmitted in beacon frames.
VLAN ID	VLAN ID used when sending DLR protocol frames.

Table 169 - Redundant Gateway

Parameter	Description
Status	Active, Backup, or not enabled.
Advertise Internal	Interval for gateway to transmit advertise messages.
Advertise TImeout	Amount of time nodes wait before timing out in the absence of received advertise messages.
Gateway Precedence	Precedence value assigned to redundant gateway and transmitted in advertise messages.
Learning Enabled	Whether learning update is enabled.
Uplink Ports	Names of gateway uplink ports.

Table 170 - DHCP Server Status

Parameter	Description
Role	Role of the Ring DHCP server: • None • Primary • Backup • Secondary
Status	Ring DHCP server status: • Active • Standby • Not in Active or Standby state

Dynamic Host Configuration Protocol (DHCP) Clients

In the WebUI, you can view information about devices that receive IP addresses from the switch when it is configured as a DHCP server. These devices are known as DHCP clients.

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.

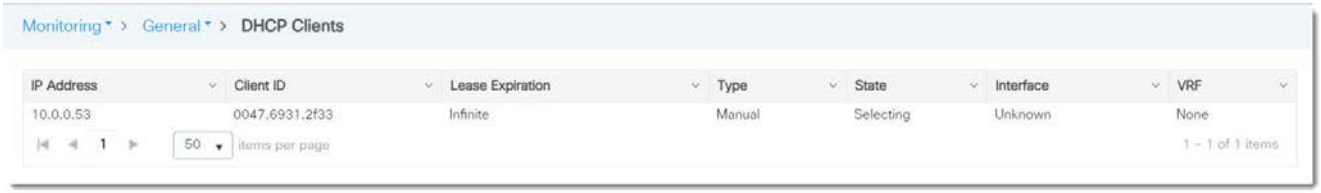


Table 171 - Monitor DHCP Clients

Field	Description
IP Address	The IP address that the switch assigned to the DHCP client.
Client ID	The MAC ID of the DHCP client.
Lease Expiration	The lease expiration date of the IP address.
Type	The manner in which the IP address was assigned to the host: • Automatic—The IP address of the DHCP client was dynamically assigned from the DHCP pool of IP addresses. • Manual—The IP address of the DHCP client was set to a specific IP address via the DHCP Persistence feature.
State	The state port that connects to the DHCP client.
Interface	The port that connects to the DHCP client.
VRF	The table that provides virtual routing and forwarding.

HSR (Stratix 5800 Switch Only)

Open the HSR page under the Monitoring tab to view information and status of the HSR ring configured on the system. A diagram of the configured ring provides a visual representation of the ring port status, as indicated by the following table.

State	Description
Green	Port in use
Red	Port not in use

The ring states, indicated by the ring colors, are listed in the following table.

State	Description
Green Solid Line	Ring in use The HSR mode (HSR-SAN) is displayed.
Red Open Line	Ring not in use "Unknown" is displayed for the HSR mode.



The HSR feature is only available on hardware systems that support advanced features.

Table 172 - Monitor HSR

Parameter	Description
Ring Name	HS1
Layer Type	Network type of the ports in the HSR ring - Layer2 or Layer3.
Port 1	Port name and number of HSR ring port number 1.
Port 2	Port name and number of HSR ring port number 2.
Ring Status	InUse or Not-InUse.
MAC Address	RedBox MAC address.
Description	If configured, a description of the HSR ring.

To display information about Virtual DAN (VDAN) and Node entries in the HSR network, click the VDAN or Node tab.

VDAN

Table 173 - HSR VDAN

Parameter	Description
Ring Number	HSR ring 1.
MAC Address	MAC Address of the VDAN.
TTL	Amount of time before the learned MAC address expires.
Dynamic	Whether or not (Y or N) the entry was added as a learned MAC address.

Node

Table 174 - HSR Node

Parameter	Description
Ring Number	HSR ring 1.
Type	Type of HSR ring node: • DANH—Dual Attached Node • SAN —Singly Attached Node
MAC Address	MAC Address of the HSR ring node.
TTL	Amount of time before the learned MAC address expires.
Dynamic	Whether or not (Y or N) the entry was added as a learned MAC address.

HSRP (Stratix 5800 Switch Only)

The Stratix 5800 Switch allows you to monitor HSRP.

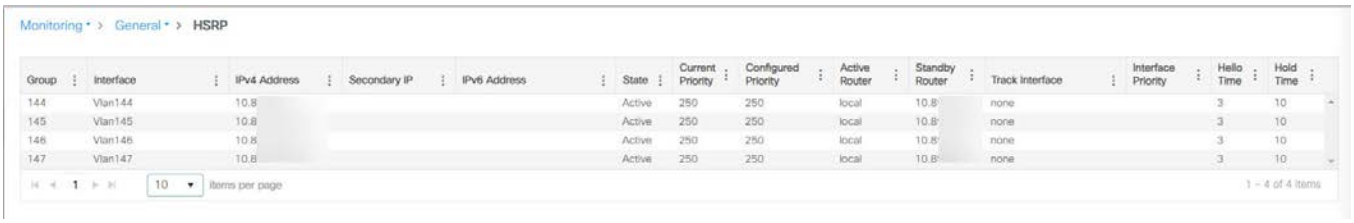


Table 175 - HSRP Parameters

Parameter	Description
Group	Hot Standby group number for the interface.
Interface	Interface type and number.
IPv4 Address	IPv4 address of the Hot Standby router interface.
Secondary IP	Secondary IP address of the Hot Standby router interface.
IPv6 Address	IPv6 address of the Hot Standby router interface.
State	State of local router; can be one of the following: • Active—Indicates the current Hot Standby router. • Standby—Indicates the router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak. • Init or Disabled—Router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state. For these cases, the Active Router and Standby Router fields show "unknown." The state is listed as disabled in the fields when the IP address of the Hot Standby router interface has not been specified. • Init (tracking shutdown)—HSRP groups appear in the Init state when HSRP group shutdown has been configured and a tracked object goes down.
Priority	The priority value used in choosing the active router.
Active Priority	Address of the current active Hot Standby router. Value can be "local," "unknown," or an IP address.
Standby Router	Address of the "standby" router (the router that is next in line to be the Hot Standby router). Value can be "local," "unknown," or an IP address.
Track Interface	Name of interface that is being tracked.
Interface Priority	Amount by which the Hot Standby priority for the router is decremented (or incremented) when the tracked interface goes down (or comes back up).
Hello Time	Time (in seconds) between hello packets.
Hold TIme	Time (in seconds) before other routers declare the active or standby router to be down.

Network Address Translation (NAT)

You can view details about NAT globally and per instance in both the WebUI and the Logix Designer application.

Monitor NAT Statistics via the WebUI

From the Monitoring menu, choose L2NAT:

- To view global and per instance statistics, see the header and grid area on the L2NAT page as described in Table 176.
- To view statistics for a single NAT instance, click the instance in the grid to display the Instance Details page as described in Table 177 and Table 178.
- To reset counters to zero, click Clear All.

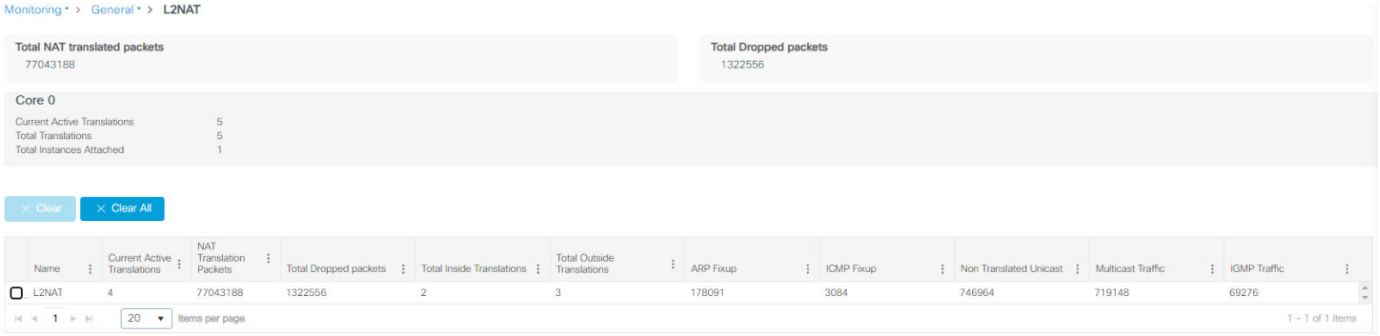


Table 176 - L2NAT

Field	Description
Global Statistics	
Total NAT translated packets	The number of packets that were translated by the switch.
Total Dropped packets	The number of packets that were dropped due to NAT rules.
Core 0	Statistics for Core 0 (on the Stratix® 5800 switch, there is only one core named Core 0).
Current Active Translations	The number of translations in applied NAT instances.
Total Translations	The total number of private and public translations.
Total Instances Attached	The number of NAT instances.
Instance Statistics	
Name	The name of the NAT instance.
Current Active Translations	The number of translations in the NAT instance.
NAT Translation Packets	The number of translated packets in the NAT instance.
Total Dropped packets	The number of packets that were dropped due to settings in the NAT instance.
Total Inside Translations	The number of internal addresses translated to external addresses in the NAT instance.
Total Outside Translations	The number of external addresses translated to internal addresses in the NAT instance.
ARP Fixup	The number of packets handled with the ARP Fixup to change dynamic ARP entries into static entries in the NAT instance.
ICMP Fixup	The number of packets handled with the ICMP Fixup to change dynamic ICMP entries into static entries in the NAT instance.
Non Translated Unicast	The number of unicast traffic packets that were not translated in the NAT instance.
Multicast Traffic	The number of multicast traffic packets in the NAT instance.
IGMP Traffic	The number of ICMP traffic packets in the NAT instance.

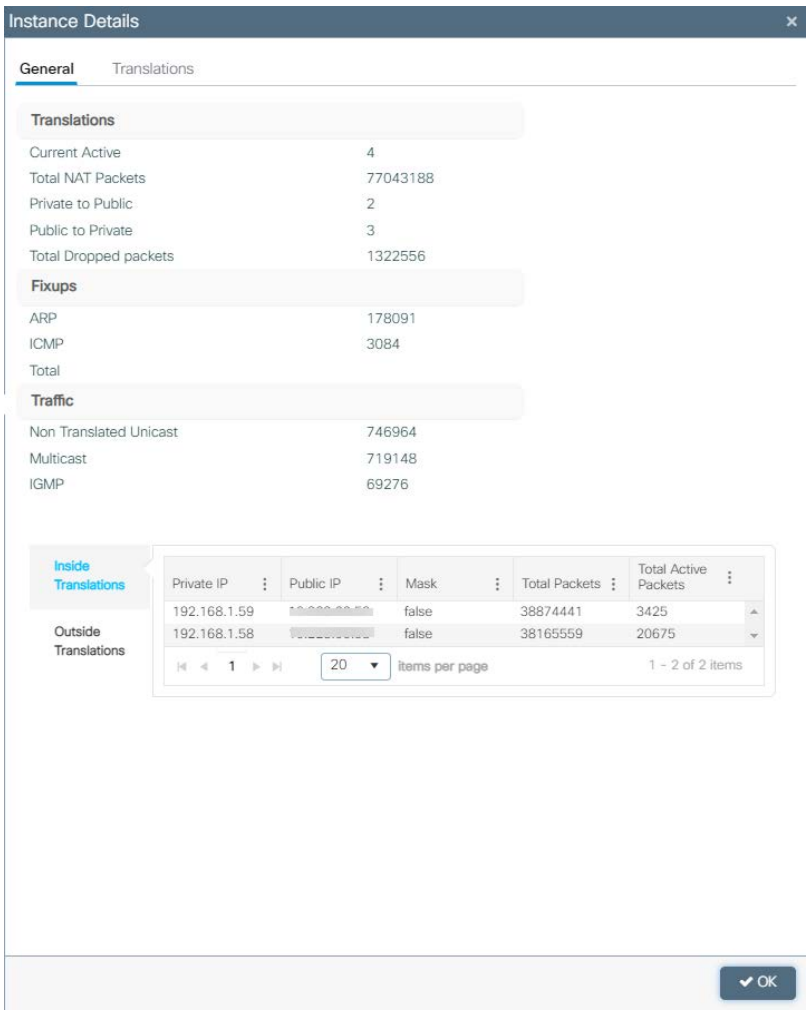


Table 177 - Instance Details—General Tab

Field	Description
Translations	
Current Active Translations	The number of translations in the NAT instance.
Total NAT Packets	The number of translated packets in the NAT instance.
Private to Public	The number of private addresses translated to public addresses in the NAT instance.
Public to Private	The number of public addresses translated to private addresses in the NAT instance.
Total Dropped packets	The number of packets that were dropped due to settings in the NAT instance.
Fixups	
ARP	The number of packets handled with ARP Fixup to change dynamic ARP entries into static entries in the NAT instance.
ICMP	The number of packets handled with the ICMP Fixup to change dynamic ICMP entries into static entries in the NAT instance.
Total	The total number of packets that were fixed up.
Traffic	
Non Translated Unicast	The number of unicast traffic packets that were not translated.
Multicast	The number of multicast traffic packets.
IGMP	The number of ICMP traffic packets.

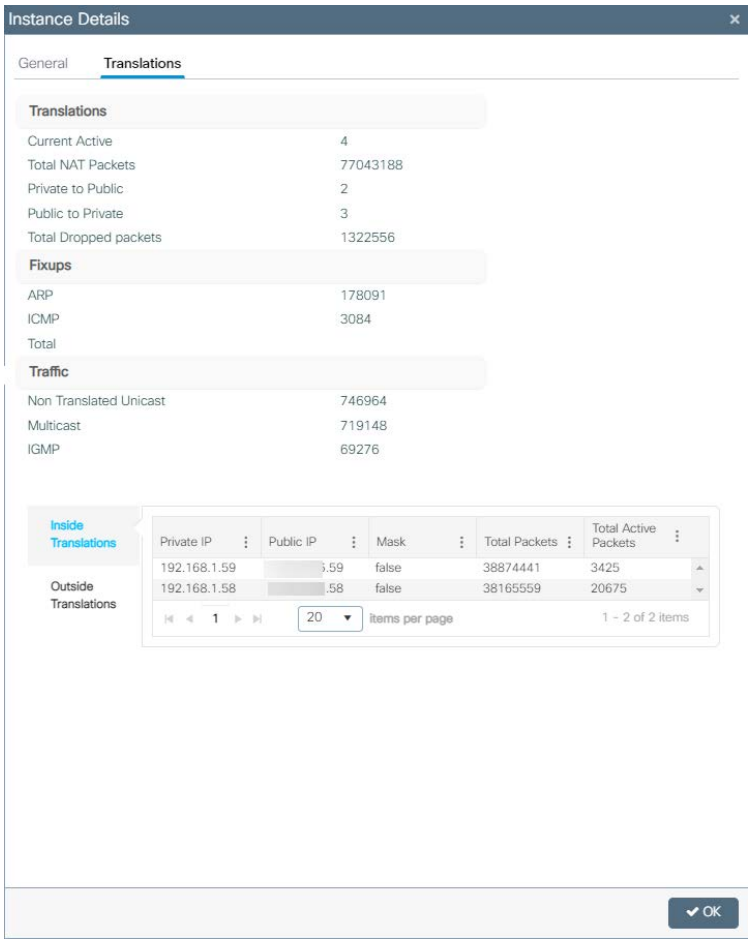


Table 178 - Instance Details—Translations Tab

Field	Description
Private IP	The IP address on the private (inside) network.
Public IP	The IP address on the public (outside) network.
Mask	The subnet mask for the network IP address.
Total Packets	The total number of translated packets.
Total Active Packets	The total number of active packets translated.

Monitor NAT Statistics via the Logix Designer Application

In the navigation pane, click NAT:

- To view NAT statistics across all NAT instances, see the Global Diagnostics area described in Table 179.
- To view statistics for a specific NAT instance, click the Ellipse button in the Diagnostics column for the instance. See Table 180.

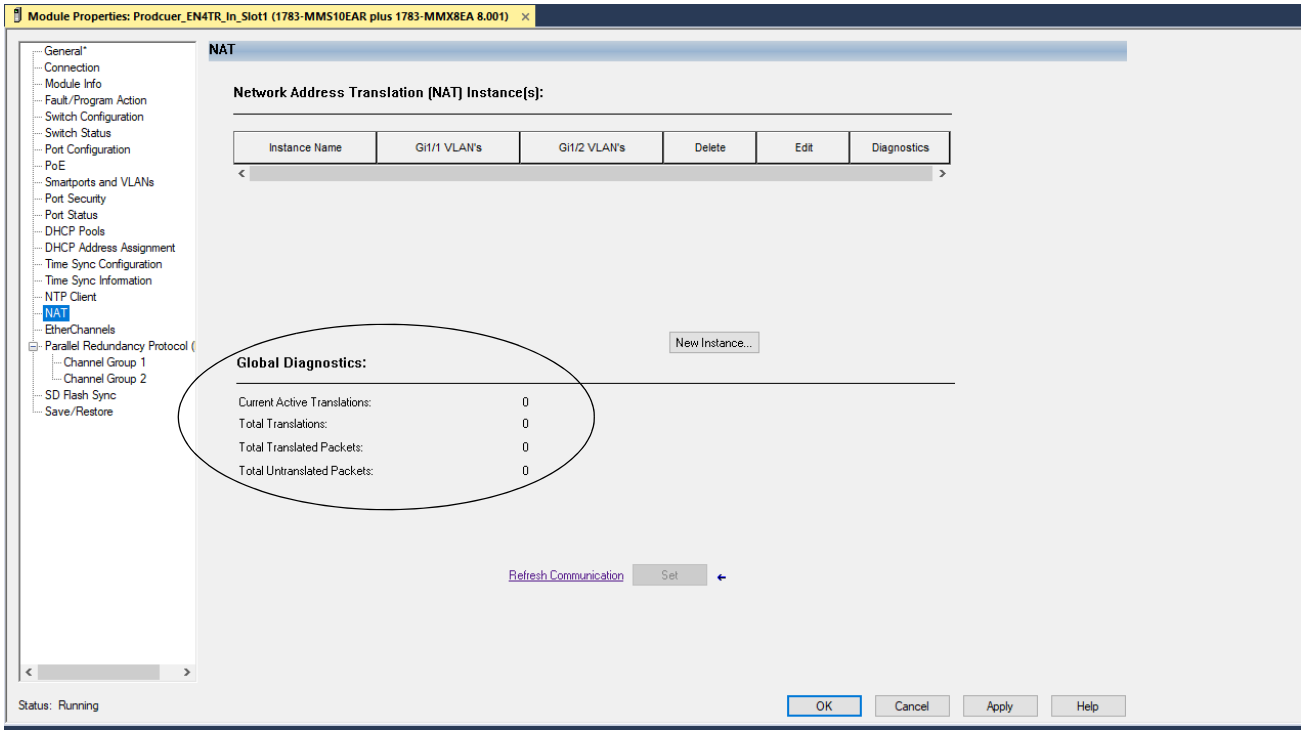


Table 179 - Global Diagnostics

Field	Description
Current Active Translations	The total number of translations that occurred within the last 90 seconds across all NAT instances.
Total Translations	The total number of translations across all NAT instances.
Total Translated Packets	The total number of translated packets across all NAT instances.
Total Untranslated Packets	The total number of packets that have been bypassed across all NAT instances.

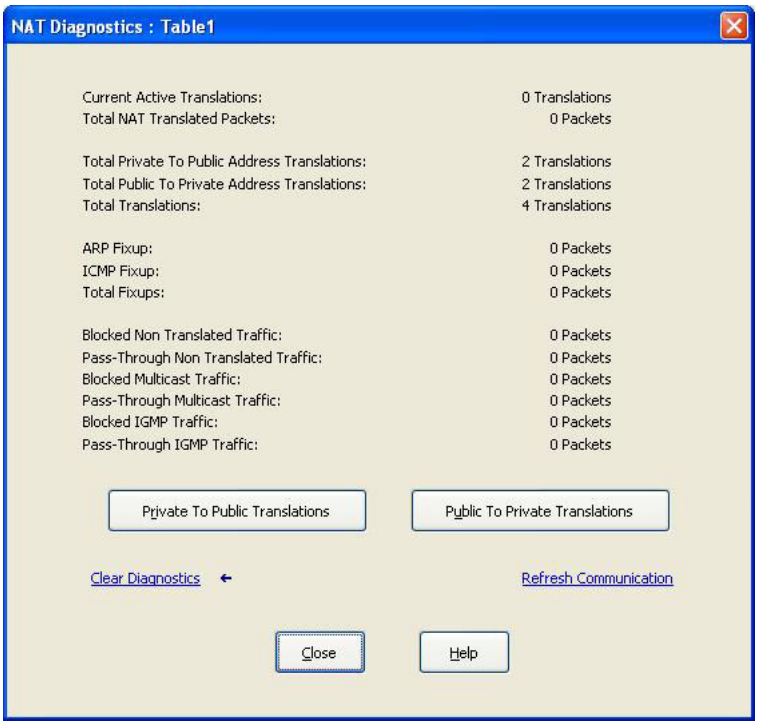


Table 180 - Per Instance Diagnostics

Field	Description
Current Active Translations	The number of translations that have occurred within the last 90 seconds across all NAT instances.
Total NAT Translated Packets	The total number of packets that have been translated for this instance.
Total Private to Public Address Translations	The total number of private-to-public translations for this instance.
Total Public to Private Address Translations	The total number of public-to-private translations for this instance.
ARP Fixup	The number of ARP packets that have been fixed up for this instance.
ICMP Fixup	The number of ICMP packets that have been fixed up for this instance.
Total Fixups	The number of ARP and ICMP packets that have been fixed up for this instance.
Incoming Non Translated Traffic (Pass-Through)	The number of incoming packets with untranslated traffic that NAT passed through for this instance.
Outgoing Non Translated Traffic (Blocked)	The number of outgoing packets with untranslated traffic that NAT blocked for this instance.
Incoming Multicast Traffic (Blocked)	The number of incoming packets with multicast traffic that NAT blocked for this instance.
Outgoing Multicast Traffic (Pass-Through)	The number of outgoing packets of multicast traffic that NAT passed through for this instance.
Incoming IGMP Traffic (Blocked)	The number of incoming packets with IGMP traffic that NAT blocked for this instance.
Outgoing IGMP Traffic (Blocked)	The number of outgoing packets with IGMP traffic that NAT blocked for this instance.
Private to Public Translations	Click to view private-to-public translations that have changed within the last 90 seconds. See Table 181.
Public to Private Translations	Click to view public-to-private translations that have changed within the last 90 seconds. See Table 182.

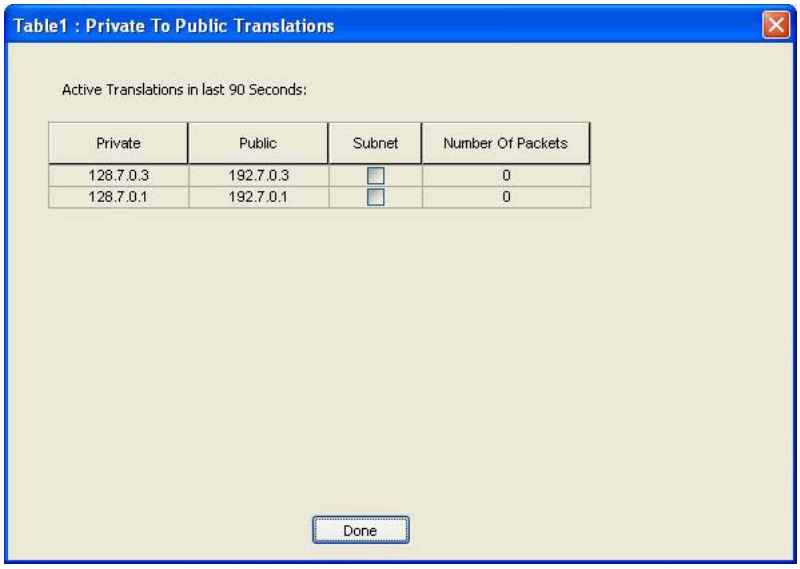


Table 181 - Private-to-Public Translations

Field	Description
Private	The existing address for a device on the private subnet.
Public	The 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	The number of packets that contain the translation.

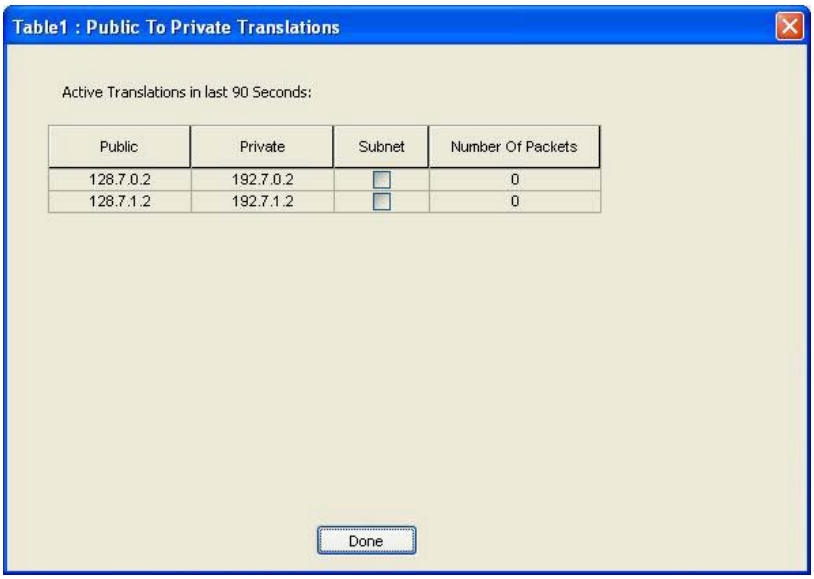


Table 182 - Public-to-Private Translation Diagnostics

Field	Description
Public	The unique IP address on the public subnet that represents the corresponding IP address on the private subnet.
Private	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	The number of packets that contain the translation.

MODBUS (Modicon Communication Bus)

In the WebUI, you can view statistics for the MODBUS TCP server and connections from MODBUS TCP clients.

From the Monitoring menu, choose MODBUS:

- To view server details, see the information on the Server Details tab as described in Table 183.
- To view client details, see the information on the Client Details tab as described in Table 184.
- To reset all counters to zero, click Clear Statistics.

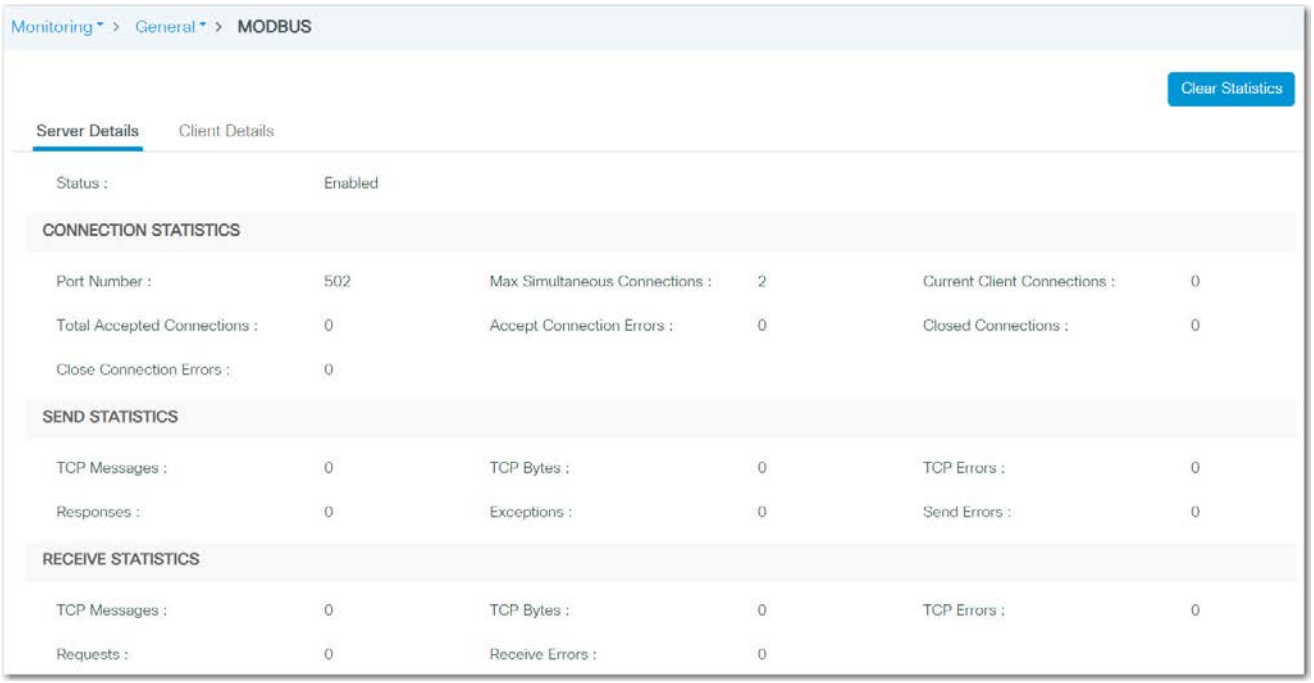


Table 183 - MODBUS—Server Details Tab

Field	Description
Server Details	
Status	Shows whether MODBUS is enabled on the switch as configured on the Administration MODBUS page.
CONNECTION STATISTICS	
Port Number	The MODBUS TCP server port number as configured on the Administration MODBUS page. Valid values: 1...65535 Default value: 502
Max Simultaneous Conncections	Maximum number of simultaneous connection requests sent to the switch, configured on the Administration MODBUS page. Valid values: 1...5 Default value: 2
Current Client Connections	Number of MODBUS clients currently connected to the MODBUS server.
Total Accepted Connections	Number of MODBUS client connections that the MODBUS server accepted.
Accept Connection Errors	Number of times that the MODBUS server accepted a connection request and an error occurred.
Closed Connections	Number of closed client connections.
Close Connection Errors	Number of times that a connection was closed and an error occurred.
SEND STATISTICS	
TCP Messages	Number of TCP messages sent on the MODBUS TCP server port.
TCP Bytes	Number of TCP bytes sent on the MODBUS TCP server port.
TCP Errors	Number of TCP errors in packets sent on the MODBUS TCP server port.
Responses	Number of responses sent on the MODBUS TCP server port.
Exceptions	Number of MODBUS Exceptions reponses on the MODBUS TCP server port.
Send Errors	Number of send errors on the MODBUS TCP server port.
RECEIVE STATISTICS	

Table 183 - MODBUS—Server Details Tab (Continued)

Field	Description
TCP Messages	Number of TCP messages received on the MODBUS TCP server port.
TCP Bytes	Number of TCP bytes received on the MODBUS TCP server port.
TCP Errors	Number of TCP errors in packets received on the MODBUS TCP server port.
Requests	Number of requests received on the MODBUS TCP server port.
Receive Errors	Number of receive errors on the MODBUS TCP server port.
Client Details	Indicates the amount of client connections to the server.

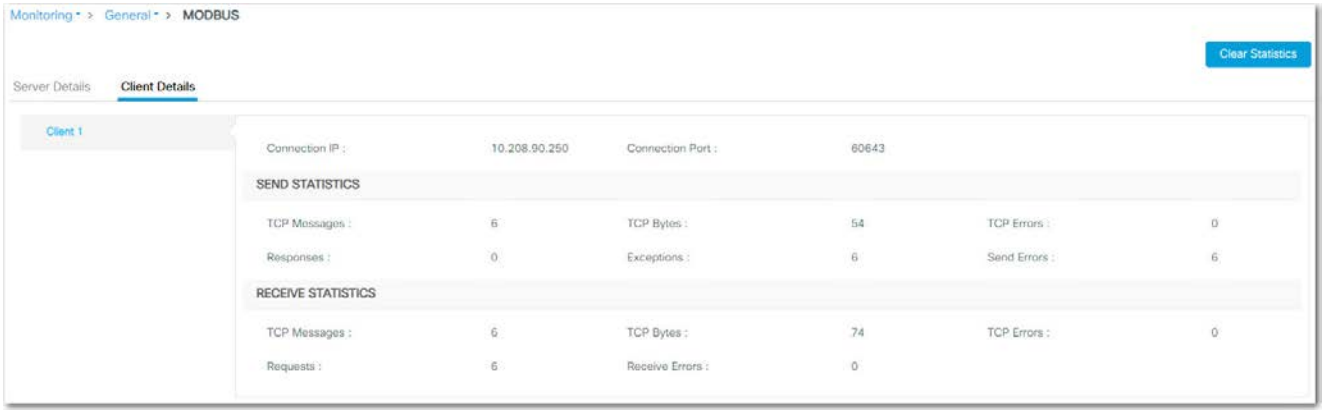


Table 184 - Monitor MODBUS—Client Details Tab

Field	Description
Client Details	
Connection IP	IP adddress of the MODBUS TCP client.
Connection Port	Port number of MODBUS TCP client.
SEND STATISTICS	
TCP Messages	Number of TCP messages sent to the MODBUS TCP client.
TCP Bytes	Number of TCP bytes sent to the MODBUS TCP client.
TCP Errors	Number of TCP errors in packets sent to the MODBUS TCP client.
Responses	Number of responses sent to the MODBUS TCP client.
Exceptions	Number of MODBUS Exception responses sent to the MODBUS TCP client.
Send Errors	Number of errors when sending messages to the MODBUS TCP client.

Table 184 - Monitor MODBUS—Client Details Tab (Continued)

Field	Description
RECEIVE STATISTICS	
TCP Messages	Number of TCP messages received from the MODBUS TCP client.
TCP Bytes	Number of TCP bytes received from the MODBUS TCP client.
TCP Errors	Number of TCP errors in packets received from the MODBUS TCP client.
Requests	Number of requests received from the MODBUS TCP client.
Receive Errors	Number of errors when receiving messages from the MODBUS TCP client.

Media Redundancy Protocol (MRP)

Use the Monitoring > General > MRP page to view information and status of the MRP rings configured on the system.The ring port status indicators are defined in Table 185.

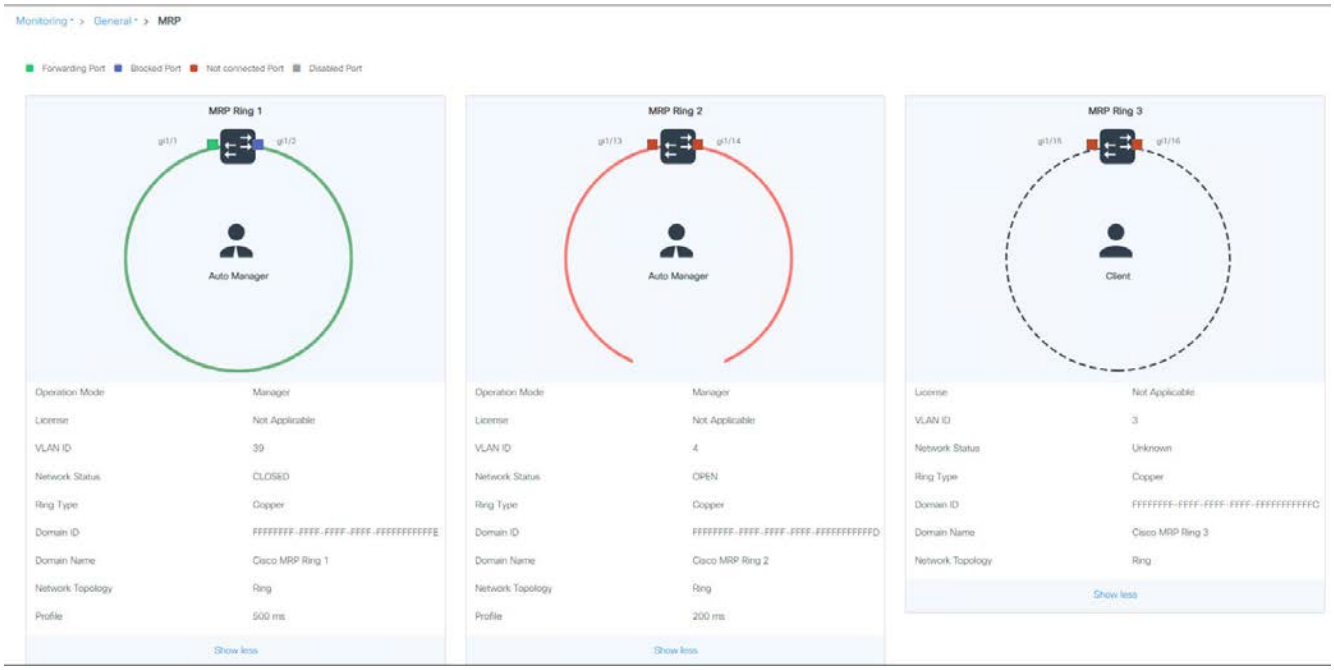


Table 185 - MRP Ring Status Port

Status	Description
Green	Forwarding Port: Ring ports forward all received frames.
Blue	Blocked Port: Ring ports drop all received frames except MRP control frames and some standard frames, for example, LLDP.
Red	Not Connected Port: The link is physically down or disconnected. (This state differs from the Disabled state, in which the MRP Port is manually disabled through software.)
Gray	Disabled Port: Ring ports drop all received frames.

The ring states, indicated by the ring colors, are shown in table Table 186.

Table 186 - MRP Ring States

Status	Description
Black dashed line	MRP not operational.
Green solid line	Ring-Closed (normal operation).
Red open line	Ring-Open (error condition due to link failure or power loss in any other device in the ring).

Table 187 - MRP Parameters

Parameter	Description
Operation Mode	The mode of the MRP ring member: • Manager • Client
License	Not applicable
VLAN ID	VLAN for sending MRP frames
Network Status	The state of the ring: • OPEN: In the case of failure of a link connecting two Media Redundancy Clients (MRCs), both ring ports of the MRP Media Redundancy Manager (MRM) change to the forwarding state, the MRCs adjacent to the failure have a blocked and a forwarding ring port, and the other MRCs have both ring ports forwarding. • CLOSED: During normal operation, the network operates in the Ring-Closed state. To prevent a loop, one of the MRM ring ports is blocked, while the other port is forwarding. Most of the time, both ring ports of all MRCs are in the forwarding state. • UNKNOWN
Ring Type	Physical media type
Domain ID	A unique ID that represents the MRP ring.
Domain Name	Logical name of the configured MRP domain ID.
Network Topology	Ring
Profile	Ring recovery time profile: 30, 200, or 500 milliseconds (ms).

Ports

You can monitor the ports on the switch both in the WebUI and the Logix Designer application.

Monitor Ports via the WebUI

From the Monitoring menu, choose Ports:

- To view port connection status, the VLAN associated with each port, and the bits per second received and transmitted on each port, see the fields on the Ports page described in Table 188.
- To view more details for a specific port, click the port in the grid to display the Ports page. See Table 189.

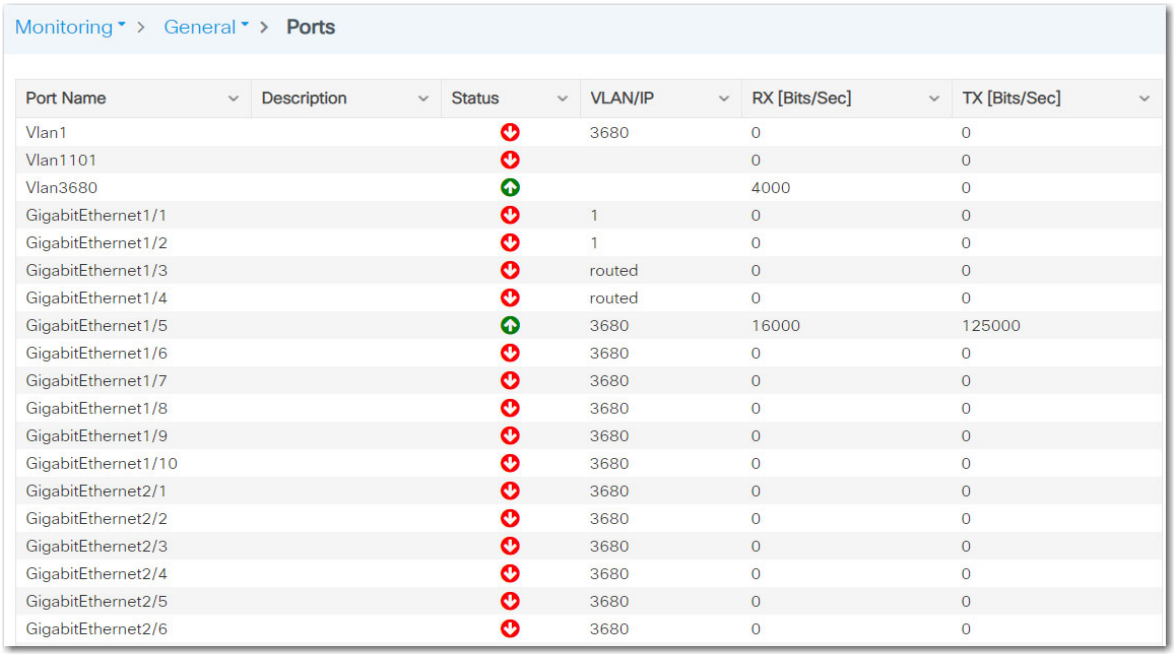


Table 188 - Ports

Field	Description
Port Name	The port type and number.
Description	The description associated with the port.
Status	The connection status of the port.
VLAN/IP	The VLAN ID or the IP address that is associated with the port.
RX [Bits/Sec]	The received bits per second.
TX [Bits/Sec]	The transmitted bits per second.

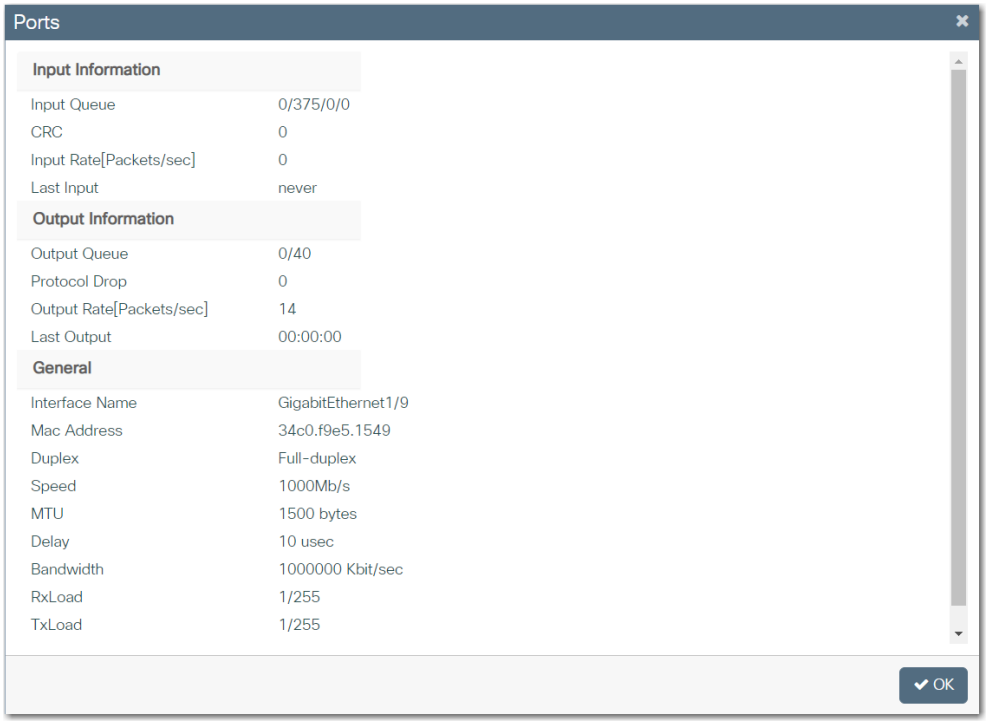


Table 189 - Ports

Field	Description
Input Information	
Input Queue	Information about packets in the input queue (size/max/drops/flushes). **EXAMPLE:** 30/75/187/0 In this example, 30 packets are in the input queue. The queue depth is 75 packets and there have been 187 drops since the interface counters were last cleared.
CRC	The cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Input Rate [Packets/sec]	The number of packets received per second for the port.
Last Input	The number of hours, minutes, and seconds since the last packet was successfully received by the port. This is useful for knowing when the port failed.
Output Information	
Output Queue	Information about packets in the output queue (size/max total/threshold/drops). **EXAMPLE:** 0/1000/64/0 In this example, 0 packets are in the output queue. The queue depth is 1000 packets and there have been 64 drops since the interface counters were last cleared.
Protocol Drop	The number of packets dropped by the port due to a full queue.
Output Rate [Packets/sec]	The number of packets output per second for the port.
Last Output	The number of hours, minutes, and seconds since the last packet was successfully transmitted by the port.
General	
Interface Name	The type and number of the port.
Mac Address	The Ethernet address of the port.

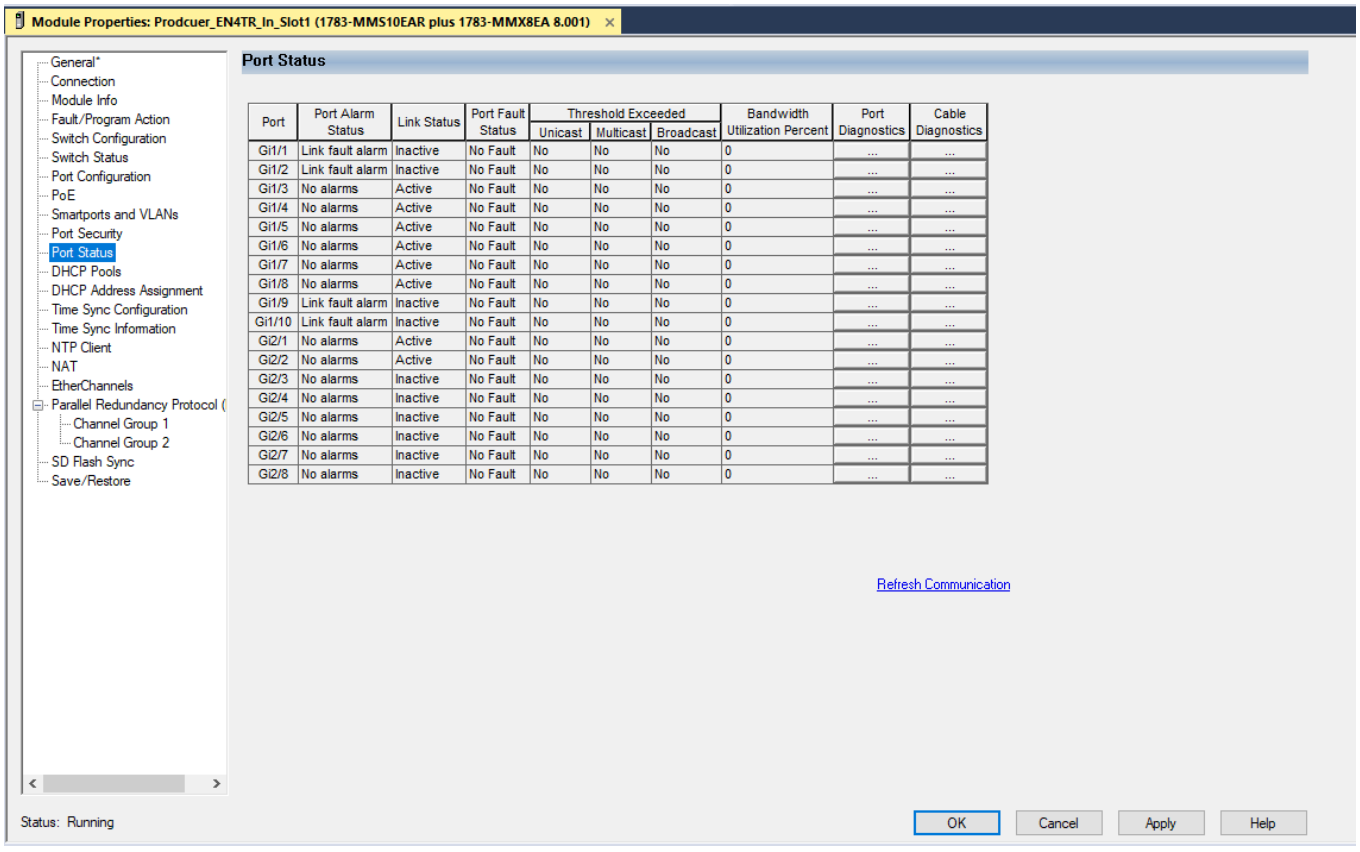
Table 189 - Ports (Continued)

Field	Description
Duplex	The duplex mode of the port.
Speed	The speed of the port.
MTU	The maximum transmission unit set for the port in bytes.
Delay	The delay of the port in microseconds. Higher-level protocols can use delay information to make operating decisions. For example, IGRP can use delay information to differentiate between a satellite link and a land link.
Bandwidth	The bandwidth of the port in kilobits per second.
RxLoad	The amount of traffic being received on the port. RxLoad is a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
TxLoad	The amount of traffic being sent from the port. TxLoad is a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Reliability	The reliability of the port as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.

Monitor Port Status via the Logix Designer Application

In the Logix Designer application, you can monitor alarms, statuses, thresholds, and bandwidth utilization for each switch port. You can also access port and cable diagnostics.

From the navigation pane, click Port Status.



Port	Port Alarm Status	Link Status	Port Fault Status	Threshold Exceeded			Bandwidth Utilization Percent	Port Diagnostics	Cable Diagnostics
				Unicast	Multicast	Broadcast			
Gi1/1	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Gi1/2	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Gi1/3	No alarms	Active	No Fault	No	No	No	0	...	...
Gi1/4	No alarms	Active	No Fault	No	No	No	0	...	...
Gi1/5	No alarms	Active	No Fault	No	No	No	0	...	...
Gi1/6	No alarms	Active	No Fault	No	No	No	0	...	...
Gi1/7	No alarms	Active	No Fault	No	No	No	0	...	...
Gi1/8	No alarms	Active	No Fault	No	No	No	0	...	...
Gi1/9	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Gi1/10	Link fault alarm	Inactive	No Fault	No	No	No	0	...	...
Gi2/1	No alarms	Active	No Fault	No	No	No	0	...	...
Gi2/2	No alarms	Active	No Fault	No	No	No	0	...	...
Gi2/3	No alarms	Inactive	No Fault	No	No	No	0	...	...
Gi2/4	No alarms	Inactive	No Fault	No	No	No	0	...	...
Gi2/5	No alarms	Inactive	No Fault	No	No	No	0	...	...
Gi2/6	No alarms	Inactive	No Fault	No	No	No	0	...	...
Gi2/7	No alarms	Inactive	No Fault	No	No	No	0	...	...
Gi2/8	No alarms	Inactive	No Fault	No	No	No	0	...	...

Table 190 - Port Status

Field	Description
Port	The port type and number.
Port Alarm Status	The status of the port alarm: • Link fault alarm • Port not forwarding alarm • Port not operating alarm • High bit error rate alarm • No alarms
Link Status	The status of the port: • Active • Inactive
Port Fault Status	The fault status of the port: • Error - Disable event • SFP error - Disabled • CDP native VLAN mismatch • MAC address flap • Port security violation • No fault
Threshold Exceeded	Indicates whether the threshold value has been exceeded for these traffic types: • 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.
Bandwidth Utilization Percent	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.
Cable Diagnostics	Click to display information to diagnose a cable issue for the corresponding port.

PROFINET

Use the Monitoring > General > PROFINET page to display information and statistics for PROFINET.

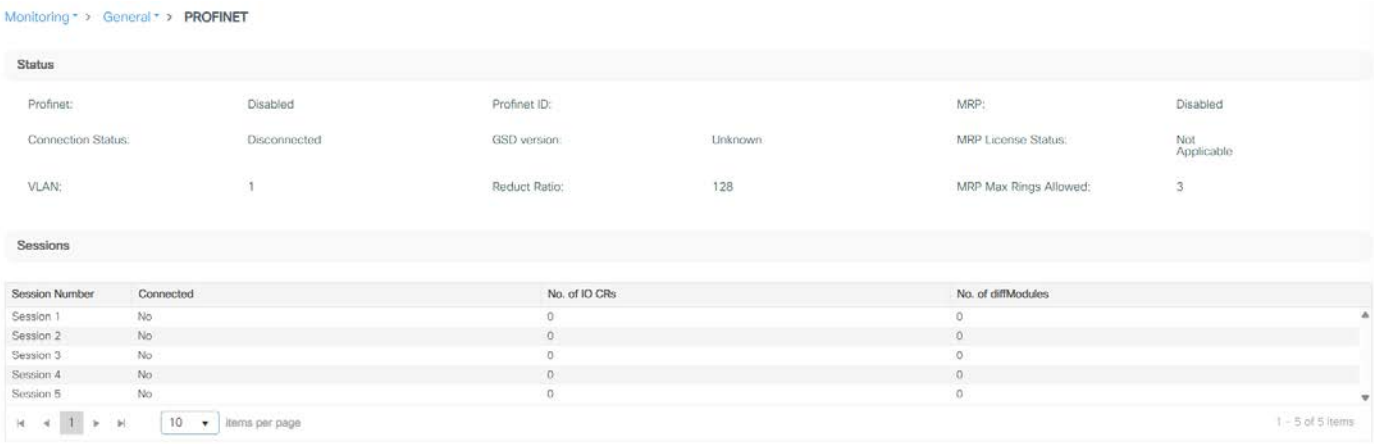


Table 191 - PROFINET Status Parameters

Parameter	Description
Profinet	Shows whether PROFINET is enabled or disabled on the switch.
Connection Status	Shows whether the switch is connected to the PROFINET PLC (I/O Controller).
VLAN	The VLAN number for PROFINET traffic.
Profinet ID	PROFINET device identifier.
GSD Version	Shows whether the General Station Description (GSD) file for the switch matches the GSD file in the controller configuration software.
Reduct Ratio	Reduction Ratio denotes the rate at which the real time (RT) packets are exchanged between controller and the IO devices. By default, the value is set to 128 ms. This denotes that the transmit and receive occurs at every 128th send clock. Other values like 256 and 512 can also be configured from the TIA tool.
MRP	Shows whether MRP is enabled or disabled.
MRP License Status	Shows whether the MRP license is active.
MRP Max Rings Allowed	The maximum number of MRP rings that can be configured based on the license.

Table 192 - PROFINET Session Parameters

Parameter	Description
Session Number	Number of the PROFINET session.
Connected	Shows whether the session is currently connected.
No. of IO CRs	Number of IO Communication Relationships (CRs) for the session.
No. of diffModules	A value greater than zero means that there is a difference in expected (configured from TIA) and the actual submodules in the device. This number denotes the count of the differences. The presence of diffmoduleblocks in the response shows the details of missing or additional submodules in the device from the ones configured.

Parallel Redundancy Protocol (PRP)

You can monitor PRP statistics in both the WebUI and the Logix Designer application.

Monitor PRP via the WebUI

From the Monitoring menu, choose PRP, and then click the VDAN, Node, and Statistics tabs to view statistics for each type of connected device.

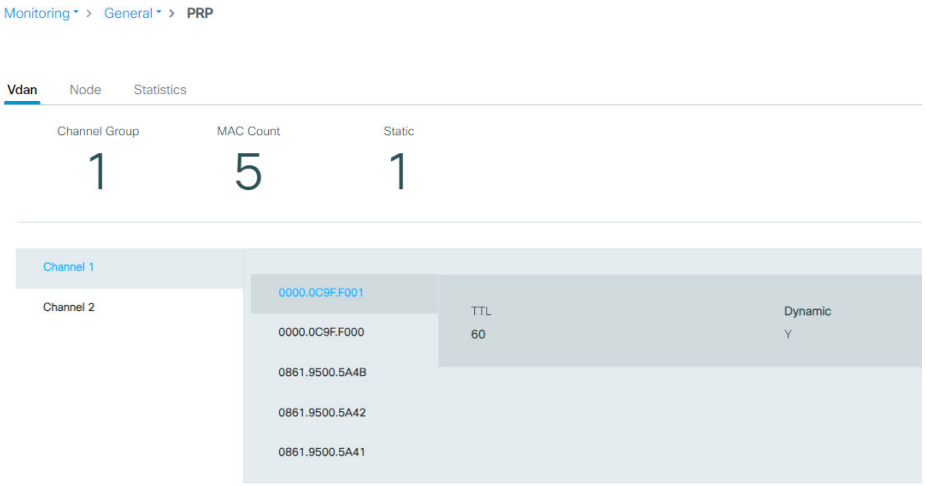


Table 193 - Monitor PRP—VDAN Tab

Field	Description
Channel Group	The channel group selected on the page.
MAC Count	The total number of static and dynamic MAC addresses for the channel group.
Static	The total number of static entries for the channel group.
Channel 1, Channel 2	Click Channel 1 or Channel 2 (Stratix 5800 Switch Only) to display VDAN table entries for the selected channel group.
TTL	The amount of time before the selected dynamic MAC address expires.
Dynamic	Indicates whether the selected MAC address is a dynamic or static entry: Y—The entry is dynamic. N—The entry is static.

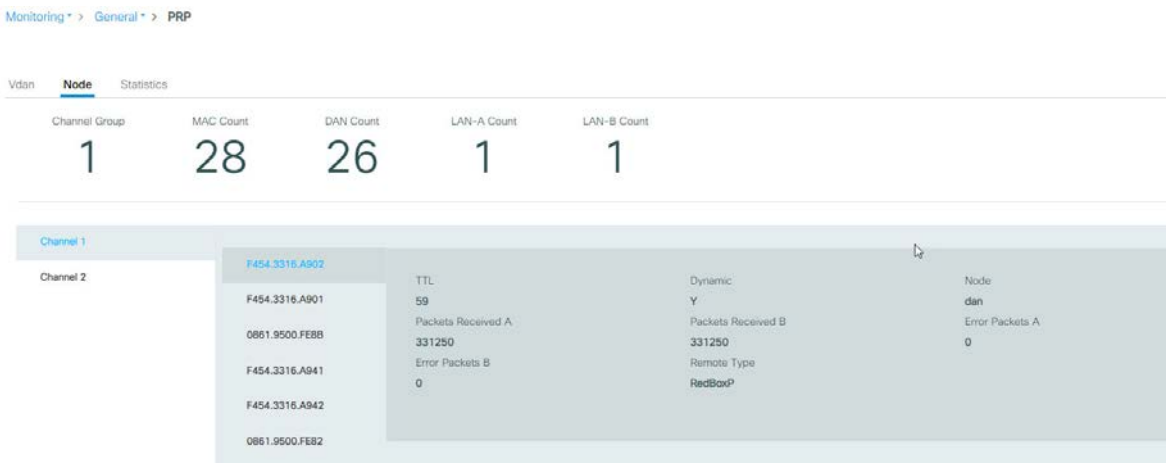


Table 194 - Monitor PRP—Node Tab

Field	Description
Channel Group	The channel group number.
MAC Count	The total number of static and dynamic MAC addresses for the channel group.
DAN Count	The total number of DAN MAC addresses for the channel group.
LAN-A Count	The total number of SANs on LAN A.
LAN-B Count	The total number of SANs on LAN B.
Channel 1, Channel 2	Click Channel 1 or Channel 2 to display Node table entries for the selected channel group.
TTL	The amount of time before the selected MAC address expires.
Dynamic	Indicates whether the selected MAC address is a dynamic or static entry: • Y—The entry is dynamic. • N—The entry is static.
Node	The type of PRP node: • DAN—Double attached node • SAN-A—Single attached node on LAN A • SAN-B—Single attached node on LAN B
Packets Received A	The number of packets received on LAN A.
Packets Received B	The number of packets received on LAN B.
Error Packets A	The number of packets received on LAN A having the wrong LAN A destination.
Error Packets B	The number of packets received on LAN B having the wrong LAN B destination.

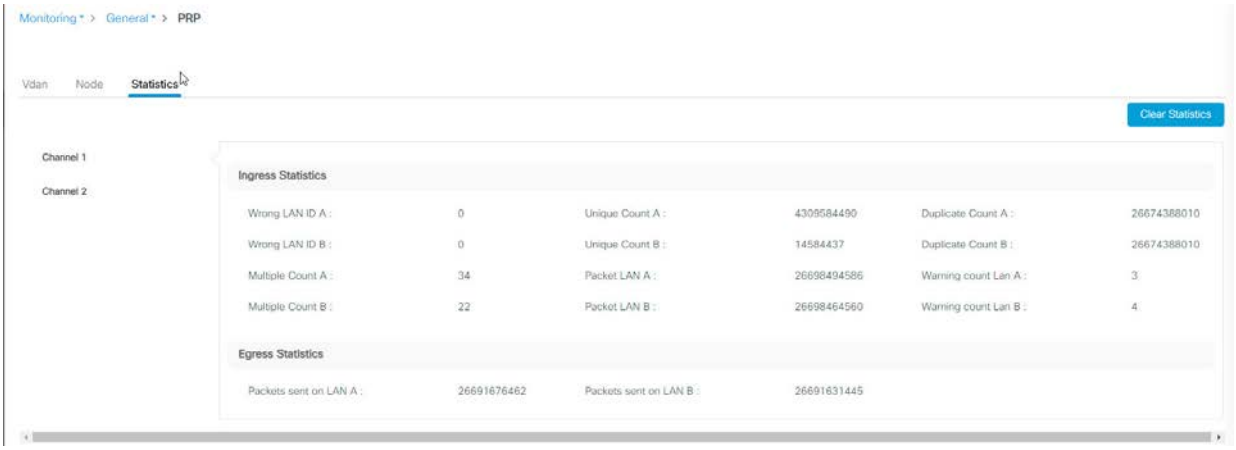


Table 195 - Monitor PRP— Statistics Tab

Field	Description
Channel Group	The channel group number.
Ingress Statistics	
Wrong LAN ID A	The number of packets received on LAN A with a LAN B PRP tag.
Wrong LAN ID B	The number of packets received on LAN B with a LAN A PRP tag.
Multiple Count A	The number of entries in the duplicate detection mechanism on Port A for which more than one duplicate was received.
Multiple Count B	The number of entries in the duplicate detection mechanism on Port B for which more than one duplicate was received.
Unique Count A	The number of entries in the duplicate detection mechanism on Port A for which no duplicate was received.
Unique Count B	The number of entries in the duplicate detection mechanism on Port B for which no duplicate was received.
Packet LAN A	The number of packets received on LAN A.
Packet LAN B	The number of packets received on LAN B.
Duplicate Count A	The number of entries in the duplicate detection mechanism on Port A for which on single duplicate was received.
Duplicate Count B	The number of entries in the duplicate detection mechanism on Port B for which on single duplicate was received.
Warning Count LAN A	The number of warnings encountered on LAN A.
Warning Count LAN B	The number of warnings encountered on LAN B.
Egress Statistics	
Packets sent on LAN A	The number of packets sent on LAN A.
Packets sent on LAN B	The number of packets sent on LAN B.

Monitor PRP via the Logix Designer Application

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

- To view the port numbers for each PRP channel group, see the fields as described in Table 196.
- To view statistics for a PRP channel group, click Channel Group 1 or Group 2 in the navigation pane. See Table 197.

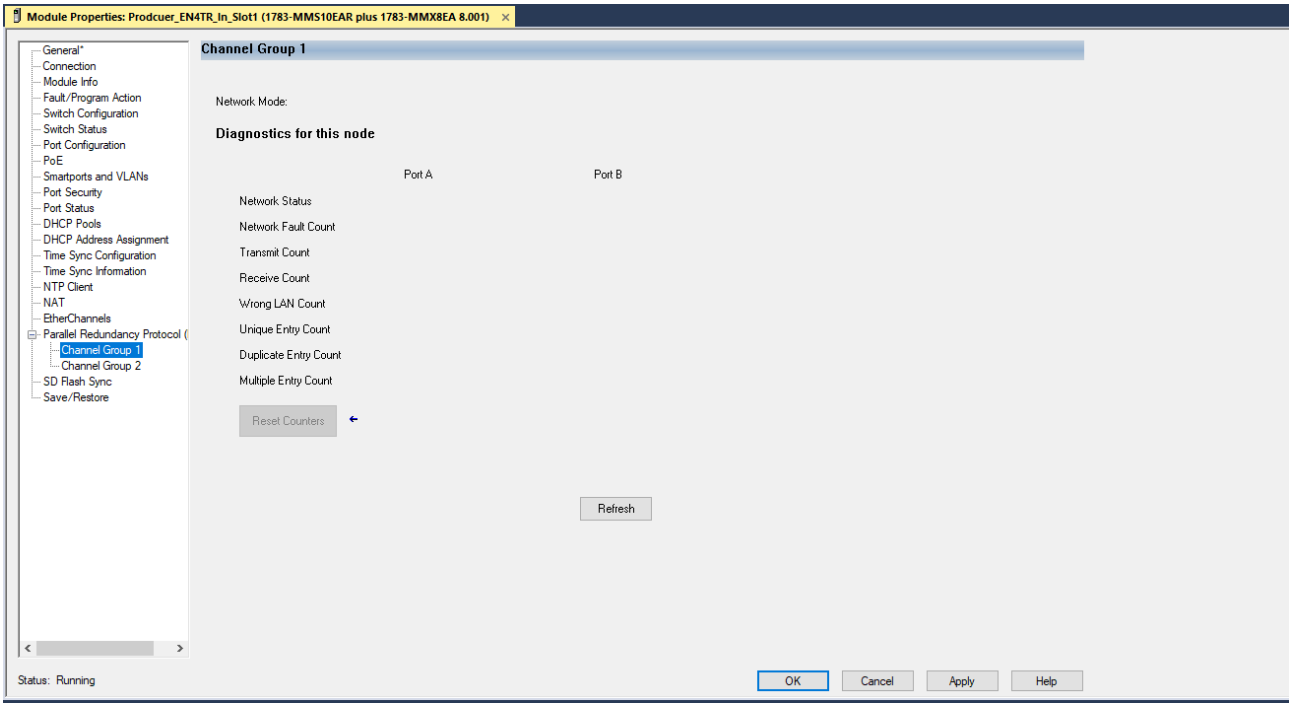


Table 196 - Parallel Redundancy Protocol (PRP)

Field	Description
Channel Group 1	
Port A	The port type and number for channel group 1, port A.
Port B	The port type and number for channel group 1, port B.
Channel Group 2	
Port A	The port type and number for channel group 2, port A.
Port B	The port type and number for channel group 2, port B.

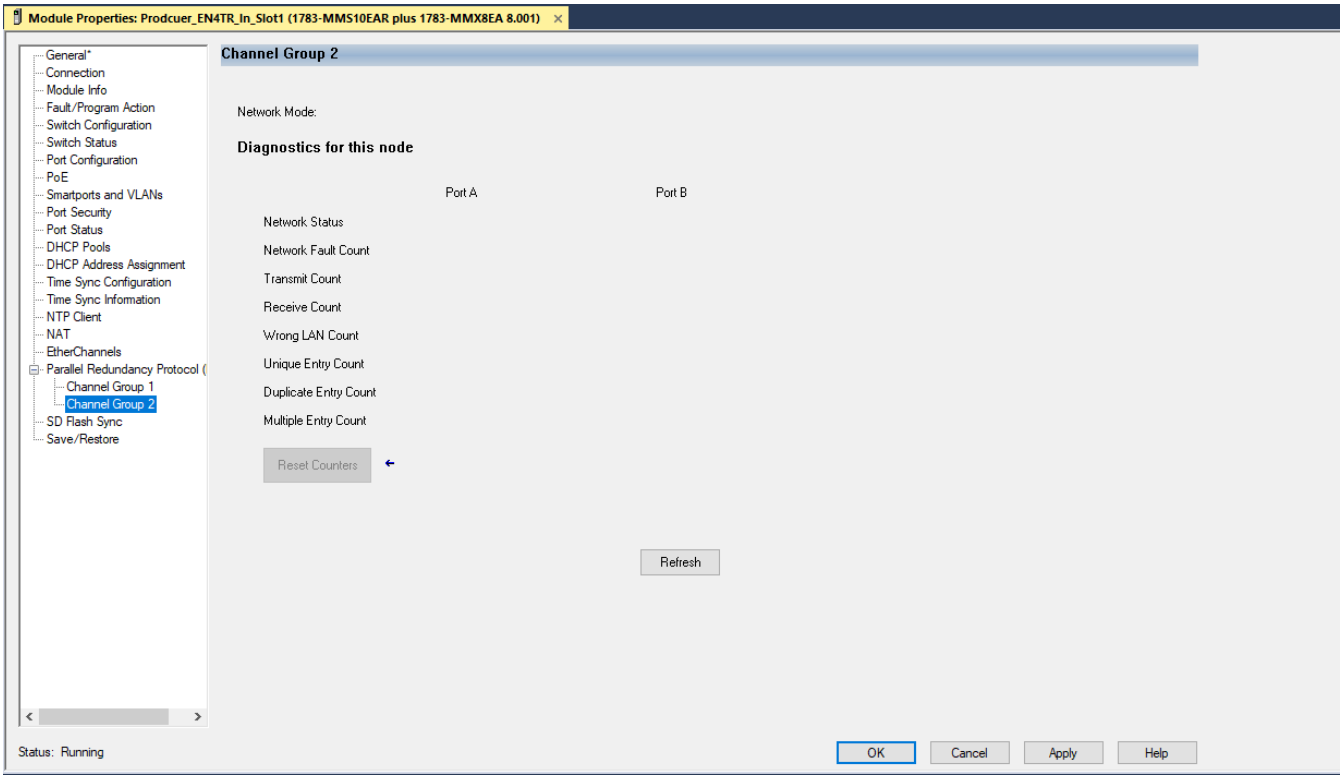


Table 197 - Channel Group

Field	Description
Network Mode	The module is online for a PRP-enabled device.
Diagnostics for this node	
Network Status	The network state of each PRP port on the device: • OK—Indicates that there is no problem with the PRP network. • Fault—Indicates that there is a problem with the PRP network.
Network Fault Count	The number of times the network status for each PRP port changed from OK to Fault since the last counter reset or power cycle.
Transmit Count	The number of PRP-tagged frames transmitted over each PRP port since the last counter reset or power cycle.
Receive Count	The number of PRP-tagged frames received on each PRP port since the last counter reset or power cycle.
Wrong LAN Count	The number of PRP-tagged frames received on the wrong PRP port since the last counter reset or power cycle.
Unique Entry Count	The number of PRP-tagged frames received on one PRP port, but not received on the other PRP port since the last counter reset or power cycle. Usually indicative of a loss of connection or loss of frames on the other PRP port.
Duplicate Entry Count	The number of PRP-tagged frames received on the PRP port that were already received on the other PRP port since the last counter reset or power cycle. **IMPORTANT:** This count increments during normal operation and is not an indication of a fault.
Multiple Entry Count	The number of PRP-tagged frames for which multiple duplicates were received on each PRP port since the last counter reset or power cycle. Usually indicative of a misconfigured network, such as a routing loop.
Reset Counters	Sets the PRP port counter values to zero, and then refreshes the values with the current counter values.

Resiliency Ethernet Protocol (REP)

In the WebUI, you can view the Resilient Ethernet Protocol (REP) topology that is configured on a network segment. You can also view the previously topology of a network segment. When a fault occurs on the segment, the topology dynamically changes.

From the Monitor menu, choose REP:

- To display the current REP topology configured on that segment, from the Segment ID pull-down menu on the Global tab, choose a network segment ID. See Table 198.
- To view the previous topology of a network segment, from the Segment ID pull-down menu on the Archived Topology tab, choose a network segment ID. See Table 199.

Figure 41 - REP Segment

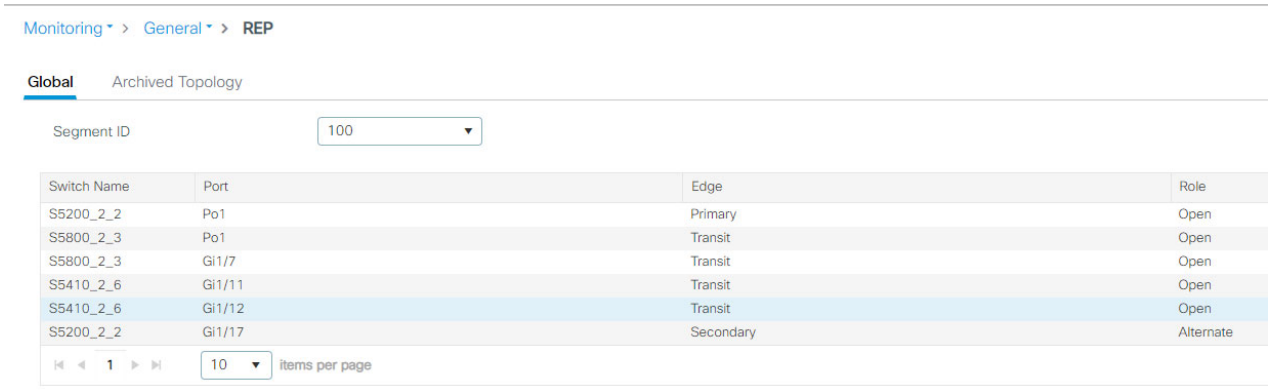


Figure 42 - Broken REP Segment

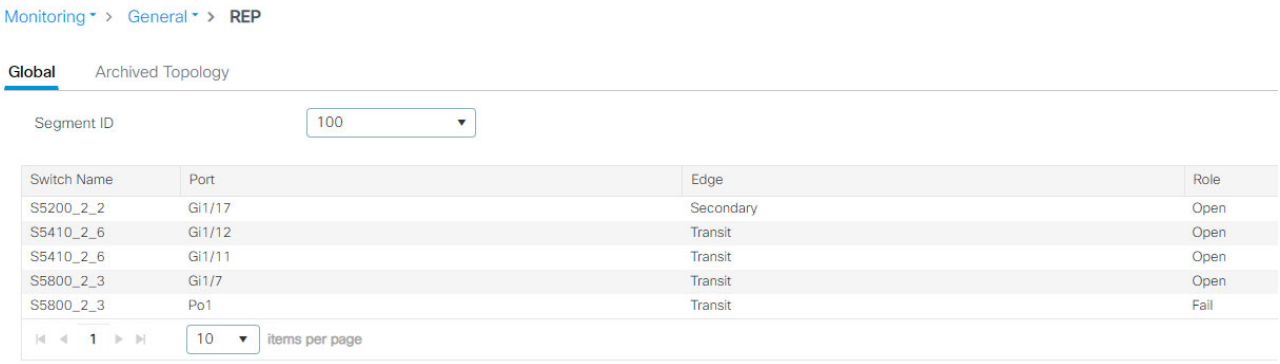


Table 198 - REP—Global Tab

Field	Description
Switch Name	The name of the switch.
Port	The port type and number.
Edge	The REP port type. For a description of REP port types, see Table 84 on page 171.
Role	The role of the REP port: • Open • Alternate • Failed

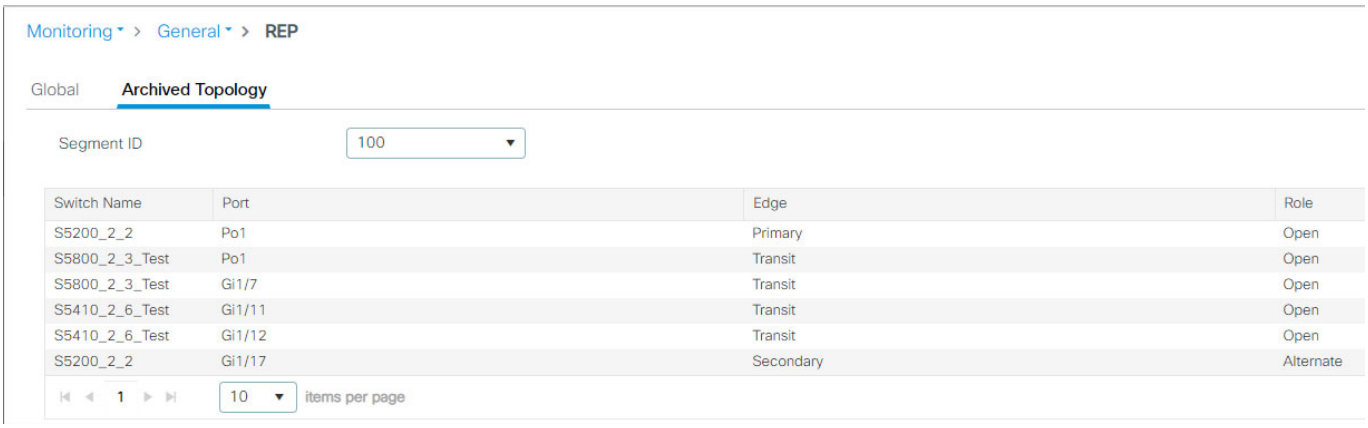


Table 199 - REP—Archived Topology Tab

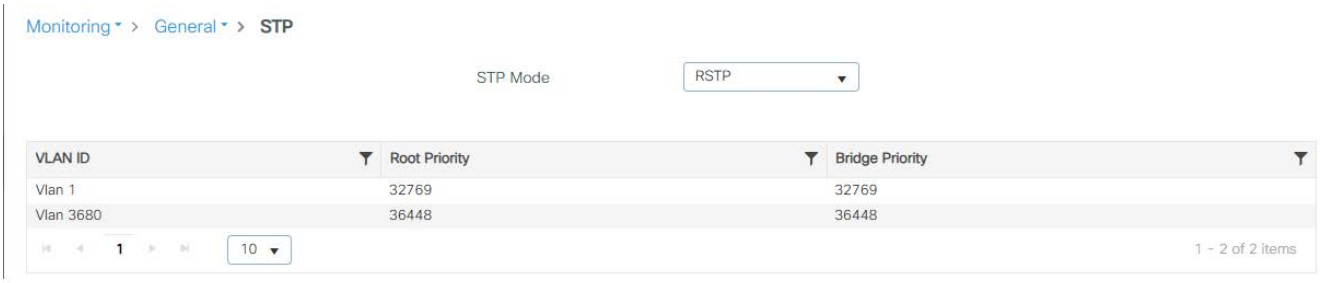
Field	Description
Switch Name	The archived name of the switch.
Port	The archived port type and number.
Edge	The archived REP port type. For a description of REP port types, see Table 84 on page 171.
Role	The archived role of the REP port: • Open • Alternate • Failed

Spanning Tree Protocol (STP)

The Monitoring > General > STP page displays information about Spanning Tree Protocol (STP). To display STP data, select the STP Mode configured on the switch from the pull-down menu:

- Rapid Spanning Tree Protocol (RSTP): Display spanning-tree information for the selected VLAN.
- Multiple Spanning Tree (MST): Display spanning-tree information for an MST instance.

To display RSTP information, click on the VLAN ID in the RSTP table. To display MST information, click the MST instance in the MST table.



Rapid Spanning Tree Protocol (RSTP) Mode

Display spanning-tree information for the selected VLAN.

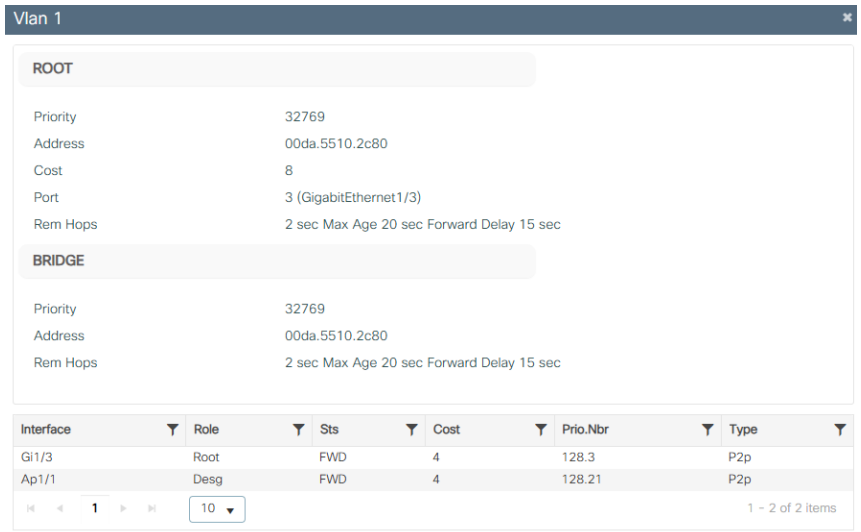


Table 200 - RSTP Mode

Parameter	Description
VLAN ID	The number of the VLAN associated with this spanning tree instance.
ROOT	
Priority	Priority Indicator.
Address	MAC address of the port.
Port	Identifier of the named port.
Cost	Cost associated with the port.
Remaining (Rem) Hops	Number of hops remaining of the maximum hop count (configured value of MaxHops) after each downstream switch decrements the hop count field on reception of Internal Spanning Tree (IST) BPDU.
BRIDGE	
Priority	Priority Indicator.
Address	MAC address of the port.

Table 200 - RSTP Mode

Parameter	Description
Remaining (Rem) Hops	Number of hops remaining of the maximum hop count (configured value of MaxHops) after each downstream switch decrements the hop count field on reception of Internal Spanning Tree (IST) BPDU.
Interface	Interface type and number of the port.
Role	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 receives 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	Cost associated with the port.
Prio.Nbr	The local port priority and port ID.
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.

System

In the WebUI, you can monitor hardware details, memory utilization, and CPU utilization.

From the Monitoring menu, choose System.

Inventory

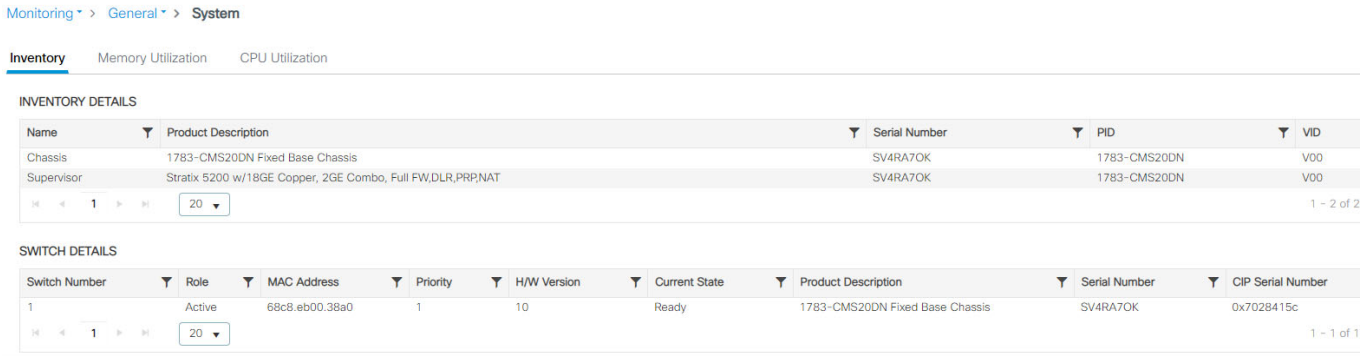


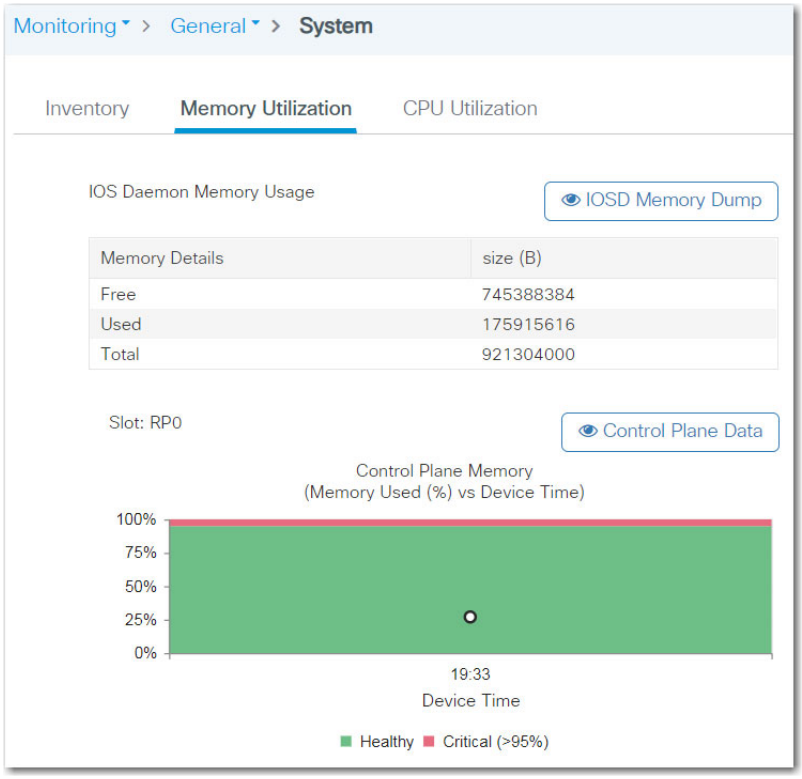
Table 201 - System—Inventory Tab

Field	Description
Inventory Details	
Name	The type of hardware product.
Product Description	The description of the hardware product.
Serial Number	The serial number of the hardware product.
PID	The catalog number of the hardware product.
VID	The version of the hardware product.
Switch Details	
Switch Number	The number of the switch in a stacked environment. The Stratix 5800 switch platform does not currently support stacking, so the switch number is always 1.
Role	The current role of the switch in a stacked environment: • Active • Member
MAC Address	The MAC address of the switch.
Priority	The priority of the switch from 1...15. The default priority value is 1.
H/W Version	The hardware version number associated with the switch. Different device models can have the same hardware version, provided they support the same system-level features.
Current State	The current state of the switch in a stacked environment: • Ready—The switch is fully operational. • Progressing—The stack master is communicating with the new switch joining the stack. • Provisioned—When a switch that previously joined a stack is removed, the port numbers remain in the running configuration, and the missing device has a state of a Provisioned. The Provisioned state is caused by a switch that is no longer connected to the stack. • v-mismatch—When a new switch that is in Installed mode tries to join the stack that is in Bundled Boot mode, the new switch has a state of v-mismatch. Auto-upgrade is supported in installed mode only. • Lic-mismatch—When there is a license mismatch. The Stratix 5800 switch platform does not currently support stacking, so the current state is always Ready.
Product Description	The switch model description.
Serial Number	The serial number of the switch.
CIP Serial Number	The CIP serial number of the switch.

Memory Utilization

The Memory Utilization tab shows the used, free, and total memory on the IOS daemon:

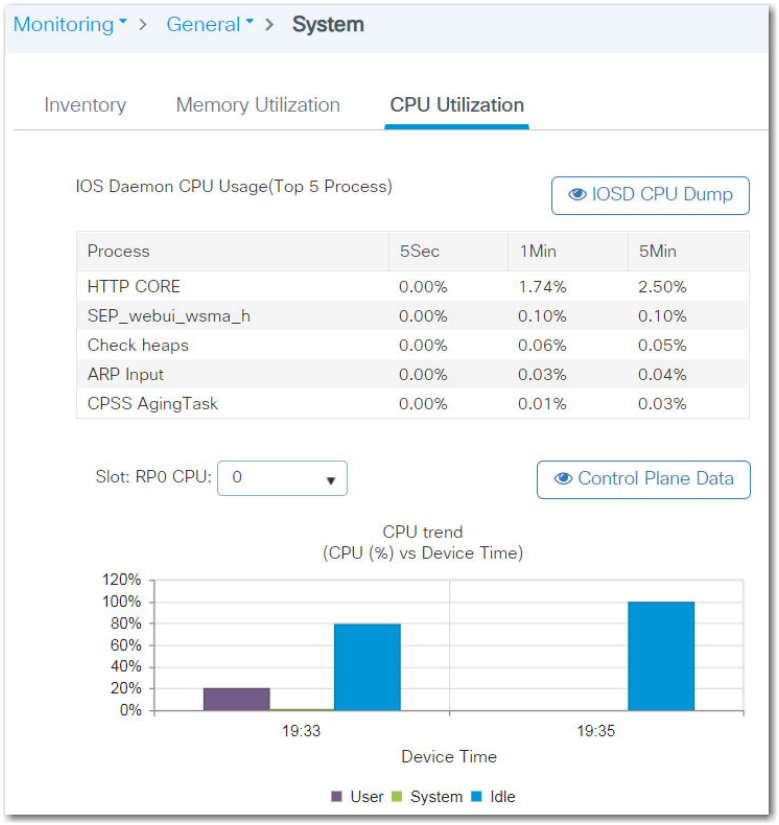
- To export memory data to a spreadsheet, click IOSD Memory Dump and then click Export to Excel.
- To export control plane memory data as a PDF, click Control Plane Data and then click Export as PDF.



CPU Utilization

The CPU Utilization tab shows the CPU utilization of the top five processes over the last 5 seconds, 1 minute, and 5 minutes.

- To export the CPU utilization data to a spreadsheet, click IOSD CPU Dump and then click Export to Excel.
- To export control plane CPU data as a PDF, click Control Plane Data and then click Export as PDF.



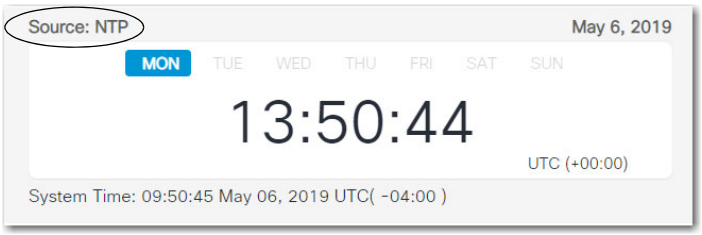
Time

PTP

In the WebUI, you can monitor time details for the time source that is configured on the switch.

From the Monitor menu, choose Time and PTP.

The clock at the top of the page shows the local time and the time source. The time source indicates where the switch is receiving its time, such as from an NTP server, PTP, or the local computer.



PTP Details

PTP Details shows the properties of the local PTP clock and the clock identity.

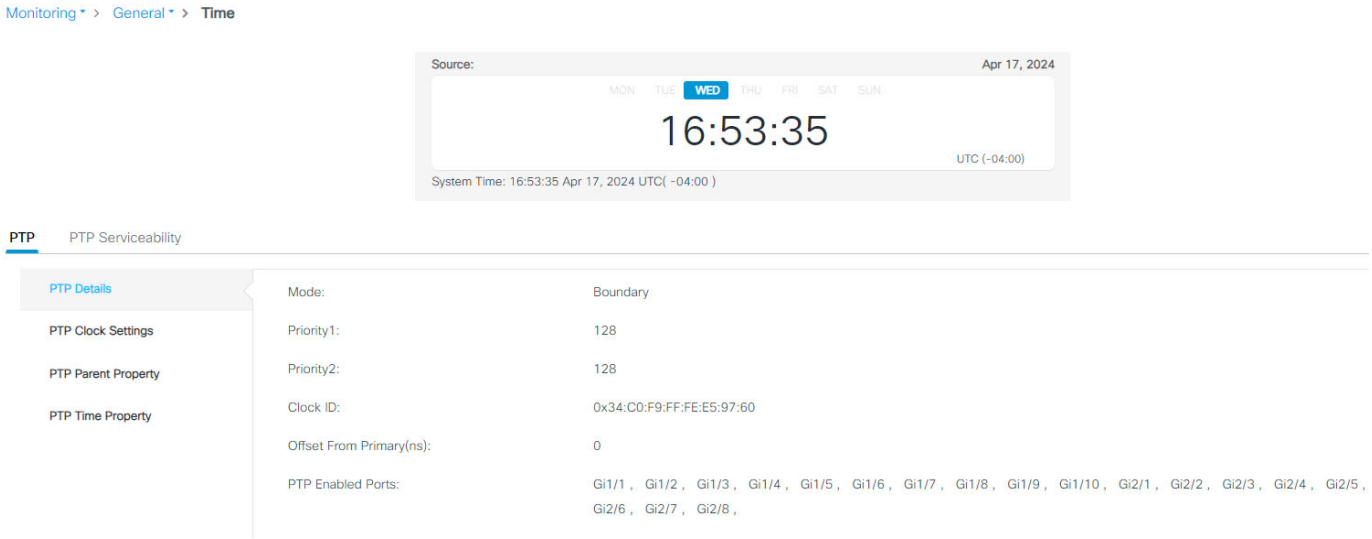


Table 202 - Monitor Time—PTP Details

Field	Description
Mode	The PTP mode configured for the switch: • Forward • Boundary • End to End Transparent • GMC-BC (NTP-PTP Clock)
Priority 1	(Appears only for Boundary and NTP-PTP mode). Priority 1 preference value of the PTP clock. The priority1 clock is considered first during clock selection.
Priority 2	(Appears only for Boundary and NTP-PTP mode). Priority 2 preference value of the PTP clock. The priority2 clock is considered after all other clock sources during clock selection.
Clock ID	(Appears only for Boundary and NTP-PTP mode). The unique clock identity.
Offset From Primary (ns)	Time offset between the time recipient and time source clocks.
PTP Enabled Ports	(Appears only for Boundary and End to End Transparent modes). The list of ports that are assigned to the PTP clock.

PTP Clock Settings

PTP Clock Settings shows the settings of the local PTP clock when PTP is in Boundary and End to End Transparent mode.

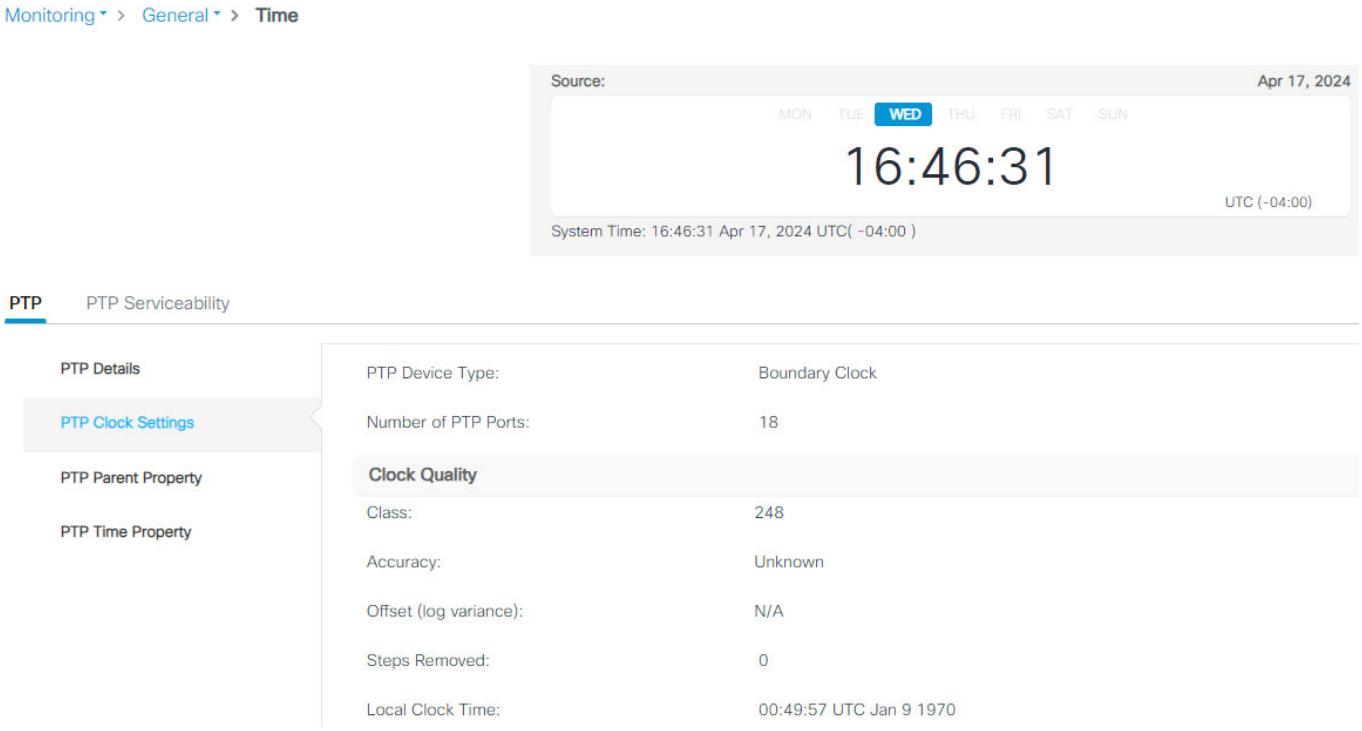


Table 203 - Monitor Time—PTP Clock Settings

Field	Description
PTP Device Type	The PTP clock type as is determined by the PTP mode configured on the switch. • Forward Clock • Boundary Clock • End to End Transparent Clock • GMC-BC (NTP-PTP Clock)
Number of PTP Ports	The number of ports that are assigned to the PTP clock.
Class	(Appears only for Boundary and NTP-PTP clock type). The time and frequency traceability of the Grandmaster clock.
Accuracy	(Appears only for Boundary and NTP-PTP clock type.) This applies only when the Best Master Clock algorithm is in use.) This is an enumerated list of ranges of accuracy to UTC.
Offset (log variance)	(Appears only for Boundary and NTP-PTP clock type). The offset between the Grandmaster clock and the parent clock.
Steps Removed	The number of hops from the local clock to the Grandmaster clock.
Local Clock Time	The time of the local PTP clock.

PTP Parent Property

PTP Parent Property shows the properties of the PTP parent clock when PTP is in Boundary and NTP-PTP mode.

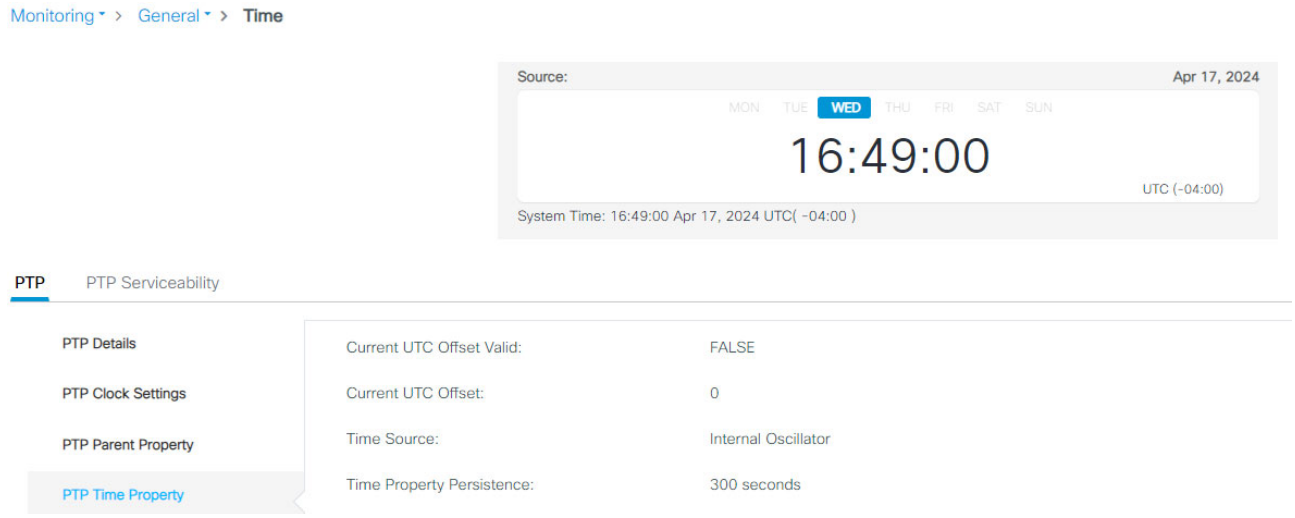


Table 204 - Monitor Time—PTP Parent Property

Field	Description
Parent Clock	The clock to which the member-slave clocks synchronize.
Parent Clock Identity	The unique parent clock identity.
Parent Port Number	The clock port ID of the parent port.
Grandmaster Clock	The root of the master-slave clock hierarchy.
Grandmaster Clock Identity	The unique Grandmaster clock identity.

PTP Time Property

PTP Time Property shows PTP clock-time properties for the PTP device.

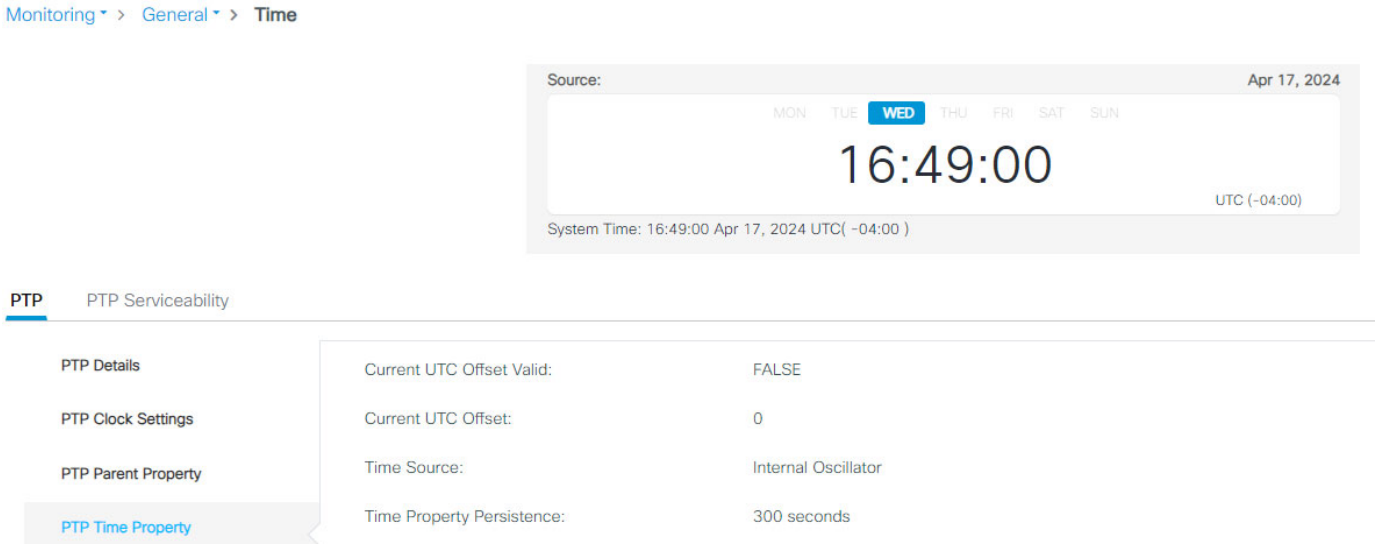


Table 205 - PTP Time Property

Field	Description
Current UTC Offset Valid	Indicates whether the current Coordinated Universal Time (UTC) offset is valid.
Current UTC Offset	Offset between the International Atomic Time (TAI) and UTC in seconds.
Time Source	Time source used by the Grandmaster clock.
Time Property Persistence	The number of seconds that time properties are preserved after a primary Grandmaster clock fails and a secondary Grandmaster clock takes over.

PTP Serviceability

The PTP Serviceability page displays PTP statistics and information. PTP statistics can help you troubleshoot and monitor the performance of PTP in the network.

From the Monitor menu, choose Time and PTP Serviceability.

Messages

Messages display counter information for the PTP messages that are sent and received.

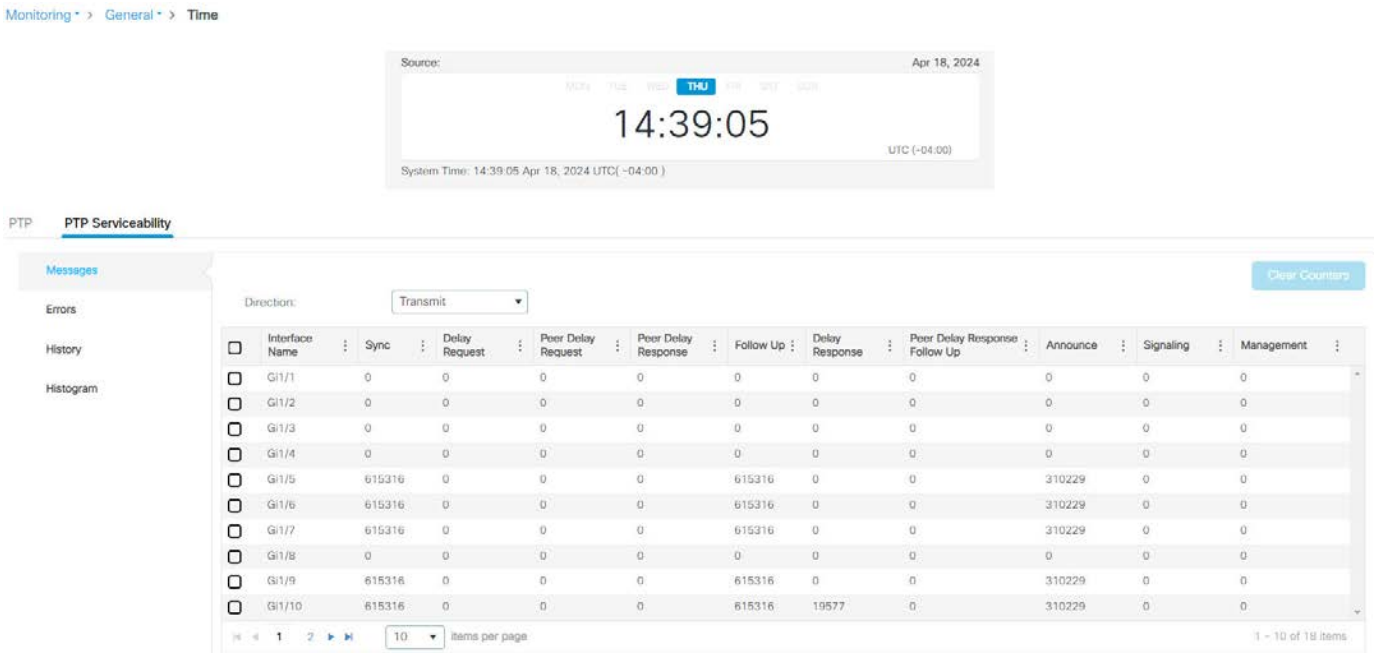


Table 206 - PTP Serviceability Messages

Field	Description
Interface Name	The port type and number.
Sync	Event message tagged with a timestamp when data packets reach or leave a port and 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.
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.
Follow Up	General message (not tagged with a timestamp) 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 Response Follow Up	General message (not tagged with a timestamp) used to measure the link delay in transparent clocks.

Table 206 - PTP Serviceability Messages

Field	Description
Announce	General message (not tagged with a timestamp) used to establish a time source-time recipient hierarchy.
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 that are used to manage clocks.

Errors

The errors tab displays counter information for the PTP errors that occurred on the various ports. PTP errors are categorized as field mismatch errors, unexpected messages, duplicate messages, and generic errors.

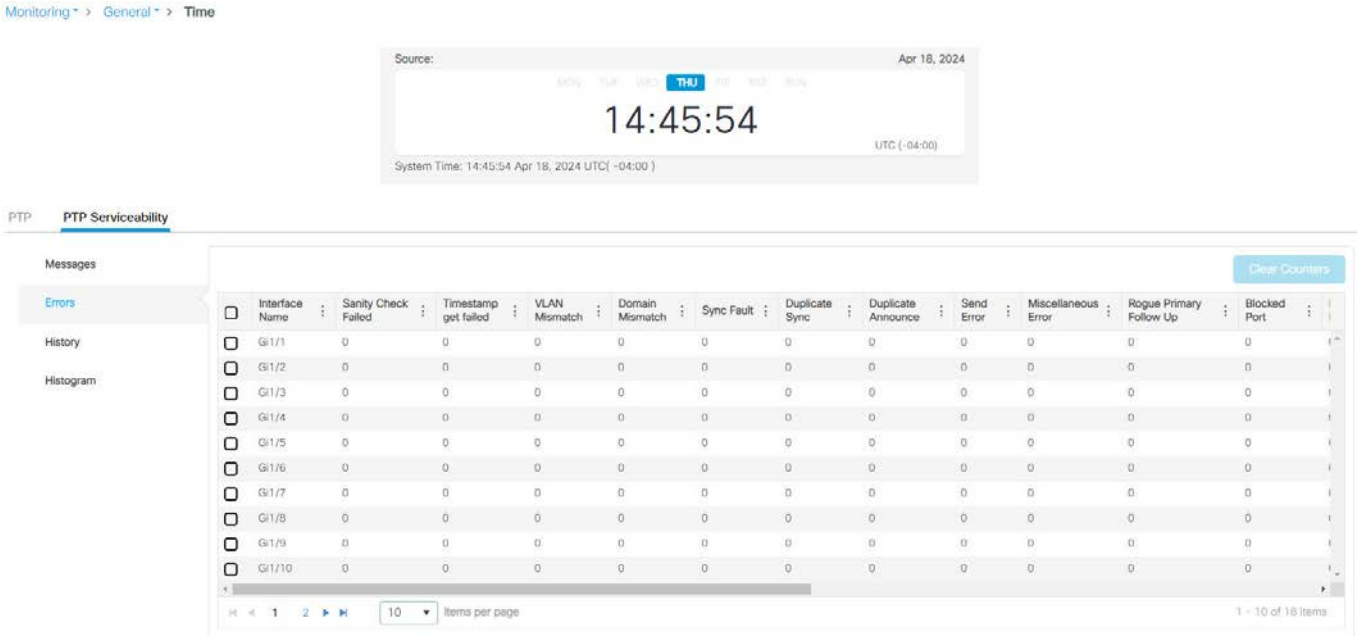


Table 207 - PTP Serviceability Errors

Field	Description
Interface Name	The port type and number.
Sanity Check Failed	The PTP message header field or fields of ingress PTP packets are invalid.
Timestamp Get Failed	This counter increments each time an ingress or egress PTP packet fails to get a timestamp.
VLAN Mismatch	The VLAN ID of ingress PTP messages differs from the VLAN ID configured in the PTP VLAN command.
Domain Mismatch	The domain number field of ingress PTP messages differs from the configured PTP clock domain (the PTP domain number configured in the PTP domain command). (Applicable only in Boundary Clock mode)
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).
Duplicate Sync	The number of duplicate PTP Sync messages received by the switch. (Duplicates are identified by checking the PTP sequence number on received messages.)
Duplicate Announce	The number of duplicate PTP Announce messages received by the switch. (Duplicates are identified by checking the PTP sequence number on received messages.)
Send Error	The number of PTP messages that could not be sent due to failures. PTP software might fail to send PTP messages due to reasons such as memory allocation failure, failure to obtain the correct outgoing interface information, etc.
Miscellaneous Error	The number of miscellaneous errors that have occurred in the PTP protocol. Any error other than the ones listed in preceding fields is classified as a miscellaneous error.
Rogue Primary Follow Up	The number of Follow-up messages blocked on the port when GMC-Block is enabled for the port.
Blocked Port	The PTP messages (except Peer-Delay messages) are received on REP/STP blocked ports.
Invalid Parent ID	The source port identity of ingress PTP messages is different from the parent port identity of the local PTP clock. (Applicable only in Boundary Clock mode).
Invalid GMC ID	The Grandmaster clock identity of ingress announce messages have an invalid value (the Grandmaster clock identity of ingress announce messages are the same as the clock identity of the local PTP clock). (Applicable only in Boundary Clock mode)
Invalid Sequence ID	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). (Applicable only in Boundary Clock mode)
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.

Table 207 - PTP Serviceability Errors

Field	Description
Unmatched Peer Delay Response Follow Up	The switch received a Peer Delay Response Follow up message without sending a Peer Delay Request.
Rogue Primary Sync	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 helps prevent the port from transitioning to the PTP SLAVE state to protect from rogue PTP devices on the Edge of the network.
Rogue Primary Announce	The number of Announce messages blocked on the port when GMC-Block is enabled for the port.

History

The history tab displays the historical maximum and minimum values for the offset from the time source and mean path delay for the last 5 seconds, 15 seconds, in increments up to 15 days, and greater than 15 days.

Information in the History tab is available when the switch is operating in NTP-PTP (NTP-PTP Clock) or BC (Boundary Clock) modes. The values are zero if the switch is the time source or Grandmaster clock.

Offset

Offset is the difference between the time on the time recipient clock and the time source. It is the measure of how accurately the time recipient synchronizes with the time source clock. This measurement indicates the amount of inaccuracy that is brought by the switch as a boundary clock. Less is better.

Mean Path Delay

The mean path delay is the average time taken by PTP frames to travel between time source and recipient. 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 jitter is representative of a complex DataCenter with buffering and latency spikes, control protocols running, a high rate of traffic, and so on.

Offset and Delay Values

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

Offset and delay values are shown for the past:

- 5 seconds
- 15 seconds
- 1 minute
- 5 minutes
- 15 minutes
- 1 hour
- 5 hours
- 15 hours
- 1 day
- 5 days
- 15 days

They are also shown fore more than 15 days

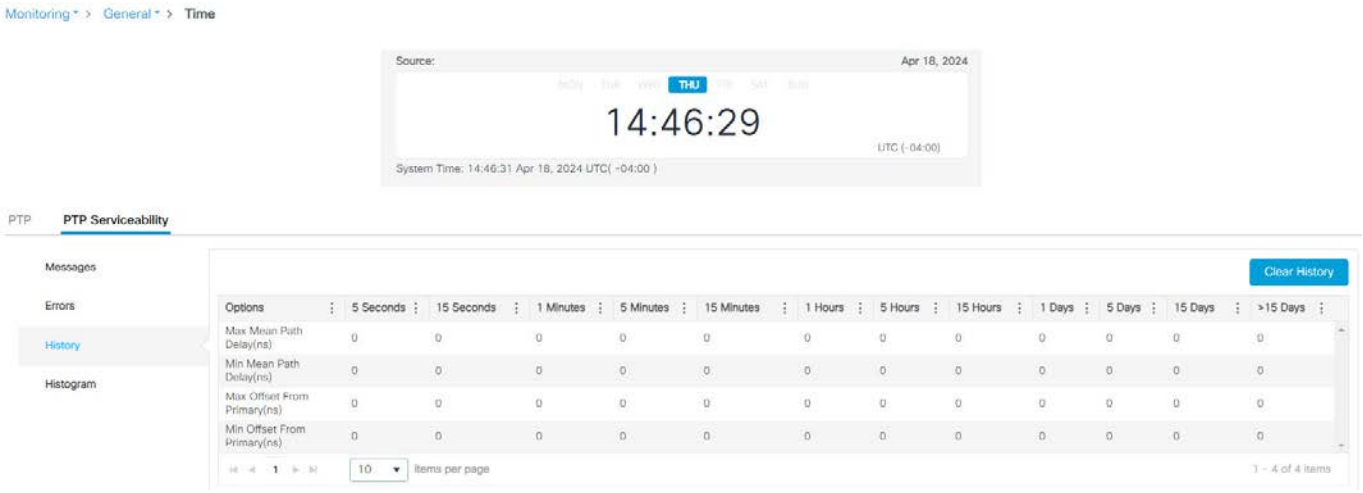


Table 208 - PTP Serviceability History

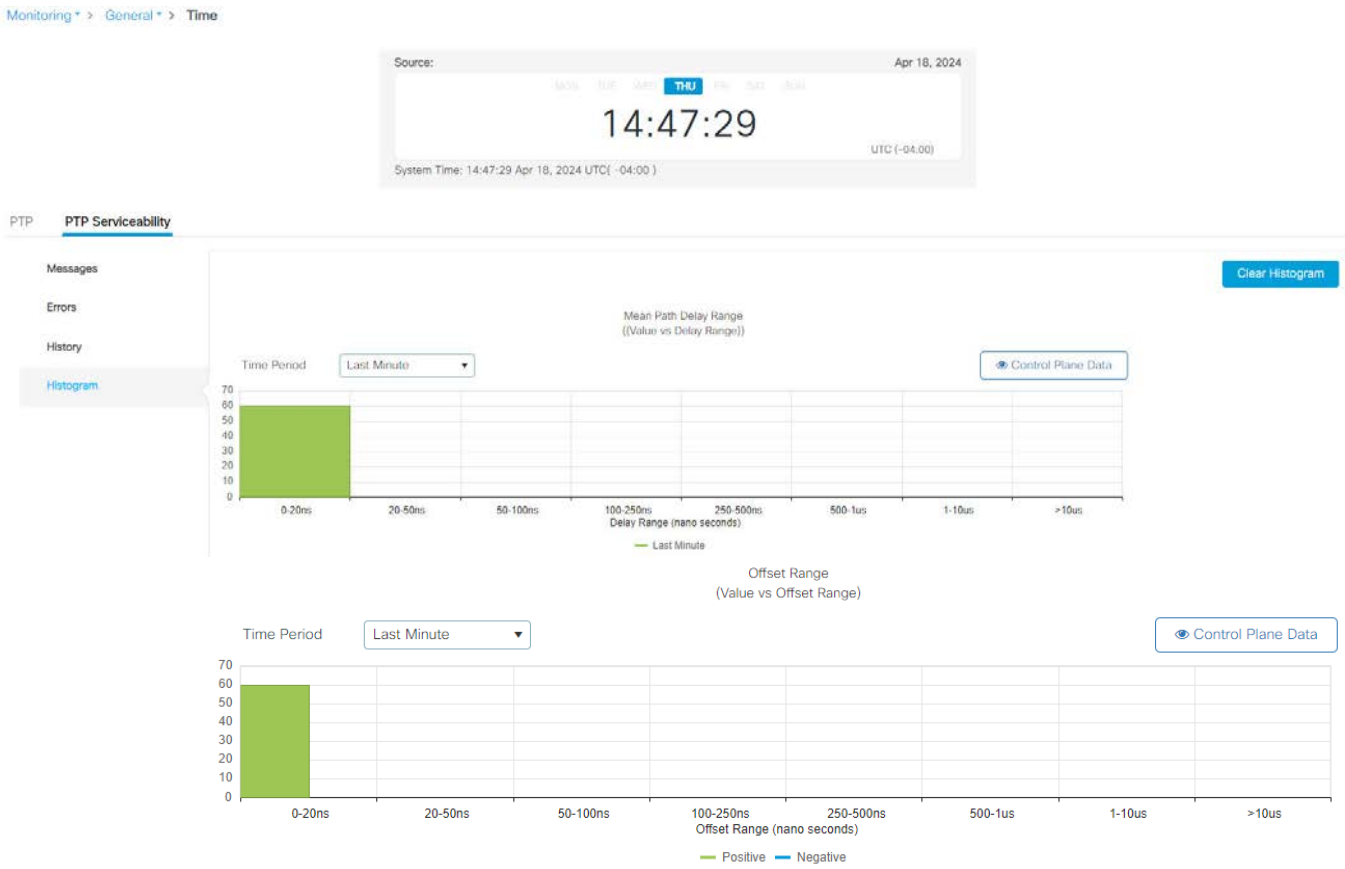
Field	Descriptions
Max Mean Path Delay(ns)	The maximum average time, in nanoseconds, taken by PTP frames to travel between time source and time recipient.
Min Mean Path Delay(ns)	The minimum average time, in nanoseconds, taken by PTP frames to travel between time source and time recipient.
Max Offset From Primary(ns)	The maximum difference, in nanoseconds, between the time on the time recipient clock and the time source clock.
Min Offset From Primary(ns)	The minimum difference, in nanoseconds, between the time on the time recipient clock and the time source clock.
Max time error (ns)	The maximum difference, in nanoseconds, between the time on the time recipient clock and the time source clock.
Min time error (ns)	The minimum difference, in nanoseconds, between the time on the time recipient clock and the time source clock.

Histogram

The Histogram tab provides a graphical display of the following 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 of 0…20 nanoseconds, 20…50 nanoseconds, 50…100 nanoseconds, 100…250 nanoseconds, 250…500 nanoseconds, 500…1000 nanoseconds, 1000…10,000 nanoseconds, and greater than 10,000 nanoseconds.
  - Select Last Minute to show the data for the last 60 seconds, Last Hour to show the data for the last 1 hour, and Last Day to show data for the last 24 hours.
  - Click Control Plane Data to display the data in table format. Click Export as PDF in the Control Plane Data window to export the table data.
- **Offset Range:** Available when the clock mode is boundary. This histogram shows data for the positive or negative variation in the offset from time source. Offset Range values are divided into ranges of 0 nanoseconds…20 nanoseconds, 20…50 nanoseconds, 50…100 nanoseconds, 100…250 nanoseconds, 250…500 nanoseconds, 500…1000 nanoseconds, 1000…10,000 nanoseconds, and greater than 10,000 nanoseconds.
  - Select Last Minute to show the data for the last 60 seconds, Last Hour to show the data for the last 1 hour, and Last Day to show data for the last 24 hours.
  - Click Control Plane Data to display the data in table format. Click Export as PDF in the Control Plane Data window to export the table data.

- **Time Error Range:** Displayed when the clock mode is e2etransparent. This histogram shows data for the positive or negative variation in the time-error (frequency error * residence time). Time Error Range values are divided into ranges of 0…20 nanoseconds, 20…50 nanoseconds, 50…100 nanoseconds, 100…250 nanoseconds, 250…500 nanoseconds, 500…1000 nanoseconds, 1000…10,000 nanoseconds, and greater than 10,000 nanoseconds.
  - Select Last Minute to show the data for the last 60 seconds, Last Hour to show the data for the last 1 hour, and Last Day to show data for the last 24 hours.
  - Click Control Plane Data to display the data in table format. Click Export as PDF in the Control Plane Data window to export the table data.



VRRP (Stratix 5800 Switch Only)

Monitor VRRP



Table 209 - Monitoring VRRP

Parameter	Description
Group	VRRP group number for the interface.
Interface	Interface type and number. Range: 0...255 Default: 0
IPv4 Address	IPv4 address of the VRRP interface.
Secondary IP	Secondary IP address of the VRRP interface.
IPv6 Address	IPv6 address of the VRRP interface.
State	State of VRRP interface; can be one of the following: • Init - Waits for startup event. • Backup - Monitors the availability and state of the virtual device master. • Master - Functions as the forwarding router for the IP address(es) associated with the virtual router.
Current Priority	The priority value used in choosing the virtual device master. Range: 1...254 Default: 100
Configured Priority	Priority configured on the VRRP interface.
Adverse Interval	Configured interval (in milliseconds) at which the VRRP interface sends VRRP advertisements when it is the virtual device master. Range: 100...40950 Default: 100
Track Interface	Name of interface that is being tracked.
Master Router	Location of the virtual device master.
Interface Priority	Amount by which the VRRP priority for the interface is decremented (or incremented) when the tracked interface goes down (or comes back up).
Master Down Interval	Time the VRRP interface waits for the virtual device master advertisements before assuming the role of master router.
Master Advertise Interval	Interval (in milliseconds) at which the virtual device master sends VRRP advertisements.

Notes:

Troubleshoot the Switch

Topic	Page
Configure and View System Logs	339
Download Core Files	342
Download a Debug Bundle	343
Troubleshoot with Ping and Trace Route	344
Troubleshoot the Installation	346
Troubleshoot IP Addresses	347
Troubleshoot the WebUI	348
Troubleshoot Switch Performance	348
Automatic Device Descriptive Analytics (ADDA)	349

Configure and View System Logs

In the WebUI for the switch, the system log (syslog) displays events that occur on the switch and its ports. The events are based on alarm settings.

Message Severity Levels

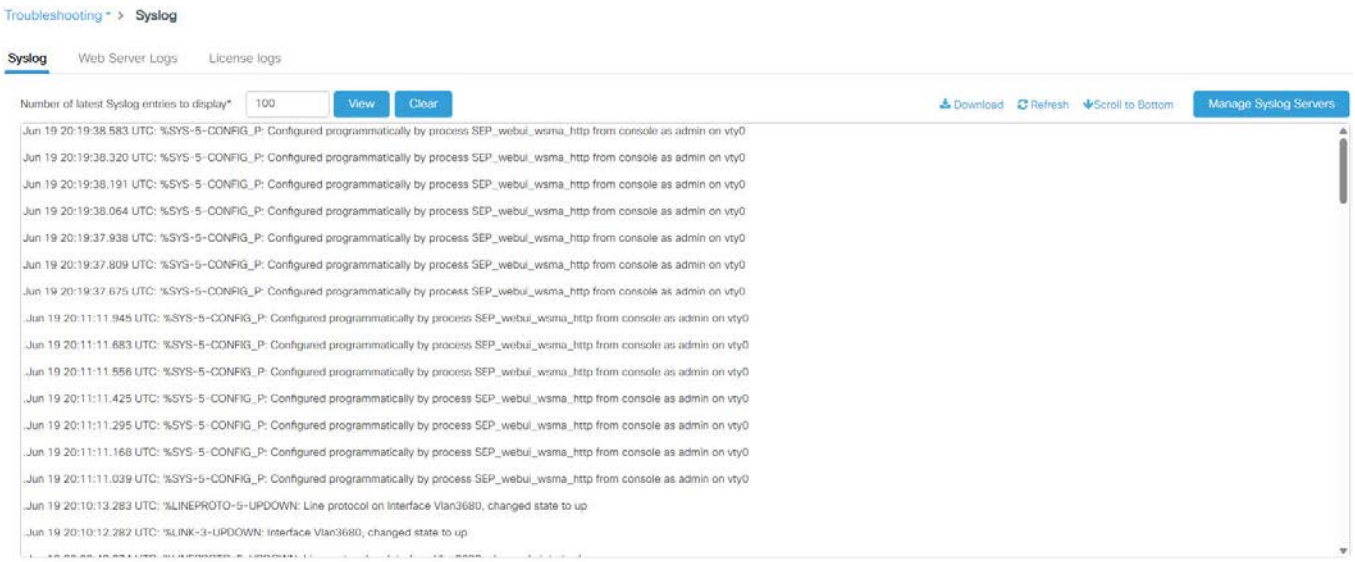
Table 210 lists the syslog message levels from the most severe level to the least severe level.

Table 210 - Syslog Message Severity Levels

Severity Level	Numerical Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warnings conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

From the Troubleshooting menu, click Logs.





From the Troubleshooting: Syslog page, you can manage Syslog servers and entries, and view Web server and License logs:

- To manage Syslog servers, click Manage Syslog Servers, complete the fields in Table 211, and then click Apply to Device.
- To change the number of log entries on the page, enter the number of entries to display, and then click View. For example, if you type 100, the most recent 100 lines in the syslog are displayed.
- To display Web server logs, click the Web Server Logs tab. To display License Logs, click the License logs tab. To download entire Web server or License logs, click Download Full Log on the respective tabs.
- To delete all of the log entries, click Clear.
- To download the log entries to your local computer, click .

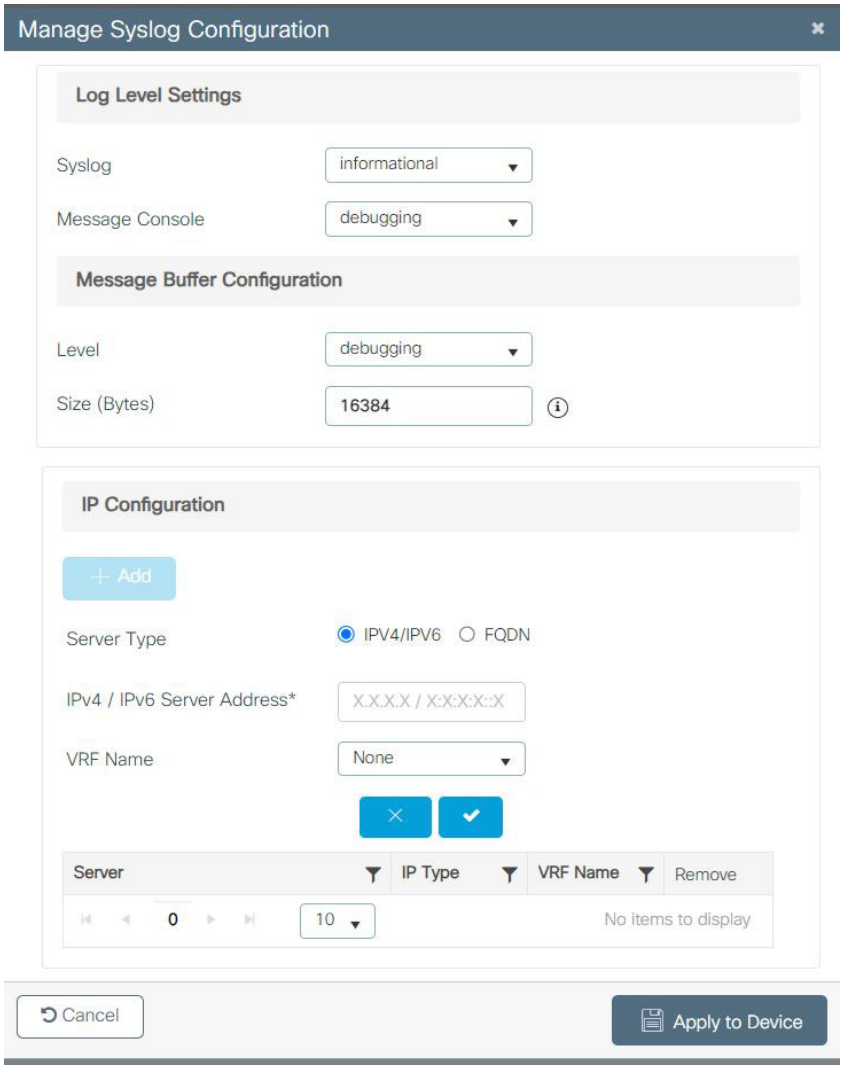


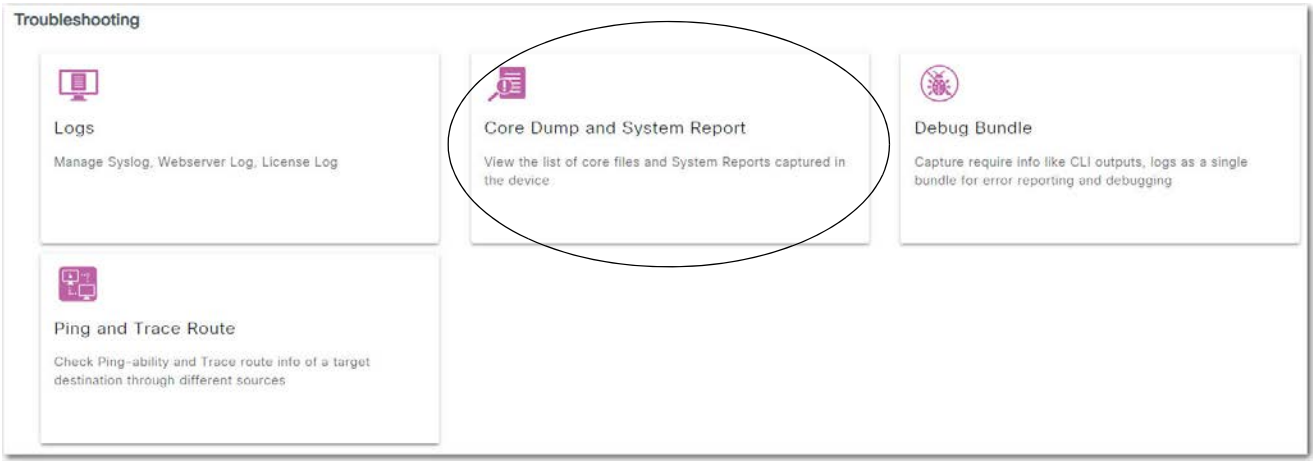
Table 211 - Manage Syslog Configuration Fields

Field	Description
Log Level Settings	
Syslog	Choose the kind of messages, by severity level, to send to the Syslog server. For information about message severity levels, see Table 210 on page 339. Default value: informational
Message Console	Choose the severity level for the messages you want sent to the device console.
Message Buffer	Choose the severity level for the messages you want sent to the internal buffer on the device.
IP Configuration	
IPV4/IPV6	Check to specify the IPv4 or IPv6 address of the server on which to store message logs.
IPv4/IPv6 Server Address	Enter the IPv4 or IPv6 address of the server on which to store message logs.
VRF Name	Choose the VPN routing/forwarding (VRF) table.
+	Click to add the IP address and VFR (if applicable) to the grid. You can add multiple servers. To delete a server, click X in the Remove column.

Download Core Files

When the switch encounters a significant error, it can take a snapshot of the data currently stored in its memory at the time of the error. Technical Support can refer to this snapshot of data, also known as a core dump, at a later time for troubleshooting. In the WebUI, you can download a core dump and share the data with technical support for intensive troubleshooting.

From the Troubleshooting menu, click Core Dump and System Report.



The information from the switch appears on the Troubleshooting: Core Dump and System Report page.

Review the date and time stamp to identify the files to download, and then click Download to save to your computer. The core files are downloaded to the location configured for your browser.



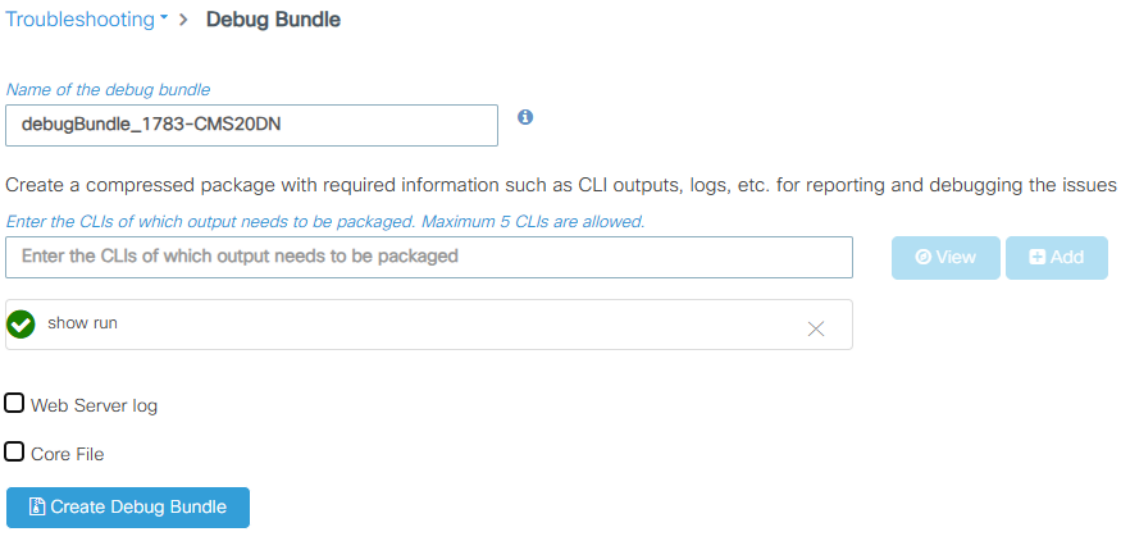
Download a Debug Bundle

A debug bundle is the output of CLI commands stored in a zip file that you can download for analysis and troubleshooting. The WebUI enables you to create a debug bundle and download it to your local computer.

From the Troubleshooting menu, click Debug Bundle.



The Troubleshooting: Debug Bundle page appears.



From the Troubleshooting: Debug Bundle page, you can create and download a debug bundle:

- To create a debug bundle, complete the fields in Table 212, and then click Create Debug Bundle. A window opens to display the status.
- To download the debug bundle once it is created, click Download Debug Bundle.

Table 212 - Troubleshooting: Debug Bundle

Field	Description
Name of the debug bundle	Enter a name to identify the debug bundle. The name can have a maximum of 25 characters and can include lowercase or uppercase letters, numbers 0...9, and the underscore (_).
Enter the CLIs of which ouptut needs to be packaged	Enter a maximum of 5 CLI commands to identify the content to capture in the debug bundle. To verify the output of the CLI commands, click View. To add a CLI command to the debug bundle, click Add. To remove a CLI command from the debug bundle, click the X to the right of the command.
Web Server log	To include the web server log in the debug file, check Web Server log.
Core File	To include core files from the internal memory of the switch in the debug bundle, check Core File. A window opens with a list of core files on the device. You can select a maximum of two core files from this list.

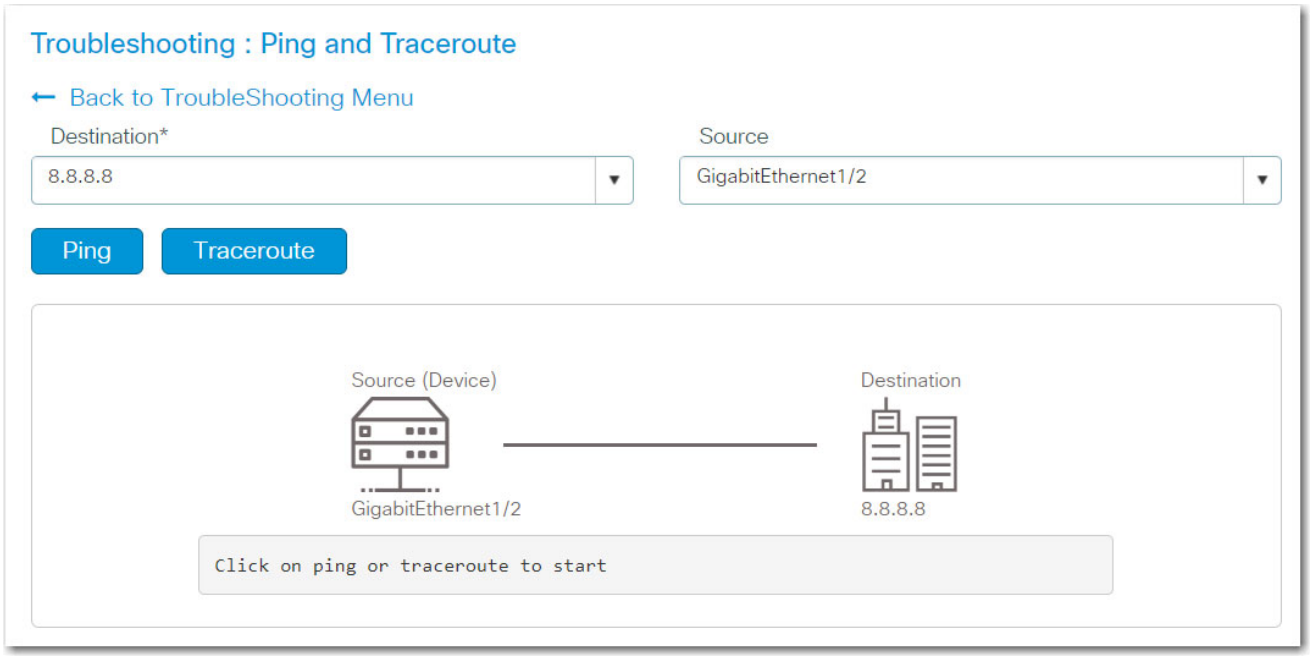
Troubleshoot with Ping and Trace Route

To troubleshoot connectivity problems, communication delays and packet loss, you can use the ping and trace route feature in the WebUI of the switch.

From the Troubleshooting menu, click Ping and Trace Route.



The Troubleshooting: Ping and Traceroute page appears.



Ping Destinations

Sending ping packets to a destination can help you verify connectivity.

1. In the Destination field, enter a destination or choose a predefined destination from the pull-down menu.

   Ping packets are sent to the specified destination.
2. (Optional) In the Source field, enter the source IP address on the switch to initiate the ping.

   The ICMP echo response is sent to the specified source.
3. Click Ping.

Discover Route Information

Discovering route information can help you identify the path of a Layer 3 transmission.

1. In the Destination field, enter a destination interface or choose a predefined destination from the pull-down menu.
2. In the Source field, enter the source IP address for which to run Traceroute.
3. Click Traceroute.

   Traceroute discovers the route and the number of Layer 3 hops that packets take when traveling to their destination.

Troubleshoot the Installation

The status indicators on the front panel provide troubleshooting information about the switch. They show 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.

Bad or Damaged Cable

Always make sure that the cable does not have damage. 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:

- For 1000 Mbps 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.

Port Status

Verify that both sides of the port connection have a network connection. A port 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 port status indicator for the port is off, 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.
- Verify the port settings, as described on page 347.

SFP Module Issues

Use SFP modules only from Rockwell Automation. 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.

If you encounter SFP module issues, try the following:

- Verify that the SFP module is valid and functional. Exchange a suspect module with a known good module on this platform. For supported modules, see the Ethernet Device Specifications Technical Data, publication 1783-TD002.
- Make sure that all fiber connections are properly cleaned and securely connected.
- Be sure that the fiber cable is compatible with the SFP module. For example, do not use single-mode cable with a multi-mode SFP module.
- Be sure to use an SFP module with same speed on both ends.
- Be sure that the fiber cable is installed correctly on the SFP module (RX connected to TX, and TX connected to RX).

Port Settings

A disabled port can cause a port connectivity failure:

- Verify that operational status of the port on the Configuration > Ethernet Ports page, as described on page 89. Users with read-only access can verify port status on the Monitoring > Ports page, as described on page 310.
- Verify the operational status of the VLAN assigned to the port on the Configuration > VLAN page, as described on page 201.

If a port or interface is manually shut down on one side of the connection, you must re-enable the port on the Configuration > Ethernet Ports page, as described on page 89.

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 and that the switch is configured for DHCP IP address assignment. 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, run Express Setup and configure the correct IP address. If the device is set for DHCP and receiving the wrong address, verify the configuration settings on your DHCP server.

Troubleshoot the WebUI

The following table includes basic troubleshooting for issues that are related to the WebUI.

Issue	Resolution
WebUI does not appear	If you cannot display the WebUI 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: – 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.
WebUI does not operate properly	Open the WebUI in a new browser window by using a private browsing mode.

Troubleshoot Switch Performance

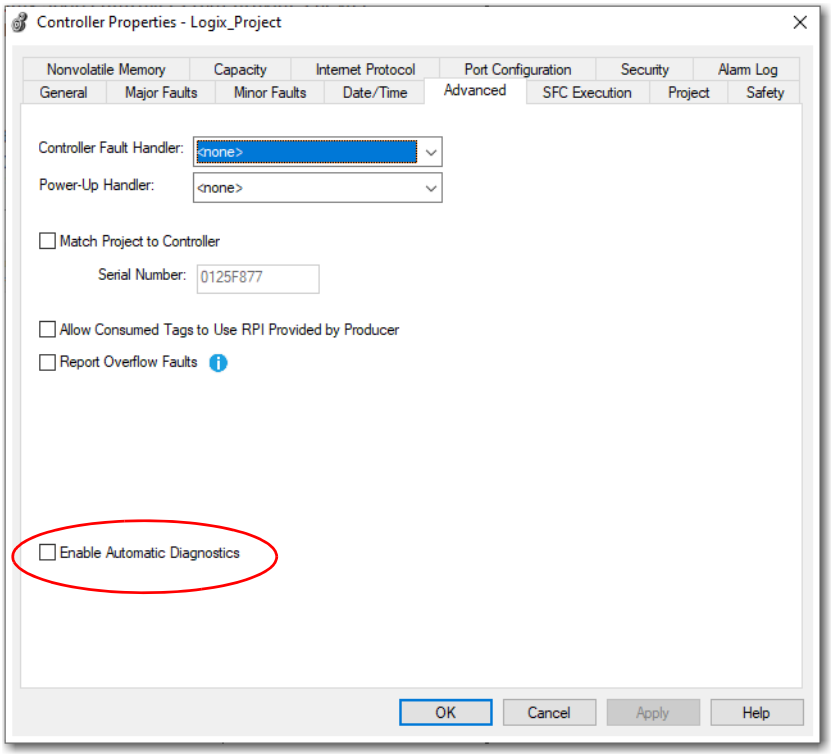
The following table includes basic troubleshooting for issues that are related to switch performance.

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.

Automatic Device Descriptive Analytics (ADDA)

Automatic Device Descriptive Analytics is a system feature that delivers device level diagnostics to HMIs and other clients with zero user programming.

This section describes how ADDA assists in troubleshooting the switch in case issues occur during normal operation. The diagnostics include device description conditions and state events. Automatic Diagnostics is enabled by default in Logix controllers with firmware revision 33 or later. You can disable and enable the whole feature while online or offline from the Advanced tab on the Controller Properties dialog box. You can also disable Automatic Diagnostics for a specific device in the device's configuration.



The following ADDA alarms are supported for Stratix switches added to the I/O tree.

Table 213 - ADDA Alarm Codes

Display Code	Display Text
S-UNDEV	Unauthorized device detected on Port %s
S-COMRT	Communication rate threshold exceeded on Port %s

Considerations for Communication Loss Diagnostics

When enabled, the Automatic Diagnostics feature enables:

- Communication loss diagnostics for all devices in the controller I/O configuration
- Device-level automatic diagnostics evaluations for all uninhibited and enabled devices.

You can disable Automatic Diagnostics for a specific device in the device configuration. The communication loss diagnostic remains active even if the device disables Automatic Diagnostics. To disable communication loss diagnostic, inhibit the device or disable Automatic Diagnostics at the controller.

Display Code Definitions

S-UNDEV - Unauthorized device detected on Port %s

The S-UNDEV status flag indicates whether any unauthorized MAC address has attempted to communicate on any port of the device. It is set to 1 when any of the individual PortXXX_XUnauthorizedDevice members are set to 1, signifying a violation on at least one port.

This indicator does not have a fallback message and is intended to provide a quick, global view of port security violations across the switch. It is useful for monitoring and alerting systems that must detect unauthorized access attempts at a device-wide level.

"This parameter indicates whether an unauthorized MAC address has attempted to communicate on a specific port. The value is defined as follows:

- 0 - No mismatch: Either port security is disabled, or it is enabled, and the number of detected MAC addresses is within the allowed limit.
- 1 - Mismatch: Port security is enabled, and a violation has occurred due to an unauthorized MAC address attempting to communicate.

These indicators are only set to 1 if port security is enabled on the device. When enabled, the switch monitors the number of MAC addresses learned on each port. If the number of detected MAC addresses exceeds the configured maximum, or if an unauthorized MAC address is detected, the port enters Restrict mode.

In Restrict mode, the switch blocks traffic from the unauthorized MAC address but continues to allow communication with authorized devices. This ensures that normal network traffic is not disrupted, avoiding a full outage. However, the presence of an unauthorized MAC address requires attention from maintenance personnel to investigate and resolve the violation.

Some customers require immediate notification or action in such cases due to heightened security policies. Note that port security is enabled by default on certain Smartport configurations, and behavior can vary depending on the specific template applied.

S-COMRT - Communication rate Threshold exceeded on Port %s

Indicates that unicast, multicast, or broadcast traffic has exceeded the configured threshold on any port. This flag is set to 1 when any PortXXX_XThreshold member is triggered. There is no fallback message; use port-level indicators for detailed diagnostics.

Indicates whether unicast, multicast, or broadcast traffic has exceeded the configured threshold on a specific port.

- 0 - Normal (traffic within limits)
- 1 - Threshold exceeded

When the threshold is exceeded, excess traffic-including legitimate packets-is dropped. This can result in data loss for devices that are connected to the affected port and intermittent connection timeouts. In some cases, excessive multicast or broadcast traffic can signal a storm condition, potentially impacting overall network stability.

The status can remain at 1 or fluctuate from 0...1 if traffic levels hover around the threshold.

Status Indicators

Topic	Page
Stratix 5200 Status Indicators	351
Stratix 5800 Status Indicators	352

Stratix 5200 Status Indicators

Stratix® 5200 switches have status indicators on the front panel. The color and behavior of each status indicator helps you to monitor the status of the switch, network, power, alarms, and individual ports.

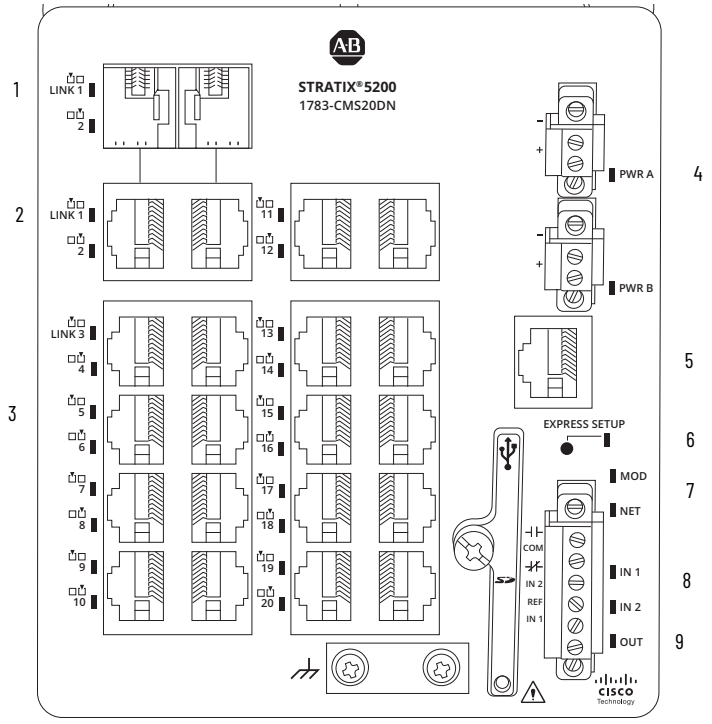


Table 214 - Stratix 5200 Status Indicators

Item	Status Indicators
1	Dual-media SFP port
2	Dual-media copper port
3	1000BASE-T port
4	Power connectors
5	Management console
6	Express setup

Table 214 - Stratix 5200 Status Indicators

Item	Status Indicators
7	EIP
8	Alarm input
9	Alarm output

Port Status Indicators

Each Ethernet port has a status indicator that displays information about the individual port. The dual-media ports have two status indicators, one by the SFP connector and the second by the RJ-45 connector.

Table 215 - Port Status Indicators

Indicator	Status	Description
Dual-media SFP port Dual-media copper port	Off	No link, or the port is administratively shut down.
	Solid Green	Link present, but no activity.
	Blinking Green	Activity: Port is sending or receiving data.
	Alternating green and amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Solid amber	Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data. After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
	Blinking amber	The port is going through the Spanning Tree process and is sending Spanning Three BPDUs on an STP blocked port.

Stratix 5800 Status Indicators

Stratix 5800 switches and expansion modules have status indicators on the front panel. The color and behavior of each status indicator helps you to monitor the status of the switch, network, power, alarms, and individual ports.

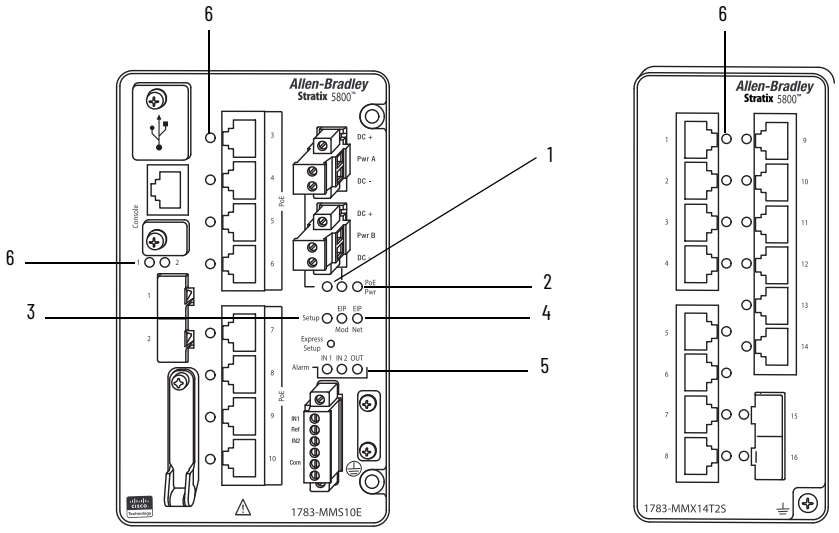


Table 216 - Stratix 5800 Status Indicators

Item	Status Indicators
1	Power (Pwr A and Pwr B indicated by lines to corresponding power connector)
2	Power over Ethernet (PoE Pwr)(1)
3	Setup
4	EIP (EIP Mod, EIP Net)
5	Alarms (Alarm IN1, Alarm IN2, Alarm OUT)
6	Ports

(1) The PoE Pwr status indicator appears only on switch models that support Power over Ethernet (PoE).

Power Status Indicators

The switch can operate with one or two DC power sources. Each DC input has an associated status indicator that shows the status of the corresponding DC input (Pwr A, Pwr B). If power is present on the circuit, the status indicator is green. If power is not present, the status indicator color depends on the alarm configuration. If alarms are configured, the status indicator is red when power is not present; otherwise, the status indicator is off.

If the switch has dual power sources, the switch draws power from the power source with the higher voltage. If one of the DC sources fails, the alternate DC source powers the switch, and the corresponding power status indicator is green. The power status for the failed DC source is either off or red, depending on the alarm configuration.

If the power input drops below the low valid level, the power status indicators show that power is not present on the switch. If the voltage at the switch input exceeds the valid level, the power status indicators only show that power is present.

Table 217 - Power Status Indicators

Indicator	Status	Description
Pwr A Pwr B	Off	Power is not present on the circuit.
	Solid green	Power is present on the associated circuit.
	Solid red	Power is not present on the associated circuit, and the power supply alarm is configured.

Power over Ethernet Status Indicator (Stratix 5800 Switch Only)

The Power over Ethernet status indicator (PoE Pwr) is available only on switch models that support PoE.

Table 218 - Power over Ethernet Status Indicator

Indicator	Status	Description
PoE Pwr	Off	The switch is not providing PoE power to any connected devices.
	Solid green	The switch is providing PoE power to one or more connected devices.
	Flashing amber	PoE is off due to a fault. **IMPORTANT:** Non-compliant cabling or powered devices can cause a PoE port fault. Use only standard-compliant cabling to connect compliant PoE devices. You must remove any cable or device that causes a PoE fault.
	Alternating green and amber	PoE is denied because providing power to a connected device exceeds the switch power capacity.

Setup Status Indicator

The Setup status indicator displays the Express Setup state during the initial configuration. For more details about the Setup status indicator and conditions during Express Setup, see Chapter 2, Express Setup on page 27.

Table 219 - Setup Status Indicator

Indicator	Status	Description
Setup	Off	The switch is configured as a managed switch or is operating normally.
	Solid green	The switch has successfully connected with a computer after the Express Setup button is pressed.
	Flashing green	• The switch has completed its power-on sequence. 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. • The Express Setup button is pressed for a duration of 1...5 seconds to enable Express Setup in Short Press mode.
	Solid red	The switch failed to start Express Setup because of the following: • There is no available switch port to which to connect the management station. Disconnect a device from a switch port, and then press the Express Setup button. • A configuration is already present on the switch. In this scenario, the status indicator is red for 10 seconds. • A condition caused Express Setup to time out.
	Flashing red	The Express Setup button is pressed for a duration of 6...10 seconds to enable Express Setup in Medium Press mode.
	Flashing green and red	The Express Setup button is pressed for a duration of 16...20 seconds to enable Express Setup in Long Press mode.

EIP Status Indicators

The EIP status indicators (EIP Mod and EIP Net) operate in conformance with ODVA standards:

- The EIP Mod status indicator shows whether the switch is receiving power and is functioning properly.
- The EIP Net status indicator shows the network status for the switch.

Table 220 - EIP Status Indicators

Indicator	Status	Description
EIP Mod	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch is operating properly.
	Flashing green	The switch has not been configured.
	Solid red	The switch has detected a major non-recoverable fault.
	Flashing Red	The switch has detected a major recoverable fault, such as an incorrect or inconsistent configuration.
	Flashing green and red	The switch is running a power on self test (POST).
EIP Net	Off	Power to the switch is off or 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 does not have an established CIP connection to one or more attached devices.
	Solid red	The switch has detected that its IP address is already in use by another device in the network.
	Flashing red	One or more connections to attached devices have timed out.
	Flashing green and red	The switch is running a power on self test (POST).

Alarm Status Indicators

The alarm status indicators show the status of the two alarm inputs and one alarm output.

Table 221 - Alarm Status Indicators

Indicator	Status	Description
Alarm IN1 Alarm IN2	Shows the status of the alarm inputs.	
	Off	Alarm IN1 or IN2 is not configured.
	Solid green	Alarm IN1 or IN2 is configured; no alarm is detected.
	Solid red	The switch has detected a minor alarm.
	Flashing red	The switch has detected a major alarm.
Alarm OUT	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.
	Solid red	The switch has detected a minor alarm.
	Flashing red	The switch has detected a major alarm.

Port Status Indicators

The port status indicators show the connection and activity status of the port.

Table 222 - Port Status Indicator

Indicator	Status	Description
Port	Off	The port is not connected to a device.
	Solid green	The port is connected to a device, but there is no activity.
	Flashing green	The port connection has activity and is sending or receiving data.
	Solid amber	The port is not forwarding data.
	Alternating green and amber	The port connection has a link fault.

Notes:

Data Types

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 via the WebUI or the command-line interface (CLI), the output bits override the port setting the next time the bits are applied. The output bits always take precedence, regardless of whether the WebUI or the CLI is used to enable or disable the port.

The following tables list module-defined data types for Stratix® 5200 and Stratix 5800 switches and expansion modules.

Stratix 5200 Data Types

Topic	Page
6-Port Data Types	358
10-Port Data Types	360
20-Port Data Types	363

6-Port Data Types

The following tables list the input and output data types for a 6-port base switch with no expansion module attached.

1783-CMS6B

Table 223 - Stratix 5200 - 1783-CMS6B - Input Data Types (6 Ports)

AB:STRATIX_5200_6PORT_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
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
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_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
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_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

Table 224 - Stratix 5200 - 1783-CMS6B - Output Data Types (6 Ports)

AB:STRATIX_5200_6PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisable	DINT	Binary	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_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

1783-CMS6P

Table 225 - Stratix 5200 - 1783-CMS6P - Input Data Types (6 Ports)

AB:STRATIX_5200_6PORT_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
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
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

Table 226 - Stratix 5200 - 1783-CMS6P - Output Data Types (6 Ports)

AB:STRATIX_5200_6PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisable	DINT	Binary	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

10-Port Data Types

The following tables list the input and output data types for a 10-port base switch with no expansion module attached.

1783-CMS10B

Table 227 - Stratix 5200 - 1783-CMS10B - Input Data Types (10 Ports)

AB:STRATIX_5200_10PORT_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
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
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_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
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_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_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 228 - Stratix 5200 - 1783-CMS10B - Output Data Types (10 Ports)

AB:STRATIX_5200_10PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisable	DINT	Binary	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_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

1783-CMS10P,1783-CMS10DP, 1783-CMS10DN

Table 229 - Stratix 5200 - 783-CMS10P, 1783-CMS10DP, 1783-CMS10DN - Input Data Types (10 Ports)

AB:STRATIX_5200_10PORT_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
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
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_6Threshold	BOOL	Decimal	ThresholdExceeded:6

Table 229 - Stratix 5200 - 783-CMS10P, 1783-CMS10DP, 1783-CMS10DN - Input Data Types (10 Ports)

AB:STRATIX_5200_10PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortGi1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_10Threshold	BOOL	Decimal	ThresholdExceeded:10

20-Port Data Types

The following tables list the input and output data types for a 20-port base switch with no expansion module attached

1783-CMS20DB.

Table 230 - Stratix 5200 - 1783-CMS20DB - Input Data Types (20 Ports)

AB:STRATIX_5200_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
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_71Connected	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
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

Table 230 - Stratix 5200 - 1783-CMS20DB - Input Data Types (20 Ports)

AB:STRATIX_5200_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortFa1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortFa1_20Threshold	BOOL	Decimal	ThresholdExceeded:20

Table 231 - Stratix 5200 - 1783-CMS20DB - Output Data Types (20 Ports)

AB:STRATIX_5200_10PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisable	DINT	Binary	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_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

1783-CMS20DP, 1783-CMS20DN.

Table 232 - Stratix 5200 - 1783-CMS20DP, 1783-CMS20DN - Input Data Types (20 Ports)

AB:STRATIX_5200_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
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_71Connected	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

Table 232 - Stratix 5200 - 1783-CMS20DP, 1783-CMS20DN - Input Data Types (20 Ports)

AB:STRATIX_5200_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortGi1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortGi1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortGi1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortGi1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortGi1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortGi1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortGi1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortGi1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortGi1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_20Threshold	BOOL	Decimal	ThresholdExceeded:20

Table 233 - Stratix 5200 - 1783-CMS20DP, 1783-CMS20DN - Output Data Types (20 Ports)

AB:STRATIX_5200_10PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisable	DINT	Binary	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 5800 Data Types

Topic	Page
10-Port Data Types	367
18-Port Data Types	368
26-Port Data Types	370

10-Port Data Types

The following tables list the input and output data types for a 10-port base switch with no expansion module attached.

Table 234 - Stratix 5800 Input Data Types (10 Ports)

AB:STRATIX_5800_10PORT_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
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
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
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	

Table 234 - Stratix 5800 Input Data Types (10 Ports) (Continued)

AB:STRATIX_5800_10PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
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	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupActive	DINT	Binary	

Table 235 - Stratix 5800 Output Data Types (10 Ports)

AB:STRATIX_5800_10PORT_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

18-Port Data Types

The following table lists the input and output data types for a 10-port base switch with an 8-port expansion module attached.

Table 236 - Stratix 5800 Input Data Types (18 Ports)

AB:STRATIX_5800_18PORT_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
PortGi2_1Connected	BOOL	Decimal	LinkStatus:11
PortGi2_2Connected	BOOL	Decimal	LinkStatus:12

Table 236 - Stratix 5800 Input Data Types (18 Ports) (Continued)

AB:STRATIX_5800_18PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi2_3Connected	BOOL	Decimal	LinkStatus:13
PortGi2_4Connected	BOOL	Decimal	LinkStatus:14
PortGi2_5Connected	BOOL	Decimal	LinkStatus:15
PortGi2_6Connected	BOOL	Decimal	LinkStatus:16
PortGi2_7Connected	BOOL	Decimal	LinkStatus:17
PortGi2_8Connected	BOOL	Decimal	LinkStatus:18
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
PortGi2_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortGi2_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortGi2_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortGi2_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortGi2_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortGi2_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortGi2_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortGi2_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
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
PortGi2_1Threshold	BOOL	Decimal	ThresholdExceeded:11
PortGi2_2Threshold	BOOL	Decimal	ThresholdExceeded:12
PortGi2_3Threshold	BOOL	Decimal	ThresholdExceeded:13
PortGi2_4Threshold	BOOL	Decimal	ThresholdExceeded:14
PortGi2_5Threshold	BOOL	Decimal	ThresholdExceeded:15
PortGi2_6Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi2_7Threshold	BOOL	Decimal	ThresholdExceeded:17
PortGi2_8Threshold	BOOL	Decimal	ThresholdExceeded:18
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortGi1_5Utilization	SINT	Decimal	

Table 236 - Stratix 5800 Input Data Types (18 Ports) (Continued)

AB:STRATIX_5800_18PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_6Utilization	SINT	Decimal	
PortGi1_7Utilization	SINT	Decimal	
PortGi1_8Utilization	SINT	Decimal	
PortGi1_9Utilization	SINT	Decimal	
PortGi1_10Utilization	SINT	Decimal	
PortGi2_11Utilization	SINT	Decimal	
PortGi2_12Utilization	SINT	Decimal	
PortGi2_13Utilization	SINT	Decimal	
PortGi2_14Utilization	SINT	Decimal	
PortGi2_15Utilization	SINT	Decimal	
PortGi2_16Utilization	SINT	Decimal	
PortGi2_17Utilization	SINT	Decimal	
PortGi2_18Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupActive	DINT	Binary	

Table 237 - Stratix 5800 Output Data Types (18 Ports)

AB:STRATIX_5800_18PORT_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
PortGi2_11Disable	BOOL	Decimal	DisablePort:11
PortGi2_12Disable	BOOL	Decimal	DisablePort:12
PortGi2_13Disable	BOOL	Decimal	DisablePort:13
PortGi2_14Disable	BOOL	Decimal	DisablePort:14
PortGi2_15Disable	BOOL	Decimal	DisablePort:15
PortGi2_16Disable	BOOL	Decimal	DisablePort:16
PortGi2_17Disable	BOOL	Decimal	DisablePort:17
PortGi2_18Disable	BOOL	Decimal	DisablePort:18

26-Port Data Types

The following table lists the input and output data types for a 10-port base switch with a 16-port expansion module attached.

Table 238 - Stratix 5800 Input Data Types (26 Ports)

AB:STRATIX_5800_26PORT_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
PortGi2_1Connected	BOOL	Decimal	LinkStatus:11
PortGi2_2Connected	BOOL	Decimal	LinkStatus:12
PortGi2_3Connected	BOOL	Decimal	LinkStatus:13
PortGi2_4Connected	BOOL	Decimal	LinkStatus:14
PortGi2_5Connected	BOOL	Decimal	LinkStatus:15
PortGi2_6Connected	BOOL	Decimal	LinkStatus:16
PortGi2_7Connected	BOOL	Decimal	LinkStatus:17
PortGi2_8Connected	BOOL	Decimal	LinkStatus:18
PortGi2_9Connected	BOOL	Decimal	LinkStatus:19
PortGi2_10Connected	BOOL	Decimal	LinkStatus:20
PortGi2_11Connected	BOOL	Decimal	LinkStatus:21
PortGi2_12Connected	BOOL	Decimal	LinkStatus:22
PortGi2_13Connected	BOOL	Decimal	LinkStatus:23
PortGi2_14Connected	BOOL	Decimal	LinkStatus:24
PortGi2_15Connected	BOOL	Decimal	LinkStatus:25
PortGi2_16Connected	BOOL	Decimal	LinkStatus:26
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
PortGi2_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortGi2_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortGi2_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortGi2_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortGi2_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortGi2_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortGi2_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortGi2_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi2_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi2_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
PortGi2_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:21

Table 238 - Stratix 5800 Input Data Types (26 Ports) (Continued)

AB:STRATIX_5800_26PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi2_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:22
PortGi2_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:23
PortGi2_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:24
PortGi2_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:25
PortGi2_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:26
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
PortGi2_1Threshold	BOOL	Decimal	ThresholdExceeded:11
PortGi2_2Threshold	BOOL	Decimal	ThresholdExceeded:12
PortGi2_3Threshold	BOOL	Decimal	ThresholdExceeded:13
PortGi2_4Threshold	BOOL	Decimal	ThresholdExceeded:14
PortGi2_5Threshold	BOOL	Decimal	ThresholdExceeded:15
PortGi2_6Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi2_7Threshold	BOOL	Decimal	ThresholdExceeded:17
PortGi2_8Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi2_9Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi2_10Threshold	BOOL	Decimal	ThresholdExceeded:20
PortGi2_11Threshold	BOOL	Decimal	ThresholdExceeded:21
PortGi2_12Threshold	BOOL	Decimal	ThresholdExceeded:22
PortGi2_13Threshold	BOOL	Decimal	ThresholdExceeded:23
PortGi2_14Threshold	BOOL	Decimal	ThresholdExceeded:24
PortGi2_15Threshold	BOOL	Decimal	ThresholdExceeded:25
PortGi2_16Threshold	BOOL	Decimal	ThresholdExceeded:26
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	
PortGi2_1Utilization	SINT	Decimal	
PortGi2_2Utilization	SINT	Decimal	
PortGi2_3Utilization	SINT	Decimal	
PortGi2_4Utilization	SINT	Decimal	
PortGi2_5Utilization	SINT	Decimal	
PortGi2_6Utilization	SINT	Decimal	
PortGi2_7Utilization	SINT	Decimal	

Table 238 - Stratix 5800 Input Data Types (26 Ports) (Continued)

AB:STRATIX_5800_26PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi2_8Utilization	SINT	Decimal	
PortGi2_9Utilization	SINT	Decimal	
PortGi2_10Utilization	SINT	Decimal	
PortGi2_11Utilization	SINT	Decimal	
PortGi2_12Utilization	SINT	Decimal	
PortGi2_13Utilization	SINT	Decimal	
PortGi2_14Utilization	SINT	Decimal	
PortGi2_15Utilization	SINT	Decimal	
PortGi2_16Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupActive	DINT	Binary	

Table 239 - Stratix 5800 Output Data Types (26 Ports)

AB:STRATIX_5800_26PORT_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
PortGi2_1Disable	BOOL	Decimal	DisablePort:11
PortGi2_2Disable	BOOL	Decimal	DisablePort:12
PortGi2_3Disable	BOOL	Decimal	DisablePort:13
PortGi2_4Disable	BOOL	Decimal	DisablePort:14
PortGi2_5Disable	BOOL	Decimal	DisablePort:15
PortGi2_6Disable	BOOL	Decimal	DisablePort:16
PortGi2_7Disable	BOOL	Decimal	DisablePort:17
PortGi2_8Disable	BOOL	Decimal	DisablePort:18
PortGi2_9Disable	BOOL	Decimal	DisablePort:19
PortGi2_10Disable	BOOL	Decimal	DisablePort:20
PortGi2_11Disable	BOOL	Decimal	DisablePort:21
PortGi2_12Disable	BOOL	Decimal	DisablePort:22
PortGi2_13Disable	BOOL	Decimal	DisablePort:23
PortGi2_14Disable	BOOL	Decimal	DisablePort:24
PortGi2_15Disable	BOOL	Decimal	DisablePort:25
PortGi2_16Disable	BOOL	Decimal	DisablePort:26

Notes:

Port Assignments for CIP Data

Port Assignments

The following table identifies the instance numbers of the Ethernet link objects that are associated with each port on Stratix® 5200 and Stratix 5800 switches and expansion modules. Instance 0 does not apply to all ports as it does for bit maps.

The bit numbers identify each port when they are contained in a structure of all ports, such as in the output assembly. Bit 0 refers to any or all ports

Table 240 - Stratix 5200 Port Assignments

Bit	6 Ports		10 Ports		20 Ports	
	1783-CMS6B	1783-CMS6P	1783-CMS10B	1783-CMS10P, 1783-CMS10DP, 1783-CMS10DN	1783-CMS20DB	1783-CMS20DP, 1783-CMS20DN
0	Any/All ports		Any/All ports		Any/All ports	
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
3	Fa1/3	Gi1/3	Fa1/3	Gi1/3	Fa1/3	Gi1/3
4	Fa1/4	Gi1/4	Fa1/4	Gi1/4	Fa1/4	Gi1/4
5	Fa1/5	Gi1/5	Fa1/5	Gi1/5	Fa1/5	Gi1/5
6	Fa1/6	Gi1/6	Fa1/6	Gi1/6	Fa1/6	Gi1/6
7			Fa1/7	Gi1/7	Fa1/7	Gi1/7
8			Fa1/8	Gi1/8	Fa1/8	Gi1/8
9			Fa1/9	Gi1/9	Fa1/9	Gi1/9
10			Fa1/10	Gi1/10	Fa1/10	Gi1/10
11					Fa1/11	Gi1/11
12					Fa1/12	Gi1/12
13					Fa1/13	Gi1/13
14					Fa1/14	Gi1/14
15					Fa1/15	Gi1/15
16					Fa1/16	Gi1/16
17					Fa1/17	Gi1/17
18					Fa1/18	Gi1/18
19					Fa1/19	Gi1/19
20					Fa1/20	Gi1/20

For the Statix 5800 switch:

- The 10-port column shows port assignments for a 10-port base switch with no expansion module attached.
- The 18-port column shows port assignments for a 10-port base switch with an 8-port expansion module attached.
- The 26-port column shows port assignments for a 10-port base switch with a 16-port expansion module attached.

Table 241 - Stratix 5800 Port Assignments

Bit	10 Ports	18 Ports	26 Ports
0	Any/All ports	Any/All ports	Any/All ports
1	Gi1/1	Gi1/1	Gi1/1
2	Gi1/2	Gi1/2	Gi1/2
3	Gi1/3	Gi1/3	Gi1/3
4	Gi1/4	Gi1/4	Gi1/4
5	Gi1/5	Gi1/5	Gi1/5
6	Gi1/6	Gi1/6	Gi1/6
7	Gi1/7	Gi1/7	Gi1/7
8	Gi1/8	Gi1/8	Gi1/8
9	Gi1/9	Gi1/9	Gi1/9
10	Gi1/10	Gi1/10	Gi1/10
11		Gi2/1	Gi2/1
12		Gi2/2	Gi2/2
13		Gi2/3	Gi2/3
14		Gi2/4	Gi2/4
15		Gi2/5	Gi2/5
16		Gi2/6	Gi2/6
17		Gi2/7	Gi2/7
18		Gi2/8	Gi2/8
19			Gi2/9
20			Gi2/10
21			Gi2/11
22			Gi2/12
23			Gi2/13
24			Gi2/14
25			Gi2/15
26			Gi2/16

Port Numbering

Topic	Page
Switch Port Numbering	377
Expansion Module Port Numbering	382

Switch Port Numbering

The port ID consists of the following:

- Port type (Gigabit Ethernet)
- Unit number (always 1 for base unit)
- Port number (1...10)

Gigabit Ethernet is abbreviated as Gi.

Table 242 - Stratix 5200 Switch Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-CMS6B	6-port switch, 4 copper 100 ports, 2 SFP 100/1000 slots, base FW	1 2 3 4 5 6	Gi1/1 Gi1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-CMS6P	6-port switch, 4 copper 100/1000 ports, 2 SFP 100/1000 slots, fullFW	1 2 3 4 5 6	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6
1783-CMS10B	10-port switch, 8 copper 100 ports, 2 Combo 100/1000 ports, base FW	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-CMS10P	10-port switch, 8 copper 100/1000 ports, 2 Combo 100/1000 ports, full FW	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10

Table 242 - Stratix 5200 Switch Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-CMS10DP	10-port switch, 8 copper 100/1000 ports, 2 Combo 100/1000 ports, full FW, DLR	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-CMS10DN	10-port switch, 8 copper 100/1000 ports, 2 Combo 100/1000 ports, full FW, DLR, PRP, NAT	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10

Table 242 - Stratix 5200 Switch Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-CMS20DB	20-port switch, 18 copper 100 ports, 2 Combo 100/1000 ports, base FW, DLR	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	Gi1/1 Gi1/2 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-CMS20DP	20-port switch, 18 copper 100/1000 ports, 2 Combo 100/1000 ports, full FW, DLR	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-CMS20DN	20-port switch, 18 copper 100/1000 ports, 2 Combo 100/1000 ports, full FW, DLR, PRP, NAT	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

The port ID consists of the following:

- Port type (Gigabit Ethernet)
- Unit number (always 1 for base unit)
- Port number (1...10)

Gigabit Ethernet is abbreviated as Gi

Table 243 - Stratix 5800 Switch Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MMS10B	10-port (8 Ethernet ports, 2 SFP ports), non-expandable base switch, Layer 2 firmware	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10BE	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), non-expandable base switch, Layer 2 firmware	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10	10-port (8 Ethernet ports, 2 SFP ports), expandable base switch, Layer 2 firmware	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10E	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), expandable base switch, Layer 2 firmware	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10R	10-port (8 Ethernet ports, 2 SFP ports), expandable base switch, Layer 3 firmware	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10

Table 243 - Stratix 5800 Switch Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MMS10ER	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), expandable base switch, Layer 3 firmware	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10EA	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), expandable base switch, Layer 2 firmware, advanced feature support	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10EAR	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), expandable base switch, Layer 3 firmware, advanced feature support	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10

Expansion Module Port Numbering

The port ID consists of the following:

- Port type (Gigabit Ethernet)
- Unit number (always 2 for expansion module)
- Port number (1...8 or 1...16)

Gigabit Ethernet is abbreviated as Gi.

Table 244 - Stratix 5800 Expansion Module Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MMX8T	8-port (8 Ethernet ports) expansion module	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX8E	8-port (8 Ethernet PoE/PoE+ ports) expansion module	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX8S	8-port (8 SFP ports) expansion module	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX6T2S	8-port (6 Ethernet ports, 2 SFP ports) expansion module	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX16T	16-port (16 Ethernet ports) expansion module	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8 Gi2/9 Gi2/10 Gi2/11 Gi2/12 Gi2/13 Gi2/14 Gi2/15 Gi2/16

Table 244 - Stratix 5800 Expansion Module Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MMX16E	16-port (16 Ethernet PoE/PoE+ ports) expansion module	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8 Gi2/9 Gi2/10 Gi2/11 Gi2/12 Gi2/13 Gi2/14 Gi2/15 Gi2/16
1783-MMX14T2S	16-port (14 Ethernet, 2 SFP ports) expansion module	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8 Gi2/9 Gi2/10 Gi2/11 Gi2/12 Gi2/13 Gi2/14 Gi2/15 Gi2/16
1783-MMX8EA	8-port (8 Ethernet PoE/PoE+ ports) expansion module, advanced feature support	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX8SA	8-port (8 SFP ports) expansion module, advanced feature support	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8

Notes:

MODBUS Register Lists

Topic	Page
Stratix 5200 6-port Register Files	385
Stratix 5200 10-port Register Files	386
Stratix 5200 20-port Register Files	387
Stratix 5800 10-port Register Files	389
Stratix 5800 18-port Register Files	390
Stratix 5800 26-port Register Files	393
System Register File	396

Stratix 5200 Register Files

Stratix 5200 6-port Register Files

The following table lists the 6-port register files for the Stratix 5200 Switch.

Table 245 - Stratix 5200 MODBUS 6-port Register Files

Address	Number of Registers	Description	Read/Write	Format
1000	64	Port 1 Name	R	Text
1040	64	Port 2 Name	R	Text
1080	64	Port 3 Name	R	Text
10C0	64	Port 4 Name	R	Text
1100	64	Port 5 Name	R	Text
1140	64	Port 6 Name	R	Text
1180	1	Port 1 State	R	Uint16
1181	1	Port 2 State	R	Uint16
1182	1	Port 3 State	R	Uint16
1183	1	Port 4 State	R	Uint16
1184	1	Port 5 State	R	Uint16
1185	1	Port 6 State	R	Uint16
1186	4	Port 1 Statistics—Number of packets received	R	Uint64
118A	4	Port 2 Statistics—Number of packets received	R	Uint64
118E	4	Port 3 Statistics—Number of packets received	R	Uint64
1192	4	Port 4 Statistics—Number of packets received	R	Uint64
1196	4	Port 5 Statistics—Number of packets received	R	Uint64
119A	4	Port 6 Statistics—Number of packets received	R	Uint64
119E	4	Port 1 Statistics—Number of packets sent	R	Uint64
11A2	4	Port 2 Statistics—Number of packets sent	R	Uint64
11A6	4	Port 3 Statistics—Number of packets sent	R	Uint64
11AA	4	Port 4 Statistics—Number of packets sent	R	Uint64
11AE	4	Port 5 Statistics—Number of packets sent	R	Uint64
11B2	4	Port 6 Statistics—Number of packets sent	R	Uint64

Stratix 5200 10-port Register Files

The following table lists the 6-port register files for the Stratix 5200 Switch.

Table 246 - Stratix 5200 MODBUS 10-port Register Files

Address	Number of Registers	Description	Read/Write	Format
1000	64	Port 1 Name	R	Text
1040	64	Port 2 Name	R	Text
1080	64	Port 3 Name	R	Text
10C0	64	Port 4 Name	R	Text
1100	64	Port 5 Name	R	Text
1140	64	Port 6 Name	R	Text
1180	64	Port 7 Name	R	Text
11C0	64	Port 8 Name	R	Text
1200	64	Port 9 Name	R	Text
1240	64	Port 10 Name	R	Text
1280	1	Port 1 State	R	Uint16
1281	1	Port 2 State	R	Uint16
1282	1	Port 3 State	R	Uint16
1283	1	Port 4 State	R	Uint16
1284	1	Port 5 State	R	Uint16
1285	1	Port 6 State	R	Uint16
1286	1	Port 7 State	R	Uint16
1287	1	Port 8 State	R	Uint16
1288	1	Port 9 State	R	Uint16
1289	1	Port 10 State	R	Uint16
128A	4	Port 1 Statistics—Number of packets received	R	Uint64
128E	4	Port 2 Statistics—Number of packets received	R	Uint64
1292	4	Port 3 Statistics—Number of packets received	R	Uint64
1296	4	Port 4 Statistics—Number of packets received	R	Uint64
129A	4	Port 5 Statistics—Number of packets received	R	Uint64
129E	4	Port 6 Statistics—Number of packets received	R	Uint64
12A2	4	Port 7 Statistics—Number of packets received	R	Uint64
12A6	4	Port 8 Statistics—Number of packets received	R	Uint64
12AA	4	Port 9 Statistics—Number of packets received	R	Uint64
12AE	4	Port 10 Statistics—Number of packets received	R	Uint64
12B2	4	Port 1 Statistics—Number of packets sent	R	Uint64
12B6	4	Port 2 Statistics—Number of packets sent	R	Uint64
12BA	4	Port 3 Statistics—Number of packets sent	R	Uint64
12BE	4	Port 4 Statistics—Number of packets sent	R	Uint64
12C2	4	Port 5 Statistics—Number of packets sent	R	Uint64
12C6	4	Port 6 Statistics—Number of packets sent	R	Uint64
12CA	4	Port 7 Statistics—Number of packets sent	R	Uint64
12CE	4	Port 8 Statistics—Number of packets sent	R	Uint64
12D2	4	Port 9 Statistics—Number of packets sent	R	Uint64
12D6	4	Port 10 Statistics—Number of packets sent	R	Uint64

Stratix 5200 20-port Register Files

The following table lists the 20-port register files for the Stratix 5200 Switch.

Table 247 - Stratix 5200 MODBUS 20-port Register Files

Address	Number of Registers	Description	Read/Write	Format
1000	64	Port 1 Name	R	Text
1040	64	Port 2 Name	R	Text
1080	64	Port 3 Name	R	Text
10C0	64	Port 4 Name	R	Text
1100	64	Port 5 Name	R	Text
1140	64	Port 6 Name	R	Text
1180	64	Port 7 Name	R	Text
11C0	64	Port 8 Name	R	Text
1200	64	Port 9 Name	R	Text
1240	64	Port 10 Name	R	Text
1280	64	Port 11 Name	R	Text
12C0	64	Port 12 Name	R	Text
1300	64	Port 13 Name	R	Text
1340	64	Port 14 Name	R	Text
1380	64	Port 15 Name	R	Text
13C0	64	Port 16 Name	R	Text
1400	64	Port 17 Name	R	Text
1440	64	Port 18 Name	R	Text
1480	64	Port 19 Name	R	Text
14C0	64	Port 20 Name	R	Text
1500	1	Port 1 State	R	Uint16
1501	1	Port 2 State	R	Uint16
1502	1	Port 3 State	R	Uint16
1503	1	Port 4 State	R	Uint16
1504	1	Port 5 State	R	Uint16
1505	1	Port 6 State	R	Uint16
1506	1	Port 7 State	R	Uint16
1507	1	Port 8 State	R	Uint16
1508	1	Port 9 State	R	Uint16
1509	1	Port 10 State	R	Uint16
150A	1	Port 11 State	R	Uint16
150B	1	Port 12 State	R	Uint16
150C	1	Port 13 State	R	Uint16
150D	1	Port 14 State	R	Uint16
150E	1	Port 15 State	R	Uint16
150F	1	Port 16 State	R	Uint16
1510	1	Port 17 State	R	Uint16
1511	1	Port 18 State	R	Uint16
1512	1	Port 19 State	R	Uint16
1513	1	Port 20 State	R	Uint16
1514	4	Port 1 Statistics—Number of packets received	R	Uint64
1518	4	Port 2 Statistics—Number of packets received	R	Uint64
151C	4	Port 3 Statistics—Number of packets received	R	Uint64
1520	4	Port 4 Statistics—Number of packets received	R	Uint64
1524	4	Port 5 Statistics—Number of packets received	R	Uint64
1528	4	Port 6 Statistics—Number of packets received	R	Uint64
152C	4	Port 7 Statistics—Number of packets received	R	Uint64

Table 247 - Stratix 5200 MODBUS 20-port Register Files

1530	4	Port 8 Statistics—Number of packets received	R	Uint64
1534	4	Port 9 Statistics—Number of packets received	R	Uint64
1538	4	Port 10 Statistics—Number of packets received	R	Uint64
153C	4	Port 11 Statistics—Number of packets received	R	Uint64
1540	4	Port 12 Statistics—Number of packets received	R	Uint64
1544	4	Port 13 Statistics—Number of packets received	R	Uint64
1548	4	Port 14 Statistics—Number of packets received	R	Uint64
154C	4	Port 15 Statistics—Number of packets received	R	Uint64
1550	4	Port 16 Statistics—Number of packets received	R	Uint64
1554	4	Port 17 Statistics—Number of packets received	R	Uint64
1558	4	Port 18Statistics—Number of packets received	R	Uint64
155C	4	Port 19 Statistics—Number of packets received	R	Uint64
1560	4	Port 20 Statistics—Number of packets received	R	Uint64
1564	4	Port 1 Statistics—Number of packets sent	R	Uint64
1568	4	Port 2 Statistics—Number of packets sent	R	Uint64
156C	4	Port 3 Statistics—Number of packets sent	R	Uint64
1570	4	Port 4 Statistics—Number of packets sent	R	Uint64
1574	4	Port 5 Statistics—Number of packets sent	R	Uint64
1578	4	Port 6 Statistics—Number of packets sent	R	Uint64
157C	4	Port 7 Statistics—Number of packets sent	R	Uint64
1580	4	Port 8 Statistics—Number of packets sent	R	Uint64
1584	4	Port 9 Statistics—Number of packets sent	R	Uint64
1588	4	Port 10 Statistics—Number of packets sent	R	Uint64
158C	4	Port 11 Statistics—Number of packets sent	R	Uint64
1590	4	Port 12 Statistics—Number of packets sent	R	Uint64
1594	4	Port 13 Statistics—Number of packets sent	R	Uint64
1598	4	Port 14 Statistics—Number of packets sent	R	Uint64
159C	4	Port 15 Statistics—Number of packets sent	R	Uint64
15A0	4	Port 16 Statistics—Number of packets sent	R	Uint64
15A4	4	Port 17 Statistics—Number of packets sent	R	Uint64
15A8	4	Port 18 Statistics—Number of packets sent	R	Uint64
15AC	4	Port 19 Statistics—Number of packets sent	R	Uint64
15B0	4	Port 20 Statistics—Number of packets sent	R	Uint64

Stratix 5800 Register Files Stratix 5800 10-port Register Files

The following table lists the 10-port register files for the Stratix 5800 Switch.

Table 248 - MODBUS 10-port Register Files

Address	Number of Registers	Description	Read/Write	Format
1000	64	Port 1 Name	R	Text
1040	64	Port 2 Name	R	Text
1080	64	Port 3 Name	R	Text
10C0	64	Port 4 Name	R	Text
1100	64	Port 5 Name	R	Text
1140	64	Port 6 Name	R	Text
1180	64	Port 7 Name	R	Text
11C0	64	Port 8 Name	R	Text
1200	64	Port 9 Name	R	Text
1240	64	Port 10 Name	R	Text
1280	1	Port 1 State	R	Uint16
1281	1	Port 2 State	R	Uint16
1282	1	Port 3 State	R	Uint16
1283	1	Port 4 State	R	Uint16
1284	1	Port 5 State	R	Uint16
1285	1	Port 6 State	R	Uint16
1286	1	Port 7 State	R	Uint16
1287	1	Port 8 State	R	Uint16
1288	1	Port 9 State	R	Uint16
1289	1	Port 10 State	R	Uint16
128A	4	Port 1 Statistics—Number of packets received	R	Uint64
128E	4	Port 2 Statistics—Number of packets received	R	Uint64
1292	4	Port 3 Statistics—Number of packets received	R	Uint64
1296	4	Port 4 Statistics—Number of packets received	R	Uint64
129A	4	Port 5 Statistics—Number of packets received	R	Uint64
129E	4	Port 6 Statistics—Number of packets received	R	Uint64
12A2	4	Port 7 Statistics—Number of packets received	R	Uint64
12A6	4	Port 8 Statistics—Number of packets received	R	Uint64
12AA	4	Port 9 Statistics—Number of packets received	R	Uint64
12AE	4	Port 10 Statistics—Number of packets received	R	Uint64
12B2	4	Port 1 Statistics—Number of packets sent	R	Uint64
12B6	4	Port 2 Statistics—Number of packets sent	R	Uint64
12BA	4	Port 3 Statistics—Number of packets sent	R	Uint64
12BE	4	Port 4 Statistics—Number of packets sent	R	Uint64
12C2	4	Port 5 Statistics—Number of packets sent	R	Uint64
12C6	4	Port 6 Statistics—Number of packets sent	R	Uint64
12CA	4	Port 7 Statistics—Number of packets sent	R	Uint64
12CE	4	Port 8 Statistics—Number of packets sent	R	Uint64
12D2	4	Port 9 Statistics—Number of packets sent	R	Uint64
12D6	4	Port 10 Statistics—Number of packets sent	R	Uint64
12DA	4	Port 1 Statistics—Number of bytes received	R	Uint64
12DE	4	Port 2 Statistics—Number of bytes received	R	Uint64
12E2	4	Port 3 Statistics—Number of bytes received	R	Uint64
12E6	4	Port 4 Statistics—Number of bytes received	R	Uint64
12EA	4	Port 5 Statistics—Number of bytes received	R	Uint64
12EE	4	Port 6 Statistics—Number of bytes received	R	Uint64
12F2	4	Port 7 Statistics—Number of bytes received	R	Uint64

Table 248 - MODBUS 10-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
12F6	4	Port 8 Statistics—Number of bytes received	R	Uint64
12FA	4	Port 9 Statistics—Number of bytes received	R	Uint64
12FE	4	Port 10 Statistics—Number of bytes received	R	Uint64
1302	4	Port 1 Statistics—Number of bytes sent	R	Uint64
1306	4	Port 2 Statistics—Number of bytes sent	R	Uint64
130A	4	Port 3 Statistics—Number of bytes sent	R	Uint64
130E	4	Port 4 Statistics—Number of bytes sent	R	Uint64
1312	4	Port 5 Statistics—Number of bytes sent	R	Uint64
1316	4	Port 6 Statistics—Number of bytes sent	R	Uint64
131A	4	Port 7 Statistics—Number of bytes sent	R	Uint64
131E	4	Port 8 Statistics—Number of bytes sent	R	Uint64
1322	4	Port 9 Statistics—Number of bytes sent	R	Uint64
1326	4	Port 10 Statistics—Number of bytes sent	R	Uint64

Stratix 5800 18-port Register Files

The following table lists the 18-port register files for the Stratix 5800 Switch.

Table 249 - 18-port Register Files

Address	Number of Registers	Description	Read/Write	Format
1000	64	Port 1 Name	R	Text
1040	64	Port 2 Name	R	Text
1080	64	Port 3 Name	R	Text
10C0	64	Port 4 Name	R	Text
1100	64	Port 5 Name	R	Text
1140	64	Port 6 Name	R	Text
1180	64	Port 7 Name	R	Text
11C0	64	Port 8 Name	R	Text
1200	64	Port 9 Name	R	Text
1240	64	Port 10 Name	R	Text
1280	64	Port 11 Name	R	Text
12C0	64	Port 12 Name	R	Text
1300	64	Port 13 Name	R	Text
1340	64	Port 14 Name	R	Text
1380	64	Port 15 Name	R	Text
13C0	64	Port 16 Name	R	Text
1400	64	Port 17 Name	R	Text
1440	64	Port 18 Name	R	Text
1480	1	Port 1 State	R	Uint16
1481	1	Port 2 State	R	Uint16
1482	1	Port 3 State	R	Uint16
1483	1	Port 4 State	R	Uint16
1484	1	Port 5 State	R	Uint16
1485	1	Port 6 State	R	Uint16
1486	1	Port 7 State	R	Uint16
1487	1	Port 8 State	R	Uint16
1488	1	Port 9 State	R	Uint16
1489	1	Port 10 State	R	Uint16
148A	1	Port 11 State	R	Uint16
148B	1	Port 12 State	R	Uint16

Table 249 - 18-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
148C	1	Port 13 State	R	Uint16
148D	1	Port 14 State	R	Uint16
148E	1	Port 15 State	R	Uint16
148F	1	Port 16 State	R	Uint16
1490	1	Port 17 State	R	Uint16
1491	1	Port 18 State	R	Uint16
1492	4	Port 1 Statistics—Number of packets received	R	Uint64
1496	4	Port 2 Statistics—Number of packets received	R	Uint64
149A	4	Port 3 Statistics—Number of packets received	R	Uint64
149E	4	Port 4 Statistics—Number of packets received	R	Uint64
14A2	4	Port 5 Statistics—Number of packets received	R	Uint64
14A6	4	Port 6 Statistics—Number of packets received	R	Uint64
14AA	4	Port 7 Statistics—Number of packets received	R	Uint64
14AE	4	Port 8 Statistics—Number of packets received	R	Uint64
14BA	4	Port 9 Statistics—Number of packets received	R	Uint64
14BE	4	Port 10 Statistics—Number of packets received	R	Uint64
14C2	4	Port 11 Statistics—Number of packets received	R	Uint64
14C6	4	Port 12 Statistics—Number of packets received	R	Uint64
14CA	4	Port 13 Statistics—Number of packets received	R	Uint64
14CE	4	Port 14 Statistics—Number of packets received	R	Uint64
14D2	4	Port 15 Statistics—Number of packets received	R	Uint64
14D6	4	Port 16 Statistics—Number of packets received	R	Uint64
14DA	4	Port 17 Statistics—Number of packets received	R	Uint64
14DE	4	Port 18 Statistics—Number of packets received	R	Uint64
14E2	4	Port 1 Statistics—Number of packets sent	R	Uint64
14E6	4	Port 2 Statistics—Number of packets sent	R	Uint64
14EA	4	Port 3 Statistics—Number of packets sent	R	Uint64
14EE	4	Port 4 Statistics—Number of packets sent	R	Uint64
14F2	4	Port 5 Statistics—Number of packets sent	R	Uint64
14F6	4	Port 6 Statistics—Number of packets sent	R	Uint64
14FA	4	Port 7 Statistics—Number of packets sent	R	Uint64
14FE	4	Port 8 Statistics—Number of packets sent	R	Uint64
1502	4	Port 9 Statistics—Number of packets sent	R	Uint64
1506	4	Port 10 Statistics—Number of packets sent	R	Uint64
150A	4	Port 11 Statistics—Number of packets sent	R	Uint64
1506	4	Port 12 Statistics—Number of packets sent	R	Uint64
150A	4	Port 13 Statistics—Number of packets sent	R	Uint64
150E	4	Port 14 Statistics—Number of packets sent	R	Uint64
1512	4	Port 15 Statistics—Number of packets sent	R	Uint64
1516	4	Port 16 Statistics—Number of packets sent	R	Uint64
151A	4	Port 17 Statistics—Number of packets sent	R	Uint64
151E	4	Port 18 Statistics—Number of packets sent	R	Uint64
1522	4	Port 1 Statistics—Number of bytes received	R	Uint64
1526	4	Port 2 Statistics—Number of bytes received	R	Uint64
152A	4	Port 3 Statistics—Number of bytes received	R	Uint64
152E	4	Port 4 Statistics—Number of bytes received	R	Uint64
1532	4	Port 5 Statistics—Number of bytes received	R	Uint64
1536	4	Port 6 Statistics—Number of bytes received	R	Uint64
153A	4	Port 7 Statistics—Number of bytes received	R	Uint64
153E	4	Port 8 Statistics—Number of bytes received	R	Uint64
1542	4	Port 9 Statistics—Number of bytes received	R	Uint64

Table 249 - 18-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
1546	4	Port 10 Statistics—Number of bytes received	R	Uint64
154A	4	Port 11 Statistics—Number of bytes received	R	Uint64
154E	4	Port 12 Statistics—Number of bytes received	R	Uint64
1552	4	Port 13 Statistics—Number of bytes received	R	Uint64
1556	4	Port 14 Statistics—Number of bytes received	R	Uint64
155A	4	Port 15 Statistics—Number of bytes received	R	Uint64
155E	4	Port 16 Statistics—Number of bytes received	R	Uint64
1562	4	Port 17 Statistics—Number of bytes received	R	Uint64
1566	4	Port 18 Statistics—Number of bytes received	R	Uint64
156A	4	Port 1 Statistics—Number of bytes sent	R	Uint64
156E	4	Port 2 Statistics—Number of bytes sent	R	Uint64
1572	4	Port 3 Statistics—Number of bytes sent	R	Uint64
1576	4	Port 4 Statistics—Number of bytes sent	R	Uint64
157A	4	Port 5 Statistics—Number of bytes sent	R	Uint64
157E	4	Port 6 Statistics—Number of bytes sent	R	Uint64
1582	4	Port 7 Statistics—Number of bytes sent	R	Uint64
1586	4	Port 8 Statistics—Number of bytes sent	R	Uint64
158A	4	Port 9 Statistics—Number of bytes sent	R	Uint64
158E	4	Port 10 Statistics—Number of bytes sent	R	Uint64
1592	4	Port 11 Statistics—Number of bytes sent	R	Uint64
1596	4	Port 12 Statistics—Number of bytes sent	R	Uint64
159A	4	Port 13 Statistics—Number of bytes sent	R	Uint64
159E	4	Port 14 Statistics—Number of bytes sent	R	Uint64
15A2	4	Port 15 Statistics—Number of bytes sent	R	Uint64
15A6	4	Port 16 Statistics—Number of bytes sent	R	Uint64
15AA	4	Port 17 Statistics—Number of bytes sent	R	Uint64
15AE	4	Port 18 Statistics—Number of bytes sent	R	Uint64

Stratix 5800 26-port Register Files

The following table lists the 26-port register files for the Stratix 5800 Switch.

Table 250 - MODBUS 26-port Register Files

Address	Number of Registers	Description	Read/Write	Format
1000	64	Port 1 Name	**R**	Text
1040	64	Port 2 Name	R	Text
1080	64	Port 3 Name	R	Text
10C0	64	Port 4 Name	R	Text
1100	64	Port 5 Name	R	Text
1140	64	Port 6 Name	R	Text
1180	64	Port 7 Name	R	Text
11C0	64	Port 8 Name	R	Text
1200	64	Port 9 Name	R	Text
1240	64	Port 10 Name	R	Text
1280	64	Port 11 Name	R	Text
12C0	64	Port 12 Name	R	Text
1300	64	Port 13 Name	R	Text
1340	64	Port 14 Name	R	Text
1380	64	Port 15 Name	R	Text
13C0	64	Port 16 Name	R	Text
1400	64	Port 17 Name	R	Text
1440	64	Port 18 Name	R	Text
1480	64	Port 19 Name	R	Text
14C0	64	Port 20 Name	R	Text
1500	64	Port 21 Name	R	Text
1540	64	Port 22 Name	R	Text
1580	64	Port 23 Name	R	Text
15C0	64	Port 24 Name	R	Text
1600	64	Port 25 Name	R	Text
1640	64	Port 26 Name	R	Text
1680	1	Port 1 State	R	Uint16
1681	1	Port 2 State	R	Uint16
1682	1	Port 3 State	R	Uint16
1683	1	Port 4 State	R	Uint16
1684	1	Port 5 State	R	Uint16
1685	1	Port 6 State	R	Uint16
1686	1	Port 7 State	R	Uint16
1687	1	Port 8 State	R	Uint16
1688	1	Port 9 State	R	Uint16
1689	1	Port 10 State	R	Uint16
168A	1	Port 11 State	R	Uint16
168B	1	Port 12 State	R	Uint16
168C	1	Port 13 State	R	Uint16
168D	1	Port 14 State	R	Uint16
168E	1	Port 15 State	R	Uint16
168F	1	Port 16 State	R	Uint16
1690	1	Port 17 State	R	Uint16
1691	1	Port 18 State	R	Uint16
1692	1	Port 19 State	R	Uint16
1693	1	Port 20 State	R	Uint16
1694	1	Port 21 State	R	Uint16
1695	1	Port 22 State	R	Uint16

Table 250 - MODBUS 26-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
1696	1	Port 23 State	R	Uint16
1697	1	Port 24 State	R	Uint16
1698	1	Port 25 State	R	Uint16
1699	1	Port 26 State	R	Uint16
169A	4	Port 1 Statistics—Number of packets received	R	Uint64
169E	4	Port 2 Statistics—Number of packets received	R	Uint64
16A2	4	Port 3 Statistics—Number of packets received	R	Uint64
16A6	4	Port 4 Statistics—Number of packets received	R	Uint64
16AA	4	Port 5 Statistics—Number of packets received	R	Uint64
16AE	4	Port 6 Statistics—Number of packets received	R	Uint64
16B2	4	Port 7 Statistics—Number of packets received	R	Uint64
16B6	4	Port 8 Statistics—Number of packets received	R	Uint64
16BA	4	Port 9 Statistics—Number of packets received	R	Uint64
16BE	4	Port 10 Statistics—Number of packets received	R	Uint64
16C2	4	Port 11 Statistics—Number of packets received	R	Uint64
16C6	4	Port 12 Statistics—Number of packets received	R	Uint64
16CA	4	Port 13 Statistics—Number of packets received	R	Uint64
16CE	4	Port 14 Statistics—Number of packets received	R	Uint64
16D2	4	Port 15 Statistics—Number of packets received	R	Uint64
16D6	4	Port 16 Statistics—Number of packets received	R	Uint64
16DA	4	Port 17 Statistics—Number of packets received	R	Uint64
16DE	4	Port 18Statistics—Number of packets received	R	Uint64
16E2	4	Port 19 Statistics—Number of packets received	R	Uint64
16E6	4	Port 20 Statistics—Number of packets received	R	Uint64
16EA	4	Port 21 Statistics—Number of packets received	R	Uint64
16EE	4	Port 22 Statistics—Number of packets received	R	Uint64
16F2	4	Port 23 Statistics—Number of packets received	R	Uint64
16F6	4	Port 24 Statistics—Number of packets received	R	Uint64
16FA	4	Port 25 Statistics—Number of packets received	R	Uint64
16FE	4	Port 26 Statistics—Number of packets received	R	Uint64
1702	4	Port 1 Statistics—Number of packets sent	R	Uint64
1706	4	Port 2 Statistics—Number of packets sent	R	Uint64
170A	4	Port 3 Statistics—Number of packets sent	R	Uint64
170E	4	Port 4 Statistics—Number of packets sent	R	Uint64
1712	4	Port 5 Statistics—Number of packets sent	R	Uint64
1716	4	Port 6 Statistics—Number of packets sent	R	Uint64
171A	4	Port 7 Statistics—Number of packets sent	R	Uint64
171E	4	Port 8 Statistics—Number of packets sent	R	Uint64
1722	4	Port 9 Statistics—Number of packets sent	R	Uint64
1726	4	Port 10 Statistics—Number of packets sent	R	Uint64
172A	4	Port 11 Statistics—Number of packets sent	R	Uint64
172E	4	Port 12 Statistics—Number of packets sent	R	Uint64
1732	4	Port 13 Statistics—Number of packets sent	R	Uint64
1736	4	Port 14 Statistics—Number of packets sent	R	Uint64
173A	4	Port 15 Statistics—Number of packets sent	R	Uint64
173E	4	Port 16 Statistics—Number of packets sent	R	Uint64
1742	4	Port 17 Statistics—Number of packets sent	R	Uint64
1746	4	Port 18 Statistics—Number of packets sent	R	Uint64
174A	4	Port 19 Statistics—Number of packets sent	R	Uint64
174E	4	Port 20 Statistics—Number of packets sent	R	Uint64
1752	4	Port 21 Statistics—Number of packets sent	R	Uint64

Table 250 - MODBUS 26-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
1756	4	Port 22 Statistics—Number of packets sent	R	Uint64
175A	4	Port 23 Statistics—Number of packets sent	R	Uint64
175E	4	Port 24 Statistics—Number of packets sent	R	Uint64
1762	4	Port 25 Statistics—Number of packets sent	R	Uint64
1766	4	Port 26 Statistics—Number of packets sent	R	Uint64
176A	4	Port 1 Statistics—Number of bytes received	R	Uint64
176E	4	Port 2 Statistics—Number of bytes received	R	Uint64
1772	4	Port 3 Statistics—Number of bytes received	R	Uint64
1776	4	Port 4 Statistics—Number of bytes received	R	Uint64
177A0	4	Port 5 Statistics—Number of bytes received	R	Uint64
177E	4	Port 6 Statistics—Number of bytes received	R	Uint64
1782	4	Port 7 Statistics—Number of bytes received	R	Uint64
1786	4	Port 8 Statistics—Number of bytes received	R	Uint64
178A	4	Port 9 Statistics—Number of bytes received	R	Uint64
178E	4	Port 10 Statistics—Number of bytes received	R	Uint64
1792	4	Port 11 Statistics—Number of bytes received	R	Uint64
1796	4	Port 12 Statistics—Number of bytes received	R	Uint64
179A	4	Port 13 Statistics—Number of bytes received	R	Uint64
179E	4	Port 14 Statistics—Number of bytes received	R	Uint64
17A2	4	Port 15 Statistics—Number of bytes received	R	Uint64
17A6	4	Port 16 Statistics—Number of bytes received	R	Uint64
17AA	4	Port 17 Statistics—Number of bytes received	R	Uint64
17AE	4	Port 18 Statistics—Number of bytes received	R	Uint64
17B2	4	Port 19 Statistics—Number of bytes received	R	Uint64
17B6	4	Port 20 Statistics—Number of bytes received	R	Uint64
17BA	4	Port 21 Statistics—Number of bytes received	R	Uint64
17BE	4	Port 22 Statistics—Number of bytes received	R	Uint64
17C2	4	Port 23 Statistics—Number of bytes received	R	Uint64
17C6	4	Port 24 Statistics—Number of bytes received	R	Uint64
17CA	4	Port 25 Statistics—Number of bytes received	R	Uint64
17CE	4	Port 26 Statistics—Number of bytes received	R	Uint64
17D2	4	Port 1 Statistics—Number of bytes sent	R	Uint64
17D6	4	Port 2 Statistics—Number of bytes sent	R	Uint64
17DA	4	Port 3 Statistics—Number of bytes sent	R	Uint64
17DE	4	Port 4 Statistics—Number of bytes sent	R	Uint64
17E2	4	Port 5 Statistics—Number of bytes sent	R	Uint64
17E6	4	Port 6 Statistics—Number of bytes sent	R	Uint64
17EA	4	Port 7 Statistics—Number of bytes sent	R	Uint64
17EE	4	Port 8 Statistics—Number of bytes sent	R	Uint64
17F2	4	Port 9 Statistics—Number of bytes sent	R	Uint64
17F6	4	Port 10 Statistics—Number of bytes sent	R	Uint64
17FA	4	Port 11 Statistics—Number of bytes sent	R	Uint64
17FE	4	Port 12 Statistics—Number of bytes sent	R	Uint64
1802	4	Port 13 Statistics—Number of bytes sent	R	Uint64
1806	4	Port 14 Statistics—Number of bytes sent	R	Uint64
180A	4	Port 15 Statistics—Number of bytes sent	R	Uint64
180E	4	Port 16 Statistics—Number of bytes sent	R	Uint64
1812	4	Port 17 Statistics—Number of bytes sent	R	Uint64
1816	4	Port 18 Statistics—Number of bytes sent	R	Uint64
181A	4	Port 19 Statistics—Number of bytes sent	R	Uint64
181E	4	Port 20 Statistics—Number of bytes sent	R	Uint64

Table 250 - MODBUS 26-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
1822	4	Port 21 Statistics—Number of bytes sent	R	Uint64
1826	4	Port 22 Statistics—Number of bytes sent	R	Uint64
182A	4	Port 23 Statistics—Number of bytes sent	R	Uint64
182E	4	Port 24 Statistics—Number of bytes sent	R	Uint64
1912	4	Port 25 Statistics—Number of bytes sent	R	Uint64
1916	4	Port 26 Statistics—Number of bytes sent	R	Uint64

System Register File

The following table shows the details of the system register file.

Table 251 - MODBUS System Register File

Address	Number of Registers	Description	Read/Write	Format
800	64	Product ID	R	Text
840	64	Software Image Name	R	Text
880	64	Software Image Version	R	Text
8C0	64	Host Name	R	Text
900	64	Alarm 1—Description	R	Text
940	64	Alarm 2—Description	R	Text
980	1	Alarm 1—Status	R	Uint16
981	1	Alarm 2—Status	R	Uint16
982	1	Number of 10/100 Ethernet Ports	R	Uint16
983	1	Number of Gig Ethernet Ports	R	Uint16
984	1	Number of Alarms	R	Uint16
985	1	Number of Power Supplies	R	Uint16
986	1	PS1—Status	R	Uint16
987	1	PS2—Status	R	Uint16
988	1	System Temperature (in Celsius)	R	Uint16

History of Changes

This appendix contains the new or updated information for each revision of this publication. These lists include substantive updates only and are not intended to reflect all changes. Translated versions are not always available for each revision.

Change Log

1783-UM012M-EN-P, October 2024

Change
Supported Catalog Numbers and Software for Switch Features
Associate ACLs with Interfaces
Configure EIGRP via the WebUI
Configure Interface General
Add an HSR Ring via the WebUI
Configure HSRP via the WebUI
NetFlow (Stratix 5800 Switch Only)
Requirements and Restrictions
Routing Information Protocol (RIP) (Stratix 5800 Switch Only)
Virtual Routing and Forward (VRF) (Stratix 5800 Switch Only)
SPAN Page
PTP Modes
PTP Details
Create DHCP Pool
Configure FPGA Profiles in WebUI
Reload the Switch Via the WebUI
Configure SNMP Users and Authentication
Security Requirements (IEC-62443-4-2)
Time

1783-UM012L-EN-P, January 2024

Change
Device Level Ring (DLR) Topology
DLR Port Choices
Secure Digital (SD) Card
Software Upgrade
Upgrade Mode
Destination

1783-UM012K-EN-P, October 2023

Change
Stratix 5200 Switch Added
Stratix 5200 Switches
Software Features
Hardware Features
Console Ports

1783-UM012K-EN-P, October 2023

Change
Express Setup Button
Account Settings
Create AAA RADIUS Server Group
AAA Advanced-RADIUS Fallback
Device Level Ring (DLR) Topology
Ethernet Ports
Add Port Channel Interface
MACsec (Stratix 5800 Switch Only)
Configure MRP via the WebUI
Configure NAT Instance-Advanced Tab
Configure a Switch as a RedBox via the WebUI
Utility Features
Global Alarm Types
Back Up and Restore Sync Via the WebUI
Reload the Switch Via the WebUI
Secure Digital (SD) Card
Stratix 5200 Boot Order
Stratix 5800 Boot Order
Software Upgrade
Device Level Ring (DLR)
HSRP (Stratix 5800 Switch Only)
Media Redundancy Protocol (MRP)
PROFINET
Parallel Redundancy Protocol (PRP)
Stratix 5200 Status Indicators
Stratix 5200 Data Types
Stratix 5200 Port Assignments
Stratix 5200 Switch Port Numbering
MODBUS Register Lists

1783-UM012J-EN-P, February 2023

Change
Added Media Redundancy Protocol (MRP)
Revised Smartports for Multi-port Assignment

1783-UM012I-EN-P, August 2022

Change
Supported Catalog Numbers and Software for Switch Features
Wiring for Alarm Connector
Switch Virtual Interfaces (SVIs)
Back Up and Restore Procedures
Field-programmable Gate Array (FPGA) Profiles

1783-UM012H-EN-P, February 2022

Change
1783-MMS10A Series B, 1783-MMS10AR Series B, and 1783-MMX8TA Series A Catalog Numbers
Supported Catalog Numbers and Software for Switch Features
Monitor PRP- Statistics Tab

1783-UM012G-EN-P, September 2021

Change
Supported Catalog Numbers and Software for Switch Features
Console Ports
High-availability Seamless Redundancy (HSR)
IOx Services
Virtual Router Redundancy Protocol (VRRP)
Device Settings-General
CIP Sync (PTP)
Configure HTTP/HTTPS/Netconf/VTY Access via the WebUI

1783-UM012F-EN-P, May 2021

Change
REP Over Port Channel

1783-UM012E-EN-P, March 2021

Change
Discovery Protocols
Enhanced Interior Gateway Routing Protocol (EIGRP)
Flow-based SPAN (FSPAN)
Hot Standby Router Protocol (HSRP)
Intermediate System-to-Intermediate System (IS-IS)
Multicast Services
Neighbors
PROFINET
PRP Supported on Expansion Module
Quality of Service (QoS)
Remote Switch Port Analyzer (RSPAN)
Routing Information Protocol (RIP)
SDM-Template
Security Requirements (IEC-62443-4-2)
TrustSec
Virtual Router Redundancy Protocol (VRRP)

1783-UM012D-EN-P, December 2020

Change
Flow-based SPAN (FSPAN)
Hot Standby Router Protocol (HSRP)
Remote Switch Port Analyzer (RSPAN)

1783-UM012D-EN-P, December 2020

Change
Routing Information Protocol (RIP)
Virtual Router Redundancy Protocol (VRRP)
SDM-Template
Security Requirements (IEC-62443-4-2)

1783-UM012C-EN-P, July 2020

Change
Discovery Protocols
Enhanced Interior Gateway Routing Protocol (EIGRP)
Intermediate System-to-Intermediate System (IS-IS)
Multicast Services-Layer 3 support
Quality of Service (QoS)-Layer 3 support
Neighbors
TrustSec

1783-UM012B-EN-P, January 2020

Change
AAA Global Configuration
Configure Multiple Ports Simultaneously
Configure VRF-Lite
Logical Interfaces
File Manager
MODBUS (Modicon Communication Bus)
Netconf Yang Configuration
NetFlow
Network Address Translation (NAT)
Parallel Redundancy Protocol (PRP)
SDM-Template
SNMP-V3 User Groups
TrustSec
Port Numbering
MODBUS Register Lists

Numerics

10/100/100 ports 23

A

AAA
about 54
configuration 54
configure via WebUI 55
map 59
method lists 60
policy password 73
access control list. See ACL
access port 94, 107, 178
access the WebUI 44
access VLAN 95, 176
accounts, user 277
ACL
about 75
associate with interface 77
configure via WebUI 75
adapter pinouts 22
add switch to controller project 37
Add-on Profile. See AOP
address pools 245
administrative VLAN, REP 171
administrator
login name 33
password 33, 41
user name 41
alarm actions 212, 215
alarm configuration 217
alarm connector 19, 20
alarm labels 20
alarm profile
about 212
configure via WebUI 213
default 212
alarm relay setup 215
alarm settings
about 214
configure via WebUI 215
alarm status indicators 355
alarm types 212, 214
alarm, input 19
alarm, output 19
allowed VLANs 95
announce interval 234
announce timeout 233
AOP 28
assign VLAN to NAT instance 140
authenticate users 54, 270
Authentication, Authroization, and Accounting. See AAA
authorize users 54
auto QoS 163
auto-MDIX 23
autonegotiation
about 23
configure 94, 98
troubleshoot 348

B

back up configuration 218, 221
BASE-T ports 23
bit numbers 375
Boundary mode 233
BPDU filtering 184
BPDU guard 184
broadcast storm 96
browser
Express Setup 28, 43
requirements for WebUI 43
troubleshoot 348
bundle, debug 343

C

CA Trustpoints 257
cable diagnostics 313
cable schematics
twisted-pair crossover 24
twisted-pair straight through 23
cables
crossover 24
damaged 346
Ethernet and fiber 346
guidelines 23
straight-through 24
CDP 78, 287
certificate authority 257
CIP
about 15, 224
configure via WebUI 224
data 375
device settings 36
enable 36
IP address 36
password 28, 31, 36
status and statistics 293
VLAN 28, 31, 36
CIP Sync time 224, 232
Cisco Discovery Protocol. See CDP
CLI
about 238
modes 238
password 33
run commands via WebUI 238
clients, DHCP 298
clock modes
Boundary 233
End to End Transparent 234
clock settings, monitor 290, 328
command, CLI 238
command-line interface. See CLI
Common Industrial Protocol. See CIP

community strings, SNMP 272
comparison, software 15
configuration
back up and restore via Logix Designer application 221
back up and restore via WebUI 218
configuration software 15
connection faults 99
connection settings 241
connectors 23
alarm 19, 20
dual LC 26
front panel 19
PoE pinout 25
power 19
console port 23
connectors 21
location on switch 18
contacts, normally closed 19
contacts, normally open 19
controller project 37
core dump 342
CPU utilization 326
crossover cables 24
custom Smartport roles 179
customize WebUI dashboard 50

D

dashboard
customize 50
dashlet descriptions 50
data types 357
DB-25 pin 22
DB-9 pin 22
DC power connectors 19
debug bundle 343
default alarm profile 212
default gateway
NAT 137
default gateway IP address 35
default global macro 41
delay request interval 233
device name 33
device settings
configure via Logix Designer application 241
configure via WebUI 239
device settings, CIP 36
device temperature 50
device time
configure via Logix Designer application 232
configure via WebUI 225
set manually 225, 243
set via NTP 243
set via PTP 224, 228
DHCP 35, 41, 245
troubleshoot 347
DHCP clients, monitor 298
DHCP persistence 245, 246
DHCP pools 245
configure via Logix Designer application 250
configure via WebUI 247
DHCP snooping 247
disable switch port 357
discovery protocols 78
DLR
port choices 85
DNS
about 244
add server 244
domain name system. See DNS
download
core files 342
debug bundle 343
driver, USB device 21
dual LC connector 26
dump, core 342
Duplex mode 94, 98
troubleshoot 348
Dynamic Host Control Protocol. See DHCP

E

edge port 169, 171
EIGRP 86
EIP status indicators 354
enable CIP 36
End to End Transparent mode 234
Enhanced Interior Gateway Routing Protocol. See EIGRP
EtherChannels
about 105
configure 109
modes 105
Ethernet ports
configuration via Logix Designer application 98
configure via WebUI 89
Duplex mode 94, 98
fault/program action 99
numbering 377, 379
speed 94, 98
status indicators 355
EtherNet/IP interface 15
EtherNet/IP protocol 178
expansion modules 14
Express Setup
button 29
global macro 41
Long Press mode 32
Medium Press mode 31
modes 27
requirements 28
Short Press mode 30
status indicator 354
via Logix Designer application 37
via WebUI 32
external alarm 214

F

factory default settings 32

fallback, RADIUS 73
fault/program action 99
faults, connection 99
features
hardware 17
software 15
fiber
multimode 26
singlemode 26
File Manager 253
fixed switches 14
flash 221, 222
front panel
connectors 19
overview 18
status indicators 351, 352
FTP/TFTP settings 240
full-duplex 23

G

gateway IP address 35, 41
global alarm actions 215
global alarm configuration 216
global alarm types 214
global macro 41
GMC 289, 290, 327, 328

H

half-duplex 23
hardware features 17
hosts, SNMP 274
HTTP/HTTPS 257

I

ID, management VLAN 35
IEEE 1588 224
IEEE 802.1AB 78
IEEE 802.1D 182
IEEE 802.1s 182
IEEE 802.1w 182
IEEE 802.3 78, 260
IGMP snooping 133
IGMP snooping querier 133
input alarm 19
installation instructions 11
interfaces, logical 105
interfaces, loopback 108
Intermediate System-to-Intermediate System. See IS-IS
IP address
CIP 36
default gateway 35, 41
DHCP 41
NTP server 33
static 41
SVI 200
switch 35, 41
troubleshoot 347
IP address pools 245
IS-IS 118

L

labels, alarm 20
Layer 2 Network Address Translation (L2NAT) 301
LC connector 26
LDAP
server configuration 69
server group configuration 70
LED. See status indicators
Link Layer Discovery Protocol. See LLDP
LLDP 78, 287
llel 315
Logical 105
logical interfaces 105
login name
administrator 33
WebUI user 277
logs, system 340
Long Press mode, Express Setup 27, 32
loopback interfaces 108

M

MAC table 95
macros
default global 41
QoS 163
management interface
NAT 141
management VLAN 41, 200
mask, subnet 35, 36
Medium Press mode, Express Setup 27, 28, 31
memory utilization 325
method lists, AAA 60
mismatch prevention, Smartports 175
MODBUS 257, 307
modes
Access 178
Boundary 227, 233
CLI 238
Duplex 94, 98
End to End Transparent 227, 234
EtherChannel 105
Express Setup 27
Forward 227
PoE 260
Program 99
STP 182
Trunk 178
user security 270
modular switches 14
module-defined data types 357
modules, expansion 14

monitor
CIP status 293
clock settings 290, 328
CPU utilization 326
DHCP clients 298
port status 310, 312
PTP 289, 327
REP 320
status indicators 351, 352
switch memory 325
MRP
about 127
configure via WebUI 131
requirements and restrictions 130
MTU 202
Multi Port Configuration 98
multicast services 133
multimode fiber 26

N

NAT
configuration considerations 142
configuration overview 137
configure via Logix Designer application 152
diagnostics 304 – 306
management interface 141
traffic permits and fixups 141
translation entry types 139
native VLAN 95, 176
neighbors 78, 287
Netconf 258
NetFlow 134
Network Time Protocol. See NTP
network, EtherNet/IP 15
normally closed contacts 19
normally open contacts 19
NTP 243
NTP server 33, 41

O

ODVA 15
Open Shortest Path First (OSPF) Routing Protocol 137
operating system
Express Setup 28, 43
requirements for WebUI 43
OSPF 153
output alarm 19
output bits 357

P

Parallel Redundancy Protocol (PRP) 155
password
administrator 33
CIP 36
CLI 33
password policies 277
password, administrator 41
password, CIP 28, 31
password, policy 73
persistence, DHCP 245, 246
pin
DB-25 22
DB-9 22
ping 344
pinouts
DB-25 pin 22
DB-9 pin 22
PoE 25
PoE
about 260
configure via Logix Designer application 263
configure via WebUI 261
modes 260
pinouts 25
power consumption 50
requirements and restrictions 260
status indicator 353
PoE ports 25
policies, password 277
policy password 73
pools, DHCP 247
pools, IP address 245
pop-up blockers 43
port
configuration 98
states 99
port alarms
configure 217
port assignments for CIP data 375
port channels
about 105
configure 106
port configuration 89, 98
port mirroring
about 187
configure via WebUI 187
requirements and restrictions 187
port numbering 377, 379
port security 95
about 161
configure via Logix Designer application 162
configure via WebUI 161, 164
port speed 23, 94
port state 99
port status indicators 355
port status, monitor 310, 312
port thresholds 96
port types, REP 171
PortFast 94
ports
10/100/1000 23
BASE-T 23
PoE 25
power connectors 19
power consumption, PoE 50
power management 261
Power over Ethernet. See PoE
power status indicators 353
privilege levels, user 277
profile, alarm
about 212
configure via WebUI 213

Program mode 99
project, controller 37
proxy settings 43
PRP 155
  node and VDAN limitations 157
  RedBox 155
  traffic and supervisory frames 157
PTP
  configure via WebUI 232
  monitor 289, 327
PTP modes
  Boundary 233
  End to End Transparent 234

Q

QoS
  about 163
  configure via WebUI 164
  macros 163
  settings 41
Quality of Service. See QoS
querier, IGMP snooping 133

R

RADIUS
  fallback 73
  server configuration 64
  server group configuration 65
rapid commit 202
RedBox 155
relay 19
reload configuration 266
REP
  about 169
  administrative VLAN 171
  configure via WebUI 172
  default configuration 169
  monitor 320
  port types 171
  segment 173
Requirements 130
requirements
  Express Setup 28
  WebUI 43
Resiliency Ethernet Protocol. See REP
restart with factory default settings 32
restore configuration 218, 221
roles, Smartport 175
routing, static
  configure via WebUI 186
routing,static 186
run CLI commands 238

S

schematics, cable 24
screen resolution
  Express Setup 28, 43
  requirements for WebUI 43
SD card
  sync with configuration 221
SD flash 221, 222
security, port 95, 161
segment, REP 173
server
  DNS 244
  NTP 33, 41
server configuration
  LDAP 69
  RADIUS 64
  TACACS+ 67
server group configuration
  LDAP 70
  RADIUS 65
  TACACS+ 68
services, multicast 133
set switch IP address 35
settings
  factory default 32
Setup status indicator 354
SFP modules 26
SFP slots 26
Short Press mode, Express Setup 27, 28, 30
Simple Network Management Protocol. See SNMP
singlemode fiber 26
slots, SFP 26
Smartports
  about 175
  assign via Logix Designer application 181
  assign via WebUI 176
  custom roles 179
  mismatch prevention 175
  requirements and restrictions 175
  roles 175
  VLAN types 176
SNMP
  about 270
  community strings 272
  configure via WebUI 271
  hosts 274
  supported versions 270
  traps 271
SNMPv3 270, 273
snooping, DHCP 247
snooping, IGMP 133
software comparison 15
software features 15
software upgrade 275
software, configuration 15
SPAN
  about 187
  configure via WebUI 187
  requirements and restrictions 187
Spanning Tree Protocol. See STP
specifications, switch 11
speed
  about 23
  configure 94, 98
  troubleshoot 348
SSH 36
static IP address 35, 41
static MAC table 95

static routing
about 186
configure via WebUI 186
status indicators
alarm 355
EIP Mod 354
EIP Net 354
front panel 351, 352
PoE 353
port 355
power 353
setup 354
storm
broadcast 96
unicast 96
STP
about 182
configure via Logix Designer application 185
configure via WebUI 184
modes 182
requirements and restrictions 182
straight-through cable 24
subnet mask 35, 36
subnet translation 140, 149
supported SFP modules 26
SVI 200, 202
switch
installation instructions 11
IP address 41
setup 27
specifications 11
status 286
troubleshoot 346, 347
switched port analyzer. See SPAN
switches, fixed 14
switches, modular 14
sync configuration with SD card 221
sync interval 234
sync limit 234
system logs 340
system report 342

T

TACACS+ server configuration 67
TACACS+ server group configuration 68
Telnet 35
temperature of device 50
thresholds, port 96
time
CIP Sync 224, 232
configure via Logix Designer application 232
configure via WebUI 225, 232
PTP 232
set manually 225, 243
set via NTP 243
set via PTP 228
via PTP 224
time sync information
view via Logix Designer application 235
TLV structures 78
toolbar, WebUI 48
trace route 344
traffic fixups and NAT 141
traffic permits and NAT 141
translation entry types 139
traps, SNMP 271
troubleshoot
core dump 342
debug bundle 343
DHCP 347
IP address problems 347
ping and trace route 344
speed, duplex, and autonegotiation 348
status indicators 351, 352
switch performance 348
system logs 340
system report 342
WebUI 348
wrong IP address 347
trunk port 94, 107, 178
trustpoints 257
TrustSec 190

U

unicast storm 96
upgrade software 275
USB device driver 21
USB-mini console 21
user administration 277
user authentication 270
user name, administrator 41
user password policies 277
user privilege levels 277
user security modes 270
users
authenticate 54
authorize 54
SNMPv3 273
WebUI accounts 277

V

V3 User Groups 272
virtual local area network. See VLAN
VLAN
about 200
access 95
allowed 95
CIP 36
configure via Logix Designer application 205
configure via WebUI 201
for Smartports 176
management 35, 41, 200
native 95
REP administrative 171
support 200
trunking protocol 209
VLAN Trunking Protocol. See VTP
VLANs
assign to NAT instance 140, 148
voice VLAN 176
VTP
about 209
configure via WebUI 210

W

WebUI
AAA wizard 55
access 44
dashboard 50
preferences 49
requirements 43
toolbar 48
troubleshoot 348
user accounts 277
WebUI wizard 55
wire alarm connector 20
wizard, AAA 55

Notes:

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)



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

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

Allen-Bradley, expanding human possibility, FactoryTalk Network Manager, Integrated Architecture, Logix 5000, Rockwell Automation, Rockwell Software, Stratix, and Studio 5000 Logix Designer are trademarks of Rockwell Automation, Inc.

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

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

Microsoft is a trademark of Microsoft Corporation.

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
UNITED KINGDOM: Rockwell Automation Ltd. Pitfield, Kiln Farm Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication 1783-UM012N-EN-P - October 2025
Supersedes Publication 1783-UM012M-EN-P - October 2024

Copyright © 2025 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.