ExtremeSwitching™

ISW Series Managed Industrial Ethernet Switch Quick Installation Guide

ISW 4-10/100P, 2-10/100T, 2-SFP (PN 16801)
ISW 4GbP, 2GbT, 2-SFP (PN 16803)
ISW 8-10/100P, 4-SFP (PN 16802)
ISW 8GbP, 4-SFP (PN 16804)

9034964 Rev. 03

Published August 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Table of Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.

The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1 Go to www.extremenetworks.com/support/service-notification-form.
2 Complete the form with your information (all fields are required).
3 Select the products for which you would like to receive notifications.

Note
You can modify your product selections or unsubscribe at any time.

4 Click **Submit**.

Related Publications

ISW-Series

- *ISW-Series Managed Industrial Ethernet Switch Command Reference Guide*
- *ISW-Series Managed Industrial Ethernet Switch Hardware Installation & User Guide*
- *ISW-Series Managed Industrial Ethernet Switch Quick Installation Guide*
- *ISW-Series Managed Industrial Ethernet Switch Web Configuration Guide*

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

1 Industrial Series Switch Overview

ISW-Series Managed Industrial Ethernet Switch deliver high quality, wide operation temperature range, extended power input range, and advanced *VLAN (Virtual LAN)* & *QoS (Quality of Service)* features. It's ideal for harsh environments and mission-critical applications.

The Managed Ethernet Switch solutions are designed for supporting standard industrial applications. Managed switches are easier to prioritize, partition, and organize user's network, providing a more reliable and better quality services.

This guide covers installation for the following Industrial Switches:

- ISW 4-10/100P,2-10/100T,2-SFP
- ISW 8-10/100P,4-SFP
- ISW 4GBP,2GBT,2-SFP
- ISW 8GBP,4-SFP

Package Checklist

Please verify the box contains the following items:

Item	Quantity
Management Ethernet switch	1
Wall-mount plates	2
DIN-Rail CLIP	1
M3 Screws (for the wall mount plates & DIN CLIP)	4
DC power terminal block	1
RJ45 Ethernet port Dust Cover	Some
SFP Ethernet port Dust cover	Same as SFP port number

Safety Instructions

When a connector is removed during installation, testing, or servicing, or when an energized fiber is broken, a risk of ocular exposure to optical energy that may be potentially hazardous occurs, depending on the laser output power.

The primary hazards of exposure to laser radiation from an optical-fiber communication system are:

- Damage to the eye by accidental exposure to a beam emitted by a laser source.
- Damage to the eye from viewing a connector attached to a broken fiber or an energized fiber.

Technical Specifications

Model	ISW
Ethernet	
Copper RJ45 Ports	10/100/1000 Mbps speed auto-negotiation MDI/MDIX Auto-crossover
SFP (pluggable Ports)	100/1000Base SFP slot
Fiber port connector	LC typically for fiber (depends on module)
Power	
Power input	Redundant Input Terminals; Reverse power protection
Input voltage range	12-58 VDC (with POE: 46-58 VDC)
Maximum Power consumption	Without *PoE (Power over Ethernet)*: 14 Watts With PoE: 265 Watts
Environmental and Compliances	
Operating temperature	-40 to +75°C (cold startup at -40°C)
Storage temperature	-40 to +85°C
Humidity	5 to 95% RH (non-condensing)
Mechanical	
Ingress protection	IP30
Dimension (without DIN rail clip)	154mm(H) x 128mm(D) x 77mm(W)
Weight	1410g
Installation option	DIN-Rail mounting Wall mounting

Faceplate and Panels

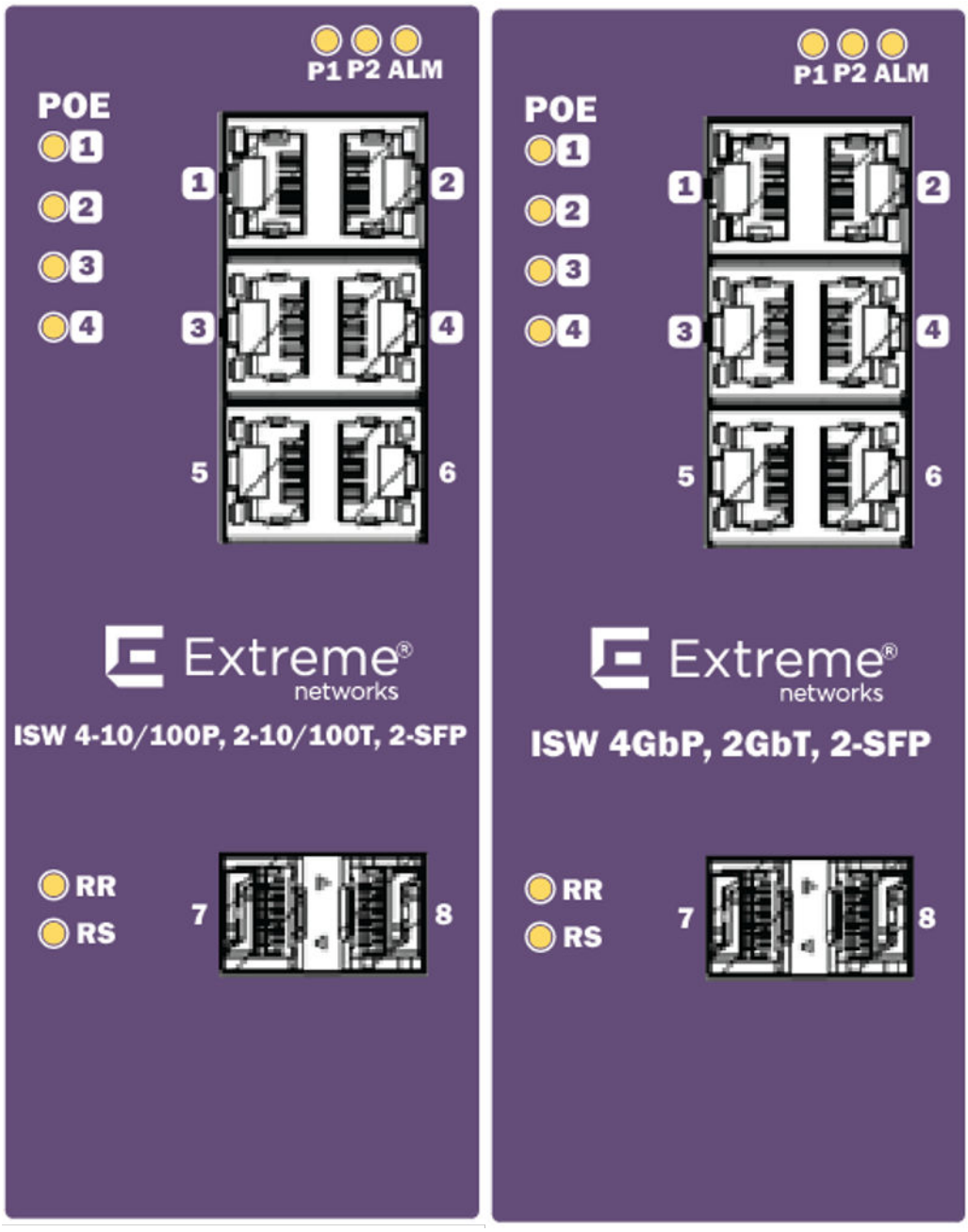


Figure 1: 4-Port PoE Series Faceplate

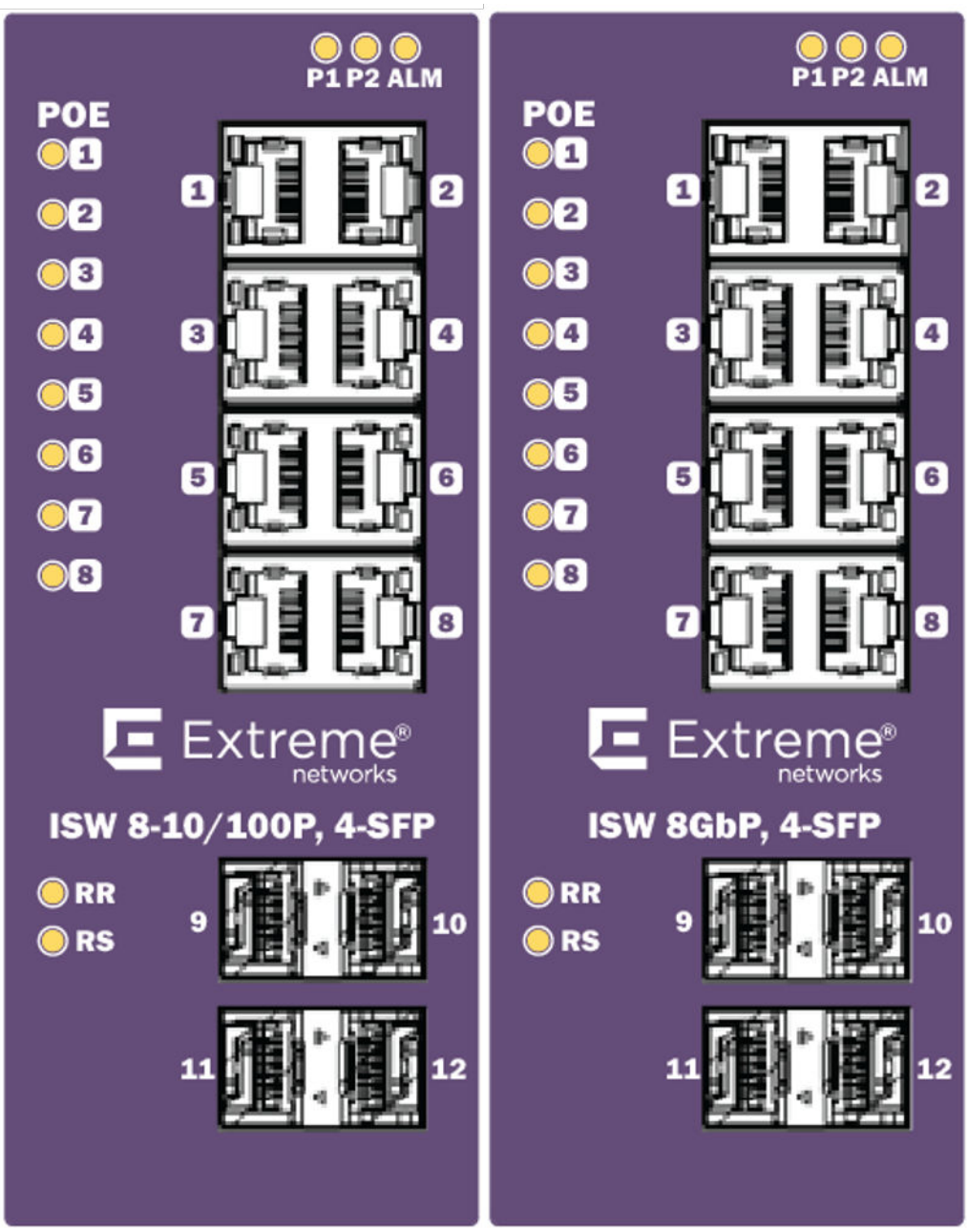


Figure 2: 8-Port PoE Series Faceplate

Front Panel	
System Status LED	P1, P2 and Alarm
Gigabit Ethernet Copper Ports	RJ45
Gigabit Ethernet SFP ports	SFP Slots
POE LED	POE port status
RR/RS LED	Device info/status

Figure 3: Top Panel

Top Panel	
Power Input (Dual)	6P Terminal Block
Console (RS232)	RJ45
Reset	Push Button

Alarm Relay and Ground Connection

The alarm relay output contacts are in the middle of the DC terminal block connector as shown in Figure 4.

The alarm relay out is “Normal Open,” and it will be closed when detected any predefined failure such as power failures or Ethernet link failures.

The relay output with current carrying capacity of 0.5A @ 24 VDC.

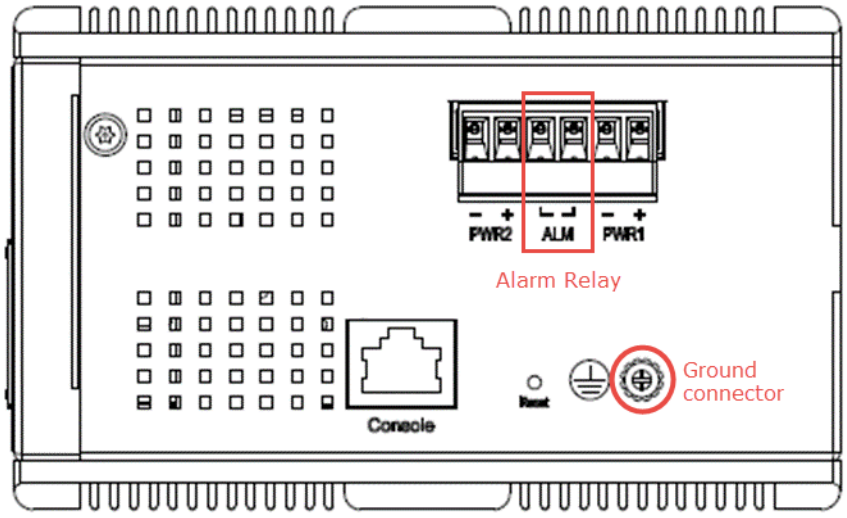


Figure 4: Alarm Relay and Ground Connector

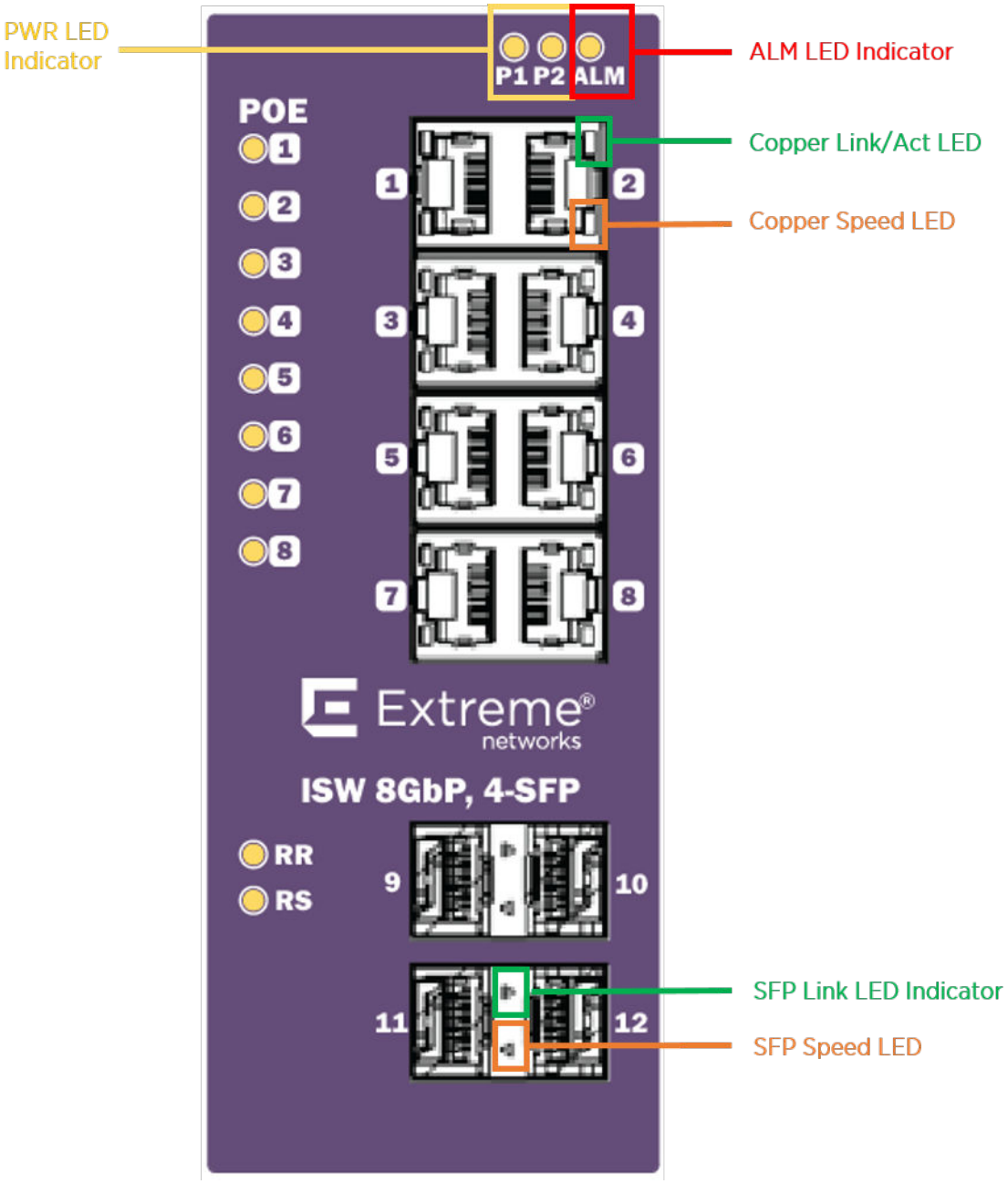
LED Status Indicators

Table 3: LED Status Indicators

LED	State	Description
P1	On Green	P1 power line has power
	Off	P1 power line disconnect or does not have supply power
P2	On Green	P2 power line has power
	Off	P2 power line disconnect or does not have supply power
Alarm	On Red	Alarm event occurs
	Off	No alarm
Copper ports Link/Act	On Green	Ethernet link up but no traffic is detected
	Flashing Green	Ethernet link up and there is traffic detected
	Off	Ethernet link down
Copper ports Speed	On Yellow	A 100 Mbps or a 1000 Mbps connection is detected
	Off	No link or a 10 Mbps connection is detected
SFP port Link/Act	On Green	Ethernet link up
	Off	Ethernet link down
SFP port Speed	On Yellow	SFP port speed 1000 Mbps connection is detected.
	Off	No link or a SFP port speed 100Mbps connection is detected

Table 3: LED Status Indicators (continued)

LED	State	Description
RR (Redundant Role)	On	Redundant Master (Ring Master, Ring Coupling Backup, Dual Homing, Chain Head, Balancing Chain Central Block) is enabled in the system.
	Off	No Redundant Master is enabled in the system.
RS (Redundant Status)	On	1 If any Ring port links are down, the RS LED will be ON. 2 If the device has any of Redundant Master (Ring Master, Ring Coupling Backup, Dual Homing, Chain Head, Balancing Chain Central Block) and detects a Ring/ Coupling/Dual Homing/Chain/Balancing Chain failure (any node is link down), and then RS LED will be ON.
	Off	All of the Ring ports are link up or Ring/ Coupling/Dual Homing/Chain/Balancing Chain is healthy.


PWR LED Indicator
P1 P2 ALM
ALM LED Indicator
Copper Link/Act LED
Copper Speed LED
POE
1
2
3
4
5
6
7
8
Extreme networks
ISW 8GbP, 4-SFP
RR
RS
9
10
11
12
SFP Link LED Indicator
SFP Speed LED

2 Installation

Mounting the ISW (DIN-Rail)

Mounting steps:

1 Screw the DIN-Rail bracket on with the bracket and screws in the accessory kit.
2 Hook the unit over the DIN rail.
3 Push the bottom of the unit towards the DIN Rail until it snaps into place.

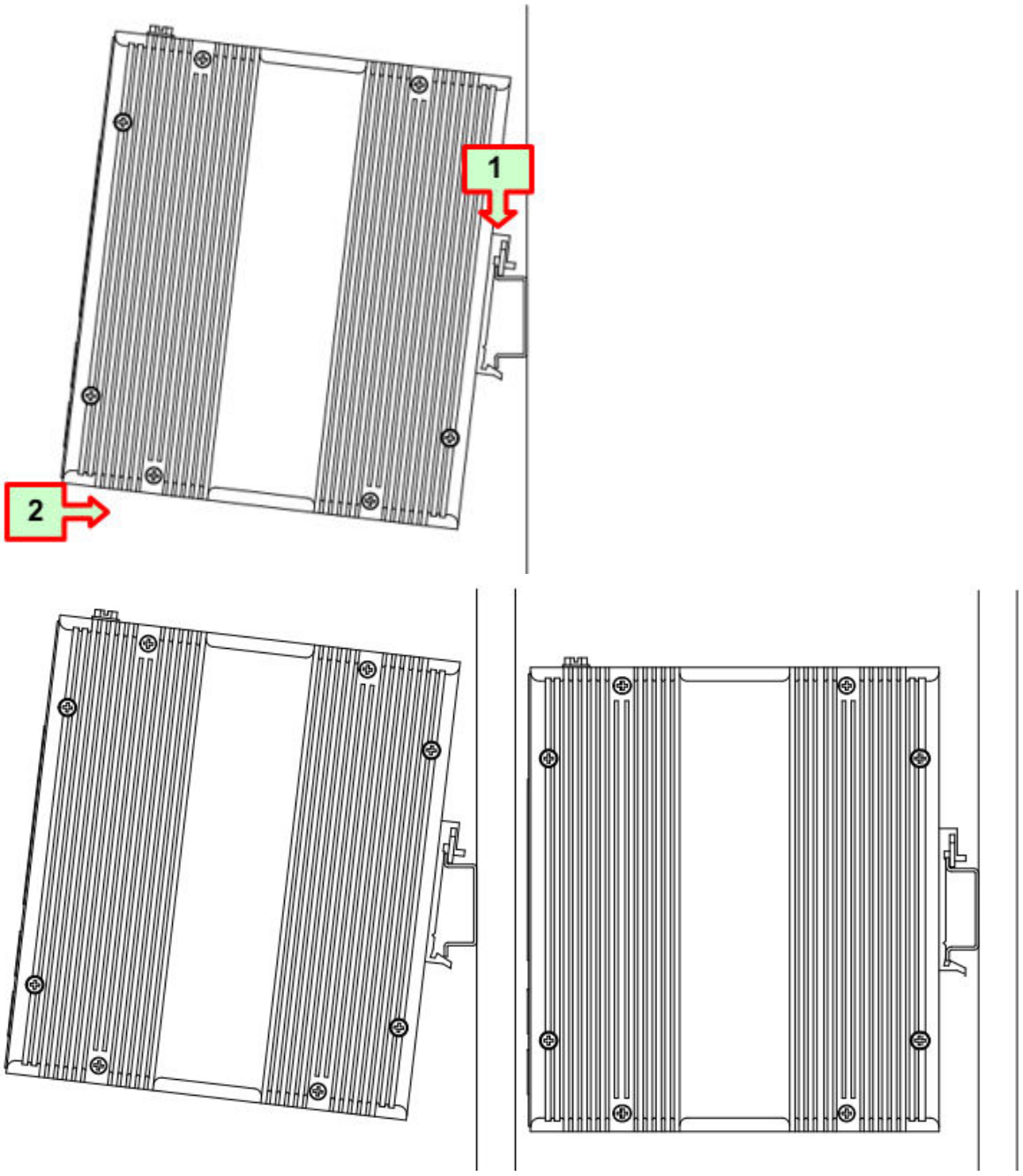
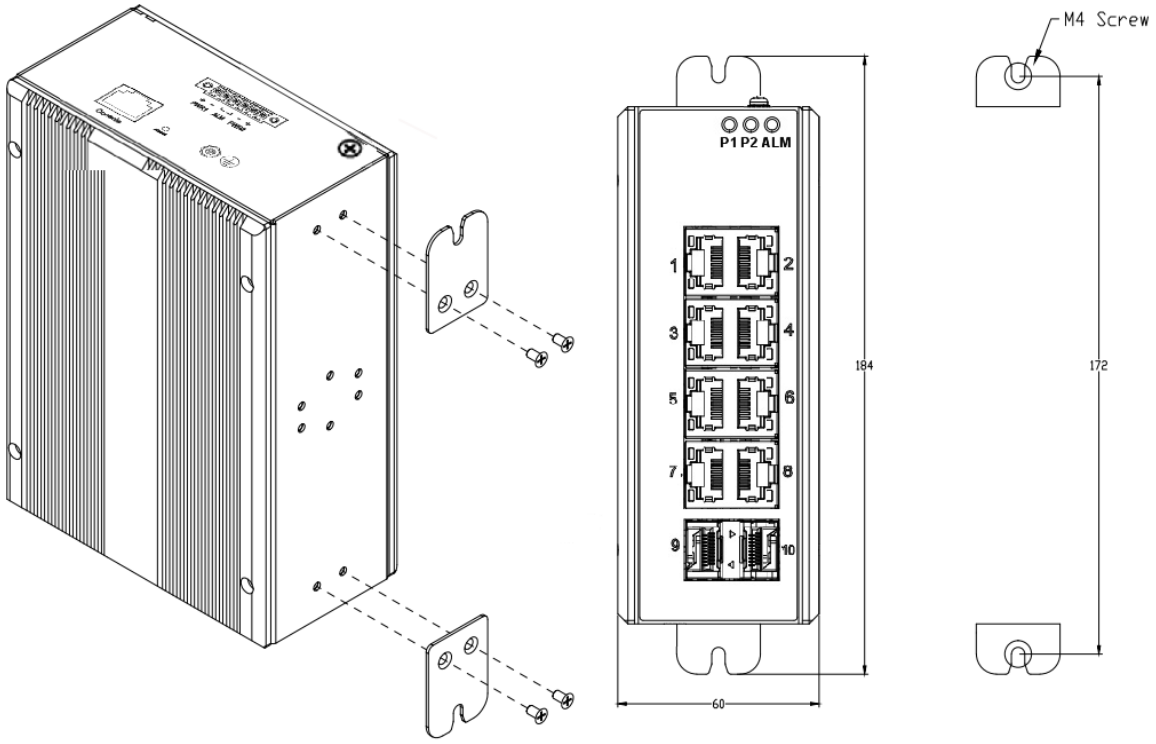


Figure 5: DIN-Rail Mounting

Mounting the ISW (Wall)

Attach the wall-mounting plates with the screws provided in the accessory kit.



Connecting the Ethernet Interface (RJ45 Ethernet)

ISW provides two types of electrical (RJ45) and optical (mini-GBIC) interfaces.

- To connect to a PC, use a straight-through or a cross-over Ethernet cable.
- To connect the ISW copper port to an Ethernet device, use UTP (Unshielded Twisted Pair) or STP (Shielded Twisted Pair) Ethernet cables.

The pin assignment of RJ45 connector is shown in Figure 6 and Table 4

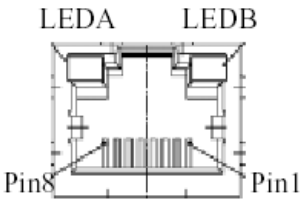


Figure 6: RJ45 Connector Pins

Table 4: RJ45 Connector Pin Assignment

Pin	Assignment	PoE Assignment
1, 2	T/Rx+, T/Rx-	Positive VPort
3, 6	T/Rx+, T/Rx-	Negative VPort
4, 5	T/Rx+, T/Rx-	X
7, 8	T/Rx+, T/Rx-	X

Connecting the Ethernet Interface (Fiber)

For both 100/1000 Mbps fiber speed connections, the SFP slots are available. The SFP slot accepts the fiber transceivers that typically have an LC connector.

The fiber transceivers have options of multimode, single mode, long-haul, or special-application transceivers.

Prepare a proper SFP module and install it into the optical port. Then you can connect fiber optics cabling that uses LC connectors or SC connectors (with the use of an optional SC-to-LC adapter) to the fiber optics connector.

Refer to LED Status Indicators on page 12 for the normal operational LED status.

Figure 7: Fiber optics cable with LC duplex connector

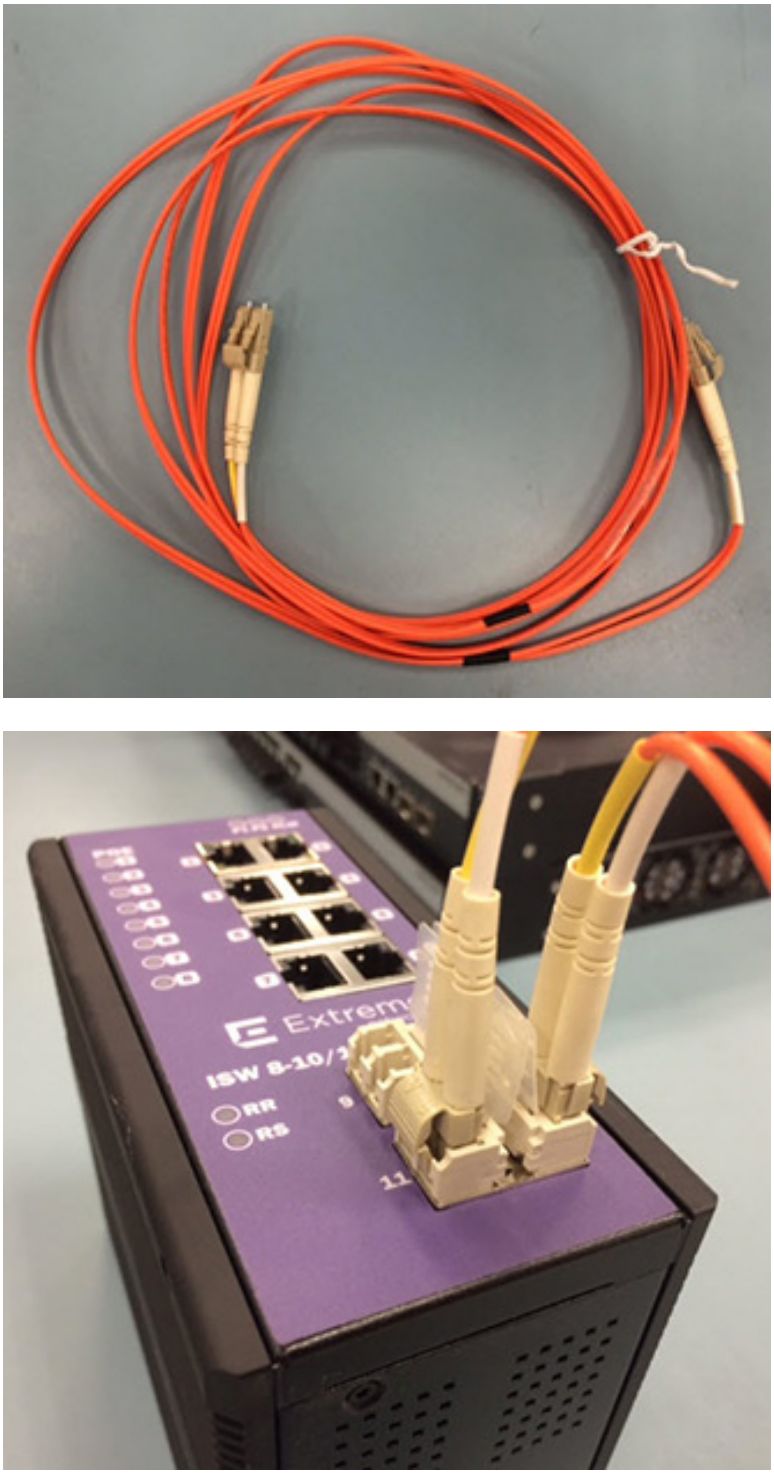


Figure 8: Connect the optical fiber to the SFP socket

Danger

Never attempt to view optical connectors that might be emitting laser energy.

Do not power up the laser product without connecting the laser to the optical fiber and putting the cover in position, as laser outputs will emit infrared laser light at this point.

Connecting the Power Terminal Block

The DC power interface is a 6-pin terminal block with polarity signs on the top panel. The ISW can be powered from two power supply (input range 12V – 58V). The DC power connector is a 6-pin terminal block; there is alarm contact on the middle terminal block.

The switch can be powered from two power supplies (input range 12V – 58V). Insert the positive and negative wires into V+ and V- contacts on the terminal block respectively and tighten the wire-clamp screws to prevent the wires from being loosened.

Note
The DC power should be connected to a well-fused power supply.

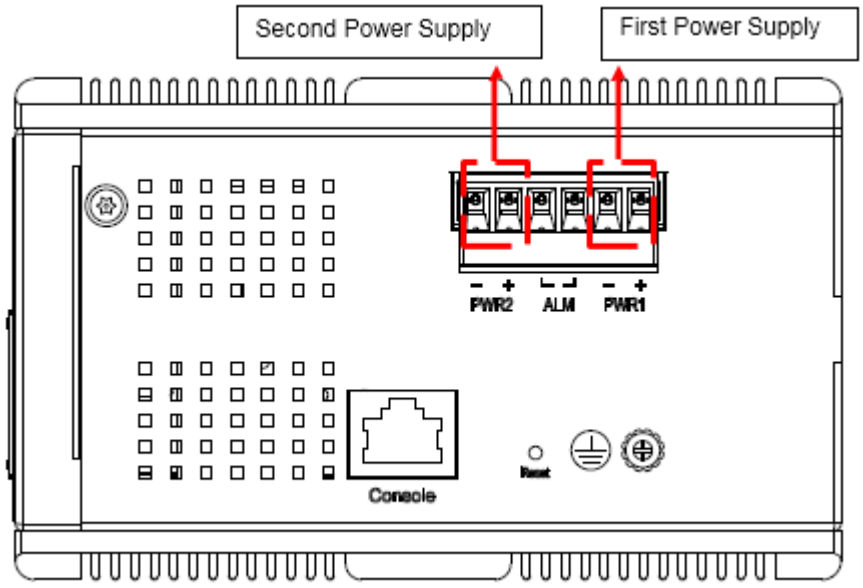


Figure 9: Power Supplies

Power Connector (6P Terminal Block)	
Input	DC 12-58V
PWR1 +/-	Power Input 1 +/-
PWR2 +/-	Power Input 2 +/-
ALM	Alarm relay output

Console Connection

The Console port is for local management by using a terminal emulator or a computer with terminal emulation software.

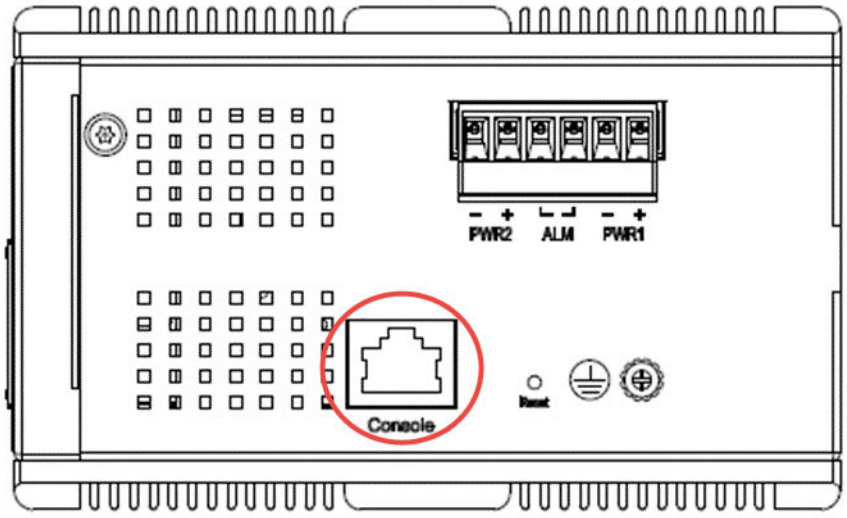


Figure 10: ISW Console Port

To connect the host PC to the switch, use the supplied RJ45 (male) connector-to-RS232 DB9 (female) connector. Connect the RJ45 connector to the switch's Console port shown in Figure 10, and then connect the DB9 connector to the PC COM port.

Important
Using a different cable than the one provided with the switch may cause bootup issues.

Once the host PC is connected to the switch, enter the following terminal settings:

- **Speed (baud rate):** 115200 bps
- **Data bits:** 8
- **Stop bits:** 1
- **Parity:** None
- **Flow control:** None

The pin assignment of the Console cable is shown in Figure 11.

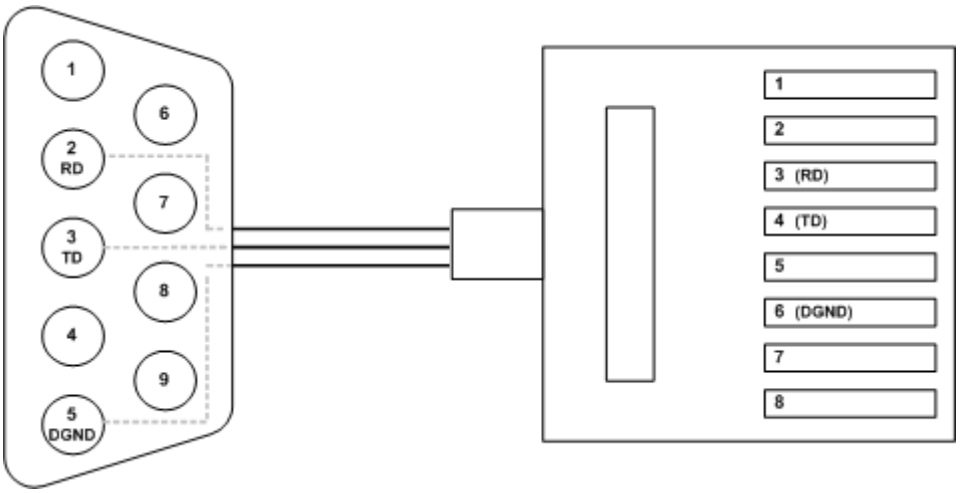


Figure 11: Console Cable Pin Assignment

3 Configuration

Connecting & Logging in to the Switch

Connecting & Logging in to the Switch

1 Connect to ISW Ethernet port (RJ45 Ethernet port) using factory default IP: `192.0.2.1`.

2 Log in with default account and password (`admin / [none]`)

3 Optional: Change the IP with commands listed below:

```
enable
configure terminal
interface vlan 1
ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
exit
```

4 To log in to the web interface, enter your switch's IP address in a web browser.

Refer to Web Browser Support on page 23 to ensure your browser is supported.

5 Enter the account name and password.

6 Click **Sign in**.

For information on configuring and monitoring the switch through the web interface, see the *ISW-Series Managed Industrial Ethernet Switch Web Configuration Guide*.

Web Browser Support

Internet Explorer

IE 7 (or newer version) with the following default settings is recommended:

Language script	Latin based
Web page font	Times New Roman
Plain text font	Courier New
Encoding	Unicode (UTF-8)
Text size	Medium

Firefox

Firefox with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	16

Chrome

Google Chrome with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	Medium

A Regulatory and Compliance Information

Federal Communications Commission (FCC) Notice

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note

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 uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

Warning

Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada NoticeCAN ICES-3 (A)/NMB-3(A)

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

Product Safety

This product complies with the following international safety standards:

- UL 60950-1 2nd edition, A2:2014
- CAN/CSA-C22.2 No.60950-1-07 2nd Ed. 2014-10
- IEC 60950-1:2005 2nd+A1:2009+A2:2013
- EN 60950-1:2006+A11+A1+A12+A2
- 2014/35/EU (2006/95/EC will invalid by 20 April 2016)

Electromagnetic Compatibility (EMC)

This product complies with the following:

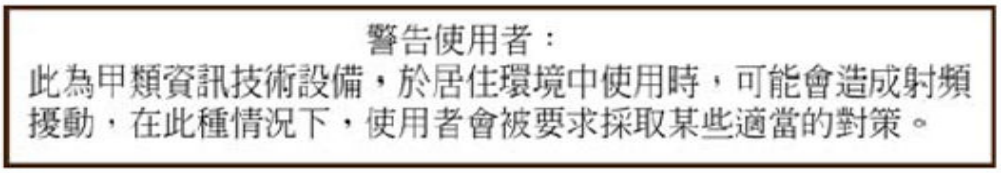
FCC 47 CFR Part 15 Subpart B Class A (US), ICES-003 (Canada)
EN 55022 (ITE Emissions), EN 55024 (ITE Immunity)
2014/30/EU (EMC Directive), EN 50121-1: 2017, EN 50121-4: 2016, EN 55011(ISM)
EN 61000-6-2 (Ind. Immunity), EN61000-6-4 Ind. Emissions)
EN 61000-3-2: 2014, EN 61000-3-3: 2013
RCM (Australia), MSIP KCC (Korea), BSMI (Taiwan)

Korea EMC Statement (KCC)

이 기기는 업무용(A급) 전자파적합기기로서 판매자
또는 사용자는 이 점을 주의 하시기 바라며, 가정
외의 지역에서 사용하는 것을 목적으로 합니다.

BSMI EMC Statement - Taiwan

This is a Class A product. In a domestic environemnt this product may cause radio interference in which case the user may be required to take adequate measurers.



Glossary

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *IBSS (Independent Basic Service Set)*.

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable

from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also *PEAP (Protected Extensible Authentication Protocol)*.)

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

Extreme Access Control

EAC, formerly NAC™, featuring both physical and virtual appliances, is a pre- and post-connect solution for wired and wireless LAN and VPN users. Using Identity and Access appliances and/or Identity and Access Virtual Appliance with the *Extreme Management Center* software, you can ensure only the right users have access to the right information from the right place at the right time. EAC is tightly integrated with the Intrusion Prevention System (IPS) and Security Information and Event Manager (SIEM) to deliver best-in-class post-connect access control. Learn more about EAC at http://www.extremenetworks.com/product/extreme-access-control/.

Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used.

This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at http://www.extremenetworks.com/product/extremeanalytics/.

Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at http://www.extremenetworks.com/product/management-center/.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: Modular (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); Stackable (X-series and A, B, C, and 7100 series switches); Standalone (SSA, X430, and D, 200, 800, and ISW series); and Mobile Backhaul (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time

over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.
Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also *EAP-TLS/EAP-TTLS*.)

PoE

The Power over Ethernet standard (IEEE 802.3af) defines how power can be provided to network devices over existing Ethernet connections, eliminating the need for additional external power supplies.

QoS

Quality of Service is a technique that is used to manage network resources and guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution.

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A

device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

VLAN

The term VLAN is used to refer to a collection of devices that communicate as if they are on the same physical LAN. Any set of ports (including all ports on the switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the CLI.