User Manual

Allen-Bradley

Stratix 8000 and 8300 Ethernet Managed Switches

Allen-Bradley • Rockwell Software

Rockwell Automation

Important User Information

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

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

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

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

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

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

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

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

	**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
	**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

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

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

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

New and Updated Information

This table contains the changes made to this revision.

Topic	Page
Updated Device Manager hardware and software requirements	48, 53
New Express Setup window	50, 51
New process for enabling static and connected routing	83, 84
New DeviceManager Web interface	87…139

Notes:

Chapter 3

Switch Software Features

Manage the Switch via the Device Manager Web Interface

Chapter 4

Notes:

This publication describes the embedded software features and tools for configuring and managing Stratix 8000™ and Stratix 8300™ Ethernet managed switches. In addition, this publication provides troubleshooting information to help you resolve basic switch and network issues.

Use this manual if you configure and monitor Stratix 8000 Ethernet managed switches. This manual assumes you understand the following:

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

Studio 5000 Environment

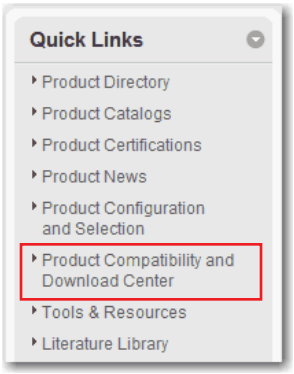
The Studio 5000™ Engineering and Design Environment combines engineering and design elements into a common environment. The first element in the Studio 5000 environment is the Logix Designer application. The Logix Designer application is the rebranding of RSLogix™ 5000 software and continues to be the product to program Logix5000™ controllers for discrete, process, batch, motion, safety, and drive-based solutions.

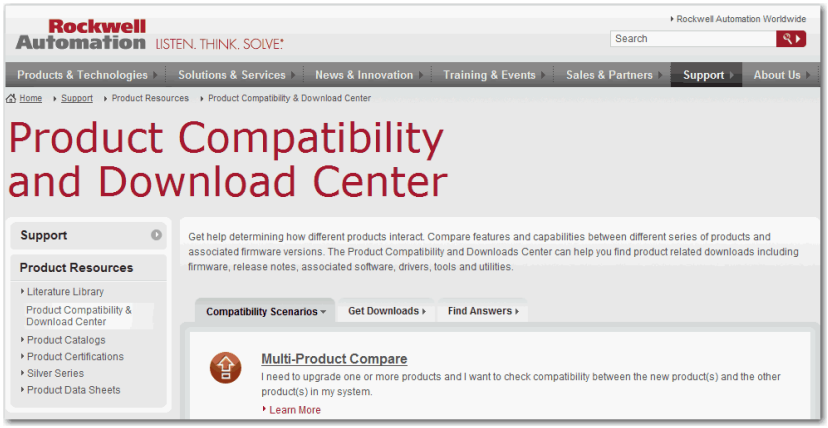
The Studio 5000 environment is the foundation for the future of Rockwell Automation® engineering design tools and capabilities. It is the one place for design engineers to develop all the elements of their control system.

Access Product Release Notes

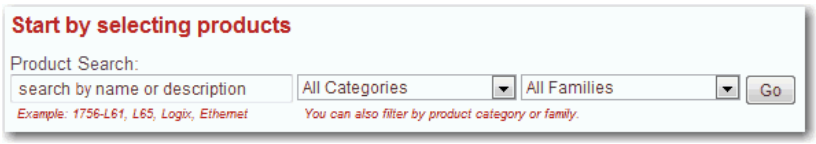
Product release notes are available online within the Product Compatibility and Download Center.

1. From the Quick Links list on http://www.ab.com, choose Product Compatibility and Download Center.





2. From the Compatibility Scenarios tab or the Get Downloads tab, search for and choose your product.



3. Click the download icon  to access product release notes.

Additional Resources

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

Resource	Description
Stratix Ethernet Managed Switches Technical Data, publication 1783-TD001	Provides specification information for the switches.
Stratix 8000 Ethernet Managed Switches Installation Instructions, publication 1783-IN005	Describes how to get started installing and configuring the switch.
Stratix 8000 Ethernet Managed Switches Release Notes, publication 1783-RN002	Lists enhancements and anomalies associated with the released software version.
Device Manager Web interface online help (provided with the switch)	Provides context-sensitive information about configuring and using the switch, including system messages.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, http://www.ab.com	Provides declarations of conformity, certificates, and other certification details.

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

For information about additional software features or further configuration, see these Cisco publications at http://www.Cisco.com:

- Cisco IE-3000 Command Line Reference Manual
- Cisco IE-3000 Software Configuration Guide
- Cisco IE-3000 Switch System Message Guide

Notes:

Install the Switch

ATTENTION: Environment and Enclosure

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

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

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

In addition to this publication, see the following:

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

North American Hazardous Location Approval

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

European Hazardous Location Approval

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

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

WARNING:

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

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

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

Before You Begin

The location where you install the switch must meet these guidelines:

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

  To prevent the switch from overheating, use these minimum clearances:
  - Top and bottom: 105 mm (4.13 in.)
  - Left and right: 90 mm (3.54 in.)
  - Front: 65 mm (2.56 in.)

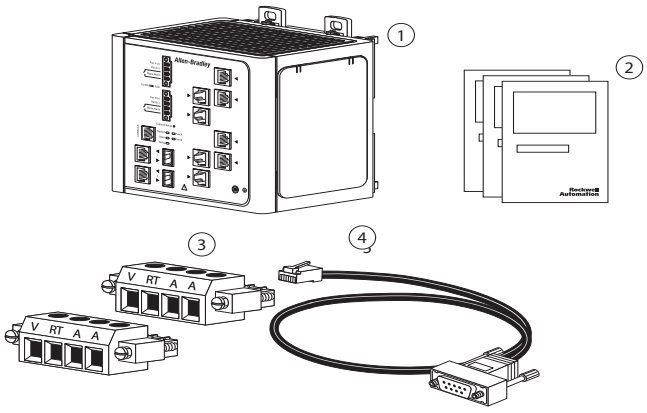
- Temperature surrounding the unit does not exceed 60 °C (140 °F).

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

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

Parts List

Verify that you have these items.



1 1783-MS10T switch(1)

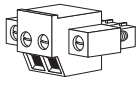
2 Documentation

3 Power and alarm relay connectors (qty. 2)

4 Console cable

(1) The 1783-MS10T switch is shown as only an example.

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



Required Tools and Equipment

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

Obtain these necessary tools and equipment:

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

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

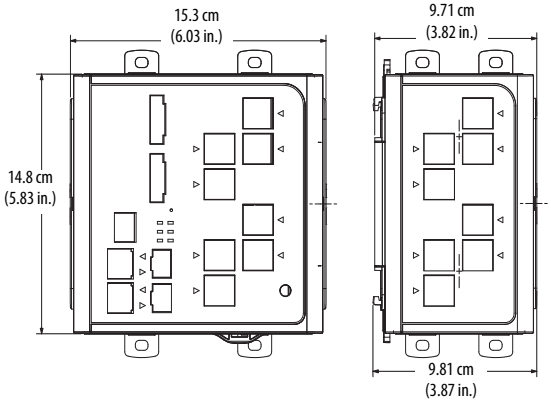
For maximum noise immunity, shielded cables must be used on the uplink ports (Gi1/1 and Gi1/2) on these switches:

- 1783-BMS06TGL
- 1783-BMS06TGA
- 1783-BMS10CGA
- 1783-BMS10CGL
- 1783-BMS10CGN
- 1783-BMS10CGP
- 1783-BMS20CGL
- 1783-BMS20CGN
- 1783-BMS20CGP
- 1783-BMS20CGPK

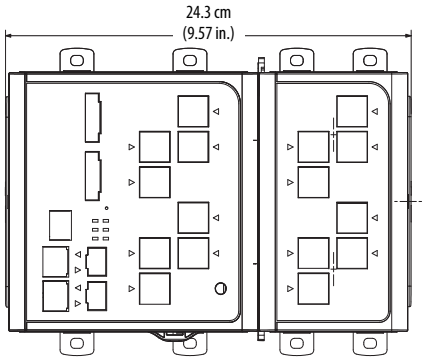
Product Dimensions

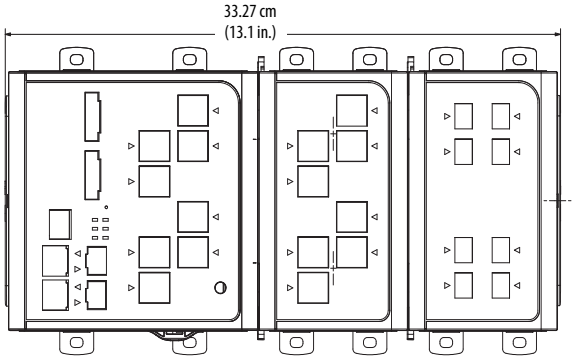
The illustrations below show dimensions for the 1783-MS10T switch and the 1783-MX08T expansion module. Dimensions for all other Stratix 8000 and Stratix 8300 switches and expansion modules are the same as shown below.

Switch and Expansion Module

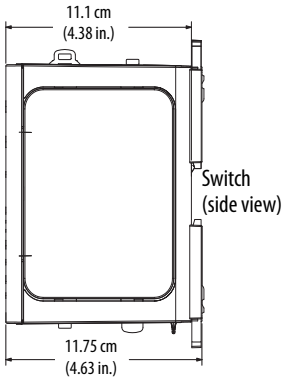


Switch and Expansion Module (mated)





Switch and Expansion Modules (mated)



31801-M

For panel-mounting, the height of the center of the mounting holes on both the top and bottom latches measures 8.73 mm (0.34 in.) above the top surface (or below the bottom surface) of the switch.
On the switch base unit, the tab hole center-to-center spacing is 6.83 cm (2.69 in.).
For expansion modules, the tab hole center-to-center spacing is 4.36 cm (1.72 in.).

Install the Switch

Follow these steps to install the switch.

1. (Optional) Attach expansion modules.
2. Mount the switch on one of the following:
   - DIN rail
   - Wall or panel
3. (Optional) Install an SFP module.
4. Ground the switch.
5. Wire the DC power source for the switch.
6. (Optional) Wire the DC power source for the PoE expansion module.
7. Attach the power and alarm connector.
8. Wire external alarms.
9. Set up the switch initially with Express Setup.
10. Connect to the switch ports:
    - 10/100 copper ports
    - PoE ports
    - Dual-purpose uplink (10/100/1000 and SFP fiber) ports
    - 100BaseFX
11. Install or remove the CompactFlash card.

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

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

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

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

ATTENTION: Prevent Electrostatic Discharge

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

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

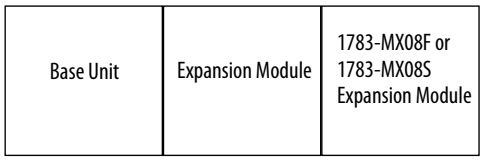
Attach Expansion Modules (optional)

IMPORTANT If you are adding expansion modules, attach the expansion modules to the switch before mounting the switch.

The switch can operate as a standalone device with two uplink ports and four or eight Fast Ethernet ports, or you can increase the number of Fast Ethernet ports by 8 or 16 by connecting expansion modules.

You can install as many as two expansion modules per base unit. However, only one of the two modules can be a 1783-MX08F or 1783-MX08S fiber expansion module.

If you install a 1783-MX08F or 1783-MX08S fiber expansion module, the module must be in the right-most position, as shown below.



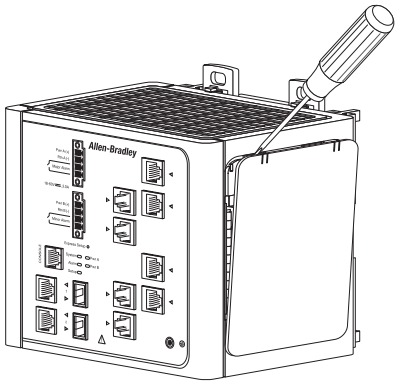
Depending on the mix of switches and expansion modules, you can have as many 24 Fast Ethernet ports.

Follow these steps to connect the expansion modules to the switch.

IMPORTANT You must add expansion modules to the base unit before applying power to the switch. Remove power from the switch when reconfiguring it.

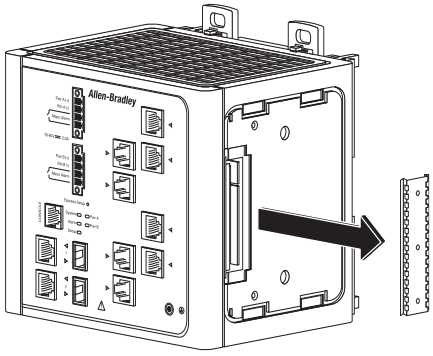
1. Remove the right side panel by firmly grasping both sides of it in the middle and pulling it outward.

   If necessary, use a screwdriver to pry open the side panel.



31779-M

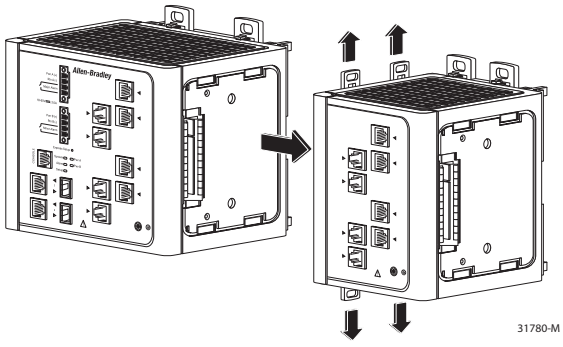
2. Remove the protective EMI-connector cover from the side panel.



31787-M

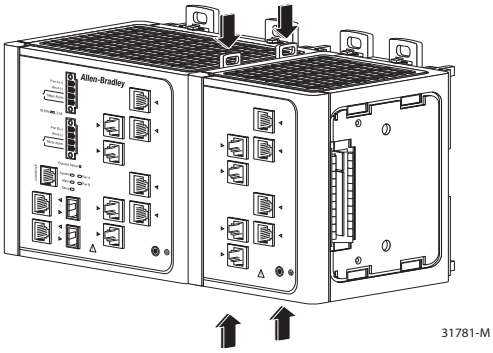
3. Push the upper module latches up and the lower module latches down. Then slide the switch and module together.

   The expansion module is shown with the side panel removed. Do not remove this panel unless you plan to install another module.



31780-M

4. Push the upper and lower module latches in to secure the module to the switch.



5. If you are installing a second module, repeat steps 1...4, but secure the second module to the right side of the first module.

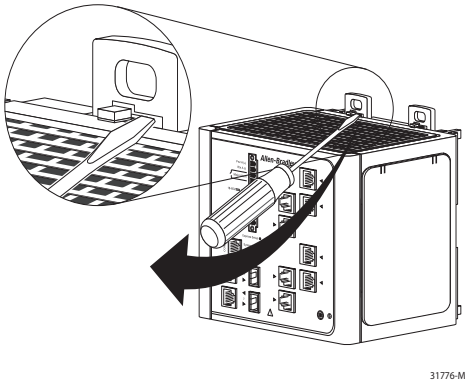
IMPORTANT You cannot install an expansion module to the right of the 1783-MX08F or 1783-MX08S fiber expansion module.

Mount the Switch on a DIN Rail

WARNING: When using DIN rail mounting, additional grounding is also accomplished through the DIN rail to chassis ground. Use zinc plated yellow-chromate steel DIN rail to assist in proper grounding. The use of other DIN rail materials (for example, aluminum or plastic)) that can corrode, oxidize, or are poor conductors, can impede proper grounding. Secure DIN rail to mounting surface approximately every 200 mm (7.8 in.) using end-anchors appropriately and using a washer plate along the entire length of the DIN rail.

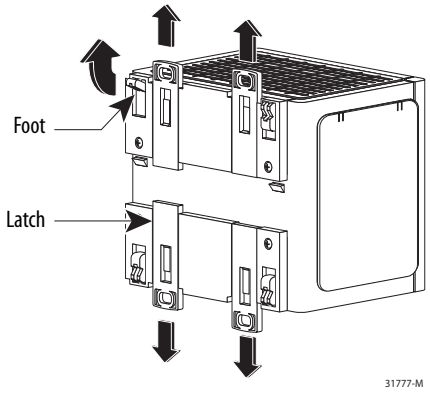
Follow these steps to mount the switch on a DIN rail.

1. Insert a sharp tool, such as a screwdriver, in the space next to the tab, push gently to release the catch, then turn the screwdriver to push the tab out.

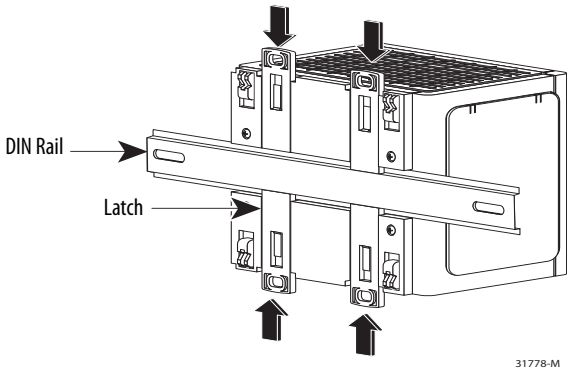


2. If you are using a heavy-duty 35 mm x 15 mm (1.38 in. x 0.59 in.) DIN rail, rotate all feet to the extended positions.

   Otherwise, if you are using 35 mm x 7.5 mm (1.38 in. x 0.30 in.) DIN rail, rotate the feet to the recessed positions.



3. Position the rear panel of the switch directly in front of the DIN rail, making sure that the DIN rail fits in the space between the two latches.



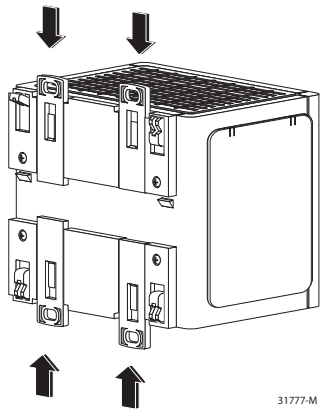
4. Push the DIN rail latches in after the switch is over the DIN rail to secure the switch to the rail.

Mount the Switch on a Wall or Panel

The switch can be mounted on a wall or a panel. You need M5 or #10-24 or #10-32 bolts or screws with 1.27 cm (0.5 in.) O.D. flat washers. This hardware is not provided with the switch.

Follow these steps to mount the switch to a wall or a panel.

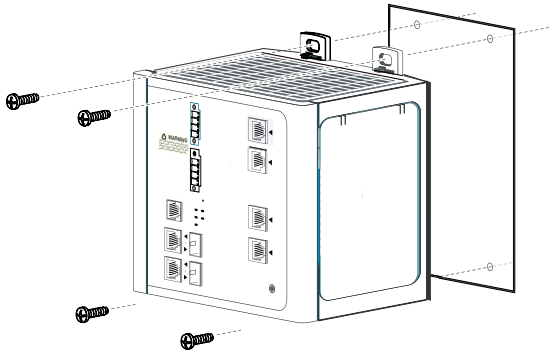
1. If the DIN rail latches are pushed out, push them in so they are fully locked in place.



2. Rotate all feet to their recessed positions so that the switch can mount flat on the wall or pane.

   If greater air circulation around the switch is required, rotate the feet to their extended positions before mounting the switch on the wall.

3. Position the rear panel of the switch against the wall or a panel in the desired location, as shown in this figure.



4. Place M5 or #10-24 or #10-32 bolts or screws with 1.27 cm (0.5 in.) O.D. flat washers through each DIN rail latch, and screw them into the wall.

Install an SFP Module (optional)

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

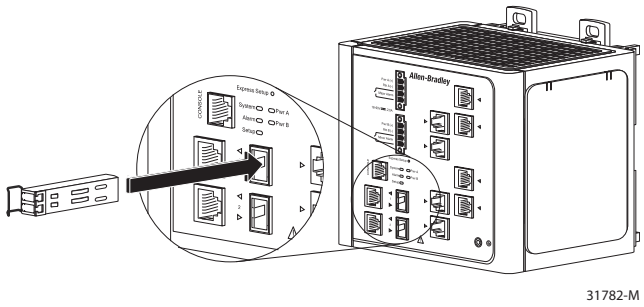
ATTENTION: SFP modules are static sensitive devices. Always use an ESD wrist strap or similar individual grounding device when handling SFP modules.

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

IMPORTANT Using an SFP module other than those provided by Rockwell Automation will disable the switch port.

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

Grasp the module on the sides, and insert it into the switch slot until you feel the connector snap into place.



31782-M

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

Ground the Switch

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

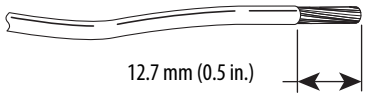
ATTENTION: You must use the external grounding screw on the front of the switch to ground the switch. Use a 5.3 mm^2 (10 AWG) ground wire.

Follow these steps to connect the switch to a protective ground.

1. Use a screwdriver to remove the ground screw from the front panel of the switch.

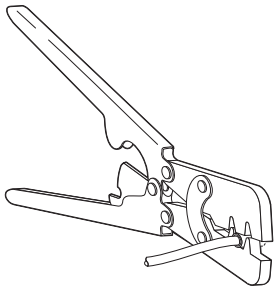
   Store the ground screw for later use.

2. If your ground wire is insulated, use a wire stripping tool to strip the 5.3 mm^2 (10 AWG) ground wire to 12.7 mm (0.5 in.) ± 0.5 mm (0.02 in.).



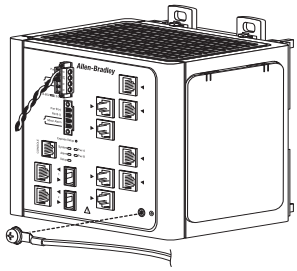
31789-M

3. Insert the ground wire into the ring terminal lug.
4. Use a crimping tool to crimp the ring terminal to the wire.



31790-M

5. Slide the ground screw through the ring terminal.
6. Insert the ground screw into the ground-screw opening on the front panel.



31791-M

7. Use a ratcheting torque screwdriver to tighten the ground screw and ring terminal lug to the switch front panel to 0.96 N•m (8.5 lb•in).
8. Attach the other end of the ground wire to a grounded bare-metal surface, such as a ground bus, or a grounded DIN rail.

Wire the DC Power Source for the Switch

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

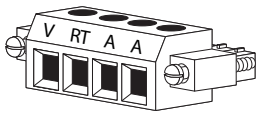
WARNING: To comply with the CE Low Voltage Directive (LVD), this equipment must be powered from a source compliant with the safety extra low voltage (SELV) or protected extra low voltage (PELV).

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

Follow these steps to wire DC power to the switch.

1. Locate the power and alarm relay connector and identify the positive and return DC power connections.

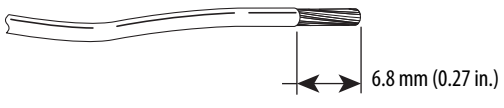
   The positive DC power connection is labeled V, and the negative DC power connection is the adjacent connection labeled RT. Connections labeled A are used for the alarm relay connectors.



31783-M

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

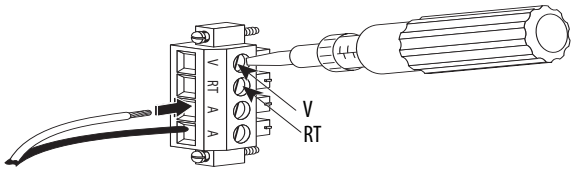
   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wire. Stripping more than the recommended amount of wire can leave exposed wire from the connector after installation.



31784-M

4. Insert the exposed part of the positive wire into the connection labeled V and the exposed part of the return wire into the connection labeled RT.

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



5. Use a ratcheting-torque screwdriver to torque the power and relay connector captive screws above the installed wire leads to 0.23 N•m (2.0 lb•in).

6. Connect the other end of the positive wire (the one connected to V) to the positive terminal on the DC power source, and connect the other end of the return wire (the one connected to RT) to the return terminal on the DC power source.

   You can use a second power source to provide redundant power. The alarm relays on the switch can be used to warn you if one of the power supplies fails. The switch operates properly with only one power source connected at either Pwr A or Pwr B.

7. If you are installing the switch and are using a second power source, repeat steps 2...6 with a second power and relay connector.

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

Wire the DC Power Source for the PoE Expansion Module (optional)

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

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

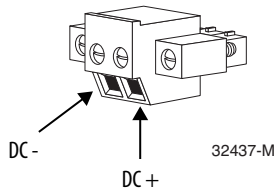
To comply with UL restrictions, this equipment must be powered from a source compliant with Class 2 or Limited Voltage/Current.

Power supply requirements for a PoE expansion module depend on your application.

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

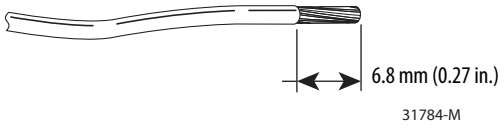
Follow these steps to wire DC power to the PoE expansion module.

1. Locate the power connector and identify the positive and return DC power connections.

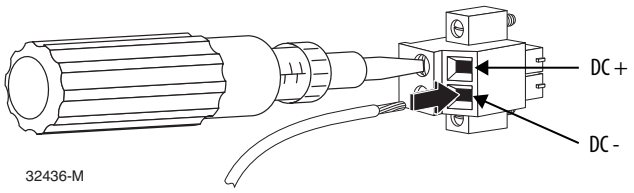


2. Measure a length of 0.82...0.52 mm^2 (18...20 AWG) copper wire long enough to connect to the DC power source.
3. Use an 18-gauge wire-stripping tool to strip each of the two wires to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

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



4. Insert the exposed part of the positive wire into the DC + connection and the exposed part of the return wire into the DC - connection.
5. Make sure that you cannot see any wire lead; only wire with insulation can extend from the connector.



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

Attach the Power and Relay Connector to the Switch

ATTENTION: The input voltage source of the alarm circuits must be an isolated source and limited to less than or equal to 24 V DC, 1 A.

ATTENTION: Exposure to some chemicals can degrade the sealing properties of materials used in the relay. Periodically inspect the relay and check for any degradation. If the relay appears damaged in any way, replace the switch.

Sealed Device: Relay Model AGN200A03, manufactured by Matsushita Electric Works

Relay Cover: Manufacture of Plastic Material—Nippon Oil Corp.
Designation of Plastic Material—Type FC-100
Generic Name of Plastic Material —Liquid crystal polymer

Relay Body: Manufacture of Plastic Material—Ueno Fine Chemicals Industry Ltd.
Designation of Plastic Material— Type 2125G
Generic Name of Plastic Materialv—Liquid crystal polymer

Relay Epoxy: Manufacture of Material—Resinous Kasei Co. Ltd.
Designation of Material – Type A-2500BK
Generic Name of Plastic Material—Epoxy Resin

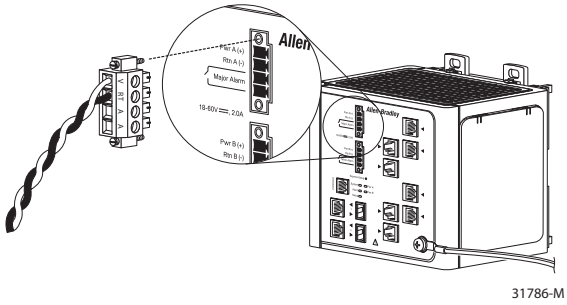
Sealed Device: Relay Model B4GA003Z, manufactured by Fujitsu Takamisawa Electric Co. Ltd.
Relay Cover: Manufacture of Plastic Material —Sumitomo Chemical Co. Ltd.
Designation of Plastic Material—Type E4009
Generic Name of Plastic Material—Liquid crystal polymer

Relay Body: Manufacture of Plastic Material—Sumitomo Chemical Co. Ltd.
Designation of Plastic Material—Type E6807LHF
Generic Name of Plastic Material—Liquid crystal polymer

Relay Epoxy: Manufacture of Material—Sumitomo Bakelite Co. Ltd.
Designation of Material—Type 'SUMIMAC' ECR-9750K2
Generic Name of Plastic Material—Epoxy Resin

Follow these steps to connect the DC power source and relay connector to the switch.

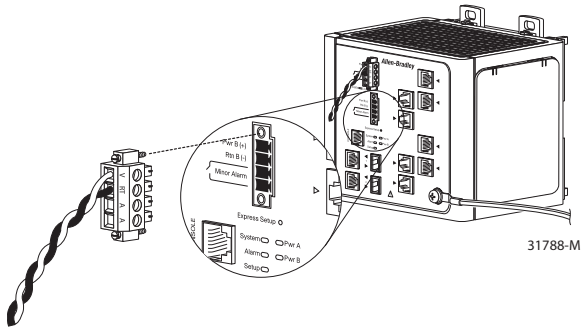
1. Insert the power and relay connector into the Pwr A receptacle on the switch front panel.



31786-M

2. Use a screwdriver to tighten the captive screws on the sides of the power and relay connector.
3. If a second power source is required, insert a second power and relay connector into the Pwr B receptacle on the switch front panel.

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



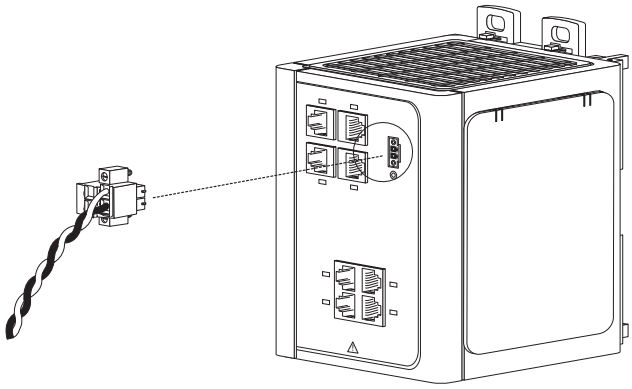
31788-M

4. Use a screwdriver to tighten the captive screws on the sides of the second power and relay connector.

Attach the Power Connector to the PoE Expansion Module (optional)

Follow these steps to connect the DC power source to the PoE expansion module.

1. Insert the power connector into the DC input terminal block on the PoE expansion module.



2. Use a screwdriver to tighten the captive screws on the sides of the power connector.

Wire External Alarms (optional)

The alarm relays on the switch are normally open. To connect an external alarm device to the relays, you must connect two relay contact wires to complete an electrical circuit. Because each external alarm device requires two connections to a relay, the switch supports a maximum of two external alarm devices.

ATTENTION: The input voltage source of the alarm circuits must be an isolated source and limited to less than or equal to 24 V DC, 1 A.

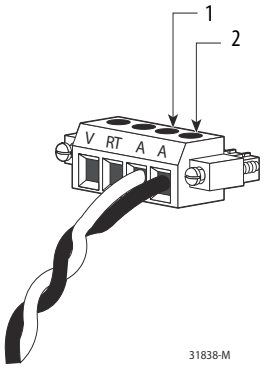
For wire connections to the power and relay connector, you must use UL and CSA rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire (such as Belden part number 9318).

Follow these steps to wire alarms.

1. Measure two strands of twisted-pair wire (18...20 AWG) long enough to connect to the external alarm device.
2. Use a wire stripper to remove the casing from both ends of each wire to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

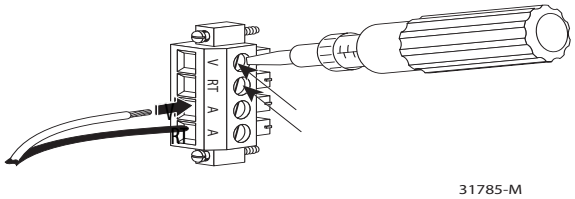
IMPORTANT Do not strip more than 6.8 mm (0.27 in.) of insulation from the wires. Stripping more than the recommended amount of wire can leave exposed wire from the power and relay connector after installation.

3. Insert the exposed wires for the external alarm device into the two connections labeled A, as shown in the following figure.



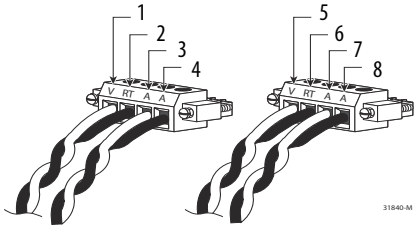
1	External device, relay wire A connection 1	**2**	External device, relay wire A connection 2

4. Use a screwdriver to torque the power and relay connector captive screw (above the installed wire leads) to 0.23 N•m (2.0 lb•in).



5. Repeat steps 1...4 to insert the input and output wires of an additional external alarm device into the second power and relay connector.

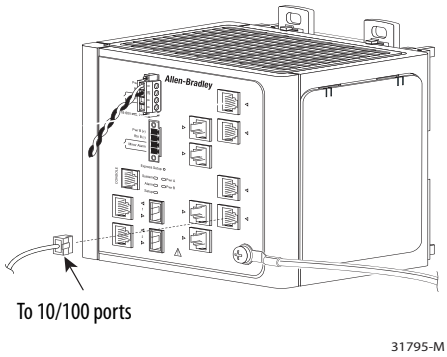
   The following figure shows the completed wiring for two power supplies and two external alarm devices.



1	Power source A positive connection	**5**	Power source B positive connection
2	Power source A return connection	**6**	Power source B return connection
3	External device 1, relay wire major alarm connection	**7**	External device 2, relay wire minor alarm connection
4	External device 1, relay wire major alarm connection	**8**	External device 2, relay wire minor alarm connection

Connect to 10/100 Copper Ports

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



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

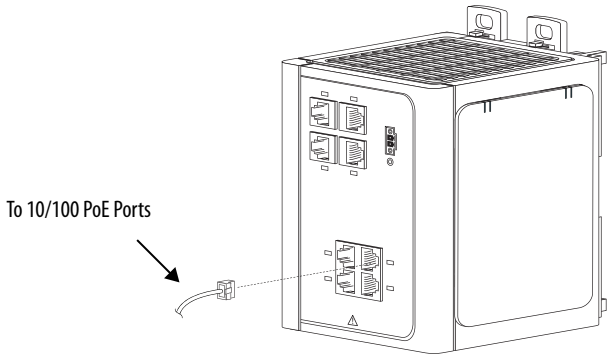
Connect to a PoE Expansion Module Port

Two expansion modules provide PoE capability:

- The 1783-MX04E PoE expansion module provides four PoE ports. You can configure as many as four ports in any combination of PoE and PoE+.
- The 1783-MX04T04E PoE expansion module provides four PoE ports and four non-PoE ports. You can configure as many as four ports in any combination of PoE and PoE+.

The PoE expansion modules each require a separate power supply. For power supply requirements based on your application, refer to page 31.

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



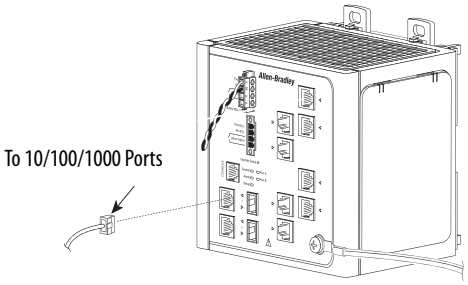
2. Insert the other cable end into an RJ45 connector on the other PoE powered device.

Connect to Dual-purpose Uplink Ports

The switches have two dual-purpose uplink ports. Each dual-purpose uplink port has a 10/100/1000 RJ45 connector for a copper interface and a slot for an SFP module. Only one port of the dual-purpose port can be active at a time. If an SFP module port is connected, the SFP module port has priority.

Connect to 10/100/1000 Uplink Ports

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



31795-M

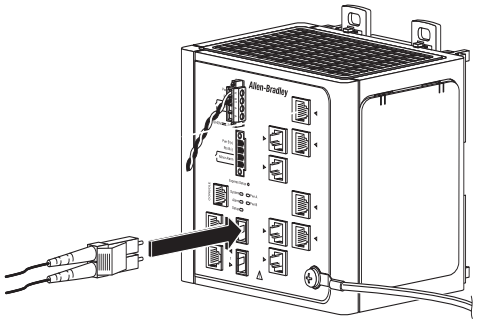
2. Insert the other cable end into an RJ45 connector on the other device.

Connect to SFP Fiber Ports

ATTENTION: Class 1 laser product. Laser radiation is present when the small form-factor pluggable (SFP) optical transceiver is open and interlocks bypassed. Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Follow these steps if you installed an SFP module. For instructions on installing, removing, and connecting to SFP modules, see the documentation that shipped with the SFP module.

1. Insert a fiber-optic cable with an LC connector into the SFP fiber port.



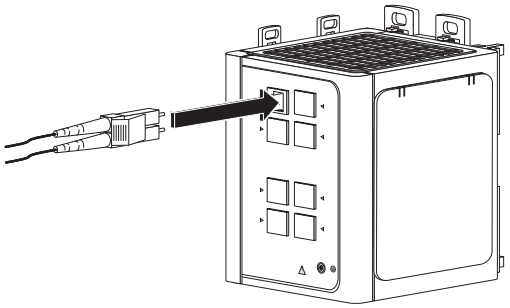
31796-M

2. Insert the other cable end into the other device.

Connect to 100BaseFX Ports

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

1. Insert a fiber-optic cable with an LC connector into the 100BASE-FX port of the 1783-MX08F expansion module.



31797-M

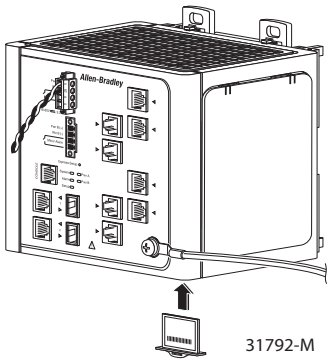
2. Insert the other cable end into the other device.

Install or Remove the CompactFlash Card

The switches ship with the CompactFlash card installed. Follow this procedure when you need to install or remove it from the switch.

WARNING: When you insert or remove the CompactFlash Card while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

Install or remove the CompactFlash card by grasping the tab on the card and either inserting it or removing it from the slot at the bottom of the switch.



31792-M

IMPORTANT You can install and remove the CompactFlash card while the switch is powered. However, if you do not have a CompactFlash card installed in the switch, you are unable to do the following:

- Start the Device Manager Web interface when you apply power to the switch.
- Save configuration changes you made with the AOP via software.
- Start up the switch.

Reset the Switch to Factory Defaults

Follow this procedure if you need to restore the switch to its factory default settings. This procedure resets the switch to its original factory settings. Any configuration changes you have made are lost.

1. Remove power from the switch.
2. Reapply power to the switch.
3. While the switch is powering up, press and hold the Express Setup button.
4. When the EIP Mod, EIP Net and Setup status indictors turn red, release the Express Setup button.

   The switch continues powering up in its factory default state.
5. To reconfigure the switch, see Set Up the Switch Initially with Express Setup on page 48.

Troubleshoot the Installation

The status indicators on the front panel provide troubleshooting information about the switch. They show power-on self-test (POST) failures, port-connectivity problems, and overall switch performance. You can also get statistics from the browser interface, the command-line interface (CLI), or a Simple Network Management Protocol (SNMP) workstation.

Switch POST Results

As power is applied to the switch, it begins the POST, a series of tests that runs automatically to ensure that the switch functions properly. It can take several minutes for the switch to complete POST.

POST starts with status indicator tests that cycle once through the EIP Mod, EIP Net, Setup, Pwr A, and Pwr B status indicators. While POST proceeds, the EIP Mod status indicator blinks green, and all the other status indicators remain off.

If POST completes successfully, the System status indicator changes to solid green, and the other status indicators display their normal operating status. If the switch fails POST, the System status indicator turns red.

ATTENTION: POST failures are usually fatal. Contact your Rockwell Automation technical support representative if your switch does not pass POST.

POST Results with a Terminal

If you have a terminal connected to the console port, you can also view POST status and test results on the terminal. If the terminal displays unclear characters, try resetting the terminal-emulation software to 9600 bits per second.

Bad or Damaged Cable

Always make sure that the cable does not have marginal damage or failure. Even if a cable is capable of connecting at the physical layer, subtle damage to the wiring or connectors can corrupt packets.

This situation is likely when the port has many packet errors or the port constantly loses and regains the link. To troubleshoot, try the following:

- Swap the copper or fiber-optic cable with a known, undamaged cable.
- Look for broken, bent, or missing pins on cable connectors.
- Rule out any bad patch panel connections or media convertors between the source and destination.

  If possible, bypass the patch panel, or eliminate faulty media convertors (fiber-optic-to-copper).
- Try the cable in another port or interface to determine if the problem follows the cable.

Ethernet and Fiber Cables

Make sure that you have the correct cable type for the connection:

- Use Category 3 copper cable for 10 Mb/s UTP connections.
- You can use Category 5, 5e, or 6 UTP or STP cable for 10/100 Mbps connections.
- For 1000 Mbps (1 gigabit per second) connections, use Category 5e or Category 6 UTP or STP cable.
- For fiber-optic connectors, verify that you have the correct cable for the distance and the port type.
- Make sure that the connected device ports both match and use the same type of encoding, optical frequency, and fiber type.

Link Status

Verify that both sides have a network link. A single broken wire or one shut down port can cause one side to show a link, but not the other side. A Link status indicator does not guarantee that the cable is fully functional. The cable can encounter physical stress that causes it to function at a marginal level. If the Link status indicator for the port is not lit, do the following:

- Connect the cable from the switch to a known good device.
- Make sure that both ends of the cable are connected to the correct ports.
- Verify that both devices have power.
- Verify that you are using the correct cable type.
- Rule out loose connections. Sometimes a cable appears to be seated, but is not. Disconnect the cable, and then reconnect it.

Transceiver Issues

Use only Rockwell Automation SFP modules on the switch. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding identifies and validates that the module meets the requirements for the switch. Other manufacturers' SFP modules do not function correctly.

Check these items:

- Verify that the SFP module is valid and functional. Exchange a suspect module with a known good module. Verify that the module is supported on this platform.
- Use the CLI show interfaces command or the CLI show int status command to verify the error-disabled or shutdown status of the port or module. Re-enable the port if needed.
- Make sure that all fiber connections are properly cleaned and securely connected.

Port and Interface Settings

A cause of port connectivity failure can be a disabled port. Verify that the port or interface is not disabled or powered down for some reason. If a port or interface is manually shut down on one side of the link or the other side, the link does not come up until you re-enable the port. Use the CLI show interfaces privileged EXEC command to verify the port or interface error-disabled, disabled, or shutdown status on both sides of the connection. If needed, re-enable the port or the interface.

Getting Started

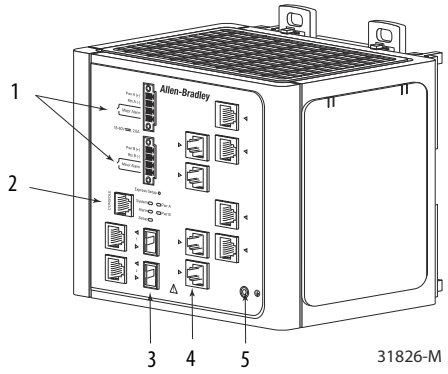
The Stratix 8000 and Stratix 8300 Ethernet managed switches provide a secure switching infrastructure for harsh environments. You can connect these switches to network devices, such as servers, routers, and other switches. In industrial environments, you can connect Ethernet-enabled industrial communication devices, including programmable logic controllers (PLCs), human-machine interfaces (HMIs), drives, sensors, and I/O.

The Stratix 8000 Ethernet managed switch is a Layer 2 switch. The Stratix 8300 Ethernet managed switch adds Layer 3 routing to the Stratix 8000 switch. The Stratix 8300 switch contains all the features of the Stratix 8000 switch, plus a number of IP routing protocols, along with enhanced security and quality of service (QoS) features.

Switch Front Panel Description

The switch front panel contains the ports, the status indicators, and the power and relay connectors.

Figure 1 - 1783-MS10T Switch

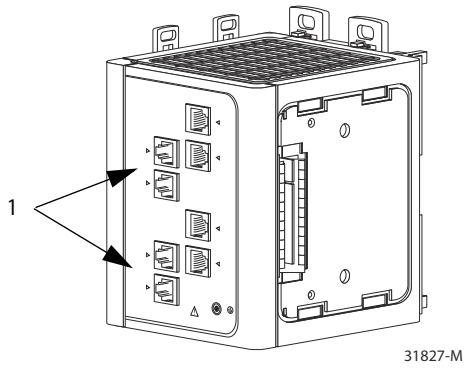


1	Power and relay connectors
2	Console port
3	Dual-purpose ports
4	10/100 ports
5	Protective ground connection

Expansion Module Front Panel Descriptions

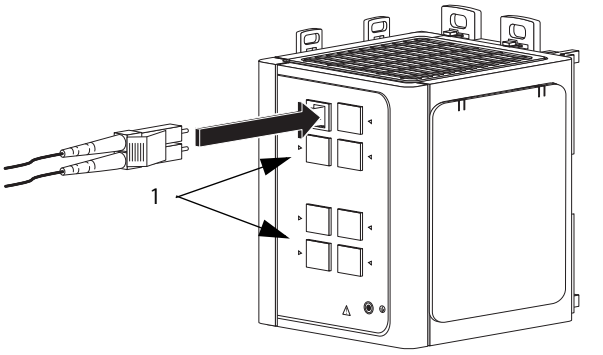
Figure 2...Figure 7 show the expansion module front panels.

Figure 2 - 1783-MX08T Switch Copper Expansion Module (side cover removed)



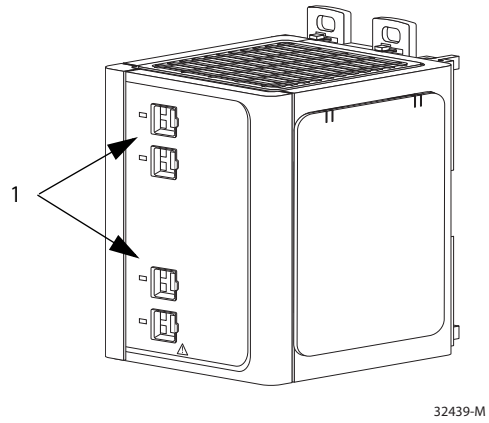
1	10/100 ports

Figure 3 - 1783-MX08F Switch Fiber Expansion Module



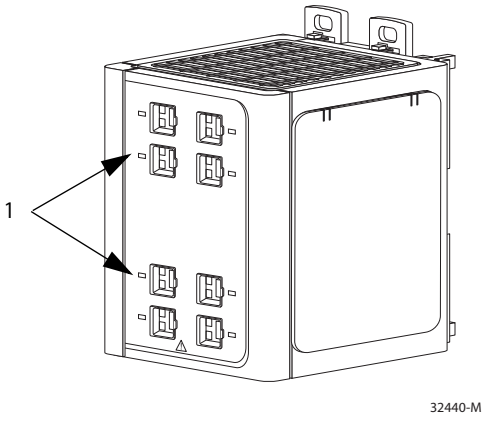
1	100BASE-FX ports

Figure 4 - 1783-MX04S SFP Expansion Module



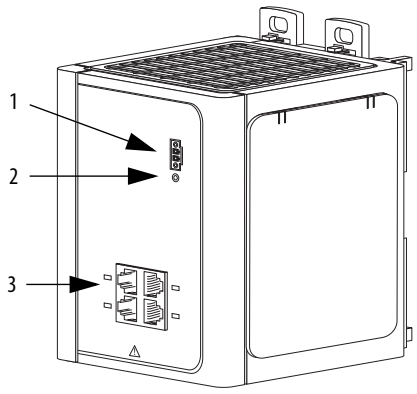
1	100BASE-FX SFP ports

Figure 5 - 1783-MX08S SFP Expansion Module



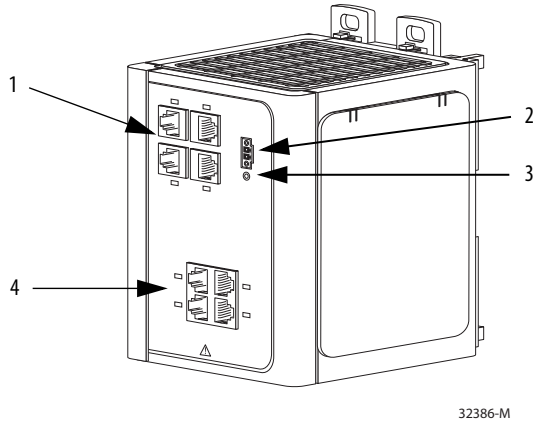
1	100BASE-FX SFP ports

Figure 6 - 1783-MX04E PoE Expansion Module



1	DC input terminal block
2	PoE status indicator
3	PoE ports

Figure 7 - 1783-MX04T04E PoE Expansion Module



1	10/100 non-PoE ports
2	DC-Input terminal block
3	PoE status indicator
4	PoE ports

Hardware Features

These features are common to both the Stratix 8000 and Stratix 8300 switches. See the figures on pages 44...46 for an illustration of these features.

Feature	Description
Power and relay connector	You connect the DC power and alarm signals to the switch through two front panel connectors. One connector provides primary DC power (supply A) and the major alarm signal, and a second connector (supply B) provides secondary power and the minor alarm signal. The two connectors are physically identical and are in the upper left side of the front panel. The switch can operate with a single 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. The power and relay connectors also provide an interface for two independent alarm relays: the major alarm and the minor alarm. The relays can be activated for environmental, power supply, and port status alarm conditions and can be configured to indicate an alarm with either open or closed contacts. The relay itself is normally open, so under power failure conditions, the contacts are open. From the Command Line Interface (CLI), you can associate any alarm condition with one alarm relay or with both relays.
Console port	For configuring, monitoring, and managing the switch, you can connect a switch to a computer through the console port and the supplied RJ45-to-DB-9 adapter cable. If you want to connect a switch to a terminal, you need to provide an RJ45-to-DB-25 female DTE adapter.
Dual-purpose uplink ports	The two dual-purpose uplink ports can each be configured for RJ45 (copper) or SFP (fiber) media types. Only one of these connections in each of the dual-purpose ports can be active at a time. If both ports are connected, the SFP module port has priority. You can set the copper RJ45 ports to operate at 10, 100, or 1000 Mbps, full-duplex or half-duplex. You can configure them as fixed 10, 100, or 1000 Mbps (Gigabit) Ethernet ports and can configure the duplex setting. You can use approved Gigabit (or 100 Mbps) Ethernet SFP modules to establish fiber-optic connections to other switches. These transceiver modules are field-replaceable, providing the uplink interfaces when inserted in an SFP module slot. You use fiber-optic cables with LC connectors to connect to a fiber-optic SFP module. These ports operate full-duplex only.
10/100 ports	You can set the 10/100 ports to operate at 10 or 100 Mbps, full-duplex or half-duplex You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3-2002. The default setting is autonegotiate. When set for autonegotiation, the port senses the speed and duplex settings of the attached device. If the connected device also supports autonegotiation, the switch port negotiates the best connection (that is, the fastest line speed that both devices support and full-duplex transmission if the attached device supports it) and configures itself accordingly. In all cases, the attached device must be within 100 m (328 ft) of the switch.
100BASE-FX ports	The IEEE 802.3-2002 100BASE-FX ports provide full-duplex 100 Mbps connectivity over multi-mode fiber (MMF) cables. These ports use a built-in, small-form-factor fixed (SFF) fiber-optic transceiver module that accepts a dual LC connector. The cable can be up to 2 km (1.24 mi.) in length.
PoE ports	The PoE expansion modules provide 10/100BASE-T PoE or PoE+ capability to the switch: • The 1783-MX04E expansion module has four ports that support PoE (IEEE 802.3af) and PoE+ (IEEE 802.3at Type 2). You can configure the four PoE/PoE+ ports on the expansion module in any combination of PoE and PoE+. • The 1783-MX04T04E expansion module provides four ports that support PoE (IEEE 802.3af) and PoE+ (IEEE 802.3at Type 2) and four 10/100BASE-T non-PoE ports. You can configure the four PoE/PoE+ ports on the expansion module in any combination of PoE and PoE+. The PoE expansion modules require a dedicated power supply for power. For power requirements, see page 31.
Rear panel	The rear panels of the switches and expansion modules have latches for installation on either a DIN rail or a wall. The latches slide outward to position the switch over the DIN rail and slide inward to secure the switch to a DIN rail. The feet must be extended when mounting the switch on heavy-duty (35 x 15 mm) DIN rail or they can be extended for improved ventilation when wall mounting.
Auto-MDIX	When connecting the switch to workstations, servers, and routers, straight-through cables are normally used. However, the automatic medium-dependent interface crossover (auto-MDIX) feature of the switch automatically reconfigures the ports to use either straight-through or crossover cable type. The Auto-MDIX feature is enabled by default. When the auto-MDIX feature is enabled, the switch detects the required cable type (straight-through or crossover) for copper Ethernet connections and configures the interfaces accordingly. You can use the command-line interface (CLI) to disable the auto-MDIX feature. See the online help for more information.

CompactFlash Memory Card

The CompactFlash card contains the switch IOS operating system, the Device Manager Web interface firmware, and user-defined configuration settings. Without the CompactFlash card installed, the switch cannot power up or restart.

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

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

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

Set Up the Switch Initially with Express Setup

When you first set up the switch, use Express Setup to enter the initial IP address. Doing this enables the switch to be used as a managed switch. You can then access the switch through the IP address for additional configuration.

You need this equipment to set up the switch:

- A personal computer with Windows 2000, Windows XP, Windows 2003, or Windows Vista operating system installed
- A supported web browser (Internet Explorer 9.0, 10.0, and 11.0, or Firefox 25, 26) with JavaScript enabled
- A straight-through or crossover Category 5 Ethernet cable to connect your personal computer to the switch

Do the following to configure your computer:

- Disable any wireless interface running on your personal computer.
- Disable other networks in your system.
- Set your computer to automatically determine its IP address (DHCP) rather than use a statically configured address.
- Disable any static DNS servers.
- Disable browser proxy settings. Typically, browser settings are in Tools > Internet Options > Connections > LAN Settings.

Follow these steps to run Express Setup.

1. Make sure that at least one of the switch's Ethernet ports is available for Express Setup.

   IMPORTANT Do not use the console port for Express Setup.

   During Express Setup, the switch acts as a DHCP server. If your personal computer has a static IP address, change your personal computer settings before you begin to temporarily use DHCP.

2. Apply power to the switch.

   When the switch powers on, it begins its power-on sequence. The power-on sequence takes approximately 90 seconds to complete.

3. Make sure that the power-on sequence is complete by verifying that the EIP Mod and Setup status indicators are flashing green.

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

4. Press and release the Express Setup button. Wait for a few seconds until the status indicator on one of the unconnected switch ports flashes green.

   This button is recessed 16 mm (0.63 in.) behind the front panel. Use a small tool, such as a paper clip, to reach the button.

5. Connect a Category 5 Ethernet cable (not provided) from the flashing switch port to the Ethernet port on your computer.

   If you wait too long to connect the cable, the Setup status indicator turns off.

   The port status indicators on your computer and on the switch both flash while the switch configures the connection.

6. While the Setup status indicator flashes green, start an Internet browser session on the computer and navigate to http://169.254.0.1.

   If you have a home page configured, the switch configuration loads instead of your normal home page.

   The switch prompts you for the default switch user name and password.

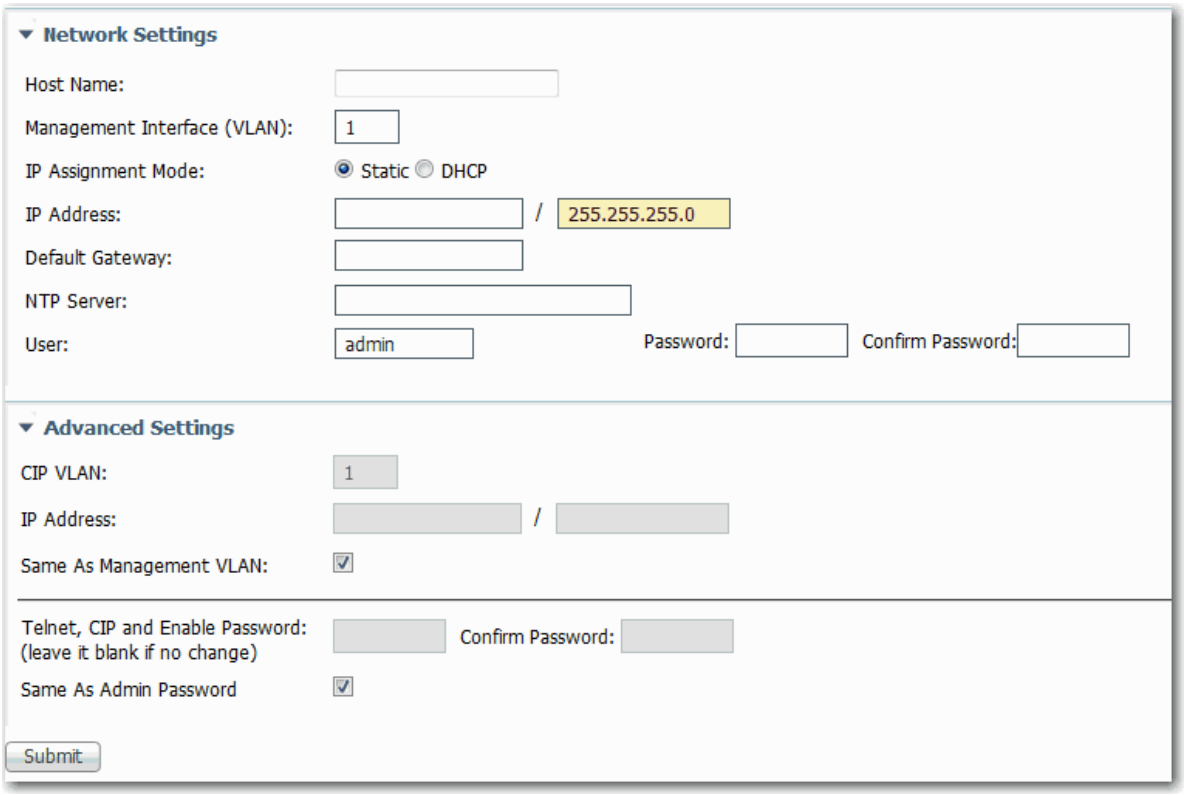
7. Enter the default password: **switch**.

   The default user name is **admin**.

   IMPORTANT In some scenarios, the switch requires you to enter the default password multiple times before it accepts the password.

8. If the window does not appear, do the following:
   - Enter the URL of a well-known website in your browser to be sure the browser is working correctly. Your browser redirects you to the Express Setup web page.
   - Verify that any proxy settings or pop-up blockers are disabled on your browser.
   - Verify that any wireless interface is disabled on your personal computer.
9. Complete the fields.

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



Field	Description
Network Settings	
Host Name	The name of the device.
Management Interface (VLAN)	The name and ID of the management VLAN through which the switch is managed. Choose an existing VLAN to be the management VLAN. The default ID is 1. The default name for the management VLAN is default. The number can be from 1…1001. Be sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch. 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 at all times.

Field	Description
IP Assignment Mode	The IP Assignment mode determines whether the switch IP information is manually assigned (static) or is automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you click Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the Device Manager Web interface. If you click DHCP, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. As long as the switch is not restarted, the switch continues to use the assigned IP information, and you are able to use the same IP address to access the Device Manager Web interface. If you manually assign the switch IP address and your network uses a DHCP server, be sure that the IP address that you give to the switch is not within the range of addresses that the DHCP server automatically assigns to other devices. This prevents IP address conflicts between the switch and another device.
IP Address	The IP address and associated subnet mask are unique identifiers for the switch in a network: • The IP address format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. • The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is enabled only if the IP Assignment mode is Static. Make sure that the IP address that you assign to the switch is not being used by another device in your network. The IP address and the default gateway cannot be the same.
Default Gateway (optional)	The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address must be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This field is enabled only if the IP assignment mode is Static. You must specify a default gateway if your network management station and the switch are in different networks or subnetworks. Otherwise, the switch and your network management station cannot communicate with each other.
NTP Server	The IP address of the Network Time Protocol (NTP) server. NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
User	Enter the user name.
Password, Confirm Password	The password for the switch can have up to 63 alphanumeric characters, can start with a number, is case-sensitive, and can have embedded spaces. The password cannot be a single digit, it cannot contain a ? or a tab, and it does not allow spaces at the beginning or the end. The default is **switch**. To complete initial setup, change the password from the default password, **switch**. This password is also used as the Control Industrial Protocol (CIP) security password. We recommend that you provide a password to the switch to secure access to the device manager.
Advanced Settings	
CIP VLAN	The VLAN on which Common Industrial Protocol (CIP) is enabled. The CIP VLAN can be the same as the management VLAN or you can isolate CIP traffic on another VLAN that is already configured on this device.
IP Address	The IP address and subnet mask for the CPI VLAN if the CIP VLAN is different from the management VLAN. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. Make sure that the IP address that you assign to this device is not being used by another device in your network.
Same As Management VLAN	Indicates whether the settings for the CIP VLAN are the same as the management VLAN.
Telnet, CIP and Enable Password (optional), Confirm Password	The password used for Telnet and CIP security.
Same As Admin Password	Sets the password used for Telnet and CIP security to the same user password specified under Network Settings.

10. Click Submit.

    The switch initializes its configuration for typical industrial EtherNet/IP applications. The switch then redirects you to the logon page for the Device Manager Web interface. You can continue to launch the Device Manager Web interface for further configuration or exit the application.

11. Turn off DC power at the source, disconnect all cables to the switch, and install the switch in your network.
12. After you complete Express Setup, refresh the personal computer IP address:
    - For a dynamically-assigned IP address, disconnect the personal computer from the switch, and reconnect the personal computer to the network. The network DHCP server assigns a new IP address to the personal computer.
    - For a statically-assigned IP address, change it to the previously configured IP address.

Switch Memory Allocation

The following table provides details on default memory allocation for the switches.

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

The following SDM templates are recommended:

- Default
- Lanbase Routing

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

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

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

Device Manager Web Interface

You can manage the switch by using the Device Manager Web interface to configure and monitor the switch. The Device Manager Web interface is a graphical device management tool for configuring, monitoring, and troubleshooting individual switches.

The Device Manager Web interface displays real-time views of switch configuration and performance. It simplifies configuration tasks with features such as Smartports to quickly set up the switch and its ports. It uses graphical, color-coded displays, such as the Front Panel view, graphs, and animated indicators to simplify monitoring tasks. It provides alert tools to help you to identify and to solve networking problems.

You can display the Device Manager Web interface from anywhere in your network through a web browser such as Microsoft Internet Explorer.

Hardware Requirements

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

Software Requirements

Web Browser	Version
Microsoft Internet Explorer	9.0, 10.0, or 11.0 with JavaScript enabled
Mozilla Firefox	25 or 26 with JavaScript enabled

The Device Manager Web interface verifies the browser version when starting a session to be sure that the browser is supported.

To make sure that the Device Manager Web interface runs properly, disable any pop-up blockers or proxy settings in your browser software and any wireless clients running on your computer or laptop.

Studio 5000 Environment

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

Hardware Requirements

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

Cisco Network Assistant

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

Follow these steps to use the software.

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

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

   You can run it directly from the Web if your browser offers this choice.
4. When you run the installer, follow the on-screen instructions.
5. On the final panel, click Finish to complete the Network Assistant installation.

See the Network Assistant online help for more information.

Command Line Interface

You can manage the switch from the command-line interface (CLI) by connecting your personal computer directly to the switch console port or through the network by using Telnet.

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

1. Connect the supplied RJ45-to-DB-9 adapter cable to the standard 9-pin serial port on the personal computer.
2. Connect the other end of the cable to the console port on the switch.

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

3. Start a terminal-emulation program on the personal computer.
4. Configure the personal computer terminal emulation software for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

Notes:

Switch Software Features

The Stratix 8000 and Stratix 8300 switches contain common Ethernet software features, unless otherwise specified.

Port Numbering

The port ID consists of port type (Gigabit Ethernet for Gigabit ports and Fast Ethernet for 10/100 Mbps ports), unit number (1, 2, or 3) and port number (1-2 for Gigabits, 1-4 for the 6 port base and 1-8 for all others). Gigabit Ethernet is abbreviated as Gi and Fast Ethernet as Fa.

The following table shows, as an example, port numbering for the 26-port Stratix 8000 switch configuration containing the following:

- One 10-port base switch
- One copper expansion module
- One fiber expansion module

Table 1 - Port Numbering

Cat. No.	Unit	Number of Ports	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MS10T	10-port base switch	10 2 Gigabit ports and eight 10/100 Mbps ports)	Gigabit ports: 1 2 10/100 Mbps ports: 1 2 3 4 5 6 7 8	Gigabit ports: Gi1/1 Gi1/2 10/100 Mbps ports: Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8
1783-MX08T	Copper expansion module	Eight 10/100 Mbps ports	1 2 3 4 5 6 7 8	Fa2/1 Fa2/2 Fa2/3 Fa2/4 Fa2/5 Fa2/6 Fa2/7 Fa2/8
1783-MX08F	Fiber expansion module	Eight 10/100 Mbps ports	1 2 3 4 5 6 7 8	Fa3/1 Fa3/2 Fa3/3 Fa3/4 Fa3/5 Fa3/6 Fa3/7 Fa3/8

Global Macro

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

- Enable IGMP snooping and Querier
- Enable CIP
- Configure QoS settings and classify CIP, PTP and other traffic
- Enables alarms, SYSLOG, SNMP Notifications
- Enable Rapid Spanning Tree (RSTP), BPDU Guard, BPDU Filter and loop guard

If you do not run Express Setup to initialize the switch, the global macro does not run. You can also run the global macro by using the CLI.

Smartports

Smartports roles are recommended configurations for the switch ports. These configurations, also referred to as port roles, optimize the switch connections and ensure security, transmission quality, and reliability for traffic from the switch ports. The port roles also help prevent port misconfigurations.

TIP Use port roles immediately after the switch initial setup. The switch ports are then correctly configured before they are connected to devices.

Optimize Ports through Port Roles

The port roles are based on the type of devices to be connected to the switch ports. For example, the Desktop for Automation port role is specifically for switch ports to be connected to desktop and laptop computers.

By default, the switch ports are set with the None port role.

Table 2 - Port Roles

Port Role	Description
Automation Device	Apply this role to ports to be connected to EtherNet/IP (Ethernet Industrial Protocol) devices. It can be used for industrial automation devices, such as logic controllers and I/O: • Port is set to Access mode. • Port security supports only one MAC ID. • Optimize queue management for CIP traffic.
Desktop for Automation	Apply this role to ports to be connected to desktop devices, such as desktop computers, workstations, notebook computers, and other client-based hosts: • Port is set to Access mode. • Portfast enabled. • Port security supports only one MAC ID. Do not apply to ports to be connected to switches, routers, or access points.
Switch for Automation	Apply this role to ports to be connected to other switches. Port is set to Trunk mode.
Router for Automation	Apply this role to routers or ports to be connected to Layer 3 switches with routing services enabled.

Table 2 - Port Roles (continued)

Port Role	Description
Phone for Automation	Apply this role to ports to be connected to IP phones. A desktop device, such as a computer, can be connected to the IP phone. Both the IP phone and the connected computer have network access through the port: • Port is set to Trunk mode. • Port security supports three MAC IDs. This role prioritizes voice traffic over general data traffic to ensure clear voice reception on the IP phones.
Wireless for Automation	Apply this role to ports to be connected to wireless access points. The access point can provide network access to up to 30 mobile (wireless) users.
Multiport Automation Device	Apply this role to ports connected to multiport EtherNet/IP devices, such as multiport EtherNet/IP devices arranged in a linear or daisy chain topology, the 1783-ETAP module (for connection to the device port only), unmanaged switches (such as the Stratix 2000™) and managed switches with Remote Spanning Tree Protocol (RSTP) disabled: • Port is set to Access mode. • No port security. • Optimized queue management for CIP traffic.
Virtual Desktop for Automation	Apply this role to ports connected to computers running virtualization software. This can be used with devices running up to two MAC addresses: • Port is set to Access mode. • Portfast is enabled. • Port security supports two MAC IDs. **IMPORTANT:** Do not apply the Virtual Desktop for Automation role to ports that are connected to switches, routers, or access points.
Port Mirroring	Apply this role to ports to be monitored by a network analyzer. For more information about port mirroring, see Port Mirroring on page 82.
None	Apply this role to ports if you do not want a specialized port role on the port. This role can be used on connections to any device, including devices in the roles described above.

Avoid Smartports Mismatches

A Smartports mismatch occurs when an attached device does not match the port role applied to the switch port. Mismatches can have adverse effects on devices and your network.

Mismatches can have these results:

- Affect the behavior of the attached device
- Lower network performance, for example 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

We recommend that you always verify which port role is applied to a port before attaching a device to the port or reconnecting devices that have been moved.

Power over Ethernet (PoE) Ports

PoE expansion module ports are software-configurable and provide these features:

- Support for IEEE 802.3af (PoE)-compliant devices.
- Support for IEEE 802.3at Type 2 (PoE+), which increases the available power that can be drawn by powered devices from 15.4...30 W per port.
- Automatic detection and power budgeting. The module maintains a power budget, monitors and tracks requests for power, and grants power only when it is available.
- Power to connected Cisco pre-standard and IEEE 802.3af-compliant powered devices if the switch detects that there is no power on the circuit.
- Support for Cisco Discovery Protocol (CDP) with power consumption. This features applies only when using PoE expansion modules with Cisco end devices. The powered Cisco end device notifies the expansion module of the amount of power it is consuming. The module can supply or remove power from the PoE port.
- Support for Cisco intelligent power management. A powered Cisco end device and the module negotiate through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-powered device consuming more than 7 W to operate at its highest power mode. The powered device first starts up in Low-power mode, consumes less than 7 W, and negotiates to obtain enough power to operate in High-power mode. The device changes to High-power mode only when it receives confirmation from the expansion module.

  Cisco intelligent power management is backward-compatible with CDP with power consumption. The module responds according to the CDP message that it receives. CDP is not supported on third-party powered devices, so the module uses the IEEE classification to determine the power usage of the device.

Powered Device Detection and Initial Power Allocation

A PoE expansion module detects a powered device when a port with PoE capability is active, PoE is enabled (the default), and the connected device is not being powered by another power source.

After device detection, the module determines the device power requirements based on its type:

- The module classifies the detected IEEE device within a power consumption class. Based on the available power in the power budget, the module determines if a PoE port can be powered. The table below lists these levels.

  Table 3 - IEEE Power Classifications

Class	Power Supplied per Port, max
0 (class status unknown)	15.4 W
1	4 W
2	7 W
3	15.4 W
4	30 W PoE+ devices only

- A Cisco pre-standard powered device does not provide its power requirement when the module detects it. A port that is not configured for PoE+ allocates 15.4 W as the initial allocation for power budgeting. A port that is configured for PoE+ switch allocates 30 W.

  The initial power allocation is the maximum amount of power that a powered device requires. The module initially allocates this amount of power when it detects and powers the powered device. As the module receives CDP messages from the powered device and as the powered device negotiates power levels with the module through CDP power-negotiation messages, the initial power allocation can be adjusted.

The module monitors and tracks requests for power and grants power only when it is available. The module tracks its power budget, which is the amount of power available on each PoE port. The module performs power-accounting calculations when a port is granted or denied power to keep the power budget up to date.

After power is applied to a PoE port, the module uses CDP (if CDP is supported by the powered Cisco end device) to determine the actual power consumption requirement of the connected powered devices and adjusts the power budget accordingly. The switch processes a request and either grants or denies power. If the request is granted, the module updates the power budget. If the request is denied, the module verifies that power to the port is turned off, generates a syslog message, and updates the status indicators. Powered devices can also negotiate with the module for more power.

If the module detects a fault caused by an undervoltage, overvoltage, overtemperature, oscillator-fault, or short-circuit condition, it turns off power to the port, generates a syslog message, and updates the power budget and status indicators.

Power Management Modes

PoE expansion module ports support these modes:

- Auto (default)—The port automatically detects if the connected device requires power. This is the default mode. If the port discovers a connected powered device and the module has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the status indicators. For status indicator information, see PoE Port Status Indicator on page 179.

  If enough power is available for all powered devices connected to the module, power is turned on to all devices. If there is not enough available power to accommodate all connected devices and if a device is disconnected and reconnected while other devices are waiting for power, it cannot be determined which devices are granted or are denied power.

  If granting power exceeds the system power budget, the module denies power, verifies that power to the port is turned off, generates a syslog message, and updates the status indicators. After power has been denied, the module periodically rechecks the power budget and continues to attempt to grant the request for power.

  If a device being powered by the module is then connected to wall power, the module can continue to power the device. The module can continue to report that it is still powering the device whether the device is being powered by the module or receiving power from an AC power source.

  If a powered device is removed, the module automatically detects the disconnect and removes power from the port. You can connect a nonpowered device without damaging it.

  You can specify the maximum wattage that is allowed on the port. If the IEEE-class maximum wattage of the powered device is greater than the configured maximum value, the module does not provide power to the port. If the module powers a powered Cisco end device, but the powered device later requests through CDP messages more than the configured maximum value, the module removes power to the port. The power that was allocated to the powered device is reclaimed into the global power budget. If you do not specify a wattage, the module delivers the maximum value.

- Static—The module pre-allocates power to the port even when no powered device is connected and guarantees that power is available for the port. The module allocates the port-configured maximum wattage, and the amount is never adjusted through the IEEE class or by CDP messages from a powered Cisco end device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed to be powered when it is connected to the static port. The port no longer participates in the first-come, first-served model.

  However, if the powered-device IEEE class is greater than the maximum wattage, the module does not supply power to it. If the module learns through CDP messages that a powered Cisco end device needs more than the maximum wattage, the powered device is shut down.

  If you do not specify a wattage, the module pre-allocates the maximum value. The module powers the port only if it discovers a powered device. Use the static setting on a high-priority interface.

- Off—The module disables powered-device detection and never powers the PoE port, even if an unpowered device is connected. Use this mode only when you want to make sure power is never applied to a PoE port, making the port a data-only port.

Maximum Power Allocation (cutoff power) on a PoE Port

The module determines the cutoff power on a PoE port in this order.

1. Manually when you configure the power level that the module budgets for the port
2. Manually when you configure the power level that limits the power allocated to the port
3. Automatically when the module sets the power usage of the device by using the IEEE classification and LLDP power negotiation or CDP power negotiation

If you do not manually configure the cutoff-power value, the module can automatically determine the value by using CDP power negotiation when connected to a Cisco end device. If the switch cannot determine the value by using one of these methods, it uses the default value of 15.4 W.

With PoE+, if you do not manually configure the cutoff-power value, the module automatically determines it by using the device IEEE classification and LLDP power negotiation or CDP power negotiation with a Cisco end device. If CDP or LLDP are not enabled, the default value of 30 W is applied. However, without CDP or LLDP, the module does not allow devices to consume more than 15.4 W of power because values from 15,400...30,000 mW are allocated based on only CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP negotiation, the device can be in violation of the maximum current limitation and can experience a fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.

Power Consumption Values

You can configure the initial power allocation and the maximum power allocation on a port. However, these values are only the configured values that determine when the module turns on or turns off power on the PoE port. The maximum power allocation is not the same as the actual power consumption of the powered device. When you manually set the maximum power allocation, you must consider the power loss over the cable from the port to the powered device. The cutoff power is the sum of the rated power consumption of the powered device and the worst-case power loss over the cable.

The actual amount of power consumed by a powered device on a PoE port is the cutoff-power value plus a calibration factor of 500 mW (0.5 W). The actual cutoff value is approximate and varies from the configured value by a percentage of the configured value. For example, if the configured cutoff power is 12 W, the actual cutoff-value is 11.4 W, which is 0.05% less than the configured value.

Because the module supports external removable power supplies for PoE/PoE+ and can configure the budget per the power supply used, the total amount of power available for the powered devices varies depending on the power supply configuration:

- If a power supply is removed and replaced by a new power supply with less power and the module does not have enough power for the powered devices, the module denies power to the PoE ports that are in Auto mode in descending order of the port numbers. If the module still does not have enough power, it denies power to the PoE ports in Static mode in descending order of the port numbers.

- If the new power supply supports more power than the previous one, and the module now has more power available, the module grants power to the PoE ports in Static mode in ascending order of the port numbers. If it still has power available, the module then grants power to the PoE ports in Auto mode in ascending order of the port numbers.

IMPORTANT The total wattage of the power supply must be manually configured via the Device Manager Web interface or CIP for power to be assigned accurately.

VLANs

A virtual local-area network (VLAN) is a logical segment of network users and resources grouped by function, team, or application. This segmentation is without regard to the physical location of the users and resources. For example, VLANs can be based on the departments in your company or by sets of users who communicate mostly with each other.

The switch ships with a default VLAN to which each switch port initially belongs. The switch supports a maximum of 255 VLANs, including the default VLAN.

Every VLAN is identified by its name and ID number. The default VLAN is named default. The ID can be from 1...1001 and 1005...4094, where 1 is the default ID.

You can assign switch ports to either the default VLAN or to VLANs that you have created. The default VLAN alone can be sufficient based on the size and requirements of your network. We recommend that you first determine your VLAN needs before creating VLANs.

The default VLAN is also the management VLAN. After the initial setup, you can create VLANs and designate any VLAN on the switch as the management VLAN. The management VLAN ensures administrative access to the switch. You must assign one of the switch ports to the management VLAN; otherwise, you do not have administrative access to the switch. Initially all ports are assigned to the management VLAN.

You can assign all ports, regardless of their port role, to the default VLAN (default).

Isolate Traffic and Users

By using VLANs, you can isolate different types of traffic, such as voice and data, to preserve the quality of the transmission and to minimize excess traffic among the logical segments. You can also use VLANs to isolate different types of users. For example, you can restrict specific data broadcasts to logical workgroups for security purposes, such as keeping information about employee salaries on devices in a VLAN created for payroll-related communication.

VLANs can also reduce the amount of administrative effort required to constantly examine requests to network resources.

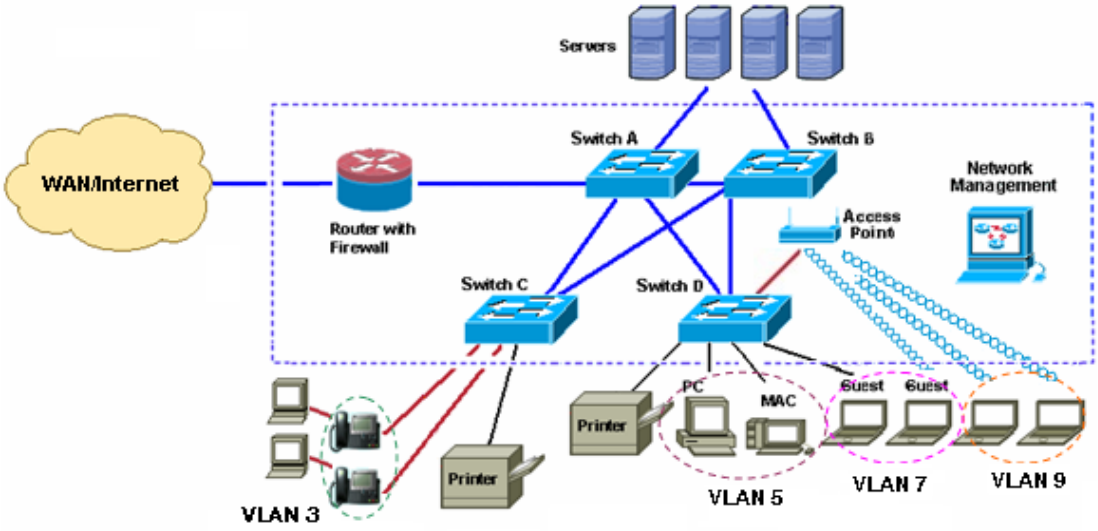
VLANs isolate parts of your network. Therefore, devices that are attached to the switch ports in the same VLAN (network users in the same VLAN) can communicate only with each other and can share the same data.

Devices attached to switch ports in different VLANs cannot communicate with each other through the switch. Inter-VLAN communication requires a router or Layer 3 switch. The router or Layer 3 switch must be configured to support routing across VLANs (inter-VLAN routing), and additional security policies must be set.

If your network is also using a DHCP server, ensure that the server is accessible to the devices in all the VLANs.

The following figure is an example network that uses VLANs based on different network traffic and network users. Organizing a network around these factors helps to define the size and membership of the VLANs in the network.

Figure 8 - VLANs in a Stratix 8000 Switch Network



Isolate Different Traffic Types

Isolating data traffic from delay-sensitive traffic, such as voice traffic, ensures the quality of the voice transmission. In Figure 8 on page 67, switch ports connected to the IP phones belong to VLAN 3, a VLAN that is configured to provide Voice over IP (VoIP) services on these connections, meaning priority is given to voice traffic over regular IP data traffic. Voice traffic from the phone and IP-phone service requests to an IP PBX server have priority over traffic from the desktop devices attached to the IP phones.

To further isolate data traffic from voice traffic, the data traffic from the attached desktop devices can be assigned to a separate VLAN.

Group Users

The network shown in Figure 8 on page 67 provides access to three types of network users: wired employees, wireless (or mobile) employees, and wired and wireless company visitors. Each user type requires different access levels to the company network.

VLANs and security policies on a router or Layer 3 switch can enforce privileges and restrictions to different user types, as shown in Figure 8 on page 67:

- VLAN 5 offers employee-level access to the company resources. This kind of network access requires a direct connection to the specific switch ports.
- VLAN 7 offers Internet-only access to company visitors. Visitors with wired or wireless connections to switch ports are assigned to this VLAN, which automatically restricts guest access to only the Internet.
- VLAN 9, which has one or more switch ports connected to the wireless access point, enforces security policies to identify the wireless user (for example, as employee or a guest) and to determine what the user can do on the network (for example, access only the Internet or access other network resources).

IGMP Snooping with Querier

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The switch supports IP multicast group-based bridging, rather than MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address aliasing issues.

The default number of supported multicast groups are as follows:

- Stratix 8000 switch: 256
- Stratix 8300 switch: 1024

You can modify the number of multicast groups supported by using the command line interface. If you have over 180 multicast groups on a Stratix 8000 we suggest modifying the number of multicast groups by changing the SDM template to the Lanbase Routing template.

The IP multicast groups learned through IGMP snooping are dynamic. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings. Multicast IP addresses used by the EtherNet/IP network for I/O traffic are learned by the switch.

IGMP implementation in the switch is IGMP V2. This version is backward-compatible with switches running IGMP V1. The switch has a built in querier function, and the global macro enables on IGMP Snooping and the querier.

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations can receive duplicate messages. Switches can also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

Rapid Spanning Tree Protocol

Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1D-2004) uses point-to-point wiring and provides rapid convergence of the spanning tree. RSTP is enabled by default.

TIP If you connect the switch to a Cisco network switch, the typical default is PVST+, not RSTP. To provide compatibility, one or the other switch must be modified.

Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.

Storm control (or traffic suppression) monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold.

Storm control uses one of these methods to measure traffic activity:

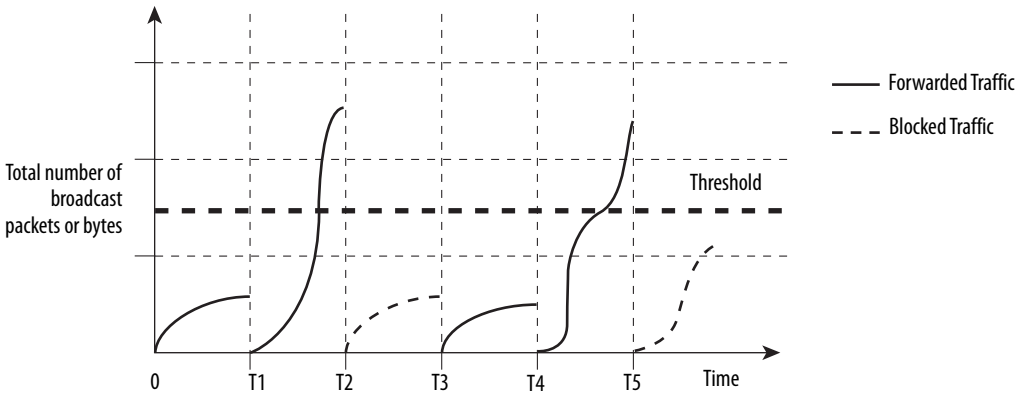
- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic.
- Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received.
- Traffic rate in bits per second at which broadcast, multicast, or unicast packets are received.

With each method, the port blocks traffic when the rising threshold is reached. The port remains blocked until the traffic rate drops below the falling threshold and then resumes normal forwarding. In general, the higher the level, the less effective the protection against broadcast storms.

IMPORTANT When the storm control threshold for multicast traffic is reached, all multicast traffic except network management traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked.

The graph shows broadcast traffic patterns on an interface over a given period of time. The example can also be applied to multicast and unicast traffic. In this example, the broadcast traffic being forwarded exceeded the configured threshold between time intervals T1 and T2 and between T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped for the next time period. Therefore, broadcast traffic is blocked during the intervals following T2 and T5. At the next time interval (for example, T3), if broadcast traffic does not exceed the threshold, it is again forwarded.

Figure 9 - Storm Control Example



The combination of the storm-control suppression level and the 1-second time interval controls the way the storm control algorithm works. A higher threshold lets more packets pass through. A threshold value of 100% means that no limit is placed on the traffic. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.

IMPORTANT Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of storm control.

Default Storm Control Configuration

By default, unicast, broadcast, and multicast storm control are disabled. You can set a threshold by using the Logix Designer application.

Port Security

The switch has two methods for limiting the MAC addresses (MAC IDs) that can access a given port:

- Dynamic
- Static

Dynamic Secure MAC Address (MAC ID)

Many port roles have a maximum number of MAC IDs that can use that port. For example, the Automation Device port role sets up the port for a maximum of one MAC ID. The MAC ID is dynamic, meaning the switch learns the first source MAC ID to use the port. Attempts by any other MAC ID to access the port are denied.

If the link becomes inactive, the switch dynamically relearns the MAC ID to be secured.

The following table shows port roles and the maximum supported MAC IDs.

Port Role	Number of MAC IDs (max)
Automation Device	1
Desktop for Automation	1
Switch for Automation	Not restricted
Router for Automation	Not restricted
Phone for Automation	3
Wireless for Automation	Not restricted
Multiport Automation Devices	Not restricted
Virtual Desktop for Automation	2
Port Mirroring	Not restricted
None	Not restricted

Static Secure MAC Address (MAC ID)

The other method of limiting MAC IDs is to statically configure a single MAC ID for a port. This address becomes part of the saved configuration of the switch. This method provides strong security but requires reconfiguration whenever the device connected to the port is replaced, because the new device has a different MAC ID from the old one.

When you use the Logix Designer application to configure the switch Add-on Profile (AOP), you can use the static secure method. This method is not available with the Device Manager Web interface.

Security Violations

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

- The maximum number of secure MAC addresses that have been configured for a port have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

When a violation occurs, the port goes into the Restrict mode. In this mode, packets with unknown source addresses are dropped and you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

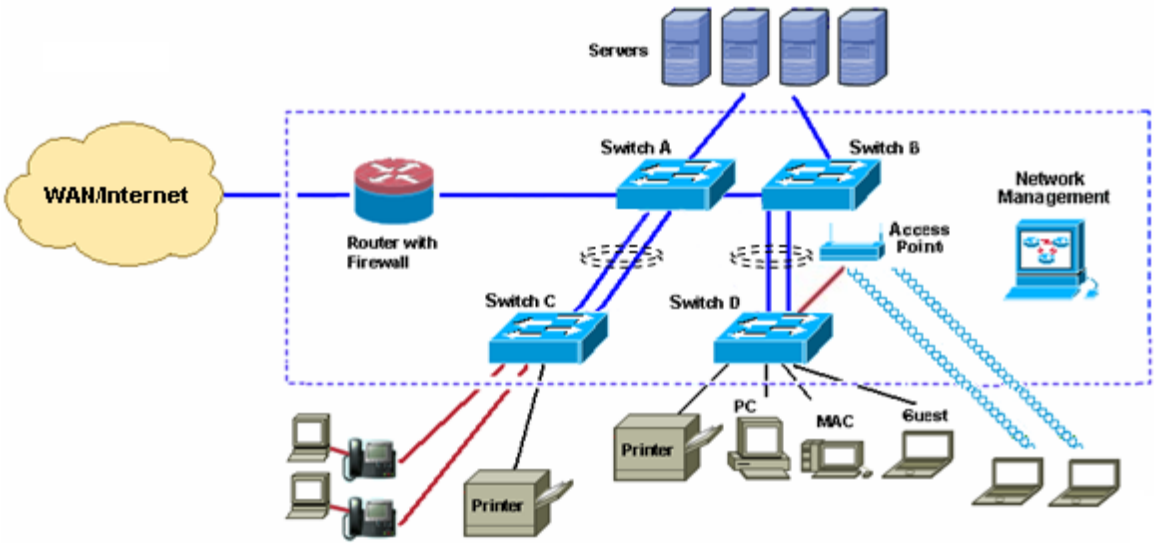
EtherChannels

An EtherChannel (or port group) is a group of two or more Fast Ethernet or Gigabit Ethernet switch ports bundled into a single logical link, creating a higher bandwidth link between two switches. The switch supports up to six EtherChannels. Each EtherChannel can consist of up to eight compatible, configured ethernet ports.

Figure 10 shows two EtherChannels. Two Full-duplex 10/100/1000-Mbps ports on Switches A and C create an EtherChannel with a bandwidth of up to 4 Gbps between both switches. Similarly, two Full-duplex 10/100 ports on Switches B and D create an EtherChannel with a bandwidth of up to 400 Mbps between both switches.

If one of the ports in the EtherChannel becomes unavailable, traffic is sent through the remaining ports within the EtherChannel.

Figure 10 - EtherChannels between Stratix 8000 Switches



You can configure an EtherChannel in one of these modes: Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or On. Configure both ends of the EtherChannel in the same mode.

- When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports become active. Incompatible ports are suspended. Instead of a suspended state, the local port is put into an independent state and continues to carry data traffic as any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

- When you configure an EtherChannel in the On mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the On mode; otherwise, packet loss can occur.

If a link within an EtherChannel fails, traffic previously carried over that failed link moves to the remaining links within the EtherChannel. If traps are enabled on the switch, a trap is sent for a failure that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

DHCP Persistence

Every device in an IP-based network must have a unique IP address. The Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address information from a pool of available addresses to newly connected devices (DHCP clients) in the network. If a device leaves and then re-joins the network, the device receives the next available IP address, which can be the same address that it had before.

The switch can be set to operate as a DHCP server to provide DHCP persistence. With DHCP persistence, you can assign a specific IP address to each port, ensuring that the device attached to a given port receives the same IP address.

The DHCP Server also serves addresses to BOOTP clients.

IMPORTANT To make sure DHCP persistence works correctly, follow the application rules. Refer to Configure DHCP on page 103.

CIP Sync Time Synchronization (Precision Time Protocol)

The IEEE 1588 standard defines a protocol called Precision Time Protocol (PTP) that enables precise synchronization of clocks in measurement and control systems. We refer to this as CIP Sync time synchronization. The clocks are synchronized over the EtherNet/IP communication network. PTP enables systems that include clocks of various precision, resolution, and stability to synchronize. PTP generates a Master-Slave relationship among the clocks in the system. All clocks ultimately derive their time from a clock selected as the Grandmaster clock.

Resilient Ethernet Protocol

The Resilient Ethernet Protocol (REP) provides an alternative to Spanning Tree Protocol (STP) to control network rings and loops, handle link failures, and improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

REP is a segment protocol. One REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (transit) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interfaces. Selecting the Switch for Automation port role enables Layer 2 trunking. REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

You can construct almost any type of network based on REP segments. REP also supports VLAN load-balancing, controlled by the primary edge port but occurring at any port in the segment.

These types of REP ports are available in the Device Manager Web interface:

- Primary—This port is a primary edge port. This port always participates in VLAN load balancing in the REP segment.
- Edge—This port is a secondary edge port. It also participates in VLAN load balancing in the REP segment. Edge ports are termination points of a REP segment. You must configure two edge ports, including one primary edge port, for each REP segment. Entering edge without primary configures the port as a secondary edge port. Primary and secondary edge ports must be configured even if support of VLAN balancing is not required.
- Transit—This port is a non-edge port in the REP segment.
- No-neighbor Primary—This port is a primary edge port connected a non-REP switch.

- No-neighbor—This port is a secondary edge port connected to a non-REP switch. The no-neighbor edge ports contain all properties of regular edge ports. These ports enable the construction of a REP ring containing a switch that does not support REP protocol.

- None—This port is not part of the REP segment.

REP and STP can coexist on the same switch, but not on the same port. REP does not interact with STP. For example, if a port is configured as a REP port, STP is disabled on that port. STP bridge protocol data units (BPDUs) are not accepted on or sent from segment ports REP ports. However, adjacent REP and STP rings or domains can share a common link. This common link can be used for passing REP and STP date plane traffic, or for the STP control plane traffic.

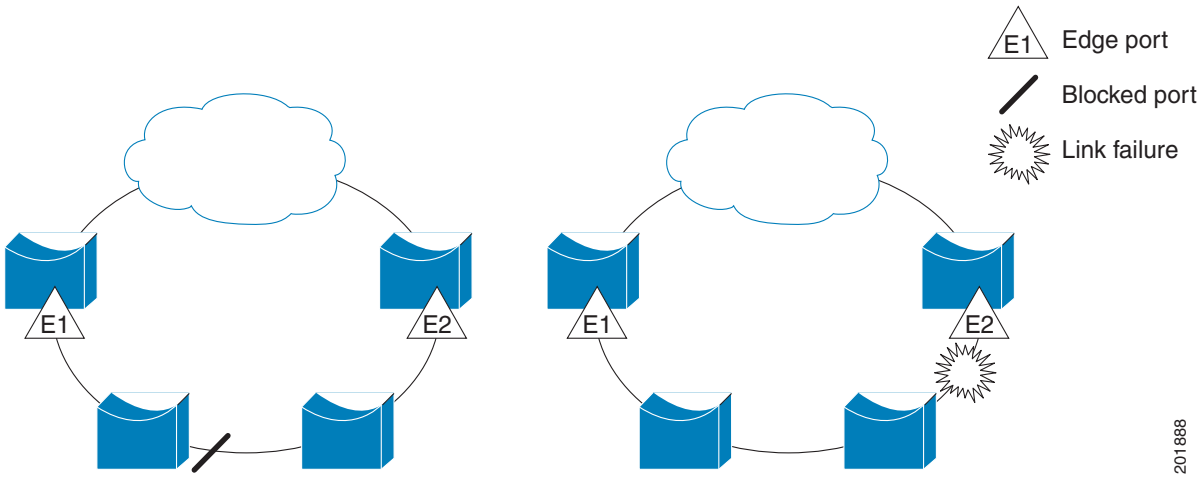
The following figure shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single port is blocked, shown by the diagonal line. When there is a failure in the network, as shown in the diagram on the right, the blocked port returns to the forwarding state to minimize network disruption.

REP Open Segment

The segment shown below is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop and it is safe to connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a failure causes a host to be unable to access its usual gateway, REP unblocks all ports to ensure that connectivity is available through the other gateway.

In Figure 11, E1 or E2 can be configured as the primary edge port.

Figure 11 - Example of REP Open Segment

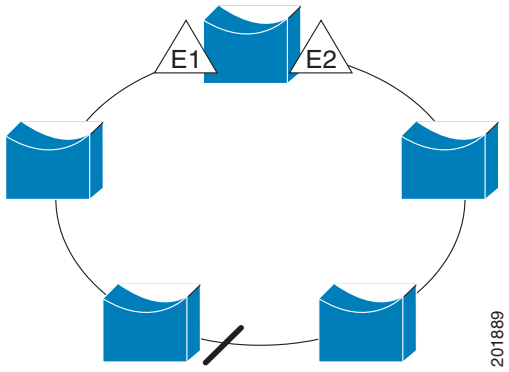


REP Ring Segment

The segment shown in the following figure, with both edge ports on the same switch, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two switches in the segment.

In Figure 12, E1 or E2 can be configured as the primary edge port.

Figure 12 - Example of REP Ring Segment



REP segments have these characteristics:

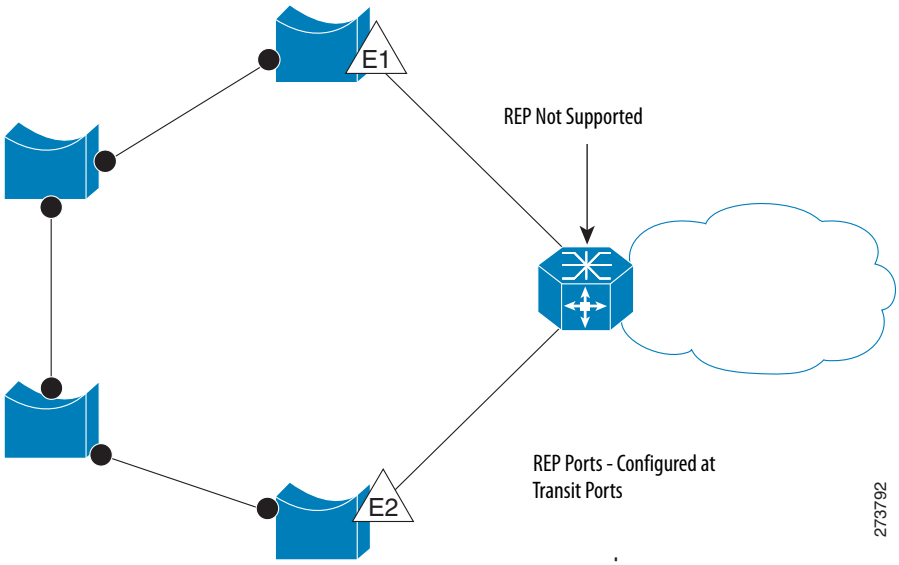
- If all ports in the segment are operational, one port (referred to as the alternate port) is in the blocked state for each VLAN.
- If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.

Access Ring Topologies

In access ring topologies, the neighboring switch does not always support REP, as shown in the following figure. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all properties of edge ports, and you can configure them the same as any edge port, including configuring them to send STP or REP topology change notices to the aggregation switch. In this case the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

In Figure 13, E1 or E2 can be configured as the primary no-neighbor port.

Figure 13 - Example of Access Ring Topology



REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.

You can configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Link Integrity

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines which neighbor port can become the alternate port and which ports can forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge), associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared as operational after it performs a three-way handshake with a neighbor in the same segment.

SNMP

The switch supports Simple Network Management Protocol (SNMP) versions 1, 2C, and 3. SNMP enables the switch to be remotely managed through other network management software. This feature is disabled by default.

SNMP is based on three concepts:

- SNMP managers (client software)
- SNMP agents (network devices)
- Management Information Base (MIB)

Refer to Supported MIBs on page 81 for the MIBs supported on the switch.

The SNMP manager runs SNMP management software. Network devices to be managed, such as bridges, routers, servers, and workstations, have an agent software module. The agent provides access to a local MIB of objects that reflects the resources and activity of the device. The agent also responds to manager commands to retrieve values from the MIB and to set values in the MIB. The agent and the MIB are on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

Both SNMPv1 and v2C use a community-based form of security. SNMP managers can access the agent MIB through passwords referred to as community strings. SNMPv1 and v2C are generally used for network monitoring without network control.

SNMPv3 provides network monitoring and control. It provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security model used by SNMPv3 is an authentication strategy that is set up for a user and the user's group. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used for an SNMP packet.

Following are some guidelines about SNMPv3 objects.

IMPORTANT SNMPv.3 is available only in the cryptographic version of the switch firmware.

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy defines which SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications that its users can receive.
- A group also defines the security model and the security level for its users.
- An SNMP view is a list of MIBs that a group can access.
- Data can be securely collected from SNMP devices without fear of the data being tampered with or corrupted.
- Confidential information, for example, SNMP Set command packets that change a router configuration, can be encrypted to prevent the contents from being exposed on the network.

Supported MIBs

The Stratix 8000 and Stratix 8300 switches support the following MIBs.

MIB Name		
BRIDGE-MIB	CISCO-MEMORY-POOL-MIB	IP-MIB
CALISTA-DPA-MIB	CISCO-PAE-MIB	LLDP-EXT-MED-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-PAGP-MIB	LLDP-MIB
CISCO-ADMISSION-POLICY-MIB	CISCO-PING-MIB	NETRANGER
CISCO-AUTH-FRAMEWORK-MIB	CISCO-PORT-QOS-MIB	NOTIFICATION-LOG-MIB
CISCO-BRIDGE-EXT-MIB	CISCO-PORT-SECURITY-MIB	OLD-CISCO-CHASSIS-MIB
CISCO-BULK-FILE-MIB	CISCO-PORT-STORM-CONTROL-MIB	OLD-CISCO-CPU-MIB
CISCO-CABLE-DIAG-MIB	CISCO-PRIVATE-VLAN-MIB	OLD-CISCO-FLASH-MIB
CISCO-CALLHOME-MIB	CISCO-PROCESS-MIB	OLD-CISCO-INTERFACES-MIB
CISCO-CAR-MIB	CISCO-PRODUCTS-MIB	OLD-CISCO-IP-MIB
CISCO-CDP-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	OLD-CISCO-MEMORY-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-RTTMON-ICMP-MIB	OLD-CISCO-SYS-MIB
CISCO-CLUSTER-MIB	CISCO-RTTMON-IP-EXT-MIB	OLD-CISCO-SYSTEM-MIB
CISCO-CONFIG-COPY-MIB	CISCO-RTTMON-MIB	OLD-CISCO-TCP-MIB
CISCO-CONFIG-MAN-MIB	CISCO-RTTMON-RTP-MIB	OLD-CISCO-TS-MIB
CISCO-DATA-COLLECTION-MIB	CISCO-SNMP-TARGET-EXT-MIB	RMON-MIB
CISCO-DHCP-SNOOPING-MIB	CISCO-STACK-MIB	RMON2-MIB
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-STACKMAKER-MIB	SMON-MIB
CISCO-ENTITY-ALARM-MIB	CISCO-STP-EXTENSIONS-MIB	SNMP-COMMUNITY-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-SYSLOG-MIB	SNMP-FRAMEWORK-MIB
CISCO-ENVMON-MIB	CISCO-TCP-MIB	SNMP-MPD-MIB
CISCO-ERR-DISABLE-MIB	CISCO-UDLDP-MIB	SNMP-NOTIFICATION-MIB
CISCO-FLASH-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	SNMP-PROXY-MIB
CISCO-FTP-CLIENT-MIB	CISCO-VLAN-MEMBERSHIP-MIB	SNMP-TARGET-MIB
CISCO-IF-EXTENSION-MIB	CISCO-VTP-MIB	SNMP-USM-MIB
CISCO-IGMP-FILTER-MIB	ENTITY-MIB	SNMP-VIEW-BASED-ACM-MIB
CISCO-IMAGE-MIB	ETHERLIKE-MIB	SNMPv2-MIB
CISCO-IP-STAT-MIB	HC-RMON-MIB	TCP-MIB
CISCO-LAG-MIB	IEEE8021-PAE-MIB	UDP-MIB
CISCO-LICENSE-MGMT-MIB	IEEE8023-LAG-MIB	
CISCO-MAC-AUTH-BYPASS-MIB	IF-MIB	
CISCO-MAC-NOTIFICATION-MIB	IP-FORWARD-MIB	

Port Mirroring

Port mirroring is for advanced users with experience in troubleshooting traffic and protocol issues on networks.

The port mirroring feature copies (or mirrors) traffic on one port to a monitoring port where the packet can be captured by a network protocol analyzer tool. Use port mirroring as a diagnostic tool or debugging feature.

Port mirroring does not affect the switching of network traffic on the monitored port. You must dedicate a monitoring port for port mirroring use. Except for traffic that is being copied for the port mirroring session, the monitoring port does not receive or forward traffic.

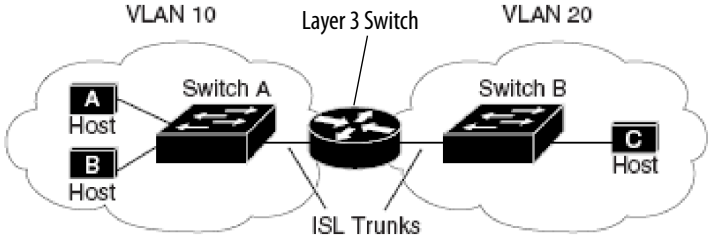
Port mirroring can be configured by assigning the Port Mirroring port role on a switch port by using the Device Manager Web interface. See Chapter 4, Manage the Switch via the Device Manager Web Interface.

Layer 3 Routing (Stratix 8300 switch only)

The Stratix 8300 Ethernet managed switch uses IP address routing to map subnetworks (subnets) to an individual VLAN. In some network environments, VLANs are associated with individual networks or subnetworks. In an IP network, each subnetwork is mapped to an individual VLAN. Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, network devices in different VLANs cannot communicate with one another without a Layer 3 device to route traffic between the VLAN, referred to as inter-VLAN routing. You configure one or more Layer 3 switches to route traffic to the appropriate destination VLAN.

Figure 14 shows a basic routing topology.

Figure 14 - Example of Routing Topology



Switch A is in VLAN 10, and Switch B is in VLAN 20. The Layer 3 switch has an interface in each VLAN.

When Host A in VLAN 10 needs to communicate with Host B in VLAN 10, it sends a packet addressed to that host. Switch A forwards the packet directly to Host B, without sending it to the Layer 3 switch.

When Host A sends a packet to Host C in VLAN 20, Switch A forwards the packet to the Layer 3 switch, which receives the traffic on the VLAN 10 interface. The Layer 3 switch checks the routing table, finds the correct outgoing interface, and forwards the packet on the VLAN 20 interface to Switch B. Switch B receives the packet and forwards it to Host C.

Types of Routing

Stratix 8300 switches can route packets by using these methods.

Table 4 - Routing

Feature	Description
Static and connected routing	See Static and Connected Routing on page 84.
Dynamic routing	Dynamic routing protocols are used by Layer 3 switches to dynamically calculate the best route for forwarding traffic. There are two types of dynamic routing protocols: • Distance-vector protocols • Link-state protocols Layer 3 switches using distance-vector protocols maintain routing tables with distance values of networked resources, and periodically pass these tables to their neighbors. Distance-vector protocols use one or a series of metrics for calculating the best routes. These protocols are easy to configure and use. Distance-vector protocols supported by the switch are Routing Information Protocol (RIP), which uses a single distance metric (cost) to determine the best path and Border Gateway Protocol (BGP), which adds a path vector mechanism. The switch also supports the Open Shortest Path First (OSPF) link-state protocol and Enhanced IGRP (EIGRP), which adds some link-state routing features to traditional Interior Gateway Routing Protocol (IGRP) to improve efficiency. Routers using link-state protocols maintain a complex database of network topology, based on the exchange of link-state advertisements (LSAs) between routers. LSAs are triggered by an event in the network, which speeds up the convergence time or time required to respond to these changes. Link-state protocols respond quickly to topology changes, but require greater bandwidth and more resources than distance-vector protocols
Unicast routing	Unicast routing is used for all network processes where a private or unique resource is requested.
Multicast routing	In multicast routing, routers create optimal distribution paths for data sent to a multicast destination address spanning tree in real-time. Multicast routing protocols supported are PIM (SM, SM, SDM), DVMRP tunneling.
Redundant routing	Redundant routing localizes the effects of route failures, and reduces control traffic overhead and route reconfiguration time by providing a redundant network path. Redundant routing protocols supported are HSRP (Hot Standby Router Protocol) and CEF (Cisco Express Forwarding).
IPv6 routing	IPv6 network segments, also known as links or subnets, are connected by IPv6 routers, which are devices that pass IPv6 packets from one network segment to another. EIGRP is the supported protocol.
VRF Lite	Virtual Routing and Forwarding (VRF) lets multiple instances of a routing table to coexist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. The simplest form of VRF implementation is VRF Lite. In this implementation, each router within the network participates in the virtual routing environment in a peer-based fashion.

IMPORTANT To enable routing in the Stratix 8300 switch, you must change the SDM template from the default template:

- For static and connected routing, you can apply the Lanbase Routing template and enable routing via the Device Manager Web interface.
- For other types of routing, you can apply SDM templates and enable routing via the CLI.

See the following manuals:

- For more information about routing features and how to modify them, see the Cisco IE3000 Switch Software Configuration Manual, available from http://www.Cisco.com.
- For information about using the CLI to configure routing, see the Cisco IE3000 Switch Command-Line Interface Manual, available from http://www.Cisco.com.

Static and Connected Routing

Static and connected routing are implemented both on the Stratix 8000 and Stratix 8300 switches.

- Static routing—Defines explicit paths between two devices (routers and switches). You must manually define the route information, including the destination IP address, destination subnet mask, and next hop router IP address.

- Connected routing—Enables all devices on any VLAN that use the switch to communicate with each other if they use the switch as their default gateway. Connected routing is automatically enabled if you enable static routing. To disable connected routing and prevent inter-VLAN communication, you must configure access control lists (ACLs) by using the CLI.

Enabling static and connected routing is a two-step process within the Device Manager Web interface:

1. Reallocate switch memory for routing by changing the SDM template from the default template to the Lanbase Routing template.
2. Enable connected routing only.

   or

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

Alarms

The switch has two hardware alarm relay contacts on the switch front panel:

- Major alarm relay

  When closed, the major alarm relay indicates a dual-mode power supply or primary temperature alarm.

- Minor alarm relay

  When closed, the minor alarm relay indicates these alarm states:
  - Link fault
  - Port not forwarding
  - Port not operating
  - Frame Check Sequence (FCS) bit error rate

Cryptographic IOS Software (optional)

The Stratix 8000 and Stratix 8300 cryptographic IOS (available as a separate catalog number for downloading) provides network security by encrypting administrator traffic during Telnet and SNMP sessions. The cryptographic IOS supports all features of the standard IOS, as well as these protocols:

- Secure Shell (SSH) Protocol v2
- SNMPv3
- HTTPS

Cable Diagnostics

The Cable Diagnostics feature lets you run a test on each switch port to determine the integrity of the cable connected to the gigabit ports or the RJ45 (copper) ports. This feature is not available for fiber ports.

The test determines the distance to the break from the switch for each cable with a plus or minus error value individually listed.

Advanced Software Features

More advanced software features are available, some of which are configured by the global macro or port roles for typical automation applications described in this manual.

For information about how to configure features not available in the Device Manager Web interface or Studio 5000 environment, see the following manuals:

- For more information about these features and how to modify them, see the Cisco IE3000 Switch Software Configuration Manual, available from http://www.Cisco.com.
- For information about using the command-line interface for more detailed configuring of these software features, see the Cisco IE3000 Switch Command-Line Interface Manual, available from http://www.Cisco.com.

Notes:

Manage the Switch via the Device Manager Web Interface

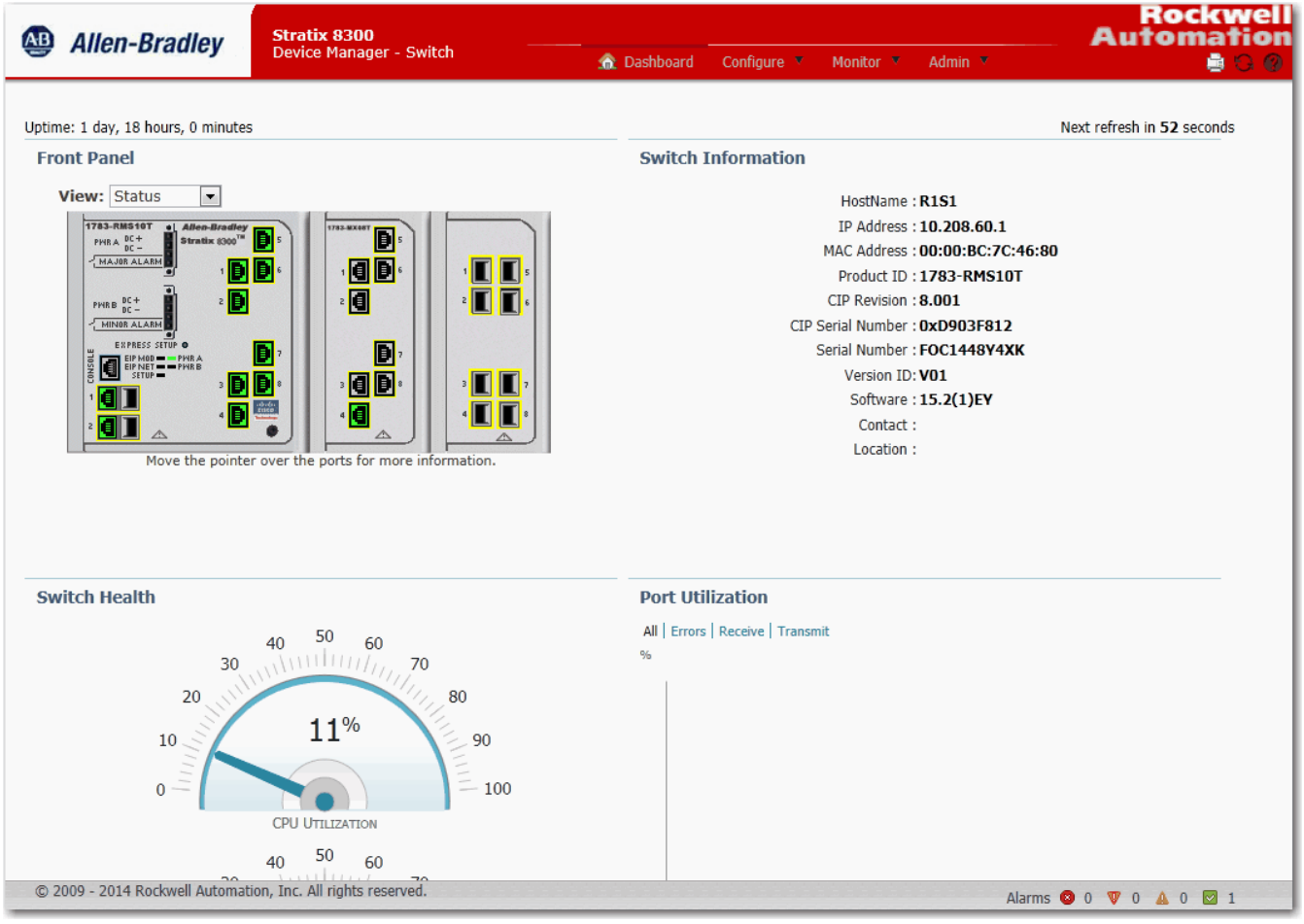
After you complete Express Setup, you can manage the switch by using the Device Manager Web interface supplied with the switch.

On all windows accessible from the Configure menu, when you save you changes, the changes are applied to the switch and stored on the CompactFlash card. If you exit the Device Manager Web interface without clicking Submit, your changes are not applied.

Access the Device Manager Web Interface

To access the Device Manager Web interface, follow these steps.

1. Launch a web browser on your workstation.
2. Enter the switch IP address in the web browser and click Enter.
3. Enter the user name and password.



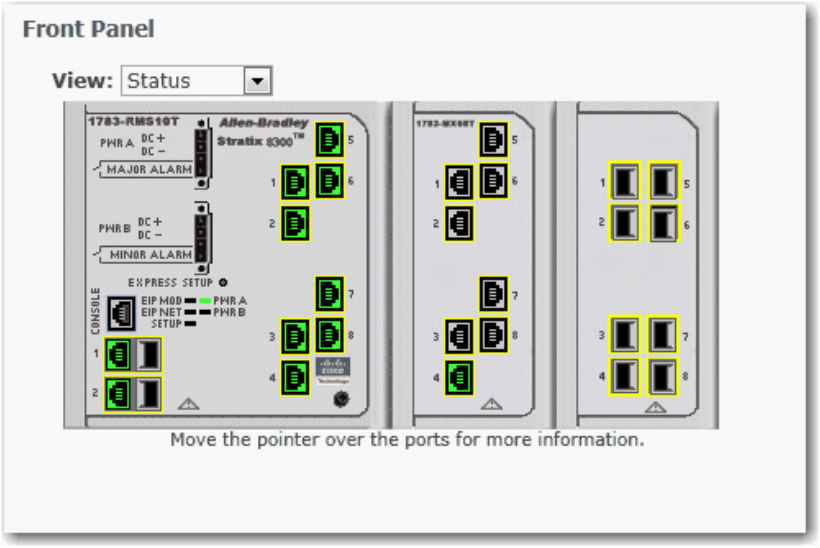
Dashboard Overview

You can use the dashboard to monitor switch status and performance.

The Dashboard window is similar to the Monitor > Trends window. The Dashboard window displays the instantaneous status while the Trends window displays the historical status. By using them together, you can gather the detailed conditions of the switch and its ports. For information about the Trends window, see page 127.

Front Panel View and Status Indicators

The Front Panel view is a graphical display of the front panels of the base switch and attached switch expansion modules.



The switch components on the Front Panel view are color-coded by status. The colors help you to quickly see if a fault or an error condition exists. The system-level status indicators and port-level status indicators shown on the Front Panel view match those on the physical switch.

Table 5 - System-level Status Indicators

Indicator	Status	Description
EIP Mod	The EIP Mod status indicator shows the status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch is operating properly.
	Blinking green	The switch is not configured. For example, the switch does not have an IP address configured.
	Blinking red	The switch has detected a recoverable system fault. Use the System Log to see more details about the problem. See View System Log Messages on page 132.
	Solid red	The switch has detected a non-recoverable system. Use the System Log to see more details about the problem. See View System Log Messages on page 132.
	Blinking green and red	The switch is running its power-on self-test (POST).

Table 5 - System-level Status Indicators (continued)

Indicator	Status	Description
EIP Net	The EIP Net status indicator shows the network status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch has an established CIP connection to one or more attached devices.
	Blinking green	The switch has an IP address but the switch does not have an established connection to one or more attached devices.
	Blinking red	One or more connections to attached devices have timed out.
	Solid red	The switch has detected that its IP address is already in use by another device in the network.
	Blinking green and red	The switch is running its power-on self-test (POST).
Setup	The Configuration mode in which the switch is operating.	
	Off	The switch is configured as a managed switch or the switch is operating as an unmanaged switch.
	Blinking green	Switch is in the initial Setup mode or is in the Direct Managed mode, or the initial setup is incomplete.
Pwr A and Pwr B	The Pwr status indicators show the DC power status.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	Power is present.
	Solid red	Power to the switch is not present and the power alarm is on.

Table 6 - Port-level Status Indicators

Indicator	Status	Description
Status	In this mode, the port status indicators show the status of the ports. This is the default mode.	
	Off	No link
	Solid green	No activity on link.
	Flashing green	Link activity.
	Solid brown	Port has been disabled.
	Yellow	An error has disabled the port.
	Flashing green and amber	Faulty link.
Status	Flashing amber	Smartports configuration mismatch on port.
	Solid amber	Port is faulty, disabled due to an error, or is in an STP-blocked state.
Duplex	In this mode, the port status indicators show the Duplex mode (Full-duplex or Half-duplex) of the ports. The 10/100/1000 ports operate only in Full-duplex mode.	
	Off	No link.
	Solid light blue	Port is in Half-duplex mode.
	Solid green	Port is in Full-duplex mode.
Speed	In this mode, the port status indicators show the operating speed (10, 100, or 1000 Mbps) of the ports.	
	Off	No link.
	Solid light blue	10 Mbps
	Solid green	100 Mbps
	Flashing green	1000 Mbps
Smartports	In this mode, each port image shows the applied port role.	

You can change the port status indicator behavior by choosing a Port mode from the View list on the Front Panel view.

Move the pointer over a port to display specific information about the port and its status.

TIP If you move the pointer over a port that is blinking green and amber, the status is one of the following:

- Link is faulty.
- Link has collisions.

In either state, the port is receiving and sending traffic.

Note the following:

- The speed and Duplex mode for a port appear only in the pop-up dialog box when a device is connected to the port.
- For dual-purpose ports, the Type field in the pop-up dialog box displays 10/100/1000BaseTX for the copper uplink port whether or not the port is active. The Type field also displays either the type of SFP module installed or Empty if a module is not installed.
- The Smartport type and VLAN type and name appear when Smartport Port mode is selected.
- The Uptime field shows how long the switch has been operating since it was last powered on or was restarted. Status is automatically refreshed every 60 seconds or when you click Refresh. The refresh counter shows the number of seconds that remain before the next refresh cycle starts.

Switch Information

The Switch Information area on the Dashboard displays information about the switch, as described in the following table.

Field	Description
Host Name	A descriptive name for this switch. The default name is Switch. You can set this parameter on the Admin > Express Setup window.
IP Address	The IP address of this switch. You can configure this setting on the Admin > Express Setup window.
MAC Address	The MAC address of this switch. This information cannot be changed.
Product ID	The model of this switch. This information cannot be changed.
CIP Revision	The version of Common Industrial Protocol (CIP) that is supported on this switch. This information cannot be changed.
CIP Serial Number	The CIP serial number. This information cannot be changed.
Serial Number	The serial number of this switch. This information cannot be changed.
Version ID	The hardware version. This information cannot be changed.
Software	The version of IOS that this switch is running. This information is updated when you upgrade the switch firmware.
Contact	The person who is the administrative contact for this switch. You can set this parameter on the Configure > SNMP window.
Location	The physical location of this switch. You can set this parameter on the Configure > SNMP window.

Switch Health

You can use the health gauges to monitor the switch.

CPU Utilization

The CPU Utilization gauge shows the percentage of CPU processing power that is in use on the switch. Data is collected at each 60-second system refresh. The gauge changes as the switch experiences the network activity from devices sending data through the network. As network activity increases, so does contention between devices to send data through the network.

As you monitor utilization on the switch, note whether the percentage of usage is what you expect during that given time of network activity. If utilization is high when you expect it to be low, perhaps a problem exists. As you monitor the switch, note if the bandwidth utilization is consistently high. This can mean there is congestion in the network. If the switch reaches its maximum bandwidth (above 90% utilization) and its buffers become full, it begins to discard the data packets that it receives. Some packet loss in the network is not considered unusual, and the switch is configured to help recover lost packets, such as by signaling to other devices to resend data. However, excessive packet loss can create packet errors, which can degrade overall network performance.

To reduce congestion, consider segmenting the network into subnetworks that are connected by other switches or routers. Look for other causes, such as faulty devices or connections, that can also increase bandwidth utilization on the switch.

Temperature

The Temperature gauge shows the internal temperature of the switch. For information about the switch temperature range and the operating environment guidelines, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Port Utilization

You can choose which types of network traffic to display and in what format:

- Types of traffic—By default, all traffic is displayed for all interfaces. Click the links above the display area to display all traffic, errors, received traffic, or transmitted traffic.
- Formats—Click the buttons below the display area to view the data in Chart Mode or Grid Mode.
- Chart details—When displaying a chart, position your mouse pointer over a bar or a point on the chart to view the data.

As you monitor the usage on the ports, note whether the percentage is what you expect during that given time of network activity. If usage is high when you expect it to be low, a problem can exist. Bandwidth allocation can also be based on whether the connection is operating in half-duplex or full-duplex mode.

These are some of the reasons for errors received on or sent from the switch ports:

- Bad cable connection
- Defective ports
- Software problems
- Driver problems

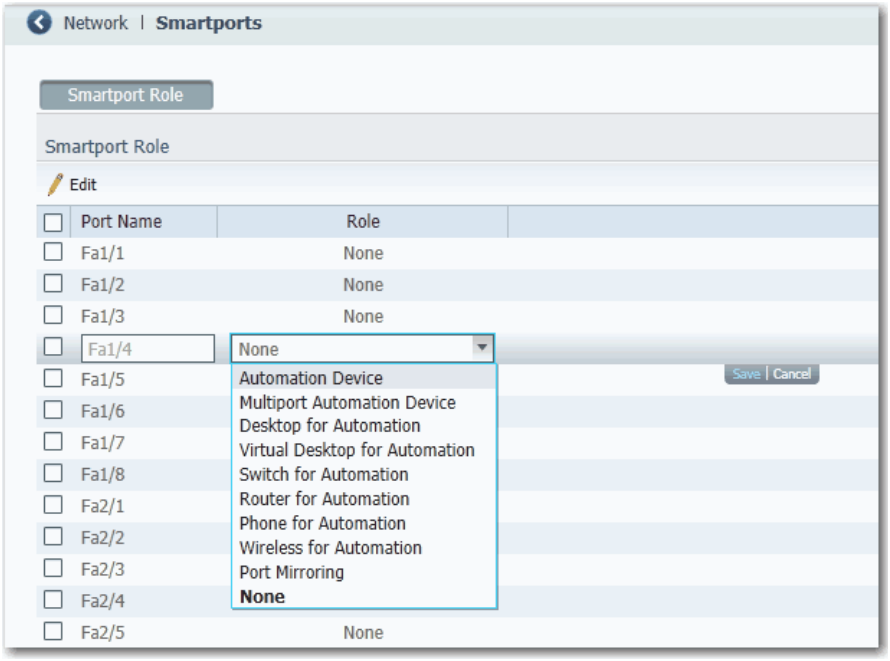
Data is collected at each 60-second system refresh.

Refer to Monitor Trends on page 127 for a graph to view per-port patterns over incremental instances in time (by 60 seconds, 1 hour, 1 day, or 1 week).

Refer to Monitor Port Statistics on page 128 for details on the specific port errors detected on each port.

Configure Smartports

To assign Smartport roles to switch ports, from the Configure menu, choose Smartports.



Follow these guidelines when using Smartport roles:

- Before using Smartports, decide which switch port to connect to which device type.
- Before attaching a device to the port or reconnecting devices that have been moved, verify which Smartports role is applied to a port.

IMPORTANT	We recommend that you do not change port settings after enabling a Smartports role on a port. Any port setting changes can alter the effectiveness of the Smartports role.

- When you attempt to apply a port role to a routed port on the Smartports page, this error message appears:

  A port role cannot be configured on a routed port.

To apply a Smartport role, follow this procedure.

1. From the Configure menu, choose Smartports.
2. Select a port.
3. From the Role column's pull-down menu, choose a Smartport role.
4. Click Save.

Customize Smartport Role Attributes

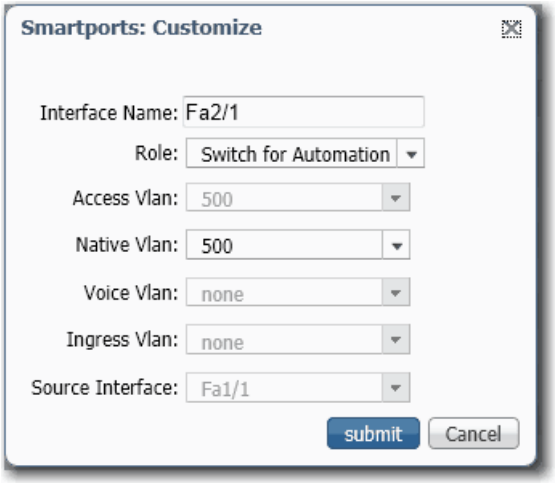
Each switch port is a member of a virtual local-area network (VLAN). Devices attached to switch ports that belong to the same VLAN share the same data broadcasts and system resources. Communication between VLANs requires a Layer 3 device, such as a router or a Layer 3 switch.

Depending on your network requirements, You can assign all ports to the default VLAN. In a small network, one VLAN can be sufficient.

Before changing the VLAN memberships, understand what a VLAN is, its purpose, and how to create a VLAN. Refer to VLANs on page 66 for more information about VLANs.

To customize a smartport role attribute for a port, follow this procedure.

1. From the Configure menu, choose Smartports.
2. Select a port.
3. Click Edit.
4. Modify the fields on the Smartports: Customize window as needed.



5. Click Submit.

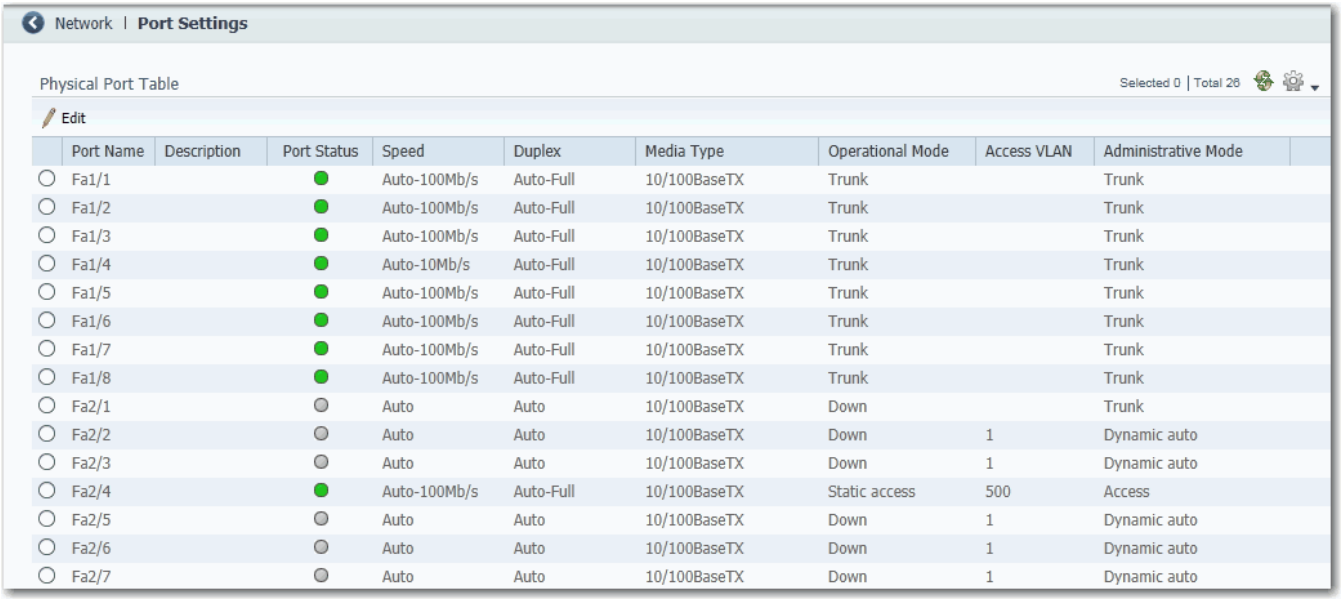
Configure Port Settings

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

Validation blocks you from configuring port roles for a routed port.

To change basic port settings, follow this procedure.

1. From the Configure menu, choose Port Settings.



	Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
○	Fa1/1		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
○	Fa1/2		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
○	Fa1/3		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
○	Fa1/4		●	Auto-10Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
○	Fa1/5		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
○	Fa1/6		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
○	Fa1/7		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
○	Fa1/8		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
○	Fa2/1		●	Auto	Auto	10/100BaseTX	Down		Trunk
○	Fa2/2		●	Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
○	Fa2/3		●	Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
○	Fa2/4		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	500	Access
○	Fa2/5		●	Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
○	Fa2/6		●	Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
○	Fa2/7		●	Auto	Auto	10/100BaseTX	Down	1	Dynamic auto

2. Click the radio button next to the port to configure.
3. Click Edit.

4. Modify the fields on the Edit Physical Port window.

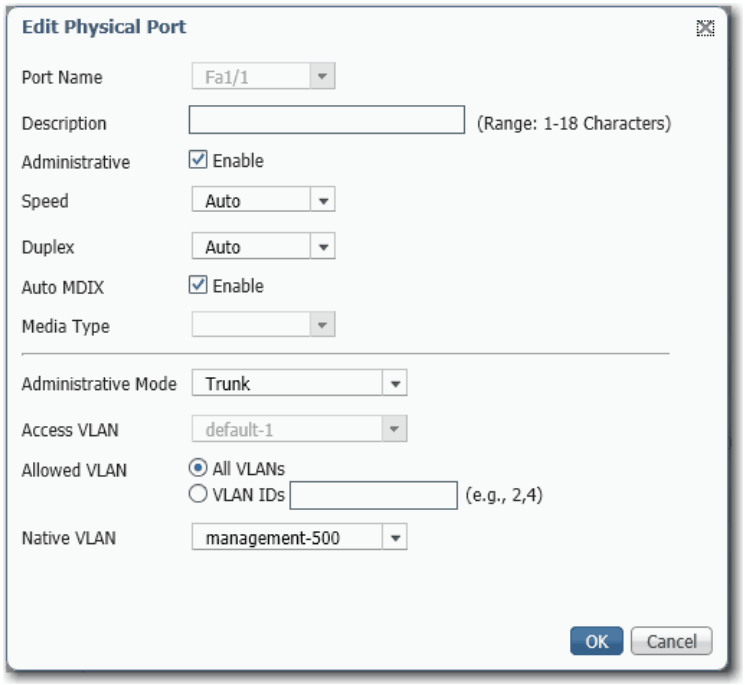


Table 7 - Edit Physical Port Fields

Field	Description
Port Name	The number of the switch port, including the port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base switch or the switch expansion module number (1, 2, or 3), and the specific port number: • Gi/1 is the gigabit port 1 of the base switch. • Fa1/1 is Fast Ethernet port 1 on the base switch. • Fa2/1 is Fast Ethernet port 1 on the first switch expansion module. • Fa3/1 is Fast Ethernet port 1 on the second switch expansion module.
Description	The description of the switch port. The limit is 18 characters. 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.
Administrative	The state of the switch port. The default is Enable. We recommend disabling the port if the port is not in use and is not attached to a device. An example of when to change this setting is during troubleshooting. You can troubleshoot a suspected unauthorized connection by manually disabling the port.
Port Status	The state of the switch port. The default is Enable. We recommend disabling the port if the port is not in use and is not attached to a device. An example of when to change this setting is during troubleshooting. You can troubleshoot a suspected unauthorized connection by manually disabling the port.
Speed	The operating speed of the switch port. You can choose Auto (autonegotiation) if the connected device can negotiate the link speed with the switch port. The default is Auto. We recommend that you use the default so that the speed setting on the switch port automatically matches the setting on the connected device. Change the switch port speed if the connected device requires a specific speed. An example of when to change this setting is during troubleshooting. If you are troubleshooting a connectivity problem, you can change this setting to verify if the switch port and connected device have a speed mismatch.
Duplex	The Duplex mode of the switch port is one of the following: • Auto (autonegotiation) if the connected device can negotiate with the switch. • Full (full-duplex) if both devices can send data at the same time. • Half (half-duplex) if one or both devices cannot send data at the same time. The default is Auto. On Gigabit Ethernet ports only, you cannot set the port to Half-duplex if the port speed is set to Auto. We recommend that you use the default so that the duplex setting on the switch port automatically matches the setting on the connected device. Change the Duplex mode on the switch port if the connected device requires a specific mode. An example of when to change this setting is during troubleshooting. If you are troubleshooting a connectivity problem, you can change this setting to verify if the switch port and connected device have a duplex mismatch.

Table 7 - Edit Physical Port Fields (continued)

Field	Description
Auto MDIX	Whether the automatic medium-dependent interface crossover (auto-MDIX) feature can automatically detect the required cable connection type (straight-through or crossover) and configure the connection appropriately. The default is Enable. This setting is not available on the SFP module ports.
Media Type	The active port type (either the RJ45 port or the SFP module port) of a dual-purpose uplink port. By default, the switch detects whether the RJ45 port or SFP module port of a dual-purpose port is connected and uses the port accordingly. Only one port can be active at a time. If both ports are connected, the SFP module port has priority. You cannot change the priority setting. Choose from the following media types: • SFP if the SFP module port must be active. If you select this option, the speed and duplex displays the current settings, and auto-MDIX displays N/A. • RJ45 if the RJ45 port must be active. If you select this option, you can set the port speed, duplex, and auto-mdix values. • Auto (autonegotiation) if either port can be active. If you select this option, the speed and duplex is set to auto, and auto-MDIX displays N/A. The default is Auto.
Administrative Mode	Displays one of the following administrative modes: • Access—The interface is in permanent nontrunking mode and negotiates to convert the neighboring link into a nontrunk link even if the neighboring interface is a trunk interface. If you choose this option, also choose an Access VLAN. An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). • Trunk—The interface is in permanent trunking mode and negotiates to convert the neighboring link into a trunk link even if the neighboring interface is not a trunk interface. If you choose this option, also choose whether to allow All VLANs or specified VLAN IDs • Dynamic Auto—The interface converts the link to a trunk link if the neighboring interface is set to Trunk or Desirable mode. This mode is the default setting. If you choose this option, specify an Access VLAN to use when the link is in Access mode. Also specify whether to allow All VLANs or specified VLAN IDs when the link is in Trunk mode. • Dynamic Desirable—The interface converts the link to a trunk link if the neighboring interface is set to Trunk, Dynamic Desirable, or Auto mode. If you choose this option, specify an Access VLAN to use when the link is in access mode. Also choose whether to allow All VLANs or specified VLAN IDs when the link is in Trunk mode.
Access VLAN	The VLAN that an interface belongs to and carries traffic for, when the link is configured as or is acting as a nontrunking interface.
Allowed VLAN	The VLAN or VLANs that this interface handles traffic for, when the link is configured as or is dynamically acting as a trunking interface. To allow traffic on all available VLANs, click All VLANs. To limit traffic to specific VLANs, click VLAN IDs and enter the VLAN numbers.
Native VLAN	The VLAN that is used to transport untagged packets.

Configure Ports to Use QuickConnect Technology

EtherNet/IP QuickConnect technology enables EtherNet/IP devices to quickly power up and join an EtherNet/IP network. The Stratix 8000 and Stratix 8300 switches can be an integral part of a network configuration that uses QuickConnect technology. To use the switches in a network that supports QuickConnect technology, you must apply certain port settings to the switch. For information about configuring the switch and applying port settings for QuickConnect technology, refer to the Ethernet QuickConnect Application Technique, publication ENET-AT001.

Configure Port Thresholds

Configure port thresholds to prevent traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces.

To configure port thresholds, from the Configure menu, choose Port Thresholds.

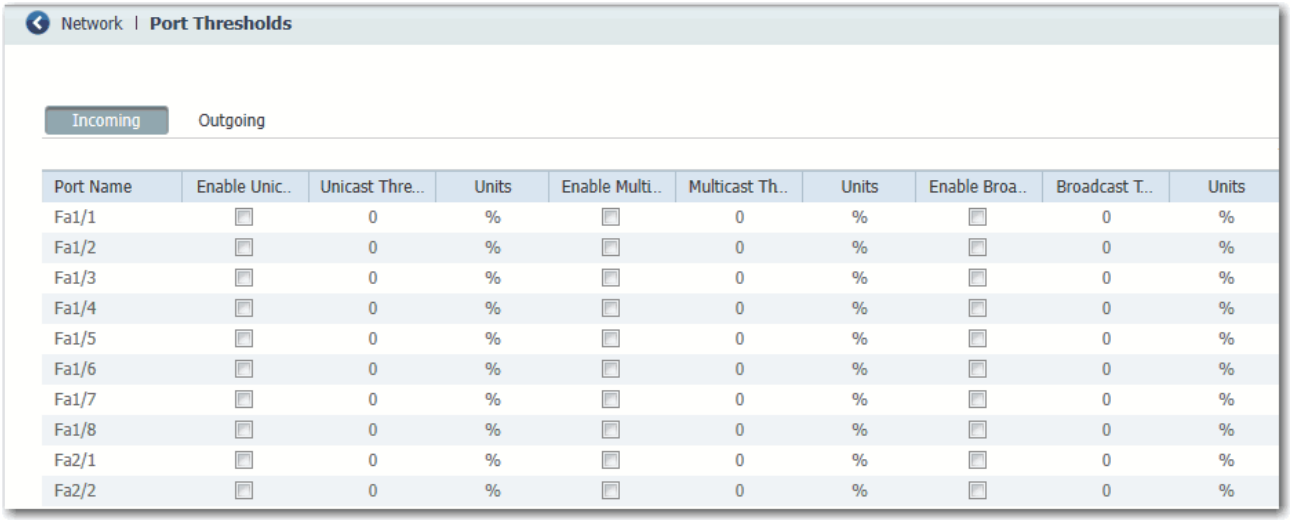


Table 8 - Port Threshold Fields

Field	Description
Incoming	
Unicast Multicast Broadcast	For each port, do the following. 1. Check or clear the Enable checkbox. 2. Type the threshold value. 3. Choose one of these units: – PPS (0…10 billion) – BPS (0…10 billion) – % (0…100)
Outgoing	
All Traffic	For each port, do the following. 1. Check or clear the Enable checkbox. 2. Type the threshold value. 3. Click Save.

Configure EtherChannels

An EtherChannel, or port group, is a group of two or more switch ports bundled into a single logical link to create a higher bandwidth link between two switches.

For example, four 10/100 switch ports can be assigned to an EtherChannel to provide full-duplex bandwidth of up to 800 Mb/s. If one of the ports in the EtherChannel becomes unavailable, traffic is carried over the remaining ports within the EtherChannel.

All ports in an EtherChannel must have the same characteristics:

- All are applied with the Smartports IE Switch port role and belong to the same VLAN.
- All are either 10/100 ports, or all are 10/100/1000 ports. You cannot group a mix of 10/100 and 10/100/1000 ports in an EtherChannel.
- All are enabled. A disabled port in an EtherChannel is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel.

IMPORTANT Do not enable Layer 3 addresses on the physical EtherChannel interfaces.

To create, modify, and delete EtherChannels, from the Configure menu, choose EtherChannels.

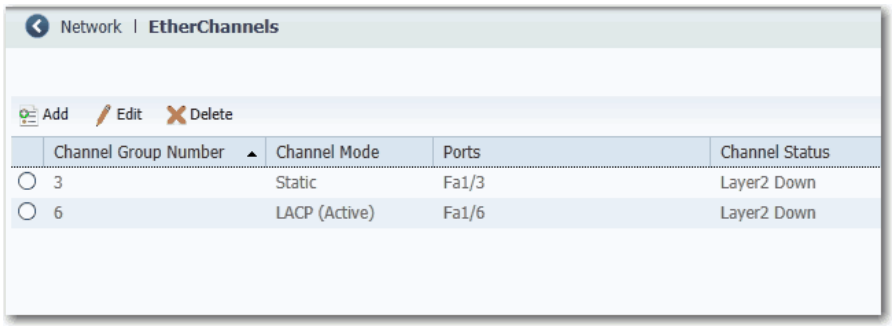


Table 9 - EtherChannel Fields

Field	Description
Channel Group Number	A number from 1 to 6 that identifies this EtherChannel. You can configure as many as six EtherChannels.
Channel Mode	Determines how ports become active. With all options except On, 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:** Verify that all of the ports in an EtherChannel are configured with the same speed and duplex mode. These are the available modes: • Static—All ports join the EtherChannel, without negotiations. This mode can be useful if the remote device does not support the protocols required by the other modes (see below). The switches at both ends of the link must be configured in On mode. • PAgP—This mode enables Port Aggregation Protocol (PAgP), a Cisco-proprietary protocol. The port responds to requests to create EtherChannels but does not initiate such negotiations. This silent mode is recommended when a port is connected to a device, such as a file server or a packet analzyer, that is unlikely to send PAgP packets. A port in the Auto mode can form an EtherChannel with another port in the Desirable mode. • PAgP (non-silent)—This mode is the same as Auto mode but is recommended when the port is connected to a device that is expected to be active in initiating EtherChannels. A port in the Auto mode can form an EtherChannel with another port in the Desirable mode. • PAgP Desirable—This mode enables Port Aggregation Protocol (PAgP), a Cisco-proprietary protocol. The port initiates negotiations to form EtherChannels by sending PAgP packets to other ports. This silent mode is recommended when a port is connected to a device, such as a file server or a packet analzyer, that is unlikely to send PAgP packets. A port in the Desirable mode can form an EtherChannel with another port that is in the Desirable or Auto mode. • PAgP Desirable (non-silent)—This mode is the same as Desirable mode but is recommended when the port is connected to a device that is expected to be active in initiating EtherChannels. • LACP (Active)—This mode enables Link Aggregation Control Protocol (LACP) unconditionally. The port sends LACP packets to other ports to initiate negotiations to create EtherChannels. A port in Active mode can form an EtherChannel with another port that is in Active or Passive mode. The ports must be configured for full duplex. • LACP (Passive)—This mode enables Link Aggregation Control Protocol only if an LACP device is detected at the other end of the link. The port responds to requests to create EtherChannels but does not initiate such negotiations. The ports must be configured for full duplex.
Ports	The ports that can participate in this EtherChannel.
Channel Status	The status of the group.

Configure DHCP

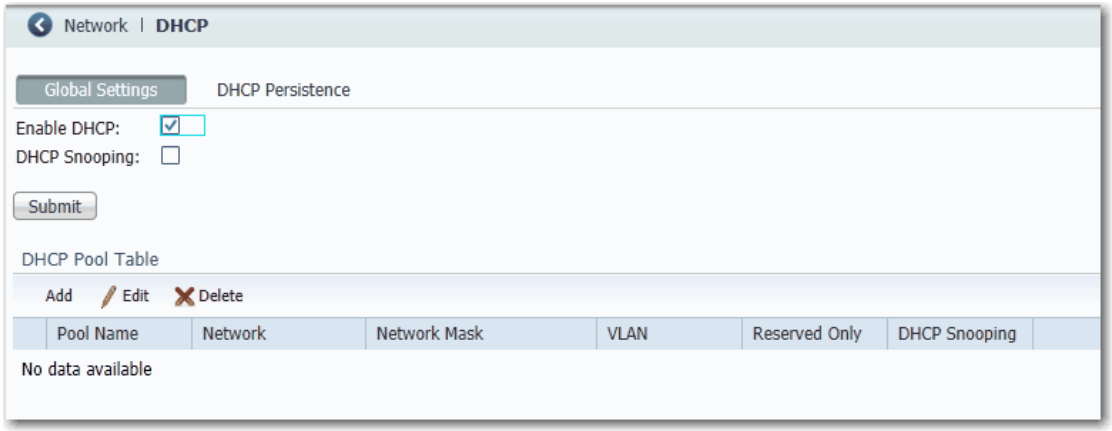
To use DHCP persistence, you must first enable DHCP and set up the IP address pool. Then you must assign a specific IP addresses to each port.

Set up the DHCP Server

To enable the DHCP Server mode on the switch, do the following.

1. From the Configure menu, choose DHCP.
2. Check Enable DHCP.
3. To enable DHCP snooping, check DHCP Snooping.

   DHCP snooping restricts the broadcast of DHCP requests beyond the connected switch. This means that devices receive address assignments from only the connected switch. This option is available only on VLAN interfaces. To enable DHCP Snooping on a specific VLAN, check DHCP Snooping for the specific VLAN in the DHCP Pool table.



4. To reserve an address pool to only the devices that are specified in the DHCP persistence table, check Reserved Only in the DHCP pool table.

   DHCP requests from ports not in the persistence table or from another device (switch) are ignored. By default, this option is disabled and the Reserved Only checkbox is cleared.

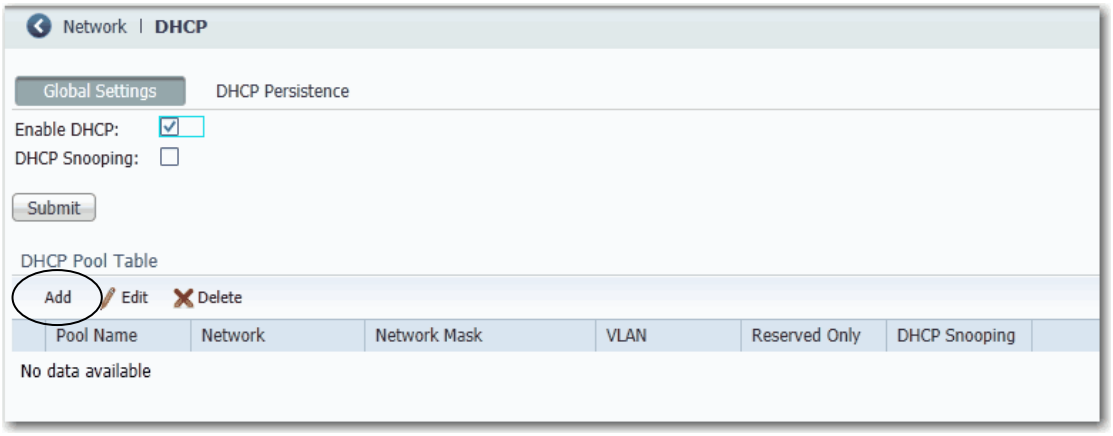
5. Click Submit.

Configure a DHCP IP Address Pool

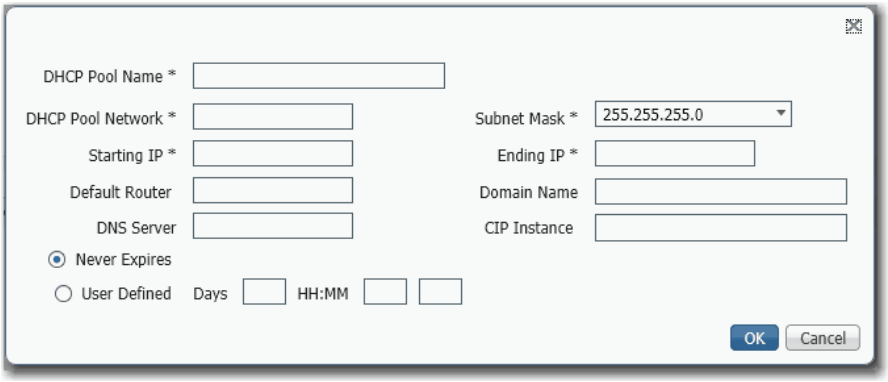
Once DHCP is enabled, you can create the DHCP address pool.

To configure a DHCP IP address pool, follow these steps.

1. From the Configure menu, c hoose DHCP.
2. Click Add.



3. Complete the fields as described below and click OK.



Field	Description
DHCP Pool Name	The name of the DHCP IP address pool configured on the switch. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab. This field is required. A DHCP IP address pool is a range (or pool) of available IP addresses that the switch can assign to connected devices.
DHCP Pool Network	The subnetwork IP address of the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. This field is required.
Subnet Mask	The network address that identifies the subnetwork (subnet) of the DHCP IP address pool. Subnets segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is required.
Starting IP	The starting IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers 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.

Field	Description
Ending IP	The ending IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. Make sure that none of the IP address you assign are being used by other devices in your network. This field is required.
Default Router	The default router IP address for the DHCP client that uses this server. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0… 255.
Domain Name	The domain name for the DHCP client. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab.
DNS Server	The IP addresses of the Domain Name System (DNS) IP servers available to a DHCP client. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255.
CIP Instance	A number from 1…15 to identify the address pool.
[Lease Length]	The duration of the lease for an IP address that is assigned to a DHCP client. Click one of the following: • Never Expires • User Defined If you click User Defined, enter the duration of the lease in the numbers of days, hours, and minutes. This lease length is used for all assignments.

Reserve IP Addresses through DHCP Persistence

You can reserve and preassign an IP address from the IP address pool to a specific switch port, so that a device connected to that switch port always receives the same IP address regardless of its MAC address.

DHCP persistence is useful in networks that are set up in advance, where dependencies on the exact IP addresses of some devices exist. Use DHCP persistence when the attached device has a specific role to play and when other devices know its IP address. If the device is replaced, the replacement device is assigned the same IP address, and the other devices in the network require no reconfiguration.

When the DHCP persistence feature is enabled, the switch acts as a DHCP server for other devices on the same subnet, including devices connected to other switches (including other Stratix 8000 switches). If the switch receives a DHCP request, it responds with any unassigned IP addresses in its pool. To prevent this from happening, check the Reserve Only box on the DHCP window. This prevents the switch from responding when it receives a request.

When DHCP persistence is enabled on a port and a DHCP request is made from a connected device on that port, the switch assigns the IP address for that port in the DHCP window. 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 attempt to respond. This can override the initial IP address assigned by the switch depending on how the end device behaves (takes first IP address response or the last). To prevent the IP address from being overridden, enable DHCP snooping on the appropriate VLAN. Doing this blocks the broadcast of this DHCP request, so that no other server, including another Stratix 8000 or Stratix 8300 switch with DHCP persistence enabled, responds.

If you are using DHCP persistence, we recommend that you initially assign static IP addresses to end devices. If an end device fails and is replaced, the DHCP persistence feature assigns an IP address from the DHCP persistence table. The device functions properly with this IP address, but we recommend that you reassign a static IP address to the replaced devices.

The following figure and table illustrate DHCP persistence behavior.

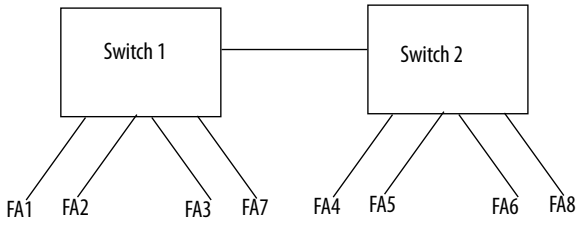


Table 10 - DHCP Persistence Behavior

If	Then
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • Reserve Only is not selected and DHCP snooping is off	A new device connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 responds if there is an unassigned address in its pool. This can override the assignment made by switch 1.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • Reserve Only is selected in both switches and DHCP snooping is off	A new device connected to switch 1 FA1 receives an IP address from the switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 does not respond to the request. Note that if the device is connected to FA7 of switch 1, it does not receive an IP address from the switch pool because it is not defined in the persistence table, and unused addresses in the pool are blocked.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • Reserve Only is selected in switch 1 and DHCP snooping is off, but not switch 2 when DHCP snooping is off	A new device is connected to FA1 receives an IP address from the persistence table. A broadcast request is also sent across the network. Switch 2 does not respond to the request. In addition, a device connected to FA4 receives an IP address from the switch 2 persistence table. A broadcast request is sent out, and switch 1 responds with an unused IP address from its pool.This can override the assigned port.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • DHCP Snooping is selected • Reserved Only is checked	A new device connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is not sent across the network, therefore Switch 2 does not respond. Note that if a device is connected to FA7 (not defined in the DHCP persistence table) of Switch 1, it does not receive an IP address from the switch pool because it is not defined in the persistence table, and unused addresses in the pool are blocked.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • DHCP Snooping is selected • Reserved Only is not checked	A new device connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is not sent across the network, therefore Switch 2 does not respond. Note that if a device is connected to FA7 (not defined in the DHCP persistence table) of Switch 1, it receives an unassigned IP address from the Switch 1 pool.

To assign, modify, or delete a switch port IP address, click the DHCP Persistence tab.

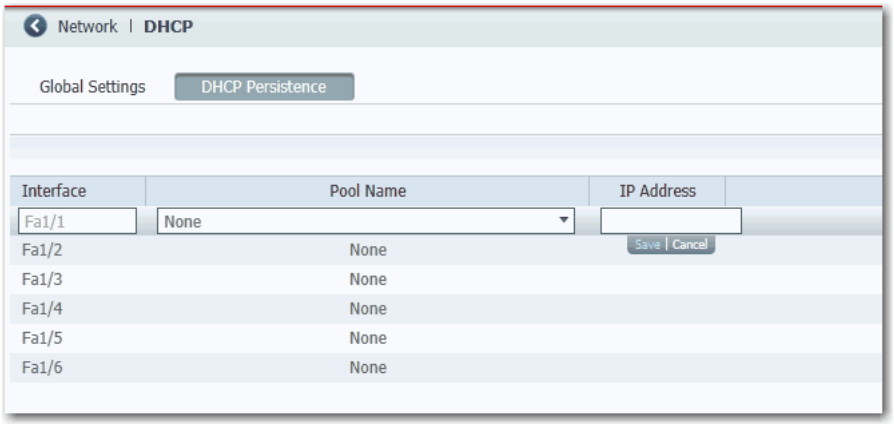
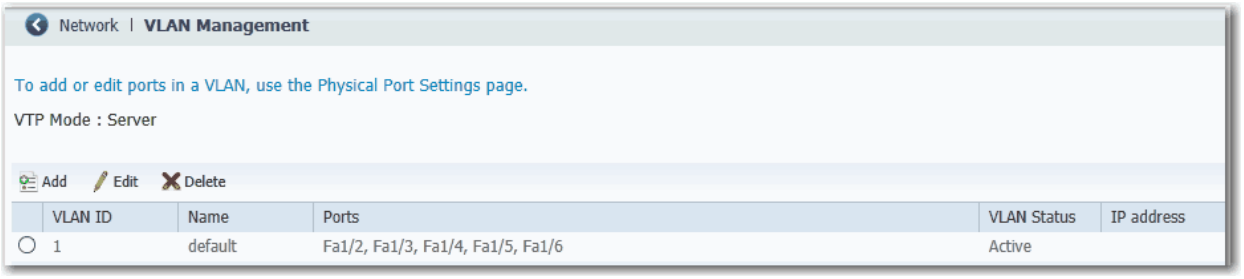


Table 11 - DHCP Persistence Fields

Field	Description
Interface	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), and the specific port number. For example, Fa1/1 is Fast Ethernet port 1 on the switch.
Pool Name	The name of the DHCP IP address pool configured on the switch.
IP Address	The IP address assigned to the switch port. The IP address that you assign is reserved for the selected port and is not available for normal DHCP dynamic assignment. The IP address must be an address from the pool specified in the DHCP Pool Name field.

Configure VLANs

To create, modify, and delete VLANs, from the Configure menu, choose VLAN Management.



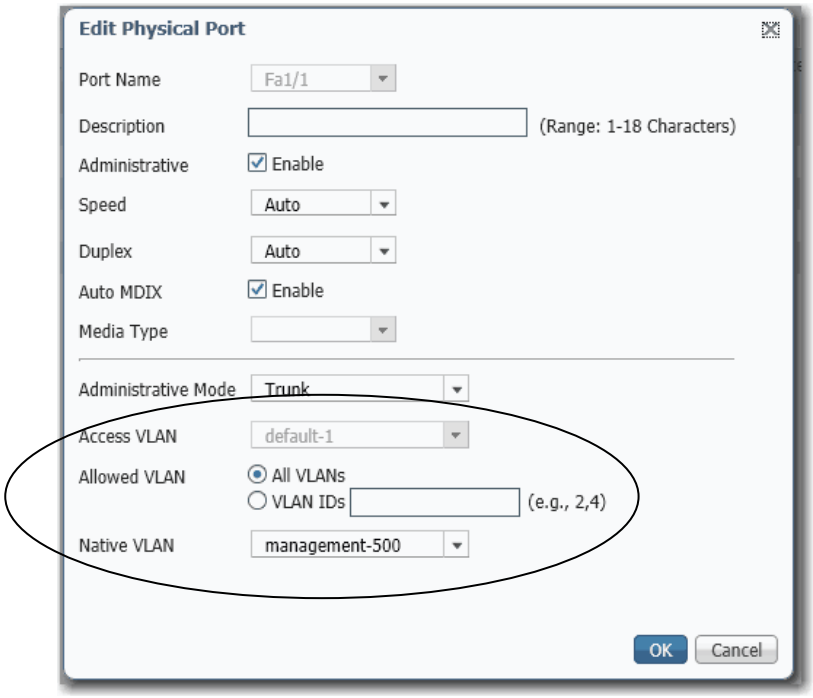
The default VLAN ID is 1 and the name for the management VLAN is default. The default VLAN alone can be sufficient based on the size and requirements of your network. We recommend that you determine your VLAN needs before creating VLANs.

To create a VLAN, you must give the VLAN a name and a unique ID number. You can modify the name of a VLAN but not its number. You cannot modify or delete the default VLAN.

After creating VLANs, you can then assign ports to VLANs. Before assigning ports to VLANs, make sure that each port has the appropriate port role.

Assign Ports to VLANs

To assign ports to VLANs, use the Edit Physical Ports window, as described on page 98.



Configure Power over Ethernet (PoE) Ports

PoE and PoE+ features are supported when the switch has a PoE expansion module installed and a correct power supply is connected to the switch. For power supply requirements, see page 31.

If a PoE expansion module is connected to the switch, you can do the following from the PoE window:

- View the PoE status of connected PoE expansion modules.
- Limit the total power supported.
- Configure mode and power settings for individual ports.

For most applications, the default configuration (Auto mode) is sufficient and no further configuration is required. However, you can customize the settings to meet your needs. For example, to give a PoE port higher power priority, set the mode to Static and allocate the power to be used. As another example, to disallow high-power devices on a port, set the mode to Auto and specify a maximum power limit.

IMPORTANT When you make PoE configuration changes to a port, the port drops power. Whether the port powers up again depends on the new configuration, the state of the other PoE ports, and the state of the power budget.

For example, if port 1 is in Auto mode and the On state, and you configure it for Static mode, the switch removes power from port 1, detects the powered device, and repowers the port.

If port 1 is in Auto mode and the On state and you configure it with a maximum wattage of 10 W, the switch removes power from the port and then redetects the powered device. The switch repowers the port only if the powered device is a Class 1, Class 2, or a Cisco-only powered device.

To configure PoE ports, from the Configure menu, choose Power Management.

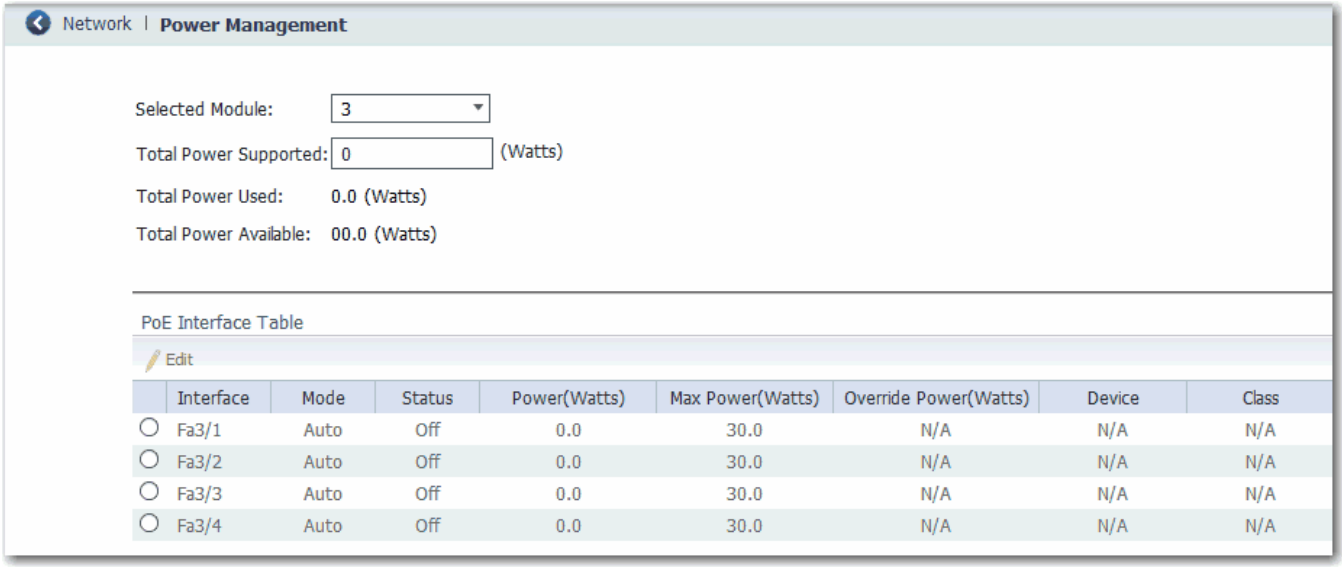


Table 12 - Power Management Fields

Field	Description
Selected Module	Choose a connected PoE module for which to view status information: • 2—Module in the left position • 3—Module in the right position
Total Power Supported	To limit the total PoE power budget, type an appropriate value based on the power source: • A 48V power source supports a maximum of 65 W. • A 54V power source supports a maximum of 130 W. When you save this setting, it changes the total PoE power budget and resets the powered devices to meet the new budget. **IMPORTANT:** A mismatch between the total power supported and the power supply can cause damage to the switch. Take care not to 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 specify 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 supported to an appropriate value and then change the power supply.
Total Power Used	Displays the amount of power the module is currently using.
Total Power Available	Displays the amount of unused power available to the module.
Interface	Displays the port number.

Table 12 - Power Management Fields (continued)

Field	Description
Mode	Displays the Power Management mode of the port: • Auto—Enables the detection of powered devices and automatically allocates power to the PoE port if a device is connected. This setting is selected by default. To limit the power used by this port, adjust the Max Power setting. • Static—Reserves power for this port even when no device is connected to make sure that power is provided upon device detection. You can also choose Static mode to prioritize a port. The switch allocates power to Static mode ports before it allocates power to Auto mode ports. • Off—PoE is disabled. For more information, see Power Management Modes on page 63.
Status	Displays whether PoE is enabled (on) or disabled (off) on the port.
Power (Watts)	Displays the amount of power allocated to the port.
Max Power (Watts)	Displays the maximum amount of power available to the port: PoE ports: 4…15.4 W PoE+ ports: 4…30 W
Override Power (Watts)	Indicates the power override configured for the port. This configuration overrides both the IEEE classification shown in the Class column and power negotiation. If no override is configured, the field displays N/A. You can configure a power override only by using the command line interface (CLI). For more information, refer to the Cisco IE-3000 Software Configuration Guide. **EXAMPLE** An administrator can choose to configure an override when the power requirement of a connected device is known and is less than the maximum value for the class. For instance, if a device requires only 5 W but is in Class 0, which allows a maximum of 15.4 W, configuring an override allows more power to other devices.
Device	Displays the device connected to the port. If no device is connected to the port, the field displays N/A.
Class	Displays the power classification of the powered device (PD). For power classification descriptions, see Table 3 on page 62.

Configure PTP Time Synchronization

The IEEE 1588 standard defines a protocol, called Precision Time Protocol (PTP), which enables precise synchronization of clocks in measurement and control systems. The clocks communicate with each other over the EtherNet/IP communication network. The PTP protocol enables heterogeneous systems that include clocks of various inherent precision, resolution and stability to synchronize. PTP generates a Master-Slave relationship among the clocks in the system. All clocks ultimately derive their time from a clock selected as the Grandmaster clock.

By default, PTP is disabled on all the Fast Ethernet and Gigabit Ethernet ports on the switch.

The switch supports these Synchronization Clock modes:

- **End-to-End Transparent mode**—The switch transparently synchronizes all slave clocks with the master clock connected to the switch.

  The switch corrects the delay incurred by every packet passing through the switch (referred to as residence time). This mode causes less jitter and error accumulation than Boundary mode.

  In End-to-End Transparent mode, all switch ports are enabled by default.

- **Boundary mode**—The switch becomes the parent clock to which the other devices connected to the switch synchronize their internal clocks.

  The switch and connected devices constantly exchange timing messages to correct time skew caused by clock offsets and network delays.

  This mode can eliminate the effects of latency fluctuations. Because jitter and errors can accumulate in cascaded topologies, use this mode for networks with only less than four layers of cascaded devices.

  In Boundary mode, one or more switch ports can be PTP-enabled.

- **Forward mode (default)**—Traffic is forwarded through the switch (while being prioritized by QoS) but is not acted on by the switch.

IMPORTANT When changing the PTP timing message settings, remember that the system does not operate properly unless all devices in the system have the same values.

To configure PTP, from the Configure menu, choose PTP.

Once you choose a mode, you can edit the settings for each port. The parameters depend on the selected mode. You can configure per-port PTP when the switch is in Boundary mode or End-to-end Transparent mode.

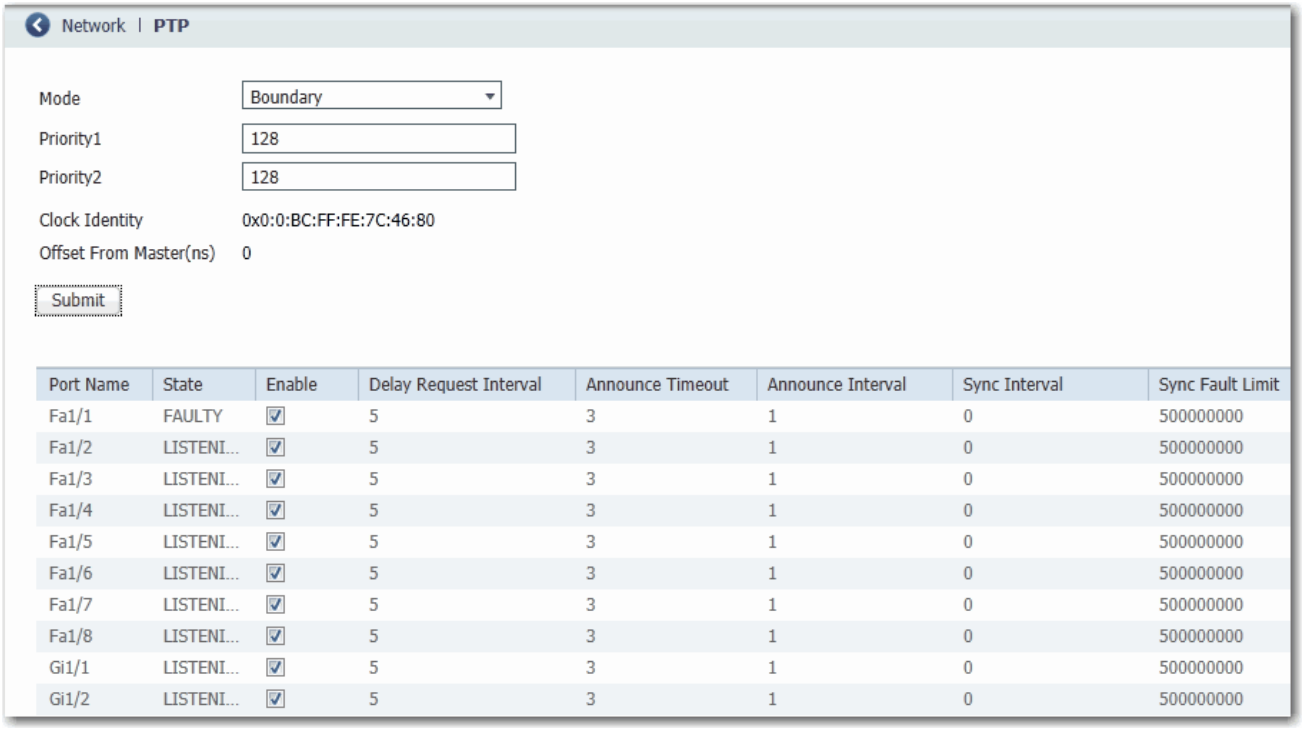


Table 13 - PTP Fields

Field	Description
Mode	Choose a PTP mode: • Boundary—Synchronizes all switch ports with the Grandmaster clock by using the IEEE 1588 V 2 Boundary clock mechanism. • End-to-End Transparent—Calculates and adds the switch delay into the PTP packet by using the IEEE 1588 V2 End-to-End Transparent clock mechanism. In this mode, all switch ports are PTP-enabled. In boundary mode, one or more switch ports can be PTP-enabled. You can enable or disable PTP on a per-port basis. • Forward (default)—Passes PTP packets through without interference.
Priority 1	The switch used to override the default criteria, such as clock quality or clock class, for the best master clock selection.
Priority 2	The switch used 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. The range is from 0…255. A lower values take precedence. The default is 128.
Clock Identity	The clock source.
Offset from Master (ns)	The accuracy in nanoseconds from the Grandmaster clock.
Port Name	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base switch number (1), and the specific port number. For example: Fa1/1 is Fast Ethernet port 1 on the base switch.

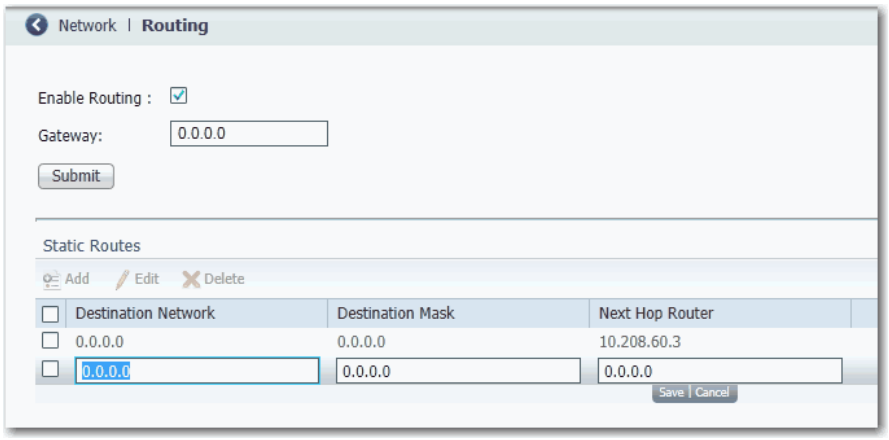
Table 13 - PTP Fields (continued)

Field	Description
State	(Boundary mode only.) The synchronization state on the switch port with the parent or Grandmaster clock: • Listening—The switch port is waiting while a parent or Grandmaster clock is selected. • Pre-master—The switch port is transitioning to change to Master state. • Master—The switch is acting as a parent clock to the devices connected to that switch port. • Passive—The switch has detected a redundant path to a parent or Grandmaster clock. For example, two different switch ports claim the same parent or Grandmaster clock. To prevent a loop in the network, one of the ports changes to Passive state. • Uncalibrated—The switch port cannot synchronize with the parent or Grandmaster clock. • Slave—The switch port is connected to and synchronizing with the parent or Grandmaster clock. • Faulty—PTP is not operating properly on that switch port. • Disabled—PTP is not enabled on the switch port.
Enable	By default, PTP is enabled on all the Fast Ethernet and Gigabit Ethernet ports on the base switch module. Only the ports on the base switch module are PTP-capable. The switch expansion modules do not support PTP. When at least one switch port is PTP-enabled, the Forward mode is selected by default. You can enable or disable PTP on a per-port basis.
Delay Request Interval	The time interval recommended to connected devices to send delay request messages when the switch port is in the master state: • **-1** means half second • **0** means 1 second • **1** means 2 seconds • **2** means 4 seconds • **3** means 8 seconds • **4** means 16 seconds • **5** means 32 seconds • **6** means 64 seconds The default is 5 (32 seconds).
Announce Timeout	The number of announce intervals that must pass without receipt of an announce message from the Grandmaster clock before the switch selects a new Grandmaster clock. The number can be from 2…10. The default is 3.
Announce Interval	The time interval for sending announce messages: • **0** means 1 second • **1** means 2 seconds • **2** means 4 seconds • **3** means 8 seconds • **4** means 16 seconds The default is 1 (2 seconds).
Sync Interval	The time interval for sending synchronization messages: • **-1** means half second • **0** means 1 second • **1** means 2 seconds The default is 0 (1 second).
Sync Fault Limit	The maximum clock offset before PTP attempts to reacquire synchronization. The value can be from 50…500,000,000 ns. The default is 50,000 ns. We recommend against setting the sync limit below the default (50,000 ns). Use values below 50,000 ns only in networks with a very-high-precision Grandmaster clock. These networks have a critical need to keep very sensitive devices synchronized.

Enable Static and Connected Routing

Before you can enable static and connected routing, you must reallocate switch memory for routing, as described on page 136.

To enable routing, from the Configure menu, choose Routing.



From the Routing window, you can enable connected routing only or both static and connected routing. When static routing is enabled, connected routing is enabled by default. For more information about these routing types, refer to Static and Connected Routing on page 84.

Enable Connected Routing Only

To enable connected routing only, check Enable Routing and click Submit.

No further configuration is required for connected routing.

Enable Both Static and Connected Routing

To enable both static and connected routing, follow these steps.

1. Check Enable Routing and click Submit.
2. Configure static route information as described below.

Field	Description
Destination Network	The IP address of the destination.
Destination Mask	The subnet mask of the destination.
Next Hop Router	The IP address of the router where this device will send the packets for the specified destination.

Configure STP

Spanning Tree Protocol (STP) modes include the following:

- Multiple Spanning Tree (MST) prevents network loops by enabling only one active path for traffic. MST also provides a redundant path if the active path becomes unavailable. This is the default STP mode.
- Per VLAN Spanning Tree Plus (PVST+) runs on each VLAN on the switch up to the maximum supported, ensuring loop-free path through the network.
- Rapid Per VLAN Spanning Tree Plus (RPVST+) immediately deletes dynamically learned MAC address entries upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC addresses.

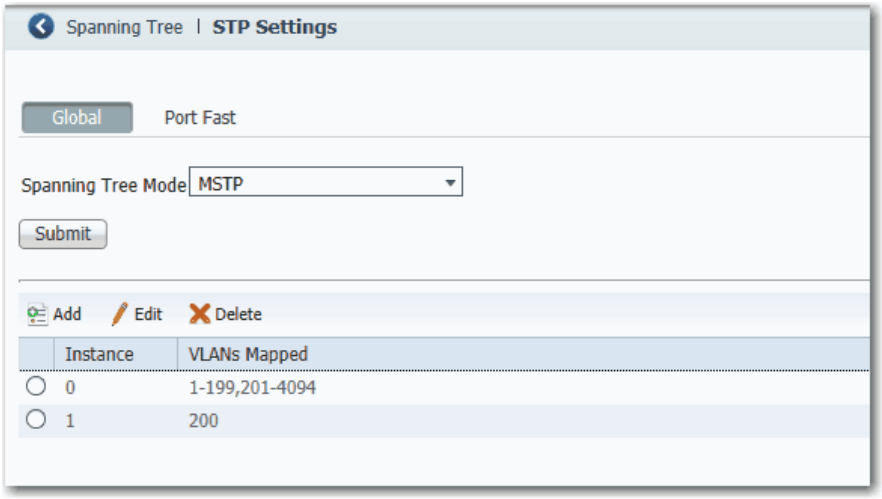
We recommend that you leave STP enabled to prevent network loops and provide a redundant path if the active path becomes unavailable.

IMPORTANT Disabling STP can affect connectivity to the network.

To configure Spanning Tree Protocol settings, from the Configure menu, choose STP.

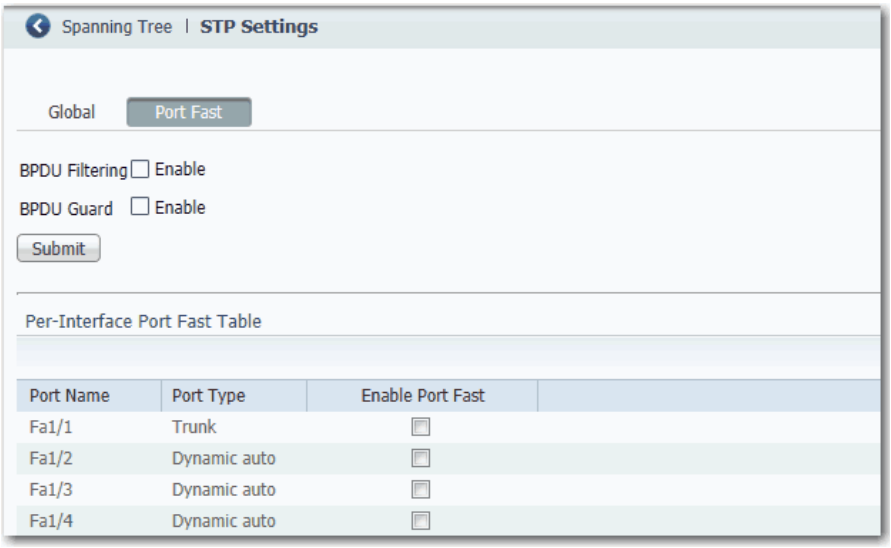
Global Settings

To choose the STP mode for the switch or to configure STP on individual VLANs, click the Global tab. On the Global tab, you can add, edit, or delete instances. If you choose PVST+ or Rapid PVST+ mode, you can enable or disable STP on each instance.



PortFast Settings

To enable PortFast and related features, click the PortFast tab. On the PortFast tab, you can change the way that STP is implemented on individual ports.



PortFast features are typically enabled only on access ports, which connect to devices such as personal computers, access points, and servers that are not expected to send bridge protocol data units (BPDUs). These features are typically not enabled on ports that connect to switches because spanning tree loops might occur.

BPDU Features

Switches exchange special frames called BPDUs to communicate network information, to track changes, and to create the STP topology. Because transmitted BPDUs reveal network information and received BPDUs can influence your STP topology, you might find it useful to enable BPDU Filtering and BPDU Guard on your access ports. These features prevent a rogue device from interfering with your STP topology. However, we recommend you use these features with caution:

- BPDU Filtering—This PortFast feature blocks all sending and receiving of BPDUs through all PortFast-enabled ports. This feature effectively disables STP on these ports and loops can result. If a BPDU is received, PortFast is disabled on the port and the global STP settings apply. To enable BPDU Filtering on all PortFast-enabled ports, check Enable.

- BPDU Guard—This PortFast feature shuts down a port if it receives a BPDU. To enable BPDU Guard on all Port Fast-enabled ports, check Enable.

Note that if you enable both of these features, BPDU Guard has no effect because BPDU Filtering prevents the port from receiving any BPDUs.

Per Interface PortFast Table

Spanning tree requires an interface to progress through the listening and learning states, to exchange information and establish a loop-free path before it can forward frames. On ports that connect to devices such as workstations and servers, you can allow an immediate connection. PortFast immediately transitions the port into STP forwarding mode upon linkup.

To enable PortFast on an interface and apply the selected BPDU features to the interface, select the interface, and then check Enable Port Fast.

Configure REP

To configure Resilient Ethernet Protocol (REP), from the Configure menu, choose REP.

To create an REP segment, set a segment ID and port type on the desired ports.

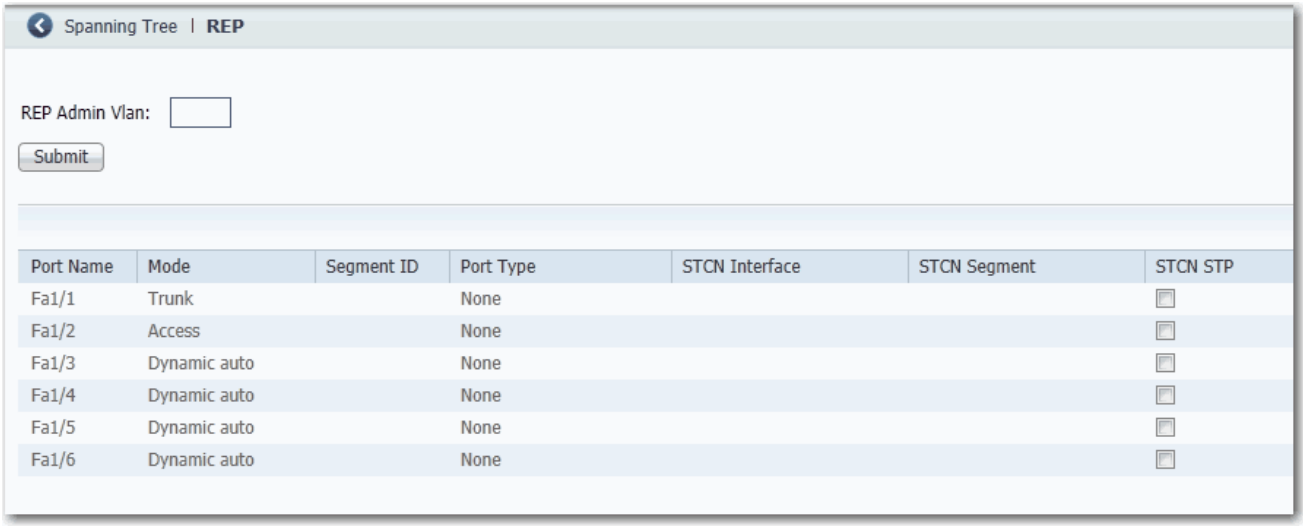


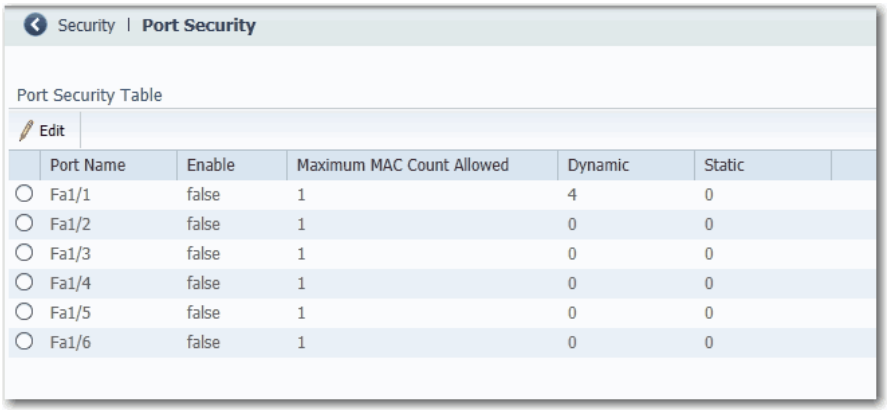
Table 14 - REP Fields

Field	Description
REP Admin VLAN	The administrative VLAN. The range is 2. . . 4094. The default is VLAN 1. REP ports are assigned to the same REP Admin VLAN. If the REP Admin VLAN changes, all REP ports are automatically assigned to the new REP Admin VLAN.
Port Name	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet).
Mode	The administrative mode. To set this mode, from the Configure menu, choose Port Settings.
Segment ID	The ID of the segment. The segment ID range is from 1. . . 1024. If no segment ID is set, REP is disabled.
Port Type	Each REP segment must have exactly two primary edge ports and may have secondary ports to use when a primary port fails. You can specify preferred primary and secondary ports. Configuring a port as preferred does not guarantee that it becomes the alternate port but gives it a slight edge among equal contenders. You also can indicate that a port is connected to switches that do not support REP. Choose one of these port types: • Edge—A secondary edge port that participates in VLAN load balancing. • Edge no-neighbor—A secondary edge port that is connected to a non-REP switch. • Edge no-neighbor preferred—A secondary edge port that is connected to a non-REP switch and is the preferred alternate port for VLAN load balancing. • Edge no-neighbor primary—A secondary edge port that always participates in VLAN load balancing in this REP segment and is connected to a non-REP switch. • Edge no-neighbor primary preferred—An edge port that always participates in VLAN load balancing in this REP segment, is connected to a non-REP switch, and is the preferred port for VLAN load balancing. • Edge preferred—A secondary edge port that is the preferred alternate port for VLAN load balancing. • Edge primary—An edge port that always participates in VLAN load balancing in this REP segment. • Edge primary preferred—An edge port that always participates in VLAN load balancing in this REP segment and is the preferred port for VLAN load balancing. • None—This port is not part of the REP segment. The default is None. • Preferred—A secondary edge port that is the preferred alternate port for VLAN load balancing.
STCN Interface	Configure segment topology change notices (STCNs) for a port. The default is None. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.
STCN Segment	Configure STCNs to a segment ID. The default is a blank field. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.
STCN STP	Configure STCNs to an STP network. The default is cleared checkbox. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.

Configure Port Security

Configure port security to limit the MAC addresses (MAC IDs) that can access a given port. Port security is based on the number of MAC addresses supported (none of which are statically defined). Static port security lets you specify whether MAC addresses are auto-learned or manually defined.

To configure port security, from the Configure menu, choose Port Security.



Port security limits and identifies the MAC addresses of devices that can send traffic through the switch port. The switch port does not forward traffic from devices outside the defined group of devices. A security violation occurs when any of the following conditions occur:

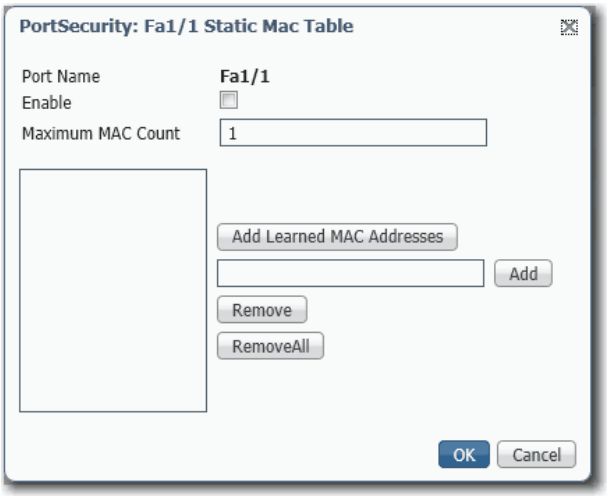
- A device, which has a MAC address different from any identified secure MAC addresses, attempts to access the switch port.
- The number of MAC addresses on the port exceeds the maximum number supported on the port.

Port security supports multiple security levels:

- The ability to define the number of devices that are connected to a given port. These are assigned on a first-come, first-served basis and time out after a certain period of inactivity.
- The ability to easily store the existing MAC Address configuration by selecting Add Learned MAC Addresses on the Static MAC Address Table.
- The ability to manually add and remove MAC Addresses on a per port basis.

To change the Static MAC Addresses table for a port, do the following.

1. Click the radio button next to the port to configure.
2. Click Edit.
3. Clear or check the Enable checkbox.
4. Configure MAC addresses as follows:
   - To add the existing MAC addresses of devices currently connected to a port, click Add Learned MAC Addresses.
   - To add a specific MAC address to the table, type a MAC address in the format fields and click Add.
   - To remove a MAC address from the table, select the MAC address and click Remove.
   - To clear the MAC address table, click Remove All.



5. Click OK.

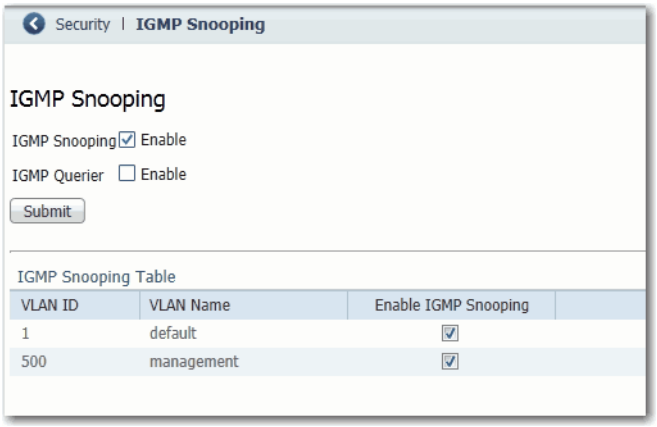
Configure IGMP Snooping

Internet Group Management Protocol (IGMP) snooping reduces duplicate and excess traffic on the network by forwarding IP multicast traffic to specific switch ports rather than by flooding all ports.

With IGMP snooping, ports that are members of only specific IP multicast groups receive multicast messages. The result is a more efficient use of bandwidth.

To configure IGMP snooping, from the Configure menu, choose IGMP Snooping:

- To enable IGMP Snooping for all VLAN IDs, check Enable next to IGMP Snooping.
- To enable IGMP Querier for all VLAN IDs, check Enable next to IGMP Querier.
- To enable or disable IGMP snooping on a VLAN, select the VLAN and check or clear the Enable IGMP Snooping checkbox.

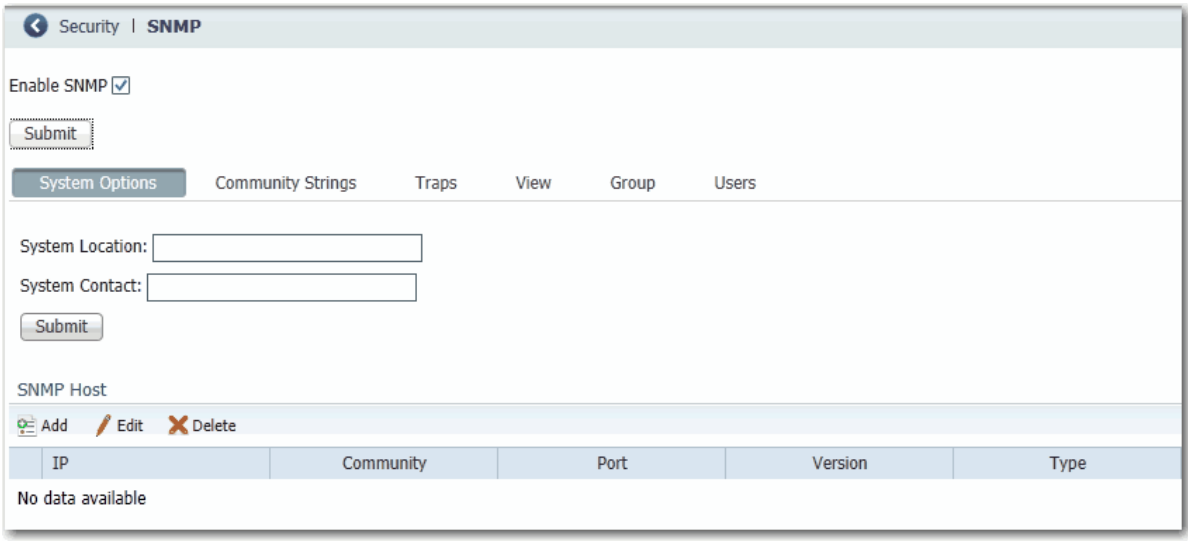


Configure SNMP

Enable SNMP if you plan to have the switch managed through another network management application. By default, SNMP is disabled.

Other general SNMP settings include the name of the switch or the network administrator and the switch location. The system name and the system contact information appear in the Switch Information area on the Dashboard.

To configure SNMP, from the Configure menu, choose SNMP.



Community strings are passwords to the switch Management Information Base (MIB). You can create community strings that provide a remote manager read-only or read-write access to the switch.

To create, modify, and delete community strings, click the Community Strings tab.

A read-only community string enables the switch to validate Get (read-only) requests from a network management station. If you set the SNMP read community, users can access MIB objects, but cannot change them.

A read-write community string enables the switch to validate Set (read-write) requests from a network management station.

Use SNMP Management Applications

You can use SNMP management applications such as IntraVue or HP OpenView to configure and manage the switch. Refer to SNMP on page 80 for more information.

Configure Alarm Settings

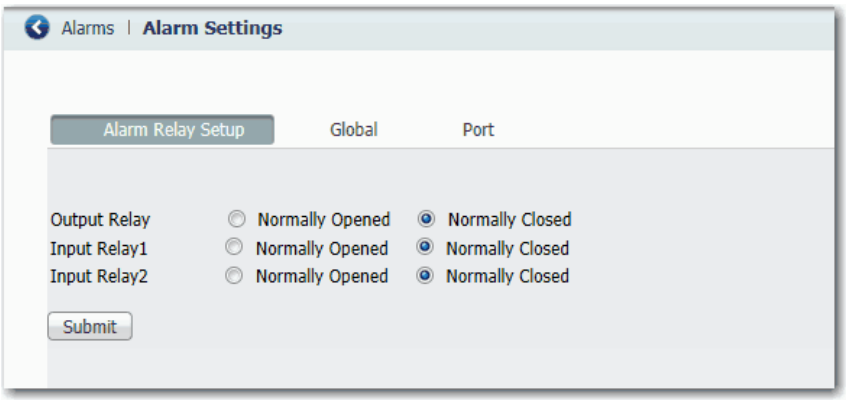
The switch software monitors conditions on a per port or a global basis. If the conditions do not match the set parameters, an alarm or a system message is triggered. By default, the switch sends the system messages to a logging facility. You can configure the switch to send SNMP traps to an SNMP server. You also can configure the switch to trigger an external alarm device by using the two independent alarm relays.

Alarm Relay Settings

You can configure the switch to trigger an external alarm device. The switch supports two alarm inputs and one alarm output. 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. Normally open contacts close and normally closed contacts open.

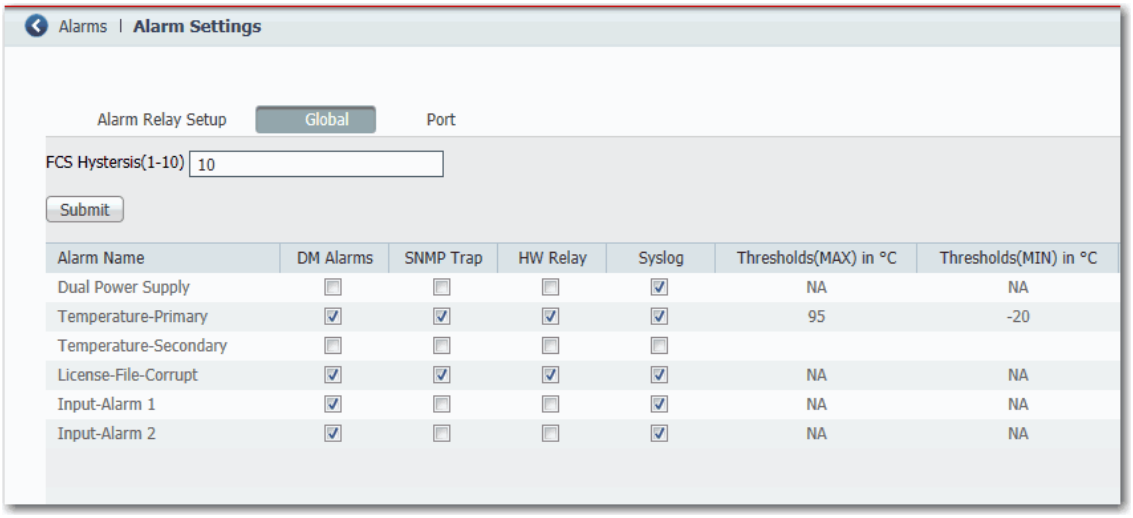
To configure alarm relay settings, from the Configure menu, choose Alarm Settings. On the Alarm Relay Setup tab, click one of these options for each type of alarm relay:

- Normally Opened—The normal condition is that no current flows through the contact. The alarm is generated when current flows.
- Normally Closed—The normal condition has current flowing through the contact. The alarm is generated when the current stops flowing.



Global Alarms

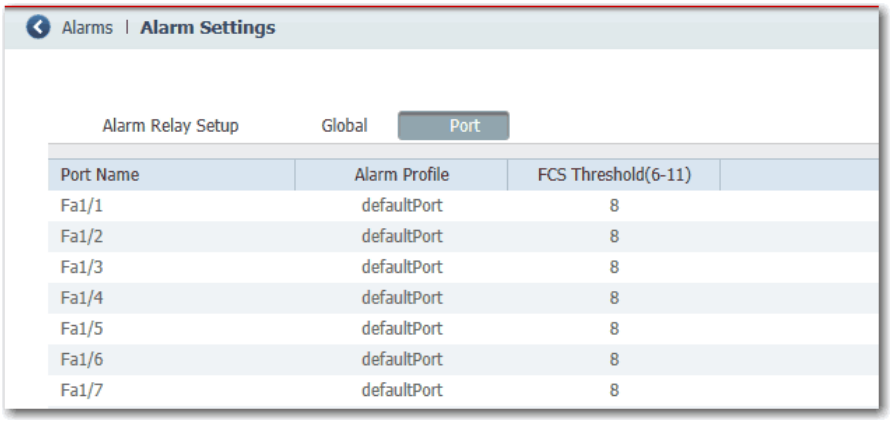
To configure global alarms, also known as facility alarms, from the Configure menu, choose Alarm Settings and click the Global tab.



Field	Description
FCS Hysteresis (1-10)	The frame check sequence (FCS) error hysteresis threshold is used to determine when an alarm condition is cleared. This value is expressed as a percentage of fluctuation from the FCS bit error rate. The default setting is 8%. You can adjust the percentage to prevent toggling the alarm condition when the FCS bit error rate fluctuates near the configured bit error rate. Valid percentages for global settings are 1…10. This setting also can be configured on an individual port by clicking the Port tab.
Alarm Name	These types of alarms can be enabled or disabled: • Dual Power Supply—The switch monitors DC power supply levels. If the system is configured to operate in a dual power mode, an alarm is triggered if a power supply fails or is missing. The alarm is automatically cleared when the power supplies are present or working. You can configure the power supply alarm to be connected to the hardware relays. • Temperature-Primary—An alarm is triggered when the system temperature is higher or lower than the configured thresholds. By default, the primary temperature alarm is associated with the major relay. • Temperature-Secondary—An alarm is triggered when the system temperature is higher or lower than the configured thresholds. • License-File-Corrupt—An alarm is triggered when the license file is corrupt.
DM Alarms	Alarm information appears on the dashboard of the Device Manager Web interface.
SNMP Trap	Alarm traps will be sent to an SNMP server, if SNMP is enabled on the Configure > Security > SNMP window.
HW Relay	The switch's alarm relay is triggered, sending a fault signal to a connected external alarm device, such as a bell, light, or other signaling device that you have configured.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Monitor > Syslog window.
Thresholds (MAX) in °C	The maximum temperature threshold for the corresponding Temperature-Primary or Temperature-Secondary alarm, if enabled.
Thresholds (MIN) in °C	The minimum temperature threshold for the corresponding Temperature-Primary or Temperature-Secondary alarm, if enabled.

Port Alarms

To create alarm profiles for individual ports, from the Configure menu, choose Alarm Settings and click the Port tab.



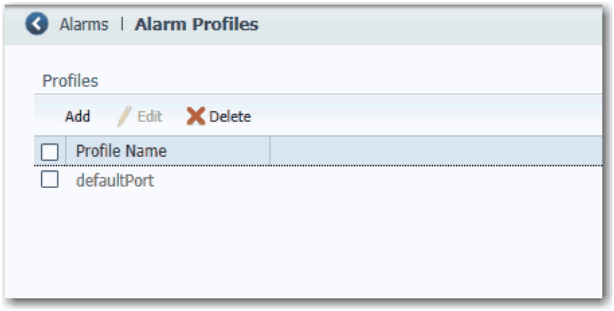
For each port, choose an Alarm Profile and set the FCS threshold. The frame check sequence (FCS) error hysteresis threshold is expressed as a percentage of fluctuation from the FCS bit error rate. The default setting is 8 percent. You can adjust the percentage to prevent toggling the alarm condition when the FCS bit error rate fluctuates near the configured bit error rate. Valid percentages for port settings are 6...11.

Configure Alarm Profiles

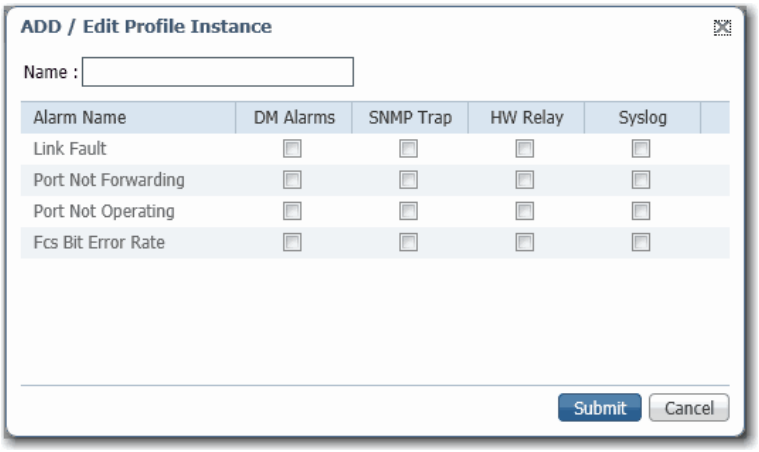
You can use alarm profiles to apply a group of alarm settings to multiple interfaces. These alarm profiles are created for you:

- defaultPort
- ab-alarm (created during Express Setup)

To create, modify, or delete alarm profiles, from the Configure menu, choose Alarm Profiles.



On the Add/Edit Profile Instance window, you can configure the alarms and actions for an alarm profile.



Field	Description
Name	A unique name for the alarm profile.
Alarm Name	These alarms can trigger an action: • Link Fault • Port Not Forwarding • Port Not Operating • Fcs Bit Error Rate
DM Alarms	Alarm information appears on the dashboard of the Device Manager Web interface.
SNMP Trap	Alarm traps will be sent to an SNMP server, if SNMP is enabled on the Configure > Security > SNMP window.
HW Relay	The switch's alarm relay is triggered, sending a fault signal to a connected external alarm device, such as a bell, light, or other signaling device that you have configured.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Monitor > Syslog window.

Monitor Trends

You can view historical data to help you to analyze traffic patterns and to identify problems. Data can be displayed in increments of seconds, minutes, hours, or days.

To view the data in a table, click the Grid Mode button below the area. To display a chart, click the Chart Mode button. Use the 60s, 1h, 1 d, and 1 w links to display the data in increments of 60 seconds, 1 hour, 1 day, or 1 week.

To monitor trends, from the Monitor menu, choose Trends.

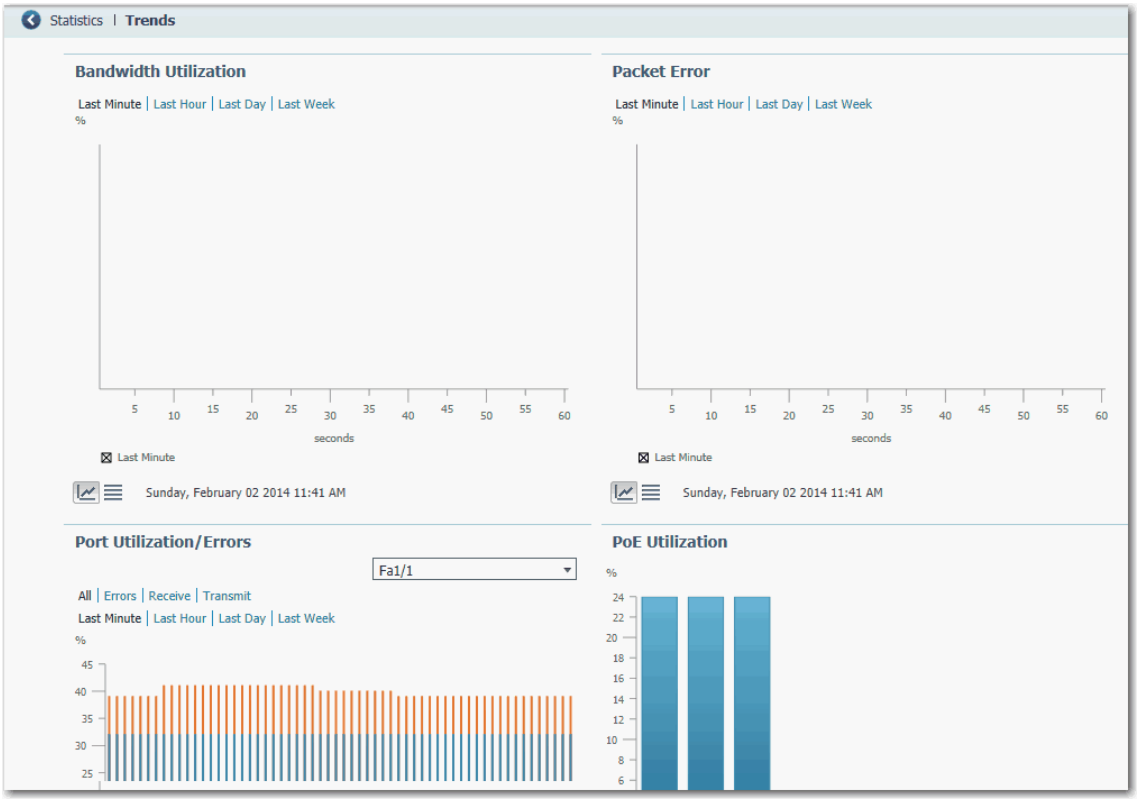


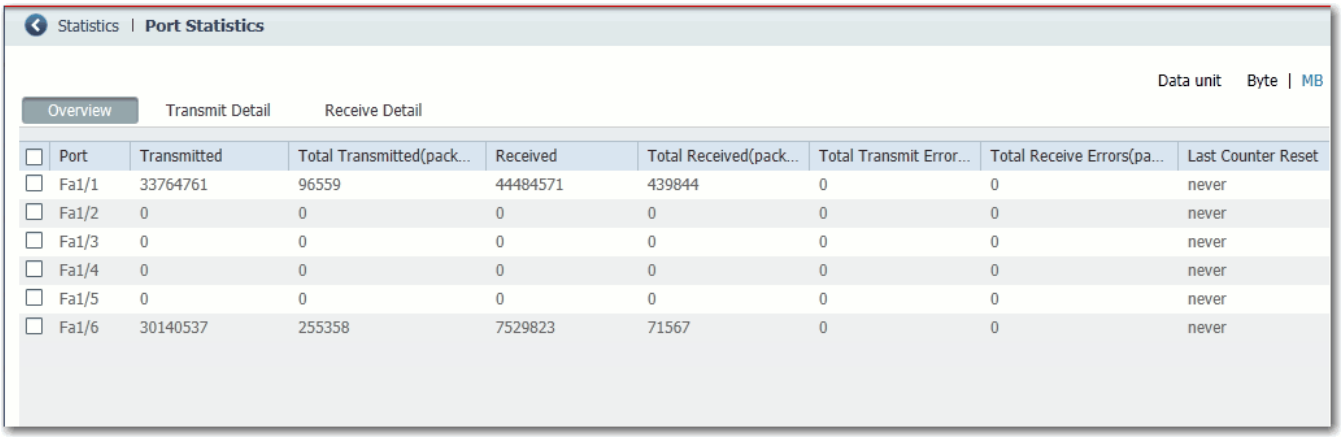
Table 15 - Trends Graphs

Graph	Description
Bandwidth Utilization	The Bandwidth Utilization graph indicates the percentage of the available bandwidth that was used. The graph can show the bandwidth usage patterns over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). This graph also marks the highest peak reached. The default is 60 seconds. You can use this data to determine when network usage is high or low.
Packet Error	The Packet Error graph shows the percentage of packet errors collected over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). The default is 60 seconds. Use this graph to audit the affects that connected devices have on the switch performance or the network. For example, if you suspect that a connected device is sending error packets, you can verify if the data on the graph changes when you disconnect and reconnect the suspected device.
Port Utilization/Errors	The Port Utilization/Errors graph show the usage patterns of a specific port over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). The default is 60 seconds. To display the trends for a specific port, choose a port from the Port list. Use these graphs to observe the performance of a specific port. For example, if a network user is having intermittent network connectivity, use the Port Utilization graph to observe the traffic patterns on the port to which the user's personal computer is connected, and use the Port Errors graph to see if the port is receiving or sending error packets.
PoE Utilization	For PoE switches, the PoE Utilization graph shows the power that is allocated to the connected devices.

Monitor Port Statistics

You can view statistics for data sent and received by the switch ports since the switch was last powered on, was restarted, or since the statistics were last cleared.

To monitor port statistics, from the Monitor menu, choose Port Statistics. See the Device Manager Web interface online help for additional information.



Port	Transmitted	Total Transmitted(pack...	Received	Total Received(pack...	Total Transmit Error...	Total Receive Errors(pa...	Last Counter Reset
Fa1/1	33764761	96559	44484571	439844	0	0	never
Fa1/2	0	0	0	0	0	0	never
Fa1/3	0	0	0	0	0	0	never
Fa1/4	0	0	0	0	0	0	never
Fa1/5	0	0	0	0	0	0	never
Fa1/6	30140537	255358	7529823	71567	0	0	never

The types of port statistics collected and displayed are grouped under these tabs on the Port Statistics window on the Device Manager Web interface:

- Overview tab—Use this tab to display the specific numbers of error packets received on and sent from the port, which is a level of detail that is not available from the Dashboard graphs.

  The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity.

- Transmit Detail tab—Use this tab to troubleshoot unusual changes in network traffic. This tab displays these statistics:

  – Unicast, multicast, and broadcast packets sent from each port
  – Detailed statistics of errors sent to each port

  If a port is sending an unusually high amount of traffic (such as multicast or broadcast packets), monitor the connected device to see if this traffic pattern is normal or if it could mean a problem.

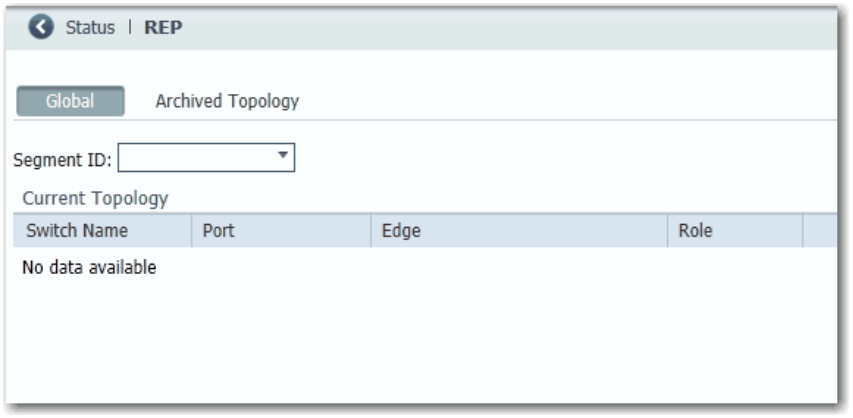
- Receive Detail tab—Use this tab to troubleshoot unusual changes in network traffic. This tab displays these statistics:

  – Unicast, multicast, and broadcast packets received on each port
  – Detailed statistics of errors received on each port

  If a port is receiving an unusually high amount of traffic (such as multicast or broadcast packets), monitor the connected device to see if this traffic pattern is normal for the connected device or if it could mean a problem.

Monitor REP Topology

To review the REP topology for one or all network segments, from the Monitor menu, choose REP. To display an archived REP topology, click the Archived Topology tab and then select the segment ID.



Monitor CIP Status

Common Industrial Protocol (CIP) is an application layer messaging protocol used by various industrial automation and control devices to communicate as part of a control system. CIP is the application layer for the EtherNet/IP network. Stratix switches contain an EtherNet/IP server that enables the switch to be part of the industrial automation and control system for basic management and monitoring.

The CIP Status window displays information about CIP status (Overview field) and statistics (Request Details field) since the switch was last powered on, was restarted, or the counters were last reset.

To troubleshoot an issue, reset the CIP counters, and see if the counters show that the issue still exists.

IMPORTANT Except for Active Multicast Groups, all other categories are related to the CIP server in the switch, that is, pertaining to CIP traffic specifically directed to the switch as a CIP target device. They do not refer to CIP (EtherNet/IP) traffic flowing through the switch among various CIP controllers, HMI devices, configuration tools, or other CIP target devices, such as drives, I/O modules, motor starters, sensors, and valves.

To monitor CIP status, from the Monitor menu, choose CIP Status.

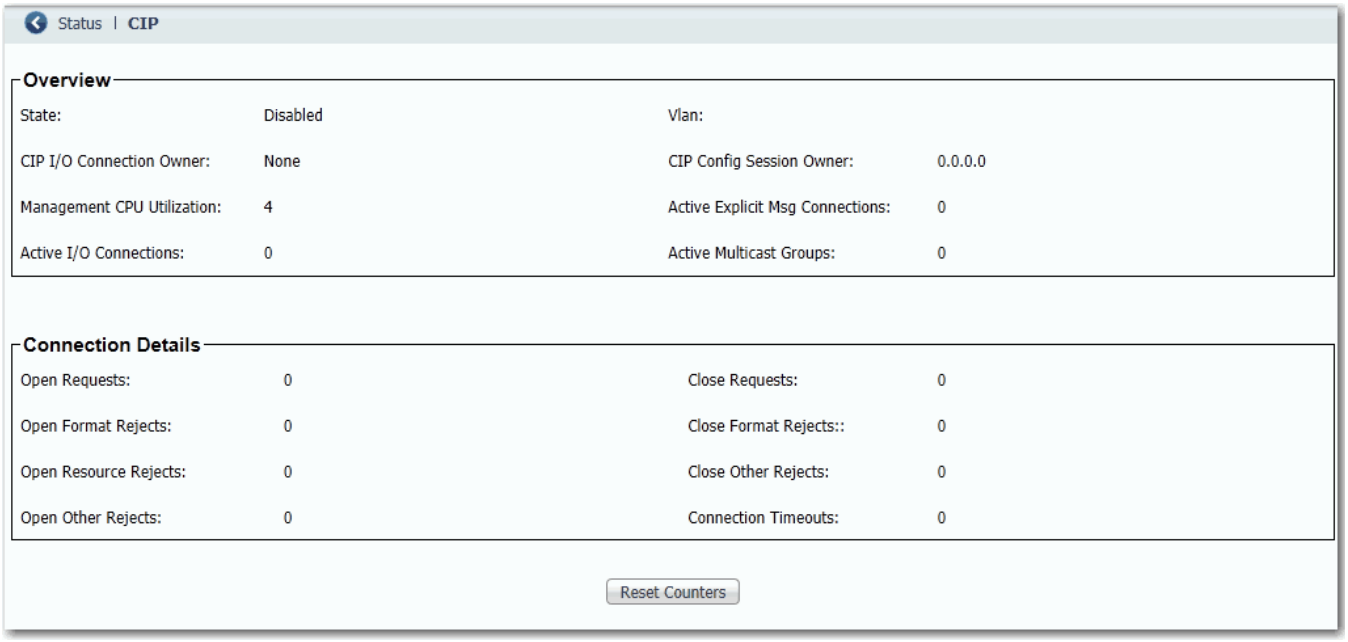


Table 16 - CIP Status Fields

Field	Description
Overview	
State	The state of the CIP connection (Enabled or Disabled).
Vlan	The VLAN ID.
CIP I/O Connection Owner	The IP address of the device to and from which application-specific I/O output data is sent and received.
CIP Config Session Owner	The IP address of the device controlling the CIP configuration session.
Management CPU Utilization (%)	Percentage of the Management CPU used for management functions. Switch functions have dedicated ASICs that are not impacted by management functions.
Active Explicit Msg Connections	The number of active, explicit messaging connections to the switch as a target.
Active I/O Connections	The number of active I/O connections with the switch as a target.
Active Multicast Groups	The number of multicast groups, including CIP multicast groups flowing through the switch.
Connection Details	
Open Requests	The number of Forward Open requests received by the switch to establish a connection with the switch.
Close Requests	The number of Forward Close requests received by the switch after a connection was successfully established with the switch.
Open Format Rejects	The number of Forward Open requests directed to the switch that failed because the request is not in the proper format.
Close Format Rejects	The number of Forward Close requests directed to the switch that failed because the request is not in the proper format.
Open Resource Rejects	The number of Forward Open requests that failed to establish a new connection for reasons such as insufficient memory.
Close Other Rejects	The number of Forward Close requests that failed for reasons such as incompatible electronic keying.
Open Other Rejects	The number of Forward Open requests that failed for reasons such as incompatible electronic keying.
Connection Timeouts	The number of CIP connections that timed out due to inactivity.

Diagnose Cabling Problems

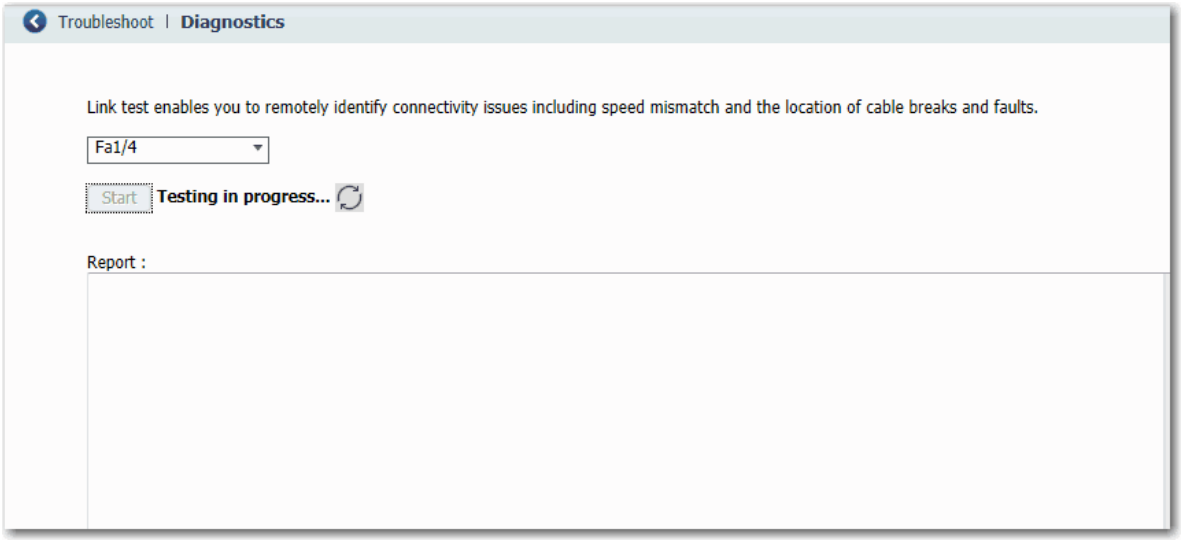
Use the Diagnostics window to run the Broken Wire Detection test, which uses Time Domain Reflectometry (TDR) detection to identify, diagnose, and resolve cabling problems. TDR detection is supported on copper Ethernet 10/100 and 10/100/1000 ports. TDR is not supported on small form-factor pluggable (SFP)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

The link test can interrupt traffic between the port and the connected device. Only run the test on a port that has a suspected problem. Before running the link test, use the Front Panel view, the Port Status, and the Port Statistics windows to gather information about a potential problem.

IMPORTANT To run a valid test on gigabit ports, you must first configure the gigabit port as an RJ45 media type, as described in Configure Port Settings on page 97.

To diagnose cabling problems, from the Monitor menu, choose Diagnostics.

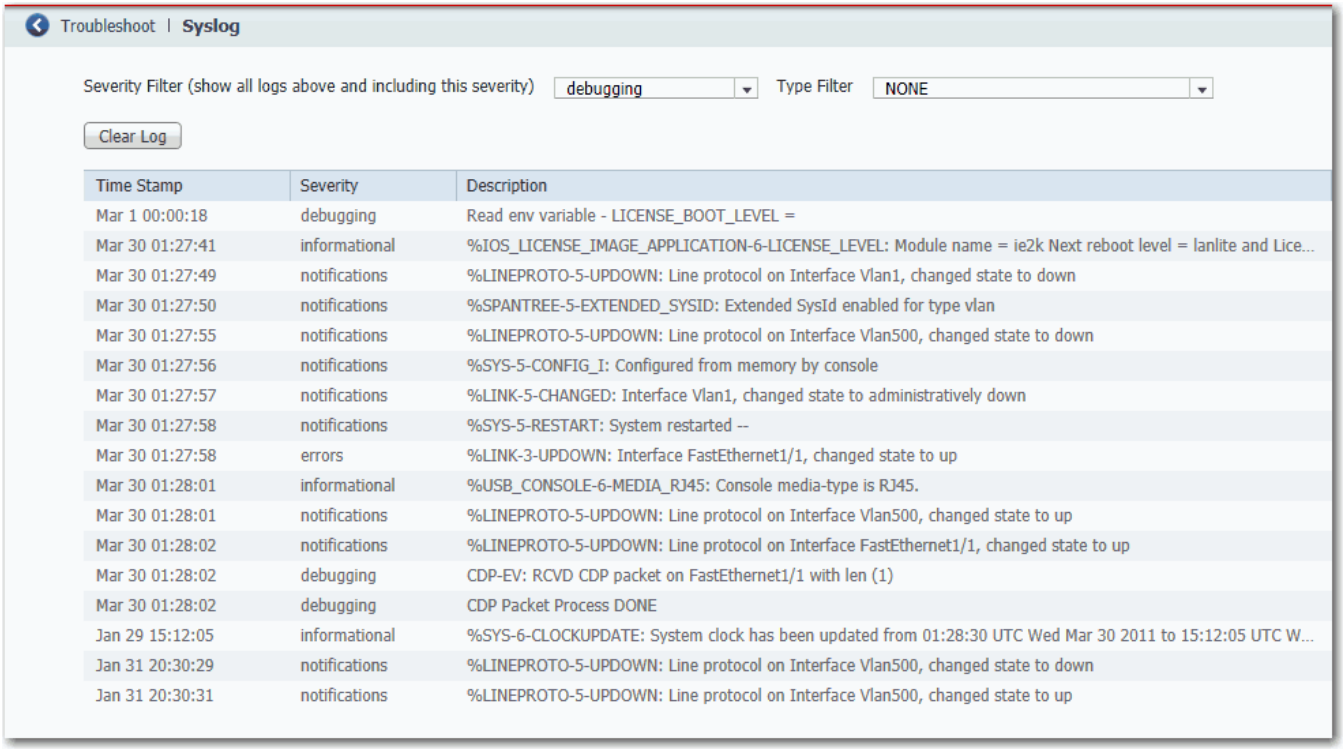
To run a test, select a port and then click Start.



View System Log Messages

The system log displays events that occurred on the device and its ports, based on the Alarm Settings you configure on the Configure > Alarm Settings window.

To view system log messages, from the Monitor menu, choose Syslog.



To filter historical events, choose a severity filter or type filter:

- Debugging—Debug messages.
- Informational—Informational messages.
- Notifications—The switch is operating normally but has a significant condition.
- Warnings—The switch has a warning condition.
- Errors—The switch has an error condition.
- Critical—The switch has a critical condition.
- Alerts—The switch requires immediate action.
- Emergencies—The switch is unusable.

Click Clear Log to acknowledge that you have read the alerts. Clicking Clear Log does not resolve the issue.

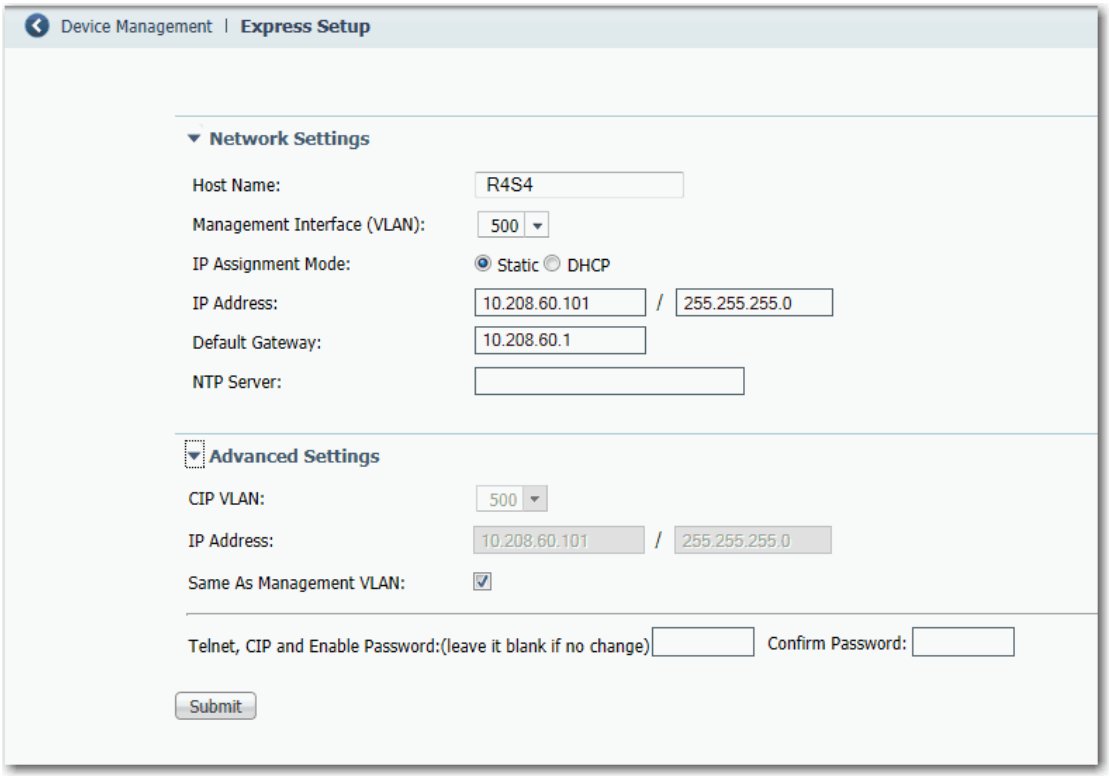
Table 17 - Syslog Fields

Field	Description
Time Stamp	The date and time the event occurred. Use the Express Setup window to connect the device to an NTP server. Time settings are lost if the switch loses power.
Severity Level	The type and severity of the event.
Description	The description of the problem, including the port on which the problem was detected.

Use Express Setup to Change Switch Settings

The network settings enable the switch to operate with its standard default settings and to be managed through the Device Manager Web interface. These settings were set during the initial setup. Change these settings if you want to move the switch to a different management VLAN or to a different network.

To update the switch IP information, from the Admin menu, choose Express Setup.

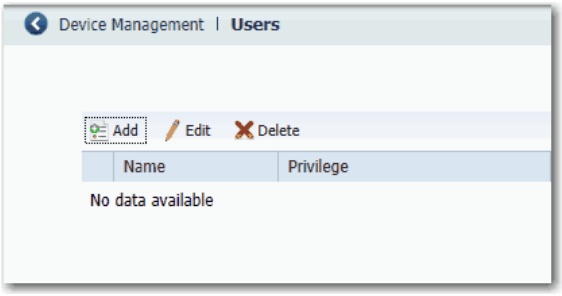


Field	Description
Network Settings	
Host Name	The name of the device.
Management Interface (VLAN)	The name and ID of the management VLAN through which the switch is managed. Choose an existing VLAN to be the management VLAN. The default ID is 1. The default name for the management VLAN is default. The number can be from 1...1001. Be sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch. 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 at all times.
IP Assignment Mode	The IP Assignment mode determines whether the switch IP information is manually assigned (static) or is automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you click Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the Device Manager Web interface. If you click DHCP, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. As long as the switch is not restarted, the switch continues to use the assigned IP information, and you are able to use the same IP address to access the Device Manager Web interface. If you manually assign the switch IP address and your network uses a DHCP server, be sure that the IP address that you give to the switch is not within the range of addresses that the DHCP server automatically assigns to other devices. This prevents IP address conflicts between the switch and another device.

Field	Description
IP Address	The IP address and associated subnet mask are unique identifiers for the switch in a network: • The IP address format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. • The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is enabled only if the IP Assignment mode is Static. Make sure that the IP address that you assign to the switch is not being used by another device in your network. The IP address and the default gateway cannot be the same.
Default Gateway (optional)	The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address must be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This field is enabled only if the IP assignment mode is Static. You must specify a default gateway if your network management station and the switch are in different networks or subnetworks. Otherwise, the switch and your network management station cannot communicate with each other.
NTP Server	The IP address of the Network Time Protocol (NTP) server. NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
Advanced Settings	
CIP VLAN	The VLAN on which Common Industrial Protocol (CIP) is enabled. The CIP VLAN can be the same as the management VLAN or you can isolate CIP traffic on another VLAN that is already configured on this device.
IP Address	The IP address and subnet mask for the CIP VLAN if the CIP VLAN is different from the management VLAN. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. Make sure that the IP address that you assign to this device is not being used by another device in your network.
Same As Management VLAN	Indicates whether the settings for the CIP VLAN are the same as the management VLAN.
Telnet, CIP and Enable Password (optional)	The password used for Telnet and CIP security.
Confirm Password	The same password as above.

Manage Users

To add, modify, or delete users and user logon information for the switch, from the Admin menu, choose Users.



For each user, you can specify the information in the table below.

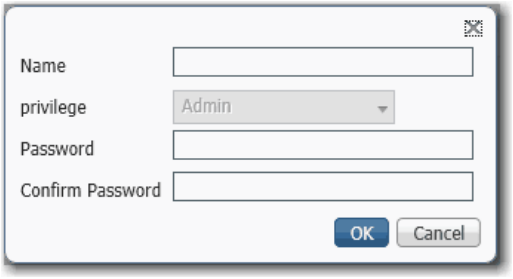


Table 18 - Add User Fields

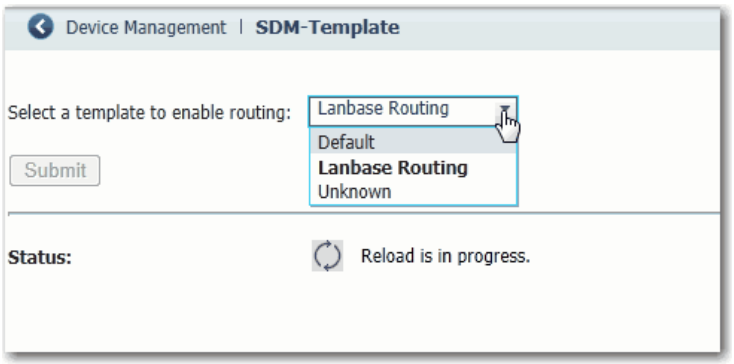
Field	Description
Name	The user name for this user.
Privilege	The level of access for this user. All users are assigned the Admin privilege and can change all parameters.
Password	The password that is required for access with this user name.
Confirm Password	The same password as above.

Reallocate Switch Memory for Routing

Switch Management Database (SDM) templates optimize how switch memory is allocated for specific features, such as routing. To enable static and connected routing, you must change the default SDM template to the Lanbase Routing template.

To apply an SDM template, follow these steps.

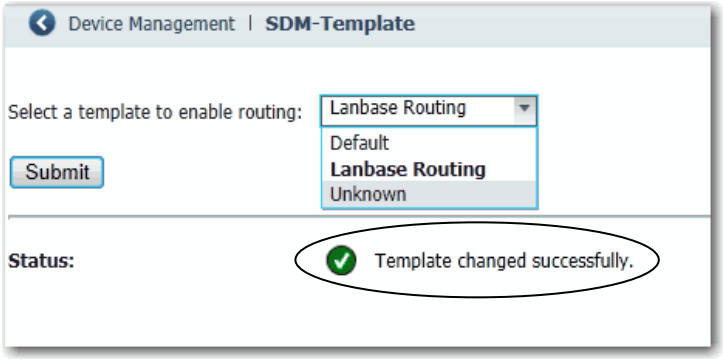
1. From the Admin menu, choose SDM-Template.
2. Choose a template from the pull-down menu:
   - Default—Gives balance to all Layer 2 functions
   - Lanbase Routing—Maximizes system resources for IPv4 unicast routing, which is required to enable routing
   - Unknown—User-configured from the CLI



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

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

A message appears once the process is complete.



5. To enable routing, proceed to Enable Static and Connected Routing on page 114.

Restart the Switch

Restarting or resetting the switch interrupts connectivity of your devices to the network.

To restart or reset the switch, from the Admin menu, choose Restart/Reset.

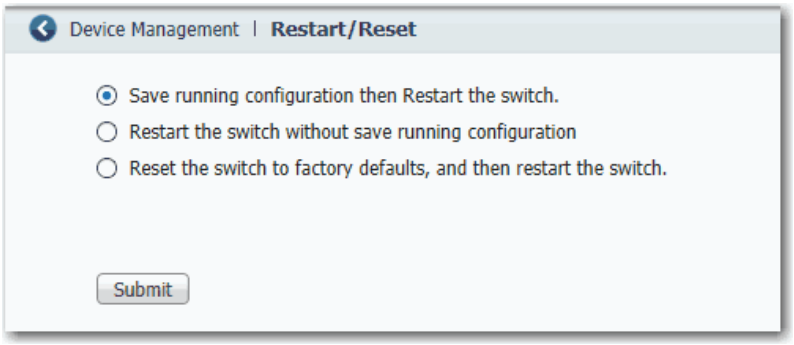


Table 19 - Restart/Reset Fields

Field	Description
Save running configuration and then restart the switch	Ensures that any changes in the running configuration are saved before the switch restarts.
Restart the switch without saving running configuration	Restarts the switch with its previously saved configuration settings.
Reset the switch to factory defaults, and then restart the switch	Resets the device to the factory-default settings, deleting the current configuration settings, and then restarts the device. You will lose connectivity with the device and need to initiate Express Setup to reconfigure the device.

Upgrade the Switch Firmware

You must have access to the Internet to download switch firmware from http://www.rockwellautomation.com to your computer or network drive.

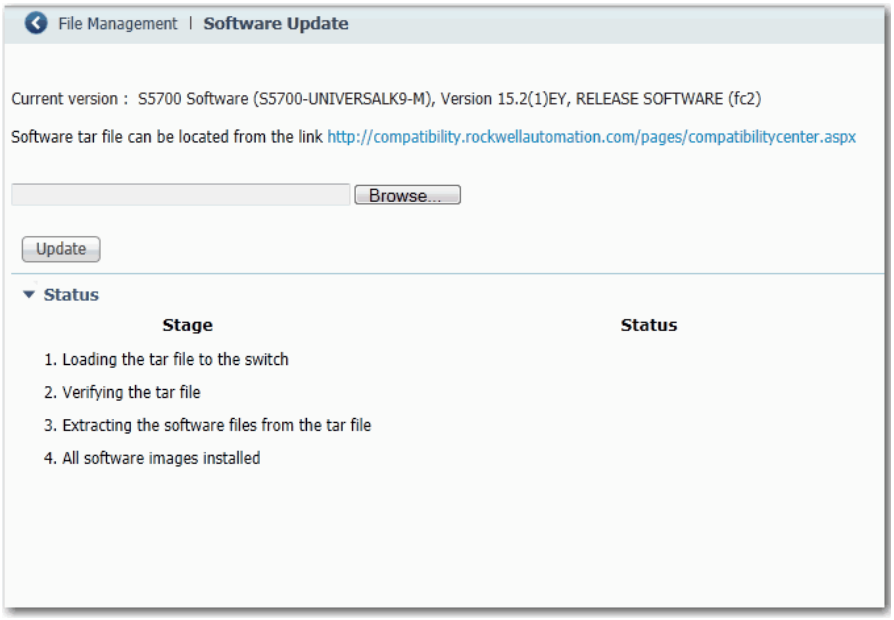
To update the switch with the latest software changes and features, from the Admin menu, choose Software Update.

From the Device Manager Web interface, you can upgrade your switches one at a time.

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

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

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



See the Device Manager Web interface online help for additional guidelines and procedures.

Upload and Download Configuration Files

To copy a configuration file from a file on another device, such as a PC, to the onboard memory, enter the directory name of the folder on the switch, browse to select the file, and click Upload.

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

Notes:

Manage the Switch via the Studio 5000 Environment

After you complete Express Setup, you can manage the switch by using the Studio 5000 Logix Designer™ application.

EtherNet/IP CIP Interface

Stratix 8000 and Stratix 8300 switches contain an EtherNet/IP network interface. EtherNet/IP is an industrial automation network specification maintained by the Open DeviceNet Vendor Association (ODVA). It uses the Common Industrial Protocol (CIP) for its application layer, and TCP/UDP/IP for its transport and network layers. This interface is accessible via any of the switch's Ethernet ports by using the IP address of the switch.

CIP Network Connections

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

- Explicit messaging
- Implicit messaging (I/O connections)

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

Table 20 - CIP Network Connections

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

IMPORTANT Because the output data is sent cyclically by the controller, it overrides any other attempt to enable or disable a port from other software tools or visualization stations.

RSLinx Software and Network Who Support

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

To perform an RSWho, from the RSLinx software toolbar, choose Communications > RSWho.

IMPORTANT If, after performing an RSWho, you access the switch and view the Ethernet link counters, you see the counts only for the first port (Port Gi1/1).

Electronic Data Sheet (EDS) Files

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

If you are using the switch in a system that does not have a Logix-based controller to monitor or control your switch, you are not be able to use the Add-on Profile (AOP) supplied with Logix controllers. You must use information from the EDS files to set up the I/O connection.

The OPC Server contained in RSLinx Classic software also uses EDS files to provide you with a list of parameters when adding items (OPC Tags) to a Topic (the switch).

EDS files for the Stratix 8000 switches are included with the following software packages:

- RSLinx software, version 2.54 or later
- RSLogix 5000 software, version 17.01.02 or later, or Studio 5000 environment, version 21.00.00 or later
- RSNetWorx for EtherNet/IP software, version 9.0 or later

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

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

Follow this procedure to upload the EDS files directly from the switch over the network.

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

Six different EDS files are supplied with the switch, one for each port count (6, 10, 14, 18, 22 and 26 ports). Regardless of the switch from which you upload EDS files, you receive all six files and the Stratix 8000 switch icon.

Data Accessible with CIP

The CIP interface lets you access the following information:

- Input Data via I/O Connection
  - Link Status per Port: not connected, connected
  - Unauthorized Device per Port: OK, not OK
  - Unicast Threshold Exceeded per Port: OK, exceeded
  - Multicast Threshold Exceeded on each Port: OK, exceeded
  - Broadcast Threshold Exceeded on each Port: OK, exceeded
  - Port Bandwidth Utilization per Port: value in %
  - Alarm Relay Minor: OK, tripped
  - Alarm Relay Major: OK, tripped
  - Multicast Groups Active: quantity
- Output Data via I/O Connection
  - Port Disable per port: enabled, disabled

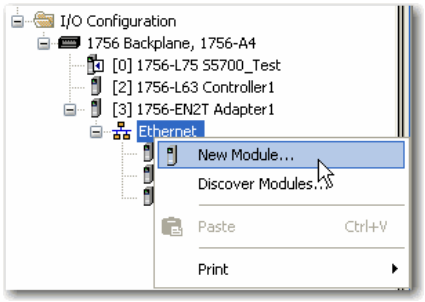
- Other Status Data
  - Switch Internal Temperature: degrees Centigrade
  - Power Supply A present: yes, no
  - Power Supply B present: yes, no
  - Identity Info: VendorID, DeviceType, ProductCode, ProductName, Revision, SerialNumber
  - IOS Release version
  - Switch Uptime (since last restart)
  - Management CPU Utilization: in %
  - CIP Connection Counters: open/close requests, open/close rejects, timeouts
  - Port Alarm Status per port: OK, not forwarding, not operating, excessive FCS errors
  - Port Fault Status per port: Error Disable, SFP error, native VLAN mismatch, MAC address flap condition, security violation
  - Port Diagnostic Counters per port: Ethernet Interface counters (10), Ethernet Media counters (12)
- Configuration Data (requires password)
  - IP Address Method: DHCP, static
  - IP Address, Subnet Mask, Default Gateway (all if static)
  - Host Name
  - Contact name
  - Geographic Location
  - Port Config per port: enable/disable, autonegotiate, forced speed/duplex
  - Authorized MACID per port
  - Unicast Storm Control Threshold per port: in packets per second, bits per sec, or %
  - Multicast Storm Control Threshold: in packets per second, bits per sec, or %
  - Broadcast Storm Control Threshold: in packets per second, bits per sec, or %
- Smart Port assignment per port: Role and VLAN
- Save and Restore of Switch Configuration (via File Obj)

Add a Switch to the I/O Configuration Tree

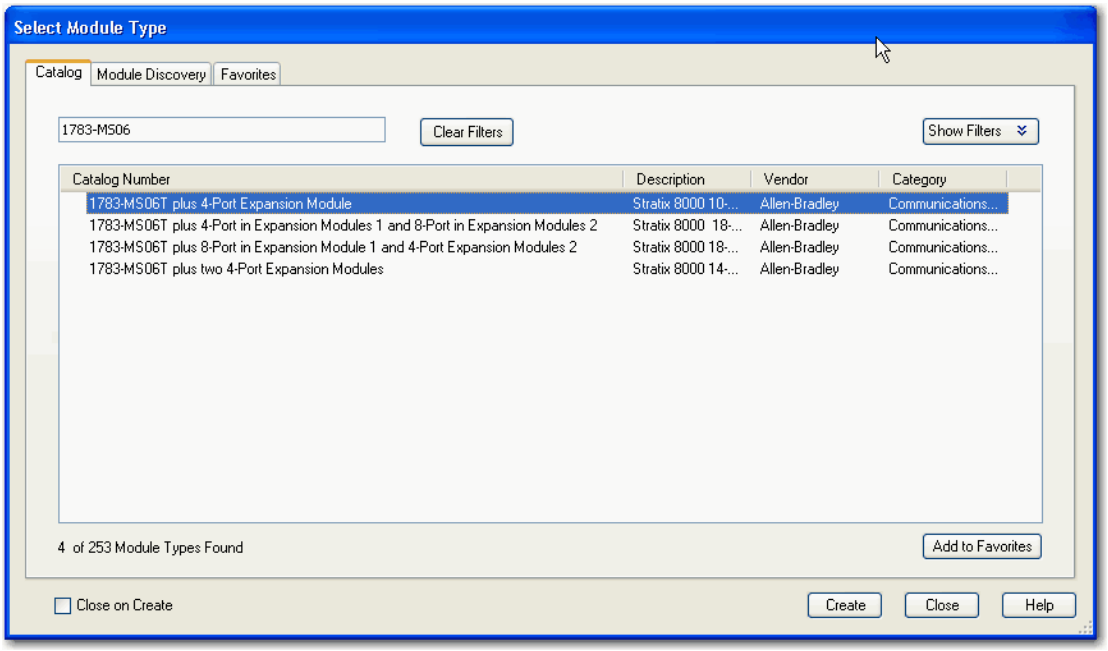
Follow this procedure to add the switch to the controller's I/O tree.

IMPORTANT You must complete these steps before you can go online to configure and monitor the switch.

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



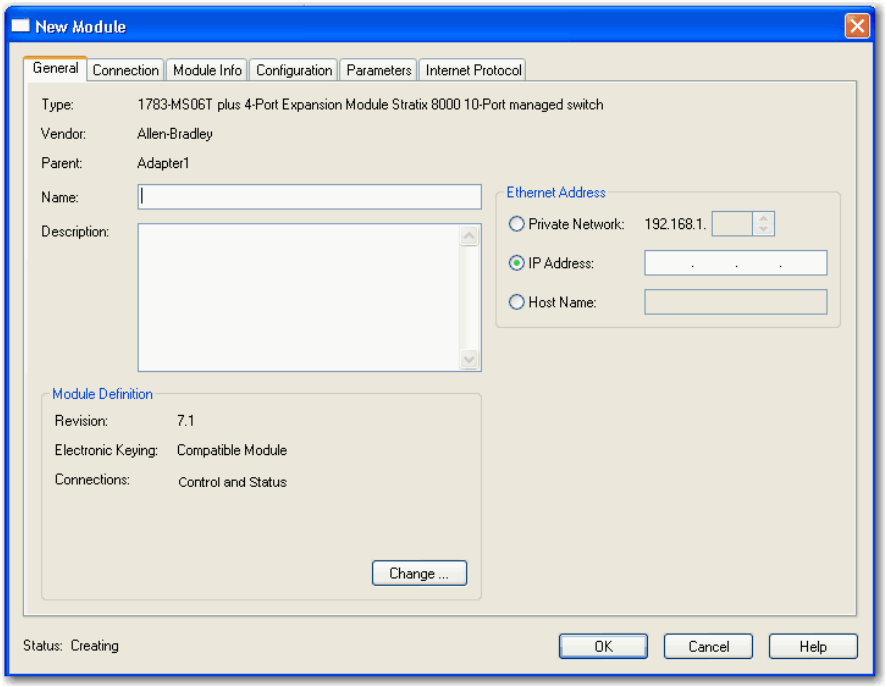
3. On the Select Module Type dialog box, select the switch and click Create.



Configure Module Properties

Follow this procedure to configure the switch.

1. On the General tab of the New Module Properties dialog box, complete the fields below.

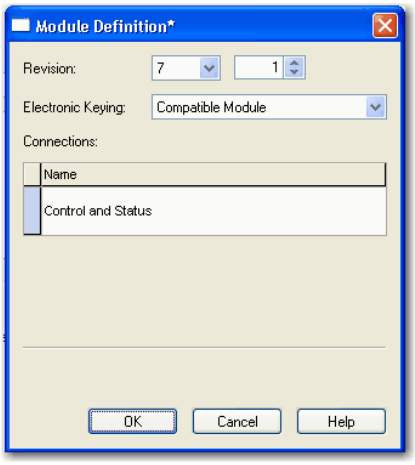


IMPORTANT Be sure that the IP address and host name are the same as those provided when you performed Express Setup. On the Module Properties dialog box, you can choose either an IP address or host name. Only one of these two choices is enabled.

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

2. In the Module Definition area, click Change.

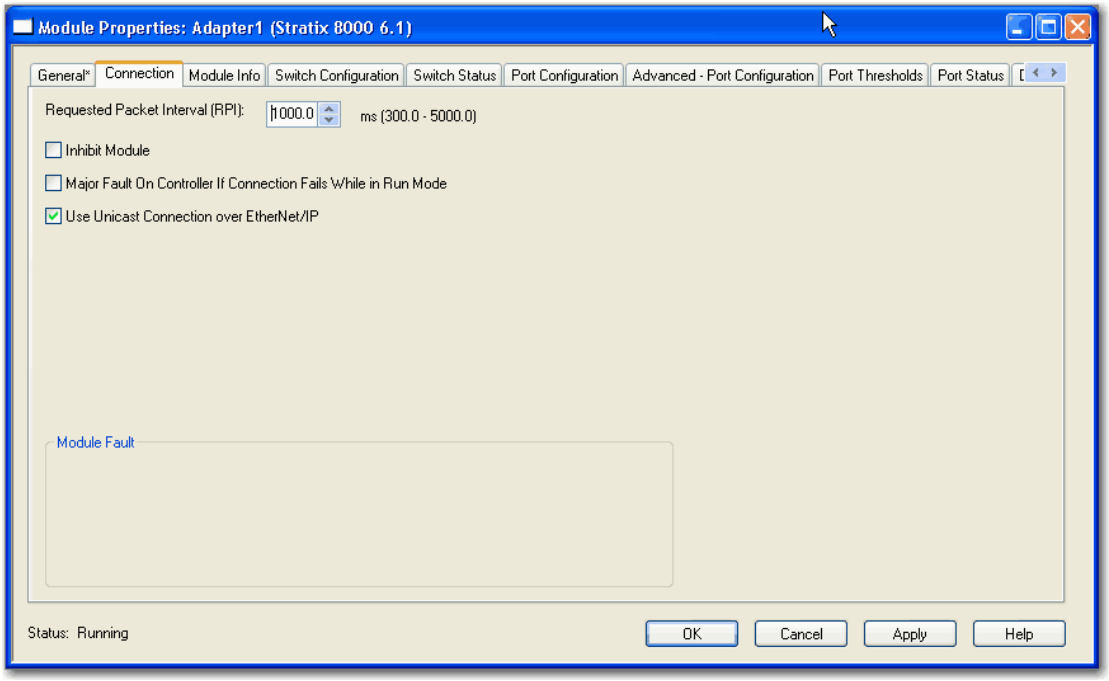
3. On the Module Definition dialog box, complete the fields below and click OK.



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

Connection Properties

The Connection tab lets you define the connection properties described below.



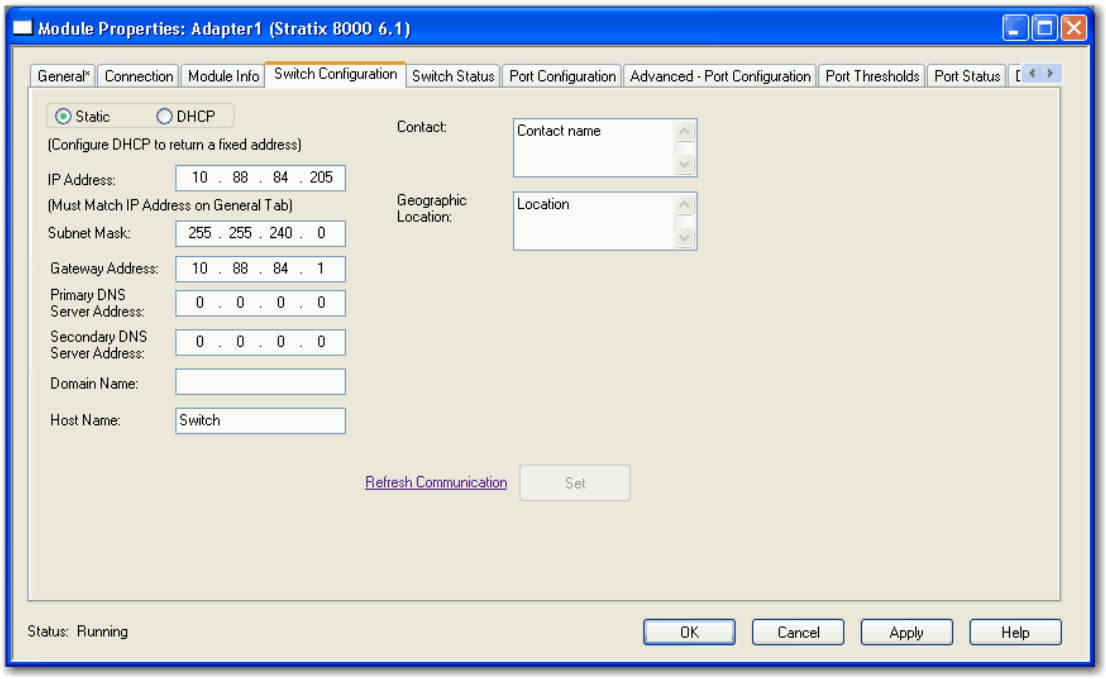
Field	Description
Requested Packet Interval (RPI)	Enter a value between 300…5000 ms.
Inhibit Module	Check to disable communication between the controller and the switch. Clear to restore communication.
Major Fault on Controller If Connection Fails While in Run mode	Check to have the controller create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

Switch Configuration Properties

Configure the parameters for the switch configuration on the Switch Configuration tab. You must be online to perform these configurations. In Offline mode, the fields on the tab are unavailable.

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

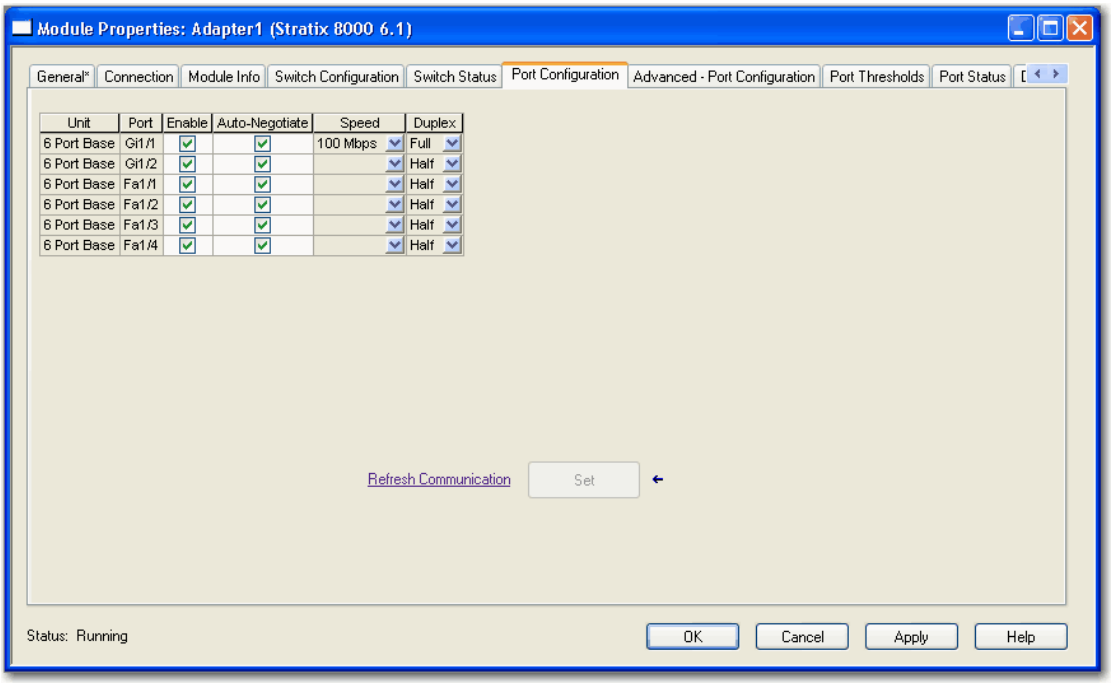
- Static—Manually enter the IP address, subnet mask, and gateway.
- DHCP—The switch automatically obtains an IP address, default gateway, and subnet mask from the DHCP server. As long as the switch is not restarted, it continues to use the assigned IP information.



Field	Description
IP Address	This value must match the IP address on the General tab. If you reconfigure your switch with a different IP address, you can lose communication with the switch when you click Set. To correct this problem, you must go back to the Express Setup and General tab, set the new IP address, and download to the controller.
Subnet Mask	Enter the appropriate subnet mask for the switch. The subnet mask is a 32-bit number. Set each octet between 0 and 255. The default is 255.255.255.0
Gateway Address	A gateway is a router or other network device through which the switch communicates with devices on other networks or subnetworks. The 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. **ATTENTION:** Communication is disrupted when the gateway (IP) address is changed.
Primary DNS Server Address	Enter the IP address of the primary Domain Name Server (DNS). Set each octet between 0…255. The first octet cannot be 127 or a number greater than 223.
Secondary DNS Server Address	Enter the IP address of the secondary Domain Name Server (DNS). Set each octet between 0…255. The first octet cannot be 127 or a number greater than 223.
Domain Name	Enter the name of the domain in which the module resides. The domain name consists of a sequence of name labels separated by periods, such as example.com. The domain name has a 48-character limit and is restricted to ASCII letters a…z, digits 0…9, and periods and hyphens.
Host Name	Enter a name to help identify the switch when monitoring or troubleshooting a problem. This feature is optional. The name can be up to 64 characters and can include alphanumeric and special characters (comma and dash).
Contact	Enter contact information for the switch, up to 200 characters. This feature is optional. The contact information can include alphanumeric and special characters (dash and comma) and a carriage return.
Geographic Location	Enter a geographic location of the switch, up to 200 characters. This feature is optional. The geographic location can include alphanumeric and special characters (dash and comma) and a carriage return.
Refresh	Click to refresh the tab with new data from the module. This button is active on many tabs.
Set	Click to send the settings to the switch. Changes can be made within 10 minutes without the Enter Password dialog box displaying and prompting you for a password. Changes are saved to the switch and the CompactFlash card (if installed).

Port Configuration Properties

Configure basic switch port settings on the Port Configuration tab. These settings determine how data is received and sent between the switch and the attached device.



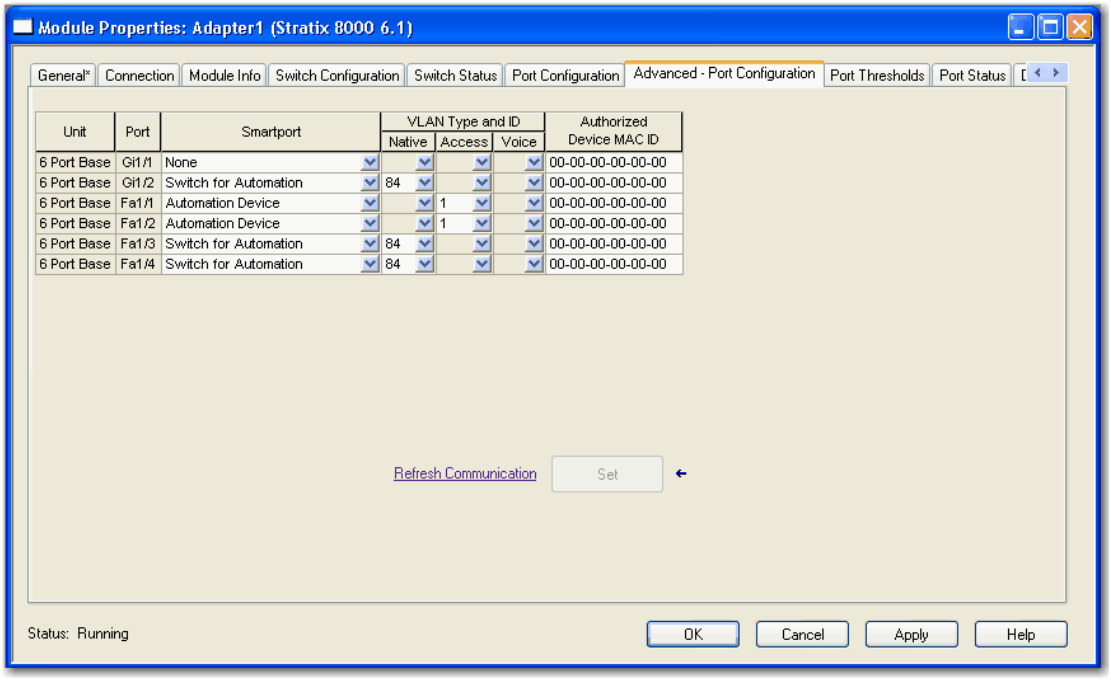
You must be online to configure the port features. Most of the information on this tab does not appear if you are offline.

Field	Description
Unit	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	Indicates the port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number such as in the following examples: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Enable	Check to enable the port. Clear the checkbox to manually disable (shut down) the port. We recommend that you disable the port if the port is not in use and is not attached to a device. You can troubleshoot a suspected unauthorized connection by manually disabling the port.

Field	Description
Auto-negotiate	Check the checkbox if you want the port and end-device to auto-negotiate the link speed and Duplex mode. Clear the checkbox to manually select the desired port speed and Duplex mode. 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 also be configured for the exact same speed and duplex, and not set to auto-negotiate, otherwise a speed/duplex mismatch occurs. Fiber-optic interfaces do not support auto-negotiation.
Speed	Choose the operating speed of the port. Gigabit (Gi): • 10 Mbps • 100 Mbps • 1 Gbps Fast Ethernet (Fa) • 10 Mbps • 100 Mbps
Duplex	Choose the Duplex mode of the port: • Half-duplex—Both devices cannot send data at the same time. Half-duplex is not available when speed is set to 1 Gbps. • Full-duplex—Both devices can send data at the same time.

Advanced Port Properties

Configure the Smartport roles VLAN and authorized MAC ID on the Advanced Port Config tab.

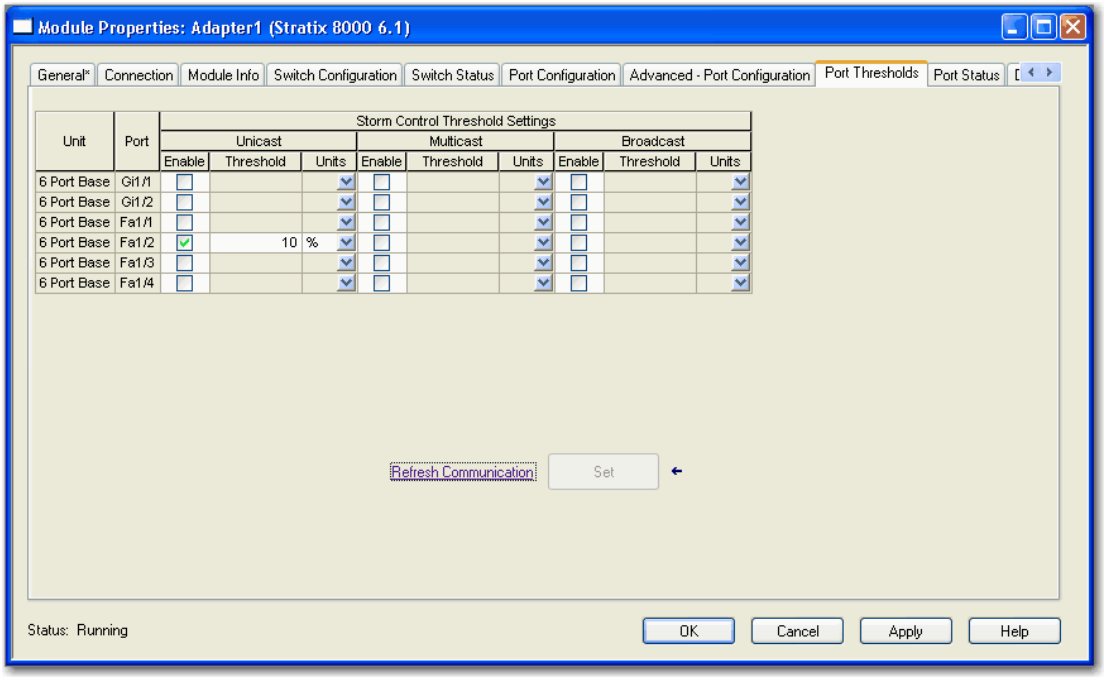


You must be online to configure these port features. Most of the information on this tab is not displayed if you are offline.

Field	Description
Unit	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	Indicates the port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number, such as in the following examples: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Smartport	Choose the Smartport role to apply to the connected port. The Smartport roles are recommended configurations for the ports. These configurations are referred to as port roles. They optimize the switch connections and ensure security, transmission quality, and reliability to traffic from the switch ports. These configurations also prevent many problems caused by port misconfigurations. The port roles are based on the type of device that is connected to the switch port. Make sure you decide which port to connect to which type of device before you choose the Smartport: • Automation Device—Apply this role to ports to be connected to EtherNet/IP (Ethernet Industrial Protocol) devices. It can be used for industrial automation devices, such as logic controllers and I/O: – Port is set to Access mode. – Port security supports only one MAC ID. – Optimize queue management for CIP traffic. • Automation Device with QoS—Apply this role to ports to devices that are generating 802.1Q tagged frames (not typically used): – Port is set to Trunk mode (supports 802.1Q Tagged Frames). – Portfast enabled. – Port security supports only one MAC ID. • Desktop for Automation—Apply this role to ports to be connected to desktop devices, such as desktop computers, workstations, notebook computers, and other client-based hosts: – Port is set to Access mode. – Portfast enabled. – Port security supports only one MAC ID. – Do not apply to ports to be connected to switches, routers, or access points. • Switch for Automation—Apply this role to ports to be connected to other switches. – Port is set to Trunk mode. – Portfast enabled. • Router for Automation—Apply this role to routers or ports to be connected to Layer 3 switches with routing services enabled. • Phone for Automation—Apply this role to ports to be connected to IP phones. A desktop device, such as a computer, can be connected to the IP phone. Both the IP phone and the connected computer have network access through the port: – Port is set to Trunk mode. – Port security supports three MAC IDs to this port. – This role prioritizes voice traffic over general data traffic to ensure clear voice reception on the IP phones. • Wireless For Automation—Apply this role to ports to be connected to wireless access points. The access point can provide network access to up to 30 mobile (wireless) users. • Port Mirroring—Apply this role to ports to be monitored by a network analyzer. For more information about port mirroring, see Port Mirroring on page 82. • None—Apply this role to ports if you do not want a specialized Smartports role on the port. This role can be used on connections to any device, including devices in the roles described above.
VLAN Type and ID	A virtual local area network (VLAN) is a logical segment of network users and resources grouped by function, team, or application. This segmentation is without regard to the physical location of the users and resources. You can choose a VLAN (native, access or voice) from a list read from the switch. Only the first 128 VLANs are listed: • Native—Represents the valid Native VLAN ID for ports set to the Router for Automation and Switch for Automation role. A native VLAN is for ports that can belong to a VLAN trunk (a port belonging to more than one VLAN). The Native VLAN feature is blank when Smart Port is set to any value other than Switch for Automation and Router for Automation, and in Offline mode. • Access—Represents the valid Access VLAN ID for ports set to Automation Device, Desktop for Automation, Phone for Automation for Automation, Wireless, and Automation Device with QoS role. An access VLAN is for ports that can belong to only one VLAN. The Access VLAN feature is blank when Smart Port is set to Switch for Automation and Router for Automation, and in Offline mode. • Voice—Represents the valid Voice VLAN ID for ports set to the Phone for Automation role. The voice VLAN ensures that all voice traffic has better quality of service and is not mixed with data traffic. The Voice VLAN feature is blank when Smart Port is set to any value other than Phone for Automation, and in Offline mode.
Authorized Device MAC ID	Type the MAC address of the device that is connected to the port. The MAC address is also known as Ethernet address, physical address, or hardware address. Each node on the network has is a unique MAC address assigned to it. The MAC ID is six hexadecimal numbers, such as 00-00-BC-22-A0-D8. You can authorize only a specific MAC address to communicate on this port. If other MAC addresses communicate on that port, they are blocked. This feature must not be set for ports connected to other switches or routers. The Authorized Device MAC ID feature is blank in Offline mode.

Port Thresholds (storm control)

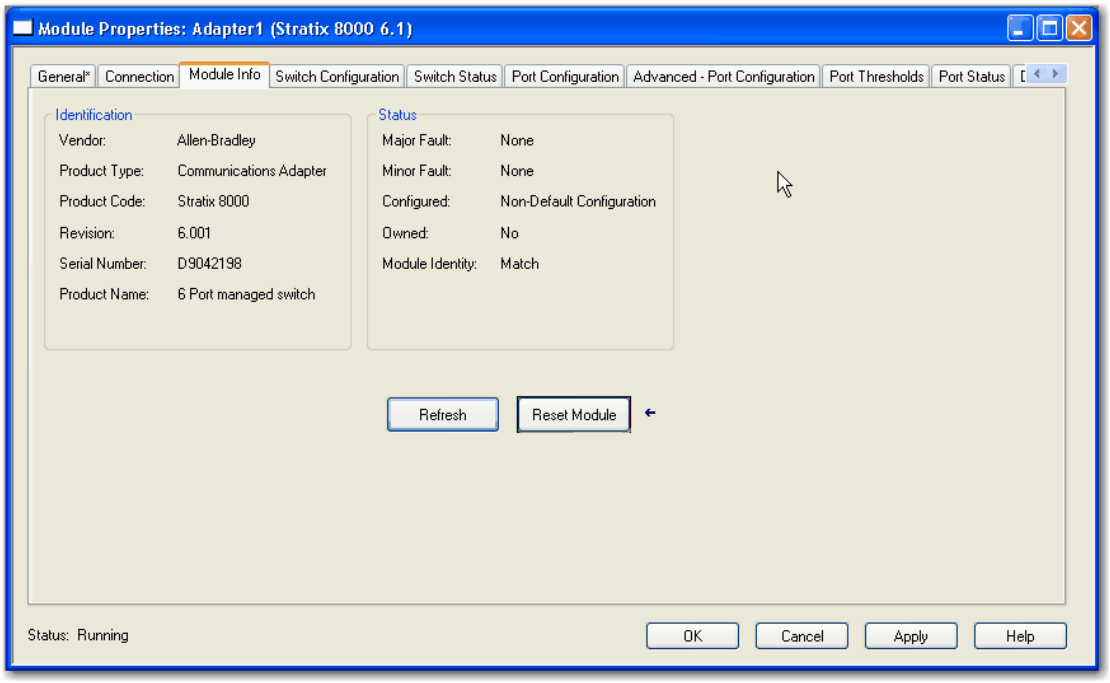
Set the threshold limits for broadcast, unicast, and multicast traffic for each active port on the Advanced - Port Thresholds tab. The number of packets sent is compared against the threshold value. These limits help to prevent a single device from sending too much traffic.



Field	Description
Unit	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	Indicates the port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number. For example: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Storm Control Threshold Settings	Set the threshold values for the broadcast, unicast, and multicast traffic for each port. The number of packets being sent is compared against the threshold value. If an undesirable network event occurs and the threshold value has been exceeded, a yes value is displayed in the appropriate column in the Port Status tab and in the Traffic Exceeded on Any Port parameter in the Switch for Automation Status tab. Network traffic of the type that exceeded threshold (broadcast, unicast, or multicast) is dropped until it falls below the falling threshold. The falling threshold is automatically set to 5% less then the entered threshold value.
Broadcast, Unicast and Multicast	Complete these fields for each traffic type: • Enable—Check to enable the storm control on the selected port. The respective threshold value and units are applied to the selected port when you click Set. Clear the checkbox to disable the storm control for the selected port. Zero (0) is applied to the threshold value and units attributes when you click Set. • Threshhold—Type the value for the threshold after you choose the unit of measurement: – If Units is set to pps or bps, type a value between 0...10000000000. – If Units is set to %, type a value between 0...100. • Units—Choose the unit of measurement for the threshold: – pps (packets per second) – bps (bits per second) – %

Monitor and Reset the Switch

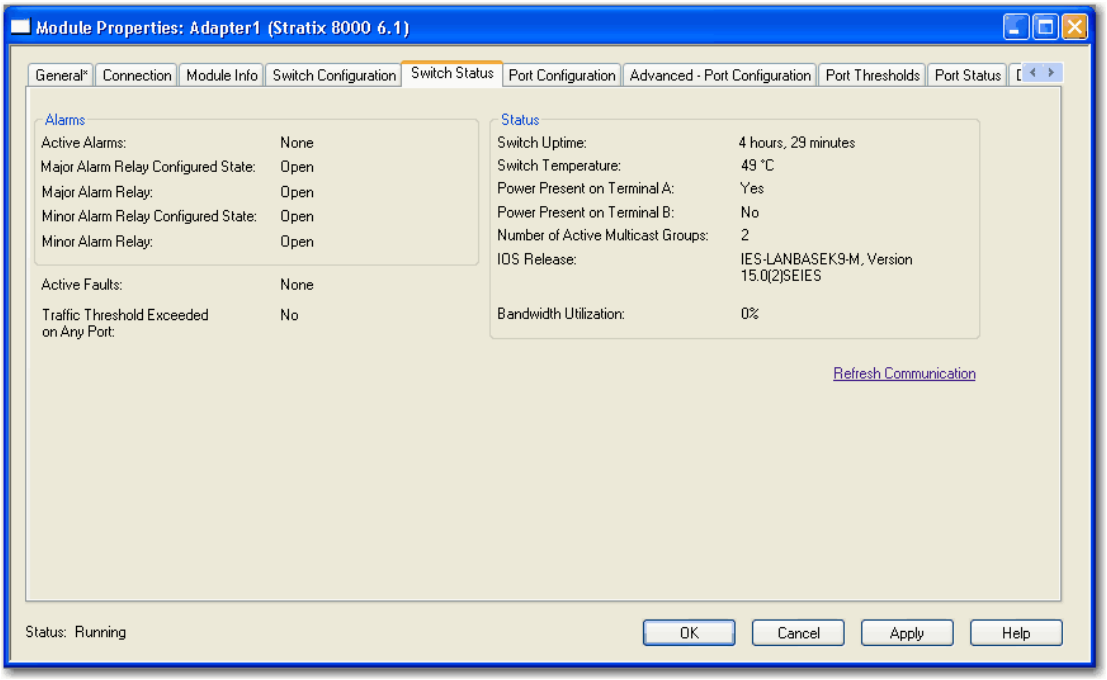
In the software, you can monitor and reset the switch by accessing the Module Properties screen.



Field	Description
Identification	Displays the following switch information: • Vendor • Product Type • Product Code • Revision • Serial Number • Product Name
Status	Displays the following status information: • Major/minor Fault Status – None – Recoverable – Non-recoverable • Configuration – Non-default Configuration – Default Configuration • Owned – Yes. There is an I/O connection. – No. There is not an I/O connection. • Module Identity – Match. Agrees with what is specified on the General Tab. In order for the Match condition to exist, the vendor, product type, product code, and major revision must agree. – Mismatch. Does not agree with what is specified on the General tab. The Module Identity field does not take into account the Electronic Keying or Minor Revision selections for the switch that were specified on the General tab.
Refresh	Click to refresh the tab with new data from the module.
Reset Module	Click to perform a switch reset (power cycle) with the current configuration file. If the Password Confirmation dialog box appears, enter a password. **IMPORTANT:** Resetting a module causes all connections to or through the module to close. This can result in a loss of control.

Switch Status

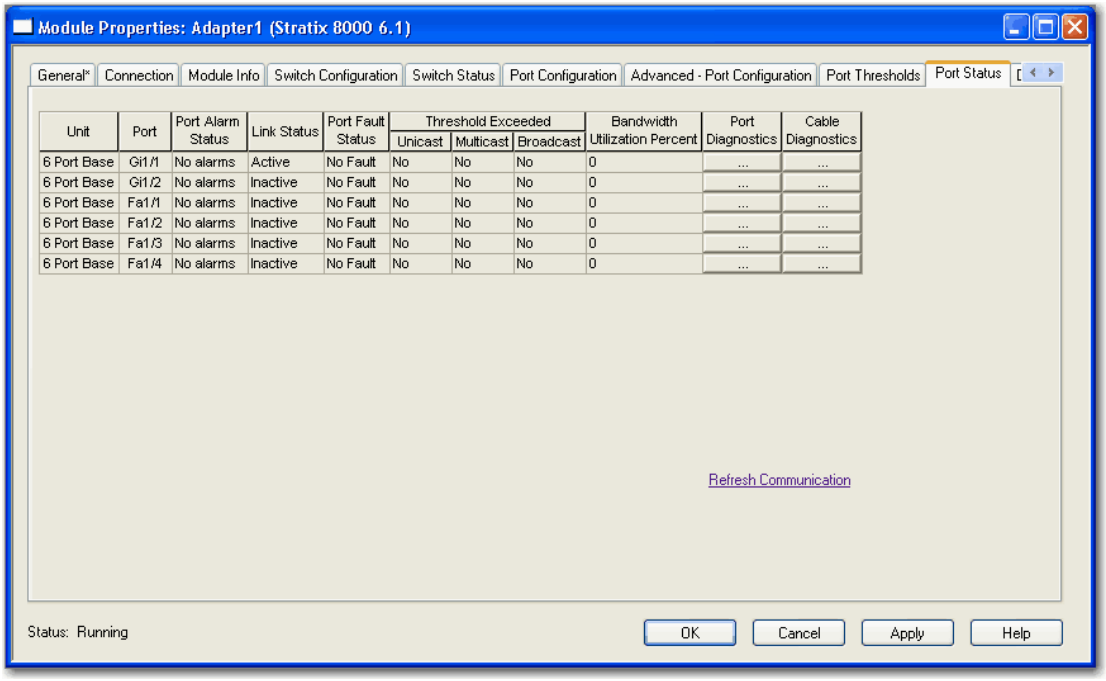
Through the software, you can monitor switch status. Use this tab to monitor the switch and port conditions to quickly see if a fault or error condition exists. This tab also shows the overall health of the switch (temperature and power).



Field	Description
Alarms	Displays the active switch and port alarms: • Active Alarms – None – Port alarm – Dual Mode Power Supply alarm – Primary Temperature alarm • Major Alarm Relay Configured State—Displays whether the major alarm relay is configured. • Major Alarm Relay—Displays whether the major alarm relay is On or Off. • Minor Alarm Relay Configured State—Displays whether the minor alarm relay is configured. • Minor Alarm Relay—Displays whether the minor alarm relay is On or Off.
Active Faults	Displays the active switch and port faults. If the port and hardware faults are active, the Hardware fault appears. Valid values: • None • Port fault • Hardware fault
Traffic Threshold Exceeded on Any Port	Displays a yes or no value indicating whether the current unicast, multicast, and broadcast thresholds have been exceeded on any port. To view the status of the active ports, click the Port Status tab. To view the threshold values, click the Advanced - Port Threshold tab.
Status	Displays the status of the switch: • Switch Uptime—Displays the days, hours, and minutes that the switch has been functioning since the last reboot. • Switch Temperature—Displays the current internal temperature (in degree Celsius) of the switch. • Power Present on Terminal A—Displays a yes or no value indicating whether power is present on Terminal A. • Power Present on Terminal B—Displays a yes or no value indicating whether power is present on Terminal B. • Number of Active Multicast Groups—Displays the number of active multicast groups. • IOS Release—Displays the current version of the switch operating system. • Bandwidth Utilization—Displays the total percentage of the switch bandwidth being used.

Port Status

The Port Status tab lets you monitor alarms, statuses, thresholds, and bandwidth utilization. As well, you can view port and cable diagnotics.



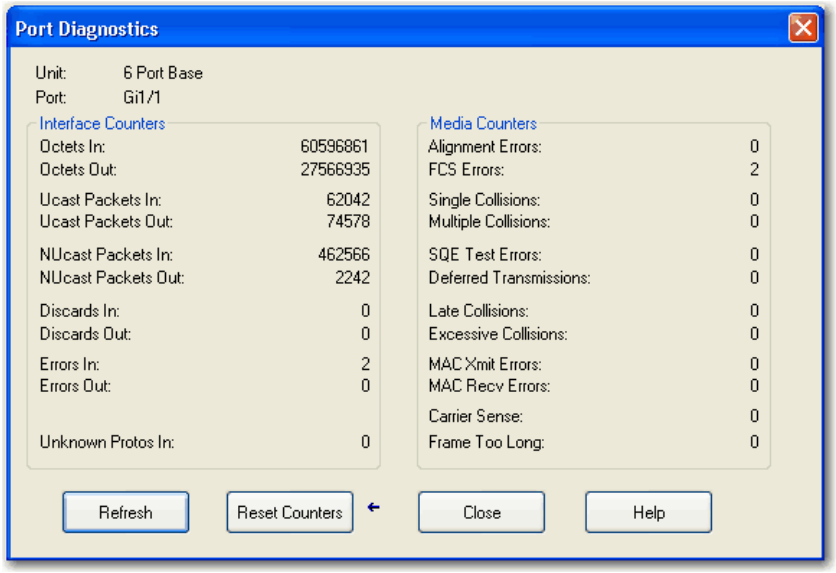
Field	Description
Unit	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	Indicates the port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number, such as in the following examples: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Port Alarm Status	Displays the current 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	Displays whether the link is active or inactive.
Port Fault Status	Displays the current status of the port alarm: • Error—Disable event • SFP error—Disabled • CDP native VLAN mismatch • MAC address flap • Port security violation • No fault
Threshold Exceeded	Displays unusual changes in the network traffic. If the threshold value set on the Advanced - Port Threshold tab has been exceeded, a yes value appears in the appropriate column. If the threshold value has not been exceeded, a no value appears in the appropriate column: • Unicast—Displays a yes or no value indicating whether the current unicast traffic has exceeded the threshold value. • Multicast—Displays a yes or no value indicating whether the current multicast traffic has exceeded the threshold value. • Broadcast—Displays a yes or no value indicating whether the current broadcast traffic has exceeded the threshold value.

Field	Description
Bandwidth Utilization Percent	Displays the percentage of the bandwidth being used. Note whether the percentage of usage is what you expect during the given time of network activity. If usage is higher than expected, an issue can exist.
Port Diagnostics	Click to display the Port Diagnostics dialog box for the corresponding port. The Port Diagnostics dialog box provides you information to diagnose a network performance issue.
Cable Diagnostics	Click to display the Cable Diagnostics dialog box for the corresponding port. The Cable Diagnostics dialog box provides information to diagnose a cable issue.

Port Diagnostics

View the status of the link performance on Port Diagnostics dialog box:

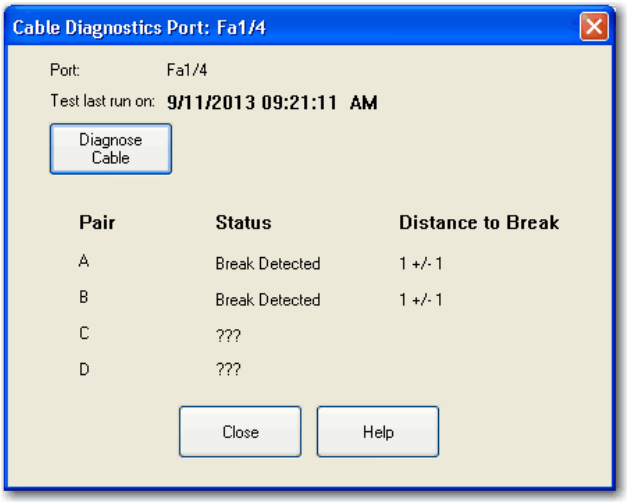
- View octet and packet counters
- View collisions on the link
- View errors on the link
- Reset and clear all status counters



Field	Description
Unit	Indicates where the port resides: • Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).
Port	Indicates the port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number, such as in the following examples: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Interface Counters	Let you view the status of octets received and sent and packets received and sent: • Octets In—The number of octets received by the port. • Octets Out—The number of octets sent by the port. • Ucast Packets In —The number of unicast packets received by the port. • Ucast Packets Out —The number of unicast packets sent by the port. • NUcast packets In—The number of multicast packets received by the port. • NUcast packets Out—The number of multicast packets sent by the port. • Discards In—The number of inbound packets that have been discarded. • Discards Out—The number of outbound packets that have been discarded. • Errors In—The number of inbound packets that contain errors. • Errors Out—The number of outbound packets that contain errors. • Unknown Protos (Protocols) In—The number of inbound packets with unknown protocols.
Media Counters	Let you view the number of collisions on a link. Collision counters: • Single —The number of single collisions. • Multiple —The number of multiple collisions. • Late —The number of late collisions. • Excessive—The number of frames for which transmission fails due to excessive collisions. Error counters: • Alignment—The number of frames received that are not an integral number of octets in length. • FCS (Frame Check Sequence)—The number of frames received that do not pass the FCS check. • SQE Test Errors—The number of times that the SQE TEST ERROR message is generated. • Deferred Transmissions—Count of transmissions deferred by busy network. • MAC Xmit Errors—The number of frames that failed to transmit due to an internal MAC sublayer transmit error. • MAC Recv Errors—The number of frames that failed to be received due to an internal MAC sublayer receive error. • Carrier Sense—The number of times the carrier sense condition was lost or never asserted when attempting to transmit a frame. • Frame Too Long—The number of frames received that exceed the maximum permitted frame size.

Cable Diagnostics

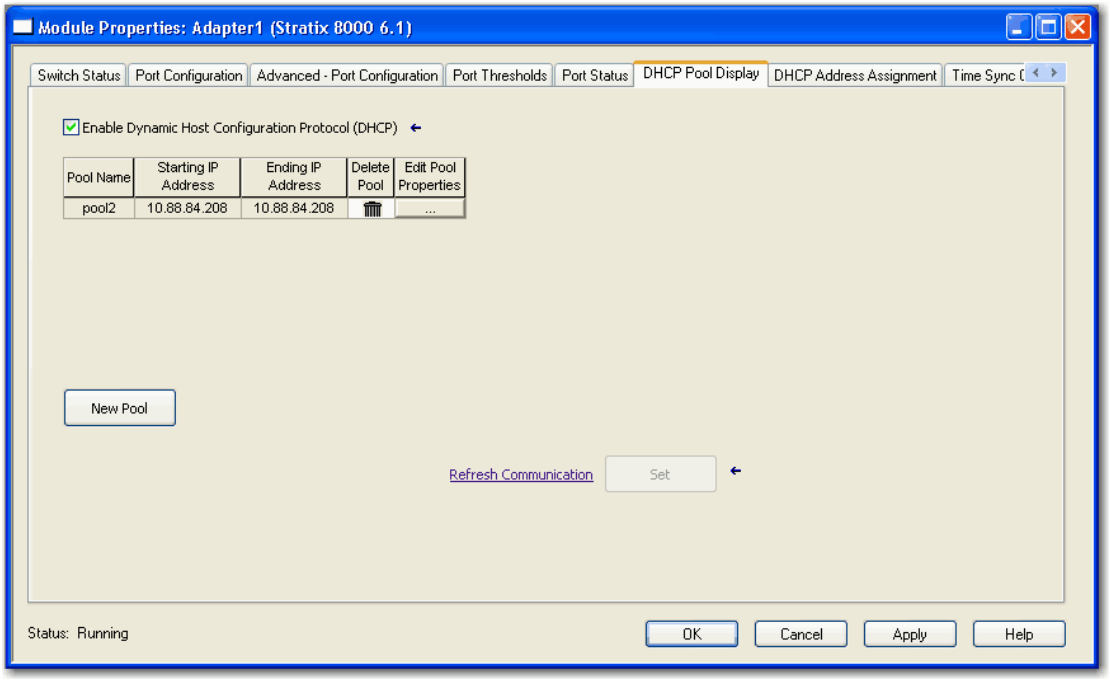
The Cable Diagnostics dialog box provides information to diagnose a cable issue. The information on this dialog box is not displayed if you are offline.



Field	Description
Port	Indicates the port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number. For example: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.
Test last run on	The time the test was last executed. The date time format is mm/dd/yy hh:mm:ss tt. If the test has never been run, the time and all distance and status information is blank.
Pair	Each pair (pair of cables in the network) individually listed. If pair does not exist or test has never been run, this is blank.
Status	Specifies the link state the last time the test was executed. If pair does not exist or test has never run, status is blank. For distance, if the pair is Normal status, 'No Break Detected' is shown. No distance is displayed.
Distance to Break	The distance to the break from the switch for each estimated pair with a plus or minus error value individually listed. A value appears only when the status of an existing pair is not Normal. This is blank if the test was never run before. If a pair does not exist, '???' appears.
Diagnose Cable	Click to run the Diagnose Cable test. A connection interruption warning appears: • If you are sure you want to continue with the test, click Yes. Be prepared to enter a valid password to run the test. • If you do not want to run the test, click No or close the window. **IMPORTANT:** To run a valid test on gigabit ports, you must first configure the gigabit port as an RJ45 media type in the Device Manager Web interface, as described in Configure Port Settings on page 97. **IMPORTANT:** This test can interrupt connections to the module and to any other modules connected through this module. Also, the connection between workstation and controller can be interrupted. You must have the correct privilege to run this test.

DHCP Pool Display

View the DHCP address pool information for the switch on the DHCP Pool Display tab. You can view 0...15 pools. This information is gathered directly from the switch. Each row represents a single instance and instance values cannot be consecutive.



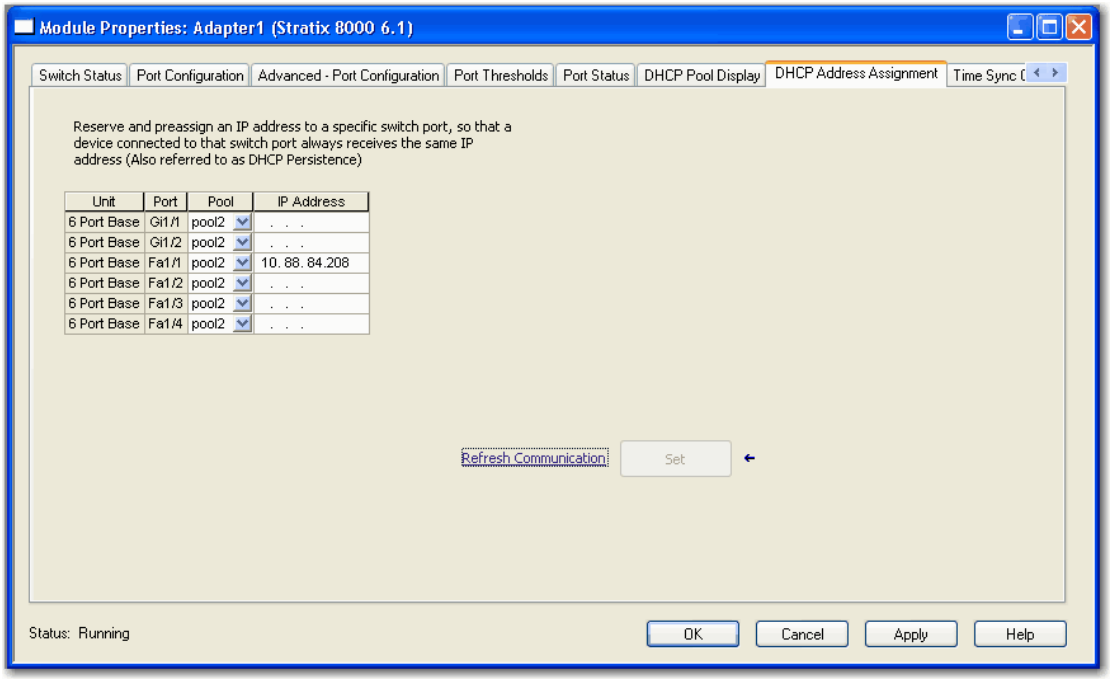
TIP You must be online to view information on this tab.

Field	Description
Enable Dynamic Host Configuration Protocol (DHCP)	Enables or disables pools. If checked, all controls on the grid are set to online and the appropriate values are obtained from the switch and displayed. If cleared, all controls on the grid are set to offline. From the keyboard, press Alt - D.
Pool Name	Displays the name of the DHCP IP address pool configured on the switch. A DHCP IP address pool is a range (or pool) of available IP addresses that the switch can assign to connected devices. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab.
Starting IP Address	Displays the starting IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods (for example, 255.255.255.255). Each number can be from 0…255.
Ending IP Address	Displays the ending IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods (for example, 255.255.255.255). Each number can be from 0…255.
Delete Pool	Click to delete the selected DHCP pool row. Afterwards, if you click the Set button, a confirmation dialog box is displayed and all of the persistent addresses associated with the selected DHCP pool row are also deleted. The Delete Pool button is available only when the switch is online, the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is checked, and when the respective row is populated. The Delete Pool button is dimmed when the switch is offline, and the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is cleared.
Refresh	Click to refresh the grid control with new data obtained directly from the switch. From the keyboard, press Alt-R. If you have changed a value in the grid and clicked Refresh before clicking Set, all values in the grid are returned to their previously set values. The Refresh button is available only when the switch is online. The Refresh button is dimmed when the switch is offline.

Field	Description
Edit Pool Properties	Click to display the DHCP Pool Definition and Edit dialog box and populate it with values from the instance corresponding to the current row. The Edit column button is available only when the switch is online, the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is checked, and when the respective row is populated. The Edit column button is dimmed when the switch is offline and the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is cleared.
New Pool	Click to display the DHCP Pool Definition and Edit dialog box (all fields are blank and the Custom radio button is not selected). Additionally, a new row/instance is added to the grid on the Module Properties dialog box - DHCP Pool Display. From the keyboard, press Alt - N. The New button is available only when the switch is online and the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is checked. The New button is dimmed when the switch is offline and the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is cleared.
Set	Click to apply attribute changes on this dialog box to the switch. If an error occurs while setting an attribute, the Set operation is terminated and all subsequent attribute values are not applied to the switch. Additionally, the Set button remains available. The Set button is available only when the switch is online and any of the attribute values have changed. The Set button is dimmed when the switch is offline.

DHCP Address Assignment

Use the DHCP Address Assignment tab to view and configure DHCP persistence. With DHCP persistence, you can assign a specific IP address to each port, so that the device attached to a given port receives the same IP address.

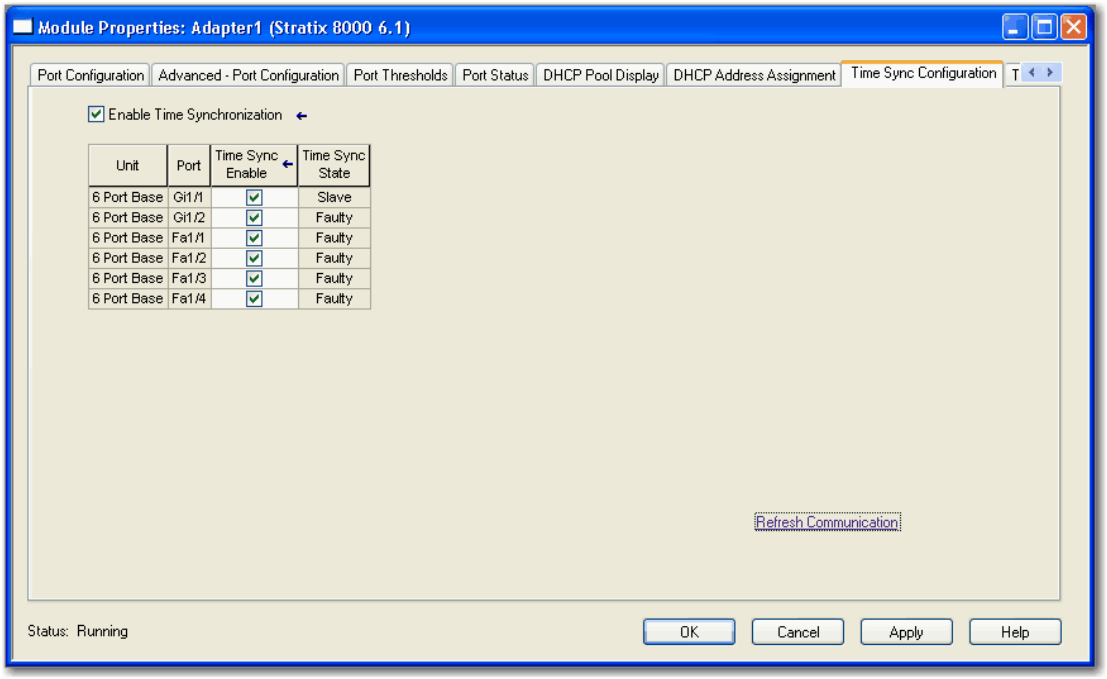


TIP You must be online to view information on this tab.

Field	Description
Unit	Displays the unit on which the selected port resides: • 6 Port Base • 10 Port Base • Expansion 1 • Expansion 2
Port	Displays the ports available for the configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa1/1 is Fast Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module. • Fa3/1 is Fast Ethernet port 1 on the second expansion module.
Pool	Displays the pool names from the DHCP IP address pool that corresponds to the instances available in the switch. If you delete all of the rows containing pools on the DHCP Pool Display tab on the Module Properties dialog box and click Refresh, Pool is blank. Pool is available only when the switch is online and dimmed when the switch is offline.
IP Address	Displays the IP address assigned to the switch port. The format is a 32-bit numeric address written as four numbers separated by periods (for example, 255.255.255.255). Each number can be from 0…255. The IP address that you assign is reserved for the selected port and is not available for normal DHCP dynamic assignment. The IP address must be an address from the pool specified in the DHCP Pool Name field. IP Address is available only when the switch is online and dimmed when the switch is offline.
Refresh	Click to refresh the grid control with new data obtained directly from the switch. From the keyboard, press Alt-R. If you have changed a value in the grid and clicked Refresh before clicking Set, all values in the grid are returned to their previously set values. The Refresh button is available only when the switch is online. The Refresh button is dimmed when the switch is offline.
Set	Click to apply changes on this dialog box to the switch. Be prepared to enter a password if the Enter Password dialog box appears.

Time Sync Configuration

Use this tab to synchronize the ports by using time synchronization (based on Precision Time Protocol [PTP]). PTP synchronizes within 25-nanosecond accuracy the real-time clocks of the devices in a network. Using the best master clock algorithm, the switch identifies the switch port that is connected to a device with the best clock source. The switch then synchronizes its internal clock with the best clock source, and that port is set to master state. The most precise clock source in the network is referred to as the Grandmaster clock..



TIP

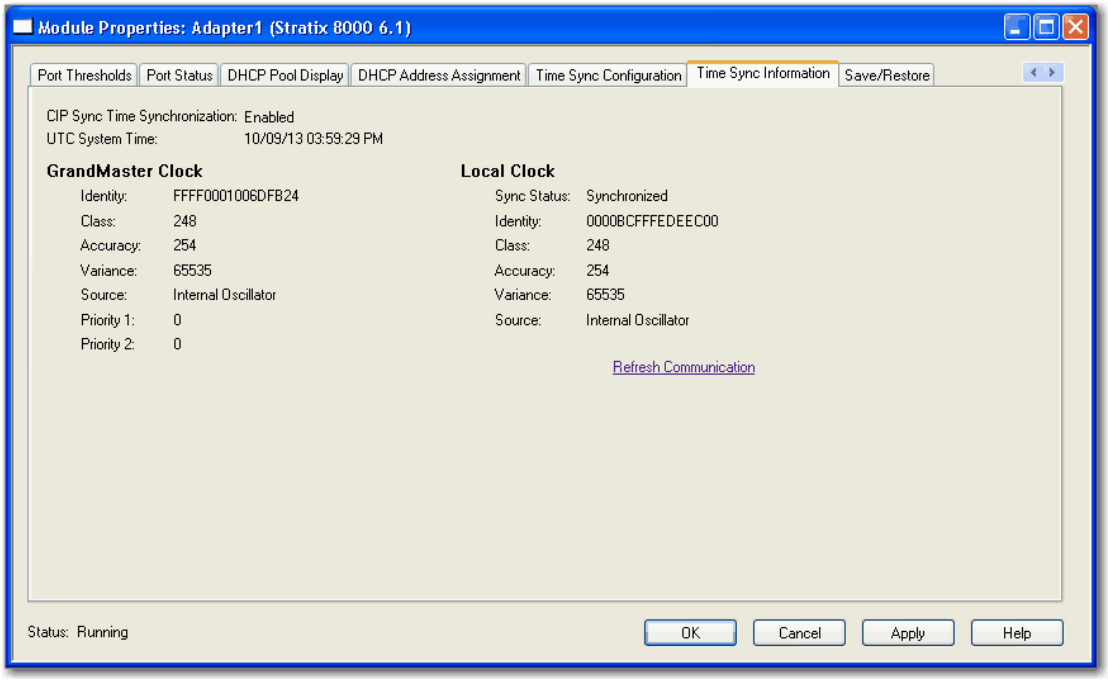
The information displayed on this tab is visible when Time Sync is not enabled. When Time Sync is enabled, you see the following fields:

- Time Sync State
- Enable Time Sync Fowarding of Time Synchronization Data checkbox
- Port Enable
- Port State

Field	Description
Time Sync Enable	Check to enable time synchronization on the device. Only the ports on the base switch module are capable of time synchronization. The switch expansion modules do not support time synchronization. However, time synchronization is interdependent with the Enable Expansion Port Forwarding of Time Synchronization setting. Expansion ports are put in Forward mode when Time Synchronization is disabled on base ports. Clear the checkbox to disable the time synchronization on the device. The Enable Time Synchronization and Port State features appear dimmed when the Enable Time Synchronization checkbox is cleared.
Time Sync State	Displays one of these states: • Initializing—The port is initializing. • Faulty—A fault is present. • Disabled—The port is disabled. • Listening—The port is in a listening state. • Pre_Master—The port is in the pre-master state. • Master—The port is the system master. • Passive—The port is receiving data. • Uncalibrated—The port is uncalibrated. • Slave—The port is a slave in the system.
Enable Expansion Port Forwarding of Time Synchronization Data	This checkbox appears only when the switch is online. When enabled, the expansion ports are put into Forward mode. In Forward mode, the expansion module port forwards time synchronization messages. If disabled, the expansion module port drops time sync messages.
Port	Displays the port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number: • Gi1/1 is Gigabit Ethernet port 1 on the base • Fa1/1 is Fast Ethernet port 1 on the base • Fa2/1 is Fast Ethernet port 1 on the first expansion module • Fa3/1 is Fast Ethernet port 1 on the second expansion module
Port Enable	Check to enable the configuration of the port on the device. Clear the checkbox to disable the port configuration on the device. The Port Enable feature appears dimmed when the Enable Time Synchronization checkbox is cleared.
Port State	Displays the current state of the time synchronization port on the device. The Port State is blank and dimmed when the Enable Time Synchronization checkbox is cleared: • Initializing • Faulty • Disabled • Listening • Pre-Master • Master • Uncalibrated • Slave
Refresh	Click to refresh the tab with new data from the switch.
Set	Click to send the settings to the switch. Be prepared to enter a valid password to set configuration settings. The Set button appears dimmed when the switch is offline.

Time Sync Information

Use the Time Sync Information tab to view current information about the real-time clocks in the network. The CIP Time Synchronization protocol provides a standard mechanism to synchronize clocks across a network of distributed devices.



TIP The CIP Sync Time Synchronization feature supports both Boundary and End-to-End Transparent mode. End-to-End Transparent mode synchronizes all switch ports with the Grandmaster clock using the IEEE 1588 V 2 End-to-End Transparent clock mechanism, and is the preferred mode.

TIP The information on this tab is not displayed if you are offline or the CIP Sync Time Synchronization feature is disabled.

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	Displays clock property information for the Grandmaster clock. The Grandmaster clock is the most precise clock source in the network.
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 represented in offset scaled log units. The lower the variance, the better the clock.

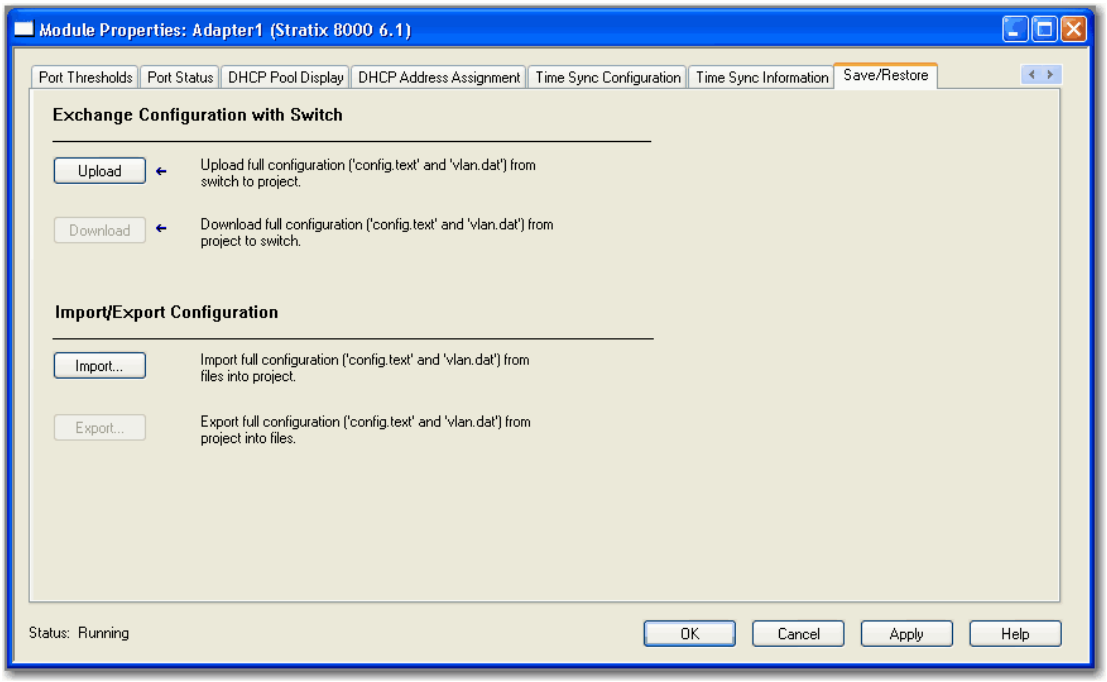
Field	Description
Source	Displays the clock time source: • Atomic Clock • GPS • Terrestrial Radio • CIP Time Synchronization • NTP • HAND Set • Other • Internal Oscillator
Priority 1 Priority 2	Displays the relative priority of the Grandmaster clock to other clocks in the system. The value is between 0…255. The highest priority is 0.
Local Clock	Displays properties for the local clock.
Sync Status	Displays whether the local clock is synchronized or asynchronized with the Grandmaster clock.
Identity	Displays the unique identifier for the local clock. The format depends on the network protocol. • The Ethernet protocol encodes the MAC address into the identifier. • The DeviceNet and ControlNet protocols encode the Vendor ID and serial number into the identifier.
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 represented 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

Save and Restore Switch Configuration

Use this tab to save the switch configuration to a file for archiving, or restore a switch configuration stored locally on the computer, or within the software project.

You must be online to save and restore configuration files. Most of the settings appear dimmed when the switch is offline.

Be prepared to enter a valid switch password to save and restore a switch configuration.



The switch configuration consists of these two files:

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

Once the switch configuration is uploaded to the software project file, the switch configuration can be exported as computer files by using the export button.

You can import a switch configuration from the appropriate files on your computer to the project by using the Import button on the switch AOP. You can then download the configuration to the switch by using the Download button on the AOP. Refer to Save and Restore Switch Configuration on page 168 for more information about the Save and Restore feature.

Troubleshoot the Switch

This chapter helps you resolve issues related to Stratix 8000 and Stratix 8300 switches and perform common functions, such as resetting a switch.

For additional troubleshooting, refer to the following:

- Diagnose Cabling Problems on page 131
- View System Log Messages on page 132

IP Address Issues

Following are some basic troubleshooting tips for issues related to the switch IP address.

Table 21 - IP Address Issues

Issue	Resolution
IP address is not received from DHCP server	If the switch does not receive an IP address from an upstream device operating as a DHCP server, make sure that the upstream device is operating as a DHCP server and again follow the procedures to set up the switch in Chapter 2, Getting Started .
Switch has wrong IP address	If the switch is installed in your network but you cannot access the switch because it has the wrong IP address, assign a new switch IP address. Refer to Access Direct Managed Mode on page 171 to assign the IP address, and then update the switch IP address on the Device Manager Express Setup window.

Device Manager Web Interface Issues

Following are some basic troubleshooting for issues related to displaying the Device Manager Web interface.

Table 22 - Device Manager Web Interface Issues

Issue	Resolution
Device Manager Web interface does not appear	If you cannot display the Device Manager Web interface from your computer or laptop, 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 or laptop are in the same network or subnetwork: • If your switch IP address is 172.20.20.85 and your computer or laptop IP address is 172.20.20.84, both devices are in the same network. • If your switch IP address is 172.20.20.85 and your computer or laptop 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 or laptop IP address. • If the issue persists, follow the procedure in the Access Direct Managed Mode section on page 171, and then update the switch network settings on the device manager Express Setup window. • If the issue still persists, follow the procedure in the Recover the Switch Firmware and Restore Factory Defaults section on page 173.
Device Manager Web interface is not operating properly	If the Device Manager Web interface does not operate properly (for instance, the device manager is not responding), follow the procedure in the Access Direct Managed Mode section on page 171, and then update the switch network settings on the Device Manager Web interface Express Setup window. If the issue persists, follow the procedure in the Recover the Switch Firmware and Restore Factory Defaults section on page 173.
Device Manager Web interface is not accessible through the network	If you cannot access the device manager remotely from a web browser, follow the procedure in the Access Direct Managed Mode section on page 171.

Switch Performance

Following are some basic troubleshooting for issues related to switch performance.

Table 23 - Switch Performance

Issue	Resolution
Speed, Duplex, and Autonegotiation	If the port statistics show a large amount of alignment errors, frame check sequence (FCS), or late-collisions errors, this can indicate a speed or duplex mismatch. A common issue with speed and duplex occurs when the duplex settings are mismatched between two switches, between a switch and a router, or between the switch and a workstation or server. This can happen when 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 is different 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 this does not solve the issue, there could be an issue with the firmware or software on your NIC. You can resolve this by upgrading the NIC driver.
Cabling distance	If the port statistics show excessive FCS, late-collision, or alignment errors, verify that the cable distance from the switch to the connected device meets the recommended guidelines.

Access Direct Managed Mode

You can display the Device Manager Web interface and manage the switch through a physical connection between one of the switch ports and your computer or laptop. This type of management connection is referred to as the Direct Managed mode. This mode is typically used to connect to the switch by using the Device Manager Web interface when the IP address of the switch is unknown.

Before you can access Direct Managed mode, you must make sure of the following:

- You must have physical access to the switch.
- Make sure that at least one switch port is enabled and is not connected to a device.

Follow these steps to access the Direct Managed mode.

1. Press the Express Setup button until the Setup status indicator blinks green and the status indicator of an available switch downlink port blinks green.

   The port with a blinking green status indicator is designated as the Direct Managed mode port. This port is determined by the following:

   - If all downlink ports are not connected to devices or if multiple downlink ports are connected to devices, the first available downlink port is selected as the Direct Managed mode port.
   - If only one downlink port is connected to a device, that port is selected as the Direct Managed mode port.

   If there is no available switch downlink port to which to connect your computer or laptop, disconnect a device from one of the switch downlink ports, and then press the Setup button again until the Setup status indicator and the port status indicator blink green.
2. Use a Category 5 Ethernet cable to connect your computer or laptop to the switch port with the blinking port status indicator.
3. Wait until the port status indicators on the switch and your computer or laptop are solid green.

   The solid green port status indicators means a successful connection between the two devices.
4. Start a web browser on your computer or laptop.

   A password prompt, followed by the Device Manager Web interface page appears.

If the Device Manager Web interface does not appear, make sure that any pop-up blockers or proxy settings in your browser software are disabled and that any wireless clients running on your computer or laptop are disabled.

If the Device Manager Web interface still does not appear, enter a URL in your browser, such as http://www.rockwellautomation.com. The browser redirects to the Device Manager Web interface.

Restart or Reset the Switch

If you cannot solve an issue by reconfiguring a feature, either restarting or resetting the switch can solve the issue or help you to eliminate probable causes. If the issue exists after you reset the switch to its default settings, it is unlikely that the switch is causing the issue.

Option	Description
Restart	This option restarts the switch without turning off power. The switch retains its saved configuration settings during the restart process. However, the Device Manager Web interface is unavailable during the process. When the process completes, the switch displays the Device Manager Web interface. **Important:** Restarting the switch interrupts connectivity of your devices to the network.
Reset the Switch to Factory Defaults	This option resets the switch, deletes the current configuration settings, returns to the factory default settings, and then restarts the switch. **Attention:** Resetting the switch deletes all customized switch settings, including the IP address, and returns the switch to the factory default settings. The same software image is retained. You need to reconfigure the basic switch settings. Refer to Set Up the Switch Initially with Express Setup on page 48. **Attention:** Resetting the switch interrupts connectivity of your devices to the network.

IMPORTANT Restarting or resetting the switch interrupts connectivity of your devices to the network.

Restart the Switch from the Device Manager Web Interface

From the Device Manager Web interface, on the Restart/Reset window, click Restart the Switch.

This option restarts the switch without turning off power. The Device Manager Web interface is unavailable during the restart process. When the process completes, the switch displays the Device Manager Web interface.

If you do not know the switch IP address, follow the procedure in the Access Direct Managed Mode on page 171 to access Direct Managed mode.

Restart the Switch from the Studio 5000 Environment

From the Logix Designer application in the Studio 5000 environment, do the following.

1. Click the Module Info tab.
2. Click Reset Module.

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

Reset the Switch to Factory Defaults

ATTENTION: Resetting the switch deletes all customized switch settings, including the IP address, and returns the switch to its factory default. The same software image is retained. To manage the switch or to display the device manager, reconfigure basic switch settings as described in Chapter 4, Manage the Switch via the Device Manager Web Interface and use the new IP address.

IMPORTANT Restarting the switch interrupts connectivity of your devices to the network.

From the Device Manager Web interface, do the following.

1. Access the Device Manager Web interface Restart/Reset window.
2. Click Reset the Switch.

   This option resets the switch, deletes the current configuration settings, returns to the factory default settings, and then restarts the switch.

   If you do not know the switch IP address, see Access Direct Managed Mode on page 171 to access Direct Managed mode. Then go back to step 1 above.

Recover the Switch Firmware and Restore Factory Defaults

Before you can recover switch firmware, you must make sure of the following:

- You have physical access to the switch.
- At least one switch port is enabled and is not connected to a device.

You can recover the switch firmware if needed, such as in these scenarios:

- The image is corrupted, as indicated by the switch continuously trying to restart.
- You deleted the image due to a failed firmware upgrade.
- You forget the switch password.

Recovering the switch firmware involves deleting all switch configuration settings and returning the switch to its factory default settings. Follow these steps to return the switch to its factory default settings.

1. Remove power from the switch.
2. Reapply power to the switch.
3. While the switch is powering up, press and hold the Express Setup button.
4. When the EIP Mod, EIP Net and Setup status indictors turn red, release the Express Setup button.

   The switch continues powering up in its factory default state.
5. Set up the switch, as described in Chapter 2, Getting Started.
6. Upgrade the firmware, as described in Troubleshoot a Firmware Upgrade.

Troubleshoot a Firmware Upgrade

If you attempted to upgrade the switch firmware but received a message that the upgrade failed, make sure that you still have access to the switch. If you still have switch access, follow these steps.

1. Make sure that you downloaded the correct .tar file from http://www.rockwellautomation.com.
2. If you downloaded the correct .tar file, refresh your Device Manager Web interface browser session to make sure that there is connectivity between the switch and your computer or laptop or network drive:
   - If you have connectivity to the switch and the Device Manager Web interface, retry the upgrade.
   - If you do not have connectivity to the switch and the Device Manager Web interface, see Recover the Switch Firmware and Restore Factory Defaults on page 173.

Status Indicators

Switch Status Indicators

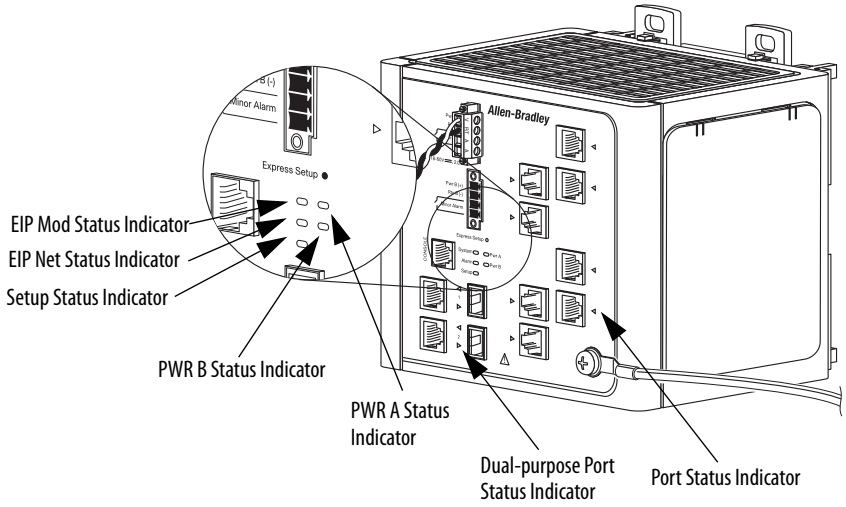


Table 24 - Switch Status Indicators

Indicator	Status	Description
EIP Mod (EtherNet/IP module status)	Off	No power. Check the power supply and cabling.
	Solid green	The switch is operating properly.
	Flashing green	The switch has not been configured as a managed switch. For example, Express Setup was not performed, or there is a missing IP address or password. The switch is operating as an unmanaged switch.
	Flashing red	A recoverable minor fault, such as an incorrect configuration, has occurred.
	Solid red	A non-recoverable major fault has occurred. Cycle power. If the problem persists, contact Rockwell Automation Technical Support.
	Flashing green and red	The switch is performing a POST.
EIP Net (EtherNet/IP network status)	Off	The switch has no power or IP address: • Check the power supply and cabling. • Make sure the switch is properly configured.
	Solid green	The switch has at least one established EtherNet/IP connection.
	Flashing green	No EtherNet/IP connection exists yet, but the switch has obtained an IP address.
	Flashing red	The EtherNet/IP connection has timed out.
	Solid red	The switch has detected that its IP address is already in use.
	Flashing green and red	The switch is performing a POST.
Setup	Off	The switch is configured as a managed switch.
	Solid green	The switch is performing initial setup.
	Flashing green	The switch is in one of the following states: • Initial setup • Recovery • Initial setup incomplete
	Solid red	The switch failed to start initial setup or recovery because there is no available switch port to which to connect the management station. Disconnect a device from a switch port and press the Express Setup button.
PWR A and PWR B	Off	The circuit or system has no power.
	Solid green	The circuit has power.
Dual-purpose port	See Dual-purpose Port Status Indicators on page 177.	
Port	See 10/100 Copper, 100BaseFX, and SFP Port Status Indicators on page 178.	

Dual-purpose Port Status Indicators

The status indicators on a dual-purpose port, as shown in the following figure, show whether the RJ45 connector or an SFP module is active. The port can be configured as either a 10/100/1000 port through the RJ45 connector or as an SFP module, but not both. The status indicators show which port is being used and the current port activity.

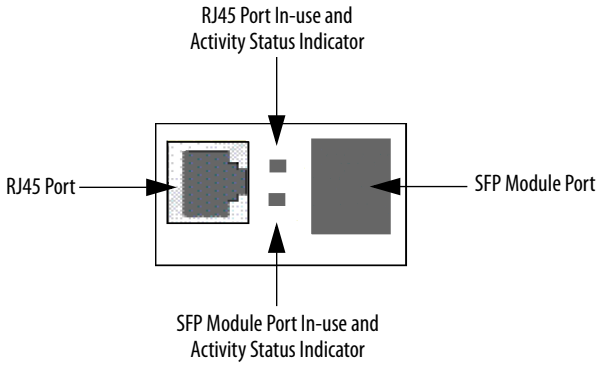
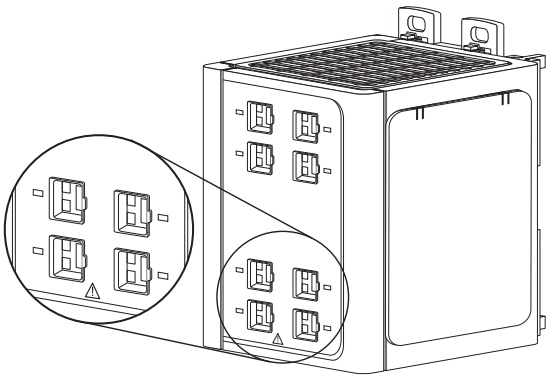


Table 25 - Dual-purpose Port Status Indicators

Status	Description
Off	No link.
Solid green	A link is present.
Flashing green	The port is sending or receiving data.
Flashing amber	A link blocked by STP is sending or receiving data.
Alternating green and amber	A link is faulted. Error frames can affect connectivity. Excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication (RJ45 connection only).
Solid amber	The port is not forwarding. The port was disabled by management, or there is an address or STP violation. After a port is reconfigured, the port status indicator can remain amber for as many as 30 seconds while STP checks the network for possible loops.

10/100 Copper, 100BaseFX, and SFP Port Status Indicators

The status indicators on a copper, fiber, or SFP port show the status of the individual port.



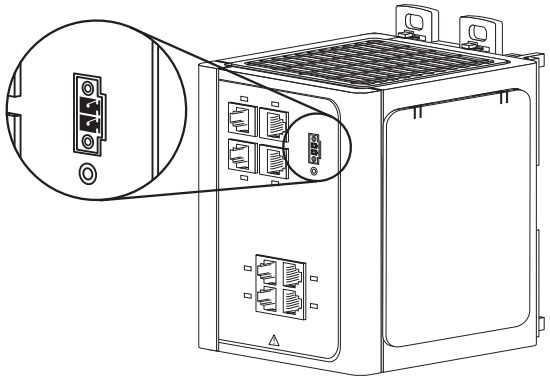
32441-M

Table 26 - Copper and Fiber Expansion Module Status Indicators

Status	Description
Off	No link.
Solid green	A link is present.
Flashing green	The port is sending or receiving data.
Flashing amber	A link blocked by STP is sending or receiving data.
Alternating green and amber	A link is faulted. Error frames can affect connectivity. Excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication (RJ45 connection only).
Solid amber	The port is not forwarding. The port was disabled by management, or there is an address or STP violation. After a port is reconfigured, the port status indicator can remain amber for as many as 30 seconds while STP checks the network for possible loops.

PoE Port Status Indicator

The PoE port status indicator on the PoE expansion modules shows the functionality and status of the PoE ports.



32443-M

Table 27 - PoE Port Status Indicator

Status	Description
Off	PoE is off. If a powered device is receiving power from an AC power source, the port status indicator is off even if a powered device is connected to the switch port.
Solid green	PoE is on. The status indicator is green only when the switch port is providing power.
Alternating green and amber	PoE is denied because providing power to a powered device exceeds the power capacity of the expansion module.
Flashing amber	PoE is off due to a fault. **ATTENTION:** Noncompliant cabling or powered devices can cause a PoE port fault. Use only standard-compliant cabling.
Solid amber	PoE for the module is disabled.

Notes:

I/O Data Types

Predefined tags in the Logix Designer application for input and output data types have a structure corresponding to the switch (module) selected when it was added to the I/O tree. Its members are named in accordance with the port names. For example, if you select the 18-port switch, the 18 port names corresponding to that module are visible. The other member names (19...26) are hidden.

You can disable a switch port by setting the corresponding bit in the output tag. The output bits are applied every time the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied.

The port is enabled if the corresponding output bit is 0. If you enable or disable a port by using the Device Manager Web interface or the CLI, the port setting can be overridden by the output bits the next time they are applied. The output bits always take precedence, regardless of whether the Device Manager Web interface or CLI was used to enable or disable the port.

The following tables show input and output data types for all 26 ports of the switch, as well as port assignments for data types.

Table 28 - Input Data Types

Tag Name	Type	Description
I:Fault	DINT	If there is s communication fault between the controller and the switch, all 32 bits in the module fault word are set to 1.
I:AnyPortConnected	BOOL	Indicates that at least one port has an active link.
I:PortGi1_1Connected	BOOL	Indicates that a particular port has an active link. 0 = Link not active 1 = Link active
I:PortGi1_2Connected	BOOL	
I:PortFa1_1Connected	BOOL	
I:PortFa1_2Connected	BOOL	
I:PortFa1_3Connected	BOOL	
I:PortFa1_4Connected	BOOL	
I:PortFa1_5Connected	BOOL	
I:PortFa1_6Connected	BOOL	

Table 28 - Input Data Types (continued)

Tag Name	Type	Description
I:PortFa1_7Connected	BOOL	Indicates that a particular port has an active link. 0 = Link not active 1 = Link active
I:PortFa1_8Connected	BOOL	
I:PortFa2_1Connected	BOOL	
I:PortFa2_2Connected	BOOL	
I:PortFa2_3Connected	BOOL	
I:PortFa2_4Connected	BOOL	
I:PortFa2_5Connected	BOOL	
I:PortFa2_6Connected	BOOL	
I:PortFa2_7Connected	BOOL	
I:PortFa2_8Connected	BOOL	
I:PortFa3_1Connected	BOOL	
I:PortFa3_2Connected	BOOL	
I:PortFa3_3Connected	BOOL	
I:PortFa3_4Connected	BOOL	
I:PortFa3_5Connected	BOOL	
I:PortFa3_6Connected	BOOL	
I:PortFa3_7Connected	BOOL	
I:PortFa3_8Connected	BOOL	
I:AnyPortUnauthorizedDevice	BOOL	Indicates that an unauthorized MAC ID has attempted to communicate on any port.
I:PortGi1_1UnauthorizedDevice	BOOL	Indicates that an unauthorized MAC ID has attempted to communicate on a particular port. 0 = No mismatch 1 = Mismatch
I:PortGi1_2UnauthorizedDevice	BOOL	
I:PortFa1_1UnauthorizedDevice	BOOL	
I:PortFa1_2UnauthorizedDevice	BOOL	
I:PortFa1_3UnauthorizedDevice	BOOL	
I:PortFa1_4UnauthorizedDevice	BOOL	
I:PortFa1_5UnauthorizedDevice	BOOL	
I:PortFa1_6UnauthorizedDevice	BOOL	
I:PortFa1_7UnauthorizedDevice	BOOL	
I:PortFa1_8UnauthorizedDevice	BOOL	
I:PortFa2_1UnauthorizedDevice	BOOL	
I:PortFa2_2UnauthorizedDevice	BOOL	
I:PortFa2_3UnauthorizedDevice	BOOL	
I:PortFa2_4UnauthorizedDevice	BOOL	
I:PortFa2_5UnauthorizedDevice	BOOL	
I:PortFa2_6UnauthorizedDevice	BOOL	
I:PortFa2_7UnauthorizedDevice	BOOL	
I:PortFa2_8UnauthorizedDevice	BOOL	
I:PortFa3_1UnauthorizedDevice	BOOL	

Table 28 - Input Data Types (continued)

Tag Name	Type	Description
I:PortFa3_2UnauthorizedDevice	BOOL	Indicates that an unauthorized MAC ID has attempted to communicate on a particular port. 0 = No mismatch 1 = Mismatch
I:PortFa3_3UnauthorizedDevice	BOOL	
I:PortFa3_4UnauthorizedDevice	BOOL	
I:PortFa3_5UnauthorizedDevice	BOOL	
I:PortFa3_6UnauthorizedDevice	BOOL	
I:PortFa3_7UnauthorizedDevice	BOOL	
I:PortFa3_8UnauthorizedDevice	BOOL	
I:AnyPortThreshold	BOOL	Indicates that unicast, multicast, or broadcast threshold limit has been exceeded on any port.
I:PortGi1_1Threshold	BOOL	Indicates that unicast, multicast, or broadcast threshold limit has been exceeded on a particular port. 0 = OK 1 = Threshold exceeded
I:PortGi1_2Threshold	BOOL	
I:PortFa1_1Threshold	BOOL	
I:PortFa1_2Threshold	BOOL	
I:PortFa1_3Threshold	BOOL	
I:PortFa1_4Threshold	BOOL	
I:PortFa1_5Threshold	BOOL	
I:PortFa1_6Threshold	BOOL	
I:PortFa1_7Threshold	BOOL	
I:PortFa1_8Threshold	BOOL	
I:PortFa2_1Threshold	BOOL	
I:PortFa2_2Threshold	BOOL	
I:PortFa2_3Threshold	BOOL	
I:PortFa2_4Threshold	BOOL	
I:PortFa2_5Threshold	BOOL	
I:PortFa2_6Threshold	BOOL	
I:PortFa2_7Threshold	BOOL	
I:PortFa2_8Threshold	BOOL	
I:PortFa3_1Threshold	BOOL	
I:PortFa3_2Threshold	BOOL	
I:PortFa3_3Threshold	BOOL	
I:PortFa3_4Threshold	BOOL	
I:PortFa3_5Threshold	BOOL	
I:PortFa3_6Threshold	BOOL	
I:PortFa3_7Threshold	BOOL	
I:PortFa3_8Threshold	BOOL	
I:AllPortsUtilization	SINT	The sum of the percentage of the bandwidth utilized of all ports on the switch.
I:PortGi1_1Utilization;	SINT	The percentage of the bandwidth utilized on a particular port.
I:PortGi1_2Utilization;	SINT	
I:PortFa1_1Utilization;	SINT	

Table 28 - Input Data Types (continued)

Tag Name	Type	Description
I:PortFa1_2Utilization;	SINT	The percentage of the bandwidth utilized on a particular port.
I:PortFa1_3Utilization;	SINT	
I:PortFa1_4Utilization;	SINT	
I:PortFa1_5Utilization;	SINT	
I:PortFa1_6Utilization;	SINT	
I:PortFa1_7Utilization;	SINT	
I:PortFa1_8Utilization;	SINT	
I:PortFa2_1Utilization;	SINT	
I:PortFa2_2Utilization;	SINT	
I:PortFa2_3Utilization;	SINT	
I:PortFa2_4Utilization;	SINT	
I:PortFa2_5Utilization;	SINT	
I:PortFa2_6Utilization;	SINT	
I:PortFa2_7Utilization;	SINT	
I:PortFa2_8Utilization;	SINT	
I:PortFa3_1Utilization;	SINT	
I:PortFa3_2Utilization;	SINT	
I:PortFa3_3Utilization;	SINT	
I:PortFa3_4Utilization;	SINT	
I:PortFa3_5Utilization;	SINT	
I:PortFa3_6Utilization;	SINT	
I:PortFa3_7Utilization;	SINT	
I:PortFa3_8Utilization;	SINT	
I:MajorAlarmRelay	BOOL	Indicates whether the major alarm relay is on or off. 0 = Contact open (off) 1 = Contact closed (on)
I:MinorAlarmRelay	BOOL	Indicates whether the minor alarm relay is on or off. 0 = Contact open (off) 1 = Contact closed (on)
I:MulticastGroupsActive	DINT	The number of active multicast groups across all ports.

Table 29 - Output Data Types

Tag Name	Type	Description
O:AllPortsDisable	BOOL	Setting this bit disables all ports on the switch. 0 = Enable 1 = Disable
O:PortGi1_1Disable	BOOL	Setting a particular bit disables that particular port. 0 = Enable 1 = Disable
O:PortGi1_2Disable	BOOL	
O:PortFa1_1Disable	BOOL	
O:PortFa1_2Disable	BOOL	
O:PortFa1_3Disable	BOOL	
O:PortFa1_4Disable	BOOL	
O:PortFa1_5Disable	BOOL	
O:PortFa1_6Disable	BOOL	
O:PortFa1_7Disable	BOOL	
O:PortFa1_8Disable	BOOL	
O:PortFa2_1Disable	BOOL	
O:PortFa2_2Disable	BOOL	
O:PortFa2_3Disable	BOOL	
O:PortFa2_4Disable	BOOL	
O:PortFa2_5Disable	BOOL	
O:PortFa2_6Disable	BOOL	
O:PortFa2_7Disable	BOOL	
O:PortFa2_8Disable	BOOL	
O:PortFa3_1Disable	BOOL	
O:PortFa3_2Disable	BOOL	
O:PortFa3_3Disable	BOOL	
O:PortFa3_4Disable	BOOL	
O:PortFa3_5Disable	BOOL	
O:PortFa3_6Disable	BOOL	
O:PortFa3_7Disable	BOOL	
O:PortFa3_8Disable	BOOL	

Notes:

Port Assignments for CIP Data

This table identifies the instance numbers of the Ethernet link object associated with each port on the switch. Instance 0 does not apply to all the ports as it does for bit maps. The bit numbers identify each port when they are contained in a structure of all the ports, for example, in the output assembly. Bit 0 refers to any or all ports.

Table 30 - Port Assignments for CIP Data

Instance/Bit	6-port Managed Ethernet Switch	10-port Managed Ethernet Switch	10-port Managed Ethernet Switch	14-port Managed Ethernet Switch	14-port Managed Ethernet Switch	14-port Managed Ethernet Switch	18-port Managed Ethernet Switch
Bit 0	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports
Instance/Bit 1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1
Instance/Bit 2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2
Instance/Bit 3	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1
Instance/Bit 4	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
Instance/Bit 5	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
Instance/Bit 6	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
Instance/Bit 7		Fa1/5			Fa1/5		Fa1/5
Instance/Bit 8		Fa1/6			Fa1/6		Fa1/6
Instance/Bit 9		Fa1/7			Fa1/7		Fa1/7
Instance/Bit 10		Fa1/8			Fa1/8		Fa1/8
Instance/Bit 11			Fa2/1	Fa2/1	Fa2/1	Fa2/1	Fa2/1
Instance/Bit 12			Fa2/2	Fa2/2	Fa2/2	Fa2/2	Fa2/2
Instance/Bit 13			Fa2/3	Fa2/3	Fa2/3	Fa2/3	Fa2/3
Instance/Bit 14			Fa2/4	Fa2/4	Fa2/4	Fa2/4	Fa2/4
Instance/Bit 15				Fa2/5			Fa2/5
Instance/Bit 16				Fa2/6			Fa2/6
Instance/Bit 17				Fa2/7			Fa2/7
Instance/Bit 18				Fa2/8			Fa2/8
Instance/Bit 19						Fa3/1	
Instance/Bit 20						Fa3/2	
Instance/Bit 21						Fa3/3	
Instance/Bit 22						Fa3/4	
Instance/Bit 23							
Instance/Bit 24							
Instance/Bit 25							
Instance/Bit 26							

Table 31 - Port Assignments for CIP Data

Instance/Bit	18-port Managed Ethernet Switch	18-port Managed Ethernet Switch	18-port Managed Ethernet Switch	22-port Managed Ethernet Switch	22-port Managed Ethernet Switch	22-port Managed Ethernet Switch	26-port Managed Ethernet Switch
Bit 0	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports
Instance/Bit 1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1
Instance/Bit 2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2
Instance/Bit 3	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1
Instance/Bit 4	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
Instance/Bit 5	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
Instance/Bit 6	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
Instance/Bit 7			Fa1/5		Fa1/5	Fa1/5	Fa1/5
Instance/Bit 8			Fa1/6		Fa1/6	Fa1/6	Fa1/6
Instance/Bit 9			Fa1/7		Fa1/7	Fa1/7	Fa1/7
Instance/Bit 10			Fa1/8		Fa1/8	Fa1/8	Fa1/8
Instance/Bit 11	Fa2/1	Fa2/1	Fa2/1	Fa2/1	Fa2/1	Fa2/1	Fa2/1
Instance/Bit 12	Fa2/2	Fa2/2	Fa2/2	Fa2/2	Fa2/2	Fa2/2	Fa2/2
Instance/Bit 13	Fa2/3	Fa2/3	Fa2/3	Fa2/3	Fa2/3	Fa2/3	Fa2/3
Instance/Bit 14	Fa2/4	Fa2/4	Fa2/4	Fa2/4	Fa2/4	Fa2/4	Fa2/4
Instance/Bit 15		Fa2/5		Fa2/5	Fa2/5		Fa2/5
Instance/Bit 16		Fa2/6		Fa2/6	Fa2/6		Fa2/6
Instance/Bit 17		Fa2/7		Fa2/7	Fa2/7		Fa2/7
Instance/Bit 18		Fa2/8		Fa2/8	Fa2/8		Fa2/8
Instance/Bit 19	Fa3/1	Fa3/1	Fa3/1	Fa3/1	Fa3/1	Fa3/1	Fa3/1
Instance/Bit 20	Fa3/2	Fa3/2	Fa3/2	Fa3/2	Fa3/2	Fa3/2	Fa3/2
Instance/Bit 21	Fa3/3	Fa3/3	Fa3/3	Fa3/3	Fa3/3	Fa3/3	Fa3/3
Instance/Bit 22	Fa3/4	Fa3/4	Fa3/4	Fa3/4	Fa3/4	Fa3/4	Fa3/4
Instance/Bit 23	Fa3/5			Fa3/5		Fa3/5	Fa3/5
Instance/Bit 24	Fa3/6			Fa3/6		Fa3/6	Fa3/6
Instance/Bit 25	Fa3/7			Fa3/7		Fa3/7	Fa3/7
Instance/Bit 26	Fa3/8			Fa3/8		Fa3/8	Fa3/8

Cables and Connectors

10/100 and 10/100/1000 Ports

The 10/100 and 10/100/1000 Ethernet ports on switches use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

TIP The auto-MDIX feature is enabled by default.

Figure 15 - 10/100 Connector Pinouts

Pin	Label
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

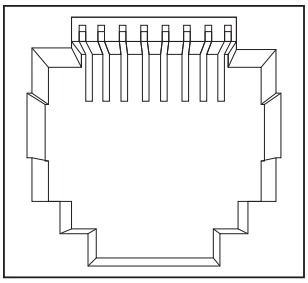
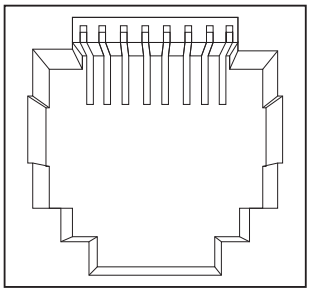


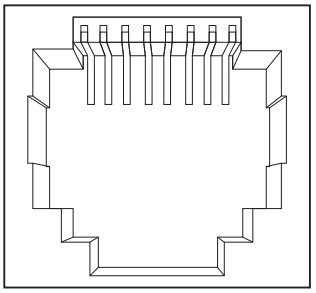
Figure 16 - 10/100/1000 Connector Pinouts

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



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

Figure 17 - 10/100 PoE Connector Pinouts and Power Sourcing Equipment (PSE) Voltage

Pin	Label	Alternative A (MDI)	1 2 3 4 5 6 7 8
1	RD+	Positive V PSE	
2	RD-	Positive V PSE	
3	TD+	Negative V PSE	
4	NC		
5	NC		
6	TD-	Negative V PSE	
7	NC		
8	NC		

Connect to 10BASE-T- and 100BASE-TX-compatible Devices

When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as servers, workstations, and routers, you can use a two or four twisted-pair, straight-through cable wired for 10BASE-T and 100BASE-TX.

To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side-by-side, with the tab at the back. The wire connected to the pin on the outside of the left plug must be a different color from the wire connected to the pin on the inside of the right plug.

The following figures show these schematics:

- Two twisted-pair, straight-through cable
- Four twisted-pair, straight-through cable

Figure 18 - Two Twisted-pair Straight-through Cable Schematic

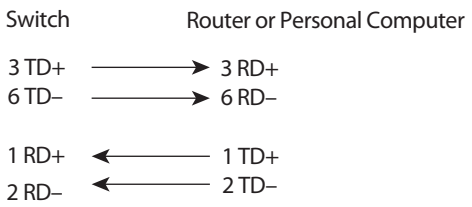
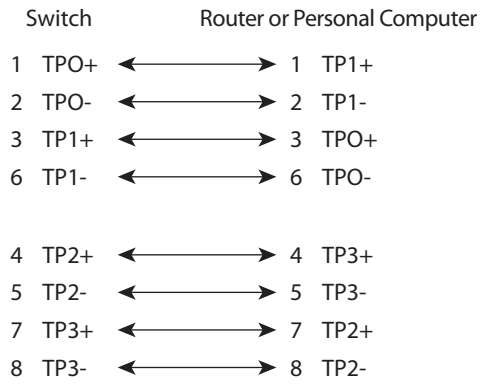


Figure 19 - Four Twisted-pair Straight-through Cable Schematic



When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable.

The following figures show these schematics:

- Two twisted-pair, crossover cable schematics
- Four twisted-pair, crossover cable schematics

Use a straight-through cable to connect two ports only when one port is designated with an X. Use a crossover cable to connect two ports when both ports are designated with an X or when both ports do not have an X.

You can use Category 3, 4, or 5 cabling when connecting to 10BASE-T-compatible devices. You must use Category 5 cabling when connecting to 100BASE-TX-compatible devices.

IMPORTANT Use a four twisted-pair, Category 5 cable when connecting to a 1000BASE-T-compatible device or PoE port.

Figure 20 - Two Twisted-pair Crossover Cable Schematic

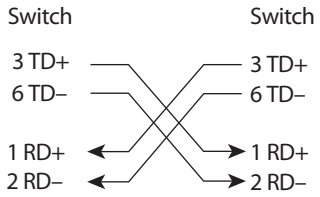
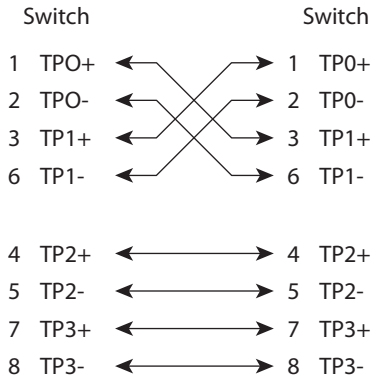


Figure 21 - Four Twisted-pair Crossover Cable Schematic

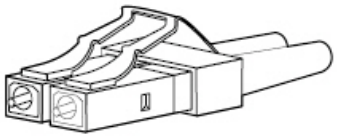


100BASE-FX Ports

The 100BASE-FX ports use the following:

- LC connectors, as shown in the following figure
- 50/125- or 62.5/125-micron multimode fiber-optic cables

Figure 22 - Fiber-optic SFP Module LC Connector



ATTENTION: Invisible laser radiation can be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

SFP Transceiver Ports

The switch uses SFP transceivers for fiber-optic uplink ports.

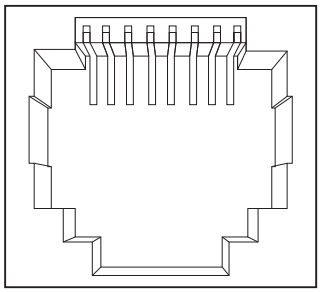
ATTENTION: Invisible laser radiation can be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

Dual-purpose Ports

The Ethernet port on a dual-purpose port uses standard RJ45 connectors. The following figure shows the pinouts.

Figure 23 - Ethernet Port RJ45 Connector

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



The SFP module slot on a dual-purpose port uses SFP modules for fiber-optic ports.

IMPORTANT The auto-MDIX feature is enabled by default. For configuration information for this feature, see the switch software configuration guide or the switch command reference.

Console Port

The console port uses an 8-pin RJ45 connector. The supplied RJ45-to-DB-9 adapter cable is used to connect the console port of the switch to a console personal computer. You need to provide an RJ45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal.

Cable and Adapter Specifications

These sections describe the cables and adapters used with the switches.

SFP Module Cable Specifications

The following lists the cable specifications for the rugged fiber-optic SFP module connections. Each port must match the wave-length specifications on the other end of the cable, and for reliable communication, the cable must not exceed the rated maximum cable length.

Table 32 - Fiber-optic SFP Module Port Cabling Specifications

SFP Module Type	Cat. No.	Wavelength (nm)	Fiber Type	Core Size/Cladding Size (micron)	Modal Bandwidth (MHz/km)(1)	Cable Distance
100BASE-FX	1783-SFP100FX	1310	MMF	50/125 62.5/125	500 500	2 km (6562 ft) 2 km (6562 ft)
100BASE-LX	1783-SFP100LX	1310	SMF	G.652[2]	—	10 km (32,810 ft)
1000BASE-SX	1783-SFP1GSX	850	MMF	62.5/125 62.5/125 50/125 50/125	160 200 400 500	220 m (722 ft) 275 m (902 ft)) 500 m (1640 ft) 550 m (1804 ft)
1000BASE-LX/LH	1783-SFP1GLX	1310	SMF	G.652[2]	—	10 km (32,810 ft)

(1) Modal bandwidth applies only to Multi-mode fiber.

PoE Port Cable Specifications

For PoE ports, use a Category 5 (Cat 5) cable with a distance of up to 100 m (328 ft).

Adapter Pinouts

The following table lists the pinouts for the console port, the RJ45-to-DB-9 adapter cable, and the console device.

Table 33 - Pinouts with CB-9 Pin

Switch Console Port (DTE)	RJ45-to-DB-9 Terminal Adapter	Console Device
Signal	**DB-9 Pin**	**Signal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

The following table lists the pinouts for the console port, RJ45-to-DB-25 female DTE adapter, and the console device.

The RJ45-to-DB-25 female DTE adapter is not supplied with the switch.

Table 34 - Pinouts with DB-25 Pin

Switch Console Port (DTE)	RJ45-to-DB-25 Terminal Adapter	Console Device
Signal	**DB-25 Pin**	**Signal**
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

Notes:

History of Changes

This appendix summarizes the revisions to this manual. Reference this appendix if you need information to determine what changes have been made across multiple revisions. This can be especially useful if you are deciding to upgrade your hardware or software based on information added with previous revisions of this manual.

1783-UM003H-EN-P, September 2013

Change
Studio 5000 Logix Designer application is the rebranding of RSLogix 5000 software
Product release notes
Switch installation chapter
SFP and PoE expansion module front panel descriptions
PoE port descriptions
PoE feature descriptions
PoE port configuration via the Device Manager Web interface
Status indicators
Port assignments for CIP data
PoE port connector pinouts and cable specifications
History of changes

1783-UM003G-EN-P, December 2012

Change
Express Setup
Switch memory allocation
Operating system requirements
Multicast groups
New MIBs
Static routing
Cryptographic IOS software
Forward synchronization clock mode
Select Module Type dialog box

1783-UM003F-EN-P, August 2011

Change
New Smartports roles
New MIBs
Cryptographic IOS software
Cable Diagnostics feature
QuickConnect systems
Port Status dialog box
Cable Diagnostics dialog box
Time Sync Configuration and Time Sync Information dialog boxes

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at https://rockwellautomation.custhelp.com/ for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/services/online-phone.

Installation Assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/rockwellautomation/support/overview.page, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to help ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

Rockwell Automation maintains current product environmental information on its website at http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-UM003I-EN-P - March 2014

Supersedes Publication 1783-UM003H-EN-P - September 2013