

Cisco IE3500 Heavy Duty Series Switches Hardware Installation Guide

First Published: 2025-10-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface vii

Audience vii

Purpose vii

Conventions vii

Related Publications viii

Communications, Services, and Additional Information viii

CHAPTER 1

Overview 1

Switch Models 1

Front Panel of the Switch 3

Ethernet Ports 4

Power Connector 5

Alarm Connector 5

Console Management Port 6

LEDs 6

System LED 7

Express Setup LED 7

Power status LEDs 7

Alarm LEDs 8

Port status LEDs 8

Power over Ethernet status LEDs 9

CHAPTER 2

Switch Installation 11

Preparing for Installation 11

Warnings 11

EMC Environmental Conditions for Products Installed in the European Union 13

Installation Guidelines 13
Environment and Enclosure Guidelines 13
General Guidelines 14
Verifying Package Contents 15
Tools and Equipment 15
Mounting the Switch 15
Installing the Switch on the Wall 16
Installing or Removing the Memory Card (Optional) 18
Connecting a PC or Terminal to the Console Port 19
Connecting a Fiber-optic Cable Gland(CW-SFP-KIT1) 19
Connecting to Power 23
Grounding the Switch 23
Connecting the earth ground wire 25
Connecting Alarm Circuits 25
Wiring the External Alarms 25
Connecting Destination Ports 26
Connecting to 10/100 and 10/100/1G/2.5G Ports 26
Where to Go Next 27

CHAPTER 3 **Express Setup 29**
Required Equipment 29
Run Express Setup 29

CHAPTER 4 **Configuring the switch with the CLI setup program 35**
IP and Password Settings 35
Initial Configuration 35
Configure System Security 39

CHAPTER 5 **Troubleshooting 41**
Diagnosing Problems 41
Switch Connections 41
Bad or Damaged Cable 41
Link Status 41
10/100, 1G, 2.5G, 10G Port Connections 42

Interface Settings 42
Ping End Device 42
Switch Performance 42
Speed, Duplex, and Autonegotiation 42
Autonegotiation and Network Interface Cards 43
Cabling Distance 43
Reset the Switch 43
How to Recover Passwords 43
Troubleshooting Express Setup 44
Finding the Switch Serial Number 44

CHAPTER 6 **Technical Specifications** 45
Operating Temperature Specifications 45
Technical Specifications 46
Connectors and Cabling 46
Torque Specifications 47
Alarm Ratings 48

Preface

Audience

This guide is for the networking or computer technician responsible for installing Cisco IE3500 Heavy Duty Series Switches. We assume that you are familiar with the concepts and terminology of local area networking (LAN).

Purpose

This guide describes the physical and performance characteristics of the switch, explains how to install a switch, and provides troubleshooting information.

Conventions

This document uses the following conventions and symbols for notes, cautions, and warnings.



Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.



Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.



Warning **Statement 1071—**Warning Definition

IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number at the beginning of each warning statement to locate its translation in the translated safety warnings for this device.

SAVE THESE INSTRUCTIONS



The safety warnings for this product are translated into several languages in the *Regulatory Compliance and Safety Information for the Cisco Catalyst IE3500 Heavy Duty Series Switches*, which is published on Cisco.com. The EMC regulatory statements are also included in this guide.

Related Publications

All user documentation for Cisco IE3500 Heavy Duty Series Switches is available at:

https://www.cisco.com/c/en/us/support/switches/ie3500-heavy-duty-series/series.html

- Datasheet

  https://www.cisco.com/c/en/us/products/collateral/networking/industrial-switches/ie3500-heavy-duty-series/ie3500-heavy-duty-series-ds.html

- Regulatory Compliance and Safety Information

  https://www.cisco.com/c/dam/en/us/td/docs/IIOT/compliance/switches/rcsi-0491-book.pdf

- Configuration Guide

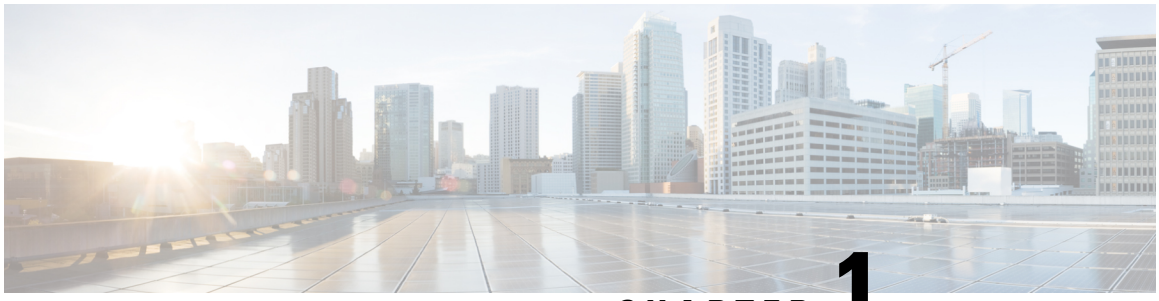
  https://www.cisco.com/c/en/us/support/switches/ie3500-heavy-duty-series/series.html#Configuration

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

Overview

Cisco IE3500 Heavy Duty Series Switches are the next generation IP66, IP67-rated Industrial Ethernet switches. They bring robust capabilities to demanding IoT environments such as manufacturing, connected energy, and smart cities. These devices are engineered for harsh conditions, featuring IP67 ingress protection, Power over Ethernet (PoE) capabilities, and durable circular connectors.

A key highlight of the Cisco IE3500H family is its diverse port configurations, offering a comprehensive mix of Fast Ethernet (D-coded), Gigabit Ethernet (X-coded), 2.5GE, 10GE M12 ports. The switches can be wall mounted and deployed without a housing cabinet to meet varied industrial networking requirements.

The Cisco IE3500H series switches can be managed with powerful tools such as Cisco IOS-XE software, Cisco Catalyst Center, and can be easily set up with an on-device modern GUI tool called WebUI. The platform also supports Flexible NetFlow for real-time visibility into traffic patterns and threat analysis.

- Switch Models, on page 1
- Front Panel of the Switch, on page 3
- LEDs, on page 6

Switch Models

Figure 1: Cisco IE3500H Series Switches



	License Level	Description
IE-3500H-8T-E	Network Essentials	8x 10/100/1G X-code M12 ports, non-PoE

	License Level	Description
IE-3500H-16T-E	Network Essentials	16x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-24T-E	Network Essentials	24x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-12FT4T-E	Network Essentials	12x 10/100 D-code M12 ports, 4x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-20FT4T-E	Network Essentials	20x 10/100 D-code M12 ports, 4x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-14P2T-E	Network Essentials	14x 10/100/1G X-code PoE/PoE+ ports, 2x 10/100/1G X-Code M12 ports, PoE power budget of 240 W
IE-3500H-12P2MU2X-E	Network Essentials	2x 10G SFP+ ports, 2x 100/1G/2.5G UPoE X-code ports, 12x 10/100/1G M12 X-code ports, PoE power budget of 240 W
IE-3505H-16T-E	Network Essentials	16x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-8T-A	Network Advantage	8x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-16T-A	Network Advantage	16x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-24T-A	Network Advantage	24x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-12FT4T-A	Network Advantage	12x 10/100 D-code M12 ports, 4x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-20FT4T-A	Network Advantage	20x 10/100 D-code M12 ports, 4x 10/100/1G X-code M12 ports, non-PoE
IE-3500H-14P2T-A	Network Advantage	14x 10/100/1G X-code PoE/PoE+ ports, 2x 10/100/1G X-Code M12 ports, PoE power budget of 240 W
IE-3500H-12P2MU2X-A	Network Advantage	2x 10G SFP+ ports, 2x 100/1G/2.5G UPoE X-code ports, 12x 10/100/1G M12 X-code ports, PoE power budget of 240 W
IE-3505H-16T-A	Network Advantage	16x 10/100/1G X-code M12 ports, non-PoE

Table 1: Hardware Specifications

Specifications	All PIDs
Removable storage	SD card[1]
Alarm[2,3]	1 alarm output relay 1 alarm input relay

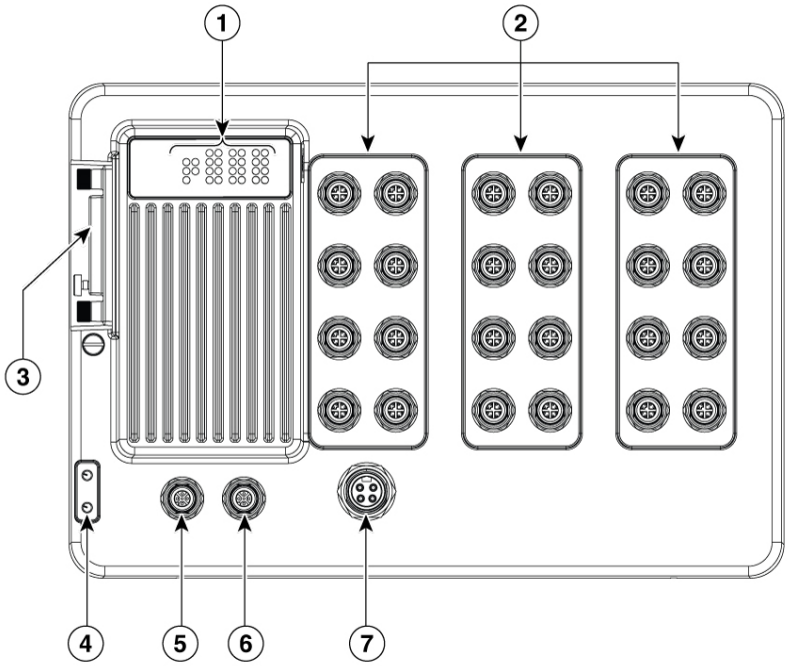
Specifications	All PIDs
Console port[2]	1

1. The SD card is optional and is not shipped by default with the switch.
2. Using an M12 A-coded 5-pin connector.
3. Relay max. rating: 24Vdc at 1A, 48Vdc at 0.5A.

Front Panel of the Switch

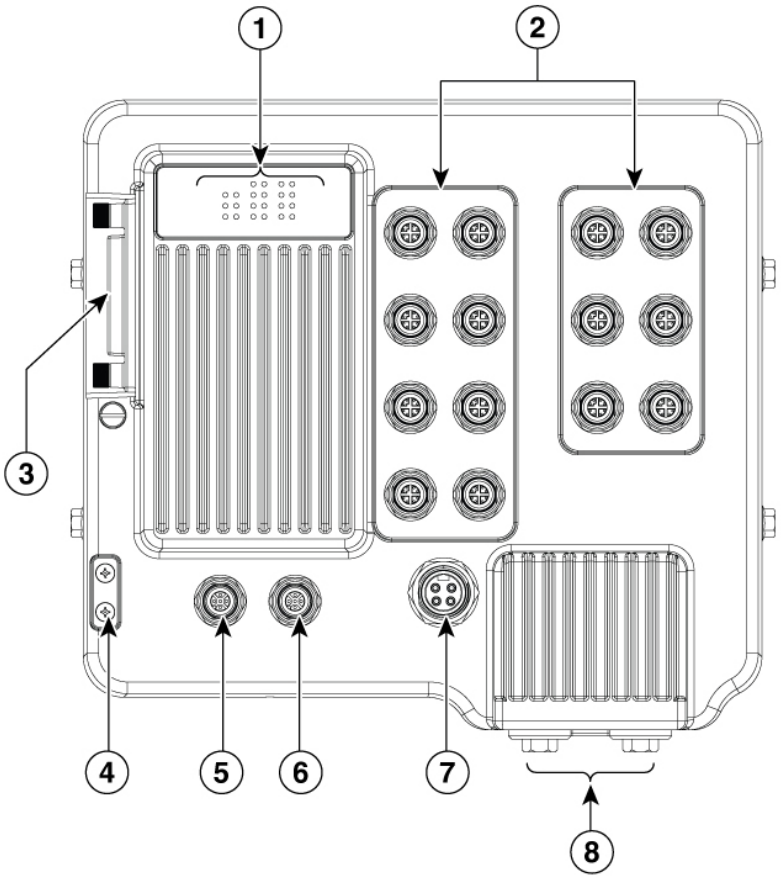
This section describes the front panel components. The following figures depict the components available on the various models in this product family. Not all models are illustrated.

Figure 2: Cisco IE3500H front panel



1	Switch status LEDs	5	Console port
2	Ethernet ports	6	Alarm port
3	SD card cover	7	Power input Port
4	Ground lug		

Figure 3: Cisco IE3500H SFP model front panel

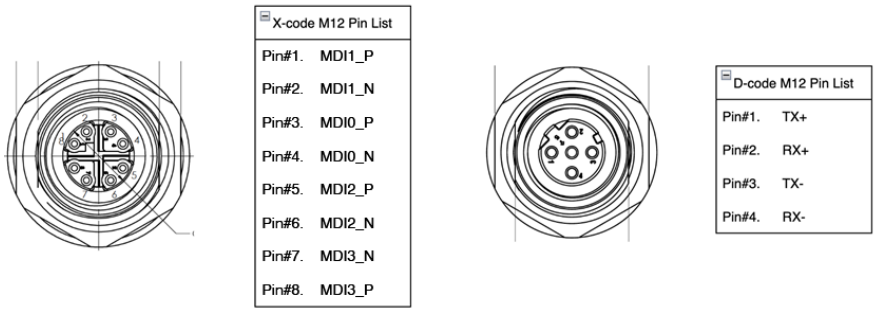


1	Switch status LEDs	5	Console port
2	Ethernet ports	6	Alarm port
3	SD card cover SFP ports	7	Power input port
4	Ground lug	8	2x SFP ports

Ethernet Ports

The Cisco IE3500H series switches have Ethernet ports supporting 1000Base-T, 100Base-TX and 10Base-T with autonegotiation, auto-MDIX, and cable diagnostics on X-code M12 connectors.

Figure 4: M12 Ethernet Ports



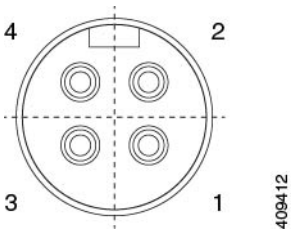
1	RD +	3	RD –
2	TD +	4	TD –

Power Connector

Power the switch using DC power through the front panel connector. The power connector labeling is on the panel. Torque power connection to 10in/lbs.

A Mini-Change (A-size) Single-Ended cord set power cord must be used to power the switch.

Figure 5: Power Connector



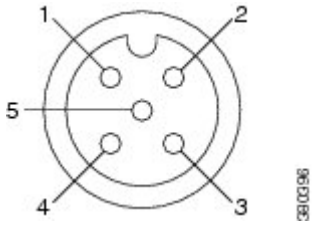
1	NC	3	DC–
2	DC+	4	NC

Alarm Connector

Connect the alarm signals to the switch through the alarm connector. The switch supports one alarm output relay.

The alarm output circuit is a relay with a normally open and a normally closed contact. The switch is configured to detect faults that are used to energize the relay coil and change the state on both of the relay contacts: normally open contacts close, and normally closed contacts open. The alarm output relay can be used to control an external alarm device, such as a bell or a light. The alarm output is rated at 24Vdc/1A, 48Vdc/0.5A maximum.

Figure 6: Alarm Connector



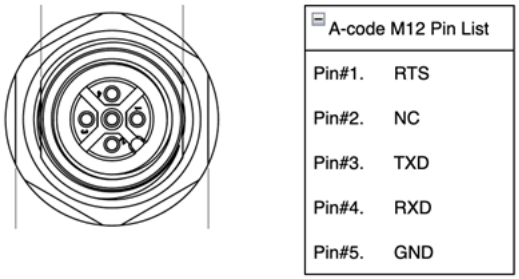
1	NO Alarm Output Normally Open (NO) connection	4	Alarm In Reference
2	NC Alarm Output Normally Closed (NC) connection	5	COMMON Alarm Common connection
3	Alarm In		

Console Management Port

Connect the switch to a PC running Microsoft Windows or to a terminal server through the A-code M12 connector console port and configure it by using the CLI. The baud rate and format of the console port is:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Figure 7: Console Connector

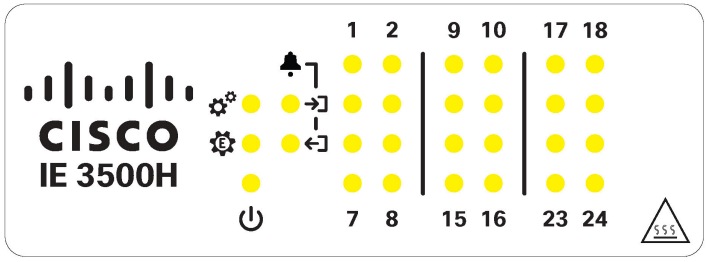


Note For specified cable, use Cisco Product CAB-CONSOLE-M12=

LEDs

Use the LEDs to monitor overall system status and power supply input and output status as well as port and alarm status.

Figure 8: Switch LEDs



System LED

The system LED shows whether the device is receiving power and is functioning properly.

Table 2: System LED

Color	Status
Off	Switch is not powered on.
Blinking green	Power-On Self Test (POST) is in progress.
Green	Switch is operating normally.
Red	Switch is receiving power, however not functioning properly.

Express Setup LED

The Express Setup LED displays the status of the initial setup for the initial configuration.

Table 3: Express Setup LED Status

Color	Status
Off	Configured as a managed switch.
Solid Green	System is operating normally.
Blinking Green	Performing the initial setup, in recovery, or the initial setup is incomplete.
Solid Red	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 then press the Express Setup button.

Power status LEDs

The power LED shows the device power status.

Table 4: Power Status LEDs

Color	System Status
Green	Power is present on the associated circuit.
Off	Power is not present on the circuit or the system is not powered up.

Alarm LEDs

The following table list the alarm LED colors and their meanings.

Table 5: Alarm Out Status LEDs

Color	System Status
Off	Alarm out is not configured or the Switch is off.
Green	Alarm out is configured, no alarms detected.
Blinking red	Major alarm detected.
Red	Minor alarm detected.

Port status LEDs

Each 10/100, 1G, 2.5G, 10G port (identified by numbers, depending upon the model) has a port status LED.

Table 6: Port status LEDs

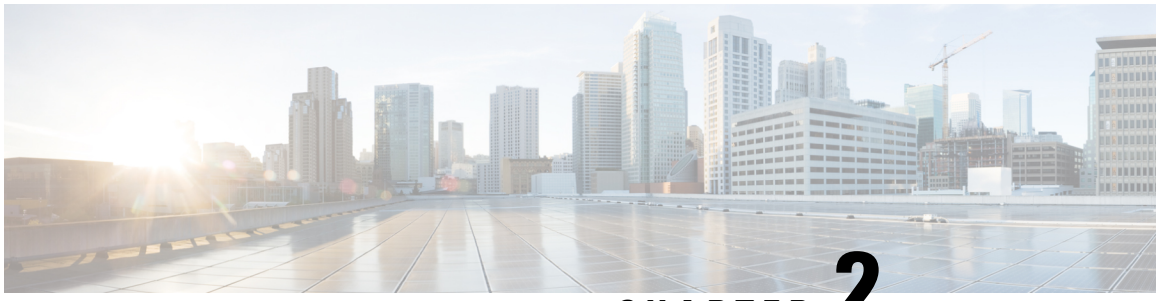
Color	Status
Off	No link, or port administratively shut down, or port is in Error disable state
Solid green	Link present, no activity
Blinking green	Activity. Port is sending or receiving data
Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
Solid amber	Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data. After a port is reconfigured, the port LED can be amber for up to 30 seconds as STP checks the switch for possible loops.
Blinking amber	System is sending Spanning Tree BPDUs on an STP blocked port (Best Effort)

Power over Ethernet status LEDs

The PoE status LED indicates the current operational state of the PoE feature.

Table 7: PoE status LEDs

Color	Status
Off	PoE is not enabled
Solid green	PoE function is enabled, and all of the PoE-enabled ports are functioning correctly
Blinking red	PoE function is enabled, but one of the PoE port's power is disconnected or has failed
Solid red	PoE function is enabled, but all of the PoE ports have failed



CHAPTER 2

Switch Installation

This chapter describes how to install your switch and connect the switch to other devices. It also includes information specifically for installations in hazardous environments.

We recommend performing a preliminary configuration of the switch before it is installed in a permanent location.

- Preparing for Installation, on page 11
- Mounting the Switch, on page 15
- Installing or Removing the Memory Card (Optional), on page 18
- Connecting a PC or Terminal to the Console Port, on page 19
- Connecting a Fiber-optic Cable Gland(CW-SFP-KIT1), on page 19
- Connecting to Power, on page 23
- Connecting Alarm Circuits, on page 25
- Connecting Destination Ports, on page 26
- Where to Go Next, on page 27

Preparing for Installation

Warnings

These warnings are translated into several languages in the Regulatory Compliance and Safety Information for this switch.

Warning

Statement 1003—DC Power Disconnection

To reduce risk of electric shock or personal injury, disconnect DC power before removing or replacing components or performing upgrades.

Warning

Statement 1017—Restricted Area

This unit is intended for installation in restricted access areas. Only skilled, instructed, or qualified personnel can access a restricted access area.

Warning **Statement 1024—**Ground Conductor

This equipment must be grounded. To reduce the risk of electric shock, never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Warning **Statement 1033—**Safety Extra-Low Voltage (SELV)—IEC 60950/ES1–IEC 62368 DC Power Supply

To reduce the risk of electric shock, connect the unit *only* to a DC power source that complies with the SELV requirements in the IEC 60950-based safety standards or the ES1 requirements in the IEC 62368-based safety standards.

Warning **Statement 1074—**Comply with Local and National Electrical Codes

To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

Warning **Statement 1079—**Hot Surface

This icon is a hot surface warning. To avoid personal injury, do not touch without proper protection.



Note **Statement 1089—**Instructed and Skilled Person Definitions

An instructed person is someone who has been instructed and trained by a skilled person and takes the necessary precautions when working with equipment.

A skilled person or qualified personnel is someone who has training or experience in the equipment technology and understands potential hazards when working with equipment.

Warning **Statement 1091—**Installation by an Instructed Person or Skilled Person

Only an instructed person or skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of an instructed person or skilled person.

Warning **Statement 9001—**Product Disposal

Ultimate disposal of this product should be handled according to all national laws and regulations.

Caution Airflow around the switch must be unrestricted. To prevent the switch from overheating, there must be the following minimum clearances:– Top and bottom: 1.0 in. (25 mm)– Sides: 1.0 in. (25 mm)– Front: 1.0 in. (25 mm)

Caution If the installer is providing cabling for an IP66/IP67 and Type 4X rated environment, the cables must be suitably rated for IP66/IP67 and Type 4X requirements

EMC Environmental Conditions for Products Installed in the European Union

This section applies to products to be installed in the European Union.

The equipment is intended to operate under the following environmental conditions with respect to EMC:

- A separate defined location under the user's control.
- Earthing and bonding shall meet the requirements of ETS 300 253 or CCITT K27.
- AC-power distribution shall be one of the following types, where applicable: TN-S and TN-C as defined in IEC 364-3.

Note When used with an AC power supply.

In addition, if equipment is operated in a domestic environment, interference could occur.

Installation Guidelines

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

Environment and Enclosure Guidelines

Review these environmental and enclosure guidelines before installation:

- This equipment is considered Group 1, Class A industrial equipment, according to IEC/CISPR Publication 11. Without appropriate precautions, there may be potential difficulties ensuring electromagnetic compatibility in other environments due to conducted as well as radiated disturbance.

Caution To meet IP67 Compliance, all cables, dust caps, or the captive screws on the SD card cover must be torqued to the recommended spec before operating the unit.

Caution Use caution when removing dust caps. Dust caps in an over-tightened state may adhere to the connector O-ring seal. Ensure that the O-ring remains in place when dust caps are removed and follow all torque specifications from Torque Specifications, on page 47.

General Guidelines

Before installation, observe these general guidelines:

Caution Proper ESD protection is required whenever you handle Cisco equipment. Installation and maintenance personnel should be properly grounded by using ground straps to eliminate the risk of ESD damage to the switch. Do not touch connectors or pins on component boards. Do not touch circuit components inside the switch. When not in use, store the equipment in appropriate static-safe packaging.

- If you are responsible for the application of safety-related programmable electronic systems (PES), you need to be aware of the safety requirements in the application of the system and be trained in using the system.

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

- Before installing the switch, first verify that the switch is operational by powering it on and observing boot fast.
- For 10/100 ports and 10/100/1000/2500 ports, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).

  The 10GE SFP+ transceiver module determines the supported maximum cable length for 10G ports.
- Operating environment is within the ranges listed in Technical Specifications, on page 46.
- Clearance to front and rear panels meets these conditions:
  - Front-panel LEDs can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Front-panel direct current (DC) power connectors and the alarm connector are within reach of the connection to the DC power source.
- Airflow around the switch must be unrestricted. To prevent the switch from overheating, you must have the following minimum clearances:
  - Top and bottom: 1.0 in. (25 mm)
  - Sides: 1.0 in. (25 mm)
  - Front: 1.0 in. (25 mm)
- Ambient temperature does not exceed 140°F (60°C).
- For optimal signal integrity, you must adjust the distance between cables and electrical noise sources (such as radios, power lines, and fluorescent lighting) based on the magnitude of the noise.

Verifying Package Contents

The box contains the following items.

- The Cisco switch with a pre-installed mounting bracket
- Pointer card

Tools and Equipment

Obtain these necessary tools and equipment:

- A single or a pair of stud-size 6 ring terminals (Hollingsworth part number R3456B or equivalent) for use as a protective ground connector.
- Crimping tool (Thomas & Bett part number WT2000, ERG-2001 or equivalent).
- 6 AWG copper ground wire.
- UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire for DC power connections.
- Wire-stripping tool for stripping wires.
- Screws to mount the switch. (Not supplied.)

Note The screw type and size depend on the mounting material and building codes.

- Number-2 Phillips screwdriver.
- Flat-blade screwdriver.
- 15mm 12-point socket for IP67 dust caps
- Torque Driver (Such as a Torqueleader TT500 or equivalent)

Mounting the Switch

Caution To prevent the switch from overheating, ensure these minimum clearances:– Top and bottom: 1.0 in. (25 mm)– Exposed side (not connected to the module): 1.0 in. (25 mm) – Front: 1.0 in. (25 mm)

Installing the Switch on the Wall

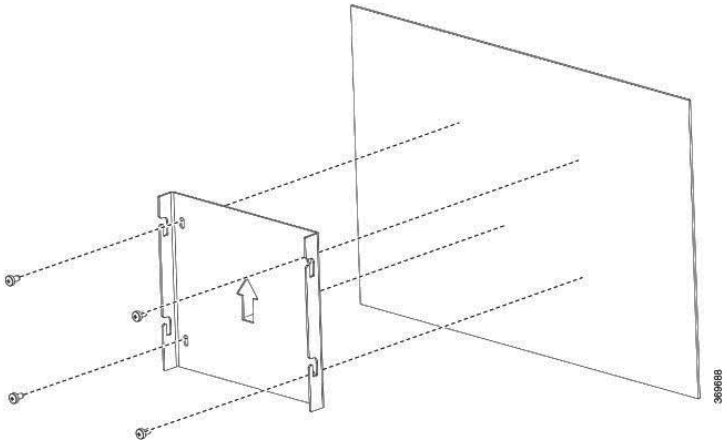
Warning **Statement 1094—**Read Wall-Mounting Instructions Before Installation

Read the wall-mounting instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system.

Procedure

Step 1 Position the switch mounting bracket against the wall or a panel in the desired location, with the arrow pointing up. See the following figure. Attach the bracket to the wall with the 4 enclosed Phillips screws.

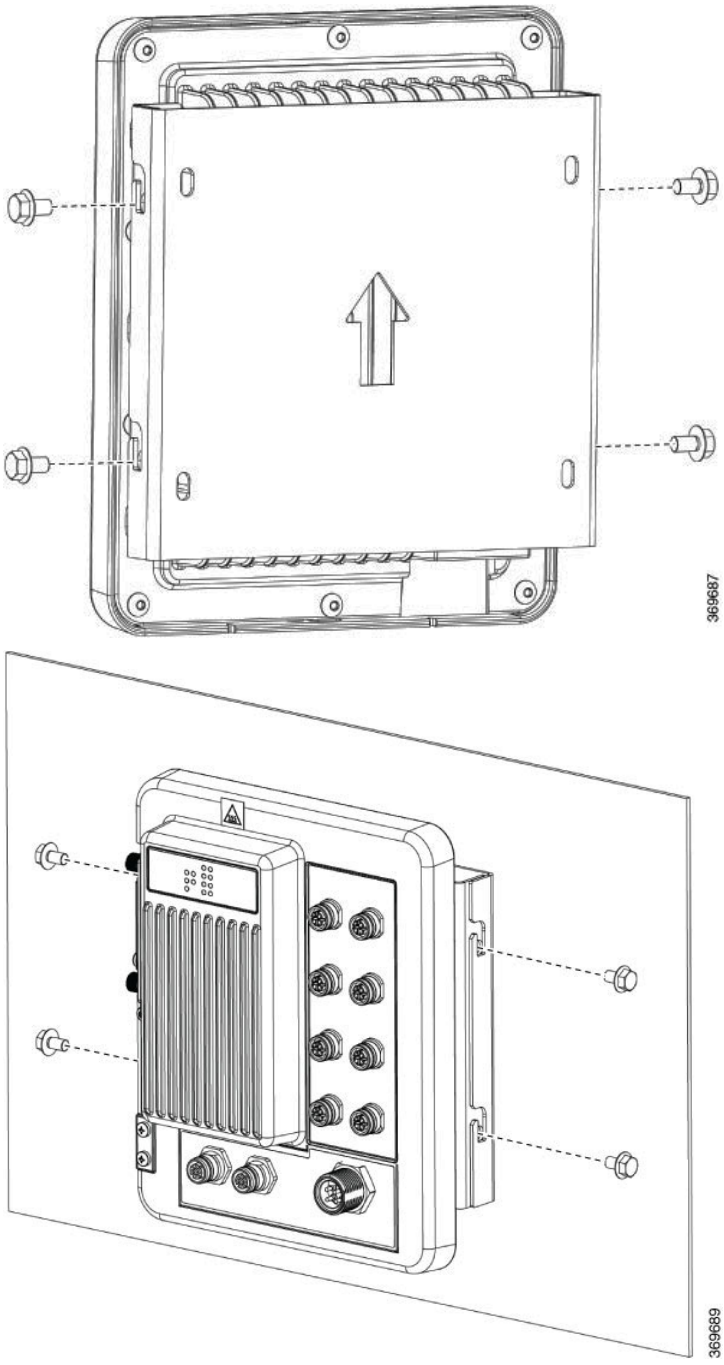
Figure 9: Mounting Wall Bracket to Wall



Note
When attaching the bracket to the wall or panel, ensure that the screws engage a stud or support structure capable of supporting the weight of the bracket and the switch.

Step 2 Loosely attach the 4 mounting screws to the switch and slide it into the bracket and down. See the following figure.

Figure 10: Attaching the Switch to the Mounting Bracket



Step 3 To remove the switch, loosen the 4 mounting screws and slide the switch up and forward, out of the mounting bracket. Then the bracket itself can be unscrewed from the wall, if necessary.

What to do next

After the switch is mounted on the wall or panel, connect the power and alarm wires, as described in the Connecting Alarm Circuits, on page 25.

Installing or Removing the Memory Card (Optional)

The switch supports a hot-swappable SD memory card. The firmware and startup configuration are stored on the card, which makes it possible to replace a failed switch without reconfiguring the replacement.

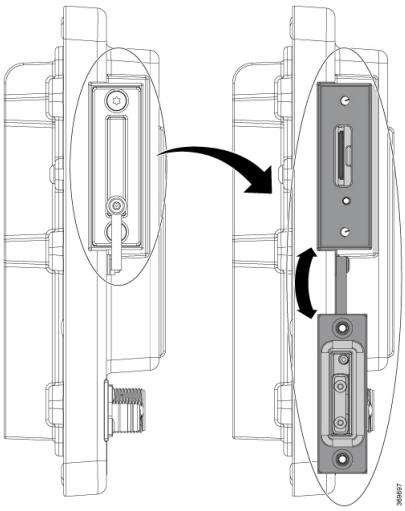
The SD memory card cover protects the flash card against shock and vibration by holding the card in place. The cover is attached with a lanyard and secured with captive screws. The slot for the SD memory card is on the side of the switch.

Note The switch supports SD memory cards up to 16 GB in capacity.

To install or replace the SD memory card, follow these steps:

Procedure

Step 1 On the side of the switch, loosen the captive screws until they are free of the chassis. See the figure.



Step 2 Install or remove the card:

- To remove the card, push it in until it releases and it pops out. Then, place it in an anti-static bag to protect it from static discharge.
- To install a card, slide it into the slot and press on it until it clicks in place. The card is keyed so it can only be inserted in the correct orientation.

Step 3 Close the guard door and fasten the captive screws to 16.0 to 19.5 in/lbs (1.8 -2.2Nm) to maintain IP67 compliance.

Connecting a PC or Terminal to the Console Port

To configure the device, you can connect a PC or terminal to the console port and enter Cisco IOS-XE commands through the CLI. This section describes the procedure for connecting a PC to the console port and using a terminal emulator application, such as PuTTY or HyperTerminal, to configure the device.

Procedure

Step 1 Connect the console cable (Cisco PID CAB-CONSOLE-M12=) to a 9-pin serial port on a PC. Connect the other end of the cable to the switch console port.

Step 2 Start a terminal-emulation program on the PC or the terminal. The program (such as PuTTY or HyperTerminal) enables communication between the switch and your PC or terminal..

Step 3 Configure the baud rate and character format of the PC or terminal to match the console port characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 4 Connect power to the switch.

Step 5 The PC or terminal shows the status of the bootup sequence. The switch will automatically boot. When the IOS XE software has completed the bootup process the words "Press RETURN to get started!".

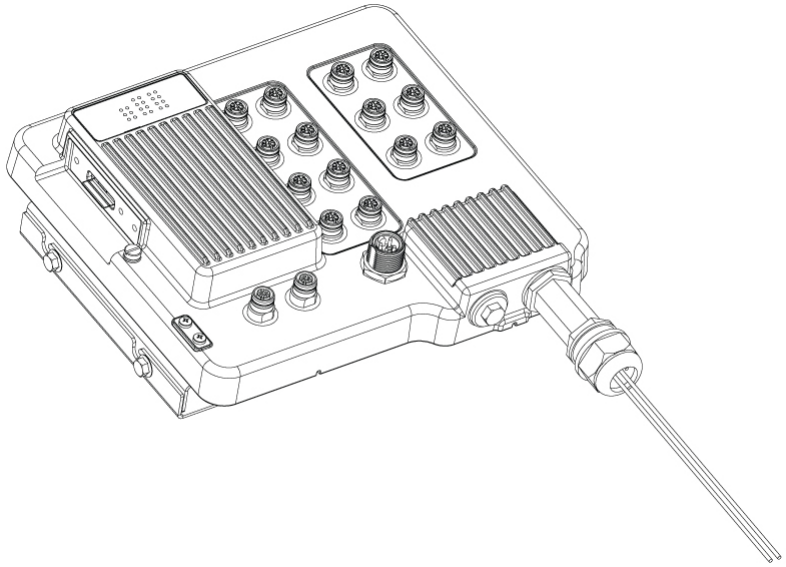
Note
If you plan to use the Plug N Play (PnP) agent for automating day 1 install, then do not press return. this stops the automated install of PnP. Press return only to use the CLI to complete the Day 1 install process.

Connecting a Fiber-optic Cable Gland(CW-SFP-KIT1)

The optional Cisco accessory fiber-optic kit enables the switch to support fiber-optic network connections.

You can connect the fiber-optic networking cable to the SFP port. The small form-factor pluggable (SFP) transceiver module connects the cable to the SFP port.

Figure 11: Fiber-Optic cable and gland installed on the switch



Before you begin

You require the following materials for connecting the fiber-optic cable gland to the switch:

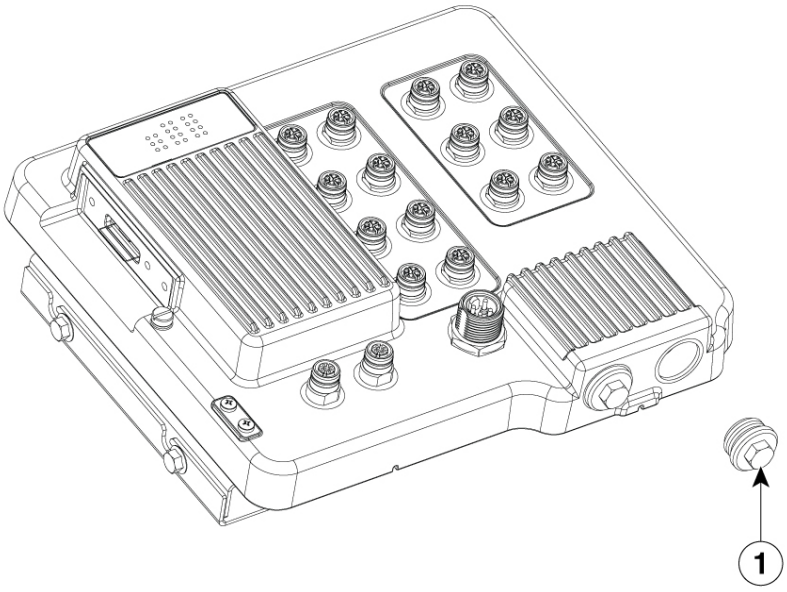
- Cisco Small form-factor pluggable (SFP) adapter kit
- SFP transceiver module
- SC or Duplex LC fiber-optic cables. The fiber optic cable's outer diameter should be 0.24 to 0.50 inch (6 to 12.7 mm). The cable gland cannot hold a cable with a diameter more than 0.50" (12.7 mm)
- 12–mm wrench or large flat blade or Philips screwdriver
- Adjustable wrench

Procedure

Step 1 Disconnect all power sources from the switch.

Step 2 Remove the plug from the SFP port by following the guidelines given in this step.

Figure 12: Removing the SFP port plug



1	SFP Port Plug

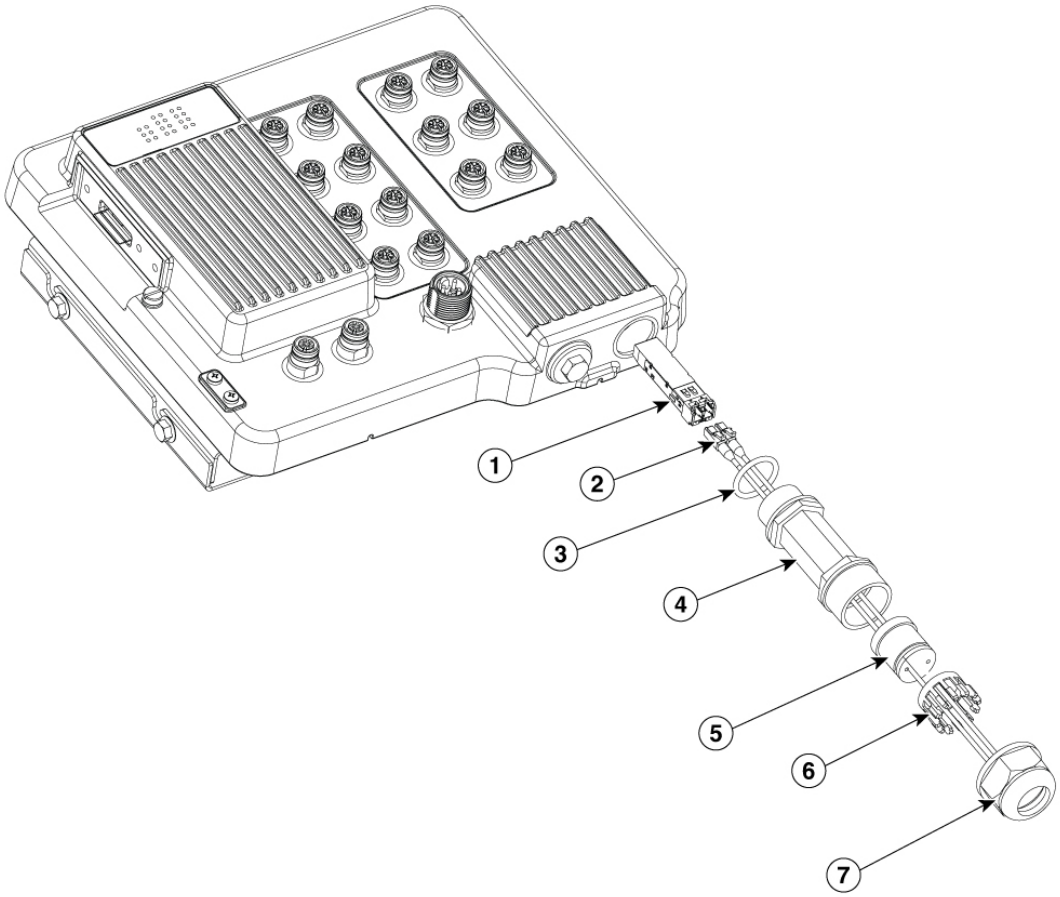
Do not discard the plug unless you are sure the SFP port will never need to be sealed in the future.

a) Place the switch on its back on a stable but padded surface to avoid scratching the paint.
b) Using a 12-mm wrench or large flat blade, or Philips screwdriver, turn the SFP port plug counterclockwise and remove it.

Step 3 Insert the SFP module into the SFP port and ensure that it latches properly.

Step 4 Loosen and dis-assemble the SFP adapter gland components.

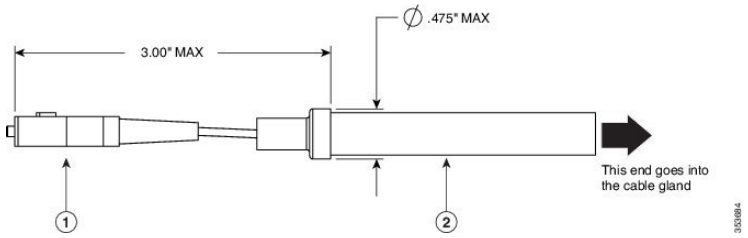
Figure 13: Exploded view of Fiber-Optic cable and Gland assembly



1	SFP Transceiver Module	5	Large Cable Rubber Gland 0.30 to 0.50 inch (7.6 to 12.7 mm) diameter
2	Duplex LC/SC Fiber-optic cable	6	Gland Compression Ferrule
3	Body O-ring	7	Gland nut
4	SFP Gland Adapter body		

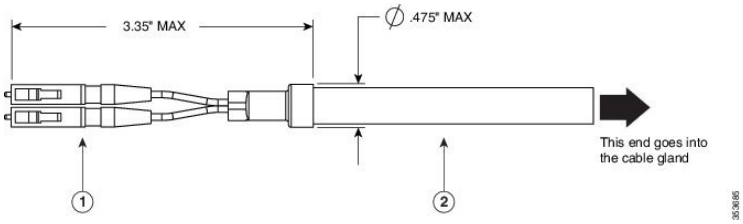
Step 5 Terminate the SC or LC fiber optic cable.

Figure 14: SC Fiber-optic cable



1	SC optic fiber connector	2	Optic fiber cable

Figure 15: Duplex LC Fiber Optic Cable



1	Duplex LC optic fiber connector	2	Optic fiber cable

Step 6 Using caution, avoid damaging the fiber connector end, pass the fiber connector through the adapter gland components. Ensure components are ordered and oriented.

Step 7 Verify the O-ring is correctly seated on the gland adapter body. Reassemble the components of the adapter gland. Do not tighten the gland nut on the rubber inserts. Leave it loose so the gland can easily slide on the fiber cable. If you tightened the cable in this step, you might damage the cable.

Step 8 Insert the SC or LC optic fiber connector-end of the cable into the SFP transceiver module and ensure it latches into place.

Step 9 Thread the adapter body into the SFP port on the switch. Tighten the adapter body by hand until it is fully seated. Inspect that the body is seated correctly. Using an adjustable wrench, tighten the body snugly to the switch body to approximately 13 to 17 in/lbs (1.5 to 1.9 Nm) of torque.

Step 10 To seal the rubber gland to the fiber cable, hand-tighten the gland nut. Using an adjustable wrench, tighten the nut ¼ revolution to make a water-tight seal on the cable to approximately 15 to 22 in/lbs (1.7 to 2.4 Nm) torque.

Caution
When removing this SFP assembly, you must proceed in the reverse order of this installation. Start by loosening the cable gland's nut.

Connecting to Power

You must supply a power solution for the device. The input voltage should be between 12–54 Vdc.

Warning **Statement 1005—**Circuit Breaker

This product relies on the building's installation for short-circuit (overcurrent) protection. To reduce risk of electric shock or fire, ensure that the protective device is rated not greater than: **20 A**

Grounding the Switch

Follow any grounding requirements at your site.

Warning **Statement 2004—**Grounded Equipment

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

Caution To make sure that the equipment is reliably connected to earth ground, follow the grounding procedure instructions, and use a UL-listed ring terminal lug suitable for number 6 AWG (13.3 mm^2) wire (Hollingsworth part number R3456B or equivalent).

Caution Use at least a 4 mm^2 conductor to connect to the external grounding screw.

A ground lug is not supplied with the switch. You can select from these options:

- Single ring terminal
- Two single ring terminals

To ground the switch to earth ground by using the ground screw, follow these steps:

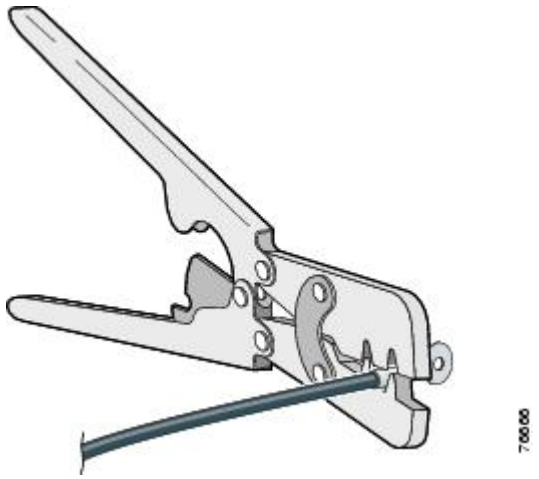
Procedure

Step 1 Use a standard Phillips screwdriver or a ratcheting torque screwdriver with a Phillips-head to remove the ground screw from the switch. Store the ground screw for later use.

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

Step 3 Insert the ground wire into the ring terminal lug, and using a crimping tool, crimp the terminal to the wire. See the following figure. If two ring terminals are being used, repeat this action for a second ring terminal.

Figure 16: Crimping the Ring Terminal



Step 4 Slide the ground screw through the terminal.

Step 5 Insert the ground screw into the ground screw opening.

Step 6 Use a ratcheting torque screwdriver to tighten the ground screws and ring terminal to the switch front panel to 3.5 in-lb (0.4 Nm). The torque must not exceed 3.5 in-lb (0.4 Nm).

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

Connecting the earth ground wire

Procedure

Step 1 Measure a single length of stranded copper wire long enough to connect the power supply to the earth ground. The wire color might differ depending on the country of use.

The power supply must be grounded in accordance with local/state/national codes and per the installation guidelines of the power supply.

Step 2 Connect one end of the stranded copper wire to a grounded bare metal surface, such as a ground bus, a grounded DIN rail, or a grounded bare rack.

Connect the other end of the wire to the grounding screw on the power supply. Only wire with insulation should extend from the connection.

Note
The position of the power supply may vary on different switch models.

Step 3 Tighten the earth-ground wire connection screw.

Note
Torque to 8 in.-lb, not to exceed 10 in-lb.

Connecting Alarm Circuits

After the switch is installed, you can connect the alarm.

Wiring the External Alarms

Use M12 A-coded cable to connect to the alarm connector on the switch. Recommended torque is 4.43 to 7.08 in/lbs (0.5 to 0.8 Nm).

The recommended cable part number from Molex is 1200650523. One end of the cable has M12 A-coded connector and the other end is open.

The labels for the alarm connector are on the switch panel and are displayed in the following table.

Table 8: Alarm Connector Labels (Top to Bottom)

Pin	Label	Connection
1	NO	Alarm Output Normally Open (NO) connection
2	NC	Alarm Output Normally Closed (NC) connection
3	UNCONNECTED	Unused
4	UNCONNECTED	Unused
5	COMMON	Alarm Common connection

Caution The input voltage source of the alarm output relay circuit must be an isolated source and limited to less than or equal to 30 Vdc, 1.0 A or 60 Vdc, 0.5 A.

Connecting Destination Ports

This section provides information about connecting to the destination ports.

Connecting to 10/100 and 10/100/1G/2.5G Ports

The 10/100 and 10/100/1G/2.5G ports automatically configure themselves to operate at the speed of attached devices. If the attached ports do not support autonegotiation, you can explicitly set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have their speed and duplex parameters manually set can reduce performance or result in no link.

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

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

Caution To prevent electrostatic-discharge (ESD) damage, follow your normal board and component handling procedures.

Procedure

Step 1 When connecting to workstations, servers, routers, and Cisco IP phones, connect a straight-through cable to a M12 connector (IP67 Torque: 4.5 to 7.0 in-lbs or 0.5 to 0.8 Nm) on the front panel.

When connecting to 1G/2.5G compatible devices, use a twisted four-pair, Category 5 or higher cable.

The auto-MDIX feature is enabled by default.

Step 2 Connect the other end of the cable to a M12 connector on the other device. The port LED turns on when both the switch and the connected device have established a link.

The port LED is amber while Spanning Tree Protocol (STP) discovers the topology and searches for loops. This can take up to 30 seconds and then the port LED turns green. If the port LED does not turn on:

- The device at the other end might not be turned on.
- There might be a cable problem or a problem with the adapter installed in the attached device. See Chapter 4, “Troubleshooting,” for solutions to cabling problems.

Step 3 Reconfigure and reboot the connected device if necessary.

Step 4 Repeat Steps 1 through 3 to connect each device.

Where to Go Next

If the default configuration is satisfactory, the switch does not need further configuration. You can use any of these management options to change the default configuration:

- WebUI

  You can use WebUI to manage and monitor individual switches. Device Manager can be accessed from anywhere in your network through a web browser by using the management IP address of the switch. For more information, see the Device Manager online

- Cisco IOS-XE CLI

  The switch CLI is a version of Cisco IOS-XE firmware that can be used to configure and monitor the switch. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station.

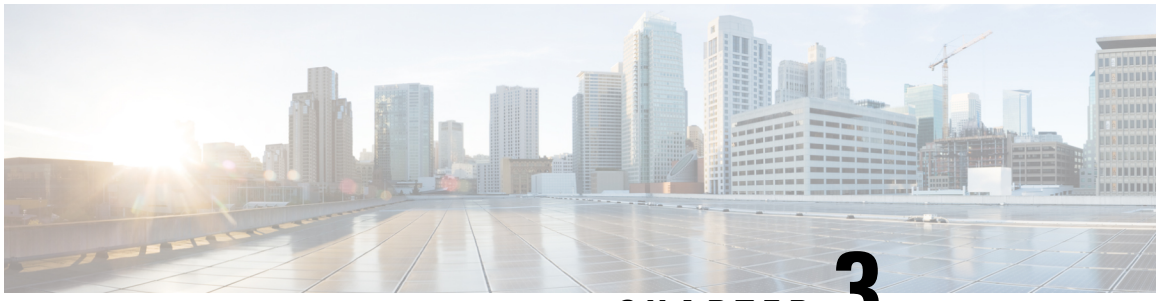
- Cisco Catalyst Center

- SNMP

  Switches can be managed by using a SNMP-compatible management platforms. The switch supports a comprehensive set of Management Information Base (MIB) extensions and four Remote Monitoring (RMON) groups.

- Common Industrial Protocol

  Common Industrial Protocol (CIP) management objects are supported by the switch, allowing you to manage an entire industrial automation system with one tool.



CHAPTER 3

Express Setup

- Required Equipment, on page 29
- Run Express Setup, on page 29

Required Equipment

You need this equipment to set up the switch:

- Computer running Windows or a Mac.
- A web browser (IE or Firefox) with JavaScript enabled.
- A straight-through or crossover Category 5 Ethernet cable to connect your computer to the switch port.

Note Do not use any of the Console ports for Express Setup.

- A small paper clip to reach the button.

Note Before running Express Setup, disable any pop-up blockers or proxy settings on your browser and any wireless client running on your computer.

Run Express Setup

Complete the steps in this section to use Express Setup to enter the initial IP information.

Before you begin

Perform the following checks before you use Express Setup.

- Make sure that the switch is in default factory mode.
- Make sure that nothing is connected to the switch.

During Express Setup, the switch acts as a DHCP server. Ensure that the computer that is connected to the switch is configured with DHCP.



Note Exception: You can add a serial console cable to monitor the booting sequence. *Do not press [return key] on the console screen*.

Procedure

Step 1 Complete one of the following actions:

If the switch...	Then...
Is fresh out of the box	Go to Step 2.
Is not fresh out of the box	Use a paper clip to reset the switch for 15-20 seconds until the Express Setup LED turns alternating red and green, then release the paper clip The switch automatically reboots once the Express Setup LED blinks alternating red and green.

Note
The Express setup long press (press the button for 15 seconds to reset the switch to use factory default settings) deletes the configurations (nvram_config and vlan.dat) from the flash and removable media (SD card or USB flash drive). Remove any removable media if you do not want any files to be deleted from the SD card or USB flash drive.

Step 2 On the computer that is connected to the switch, disable web browser pop-up blockers and proxy settings.

Step 3 Power on or reset the switch.

Use LEDs to monitor boot progress:

- Blinking Express Setup LED: Ready for express setup process

Step 4 Insert paper clip into Express Setup button for 3–5 seconds.

When released, the lowest free copper port will start flashing green.

Step 5 Connect the computer to the port blinking green.

The LED continues to blink.

Step 6 After the computer has the IP Address 192.168.1.x, point the browser to http://192.168.1.254.

The setup using a wizard screen appears.

Step 7 Select **Classic Day 0 Wizard**

The Login page appears.

Step 8 Enter the Username and Password.

The username is admin, and the password is the system serial number. To find the serial number of the device, see .

The **Account Settings** window appears.

Step 9 In the **Account Settings** window, complete the following tasks:

a) Fill out the fields in the **Account Settings** window as follows:

- *Login Name:* admin

  You can change the login name here, if you like.

- *Login User Password*: By default, the login user password is the serial number of the switch.

  You can change the login user password here if you like.

- *Confirm Login User Password*: Retype the password that you used earlier.

- *Command-Line Password* (Optional): This defaults to Sync to Login Password.

  You can change the command login password here by using the drop-down menu.

- *Device Name*: Create an identifier for the device in the network.

- *NTP Server* (Optional): You may identify an NTP server for the device here.

- *Date & Time Mode* (Optional): Identify the mode here, through the drop-down.

Trouble
If the account settings window does not appear, make sure that any pop-up blockers or proxy settings on your browser are disabled. Also make sure that any wireless client is disabled on your computer.

b) After you finish filling in the fields in the **Account Settings** window, click **Basic Settings**.

Step 10 In the **Basic Settings** window, complete the following tasks:

a) Fill out the fields as follows, using English letters and Arabic numbers:

- *IP Address*: Choose Static or DHCP.

- *VLAN ID*: Enter a valid VLAN ID.

  This is the management VLAN for the switch.

- *IP Address*: Enter a valid IP Address.

- *Subnet Mask*: Enter a valid subnet mask.

- *Default Gateway*: Enter the IP address of the router (not optional if IP is static).

  You must enter the router IP address if the IP address is static.

(Optional) On this screen you can also enable or disable Telnet and SSH and configure CIP settings.

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 the switch. The default CIP VLAN is VLAN 1. Only one VLAN on a switch can have CIP enabled. If the CIP VLAN is different from the management VLAN, you must specify an IP address for the CIP VLAN. Make sure that the IP address that you assign to the switch is not being used by another device in your network.

For more information about the CIP VLAN settings, click Help on the toolbar.

b) After you finish filling in the fields in the **Basic Settings** window, click **Switch Wide Settings**.

Step 11 In the **Switch Wide Settings** window, complete the following tasks:

a) Fill out the fields as follows:

- *Data VLAN*: You can enable or disable the data VLAN with the button here.
- *Voice VLAN*: You can enable/disable Voice VLAN here.
- *STP Mode* (Optional): Select an STP Mode from the drop-down
- *Bridge Priority* (Optional): You can update, enable, or disable Bridge Priority here.
- *Domain Name* (Optional): Enter a valid Domain Name.

b) After you finish filling in the fields in the **Switch Wide Settings** window, click **Day 0 Config Summary**.

The **Summary** window displays the configuration settings that you made.

Step 12 In the **Summary**window, confirm that the settings are accurate and complete one of the following actions:

If the settings...	Then...
Are correct	Click **Submit** to complete the initial setup.
Are not correct	**a.** Click the back button and make the required changes. **b.** Navigate back to the **Summary** window. **c.** Click **Submit** to complete the initial setup.

After you click **Submit**, the following events occur:

a. The switch is configured and exits Express Setup mode.

b. The browser displays a warning message and tries to connect with the earlier switch IP address.

c. Success dialog appears. Click **OK**.

Typically, connectivity between the computer and the switch is lost because the configured switch IP address is in a different subnet from the IP address on the computer.

Step 13 Turn off DC power at the source, disconnect all cables to the switch, and install the switch in your network.

Step 14 If you changed the static IP address on your computer, revert to the previous configuration.

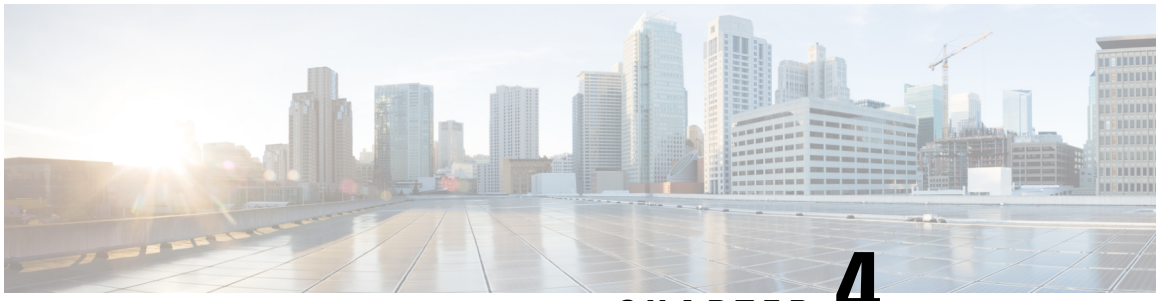
What to do next

You can display Web UI by following these steps:

1. Start a web browser on your computer.
2. Enter the switch IP address, username, and password in the web browser, and press Enter. The WebUI page appears.

Trouble If the WebUI page does not appear:

- Confirm that the port LED for the switch port connected to your network is green.
- Confirm that the computer that you are using to access the switch has network connectivity by connecting it to a well-known web server in your network. If there is no network connection, troubleshoot the network settings on the computer.
- Make sure that the switch IP address in the browser is correct.
- Ping the Switch IP Address and confirm IP reachability.
- If the switch IP address in the browser is correct, the switch port LED is green, and the computer has network connectivity, continue troubleshooting by reconnecting the computer to the switch. Configure a static IP address on the computer that is in the same subnet as the switch IP address.
- When the LED on the switch port that is connected to the computer is green, reenter the switch IP address in a web browser to display the Web UI. When Web UI appears, you can continue with the switch configuration.



CHAPTER 4

Configuring the switch with the CLI setup program

To set up the switch, you need to complete the setup program, which runs automatically after the switch is powered on. You must assign an IP address and other configuration information necessary for the switch to communicate with the local routers and the Internet. This information is also required if you plan to use WebUI to configure and manage the switch.

- IP and Password Settings, on page 35
- Initial Configuration, on page 35
- Configure System Security, on page 39

IP and Password Settings

You need this information from your network administrator before you complete the setup program:

- Encryption level and Master key
- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password
- Enable password

Initial Configuration

Complete the following steps to create an initial configuration for the switch with the setup program:

Procedure

Step 1 Enter **Yes** at these two prompts:

```
Would you like to enter the initial configuration dialog? [yes/no]:yes
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.
Would you like to enter basic management setup? [yes/no]:yes
```

Step 2 Enter a hostname for the switch.

On a command switch, the hostname is limited to 28 characters; on a member switch, it is limited to 31 characters. Do not use *-n* , where n is a number, as the last character in a hostname for any switch.

Configuring global parameters:

```
Enter host name [Switch]:host_name
```

Step 3 Enter an enable secret password.

The password can be of minimum 10 to maximum 25 alphanumeric characters, and must contain at least one uppercase, one lowercase, and a digit.

Note
The password should not contain the word **cisco** in it.

```
Enter enable secret:secret_password
Confirm enable secret:secret_password
```

Step 4 Enter an enable password.

```
Enter enable password:enable_password
```

Step 5 Enter a virtual terminal password.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

```
Enter virtual terminal password:terminal-password
```

Step 6 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network.

For this release, always use **vlan1** as the interface connecting to the management network.

Note
The switch will transmit a DHCP discover message on the **vlan1** interface. If the switch is connected to the network before the CLI initial setup process is started, the interface may have been assigned a dynamic IP address. If you do not see an IP address on the **vlan1** interface, this process allows you set a static IP address for management. This will overwrite the dynamically assigned IP address.

```
Current interface summary

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      10.0.113.39     YES DHCP   up                      up
GigabitEthernet1/1         unassigned      YES unset  down                    down
GigabitEthernet1/2         unassigned      YES unset  down                    down
GigabitEthernet1/3         unassigned      YES unset  down                    down
```

```
GigabitEthernet1/4          unassigned      YES unset  down                    down
GigabitEthernet1/5          unassigned      YES unset  down                    down
GigabitEthernet1/6          unassigned      YES unset  down                    down
GigabitEthernet1/7          unassigned      YES unset  down                    down
GigabitEthernet1/8          unassigned      YES unset  down                    down
GigabitEthernet1/9          unassigned      YES unset  down                    down
GigabitEthernet1/10         unassigned      YES unset  down                    down
GigabitEthernet1/11         unassigned      YES unset    up                      up
AppGigabitEthernet1/1       unassigned      YES unset    up                      up

Enter interface name used to connect to the
management network from the above interface summary:
 vlan1
```

Step 7 Configure the interface by entering the switch IP address and subnet mask.

The configuration summary is displayed.

Step 8 Select option 2 to save the configuration and exit the configuration menu.

Example

```
        --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

 Enter host name [Switch]: Switch

 The enable secret is a password used to protect
 access to privileged EXEC and configuration modes.
 This password, after entered, becomes encrypted in
 the configuration.
 ------------------------------------------------
 secret should be of minimum 10 characters and maximum 32 characters with
 at least 1 upper case, 1 lower case, 1 digit and
 should not contain [cisco]
 ------------------------------------------------
 Enter enable secret: **********
 Confirm enable secret: **********
Netconf SSH RSA key generated
Key Name: NETCONF_SSH_RSA_KEY
Key Type: ssh-rsa
Modulus Size: 2048
Public Key: ssh-rsa AAAAB3AAAADAQABAAABAQC46E6OfS9Tl6bHuxJkyrCy9JDwgkE9tK
XJcgD2Mu26NTCGpIDRyGAjaj9+gc04Gc/TOHruWEt/XTZu9hWK1dN+rZytJMNw3nEavFcsm+d
gDzYwh3BAi16edDil97YzlNr5bsisrgehSqKoq7Srj8fW3SyPNRU2WNdbeLkwjLtZQSgA7hBL
x1r9V+wS9+hk8SQJsMRBhMSLMo7Mo/XZ22risylZPeWvypmip6zGakKm14K8TbgnKmTbgZscp
hn/qJ9ag+tzuDQug+ZLWw/QE3MJHZmcbXdt1gcE8b0lTRT
```

```
 The enable password is used when you do not specify an
 enable secret password, with some older software versions, and
 some boot images.
 Enter enable password: **********

 The virtual terminal password is used to protect
 access to the router over a network interface.
 Enter virtual terminal password: *********

Current interface summary

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      10.0.113.39     YES DHCP   up                      up
GigabitEthernet1/1         unassigned      YES unset  down                    down
GigabitEthernet1/2         unassigned      YES unset  down                    down
GigabitEthernet1/3         unassigned      YES unset  down                    down
GigabitEthernet1/4         unassigned      YES unset  down                    down
GigabitEthernet1/5         unassigned      YES unset  down                    down
GigabitEthernet1/6         unassigned      YES unset  down                    down
GigabitEthernet1/7         unassigned      YES unset  down                    down
GigabitEthernet1/8         unassigned      YES unset  down                    down
GigabitEthernet1/9         unassigned      YES unset  down                    down
GigabitEthernet1/10        unassigned      YES unset  down                    down
GigabitEthernet1/11        unassigned      YES unset  up                      up
AppGigabitEthernet1/1      unassigned      YES unset  up                      up

Enter interface name used to connect to the
management network from the above interface summary: Vlan1

Configuring interface Vlan1:
   IP address for this interface [10.0.113.39]:
   Subnet mask for this interface [255.0.0.0] :
   Class A network is 10.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch
enable secret 9 $9$IjMTkpAcbKRIK.$W27WanN6KUn4NnrjTTJteGEox1u.
enable password enable_password
line vty 0 15
password terminal_password
no snmp-server
!
no ip routing

!
interface Vlan1
no shutdown
ip address 22.1.1.39 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
```

```
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
interface GigabitEthernet1/11
!
interface AppGigabitEthernet1/1
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

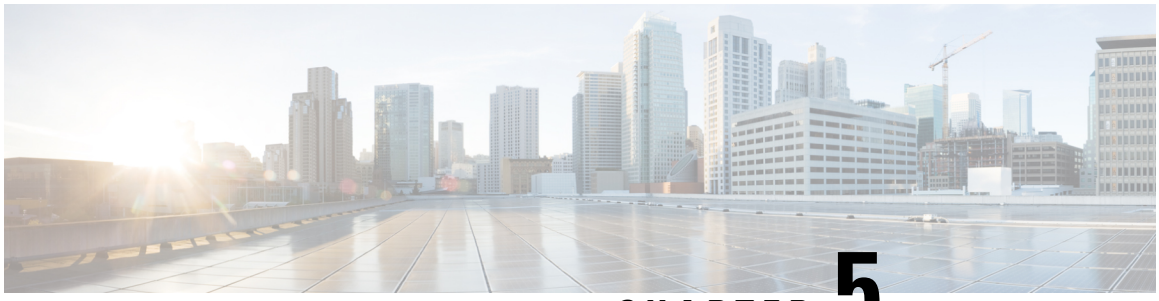
Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

Configure System Security

The device is configured with Type-6 encryption by default. To change the encryption type, see Controlling Switch Access with Passwords and Privilege Levels.



CHAPTER 5

Troubleshooting

This chapter provides troubleshooting recommendations.

- Diagnosing Problems, on page 41
- Reset the Switch, on page 43
- How to Recover Passwords, on page 43
- Troubleshooting Express Setup, on page 44
- Finding the Switch Serial Number, on page 44

Diagnosing Problems

The switch LEDs provide troubleshooting information about the switch. They show boot failures, port-connectivity problems, and overall switch performance. You can also get statistics from Device Manager, the CLI, or an SNMP workstation.

Switch Connections

Bad or Damaged Cable

Examine the cable for marginal damage or failure. A cable might be just good enough to connect at the physical layer, but it could corrupt packets as a result of subtle damage to the wiring or connectors. You can identify this problem because the port has many packet errors or it constantly flaps (loses and regains link).

- Exchange the cable with a known good cable.
- Look for broken or missing pins on cable connectors.
- Rule out any bad patch panel connections or media converters between the source and the destination. If possible, bypass the patch panel.
- Try the cable in another port to see if the problem follows the cable.

Link Status

Verify that both sides have a link. A broken wire or a shutdown port can cause one side to show a link even though the other side does not have a link.

A port LED that is on does not guarantee that the cable is functional. It might have encountered physical stress, causing it to function at a marginal level. If the port LED does not turn on:

- 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.
- Look for loose connections. Sometimes a cable appears to be seated but is not. Disconnect the cable, and then reconnect it.

10/100, 1G, 2.5G, 10G Port Connections

If a port appears to malfunction:

- Verify the status of all ports. See Port status LEDs, on page 8 for descriptions of the LEDs and their meanings.
- Use the **show interfaces** privileged EXEC command to see if the port is error-disabled, disabled, or shut down. Reenable the port if necessary.
- Verify the cable type.

Interface Settings

Verify that the interface is not disabled or powered off. If an interface is manually shut down on either side of the link, it does not come up until you reenable the interface. Use the **show interfaces** privileged EXEC command to see if the interface is error-disabled, disabled, or shut down on either side of the connection. If needed, reenable the interface.

Ping End Device

Ping from the directly connected switch first, and then work your way back port by port, interface by interface, trunk by trunk, until you find the source of the connectivity issue. Make sure that each switch can identify the end device MAC address in its Content-Addressable Memory (CAM) table.

Switch Performance

Speed, Duplex, and Autonegotiation

Port statistics that show a large amount of alignment errors, frame check sequence (FCS), or late-collision errors, a common issue when duplex and speed settings are mismatched between two devices.

To maximize switch performance and to ensure a link, follow one of these guidelines when changing the duplex or the speed settings.

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the interfaces on both ends of the connection.
- If a remote device does not autonegotiate, use the same duplex settings on the two ports. The speed parameter adjusts itself even if the connected port does not autonegotiate.

Autonegotiation and Network Interface Cards

Problems sometimes occur between the switch and third-party network interface cards (NICs). By default, the switch ports and interfaces autonegotiate. Laptops or other devices are commonly set to autonegotiate, yet sometimes issues occur.

To troubleshoot autonegotiation problems, try manually setting both sides of the connection to the same speed and duplex mode. If this does not solve the problem, there could be a problem with the firmware or software on the NIC. You might resolve this by upgrading the NIC driver to the latest version.

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.

Reset the Switch

Resetting the switch deletes the configuration and reboots the switch.

Reasons why you might want to reset the switch to the factory default settings include:

- You installed the switch in your network and cannot connect to it because it is assigned an unknown IP address.
- You want to reset the password on the switch.



Caution If you press the Express Setup button when you power on, the automatic boot sequence stops and the switch enters bootloader mode.

To reset the switch:

Procedure

Step 1 Press and hold the Express Setup button for 15 seconds or more. The switch reboots. The system led turns green and the Express Setup LED starts to blink green.

Step 2 Press the Express Setup button again for 1-3 seconds. LED for port 1/1 blinks green.

The switch now behaves like a factory-default configured switch. See Run Express Setup, on page 29 section to complete the reinstallation.

How to Recover Passwords

Password recovery is a feature that a system administrator can enable or disable. If password recovery is disabled, the only way to recover from a lost or forgotten password is to clear the switch configuration entirely. For this procedure, see the “Resetting the Switch” section.

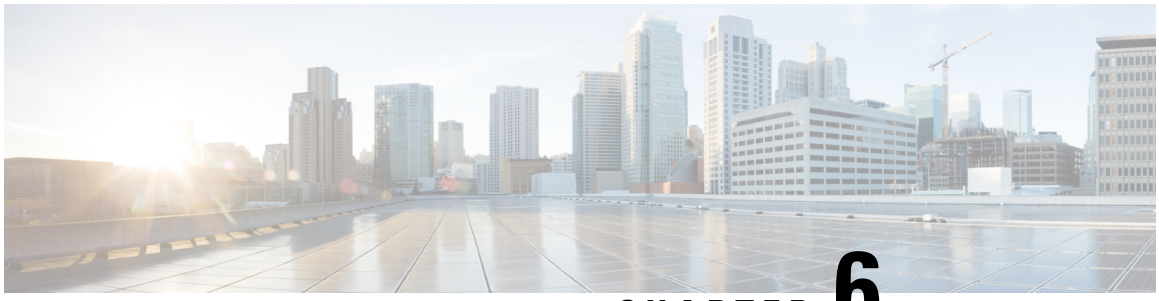
Troubleshooting Express Setup

This section provides troubleshooting tips for the initial switch configuration.

Checklist	Recommendation
Was the SETUP LED blinking when you pressed the Express Setup button?	If no, or you are not sure, restart the switch. Make sure that the SETUP LED is blinking when you press the Express Setup button.
Did you connect your PC to the wrong switch port?	Verify that you are connected to the switch port with the blinking LED.
Did you start a browser session on your PC before the SETUP LED was solid green?	If yes, or you are not sure, restart the switch, and repeat the Express Setup procedure.
Did you start a browser session on your PC and the setup page did not appear?	If the window does not appear, enter a URL in your browser, such as *Cisco.com* or another well known website.
Did you have a pop-up blocker running on your PC when you connected to the switch port?	If yes, disconnect the cable from the switch port, disable the pop-up blocker, press the Express Setup button, and reconnect the cable to the blinking Ethernet port.
Did you have proxy settings enabled in your browser software when you connected to the switch port?	If yes, disconnect the cable from the switch port, disable the proxy settings, press the Express Setup button, and reconnect the cable to the blinking Ethernet port.
Did you have a wireless client running on your PC when you connected to the switch port?	If yes, disconnect the cable from the switch port, disable the wireless client, press the Express Setup button, and reconnect the cable to the blinking Ethernet port.
Do you need to change the switch IP address after you have already completed the initial setup?	Go to the **Configure > Express Setup** Device Manager screen to change the switch IP address. For more information about changing the switch IP address, see the Cisco IE3500H Switch Software Configuration Guide at Cisco.com.

Finding the Switch Serial Number

If you contact Cisco Technical Assistance, you need to know the serial number of your switch. The serial number is on the compliance label on left-hand side under the removable door. You can also use the **show version** privileged EXEC command to obtain the switch serial number.



CHAPTER 6

Technical Specifications

This appendix provides the technical specifications for the Cisco IE3500 Heavy Duty Series Switches.

- Operating Temperature Specifications, on page 45
- Technical Specifications, on page 46
- Connectors and Cabling, on page 46
- Torque Specifications, on page 47
- Alarm Ratings, on page 48

Operating Temperature Specifications

Note The safety certifications apply only to ambient temperatures under 140°F (60°C). However, the Cisco IE3500 Heavy Duty Series Switches can function in substation and traffic signal installations under the environmental conditions described in the table.

The table lists the operating temperatures for the Cisco IE3500 Heavy Duty Series Switches in three different environments.

Table 9: Operating Temperature for the Cisco IE3500H switches

	Industrial Automation and Other Locations Requiring Enclosures	**Substation**	**Traffic Signal**
Enclosure types	Sealed enclosures For example: NEMA 4, NEMA 4X, NEMA 12, NEMA 13, IP54, and IP66 -40 °C to +60 °C (-40 °F to +140 °F)	Vented enclosures For example: NEMA 1, IP66, and IP67 -40 °C to +70 °C (-40 °F to +158 °F)	Fan or blower-equipped enclosures For example: NEMA TS-2. -34 °C to +75 °C (-29.2 °F to +167 °F) **Note** The minimum airflow is 200 LFM[1].

[1] LFM= linear feet per minute.

Technical Specifications

Table 10: Cisco IE3500H Technical Specifications

Environment	Values
Storage temperature	–40 to 85 °C (–40 to 185 °F)
Operating temperature (measured inside the enclosure, 1 inch below the bottom surface of the switch)	–40 to 75°C (–40 to 167 °F) **Caution** Operating temperatures exceeding 60 °C are not covered by the product safety certifications and approvals. • Sealed Enclosure Operating: -40 °C to +60 °C (-40 °F to +140 °F) • Vented Enclosure Operating: -40 °C to +70 °C (-40 °F to +158 °F) • 200 LFM or more Fan or Blower equipped Enclosure Operating: -34 °C to +75 °C (-29.2 °F to +167 °F) • Type-tested to +85C for 16 hours: -40 °C to +85 °C (-40 °F to +185 °F)
Operating humidity	5 to 95% (non-condensing)
Ingress Protection/Type Ratings	IP66 and IP67 Rated for protection against dust and submersion in water NEMA Type 4X **Caution** IP66 and IP67, NEMA Type 4X compliant only when all IP67 cables are mated and torqued appropriately or with the supplied dust caps attached.
Operating altitude	Up to 40,000 feet (4570 meters)
Storage altitude	Up to 40,000 feet (4570 meters)

Connectors and Cabling

The connectors and cabling for the Cisco IE3500 Heavy Duty Series Switches are below.

Table 11: Cisco IE3500H Cables and Connectors

Data Ports	Downlink connections • Copper 100 Base-T M12 D-coded 4-pole (pin) cable: M12 Male and/or M12/RJ-45 connector • Copper GE M12 X-coded 8-pole (pin) shielded cable: M12 Male and/or M12/RJ-45 connector • Copper 2.5 GE M12 X-coded 8-pole (pin) shielded cable: M12 Male and/or M12/RJ-45 connector • For IE-3500H-12P2MU2X: 2.5G (mGig) Copper M12 X-coded 8-pole (pin) shielded cable: M12 Male and/or M12/RJ-45 connector Uplink connections • For IE-3500H-12P2MU2X: 1G/10G SFP Fiber-optic cable: LC or SC connector (for fiber-optic cable) with SFP/SFP+ module. **Note** The SFP/SFP+ module determines the type of fiber-optic cable (LC or SC) to be used with the switch.
Alarm Port	• Copper M12 A-coded 5 Pin connector
Power Input	• Mini-Style 4-pin connector for power input
Console Cable: CAB-CONSOLE-M12=	• Console Cable 6 ft with M12 and DB9F for IE3500H Switch

Torque Specifications

The torque specifications for Cisco IE3500 Heavy Duty Series Switches are below.

Table 12: Cisco IE3500H torque specs

Alarm, Console, Ethernet ports (M12 Connectors)	• 4.5 to 7.0 in-lbs (0.5 to 0.8 Nm)
M12 Connector Dust Cap (Alarm, Console, Ethernet ports)	• 3.5 in-lbs (0.4 Nm)
Power Supply Connector (Mini-Change)	• 10 in-lbs (1.13 Nm)
SD Card Access Door Captive Screws	• 16 to 19.5 in-lbs (1.8 to 2.2Nm)

SFP Gland	• Adapter body: 13 to 17 in-lbs (1.5 to 1.9 Nm) • Gland nut: 15 to 22 in-lbs (1.7 to 2.4 Nm)

Alarm Ratings

The alarm ratings for the Cisco IE3500 Heavy Duty Series Switches are below.

Table 13: Cisco IE3500H Alarm Ratings

Alarm Ratings	Specification
Alarm	One alarm output relay using an M12 A Coded 5 Pin connector (Max. rated: 30 Vdc @ 1A / 60 Vdc @ 0.5A)