OmniSwitch 6350
Hardware Users Guide

Alcatel·Lucent
Enterprise

www.al-enterprise.com

This user guide documents OmniSwitch 6350 hardware, including chassis and associated components. The specifications described in this guide are subject to change without notice.

Alcatel·Lucent
Enterprise

26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500 FAX (818) 880-3505

Service & Support Contact Information
North America: 800-995-2696
Latin America: 877-919-9526
EMEA: +800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific: +65 6240 8484
Web: businessportal2.alcatel-lucent.com
Email: ebg_global_supportcenter@al-enterprise.com

Contents

About This Guide

This *OmniSwitch 6350 Hardware Users Guide* describes your switch hardware components and basic switch hardware procedures.

Supported Platforms

The information in this guide applies to the following products:

- OS6350-10
- OS6350-P10
- OS6350-24
- OS6350-P24
- OS6350-48
- OS6350-P48

Who Should Read this Manual?

The audience for this users guide is network administrators and IT support personnel who need to config-
ure, maintain, and monitor switches and routers in a live network. However, anyone wishing to gain
knowledge on the OmniSwitch 6350 hardware will benefit from the material in this guide.

When Should I Read this Manual?

Read this guide as soon as you are ready to familiarize yourself with your switch hardware components.
You should have already stepped through the first login procedures.

You should already be familiar with the very basics of the switch hardware, such as module LEDs and
module installation procedures. This manual will help you understand your switch hardware components
(e.g., chassis, cables, power supplies, etc.) in greater depth.

What is in this Manual?

This users guide includes the following hardware-related information:

• Descriptions of switch configurations.

• Descriptions of "availability" features.

• Descriptions of chassis types.

• Instructions for mounting the chassis.

• Descriptions of hardware components (status LEDs, chassis, cables, etc.).

• Managing a chassis.

• Hardware-related Command Line Interface (CLI) commands

What is Not in this Manual?

The descriptive and procedural information in this manual focuses on switch hardware. It includes infor-
mation on some CLI commands that pertain directly to hardware configuration, but it is not intended as a
software users guide. There are several OmniSwitch 6350 users guides that focus on switch software
configuration. Consult those guides for detailed information and examples for configuring your switch
software to operate in a live network environment. See "Documentation Roadmap" on page -xi and
"Related Documentation" on page -xiii for further information on software configuration guides available
for your switch.

How is the Information Organized?

This users guide provides an overview of OmniSwitch 6350 switches, specifications of the hardware
components, steps for setting up and managing OmniSwitch 6350 switches, and an overview and proce-
dures for managing Power over Ethernet (PoE).

Documentation Roadmap

The OmniSwitch user documentation suite was designed to supply you with information at several critical junctures of the configuration process.The following section outlines a roadmap of the manuals that will help you at each stage of the configuration process. Under each stage, we point you to the manual or manuals that will be most helpful to you.

Stage 1: Using the Switch for the First Time

Pertinent Documentation: *Getting Started Chapter*
Release Notes

The *Getting Started* chapter in this manual provides all the information you need to get your switch up and running the first time. This chapter provides information on unpacking the switch, installing power supplies, unlocking access control, setting the switch's IP address, and setting up a password. It also includes succinct overview information on fundamental aspects of the switch, such as hardware LEDs, the software directory structure, CLI conventions, and web-based management.

At this time you should also familiarize yourself with the Release Notes that accompanied your switch. This document includes important information on feature limitations that are not included in other user guides.

Stage 2: Gaining Familiarity with Basic Switch Functions

Pertinent Documentation: *Hardware Users Guide*
Switch Management Guide

Once you have your switch up and running, you will want to begin investigating basic aspects of its hard ware and software. Information about switch hardware is provided in the *Hardware Users Guide*. This guide provides specifications, illustrations, and descriptions of all hardware components—e.g., chassis, power supplies, etc.

The *Switch Management Guide* is the primary user guide for the basic software features on a switch. This guide contains information on the switch directory structure, basic file and directory utilities, switch access security, SNMP, and web-based management. It is recommended that you read this guide before connecting your switch to the network.

Stage 3: Integrating the Switch Into a Network

Pertinent Documentation: *Network Configuration Guide*

When you are ready to connect your switch to the network, you will need to learn how the OmniSwitch implements fundamental software features, such as 802.1Q, VLANs, and Spanning Tree. The *Network Configuration Guide* contains overview information, procedures and examples on how standard networking technologies are configured in the OmniSwitch.

Anytime

The *CLI Reference Guide* contains comprehensive information on all CLI commands supported by the switch. This guide includes syntax, default, usage, example, related CLI command, and CLI-to-MIB variable mapping information for all CLI commands supported by the switch. This guide can be consulted anytime during the configuration process to find detailed and specific information on each CLI command.

Related Documentation

The following are the titles and descriptions of OmniSwitch 6350-related user manuals:

- *OmniSwitch 6350 Hardware Users Guide*

  Detailed technical specifications and procedures for the OmniSwitch chassis and components.

- *OmniSwitch AOS Release 6 CLI Reference Guide*

  Complete reference to all CLI commands supported on OmniSwitch products. Includes syntax definitions, default values, examples, usage guidelines and CLI-to-MIB variable mappings.

- *OmniSwitch AOS Release 6 Switch Management Guide*

  Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, image rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).

- *OmniSwitch AOS Release 6 Network Configuration Guide*

  Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols, such as RIP), security options (authenticated VLANs), Quality of Service (QoS), and link aggregation.

- *OmniSwitch AOS Release 6 Transceivers Guide*

  Includes transceiver specifications and product compatibility information.

- Technical Tips, Field Notices

  Includes information published by Alcatel-Lucent's Customer Support group.

- *Release Notes and Upgrade Instructions*

  Includes open problem reports, feature exceptions, and other important information on the features supported in the current release and any limitations to their support.

Published / Latest Product Documentation

All user guides for the OmniSwitch Series are included on the Alcatel-Lucent public website. This website also includes user guides for other Alcatel-Lucent Enterprise products.

The latest user guides can be found on our website at: businessportal2.alcatel-lucent.com

Technical Support

An Alcatel-Lucent Enterprise service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel-Lucent Enterprise product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners. Additionally, with 24-hour-a-day access to Alcatel-Lucent's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel-Lucent's technical support, open a new case or access helpful release notes, technical bulletins, and manuals. For more information on Alcatel-Lucent Enterprise's Service Programs, see our web page at businessportal2.alcatel-lucent.com, call us at 1-800-995-2696, or email us at ebg_global_supportcenter@al-enterprise.com.

1 OmniSwitch 6350 Switches

OmniSwitch 6350 switches are fixed-configuration Gigabit Ethernet switches available in 10-, 24-, and 48-port models. Options also include 10-, 24-, and 48-port Power-over-Ethernet (PoE). All models provide internal AC power.

Chassis Configurations

10-Port Models

- OmniSwitch 6350-10: Provides eight (8) 10/100/1000 BaseT ports; two (2) RJ-45/SFP combo ports. The chassis features fanless design and internal AC power.

- OmniSwitch 6350-P10: Provides eight (8) 10/100/1000 BaseT PoE ports; two (2) RJ-45/SFP combo ports. The chassis features fanless design and internal AC power.

24-Port Models

- OmniSwitch 6350-24: Provides 24 10/100/1000 BaseT ports and four (4) fixed SFP ports. The chassis features fanless design and internal AC power.

- OmniSwitch 6350-P24: Provides 24 PoE 10/100/1000 PoE ports and four (4) fixed SFP ports. The chassis provides three (3) fans and internal AC power.

48-Port Models

- OmniSwitch 6350-48: Provides 48 10/100/1000 BaseT ports and four (4) fixed SFP ports. The chassis provides one (1) fan and internal AC power.

- OmniSwitch 6350-P48: Provides 48 10/100/1000 PoE ports and four (4) fixed SFP ports. The chassis provides four (4) fans and internal AC power.

OmniSwitch 6350 Feature Overview

Security Features

OmniSwitch 6350 switches offer security features for network access control, policy enforcement and attack containment, enabling fully secure networks and OmniVista Network Management System (NMS) support.

Availability Features

OmniSwitch 6350 switches incorporate advanced Alcatel-Lucent Operating System (AOS) protocols to ensure high availability for mission critical applications. Availability features are hardware- and software-based safeguards that help to prevent the loss of data flow in the unlikely event of a subsystem failure.

In addition, some availability features allow users to maintain or replace hardware components without powering off the switch or interrupting switch operations. Combined, these features provide added resiliency and help to ensure that the switch or virtual chassis is consistently available for high-impact network operations.

Hardware-related availability features include:

- **Software Rollback**
- **Hot Swapping**
- **Hardware Monitoring**

Software Rollback

Software rollback (also referred to as *image rollback*) essentially allows the switch to return to a prior "last known good" version of software in the event of a system software problem. The switch controls software rollback through its resilient directory structure design (i.e., **/flash/working** and **/flash/certified**).

For detailed information on the software rollback feature, as well as the switch's **/flash/working** and **/flash/certified** directories, refer to the "Managing CMM Directory Content" chapter in the *Switch Management Guide*.

Hot Swapping

Hot swapping refers to the action of adding, removing, or replacing components without powering off switches or disrupting other components.This feature facilitates hardware upgrades and maintenance and allows users to easily replace components in the unlikely event of hardware failure.

The following components can be hot swapped:

- SFP transceivers. Refer to *OmniSwitch 6350 Transceivers Guide* for more information.

Hardware Monitoring

Automatic Monitoring

Automatic monitoring refers to the switch's built-in sensors that automatically monitor operations. If an error is detected (e.g., over-threshold temperature), the switch immediately sends a trap to the user. The trap is displayed on the console in the form of a text error message.

LEDs

LEDs, which provide visual status information, are provided on the chassis front panel. LEDs are used to indicate conditions such as hardware and software status, temperature errors, link integrity, data flow, etc. For detailed LED descriptions, refer to Chapter 3, "OmniSwitch 6350 Chassis and Hardware Components."

User-Driven Monitoring

User-driven hardware monitoring refers to CLI commands that are entered by the user in order to access the current status of hardware components. The user enters "show" commands that output information to the console. Monitoring information for chassis components, such as the optional back up power supply, chassis temperature sensor, and chassis fans is provided in Chapter 3, "OmniSwitch 6350 Chassis and Hardware Components." The show commands for all the features are described in detail in the *CLI Reference Guide*.

2   Getting Started

Installing the Hardware

Items Required

- Grounding wrist strap
- Phillips screwdriver
- Flat-blade screwdriver

Site Preparation

Environmental Requirements

OmniSwitch 6350 switches have the following environmental and airflow requirements:

- The installation site must maintain a temperature between 0° and 45° Celsius (32° and 113° Fahrenheit) and not exceed 95 percent maximum humidity (non-condensing) at any time.

- Be sure to allow adequate room for proper air ventilation at the front, back, and sides of the switch. Refer to "Airflow Considerations" on page 2-5 for minimum clearance requirements. No clearance is necessary at the top or bottom of the chassis.

Electrical Requirements

Note. Alcatel-Lucent switches must be installed by a professional installer. It is the responsibility of the installer to ensure that proper grounding is available and that the installation meets applicable local and national electrical codes.

Reliable Earthing

Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch (e.g., use of power strips).

OmniSwitch 6350 switches have the following general electrical requirements:

- Each switch requires one grounded electrical outlet *for each power supply installed in the chassis.*

- OmniSwitch 6350 switches offer both AC and DC power supply support.

- For switches using AC power connections, each supplied AC power cord is 2 meters (approx. 6.5 feet). Do not use extension cords.

    Redundant AC Power. It is recommended that each AC outlet resides on a separate circuit. With redundant AC power, if a single circuit fails, the switch's remaining power supplies (on separate circuits) can remain operational.

For switches using DC power, refer to the "DC Power Supply Connections" for more information.

Electrical Surge Warning

In order to help protect equipment against electrical surges please take note of the following recommendations and guidelines:

1. Earth grounding of all devices is fundamental to ensure long term reliability.

- All electrical equipment must be installed by a qualified, licensed electrician.

- Every power supply that is connected to building power should be earth grounded.

- Earth grounding for the power cable, should be verified to be 0.01 ohm or less.

- Each switch should be grounded to same earth ground as the power supply.

- Each powered device, such as an AP or camera, should be connected to earth ground.

- Each surge suppression device should be connected to earth ground.

2. Shielded cables (STP) offer some minimal level of additional protection over unshielded Ethernet cables (UTP) but the use of a surge protector is still recommended.

- It is suggested to use STP Cat5e or better for 1Gbps Ethernet switches for any outdoor application or applications where Ethernet cables come in close proximity to alternating current conductors.

- Always install cables according to manufacturer requirements.

3. For any connections where integrity of the cabling within a building ground is questionable (i.e outdoor connections), copper Ethernet ports must be connected with an appropriate surge protection device, inline, between the PSE and PD per the manufacturer's recommendations for connection and grounding.

4. Caution should be taken for any cable connected to any outdoor device, not only on the device grounding, but to ensure that any outdoor device cables that could carry surge currents, do not pass those surge currents to upstream Ethernet switches.

    Caution - Category 5e, Category 6, and Category 6a cables can store large amounts of static electricity due to the dielectric properties of their construction materials in addition, this build up of electricity could lead to a Cable Discharge Event (CDE). A CDE can occur due to the differential in charges on the cable and the equipment it's being connected to. It is recommended that installers momentarily ground all copper Ethernet cables (especially in new cable runs) to a suitable and safe earth ground before connecting them to the port.

Unpacking and Installing the Switch

To protect your switch components from damage, read all unpacking recommendations and instructions carefully before beginning.

Unpack your OmniSwitch 6350 chassis as close as possible to the location where it will be installed.

Items Included

Your OmniSwitch 6350 includes the following items:

- OmniSwitch chassis
- Transceivers, per order
- Rack mount brackets
- Country-specific power cord(s)
- Assorted instructional cards, anti-static bags and additional packaging

Weight Considerations

Check the specifications table for the OmniSwitch 6350 being installed for chassis weights.

Airflow Considerations

To ensure proper airflow, be sure that your switch is placed in a well-ventilated area and provide minimum recommended clearance at the front, back and sides of the switch.

Never obstruct chassis air vents.

Rear. 6 inches minimum at rear of chassis.

Sides. 2 inches minimum at left and right sides.

Front. 6 inches minimum at front of chassis.
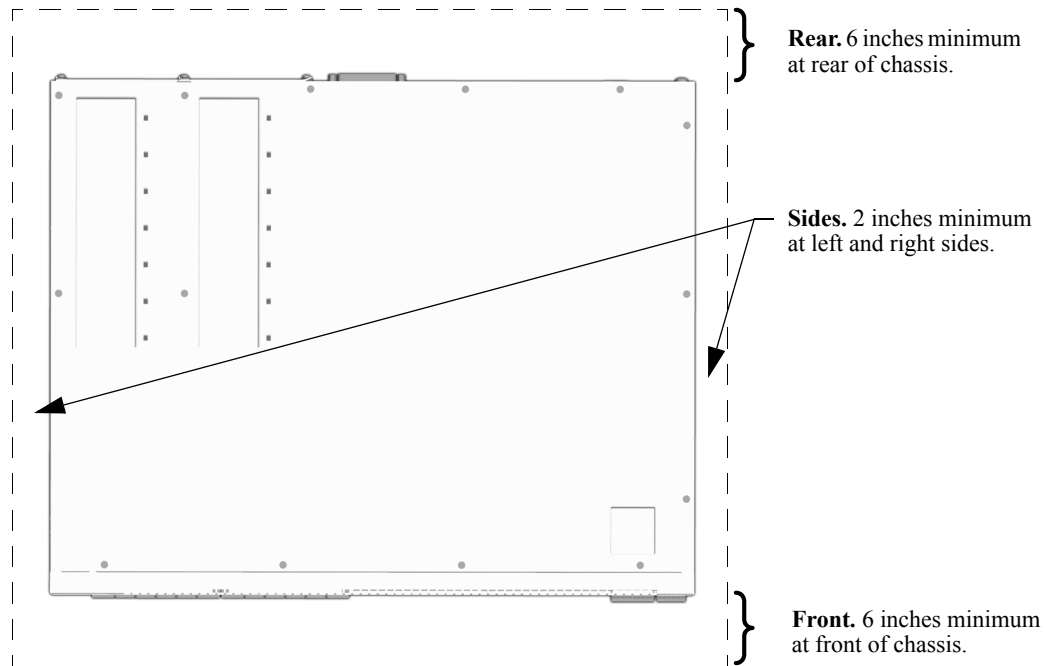
Chassis Top View

Note. Clearance is not required at the top and bottom of the chassis.

Mounting the Switch

For information on mounting OmniSwitch 6350 switches, refer to Chapter 3, "OmniSwitch 6350 Chassis and Hardware Components."

Connections and Cabling

Once your switch is properly installed, you should connect all network and management cables required for your network applications. Connections may include:

- DB9-to-RJ-45 cable to the console connector

- Cables to 10/100/1000 Ethernet or SFP ports

Note. For additional information on cabling connections, refer to the *OmniSwitch AOS Release 6 Switch Management Guide.*

Serial Connection to the Console Port

The console port provides a serial connection to the switch using a USB connector and is required when logging into the switch for the first time. By default, this connector provides a DCE console connection.

Serial Connection Default Settings

baud rate	9600
parity	none
data bits (word size)	8
stop bits	1

For information on modifying these settings, refer to the *Switch Management Guide.*

Booting the Switch

Now that you have installed the switch components and connected network and management cables, you can boot the switch. To boot the switch, plug the power supply cord into an easily-accessible, properly grounded power outlet. (Do not use extension cords.) The switch will power on and boot automatically.

Note. For a few seconds, at the beginning of the boot up process, random characters may briefly display on the console of an OS6350. This is due to an initial baud rate mismatch. As soon as the bootrom is initialized, the issue is automatically resolved.

Component LEDs

During the boot process, component LEDs will flash and change color, indicating different stages of the boot. Following a successful boot, chassis LEDs will vary based on chassis mode, for example:

OK1	Solid Green
PRI	Solid or blinking / green or amber (mode dependent)
PWR	Solid Green

Note. The LEDs will vary based on the chassis mode. For information on LED states, refer to "OmniSwitch 6350 LED Status" on page 3-21. If the LEDs do not display as indicated following a complete boot sequence, contact Alcatel-Lucent Enterprise Customer Support.

Once the switch has completely booted and you have accessed your computer's terminal emulation software via the console port, you are ready to log in to the switch's Command Line Interface (CLI) and configure basic information. Continue to "Your First Login Session" on page 2-8.

Your First Login Session

In order to complete the setup process for the switch, you must complete the following steps during your first login session:

- Log in to the switch

- Unlock session types

- Change the login password

- Set the date and time

- Set optional system information

- Save your changes

Important. You must be connected to the switch via the console port before initiating your first login session.

Logging In to the Switch

When you first log in to the switch, you will be prompted for a login name and password. Use the switch's default settings:

- Login: **admin**

- Password: **switch**

The default welcome banner, which includes information such as the current software version and system date, is displayed followed by the CLI command prompt:

```
Welcome to the Alcatel-Lucent OmniSwitch 6350
Software Version 6.7.1.80.R01 Development, July 08, 2015.

Copyright(c), ALE USA Inc., 2015. All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel-Lucent Enterprise registered
in the United States Patent and Trademark Office.

->
```

Note. A user account includes a login name, password, and user privileges. Privileges determine whether the user has read or write access to the switch and which commands the user is authorized to execute. For detailed information on setting up and modifying user accounts, refer to the *Switch Management Guide.*

Unlocking Session Types

Security is a key feature on OmniSwitch 6350 switches. As described on page 2-8, when you access the switch for the first time, you must use a *direct console port connection*. All other session types (Telnet, FTP, WebView, and SNMP) are locked out until they are manually unlocked by the user.

The CLI command used to unlock session types is **aaa authentication**.

Note. When you unlock session types, you are granting switch access to non-local sessions (e.g., Telnet). As a result, users who know the correct user login and password will have remote access to the switch. For more information on switch security, refer to the *Switch Management Guide.*

Unlocking All Session Types

To unlock all session types, enter the following command syntax at the CLI prompt:

```
-> aaa authentication default local
```

Unlocking Specified Session Types

You can also unlock session types on a one-by-one basis. For example, to unlock Telnet sessions only, enter the following command:

```
-> aaa authentication telnet local
```

To unlock WebView (HTTP) sessions only, enter the following command:

```
-> aaa authentication http local
```

You cannot specify more than one session type in a single command line. However, you can still unlock multiple session types by using the **aaa authentication** command in succession. For example:

```
-> aaa authentication http local
-> aaa authentication telnet local
-> aaa authentication ftp local
```

Refer to the *CLI Reference Guide* for complete **aaa authentication** command syntax options.

Changing the Login Password

Change the login password for **admin** user sessions by following the steps below:

1 Be sure that you have logged into the switch as user type **admin** (see "Logging In to the Switch" on page 2-8).

2 Enter the keyword **password** and press **Enter**.

3 Enter your new password at the prompt.

Note. Be sure to remember or securely record all new passwords; overriding configured passwords on an OmniSwitch is restricted.

---

4 You will be prompted to re-enter the password. Enter the password a second time.

New password settings are automatically saved in real time to the local user database; the user is not required to enter an additional command in order to save the password information. Also note that new password information is retained following a reboot. All subsequent login sessions, including those through the console port, will require the new password to access the switch.

For detailed information on managing login information, including user names and passwords, refer to the *Switch Management Guide*.

Setting the System Time Zone

The switch's default time zone is UTC. If you require a time zone that is specific to your region, or if you need to enable Daylight Savings Time (DST) on the switch, you can configure these settings via the **system timezone** and **system daylight-savings-time** commands.

For detailed information on configuring a time zone for the switch, refer to the *Switch Management Guide*.

Setting the Date and Time

Set the current time for the switch by entering **system time**, followed by the current time in *hh:mm:ss*.

To set the current date for the switch, enter **system date**, followed by the current date in *mm/dd/yyyy*.

Setting Optional Parameters

Specifying an Administrative Contact

An administrative contact is the person or department in charge of the switch. If a contact is specified, users can easily find the appropriate network administrator if they have questions or comments about the switch.

To specify an administrative contact, use the **system contact** command.

Specifying a System Name

The system name is a simple, user-defined text description for the switch.

To specify a system name, use the **system name** command.

Specifying the Switch's Location

It is recommended that you use a physical labeling system for locating and identifying your switch(es). Examples include placing a sticker or placard with a unique identifier (e.g., the switch's default IP address) on each chassis.

However, if no labeling system has been implemented or if you need to determine a switch's location from a remote site, entering a system location can be very useful.

To specify a system location, use the **system location** command.

Viewing Your Changes

To view your current changes, enter **show system** at the CLI prompt.

Saving Your Changes

Once you have configured this basic switch information, save your changes by entering **write memory** at the CLI command prompt.

3 OmniSwitch 6350 Chassis and Hardware Components

OmniSwitch 6350 (OS6350) switches are available in the chassis configurations as shown in the table below:

OS6350-10	Eight (8) 10/100/1000 BaseT ports; two (2) RJ-45/SFP combo ports; fanless design; internal AC power.
OS6350-P10	Eight (8) 10/100/1000 BaseT PoE ports; two (2) RJ-45/SFP combo ports; fanless design; internal AC power.
OS6350-24	(24) 10/100/1000 BaseT ports; four (4) fixed SFP ports; fanless design; internal AC power.
OS6350-P24	(24) PoE 10/100/1000 BaseT ports; four (4) fixed SFP ports; three (3) fans; internal AC power.
OS6350-48	(48) 10/100/1000 BaseT ports; four (4) fixed SFP ports; one (1) fan; internal AC power.
OS6350-P48	(48) 10/100/1000 BaseT PoE ports; four (4) fixed SFP ports; four (4) fans; internal AC power.

This chapter includes detailed information on these chassis types. Topics include:

- OmniSwitch 6350 chassis descriptions
- Technical specifications
- Power Supplies
- Cables and power cords
- Console port and pinout specifications

OmniSwitch 6350-10

Chassis Features

System status LEDs   Internal AC Power Supply

(8) 10/100/1000Base-T Ports   Console port (RJ-45)

(2) RJ-45/SFP 10/100/1000 combo ports   USB port (USB 2.0)
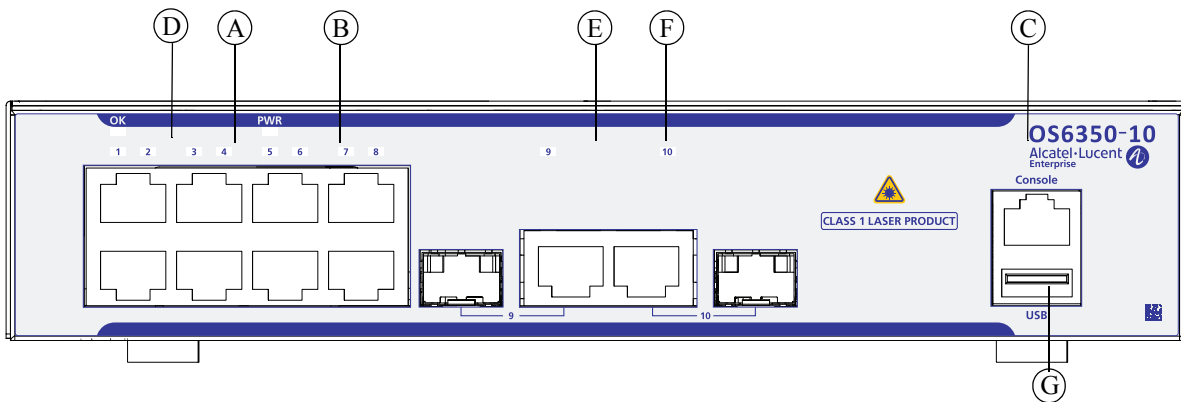
Front Panel

OmniSwitch 6350-10 Front Panel

Item	Description
A	(8) 10/100/1000Base-T Ports
B	Ethernet Port Status LEDs
C	Console Port
D	System Status LEDs
E	(2) RJ-45/SFP 10/100/1000 combo ports
F	Combo Port Status LEDs
G	USB Port

Refer to for LED status information.

OmniSwitch 6350-10 Rear Panel

Note. The figure shows a pre-production version of the chassis without product, safety, and compliance information labels. All production versions of the chassis have these labels.

OmniSwitch 6350-10 Rear Panel

Item	Description
A	**Power Supply Connector** Internal AC power supply.
B	**Grounding Block** Type LCD8-10A-L grounding lug

OmniSwitch 6350-10 Specifications	
Fans	None
Power Supplies	One (1) internal power supply
Rack Unit Dimensions	1 RU
Dimensions (WxHxD)	21.5 cm (8.50 in) x 4.4 cm (1.73 in) x 29.21 cm (11.5 in)
Weight	1.97 kg (4.34 lb)
Operating Temperature	0˚C to +45˚C (32˚F to +113˚F)
Storage Temperature	-40˚C to +75˚C (-40˚F to +167˚F)
Upper Threshold Temperature	71˚C
Danger Threshold Temperature	80˚C
Operating and Storage Humidity	5% to 95% non-condensing
Acoustic (dB)	0
RJ-45 10/100/1000 Ports	8
RJ-45/SFP 10/100/1000 Combo Ports	2
PoE Ports	N/A
PoE Power Budget	N/A

OmniSwitch 6350-10 Specifications	
Input Voltage	100 VAC to 240 VAC, 0.9 A, 50-60 Hz
Output Voltage	12 VDC, 2.5 A
Max Power	30 W

OmniSwitch 6350-P10

Chassis Features

System status LEDs   Internal AC Power Supply

(8) 10/100/1000Base-T PoE ports   Console port (RJ-45)

(2) RJ-45/SFP 10/100/1000 combo ports   USB port (USB 2.0)
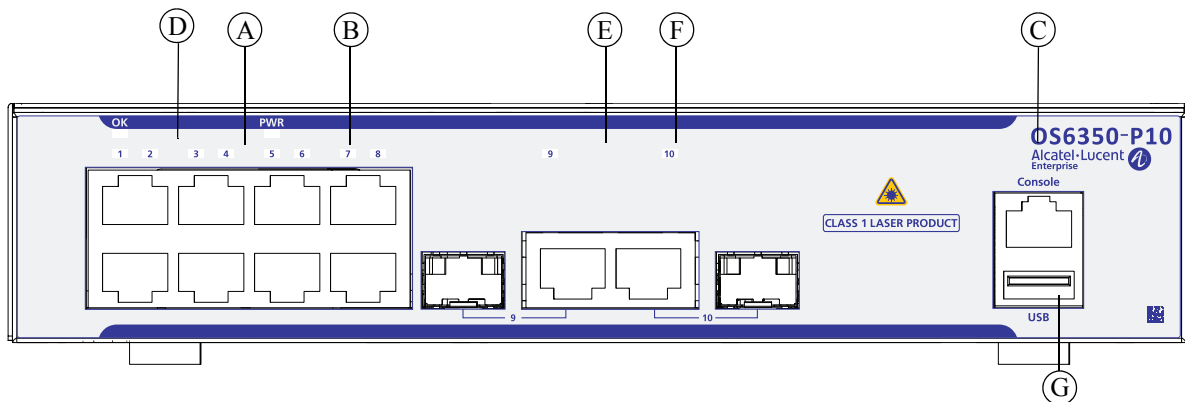
Front Panel

OmniSwitch 6350-P10 Front Panel

Item	Description
A	(8) 10/100/1000 Power over Ethernet (PoE) Ports
B	Ethernet Port Status LEDs
C	Console Port
D	System Status LEDs
E	(2) RJ-45/SFP 10/100/1000 combo ports
F	Combo Port Status LEDs
G	USB Port

Refer to for LED status information.

OmniSwitch 6350-P10 Rear Panel

Note. The figure shows a pre-production version of the chassis without product, safety, and compliance information labels. All production versions of the chassis have these labels.

OmniSwitch 6350-P10 Rear Panel

Item	Description
A	**Power Supply Connector** Internal AC power supply.
B	**Grounding Block** Type LCD8-10A-L grounding lug

OmniSwitch 6350-P10 Specifications	
Fans	None
Power Supplies	One (1) internal power supply
Rack Unit Dimensions	1 RU
Dimensions (WxHxD)	21.5 cm (8.50 in) x 4.4 cm (1.73 in) x 29.21 cm (11.5 in)
Weight	1.97 kg (4.34 lb)
Operating Temperature	0˚C to +45˚C (32˚F to +113˚F)
Storage Temperature	-40˚C to +75˚C (-40˚F to +167˚F)
Upper Threshold Temperature	73˚C
Danger Threshold Temperature	82˚C
Operating and Storage Humidity	5% to 95% non-condensing
Acoustic (dB)	0
RJ-45 10/100/1000 Ports	8
RJ-45/SFP 10/100/1000 Combo Ports	2
PoE Ports	8
PoE Power Budget	120W

OmniSwitch 6350-P10 Specifications	
Input Voltage	100 VAC to 240 VAC, 2.2 A, 50-60 Hz
Output Voltage	54.5 VDC, 2.5 A
Max Power	150 W (30 W System Power; 120 W PoE Power)

OmniSwitch 6350-24

Chassis Features

System status LEDs   Internal AC Power Supply

(24) 10/100/1000Base-T Ports   Console port (RJ-45)

(4) Non-combo SFP Ports   USB port (USB 2.0)
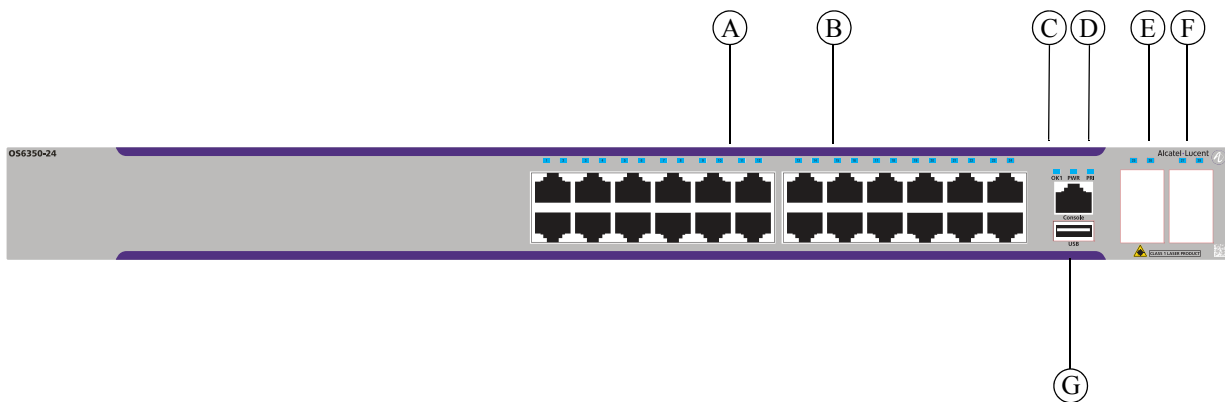
Front Panel

OmniSwitch 6350-24 Front Panel

Item	Description
A	(24) 10/100/1000 BaseT Ethernet Ports
B	Ethernet Port Status LEDs
C	Console Port
D	System Status LEDs
E	Four (4) Fixed SFP Ports
F	SFP Port Status LEDs
G	USB Port

Refer to "OmniSwitch 6350 LED Status" on page 3-21 for LED status information.

OmniSwitch 6350-24 Rear Panel

Note. The figure shows a pre-production version of the chassis without product, safety, and compliance information labels. All production versions of the chassis have these labels.
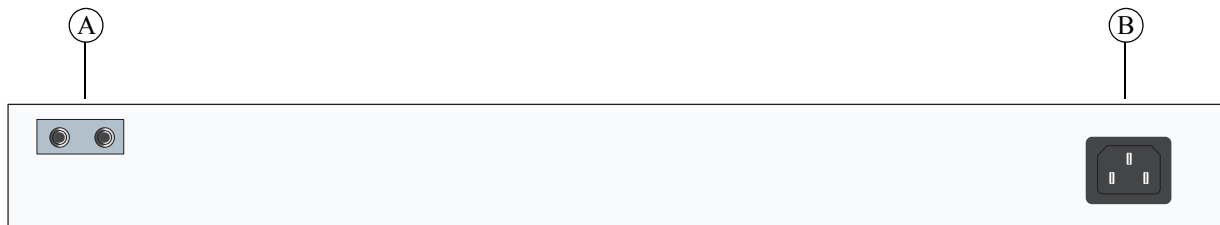
OmniSwitch 6350-24 Rear Panel

Item	Description
A	**Grounding Block** Type LCD8-10A-L grounding lug
B	**Power Supply Connector** Internal AC power supply.

OmniSwitch 6350-24 Internal AC Power Supply

P/S Component	Description
Model	OmniSwitch 6350-24
Nominal Input Voltage	100-240 VAC
Maximum Output Power	30 W
Output Voltage	12V DC

OS6350-24 Specifications

10/100/1000BaseT ports	24
SFP ports	4
Chassis Width	44.0 cm (17.32 in)
Chassis Height	4.4 cm (1.73 in) (1 RU)
Chassis Depth	25.2 cm (9.92 in)
Weight	4.08 kg (9.0 lb)
Operating Humidity	5% to 95%
Storage Humidity	5% to 95%
Operating Temperature	0C to +45C
Storage Temperature	-40C to +75C
Upper Threshold Temperature	75C
Danger Threshold Temperature	80C

OmniSwitch 6350-P24

Chassis Features

System status LEDs   Internal AC Power Supply

(24) 10/100/1000Base-T PoE ports   Console port (RJ-45)

(4) Non-combo SFP Ports   USB port (USB 2.0)
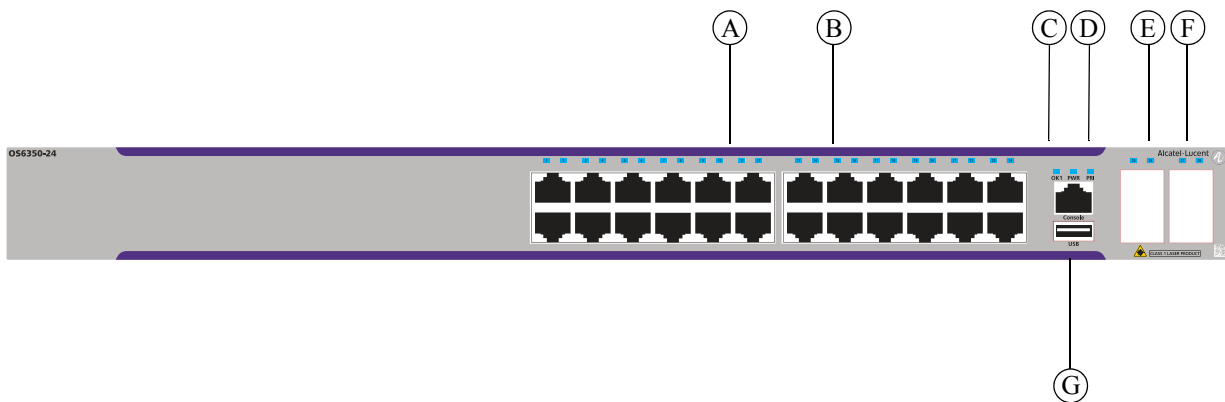
Front Panel

OmniSwitch 6350-P24 Front Panel

Item	Description
A	(24) 10/100/1000 Power over Ethernet (PoE) Ports
B	Ethernet Port Status LEDs
C	Console Port
D	System Status LEDs
E	Four (4) Fixed SFP Ports
F	SFP Port Status LEDs
G	USB Port

Refer to "OmniSwitch 6350 LED Status" on page 3-21 for LED status information.

OmniSwitch 6350-P24 Rear Panel

Note. The figure shows a pre-production version of the chassis without product, safety, and compliance information labels. All production versions of the chassis have these labels.

OmniSwitch 6350-P24 Rear Panel

Item	Description
A	**Grounding Block** Type LCD8-10A-L grounding lug
B	**Power Supply Connector** Internal AC power supply.

OmniSwitch 6350-P24 Internal AC Power Supply

P/S Component	Description
Model	OmniSwitch 6350-P24
Nominal Input Voltage	100-240 VAC
Maximum Output Power	525 W
PoE Power Budget	380 W
Output Voltage	12V DC/54V DC

OmniSwitch 6350-P24 Specifications

Standard(s) Supported	802.3at
10/100/1000BaseT Power over Ethernet (PoE) Ports	24
SFP ports	4
Chassis Width	44.0 cm (17.32 in)
Total Power Budget	525 W
System Power Budget	145 W
PoE Power Budget	380 W
Chassis Height	4.4 cm (1.73 in) (1 RU)
Chassis Depth	25.2 cm (9.92 in)
Weight	5.05 kg (11.0 lb)
Operating Humidity	5% to 95%
Storage Humidity	5% to 95%
Operating Temperature	0C to +45C
Storage Temperature	-40C to +75C
Upper Threshold Temperature	60C
Danger Threshold Temperature	65C

OmniSwitch 6350-48

Chassis Features

System status LEDs   Internal AC Power Supply

(48) 10/100/1000Base-T Ports   Console port (RJ-45)

(4) Non-combo SFP Ports   USB port (USB 2.0)
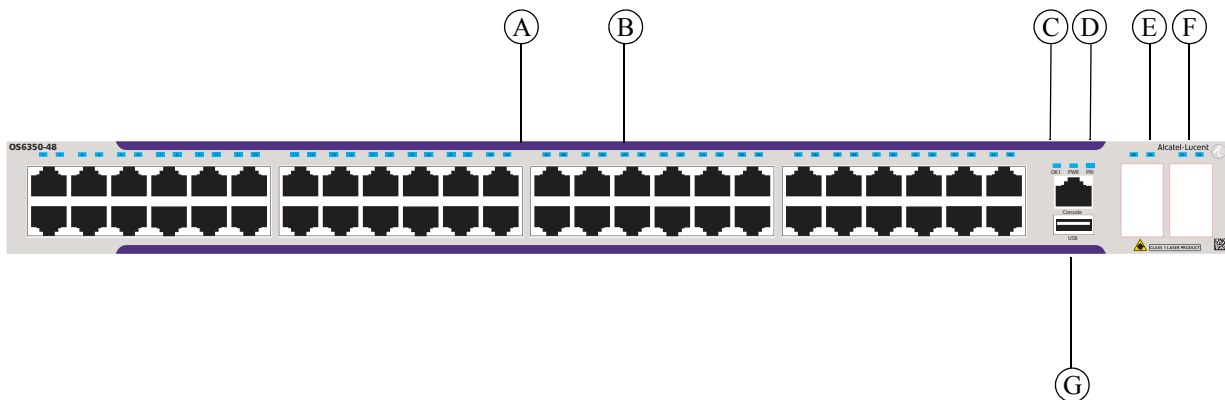
Front Panel

OmniSwitch 6350-48 Front Panel

Item	Description
A	(48) 10/100/1000 BaseT Ports
B	Ethernet Port Status LEDs
C	Console Port
D	System Status LEDs
E	Four (4) Fixed SFP Ports
F	SFP Port Status LEDs
G	USB Port

Refer to "OmniSwitch 6350 LED Status" on page 3-21 for LED status information.

OmniSwitch 6350-48 Rear Panel

Note. The figure shows a pre-production version of the chassis without product, safety, and compliance information labels. All production versions of the chassis have these labels.
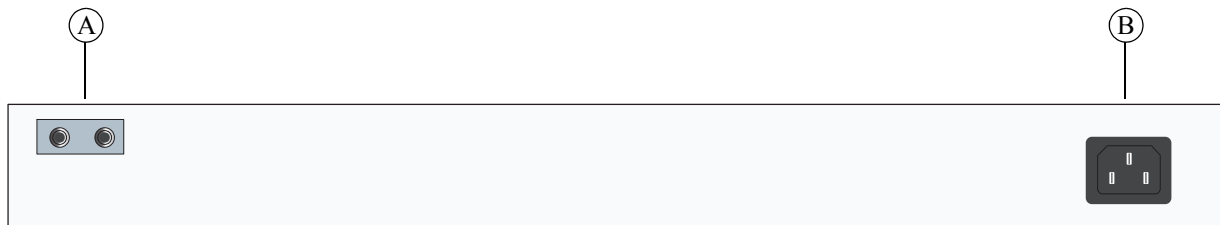
OmniSwitch 6350-48 Rear Panel

Item	Description
A	**Grounding Block** Type LCD8-10A-L grounding lug
B	**Power Supply Connector** Internal AC power supply.

OmniSwitch 6350-48 Internal AC Power Supply

P/S Component	Description
Model	OmniSwitch 6350-48
Nominal Input Voltage	100-240 VAC
Maximum Output Power	60 W
Output Voltage	12V DC

OmniSwitch 6350-48 Specifications

10/100/1000BaseT ports	48
SFP ports	4
Chassis Width	44.0 cm (17.32 in)
Chassis Height	4.4 cm (1.73 in) (1 RU)
Chassis Depth	25.2 cm (9.92 in)
Weight	5.44 kg (12.0 lb)
Operating Humidity	5% to 95%
Storage Humidity	5% to 95%
Operating Temperature	0C to +45C
Storage Temperature	-40C to +75C
Upper Threshold Temperature	62C
Danger Threshold Temperature	67C

OmniSwitch 6350-P48

Chassis Features

System status LEDs   Internal AC Power Supply

(48) 10/100/1000Base-T PoE Ports   Console port (RJ-45)

(4) Non-combo SFP Ports   USB port (USB 2.0)
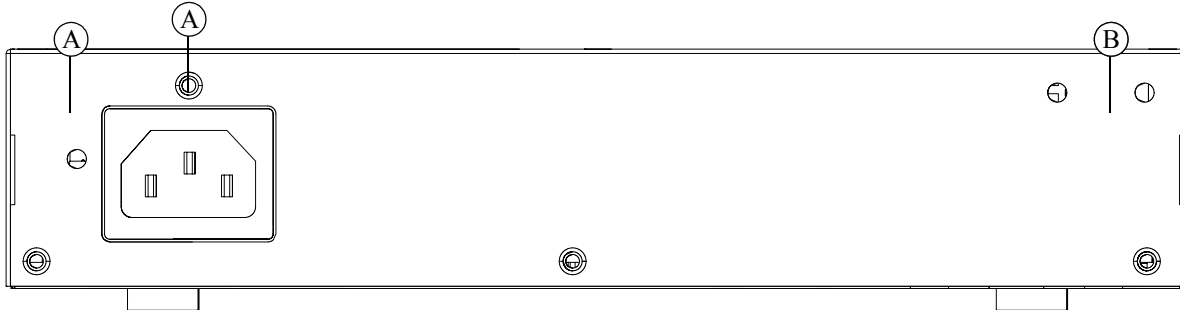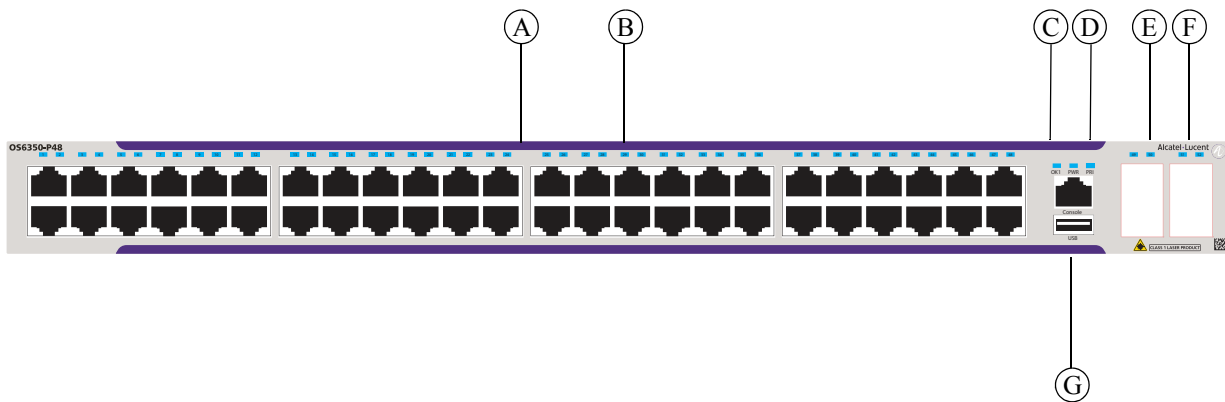
Front Panel

OmniSwitch 6350-P48 Front Panel

Item	Description
A	(48) 10/100/1000 BaseT Power over Ethernet (PoE) Ports
B	Ethernet Port Status LEDs
C	Console Port
D	System Status LEDs
E	Four (4) Fixed SFP Ports
F	SFP Port Status LEDs
G	USB Port

Refer to for LED status information.

OmniSwitch 6350-P48 Rear Panel

Note. The figure shows a pre-production version of the chassis without product, safety, and compliance information labels. All production versions of the chassis have these labels.

OmniSwitch 6350-P48 Rear Panel

Item	Description
A	**Grounding Block** Type LCD8-10A-L grounding lug
B	**Power Supply Connector** Internal AC power supply.

OmniSwitch 6350-P48 Internal AC Power Supply

P/S Component	Description
Model	OmniSwitch 6350-P48
Nominal Input Voltage	100-240 VAC
Maximum Output Power	900 W
PoE Power Budget	780 W
Output Voltage	12V DC/53V DC

OmniSwitch 6350-P48 Specifications

Standard(s) Supported	802.3at
10/100/1000BaseT Power over Ethernet (PoE) Ports	48
SFP ports	4
Chassis Width	44.0 cm (17.32 in)
Total Power Budget	900 W
System Power Budget	120 W
PoE Power Budget	780 W
Chassis Height	4.4 cm (1.73 in) (1 RU)
Chassis Depth	38.6 cm (15.20 in)
Weight	5.05 kg (11.0 lb)
Operating Humidity	5% to 95%
Storage Humidity	5% to 95%
Operating Temperature	0C to +45C
Storage Temperature	-40C to +75C
Upper Threshold Temperature	60C
Danger Threshold Temperature	65C

OmniSwitch 6350 LED Status

LED	State	Description
OK1	Solid Green	The switch has passed hardware diagnostic tests and the system software is operational
	Blinking Green	Normal diagnostics and/or Remote Config Load in progress
	Solid Amber	System fan failure or temperature threshold exceeded
PRI	Solid Green	Normal Operation (Standalone mode)
	Blinking Green	Normal Operation - Primary (Stackable mode - number of blinks indicates stack ID).
	Blinking Amber	Normal Operation - Non-primary (Stackable mode - number of blinks indicates stack ID).
PWR	Solid Green	P/S Normal Operation
	Solid Amber	P/S Present and Bad
	Off	P/S Not Present.
10/100/1000 Ports	Solid Green	Valid Link
	Blinking Green	Transmitting or receiving packets in a link up state for non-PoE
	Solid Amber	Valid PoE Link
	Blinking Amber	Transmitting or receiving packets in a link up state for PoE
	Off	No Link Detected
SFP Ports	Solid Green	Valid Link
	Blinking Green	Transmitting or receiving packets in a link up state
	Solid Amber	Active stacking port.
	Off	No Link Detected

AC Power Cords

Since the power cord is the switch's only disconnect device, it should be plugged into an easily accessible outlet. In the event that your power cord is lost or damaged, refer to the specifications below.

Specifications

The power cord included with this product contains three (3) insulated #18AWG stranded copper wires and is rated between 85-265 VAC (region dependent), 10 amps with a nominal length of 2 meters. The female end terminates in an IEC-60320-C13 attachment plug and the male end termination varies dependent upon region, as listed below.

European cords must be Harmonized (HAR) type. Refer to the information below for power plug types by region:

Power Cord Types	User Side Connectors
North America	NEMA 5-15-P
United Kingdom / Ireland	BS 1363 UK
Europe	CEE 7/7
Japan	JIS 8303
Australia	AS 3112
India	BS 546
Italy	CIE 23-16
Switzerland / Liechtenstein	SEV 1011
Denmark / Greenland	SRAF 1962 / DB 16/87
Argentina	A-10
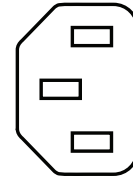
IEC-60320-C13

Power Cord Specifications

Console Port

The console port, located on the chassis front panel, provides a console connection to the switch and is required when logging into the switch for the first time. By default, this RJ-45 connector provides a DTE console connection.

Serial Connection Default Settings

The factory default settings for the serial connection are as follows:

baud rate	9600
parity	none
data bits (word size)	8
stop bits	1
flow control	none

Port Pinouts

RJ-45 Console Port – Connector Pinout

Pin Number	Signals as DTE Console Port
1	NC
2	NC
3	RXD
4	Ground
5	Ground
6	TXD
7	NC
8	NC

10/100 Ethernet Port – RJ-45 Pinout (non-PoE)

Pin Number	Description
1	RX+
2	RX-
3	TX+
4	not used
5	not used
6	TX-
7	not used
8	not used

Gigabit Ethernet Port – RJ-45 Pinout

Pin Number	Description
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-

10/100/1000 Mbps Power over Ethernet Port – RJ-45 Pinout

Pin Number	Description
1	RX+ (-VDC)
2	RX- (-VDC)
3	TX+ (+VDC)
4	
5	
6	TX- (+VDC)
7	
8	

Overtemp Condition

The OmniSwitch is designed to operate within a specified operating temperature as noted under the specifications section. However, in the event that the normal operating temperature of the switch is exceeded, the following will occur:

- Upon crossing the configured Upper Threshold, a trap will be sent. (See the *OmniSwitch AOS Release 6 Network Configuration Guide* for information on configuring switch thresholds.)

If the temperature continues to rise and reaches the Danger Threshold, the following will occur:

- OK1 LED will display solid Amber.

- The switch will automatically shutdown

- Once the temperature drops to an acceptable operating level, the switch will automatically restart.

Check the following if an overtemp condition exists:

- Verify that the switch is installed properly in an environment that adheres to the installation instructions in the following chapters.

- Verify proper airflow to the chassis.

- Time of the failure

Use the **snmp station** command and refer to the SNMP Configuration chapter for information on configuring an SNMP station.

4 Mounting OmniSwitch 6350 Switches

This chapter covers different mounting and installation options. OmniSwitch 6350 switches may be either table- or rack-mounted.

Anti-Static Warning. Before handling any components, free yourself of static by wearing a grounding strap or by grounding yourself properly. Static discharge can damage the switch and related components.

General Installation Recommendations

Airflow Recommendations

To ensure proper airflow, be sure that your switch is placed in a well-ventilated area and provide minimum recommended clearance at the front, back and sides of the switch, as shown below. Restricted airflow can cause your switch to overheat, which can lead to switch failure.

6 inches minimum at rear of chassis.

2 inches minimum at left and right sides.

6 inches minimum at front of chassis.
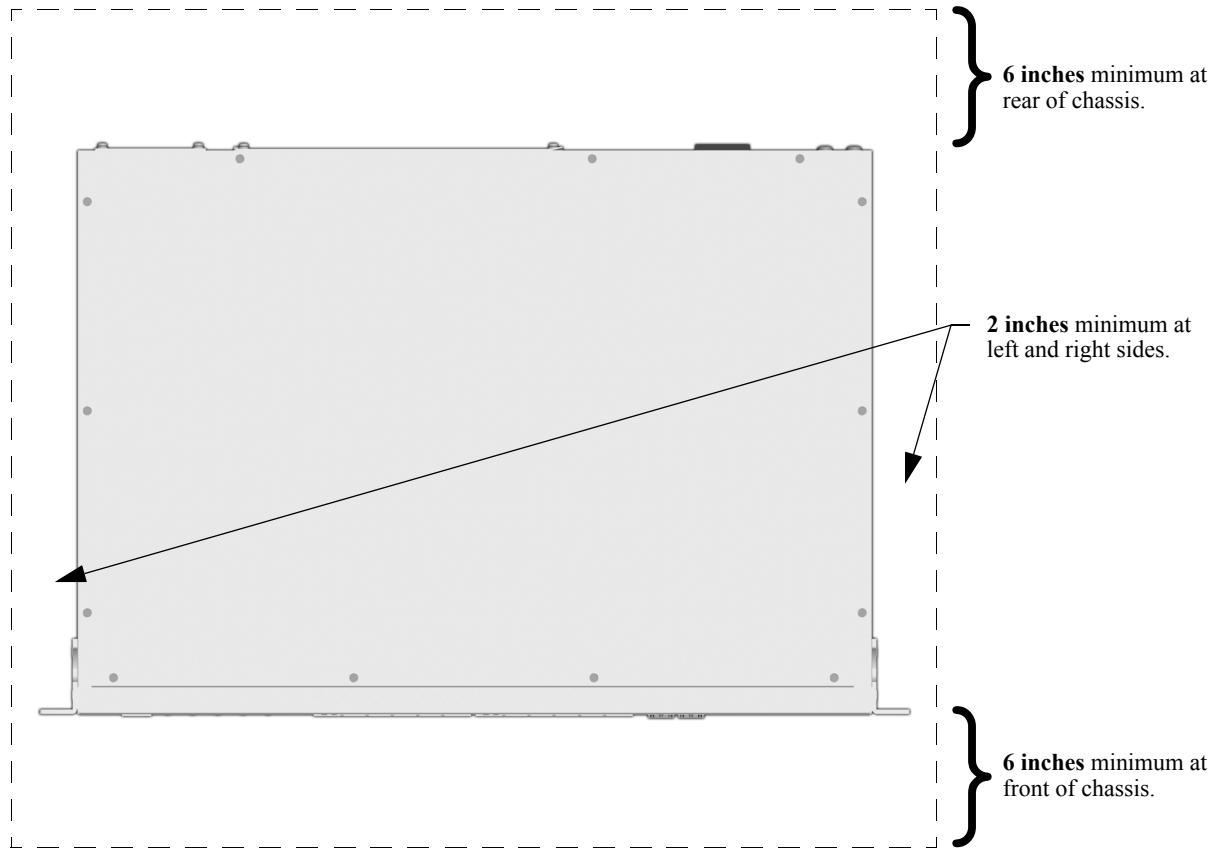
Note. Clearance is not required at the top and bottom of the chassis. Clearance recommendations at the front and rear of chassis are for access to cabling and components only and are not intended as a specific airflow requirement.

Reduced Air Flow

Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Elevated Operating Ambient Temperatures

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

Mechanical Loading

Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit Overloading

Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuit might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Earthing

Reliable earthing of rack-mount equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

General Table-Mounting Guidelines

OmniSwitch 6350 switches can be installed freestanding as tabletop-mounted units. If you will be table-mounting your switch(es), refer to the important guidelines below before installing.

- When choosing a location for the switch, be sure that adequate clearance has been provided for chassis airflow and access to the front, back, and sides of the chassis. For recommended clearances, refer to "Airflow Recommendations" on page 4-2.

- The power cord measures two (2) meters (approximately 6.5 feet) in length. When table mounting the switch, be sure that the mounting location is within the reach of all the required power sources.

Rack-Mounting

Refer to the following important guidelines before installing the chassis in a rack:

- Two people are required to rack mount the switch: One person to lift the chassis into position and one person to secure the chassis to the rack using the rack mount screws.

- The chassis has rack-mount flanges that support standard 19-inch rack mount installations.

- Alcatel-Lucent does not provide rack-mount screws. Use the screws supplied by the rack vendor.

- To prevent a rack from becoming top heavy, it is recommended that you install the switch at the bottom of the rack whenever possible.

Note. If you are installing the switch in a relay rack, be sure to install and secure the rack per rack manufacturer's specifications.

Installing Rack Mount Flanges

1 To install rack mount flanges, start by making sure the spring clip is in the out (disengaged) position.

2 Insert the tab into the chassis slot as shown.

Clip in "Out" (disengaged) position

Tab

Slot
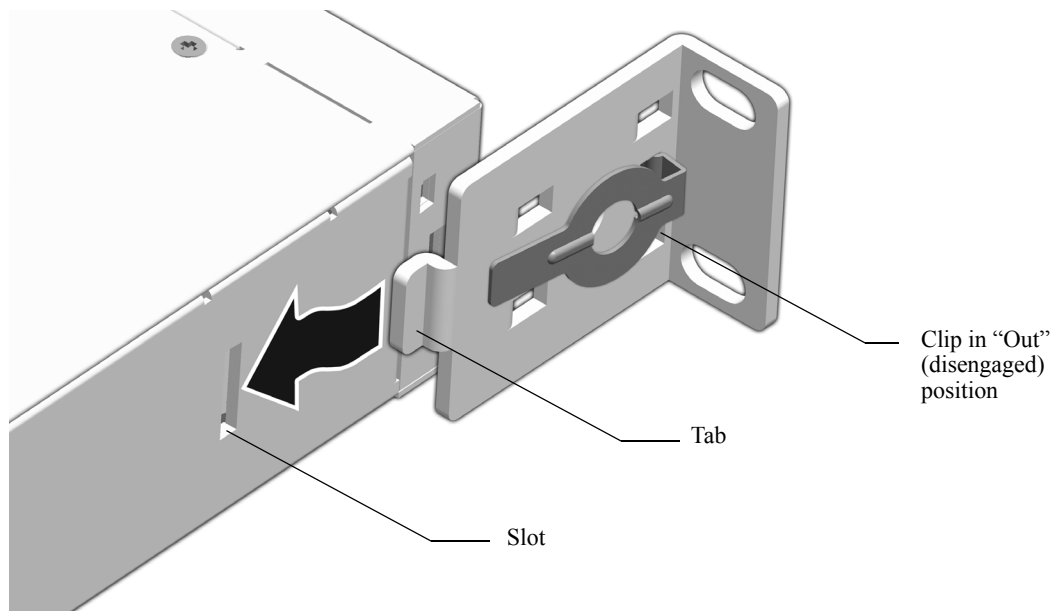
3 Press the flange and spring clip until the flange clicks into place and the clip is in the in (engaged) position.

Clip in "In"
(engaged)
position

"CLICK"
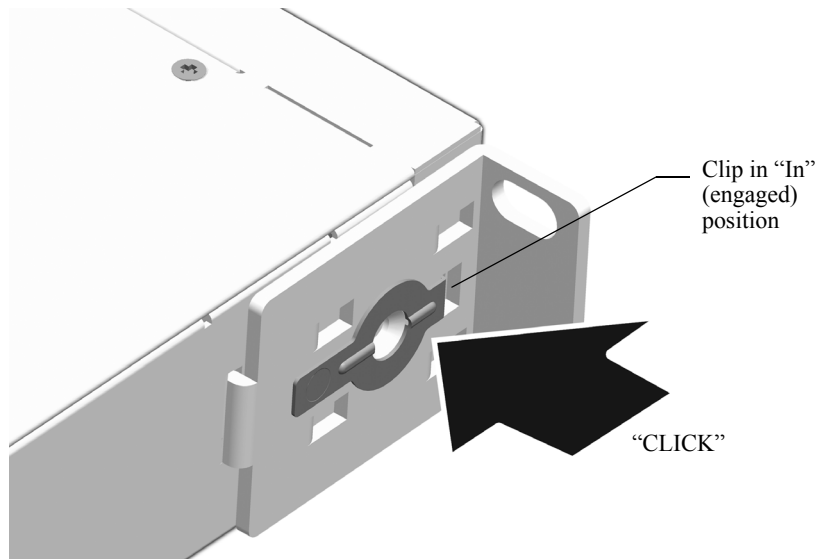
4 Secure the flange to the chassis using the attachment screw (provided).
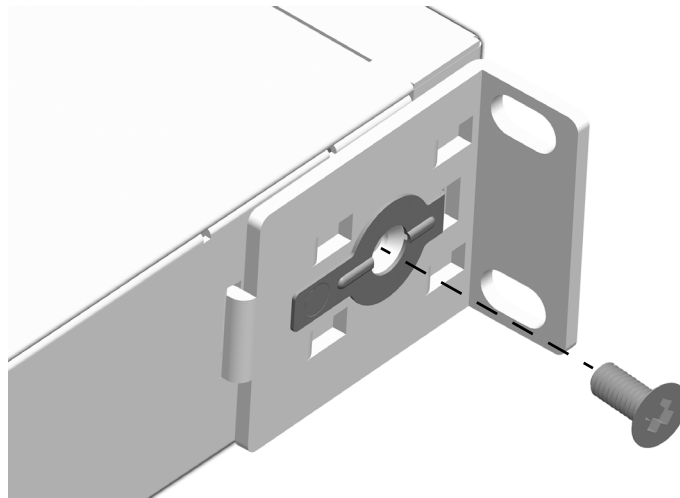
5 Repeat steps 1 through 4 for the flange on the opposite side of the chassis.

Installing the Chassis In the Rack

1 Mark the holes on the rack where the chassis is to be installed.

2 One person should lift and position the chassis until the rack-mount flanges are flush with the rack post.

3 Align the holes in the flanges with the rack holes marked in step 1.

4 Once the holes are aligned, the second person should insert a screw through the *bottom hole on each flange*. Tighten both screws until they are secure.
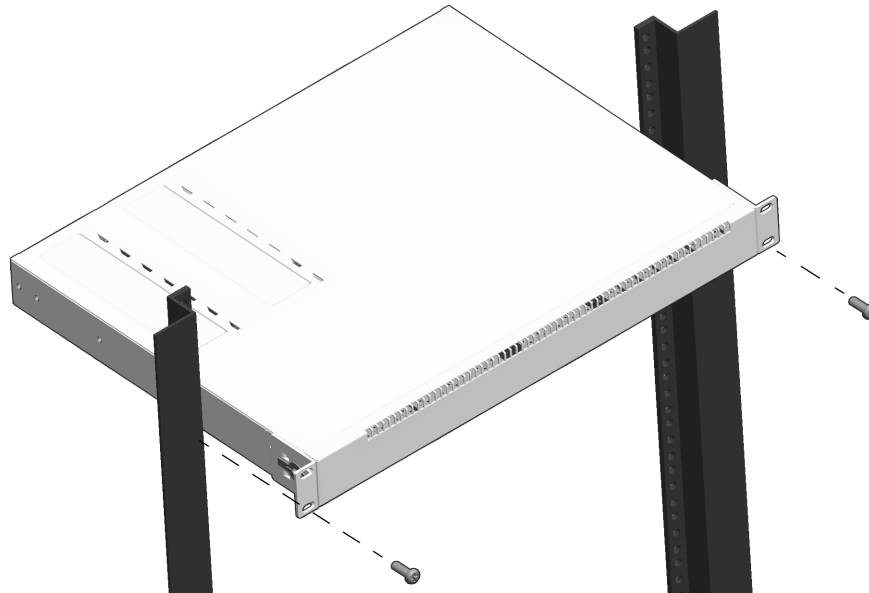
5 Install the remaining screws in the top hole of each flange. Be sure that all screws are securely tightened.
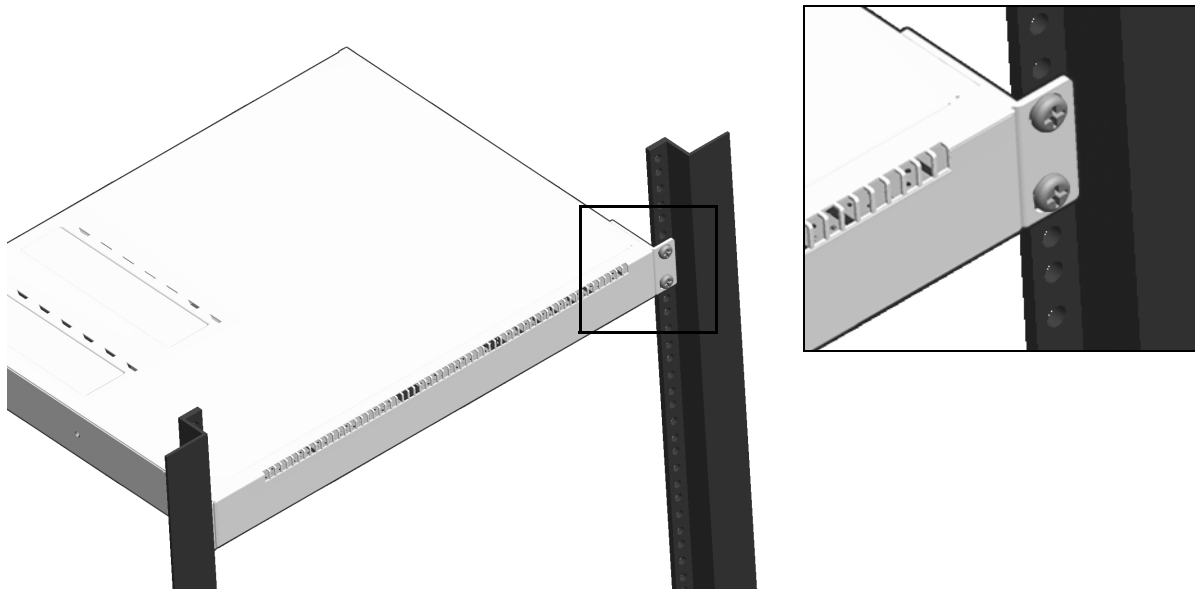
Connecting the Chassis to a Power Source

AC Power Supply Connections

Since the power cord is the switch's only disconnect device, it should be plugged into an easily accessible outlet. In the event that your power cord is lost or damaged, refer to the specifications below.

Powering On a Chassis

Follow the steps below to power on the chassis using and AC power source:

1 Connect the IEC-60320-C15 end of the supplied power cord to the chassis.

2 Connect power supply to AC power source.

3 Monitor the chassis as it boots.

5 Booting OmniSwitch 6350 Switches

Booting an OmniSwitch

The switch does not use an on/off switch. The power cord is the switch's only connect/disconnect device. The power connector socket is located on the power supply rear panel. For more information, refer to "OmniSwitch 6350 Chassis and Hardware Components" on page 3-1.

To boot the switch, plug the power supply cord into an easily-accessible, properly grounded power outlet. (Do not use extension cords.) The switch will power on and boot automatically.

Note. For a few seconds, at the beginning of the boot up process, random characters may briefly display on the console of an OS6350. This is due to an initial baud rate mismatch. As soon as the bootrom is initialized, the issue is automatically resolved.

Component LEDs

During the boot process, component LEDs will flash and change color, indicating different stages of the boot. Following a successful boot, chassis LEDs should display as follows:

OK1	Solid Green
PRI	Solid Green
PWR	Solid Green

Note. If the LEDs do not display as indicated, make sure the boot process is complete. If the LEDs do not display as indicated following a complete boot sequence, contact Alcatel-Lucent Customer Support. For information on LED states, refer to "OmniSwitch 6350 LED Status" on page 3-21.

For information on logging in and configuring your switch, refer to Chapter 2, "Getting Started."

Console Port

The console port, located on the chassis front panel, provides a console connection to the switch and is required when logging into the switch for the first time. By default, this RJ-45 connector provides a DTE console connection.

Serial Connection Default Settings

The factory default settings for the serial connection are as follows:

baud rate	9600
parity	none
data bits (word size)	8
stop bits	1
flow control	none

Modifying the Serial Connection Settings

The switch's serial connection defaults are listed above. If you wish to modify the default serial connection settings (i.e., baud rate, parity, data bits, and stop bits), refer to the following steps:

Note. You must be connected to the switch via the console port before attempting to change serial connection settings. Otherwise, an error message will display.

1 Enter the **modify boot parameters** command at the CLI prompt. The boot prompt displays:

```
Boot >
```

2 To change the baud rate, enter **boot serialbaudrate**, followed by the desired baud rate value. Options include 1200, 2400, 4800, 9600 (default), 19200, 38400, 57600, 76800, and 115200. For example:

```
Boot > boot serialbaudrate 19200
```

Note. Setting the console port to speeds above 9600 baud can cause problems with Zmodem uploads.

3 To change the parity value, enter **boot serialparity**, followed by the desired parity value. Options include none (default), even, and odd. For example:

```
Boot > boot serialparity even
```

4 To change the data bits (i.e., word size) value, enter **boot serialwordsize**, followed by the number of data bits. Options include 7 and 8 (default). For example:

```
Boot > boot serialwordsize 7
```

5 To change the stop bits value, enter **boot serialstopbits**, followed by the number of stop bits. Options include 1 (default) and 2. For example:

```
Boot > boot serialstopbits 2
```

6 Verify your current changes by entering **show** at the boot prompt:

```
Boot > show
Edit buffer contents:
Serial (console) baud        : 19200
Serial (console) parity      : even
Serial (console) stopbits    : 2
Serial (console) wordsize    : 7
```

(additional table output not shown)

7 You can save your changes to the **boot.params** file by entering **commit file** at the boot prompt:

```
Boot > commit file
```

When the **commit file** command is used, changes will not be enabled until after the next switch reboot.

8 You can also save your changes in real time to the switch's running memory by entering **commit system** at the boot prompt:

```
Boot > commit system
```

Caution. There are two important things to consider when using the **commit system** command to save serial connection changes:

- Output to the terminal may become illegible due to incompatible serial connection settings between the switch and the terminal emulation software.

- If you use the **commit system** command only, changes will *not* be saved to the switch's **boot.params** file and will be lost if the switch is rebooted. To save changes to the **boot.params** file, refer to step 7.

---

9 Return to the CLI prompt by entering **exit** at the boot prompt.

Monitoring the Chassis

The OmniSwitch can be monitored and managed via the console port using Command Line Interface (CLI) commands. The switches can also be monitored and managed via the Ethernet using CLI commands, WebView, SNMP, and OmniVista.

The section below provides some examples of useful hardware-related monitoring CLI commands. Refer to the *OmniSwitch AOS Release 6 CLI Reference Guide* for detailed information on all management and monitoring commands used with the OmniSwitch.

Checking the Overall Chassis Status

To check the overall status of a chassis, including the chassis type, and current administrative and operational status, use the **show chassis** command. For example:

```
-> show chassis

Chassis 1
  Model Name:                     6350 24 PORT COPPER GE,
  Description:                     Virtual Chassis,
  Part Number:                     903005-90,
  Hardware Revision:               03,
  Serial Number:                   M338153P,
  Manufacture Date:                AUG 13 2011,
  Admin Status:                    POWER ON,
  Operational Status:              UP,
  Number Of Resets:                4
  MAC Address:                     e8:e7:32:12:e6:6e,
```

For a complete list of output definitions for this command, refer to the *OmniSwitch AOS Release 6 CLI Reference Guide*.

Checking the Temperature Status

To check chassis temperature status, including the current temperature and configured threshold values, use the **show temperature** command. For example:

```
-> show temperature

Temperature for chassis 1
  Hardware Board Temperature (deg C)              = 54,
  Temperature Upper Threshold Range (deg C)       = 0 to 85,
  Temperature Upper Threshold (deg C)             = 81,
  Temperature Status                              = UNDER THRESHOLD,
  Temperature Danger Threshold (deg C)            = 85
```

For a complete list of output definitions for this command, refer to the *OmniSwitch AOS Release 6 CLI Reference Guide*.

Viewing the Power Supply Status

To check the status of the power supply, use the **show power** command. For example:

```
-> show power

Slot  PS   Wattage  Type    Status    Location
----+----+---------+------+----------+----------
 1    1      30      AC       UP       Internal
```

Additional Monitoring Commands

CLI Commands Used for Monitoring a Chassis	
show cmm	Displays the basic hardware and status information for primary and secondary management modules (if applicable).
show ni	Displays the basic hardware and status information for individual modules. If the switch is a standalone, information for the stand alone switch displays.
show module	Displays the basic information for individual modules. If the switch is a standalone, information for the stand-alone switch displays.
show module long	Displays the detailed information for individual modules. If the switch is a standalone, information for the standalone switch displays.
show module status	Displays the basic status information for individual modules. If the switch is a standalone, information for the standalone switch displays.

Using LEDs to Visually Monitor the Chassis

The front and rear panel of provides status LEDs that are useful in visually monitoring the status of the switches. LEDs include:

- Ethernet Port LEDs
- System Status LEDs

For tables showing LED states operating normally, refer to "OmniSwitch 6350 LED Status" on page 3-21.

6 Managing Power over Ethernet (PoE)

Power over Ethernet (PoE) is supported on OmniSwitch 6350 switches and provides inline power directly from the switch's Ethernet ports. Powered Devices (PDs) such as IP phones and wireless APs can be powered directly from the switch's RJ-45 ports.

As the feature reduces devices' dependence on conventional power sources, PoE eliminates many restrictions that traditional electrical considerations have imposed on networks.

In a PoE configuration, Power Source Equipment (PSE) detects the presence of a PD and provides an electrical current that is conducted along the data cable. The PD operates using the power received via the Ethernet data cable; no connection to an additional power source (e.g., an AC wall socket) is required.

Note on Terminology. There are several general terms used to describe this feature. The terms *Power over Ethernet (PoE)*, *LAN Power, Power over LAN (PoL), Power on LAN (PoL)*, and *Inline Power* are synonymous terms used to describe the powering of attached devices through Ethernet ports. This documentation refers to the feature as Power over Ethernet (PoE) and related CLI commands use the syntax, *lanpower*.

Additional terms, such as *Powered Device (PD)* and *Power Source Equipment (PSE)* are terms that are not synonymous, but are directly related to PoE.

* *PD* refers to any attached device that uses a PoE data cable as its only source of power. Examples include access points such as IP telephones, Ethernet hubs, wireless LAN stations, and so on.

* *PSE* refers to the actual hardware source of the electrical current for PoE.

As the OmniSwitch 6350 switches fully support Ethernet connectivity, you may also attach non-PD equipment, such as computer workstations, printers, servers, etc. to PoE ports. See Chapter 3, "OmniSwitch 6350 Chassis and Hardware Components," for more information on the OmniSwitch 6350 chassis.

Important. Alcatel-Lucent recommends that PoE-enabled switches with attached IP telephones should have operational power supply redundancy at all times for 911 emergency requirements. In addition, both the switch and the power supply should be plugged into an Uninterruptible Power Source (UPS).

In This Chapter

This chapter provides specifications and descriptions of hardware and software used to provide PoE for attached devices.

The chapter also provides information on configuring PoE settings on the switch through the Command Line Interface (CLI). CLI commands are used in the configuration examples; for more details about the syntax of commands, see the *OmniSwitch AOS Release 6 CLI Reference Guide*. Topics and configuration procedures described in this chapter include:

- Power over Ethernet Specifications on page 6-3

- Viewing Power Status on page 6-4

- Configuring Power over Ethernet Parameters on page 6-4

- Understanding Priority Disconnect on page 6-9

- Monitoring Power over Ethernet via the CLI on page 6-11

Note. You can also monitor all chassis components and manage many chassis features, including Power over Ethernet, with WebView, Alcatel-Lucent's embedded web-based device management application. WebView is an interactive and easy-to-use GUI that can be launched from the OmniVista or a web browser. Please refer to *WebView's Online Documentation* for more information.

Power over Ethernet Specifications

The table below lists general specifications for Alcatel-Lucent's Power over Ethernet support. For more detailed power supply and Power Source Equipment (PSE) specifications, refer to Chapter 3, "OmniSwitch 6350 Chassis and Hardware Components."

IEEE Standards supported	IEEE 802.3at
Default PoE administrative status	Enabled
Default PoE operational status	Enabled
Models supporting PoE	OS6350-P10, OS6350-P24, OS6350-P48
Cable distances supported	100 meters (approx.)
PoE-capable ports per switch	8 (OS6350-P10) 24 (OS6350-P24) 48 (OS6350-P48)
Default amount of inline power available	31000 milliwatts
Range of inline power allowed	3000 - 31000 milliwatts
PoE Power Available	OmniSwitch 6350-P10: ~ 120W OmniSwitch 6350-P24: ~ 380W OmniSwitch 6350-P48: ~ 780W

Viewing PoE Power Supply Status

To view the current status of power supplies installed, use the **show power** command, as shown below:

```
-> show power
Slot  PS   Wattage   Type    Status    Location
----+----+---------+------+----------+---------
 1    1     525      AC       UP       Internal
```

For detailed information on the **show power** command output, refer to the *OmniSwitch AOS Release 6 CLI Reference Guide*.

Configuring Power over Ethernet Parameters

Power over Ethernet Defaults

The following table lists the defaults for PoE configuration:

Parameter Description	Command(s)	Default Value/Comments
PoE operational status	**lanpower start** or **lanpower stop**	Disabled
Total power available to a port	**lanpower power**	Varies depending on chassis and power supply type. For more information, refer to product specifications in Chapter 3, "OmniSwitch 6350 Chassis and Hardware Components."
Total PoE power available to an entire chassis	**lanpower maxpower**	Varies depending on chassis and power supply type. For more information, refer to product specifications in Chapter 3, "OmniSwitch 6350 Chassis and Hardware Components."
Power priority level for a port	**lanpower priority**	Low
Priority disconnect status	**lanpower priority-disconnect**	Enabled

Understanding and Modifying the Default Settings

The sections below provide information on each of the key components within the Power over Ethernet software. They include information on PoE-related CLI commands. For detailed information on PoE-related commands, refer to the *OmniSwitch AOS Release 6 CLI Reference Guide*.

Note. PoE units support different wattage power supplies. If an unsupported power supply is used, a console message and a trap are generated.

PoE Class Detection

Powered devices can be classified into different classes as shown in the table below. Class detection allows for automatic maximum power adjustment based on the power class detected. This will prevent the switch from delivering more than the maximum power allowed based on a device's class.

During class detection the switch will allocate the maximum amount of power allowed based on the class detected. Once powered, if the device uses less than the maximum the remaining power will be made available for other devices.

Class	Usage Classification	Current (mA)	Power Range (Watts)	Class Description
0	Default	0-4	0.44-30.00	Unimplemented
1	Optional	9-12	0.44-3.84	Very Low Power
2	Optional	17-20	3.84-6.49	Low Power
3	Optional	26-30	6.49-15.40	Mid Power
4	Optional	36-44	15.4-31.00	High Power

Setting the PoE Operational Status

Enabling PoE

By default, Power over Ethernet is *administratively enabled* in the switch's system software. However, in order to physically activate PoE, you must issue the **lanpower start** command on a slot-by-slot basis before any connected PDs will receive inline power.

To activate power to PoE-capable in a switch, enter the corresponding slot number only. For example:

```
-> lanpower start 1
```

If power to a particular port has been disconnected via the **lanpower stop** command, you can reactivate power to the port by specifying both the *slot* and *port* in the command line. For example:

```
-> lanpower start 1/1
```

Note. You cannot use the *slot/port* syntax to initially activate PoE on a port. This syntax is intended only to reactivate power to those that have been disconnected via the **lanpower stop** command. To initially activate PoE, you must use the **lanpower start** *slot* syntax only, as described above.

Disabling PoE

To disable PoE on a particular slot or port, use the **lanpower stop** command.

To disable PoE on a *specific PoE-capable port*, enter a *slot/port* number. For example:

```
-> lanpower stop 1/4
```

To disable PoE for *all PoE-capable in a slot*, enter the corresponding slot number only.
For example:

```
-> lanpower stop 1
```

Configuring the Total Power Available to a Port

By default, each port is authorized by the system software to use up to a maximum amount of milliwatts to power any attached device.

You can either increase or decrease this value based on the range in the specifications table.

Increasing the total power available to an individual port may provide a more demanding Powered Device (PD) with additional power required for operation. Decreasing the total power available to a port helps to preserve inline power and assists in the overall management of the switch's power budget.

To increase or decrease the total power available to an individual port, use the **lanpower power** command. Since you are setting the power allowance for an individual port, you must specify a *slot/port* number in the command line. For example, the syntax

```
-> lanpower 1/1 power 3000
```

reduces the power available on port 1 of the switch to 3000 milliwatts. This new value is now the maximum amount of power the port can use to power any attached device (until the value is modified by the user).

Configuring the Total Power Available to a Switch

Like the maximum port power allowance, the system software also provides a maximum *slot-wide* power allowance. By default, each switch is authorized by the system software to use up to the maximum watts available from the PoE power supply.

As with the maximum port power allowance, the user can either increase or decrease this value based on the range in the specifications table.

Increasing the total power available to a switch may provide more demanding Powered Devices (PDs) with additional power required for operation. Decreasing the total power available helps preserve inline power and assists in the overall management of the switch's power budget.

Important. Before changing the maximum slot-wide power allowance, you must disable PoE for the slot via the **lanpower stop** command. Once the new value is assigned, re-enable PoE for the slot via the **lanpower start** command.

To increase or decrease the total power available to a slot, use the **lanpower maxpower** command. Since you are setting the power allowance for an individual slot, you must specify a *slot* number in the command line. For example, the syntax

```
-> lanpower 1 maxpower 40
```

reduces the power allowance of slot 1 to 40 watts. This value is now the maximum amount of power the slot can use to power all attached devices (until the value is modified by the user).

Note. Changing the maximum power available to a slot or port does not reserve or immediately allocate that power**.** These settings are only used for configuring a maximum amount of power that may be used, any unused power is still available and remains a part of the overall PoE budget.

Setting Port Priority Levels

As not all Powered Devices (PDs) connected to the switch have the same priority within a customer network setting, the switch allows the user to specify priority levels on a port-by-port basis. Priority levels include low, high, and critical. The default priority level for a port is low.

- **Low.** This default value is used for port(s) that have low-priority devices attached. In the event of a power management issue, inline power to low-priority is interrupted first (i.e., before critical and high-priority).

- **High.** This value is used for port(s) that have important, but *not* mission-critical, devices attached. If other in the chassis have been configured as critical, inline power to high-priority is given second priority.

- **Critical.** This value is used for port(s) that have mission-critical devices attached, and therefore require top (i.e., critical) priority. In the event of a power management issue, inline power to critical is maintained as long as possible.

To change the priority level for a particular port, use the **lanpower priority** command. Since the switch allows you to set priority levels on a port-by-port basis, be sure to specify *slot/port* information in the command line. For example, the syntax

```
-> lanpower 1/1 priority critical
```

changes the priority value of port 1 to the highest priority level of critical. Now that the default value has been reconfigured, this port should be reserved for those PDs that are mission critical for network operations.

Configuring Two-port PoE

This feature can be enabled to support the two-port PoE capability on APs with two PoE ports (i.e. OAW-AP 130 Series or OAW-AP1251). This capability enables the switch to support the appropriate detection range and recognize the AP as a PD.

- The AP will be powered in an active/standby mode, meaning only one port of the AP will be powered at a time.

- Only two-pair PoE will be supported when this feature is enabled, even on ports connected with a four-pair Ethernet cable.

- The capability of PSE-to-PSE protection function is reduced when this feature is enabled. It is recommended to disable PoE on ports that do not have PDs connected.

- Enabling this feature will cause the PoE functionality to restart on the OmniSwitch. Additionally, this functionality does not follow the PoE IEEE standards for PD detection.

Slot 1

Slot 2

Stack or Separate Switches
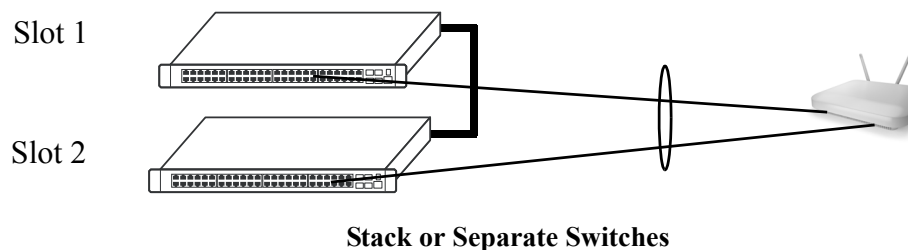
```
-> lanpower 1 high-resistance-detection enable
-> lanpower 2 high-resistance-detection enable
```

Slot 1

Standalone Switch
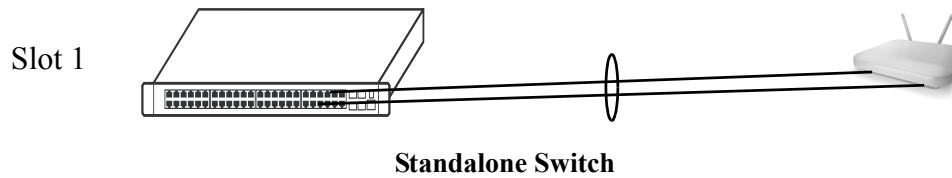
```
-> lanpower 1 high-resistance-detection enable
```

Configuring Delayed Start on PoE Ports

The power to the PoE ports can be delayed on bootup by configuring the delay timer. The LAN power will be in stop state until the delay timer expires.

To configure the delayed start on PoE port, use the **lanpower delayed-start** command. For example:

```
-> lanpower 5 delayed-start enable 200
```

In the above example, the power supply to the PoE ports on slot 5 is delayed by 200 seconds.

Note. The delay timer is activated only on bootup and not when the LAN power is restarted manually. The LAN power cannot be started or stopped while the delay timer is running.

Understanding Priority Disconnect

The priority disconnect function differs from the port priority function described on page 6-7 in that it applies only to *the addition of powered devices (PDs) in tight power budget conditions*. Priority disconnect is used by the system software in determining whether an incoming PD will be granted or denied power when there are too few watts remaining in the PoE power budget for an additional device. For example, if there are only 2 watts available in the current PoE power budget and a user plugs a 3.5W powered device into a PoE port, the system software must determine whether the device will be powered on. Based on priority disconnect rules, in some cases one or more existing devices may be powered down in order to accommodate the incoming device. In other cases, the incoming device will be denied power.

Priority disconnect rules involve the port priority status of an incoming device (i.e., low, high, and critical), as well as the port's physical port number (i.e., 1/1). Understanding priority disconnect rules is especially helpful in avoiding power budget deficits and the unintentional shutdown of mission-critical devices when PDs are being added in tight power budget conditions. For detailed information on how priority disconnect uses port priority and port number criteria for determining the power status of incoming PDs, refer to the examples on pages 6-10 through 6-11.

Reminder. Priority disconnect applies only when there is inadequate power remaining in the power budget for an incoming device.

For information on setting the priority disconnect status, refer to the section below. For information on setting the port priority status (a separate function from priority disconnect), refer to "Setting Port Priority Levels" on page 6-7.

Setting Priority Disconnect Status

By default, priority disconnect is *enabled* in the switch's system software. For information on changing the priority disconnect status, refer to the information below.

Disabling Priority Disconnect

When priority disconnect is disabled and there is inadequate power in the budget for an additional device, power will be denied to *any* incoming PD, regardless of its port priority status (i.e., low, high, and critical) or physical port number (i.e., 1/4).

To disable priority disconnect, use the **lanpower priority-disconnect** command. Since the switch allows you to set priority disconnect status on a slot-by-slot basis, be sure to specify the slot number in the command line. For example, the syntax

```
-> lanpower 1 priority-disconnect disable
```

disables the priority disconnect function on slot 1.

Enabling Priority Disconnect

To enable priority disconnect, use the **lanpower priority-disconnect** command. Be sure to specify the slot number in the command line. For example, the syntax

```
-> lanpower 1 priority-disconnect enable
```

enables priority disconnect on slot 1.

Priority Disconnect is Enabled; Same Priority Level on All PD

Reminder. Priority disconnect examples are applicable only when there is inadequate power remaining to power an incoming device.

When a PD is being connected to a port with the same priority level as all other in the slot, the physical port number is used to determine whether the incoming PD will be granted or denied power.

Lower numbered receive higher priority than higher-numbered. In other words, a PD connected to Port 1 will have a higher power priority than a PD connected to Port 2; a PD connected to Port 23 will have a higher power priority than a PD connected to Port 24.

In order to avoid a power budget deficit, another port in the slot is disconnected. In determining which port to power off, the system software disconnects the port with the highest physical port number.

Priority Disconnect is Enabled; Incoming PD Port has Highest Priority Level

Reminder. Priority disconnect examples are applicable only when there is inadequate power remaining to power an incoming device.

When a PD is being connected to a port with a *higher priority level* than all other in the slot, the incoming PD will automatically be granted power over the other devices, regardless of its physical port number.

In order to avoid a power budget deficit, another port in the slot is disconnected. In determining which port to power off, the system software first selects the port with the lowest configured priority level. For example, if a *critical priority* device is being added to a slot in which five existing devices are attached to *high priority* and one device is attached to a *low priority* port, the low priority port is automatically disconnected, regardless of its physical port number.

If all existing devices are attached to with the same lower priority level, the system software disconnects the port with both the lowest priority level *and* the highest physical port number. For example, if a critical priority device is being added to a slot in which six existing devices are attached to high priority, the high priority port with the highest physical port number is automatically disconnected.

Priority Disconnect is Enabled; Incoming PD Port has Lowest Priority Level

Reminder. Priority disconnect examples are applicable only when there is inadequate power remaining to power an incoming device.

When a PD is being connected to a port with a *lower priority level* than all other in the slot, the incoming PD will be denied power, regardless of its physical port number. Devices connected to other higher-priority will continue operating without interruption.

Priority Disconnect is Disabled

Reminder. Priority disconnect examples are applicable only when there is inadequate power remaining to power an incoming device.

When priority disconnect is disabled, power will be denied to *any* incoming PD, regardless of its port priority status (i.e., low, high, and critical) or physical port number (i.e., 1/1).

Monitoring Power over Ethernet via CLI

To monitor current PoE statistics and settings, use the **lanpower combo-port** command. The command output displays a list of all current PoE-capable, along with the following information for each port:

- Maximum power available to the port, in milliwatts

- Actual power used by the port

- Current port status

- Power priority status

- Power on/off status

Aggregate slot and chassis management information is also displayed. This information includes:

- Maximum watts available to the corresponding slot

- Amount of power budget remaining that can be available for PoE modules

- Total amount of power remaining that can be available for additional switch functions

When entering the **show lanpower** command, you must include a valid slot number in the command line syntax. For example:

```
-> show lanpower 1
Port Maximum(mW) Actual Used(mW)   Status    Priority  On/Off   Class
----+-----------+---------------+----------+---------+------+-------
  1    31000             0        Undefined    Low      OFF    None
  2    31000             0        Undefined    Low      OFF    None
  3    31000             0        Undefined    Low      OFF    None
  4    31000             0        Undefined    Low      OFF    None

Slot 1 Max Watts 225
1 Power Supplies Available
```

Note. For detailed information on **show lanpower** command output, refer to the *OmniSwitch AOS Release 6 CLI Reference Guide*.

---

7   Managing OmniSwitch 6350 Stacks

In addition to their working as individual stand-alone switches OmniSwitch 6350 switches can also be linked together to work as a single virtual chassis known as a *stack*. With stacks, users can easily expand their switching capacity simply by adding additional switches to the stack. In addition, stacks provide enhanced resiliency and redundancy features. For more information, refer to .

In This Chapter

This chapter provides information on OmniSwitch 6350 switches configured to operate as a single virtual chassis. Topics described in the chapter include:

- OmniSwitch 6350 stack overview on .

- Roles within the stack on .

- Stack cabling on .

- Slot numbering on .

- Hot-Swapping modules in a stack on .

- Reloading switches on .

- Changing the secondary module to primary on .

- Synchronizing switches in a stack on .

- Stack Split Detection (SSP) on .

- Monitoring the stack on .

Note. You can also manage and monitor OmniSwitch 6350 stacks through WebView, Alcatel-Lucent Enterprise's embedded web-based device management application. WebView is an interactive and easy-to-use GUI that can be launched from OmniVista or a web browser. Please refer to WebView's online documentation for more information.

OmniSwitch 6350 Stacking Specifications

Models Supporting Stacking	OS6350-24, OS6350-P24, OS6350-48, OS6350-P4 (Stacking OS6350-10/P10 switches is not currently supported.)
Maximum Switches in a Stack	4
Required Stacking Module	N/A (Uses built-in stacking ports)
Required Transceiver Type	Direct Attach Copper
Cable Lengths - Copper	60cm, 1m, 3m, 7m
Default Chassis Mode	Standalone

Note. Stackable OS6350 models (see table above) have 4x1G uplink ports, two of which are capable of 5Gbps stacking. For OS6350-24/P24 switches, ports 27 and 28 can be used for stacking and, for OS6350-48/P48 switches, ports 49 and 50 are both uplink (1Gbps) and stacking capable (5Gbps) ports.

OmniSwitch 6350 Stack Overview

Users can configure OmniSwitch 6350 switches into a single virtual chassis known as a *stack*. With stacks, switching capacity can be easily expanded simply by adding additional switches to the stack. For example, a user can start with a stack composed of two switches and add additional switches to that stack as network demands increase over time.

Note. Switches should be added one at a time in a stack.

Stacks also provide enhanced resiliency and redundancy features. If a switch in a stack goes down or is taken offline, the other elements in the stack will continue to operate without disruption. In addition, when a switch auto-synchronizes at boot-up, or if the user manually synchronize the switches (see "Synchronizing Switches in a Stack" on page 7-36 for more information), operating software and configuration parameters are backed up on all switches in the stack. As a result, the original operating software and configuration parameters can be easily recovered if corrupted or otherwise lost.

Note. In the user guides provided with your OmniSwitch 6350 switch, the terms *stack* and *virtual chassis* are interchangeable referring to OmniSwitch 6350 switches in a stacked configuration. The terms *module*, *switch*, *slot*, and *element* are used to refer to individual switches within a stacked configuration. The terms *Chassis Management Module (CMM)* and *management module* refer to those switches operating in a stack either in the primary or secondary management roles. OmniSwitch 6350 switches operating in an idle role are essentially acting as network interface modules and therefore may be referred to as *Network Interfaces (NIs)*.

OmniSwitch 6350 Stacking/Standalone Mode

The mode of the OS6350 can be manually configured using the **stack set slot mode** as shown below:

```
-> stack set slot 1 mode stackable
```

The switch must be rebooted for the new mode to take affect.

Roles Within the Stack

In order to operate as a virtual chassis, switches within an OmniSwitch 6350 stack are assigned specific roles. These roles include primary and secondary management roles, idle status, and pass-through. For detailed descriptions of each of these roles, including their practical functions within the virtual chassis, refer to the sections below.

Primary and Secondary Management Modules

When OmniSwitch 6350 switches operate in a stack, one switch in the stack always assumes the *primary management* role. This primary element is responsible for functions, such as software and configuration management, web-based management (i.e., WebView), SNMP management, switch diagnostics, and software rollback.

One additional switch in the stack operates in a *secondary management* role. This switch serves as a backup, and is always ready to assume the primary management role in the stack if the switch with the primary role fails or is taken offline for any reason.

Since the secondary module quickly and automatically assumes management responsibilities, switches operating in idle mode elsewhere in the stack continue to pass traffic without disruption. This redundancy provides effective safeguards for mission-critical network traffic and is one of the stack's most important failover features. Diagrams showing the management module failover sequence for stacks of three or more switches and stacks of two switches are provided on pages 7-4 and 7-5, respectively.

Note. For management module redundancy to work effectively, the software on all switches operating in the stack must be synchronized at all times. Refer to "Synchronizing Switches in a Stack" on page 7-36 for more information.

Primary / Secondary / Idle / Idle	1 A stack of four OmniSwitch 6350 switches is operating normally. The stack consists of a primary module, secondary module, and two elements operating in idle status. (The software on all elements in the stack is synchronized.)
Offline / Secondary / Idle / Idle	2 The primary management module in the stack fails or is taken offline (e.g., powered off or rebooted by the user).
Offline / Primary / Secondary / Idle	3 The switch operating as the secondary management module immediately takes over the primary role. Meanwhile, the adjacent switch—previously operating in idle status—now assumes the secondary management role.
Idle / Primary / Secondary / Idle	4 If the switch that failed or was taken offline comes back online, it will assume an idle role in the stack. In other words, it will act essentially as an NI module in the virtual chassis, passing traffic via its Ethernet.

Redundant Management Module Failover (Three or More Switches)
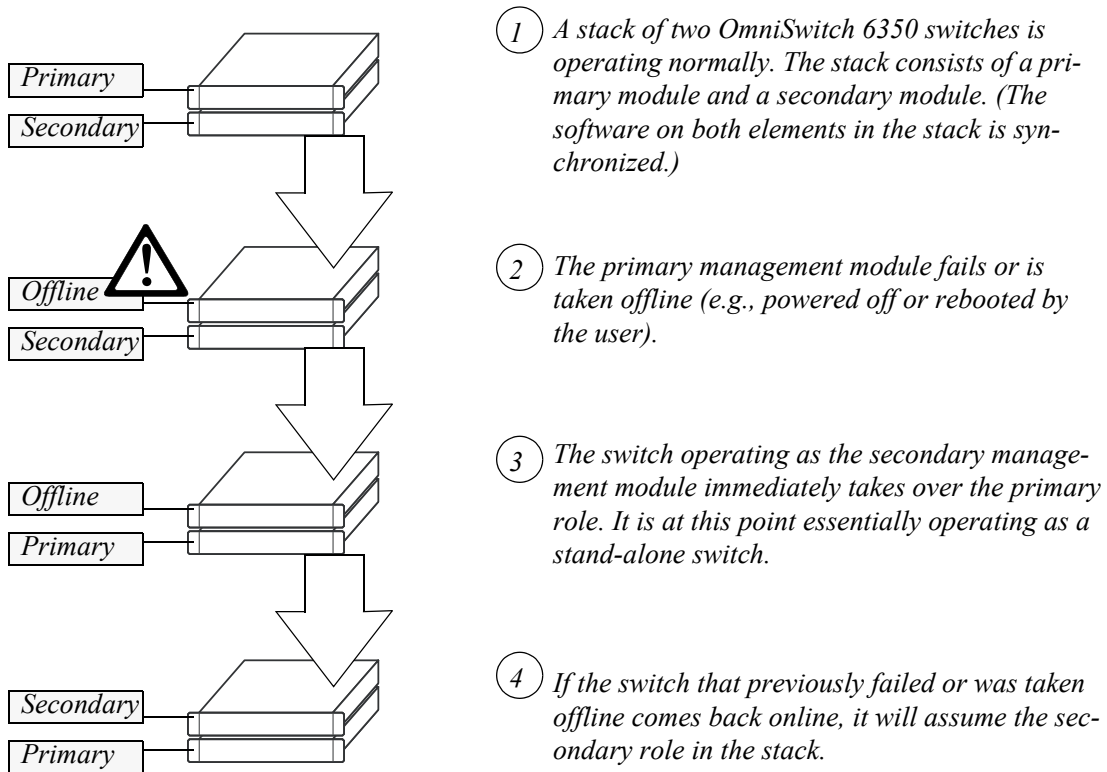
Primary
Secondary

(1) *A stack of two OmniSwitch 6350 switches is operating normally. The stack consists of a primary module and a secondary module. (The software on both elements in the stack is synchronized.)*

Offline
Secondary

(2) *The primary management module fails or is taken offline (e.g., powered off or rebooted by the user).*

Offline
Primary

(3) *The switch operating as the secondary management module immediately takes over the primary role. It is at this point essentially operating as a stand-alone switch.*

Secondary
Primary

(4) *If the switch that previously failed or was taken offline comes back online, it will assume the secondary role in the stack.*

Redundant Management Module Failover (Two Switches)

Primary Management Module Selection

For a stack of OmniSwitch 6350 switches to operate as a virtual chassis, there must be a mechanism for dynamically selecting the switch within the stack that will assume the primary management role. OmniSwitch 6350 switches use three different methods for selecting the primary switch.
These methods are:

- Chassis MAC address

- Saved slot number

- Chassis uptime

Note. Information on *secondary management module* selection is provided on page 7-9. Information on dynamic assignment of *idle module* roles is provided on page 7-11.

Using the Chassis MAC Address

By default, the primary management role will be given to the switch with the lowest chassis MAC address. However, for this to occur, all switches in the stack *must be booted within 15 seconds of each other*. In addition, switches in the stack *must have no preconfigured slot information*. Because of these two conditions, the MAC address method for selecting the primary module usually occurs with new "out of the box" switches, or switches from which any preconfigured slot information has been cleared.

For more information on using the lowest MAC address to determine the primary switch in a stack, refer to the diagram below:
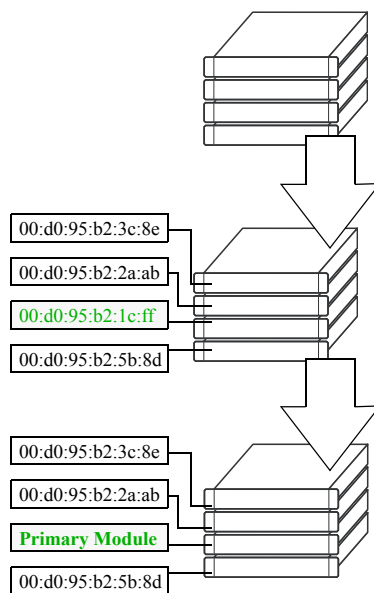
① *A stack of four OmniSwitch 6350 switches is booted. All switches are powered on within 15 seconds of each other. In addition, there is no preconfigured slot information on any of the switches.*

00:d0:95:b2:3c:8e
00:d0:95:b2:2a:ab
00:d0:95:b2:1c:ff
00:d0:95:b2:5b:8d

② *When the stack is booted, system software detects the lowest MAC address. In this stacked configuration, the lowest MAC address is 00:d0:95:b2:1c:ff.*

③ *The system software immediately assigns the corresponding switch the primary management role. When the switch is assigned as primary, it is also dynamically assigned the lowest slot number in the stack—i.e., slot 1. This slot number information is saved to the boot.slot.cfg file, located in the switch's /flash file directory.*

00:d0:95:b2:3c:8e
00:d0:95:b2:2a:ab
Primary Module
00:d0:95:b2:5b:8d

Primary Management Module Selection Using the Lowest Chassis MAC Address

---

Note. During the boot process, all other switches in the stack are also dynamically assigned unique slot numbers. As with the primary switch, these slot numbers are saved to the **boot.slot.cfg** file, located in the /flash file directory of each switch. For more information on dynamic slot number assignment, refer to "Slot Numbering" on page 7-19.

Using Saved Slot Information

The saved slot number is the slot number the switch will assume following a reboot. This information is stored in a switch's **boot.slot.cfg** file; the switch reads its slot number assignment from this file at bootup and assumes the specified slot number within the stack.

If switches in a stacked configuration have no preconfigured slot assignments, the slot number for each switch is dynamically assigned by the system software. Slot numbers can also be manually assigned by the user. For more information on manually assigning slot numbers, refer to "Manual Slot Number Assignment" on page 7-22.

When a stack with preconfigured slot information is booted, it is *not* the lowest MAC address that determines the primary management module. Instead, the slot information stored in each switch's **boot.slot.cfg** is read by the system software and used in determining the primary. The switch with the lowest saved slot number becomes the primary management module.

Note. Although, for ease-of-management purposes, it is recommended that slot numbers are assigned beginning with slot number 1, it is not a requirement. In other words, a stack of four switches can have slot assignments 3, 4, 5, and 6. However, it is important that each element in a stack is assigned a *unique* slot number. Do not assign duplicate slot numbers to elements in a stack. Otherwise, one or more switches will be forced into pass-through mode. For more information on pass-through mode, refer to page 7-12.

For more information on using saved slot information to determine the primary switch in a stack, refer to the diagram below:
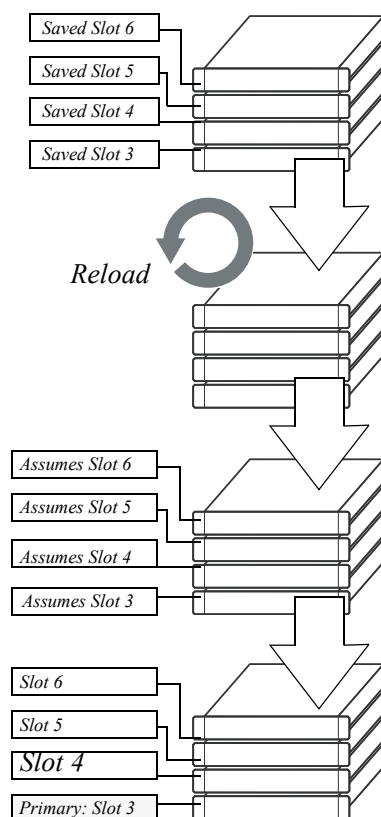
Saved Slot 6	① Four OmniSwitch 6350 switches are stacked; all switches are connected via stacking cables. The user configures each switch to have a unique saved slot number. When each saved slot number is configured, the information is automatically written to the boot.slot.cfg file located in the /flash directory of each switch.
Saved Slot 5	
Saved Slot 4	
Saved Slot 3	

Reload

② The user reloads all the elements in the stack either by issuing the reload all command or by physically powering off and then powering on all switches.

③ Instead of assigning the primary management module based on the lowest MAC address, the system software reads the slot information from each switch's boot.slot.cfg file during the boot process. The switches in the stack come up using their assigned slot numbers.

Assumes Slot 6
Assumes Slot 5
Assumes Slot 4
Assumes Slot 3

④ The switch with the lowest assigned slot number automatically assumes the primary management role. In this case, the switch assigned slot 3 has the lowest slot number in the stack and becomes the primary management module.

Slot 6
Slot 5
Slot 4
Primary: Slot 3

Primary Management Module Selection Using Saved Slot Information

---

Using Switch Uptime

A user can override both the MAC address and saved slot methods for determining a stack's primary management module. This is done by controlling the uptime of switches in the stack. If all elements of a stack are powered off, the user can force a particular switch to become primary by powering on that switch and waiting a minimum of 15 seconds before powering on any other switches. This can be useful if the user wants a switch placed in a specific location, e.g., the top-most switch in a stack, to become the primary.

As with the lowest MAC address method, the primary management module is dynamically assigned slot number 1 when the stack is booted.

For more information on using saved slot information to determine the primary switch in a stack, refer to the diagram below:
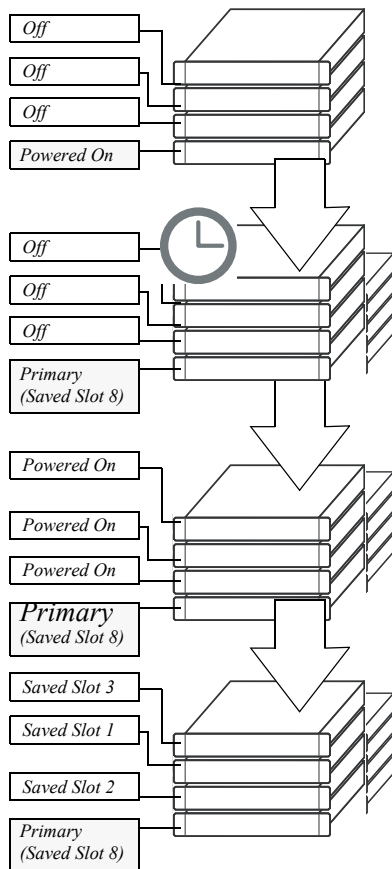
1. *Four OmniSwitch 6350 switches are stacked and connected via stacking cables. All switches are currently powered off. The user powers on a single switch in the stack. In this case, the bottom-most switch is powered on.*

2. *The user allows a minimum of 15 seconds to pass. Because no other switches have joined the stack, the switch that was powered on considers itself a stand-alone. The switch assumes a primary role by default—even if there is a high saved slot number in its boot.slot.cfg file (e.g., 8).*

3. *The user now powers on the remaining switches in the stack in short succession.*

4. *In this example, when the remaining switches come online, each has a lower saved slot value than the switch powered on at step 1. However, the switch powered on at step 1—with its slot value of 8—retains its primary management role. The joining switches are essentially ineligible for primary status because they are considered "late arrivals." For the primary switch to forfeit its role to the switch with the lowest assigned slot number (in this case, slot number 1), the stack must be rebooted by the user either by issuing the **reload all** command or by powering off and powering on all switches in close succession.*

Primary Management Module Selection Using Switch Uptime

Secondary Management Module Selection

In order to provide effective management module redundancy, all OmniSwitch 6350 stacked configurations dynamically assign a backup, or secondary, management module during the boot process. OmniSwitch 6350 stacks use two different methods for selecting the secondary switch. These methods are:

• Stacking connection to the primary switch

• Saved slot number

Using the Stacking Connection to the Primary Switch

By default, the switch that is connected to the primary switch's stacking port A is automatically assigned the secondary management role. This applies to stacks on which there is no preassigned slot information— i.e., there is no **boot.slot.cfg** file present in any switch.

For more information on using the stacking connection to the primary switch to determine the secondary management module, refer to the diagram below:

A B
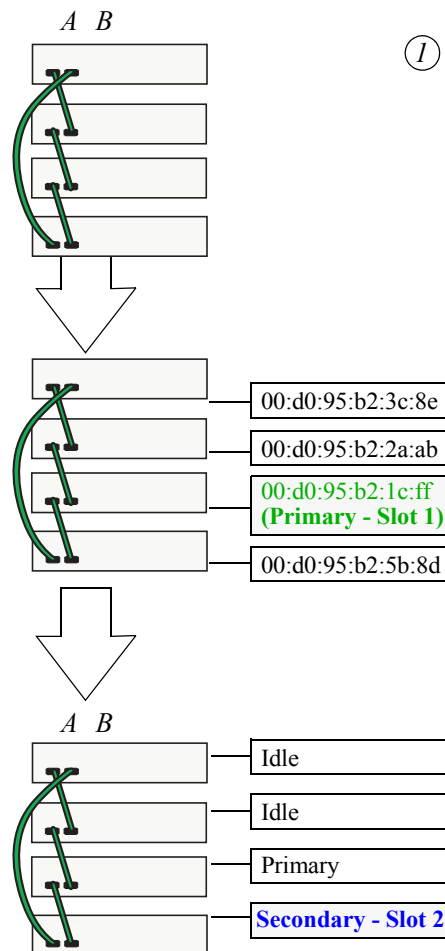
① *Four OmniSwitch 6350 switches are stacked and connected via stacking cables, as shown. All switches are currently powered off. None of the switches have preassigned slot numbers—i.e., there are no boot.slot.cfg files present. The user powers on all switches in the stack in close succession and the stack begins the boot process.*

| 00:d0:95:b2:3c:8e |

② *When the elements in the stack come online, the switch with the lowest MAC address is given the primary management role and is dynamically assigned slot number 1.*

| 00:d0:95:b2:2a:ab |
| 00:d0:95:b2:1c:ff **(Primary - Slot 1)** |
| 00:d0:95:b2:5b:8d |

A B

③ *By default, the switch connected to the primary's stacking port A is automatically assigned the secondary management role. The secondary switch is dynamically assigned slot number 2.*

| Idle |
| Idle |
| Primary |
| **Secondary - Slot 2** |

Secondary Management Module Selection Using the Stacking Connection to the Primary Switch

Note. For information on dynamic slot numbering for idle elements within the stack, refer to "Idle Module Role" on page 7-11 and "Slot Numbering" on page 7-19.

Using Saved Slot Information

If a stack with preassigned slot information for each switch is booted, the switch with the *second lowest* slot value is assigned the secondary management role. For example, if a stack of four switches is booted and the preassigned slot values for each switch are 1, 2, 3, and 4, the switch with the slot value of 2 is assigned the secondary role. Meanwhile, the switch with the slot value of 1 is assigned the primary management role (see page 7-7).

For more information on using saved slot information to determine the secondary management module in a stack, refer to the diagram below:
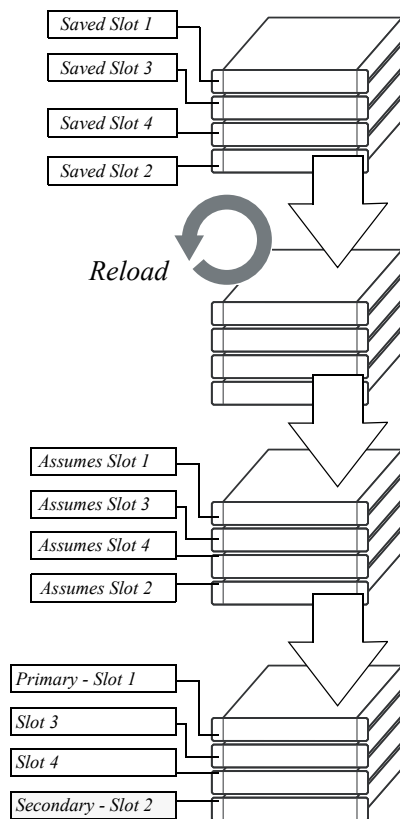
Saved Slot 1	① Four OmniSwitch 6350 switches are stacked; all switches are connected via stacking cables. The user configures each switch to have a unique saved slot number, as shown. When the saved slot number is configured, the information is automatically written to the boot.slot.cfg file located in the /flash directory of each switch.
Saved Slot 3	
Saved Slot 4	
Saved Slot 2	
Reload	② The user reloads all the elements in the stack either by issuing the reload all command or by physically powering off and then powering on all switches.
Assumes Slot 1	③ The system software reads the slot information from each switch's boot.slot.cfg file during the boot process. The switches in the stack come up using their assigned slot numbers.
Assumes Slot 3	
Assumes Slot 4	
Assumes Slot 2	
Primary - Slot 1	④ The switch with the lowest assigned slot number automatically assumes the primary management role. The switch with the second lowest assigned slot number becomes the secondary management role, regardless of whether it is attached to stacking port A of the primary switch. In this case, the switch assigned slot 2 has the second-lowest slot number in the stack and becomes the secondary management module.
Slot 3	
Slot 4	
Secondary - Slot 2	

Secondary Management Module Selection Using Saved Slot Information

---

Note. Each element in a stack should always be assigned a *unique* slot number. Do not assign duplicate slot numbers to elements in a stack. Otherwise, one or more switches will be forced into pass-through mode. For more information on pass-through mode, refer to page 7-12.

Idle Module Role

Switches that are not assigned either the primary or secondary role in a stack are, by default, assigned the role of *idle* modules. These idle modules operate similarly to Network Interface (NI) modules in a chassis-based switch. It is the job of idle modules to send and receive traffic.

In the event of a management module failure within the stack, the idle module with the next lowest slot number in the stack will automatically assume the secondary management role. In other words, if the primary module in a stack goes down for any reason and the secondary takes over the primary management role, the switch must now assign a new secondary module. The idle element with the next lowest slot number assumes this new responsibility until the situation is corrected and all elements in the stack are reloaded.

Note. Primary and secondary management modules also send and receive traffic on their Ethernet. The primary management module is like an NI module with the added task of overall stack management; the secondary management module is like an NI with the added responsibility of backing up the primary module in the event of a primary module failure. In other words, *all modules* in the virtual chassis can send and receive user data, regardless of their roles.

For more information on dynamic assignment of idle modules in a stack, refer to the diagram below:

① *Four OmniSwitch 6350 switches are stacked; all switches are connected via stacking cables. The stack is booted.*

Primary

Secondary

② *The primary and secondary management modules are dynamically assigned using any of the methods outlined on pages 7-6 through 7-10.*

Idle

Idle

Primary

Secondary

③ *The system software automatically assigns the remaining elements in the stack the idle module role. These modules act as Network Interface (NI) modules.*

In the event of a primary-to-secondary failover, the idle module with the next-lowest slot number in the stack will assume the secondary—or backup—management role.

Secondary Management Module Selection Using Saved Slot Information

Pass-Through Mode

The pass-through mode is a state in which a switch has attempted to join a stack but has been denied primary, secondary, and idle status. When a switch is in the pass-through mode, its Ethernet ports are brought down (i.e, they cannot pass traffic). Its stacking cable connections remain fully functional and can pass traffic through to other switches in the stack. In this way, the pass-through mode provides a mechanism to prevent the stack ring from being broken. However, note that when a switch comes up in pass-through mode, it should not be left unresolved. Pass-through mode is essentially an error state that should be corrected immediately.

Note. When a switch is in pass-through mode, its information will not display in hardware monitoring commands such as **show chassis**, **show ni**, **show module**, etc.

Conditions that can trigger a switch to enter pass-through mode include:

- Duplicate slot numbers have been assigned within the stack

- The user has manually forced the switch into pass-through mode using the **stack clear slot** command

---

Note. If a switch is forced into pass-through mode, the rest of the stack will not be disrupted. Any elements in the stack *not* operating in pass-through mode continue to operate normally.

The most common reason for one or more switches to enter pass-through is duplicate slot number assignments within the stack. So, in order to avoid pass-through mode, it is useful to keep track of the current saved slot numbers on all elements in the stack. Slot number assignments are stored in the **boot.slot.cfg** file in the /flash directory of each switch.

If the stack is booted and the same slot number is discovered on two or more switches, the switch with the lowest MAC address is allowed to come up and operate normally. Meanwhile, switches with the duplicate slot number *and* a higher MAC address come up in pass-through mode. To check the current slot number stored in each switch's **boot.slot.cfg** file, use the **show stack topology** command. For example:

```
-> show stack topology
                                  Link A  Link A           Link B  Link B
NI       Role      State   Saved  Link A  Remote  Remote  Link B  Remote  Remote
                           Slot   State   NI      Port    State   NI      Port
----+----------+--------+------+-------+-------+-------+-------+-------+-------
   1 PRIMARY    RUNNING    1     UP          3   StackA  UP          2   StackA
   2 SECONDARY  RUNNING    2     UP          1   StackB  UP          3   StackB
   3 IDLE       RUNNING    2     UP          1   StackA  UP          2   StackB
```

In this example, note that both slots 2 and 3 have a saved slot value of 2. If this stack is rebooted, a duplicate slot error will occur and the switch with the lower MAC address will be given the secondary management role. The slot with the higher MAC address will be forced into the pass-through mode.

To avoid a pass-through condition following a reboot, make sure that all saved slot values for the stack are unique. Use the **stack set slot** command. For example, change the saved slot value for the idle switch in slot 3 from 2 to 3:

```
-> stack set slot 3 saved-slot 2
```

Use the **show stack topology** command to verify the change:

```
-> show stack topology
                                Link A  Link A          Link B  Link B
NI      Role      State   Saved Link A  Remote  Remote  Link B  Remote  Remote
                          Slot  State   NI      Port    State   NI      Port
----+----------+--------+------+-------+-------+-------+-------+-------+-------
   1 PRIMARY     RUNNING    1    UP         3   StackA  UP          2   StackA
   2 SECONDARY   RUNNING    2    UP         1   StackB  UP          3   StackB
   3 IDLE        RUNNING    3    UP         1   StackA  UP          2   StackB
```

Recovering from Pass-Through Mode (Duplicate Slot Numbers)

The first step in recovering from pass-through is to determine which modules are currently operating in pass-through, as well as the reason for the pass-through state. To view this information, use the *show stack topology* command. For example:

```
-> show stack topology
                                Link A  Link A          Link B  Link B
NI      Role      State   Saved Link A  Remote  Remote  Link B  Remote  Remote
                          Slot  State   NI      Port    State   NI      Port
----+----------+--------+------+-------+-------+-------+-------+-------+-------
   1 PRIMARY     RUNNING    1    UP      1001   StackA  UP          2   StackA
   2 SECONDARY   RUNNING    2    UP         1   StackB  UP       1001   StackB
1001 PASS-THRU   DUP-SLOT   2    UP         1   StackA  UP          2   StackB
```

Switches operating in pass-through mode are given distinct slot numbers. These slot numbers are not related to their position in the stack. Instead, they are assigned the prefix "100," followed by the numerical order in which they were forced into pass-through (1001–1008).

Note. For pass-through elements 1001 through 1008, the slot indicator LED on the chassis front panel blinks 1 through 8, respectively. For example, if a module enters pass-through and has the slot number 1004, the LED for the module blinks the number 4. For more information on the slot indicator LED, refer to "OmniSwitch 6350 LED Status" on page 3-21.

In the example above, the switch with the NI (i.e., slot) number 1001 is operating in pass-through. Note that the role assignment is PASS-THRU; also, the state displays DUP-SLOT, or *duplicate slot number*. This can be further verified by looking down the saved slot column in the table. Note that slot 2, operating in the secondary management role, has a saved slot value of 2. Slot 1001, operating in pass-through, also has a saved slot value of 2.

To resolve this pass-through condition, simply assign slot 1001 a new saved slot value and reboot the module. This can be done in either of two ways:

- Use the **stack set slot** command to assign the new value, then use the **reload pass-through** command to reboot the module:

```
-> stack set slot 1001 saved-slot 3
-> reload pass-through 1001
```

- Use the **stack set slot** command to assign the new slot value and, using the optional **reload** syntax in the command line, reboot the module:

```
-> stack set slot 1001 saved-slot 3 reload
```

When the module comes up, it assumes the new, unique slot position—in this case, slot 3—and, because it now has the highest slot number in the stack, it assumes an idle role (leaving the primary and secondary roles to slots 1 and 2, respectively). There are now no duplicate numbers in the stack and all elements are operating normally:

```
-> show stack topology
                                    Link A  Link A              Link B  Link B
NI       Role      State   Saved   Link A  Remote  Remote  Link B  Remote  Remote
                           Slot    State   NI      Port    State   NI      Port
----+----------+--------+------+-------+-------+-------+-------+-------+-------
    1 PRIMARY    RUNNING    1      UP          3   StackA  UP          2   StackA
    2 SECONDARY  RUNNING    2      UP          1   StackB  UP          3   StackB
    3 IDLE       RUNNING    3      UP          1   StackA  UP          2   StackB
```

In some pass-through conditions (for example, larger stacks where multiple switches are in pass-through mode), it might be desirable to correct any duplicate saved slot assignments and then reboot the entire stack. The recovery from pass-through can be accomplished with fewer steps than reassigning slot numbers and rebooting modules on a slot-by-slot basis. However, be sure that there is no mission-critical traffic being passed on the non-pass-though modules; traffic will be interrupted on these modules during the reboot.

The following example shows a large stack with multiple elements operating in pass-through mode:

```
-> show stack topology
                                      Link A  Link A           Link B  Link B
NI        Role       State   Saved   Link A  Remote  Remote  Link B  Remote  Remote
                             Slot    State   NI      Port    State   NI      Port
----+----------+--------+------+-------+-------+-------+-------+-------+-------
   4 IDLE       RUNNING    4     UP        5    StackB  UP         3    StackA
   5 IDLE       RUNNING    5     UP     1001    StackB  UP         4    StackA
1001 PASS-THRU  DUP-SLOT   2     UP        2    StackB  UP         5    StackA
   2 SECONDARY  RUNNING    2     UP     1003    StackB  UP      1001    StackA
1003 PASS-THRU  DUP-SLOT   2     UP     1002    StackB  UP         2    StackA
1002 PASS-THRU  DUP-SLOT   2     UP        1    StackB  UP      1003    StackA
   1 PRIMARY    RUNNING    1     UP        3    StackB  UP      1002    StackA
   3 IDLE       RUNNING    3     UP        4    StackB  UP         1    StackA
```

This disordered stack topology, with its three modules operating in pass-through mode, can be corrected by entering the following commands:

```
-> stack set slot 4 saved-slot 1
-> stack set slot 5 saved-slot 2
-> stack set slot 1001 saved-slot 3
-> stack set slot 2 saved-slot 4
-> stack set slot 1003 saved-slot 5
-> stack set slot 1002 saved-slot 6
-> stack set slot 1 saved-slot 7
-> stack set slot 3 saved-slot 8
-> reload all
```

When all elements in the stack come up following the reboot, there are no longer any duplicate slot numbers in the stack. In addition, the stack topology is more orderly and, as a result, easier to manage:

```
-> show stack topology
                                      Link A  Link A           Link B  Link B
NI        Role       State   Saved   Link A  Remote  Remote  Link B  Remote  Remote
                             Slot    State   NI      Port    State   NI      Port
----+----------+--------+------+-------+-------+-------+-------+-------+-------
   1 PRIMARY    RUNNING    1     UP        2    StackB  UP         8    StackA
   2 SECONDARY  RUNNING    2     UP        3    StackB  UP         1    StackA
   3 IDLE       RUNNING    3     UP        4    StackB  UP         2    StackA
   4 IDLE       RUNNING    4     UP        5    StackB  UP         3    StackA
   5 IDLE       RUNNING    5     UP        6    StackB  UP         4    StackA
   6 IDLE       RUNNING    6     UP        7    StackB  UP         5    StackA
   7 IDLE       RUNNING    7     UP        8    StackB  UP         6    StackA
   8 IDLE       RUNNING    8     UP        1    StackB  UP         7    StackA
```

Stack Cabling

Switches in a stack are connected to each other by stacking cables. These stacking cables provide high-speed, dual-redundant links between switches in a stack.

Stacking cables for OmniSwitch 6350 switches must be connected in an **A-B** pattern. In other words, the cable connected to stacking port **A** of one switch must be connected to stacking port **B** of the adjacent switch. In addition, for a stack to have effective redundancy, *a redundant stacking cable must be installed between the upper-most and bottom-most switch at all times*. This provides effective failover in the event of a stacking link or module failure within the stack.

The diagram below shows the required stacking cable pattern. For detailed information on assembling a stack and connecting the cables, refer to Chapter 3, "OmniSwitch 6350 Chassis and Hardware Components."

Note. When planning the stack cabling configuration, keep in mind that the switch connected to stacking port A of the primary switch will be assigned the secondary management role by default.

A B

A stack of four switches in a crossed (stacking port A to stacking port B) configuration. Note that a redundant stacking cable connection exists between the top and bottom switches. This connection is required for effective redundancy across the stack.
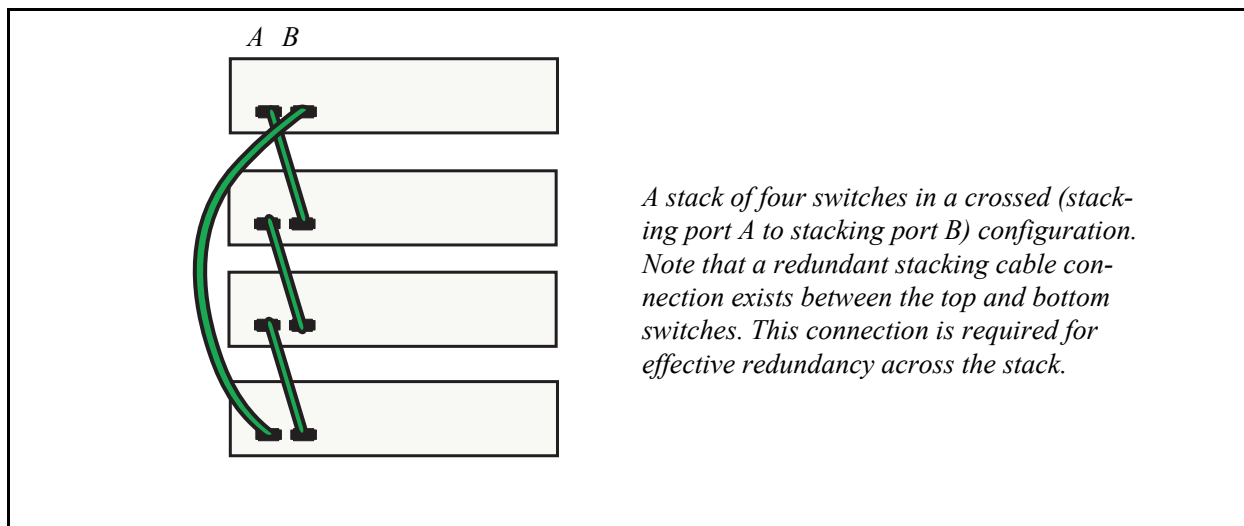
Example of Stacking Cable Pattern (Chassis Rear Panels Shown)

Redundant Stacking Cable Connection

OmniSwitch 6350 switches allow redundant stacking cable connections between the top-most and bottom-most switches in a stack.

Note. For a stacked configuration to have effective redundancy, a redundant stacking cable must be installed between the upper-most and bottom-most switch in the chassis at all times.

The figure below shows how the redundant connection between the top and bottom switches in the stack ensures that data will continue to flow throughout the stack, even in the event of a connection failure at one of the stacking cables.

Stacking Cable Redundancy: Recovery Following a Stacking Link Failure

Redundant stacking cables provide a form of *dual* redundancy. As shown in the figure above, the redundant cable allows traffic to flow in the event of a stacking link failure. The redundant cable also provides failover if a *switch* goes down within the stack. Traffic continues to flow between the modules that remain operational, as shown in the diagram below:

Stacking Cables   *Chassis Front*

① *Data enters slot 1 through an Ethernet port. The data traverses slot 2 via the stacking cables and exits slot 3 through one of its Ethernet ports.*

② *The slot 2 switch goes down unexpectedly. Data can no longer move through slot 2.*

However, because there is a redundant connection (the cable between slot 1 and slot 4), data immediately traverses slot 4 and then exits slot 3 to its destination.

Stacking Cable Redundancy: Recovery Following a Switch Failure within the Stack

Checking Redundant Stacking Cable Status

To check whether a redundant stacking cable connection exists between the top-most and bottom-most switches in the stack, use the **show stack status** command. For example:

```
Redundant cable status  : present
Tokens used             : 1
Tokens available        : 31
```

In this example, a redundant stacking cable connection is present between the top-most and bottom-most switches in the stack.

Slot Numbering

For a stack of OmniSwitch 6350 switches to operate as a virtual chassis, each module in the stack must be assigned a unique slot number. To view the current slot assignments for a stack, use the **show ni** or **show module** commands. The slot number is also displayed on the front panel of each switch by the LED located on the left side of the chassis (refer to "OmniSwitch 6350 LED Status" on page 3-21 for more information).

There are two ways stacking modules are assigned slot numbers:

- Dynamic slot number assignment by the system software

- Manual slot number assignment by the user

Dynamic Slot Number Assignment

Dynamic slot number assignment occurs when there are no **boot.slot.cfg** files present in the switches' /flash directories. This is the case for new, "out of the box," switches that have not been previously booted.

When a brand new stack (or stack with no **boot.slot.cfg** files) is booted, the system software automatically detects the module with the lowest MAC address. This module is assigned the primary management role (see) and, by default, is given the slot number 1. The module connected to the primary's stacking port A is automatically assigned the secondary management role and given the slot number 2.

As the other modules in the stack become operational, they are assigned idle roles and are automatically assigned unique slot numbers. The slot numbering for idle modules is determined by each module's physical location in the stack. Refer to the diagrams below for more information on dynamic slot numbering.

Note. As the slot numbers are dynamically assigned, **boot.slot.cfg** files are auto-generated in the /flash directory of each switch. When modules are subsequently booted, each switch reads its slot number assignment from this file and comes up accordingly.
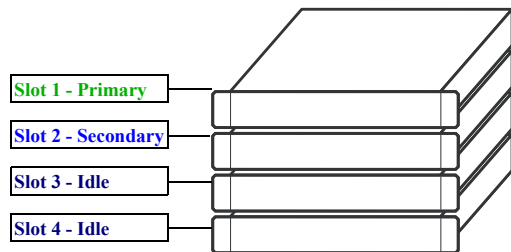
In this example, the fourth switch from the top is elected the primary management module for the stack. (It can be assumed that this switch has the lowest MAC address in the stack.) This switch is automatically assigned slot number 1.

The switch immediately below is connected to the primary switch's stacking port A and, as a result, is assigned the secondary management role and given slot number 2.

The system software allows the switch immediately below slot 2 to have the next slot number preference. It is assigned an idle role and given the slot number 3. The switch immediately below slot 3 is given the slot number 4, and so on. When the bottom of the stack is reached, the slot numbering sequence resumes at the top of the stack, as shown. This helps ensure a more ordered and manageable stack topology.

Dynamic Slot Numbering Example 1

If the switch with the lowest MAC address happens to be the bottom-most module in the stack, slot numbering will not resume from the top of the stack. Instead, the system software will select the secondary module using the standard method (i.e., the switch connected to the primary's stacking port A), then continue to number the stack from the bottom up. This intuitive slot assignment provides the cleanest and most manageable stack topology. Refer to the diagram below for more information:
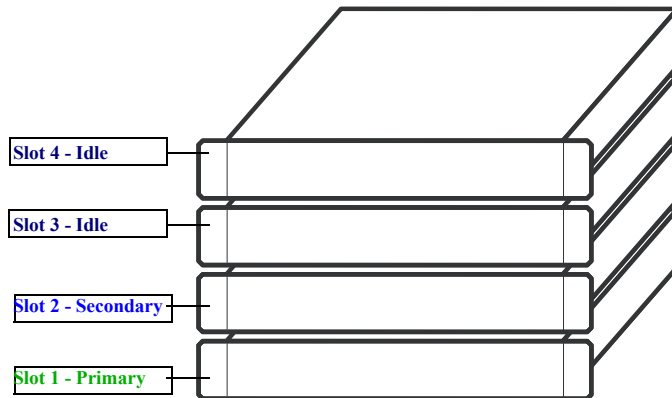
In this example, the bottom switch is elected the primary management module for the stack. (It can be assumed that this switch has the lowest MAC address in the stack.) This switch is automatically assigned slot number 1.

The switch immediately above is connected to the primary switch's stacking port A and, as a result, is assigned the secondary management role and given slot number 2.

The system software then sequentially assigns slot numbers up the stack. In other words, the switch immediately above slot 2 is assigned the slot number 3; the switch immediately above slot 3 is assigned the slot number 4, and so on. This default procedure ensures the most ordered and manageable stack topology out of the box.

Slot 4 - Idle

Slot 3 - Idle

Slot 2 - Secondary

Slot 1 - Primary

Dynamic Slot Numbering Example 2

Manual Slot Number Assignment

To manually assign slot numbers to one or more modules in a stack, use the **stack set slot** command. This command writes slot information to the **boot.slot.cfg** file located in a switch's /flash directory. It is this *saved slot* information that the switch will assume following a reboot.

Manually assigning slot numbers can be useful in reordering existing slot numbers in order to create a sequential numbering scheme from the top of the stack to the bottom (or vice-versa). Refer to the following example:
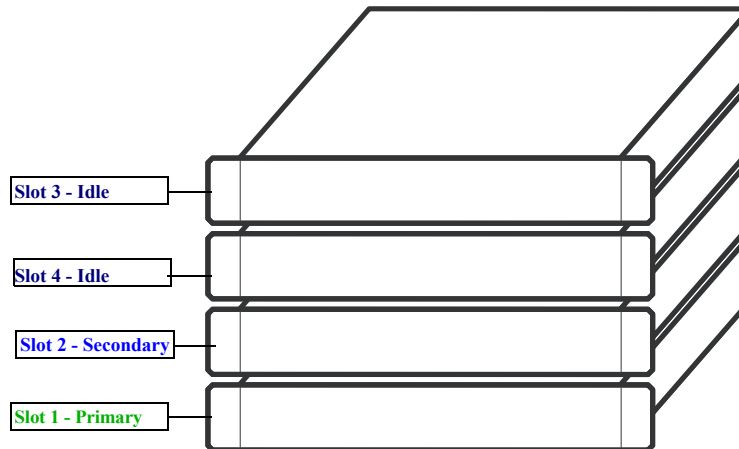
Stack Numbering Before Manual Assignment

This example, taken from page 7-20, shows a stack in which the primary and secondary switches are physically positioned in the middle of the stack. Although the stack will operate normally with this primary and secondary module positioning, it may be preferable for management purposes to have the primary and secondary switches at either the top or the bottom of the stack. For this example, the primary and secondary roles will be assigned to the top of the stack. This is accomplished by entering the following commands:

```
-> stack set slot 3 saved-slot 1
-> stack set slot 4 saved-slot 2
-> stack set slot 2 saved-slot 3
-> stack set slot 1 saved-slot 4
-> reload all
```

Because slot 3 is the top-most switch in the stack, it is reassigned the slot 1 (i.e., primary) position; because slot 4 is located immediately below slot 3, it is reassigned the slot 2 (i.e., secondary) position, etc.

Note that the modules were not reloaded one-by-one, even though the **stack set slot** command provides optional syntax for doing so. Instead, new slot number information is first saved to each **boot.slot.cfg** file across the stack. The reboot is saved for last in order to avoid duplicate slot numbers within the stack, which would cause unwanted pass-though mode conditions (see page 7-12).

When the stack comes up following the reboot, the manually-configured slot numbers display as follows:
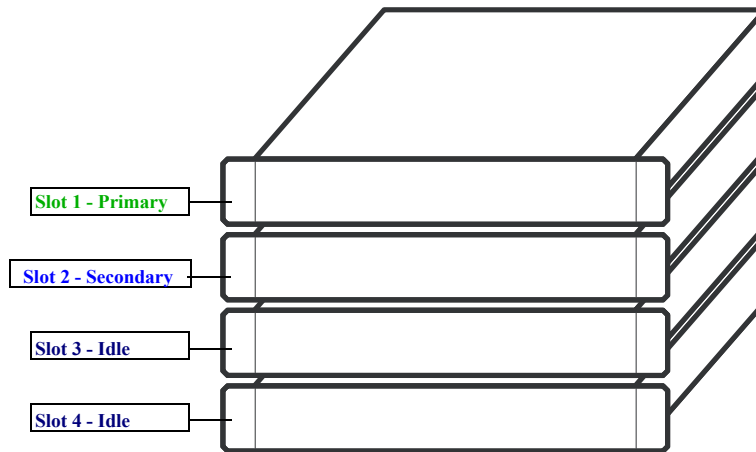
Stack Numbering Before Manual Assignment

The **stack set slot** command can also be used to manually correct duplicate saved slot assignments within the stack topology. Refer to pages 7-12 through 7-14 for detailed information.

Reverting to the Dynamic Slot Numbering Model

To clear the **boot.slot.cfg** files from the stack's /flash directories, use the **stack clear slot** command on all modules and then reboot the stack. For example:

```
-> stack clear slot 1
-> stack clear slot 2
-> stack clear slot 3
-> stack clear slot 4
-> reload all
```

The commands shown above clear the saved slot information from all modules in an eight-module stacked configuration and then reboot the stack. Because the system software no longer has preassigned slot information to read during the boot process, the stack uses the dynamic slot number assignment method described on page 7-20.

Hot-Swapping Modules In a Stack

As with chassis-based switches, NI modules within an OmniSwitch 6350 virtual chassis are hot-swappable. NI modules are essentially those modules operating in the stack in idle mode. These modules can be removed from, or added to, an existing stack without disrupting other modules in the stack.

Removing Switches from an Existing Stack

When removing switches from an existing stack, observe the following important guidelines:

• Do not attempt to hot-swap modules operating in primary or secondary management roles

• Be sure the stacking cables and stacking cable redundancy are not disrupted

Hot-swapping is intended for switches in *idle* and, if applicable, *pass-through* status only. Removing primary or secondary management modules from a stack will trigger a failover sequence, i.e., one or more additional modules within the stack must reload in order to reassign the management roles. Whenever possible, avoid removing a switch that is operating as a primary or secondary management module.

Also, removing a switch from a stacked configuration can disrupt stack cabling at the rear of the stack. When removing a module, be sure that stacking link integrity, including important stacking cable redundancy, is maintained between all remaining modules. For more information on stacking cable connections, refer to page 7-16.

Inserting Switches Into an Existing Stack

When inserting switches into an existing stack, observe the following important guidelines:

• Avoid duplicate saved slot numbers

• Never attempt to operate more than the supported number of switches in a single stack

• Make sure all switches are running the same software version.

To avoid duplicate slot numbers, simply make sure that any modules being added to an existing stack have been cleared of preassigned slot information. In other words, verify that there is no **boot.slot.cfg** file present in the /flash directory of any switch being added. When the switch is connected to the existing stack and booted, the system software automatically assigns it a unique slot number. No duplicate slot errors occur.

Note. If it is preferable to add a switch with an existing **boot.slot.cfg** file to a stack, be sure that the saved slot number of the incoming switch is not already assigned to a switch operating in the stack.

Merging Stacks

Merging stacks involves connecting two or more operational stacks and attempting to reboot them as a single virtual chassis. In most cases, errors will result. To merge stacks without causing errors, select one stack that is to remain up and running and then add modules from the other stack(s) by following the steps below:

1 Make sure all switches are running the same software version.

2 Clear the saved slot information from all incoming modules. This will ensure that they are each assigned unique slot numbers when they join the stack.

3 After clearing the saved slot information, power off all incoming modules.

4 Connect the stacking cables for all incoming modules to the existing, operational stack as required. Be sure to provide stacking cable redundancy. For information on stack cabling, refer to page 7-16.

5 Power on all incoming modules.

Note. No more than eight switches can operate in a single stacked configuration at any time.

Reloading Switches

Reloading is essentially a soft boot of a switch. Users can reload stacked modules operating in any role—i.e., primary, secondary, idle, and pass-through. Refer to the sections below for more information.

Reloading the Primary Management Module

If the switch with the primary management role is reloaded, the switch with the secondary role automatically takes over primary management functions. In other words, the switch with the secondary role assumes the primary role as soon as the reload is initiated.

Meanwhile, the idle switch with the next lowest slot number automatically assumes the secondary role. When the reloaded switch (the former primary module) comes back up, it assumes an idle role within the stack.

To reload the primary management module, use the **reload** command. The optional syntax **primary** can be used in the command line, but is not required. For example:

```
-> reload primary
```

Note. A primary management module reload can also be scheduled for a later time or date. For information on scheduling a primary module reload, as well as additional command details, refer to the *OmniSwitch AOS Release 6 CLI Reference Guide*.

Primary - Slot 1 Secondary - Slot 2 Idle - Slot 3 Idle - Slot 4	① *In this stack of four OmniSwitch 6350 switches, the slot 1 switch is the primary management module. The slot 2 switch is the secondary. Slots 3 and 4 are operating in idle roles.*
-> reload primary	② *The user reloads the stack's primary management module by issuing the reload primary command. Any data flow on the primary switch's Ethernet is interrupted.*
Booting... Primary - Slot 2 Secondary - Slot 3 Idle - Slot 4	③ *The secondary switch automatically takes over the primary role. The idle switch with the next-lowest slot number—in this case, slot 3—automatically becomes the secondary management module. The slot 4 switch remains unaffected. In addition, Ethernet traffic on slots 2, 3, and 4 remains unaffected.*
Idle - Slot 1 Primary - Slot 2 Secondary - Slot 3 Idle - Slot 4	④ *When the rebooted switch comes back up, it assumes an idle role within the stack.*

Reloading the Primary Management Module In a Stack of Three or More

---

If there are only two switches in the stack, the switch that was reloaded (the former primary) assumes the secondary role when it comes back up.

Primary - Slot 1
Secondary - Slot 2

1 *In this stack of two OmniSwitch 6350 switches, the slot 1 switch is the primary management module. The slot 2 switch is the secondary.*

-> reload primary

2 *The user reloads the stack's primary management module by issuing the reload primary command. Any data flow on the primary switch's Ethernet is interrupted.*

Booting...
Primary - Slot 2

3 *The secondary switch automatically takes over the primary role. Ethernet traffic on slot 2 remains unaffected. Meanwhile the stack has no interim secondary management module as the switch reboots.*

Secondary - Slot 1
Primary - Slot 2

4 *When the rebooted switch comes back up, it assumes the secondary management role within the stack.*

Reloading the Primary Management Module In a Stack of Two

Reloading the Secondary Management Module

If the switch with secondary management role is reloaded, the idle switch with the lowest slot number will automatically assume the secondary role. The reloaded switch (the former secondary) will assume an idle role when it comes back up.

Meanwhile, the switch with the primary management role, as well as any other idle modules in the stack, continue operations without interruption.

To reload the secondary management module, use the **reload** command. Be sure to include the syntax **secondary** in the command line. For example:
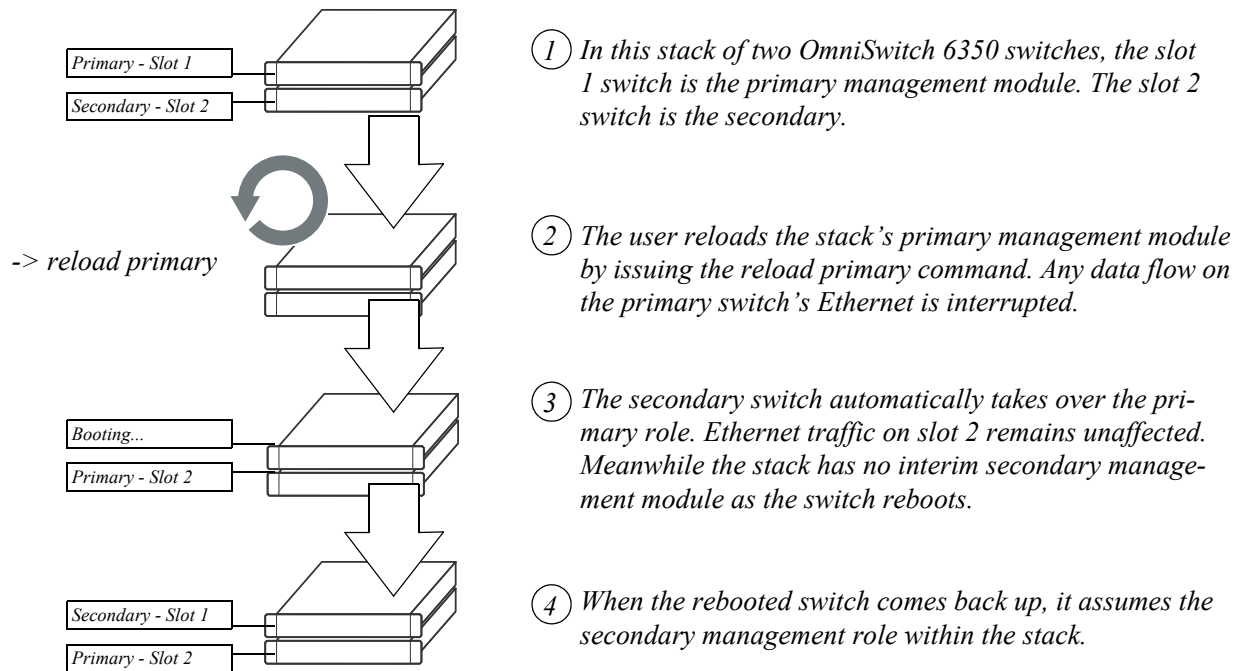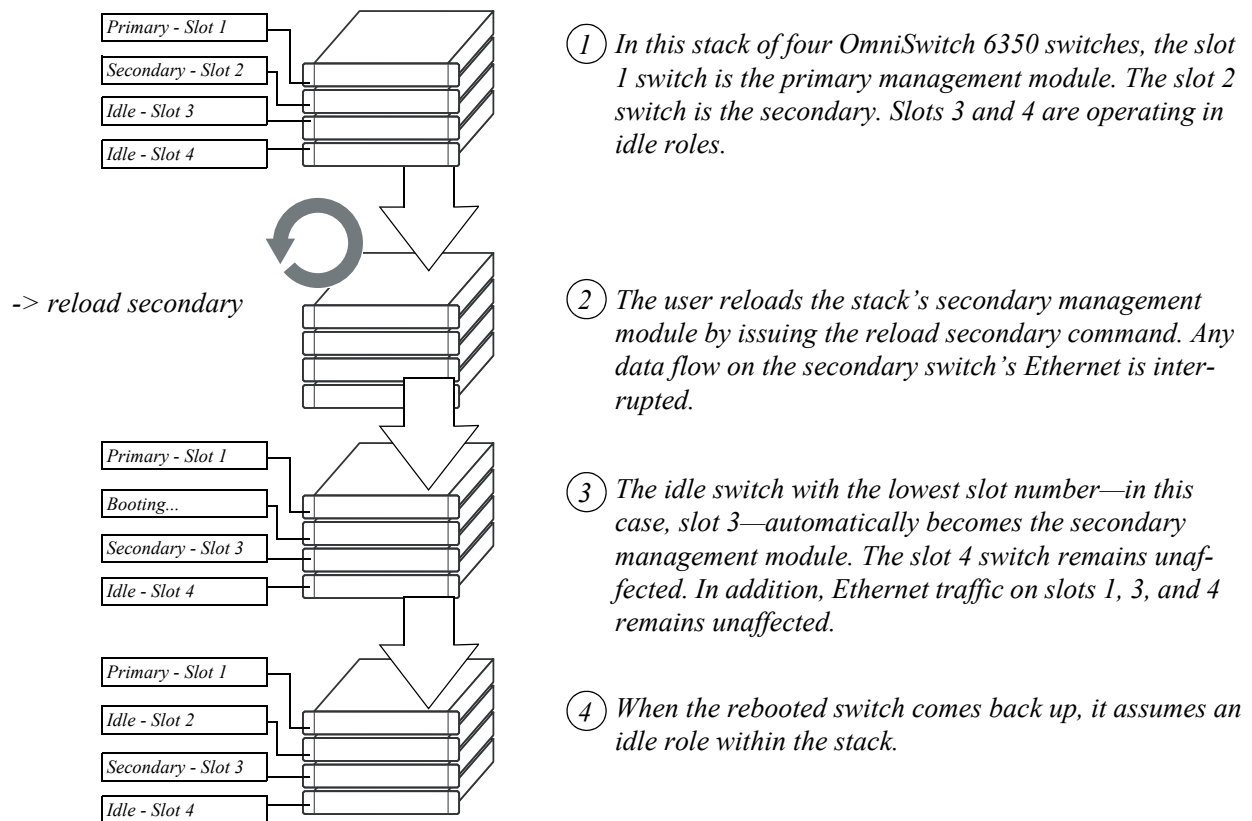
```
-> reload secondary
```

Note. A secondary management module reload can also be scheduled for a later time or date. For information on scheduling a secondary module reload, as well as additional command details, refer to the *OmniSwitch AOS Release 6 CLI Reference Guide.*

Primary - Slot 1
Secondary - Slot 2
Idle - Slot 3
Idle - Slot 4

① In this stack of four OmniSwitch 6350 switches, the slot 1 switch is the primary management module. The slot 2 switch is the secondary. Slots 3 and 4 are operating in idle roles.

-> reload secondary

② The user reloads the stack's secondary management module by issuing the reload secondary command. Any data flow on the secondary switch's Ethernet is interrupted.

Primary - Slot 1
Booting...
Secondary - Slot 3
Idle - Slot 4

③ The idle switch with the lowest slot number—in this case, slot 3—automatically becomes the secondary management module. The slot 4 switch remains unaffected. In addition, Ethernet traffic on slots 1, 3, and 4 remains unaffected.

Primary - Slot 1
Idle - Slot 2
Secondary - Slot 3
Idle - Slot 4

④ When the rebooted switch comes back up, it assumes an idle role within the stack.

Reloading the Secondary Management Module In a Stack of Three or More

If there are only two switches in the stack, the switch that was reloaded (the former secondary) resumes the secondary role when it comes back up.
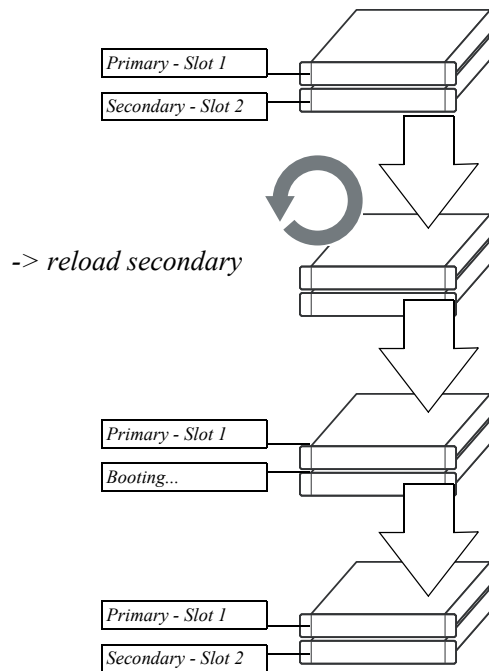
(1) *In this stack of two OmniSwitch 6350 switches, the slot 1 switch is the primary management module. The slot 2 switch is the secondary.*

(2) *The user reloads the stack's secondary management module by issuing the reload secondary command. Any data flow on the secondary switch's Ethernet is interrupted.*

(3) *As the secondary switch reboots, the primary management module continues to operate without interruption. Meanwhile the stack has no interim secondary management module as the switch reboots.*

(4) *When the rebooted switch comes back up, it assumes the secondary management role within the stack.*

Reloading the Secondary Management Module In a Stack of Two

Reloading Switches with Idle Roles

Similar to reloading Network Interface (NI) modules on chassis-based switches, modules operating in idle status within a stack can be reloaded via the CLI.

Note. Any traffic being passed on the module's Ethernet will be interrupted during the reboot. Other modules within the stack will continue to operate without interruption.

To reset a single module operating in idle mode, use the **reload ni** command. Be sure to include the slot number of the idle switch in the command line. For example:

```
-> reload ni 3
```

Only one idle switch can be reloaded at a time. In order to reload multiple idle switches at once, the entire stack must be reloaded using the **reload all** command.

After reloading a switch operating in an idle role, the switch resumes idle status when it comes back up, *despite its saved slot number*. In other words, if an idle switch with a saved slot number of 1 is reloaded, it resumes its previous idle role. Although it has the lowest possible saved slot number, it does not take over the primary management role. In order for this switch to take over the primary role, all switches in the stack must be reloaded.

Note. For more information on reloading all the switches in a stack, refer to . For more information on idle status, refer to .

Reloading Switches in Pass-Through Mode

Pass-through mode is a state in which a switch has attempted to join a stack but has been denied primary, secondary, and idle status. Because this is essentially an error state, the pass-through condition must be resolved and any modules operating in pass-through mode must be reloaded.

To reload a module operating in pass-through mode, use the **reload pass-through** command. Be sure to include the slot number of the pass-through switch in the command line. For example:

```
-> reload pass-through 1001
```

Note. Before issuing the **reload pass-through** command, be sure to resolve any conditions causing the switch to operate in pass-through mode. Otherwise, the switch is likely to come up again in pass-through mode. For detailed information, including steps used to recover from pass-through, refer to .

Reloading All Switches in a Stack

Reloading all switches in the stack is essentially a full reboot of the virtual chassis. This can be useful in restoring a stack's previously configured topology—i.e., the stack's saved slot numbers and management roles. Note, however, that all data flow on the stack is interrupted whenever a full reboot is issued.

To reset all switches in a stack use the **reload all** command. For example:

```
-> reload all
```

Note. Before issuing the **reload all** command, be sure to read the sections below. Understanding topics such as software synchronization and the effects of saved slot information can help users avoid unexpected results following a full stack reboot.

Software Synchronization During a Full Reload

If the checksum value on the stack's non-primary switches differs in any way from the checksum value on the primary switch, the primary switch automatically distributes its system and configuration software to all other switches in the stack whenever a full reload is executed.

During this automatic software synchronization, system and configuration software on the secondary and idle switches is overwritten. Because the primary switch's "last known good" software is propagated to all switches, the synchronization process helps ensure effective redundancy across the stack.

Effects of Saved Slot Number Information on the Reload Process

Depending on the status of saved slot information across the stack, there are different slot numbering and management role scenarios that can occur following a full reboot. For this reason, checking the current stack topology before issuing a full reboot is strongly recommended. To check the current stack topology, use the **show stack topology** command. Refer to the *OmniSwitch AOS Release 6 CLI Reference Guide* for detailed command information.

Possible saved slot number conditions include:

- All switches have unique saved slot information

- No switches in the stack have saved slot information

- Some switches have saved slot information, others do not

- Two or more switches have duplicate slot information

All Switches Have Unique Saved Slot Information

If a full reload is issued and all switches have unique slot numbers saved to their **boot.slot.cfg** files, the slot numbers will be assigned according to the saved slot information. The primary management role will be given to the switch with the *lowest* saved slot number. The secondary management role will be given to the switch with the *second-lowest* saved slot number. All other switches will be assigned to idle roles.

An illustrated example of this method for assigning slot numbers and management roles is provided on pages and .

No Switches In the Stack Have Saved Slot Information

If a full reload is issued and no switches in the stack have unique slot numbers, slot numbers will be assigned beginning with the switch with the lowest MAC address. (This can occur if the **boot.slot.cfg** file has been deleted from each switch's /flash directory—e.g., by issuing the **stack clear slot** command for all modules in the stack.)

The switch with the lowest MAC address is assigned slot number 1 and given the primary management role. The switch connected to stacking port A of the primary switch is automatically assigned slot number 2 and given the secondary management role. Stack cabling is then used to determine the dynamic slot numbering of the remaining modules in the stack. The switch immediately adjacent to slot 2 is assigned slot number 3 and given an idle role, etc.

An illustrated example of this method for assigning slot numbers and management roles is provided on pages 7-20 and 7-21.

Some Switches Have Saved Slot Information, Others Do Not

If only *some* switches in the stack have **boot.slot.cfg** files in their /flash directories, the system software will first read the contents of these files and then dynamically assigns unique slot numbers to any switches that do not have saved slot information. The primary management role will be given to the switch with the *lowest* saved slot number. The secondary management role will be given to the switch with the *second-lowest* saved slot number. All other switches will be assigned to idle roles.

When unique slot numbers are dynamically assigned by the system software, a **boot.slot.cfg** file is automatically generated with the new slot information. Because all switches now have unique saved slot information, any subsequent **reload all** commands issued will cause the stack to come up as described in the section, "All Switches Have Unique Saved Slot Information" on page 7-31.

Two or More Switches Have Duplicate Slot Information

If a full stack reboot is issued and the same slot number is found in the **boot.slot.cfg** file of two or more switches, the switch with the lowest MAC address is allowed to come up and operate normally. Meanwhile, any other switches with the duplicate slot number come up in *pass-through mode*.

The pass-through mode is essentially an error state in which a switch has been denied primary, secondary, and idle roles within the stack. When a switch is in pass-through mode, its Ethernet are brought down and cannot pass traffic. It is for this reason that users should always check the current saved slot number for each switch before issuing the **reload all** command. To check the current saved slot information across the stack, use the **show stack topology** command. For detailed information on pass-through mode, refer to "Pass-Through Mode" on page 7-12.

Avoiding Split Stacks

The term "splitting" a stack refers to the creation of isolated modules within the virtual chassis. A split stack can result from the following conditions:

- Two or more *non-adjacent* switches are reloaded simultaneously

- The stack is reloaded without a redundant stacking cable connection

The sections below offer simple guidelines for avoiding splitting the stack during the reload process.

Do Not Reload Non-Adjacent Switches Simultaneously

If non-adjacent switches in the stack—for example, the top switch in the stack and the third-from-top switch in the stack—are reloaded *simultaneously*, a problem will occur. The switch between the two non-adjacent switches will become isolated and the virtual chassis will be effectively split.

To avoid splitting the stack, do not reload the two non-adjacent switches simultaneously. Instead, simply reload the top switch first, then reload the third-from-top switch, or vice-versa.

Be Sure a Redundant Stacking Cable is Installed at All Times

Another important guideline for avoiding split stacks involves the redundant stacking cable. In order to avoid isolated modules within the virtual chassis, simply make sure that a redundant stacking cable connection exists between the top-most and bottom-most switches at all times.

For more information on the redundant stacking cable connection, refer to .

Changing the Secondary Module to Primary

OmniSwitch 6350 stacks allow users to manually force the secondary switch to assume the primary management role. This is referred to as "takeover." The behavior of a takeover is similar to that of reloading the primary management module (see page 7-26).

Whenever a takeover is initiated, the switch with the secondary role automatically takes over primary management functions. The primary switch is automatically reloaded and any traffic being passed on the primary switch's Ethernet is interrupted.

Meanwhile, the idle switch with the next-lowest slot number automatically assumes the secondary role. When the former primary module comes back up, it assumes an idle role within the stack.

To initiate a takeover sequence, use the **takeover** command. For example:
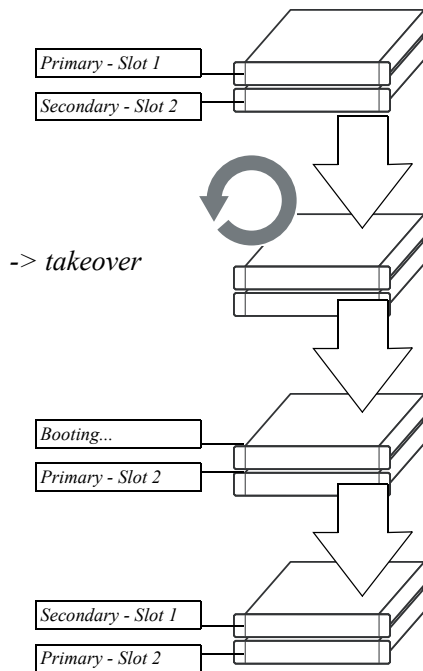
```
-> takeover
```

Note. Before using the **takeover** command, verify that the switches in the stack are synchronized. Otherwise, data flow and switch management functions may be interrupted due to incorrect or outdated software when a switch takes over the primary management role. For more information, refer to "Synchronizing Switches in a Stack" on page 7-36.
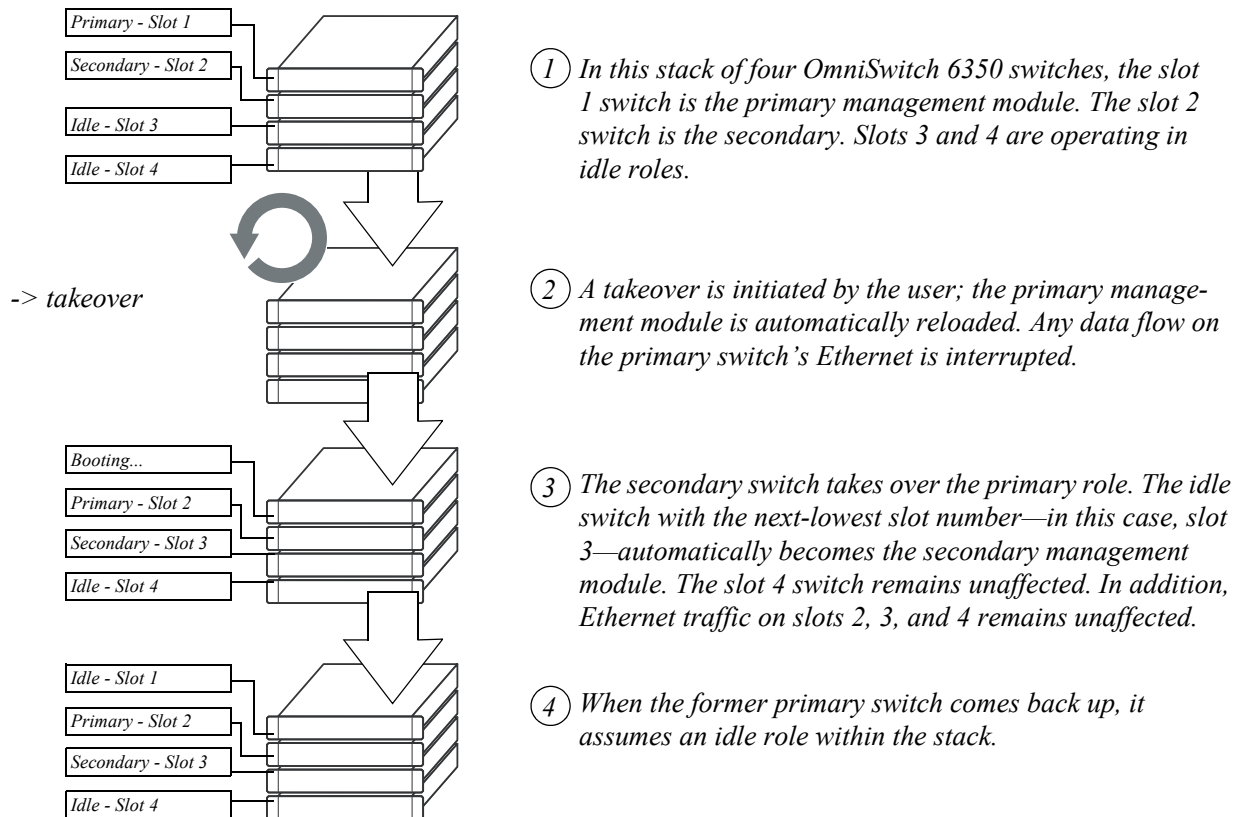
---

1. *In this stack of four OmniSwitch 6350 switches, the slot 1 switch is the primary management module. The slot 2 switch is the secondary. Slots 3 and 4 are operating in idle roles.*

2. *A takeover is initiated by the user; the primary management module is automatically reloaded. Any data flow on the primary switch's Ethernet is interrupted.*

3. *The secondary switch takes over the primary role. The idle switch with the next-lowest slot number—in this case, slot 3—automatically becomes the secondary management module. The slot 4 switch remains unaffected. In addition, Ethernet traffic on slots 2, 3, and 4 remains unaffected.*

4. *When the former primary switch comes back up, it assumes an idle role within the stack.*

Takeover Behavior In a Stack of Three or More

If there are only two switches in the stack, the former primary switch resumes the secondary role when it comes back up following the takeover.

1 *In this stack of two OmniSwitch 6350 switches, the slot 1 switch is the primary management module. The slot 2 switch is the secondary.*

Primary - Slot 1
Secondary - Slot 2

-> takeover

2 *A takeover is initiated by the user; the primary management module is automatically reloaded. Any data flow on the primary switch's Ethernet is interrupted.*

Booting...
Primary - Slot 2

3 *The secondary switch takes over the primary role. Ethernet traffic on slot 2 remains unaffected. Meanwhile the stack has no interim secondary management module as the switch reboots.*

Secondary - Slot 1
Primary - Slot 2

4 *When the former primary switch comes back up, it assumes the secondary management role within the stack.*

Takeover Behavior In a Stack of Two

Synchronizing Switches in a Stack

Management module synchronization refers to the process of copying all files in the **/flash/working** and **/flash/certified** directories of the primary management module to the **/flash/working** and **/flash/certified** directories of all the other switches in the stack. The system and configuration software on the non-primary switches—i.e., the secondary management module and any modules operating in idle—is overwritten.

The synchronization process ensures that the contents of these directories match exactly for all switches across the stack. This can be especially useful after new software has been loaded to the primary management module. Further, synchronization prevents any switch from assuming a management role within the stack with incorrect or outdated software or configuration files. Because the primary switch's "last known good" software is propagated to all switches, the synchronization process helps ensure effective redundancy across the stack.

In order to maintain effective management module redundancy, switches in the stack must be synchronized at all times. To determine whether a stack is in need of synchronization, use the **show running-directory** command. For example:

```
-> show running-configuration


CONFIGURATION STATUS
   Running CMM              : PRIMARY,
   CMM Mode                 : MONO CMM,
   Current CMM Slot         : 1,
   Running configuration    : CERTIFIED,
   Certify/Restore Status   : CERTIFY NEEDED
SYNCHRONIZATION STATUS
   Running Configuration    : NOT SYNCHRONIZED,
```

This example shows a switch on which the /flash directories between the management modules are not synchronized. To manually synchronize all switches in the stack, enter the following command:

```
  -> copy working certified flash-syncro
```

When the synchronization process is initiated, modules within the stack continue to operate without interruption and data flow across the stack is unaffected.

Automatic Synchronization During a Full Reload

If the checksum value on the stack's non-primary switches differs in any way from the checksum value on the primary switch, the primary switch automatically distributes its system and configuration software to all other switches in the stack whenever a full reload is executed.

For more information on initiating a full reload, see "Reloading All Switches in a Stack" on page 7-31.

Note. For more information on management module synchronization and managing the **/flash/working** and **/flash/certified** directories, refer to the "Managing CMM Directory Content" chapter in the *OmniSwitch AOS Release 6 Switch Management Guide*.

Stack Topology Change Notification

This feature will send a trap whenever there is a change to the stack topology such as an element being removed or added to the stack. A file (*stack_topology.txt*) containing topology information is saved and synchronized across the stack in the **/flash/switch** directory. This file is initially created 10 minutes after the element is ready and will then be updated 10 minutes after any changes in the stack topology.

Every 10 minutes the current stack topology will be compared to the topology saved in the *stack_topology.txt* file. If there is any difference between the current stack topology and the topology in the *stack_topology.txt* file a trap will be sent and the file will be updated and synchronized across the stack. The trap will have information regarding slot number, chassis name, management IP address and whether the element has been removed or added. The file will exist on a standalone switch but is not applicable and no traps will be sent.

Scenario	Description	Trap
Reload of stack	Entire stack reboots and one or more elements does not rejoin.	Trap will be sent 10 minutes after primary element is ready.
	Entire stack reboots and all elements rejoin with no issues.	Trap will not be sent.
Reload of stack element	Any element reboots but does not rejoin.	Trap will be sent 10 minutes after reboot of that element.
	Any element reboots and rejoins with no issues.	Trap will not be sent.
Takeover	All elements rejoin correctly after take-over.	Trap will not be sent.
	Any element does not rejoin after take-over.	Trap will be sent 10 minutes after primary element is ready.
Element added	New element added to the existing stack.	Trap will be sent 10 minutes after that element joins the stack.
Element removal	Element removed from the existing stack.	Trap will be sent 10 minutes after element removal
Standalone switch	Standalone switch	Trap will not be sent.

If stack split protection is enabled and a split occurs then a trap to indicate an element is down will be sent for the elements transitioning to protection mode after 10 minutes. If any element in protection mode rejoins the stack then a trap indicating an element rejoining the stack will be sent 10 minutes after rejoining. In both cases the *stack_topology.txt* file will be updated and synchronized across the stack.

Stack Topology Change Notification - Confirmation

When issuing the **write memory** command if any one of the stack elements is down the configuration for that element is lost. When the **write memory** command is issued the current stack topology will be compared against the saved stack topology and if there is any difference then a warning will be issued about possible configuration purge and ask for confirmation from the user to proceed. If the user confirms, the existing configuration for the element which is down will not be saved. If the user does not confirm then the write memory operation will not proceed. This will ensure that configurations will not be lost without notification to the user.

Stack Split Detection (SSP)

In the case of a stack split due to a stacking link failure or the failure of one of the stack elements, both of the resulting stacks could end up having the same system MAC and IP addresses. Since there is no communication between these individual stacks due to the stacking link failure they end up communicating with the rest of the network devices using the same MAC and IP addresses. This stack split scenario is disruptive to the network as the conflicting MAC and IP addresses can lead to layer 2 loops and L3 traffic disruption.

Stack Split Detection provides the following benefits:

- Avoid network disruptions by preventing duplicate MAC and IP addresses on the network when MAC retention is enabled and a stack split occurs.

- The sub-stack that forms out of the stack split is able to detect that a stack split has occurred.

- Once the stack split condition has been determined, the sub-stack will put its front-panel ports into an operationally down state preventing traffic forwarding and avoiding loops and possible traffic disruption. The SSP link will be shut down after the protection mode SSP PDU is sent to the helper and the acknowledgment is received from the helper by the protection mode unit.

- A trap can be sent by the active-stack indicating the stack split state. The trap indicates that the stack split has occurred and which elements are in the operationally down sub-stack.

- A mechanism is available to recover the non-operational sub-stack.

A redundant stacking cable connection should be used for proper SSP functionality. For more information on helping to avoid stack splits with redundant stacking cable connections, refer to .

Stack Split Key Components and Terms

- **SSP PDU** - A proprietary packet forwarded between stack elements to help determine that state of the stack.

- **SSP Helper** - A neighboring OmniSwitch, not an element of the stack, responsible for forwarding SSP PDUs between the stack elements. The SSP feature and the SSP Helper functionality cannot be enabled on the same switch for the same link aggregate ID.

- **SSP Link Aggregate** - A dedicated link aggregate configured between elements of a stack and a helper switch to be used for forwarding SSP PDUs.

- **Active-stack -** An element, or multiple elements, that results when a split stack occurs. The active-stack will keep its front panel ports enabled and continue to forward traffic on the network.

- **Sub-stack -** An element, or multiple elements, that results when a split stack occurs. The sub-stack will disable its front panel ports to prevent traffic disruption caused by duplicate MAC/IP addresses with the active stack.

- **Protection State** - A state an element will transition to after determining a stack split has occurred. Its ports will be operationally disabled to to prevent duplicate MAC and IP addresses and network disruption.

- **Guard Timer** - A configurable timer determining how long a unit will wait before beginning to send SSP PDUs after a stack recovery.

Basic Operation

When stack split detection is enabled, a proprietary protocol runs on a configured link aggregate to carry the stack information necessary for stack split detection. Stack elements share a link aggregate with an OmniSwitch that can act as a helper to assist in the stack split detection.

The lowest member port of the link aggregate hosted on the primary element is responsible for sending the SSP PDUs on the member link. When the packet arrives on the remote helper device then the helper device will forward the packet out on all member ports of the link aggregate so that the packet reaches the remote stack elements.

Use the the **stack split-protection** and **stack split-protection linkaggid** commands to enable SSP and create the SSP link aggregate on the stack.

Use the the **stack split-protection helper** and **stack split-protection helper linkagg** commands to enable the SSP helper and create the SSP helper link aggregate on the helper switch.

Protection States

Under normal stack circumstances the SSP PDUs are sent once every 3 seconds. When the stack detects a scenario which leads to a change in its size the protocol sends the SSP PDUs at a rate of 1 per 250 milliseconds for 120 seconds. This helps to quickly identify a stack split.

On reception of a SSP frame, the receiving elements match the primary of their current stack against the MAC address of the SSP sender. If there is a mismatch between the two, then that indicates the presence of an active stack in the network which is disconnected from the current stack. In this condition the stack element will monitor 3-5 such consecutive frames, after which it will transition to the **protection state**.

When an element transitions to the protection state, the following occurs:

- Each of the stack elements will independently transition into the protection state.

- In the protection state each of the stack elements will disable all the user ports except the ones belonging to the SSP protection link aggregate.

- The stack element will store the protection state transition information in a non-volatile location (EEPROM/ boot.params). This information will be used whenever an element in the protection state re-boots and needs to check its current operational state.

- An element in the protection state will send an SSP PDU back on the link aggregate carrying the SSP state as PROTECTION. This is the only frame that is sent by the protection sub-stack. The purpose of this message is to inform the active-stack to generate an SNMP trap regarding the stack split state of the stack element.

Stack Split Recovery

Once a sub-stack goes into the protection state then all the front panel ports are put into an operationally down state. There are two ways to recover the stack, manually or automatically.

Manual Recovery:

If the guard timer is 0, automatic recovery is disabled and the sub-stack stays in protection mode until the unit is reloaded by the administrator. After the re-boot the administrator has to manually recover the switch by first disabling SSP and then re-enabling SSP. This clears the protection state variables stored in the EEPROM/boot.params.

Use the **stack split-protection guard-timer** and the **stack split-protection** commands to configure the guard timer and enable/disable SSP.

Automatic Recovery

If the stacking link recovers and the sub-stack reconnects to the active stack the sub-stack will automatically reboot. The protection units will come up in the protection state; however they will now be part of the active stack but their front panel ports will still be disabled. The primary of the combined stack will detect that there are new elements in the protection state. The primary will wait for the guard timer to expire and will then bring one element at a time from the protection state until all elements are active.

Once complete, the primary will generate a trap indicating the stack has been recovered.

① Normal Operation
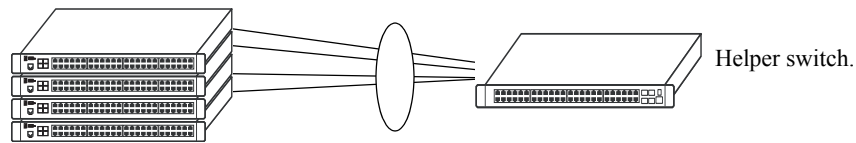
Helper switch.

SSP PDUs sent over helper linkagg and relayed by helper switch.

② Stack Split

Active-stack
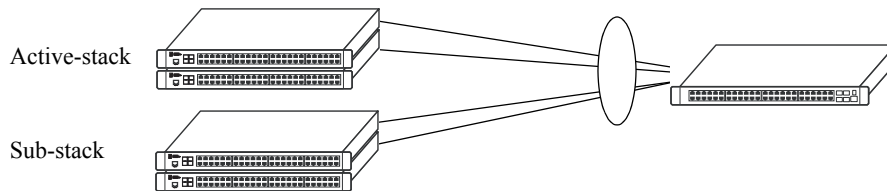
Sub-stack

1. Stack split detected, substack transitions to PROTECTION state.
2. Sub-stack front panel ports shutdown to avoid duplicate addresses on network
3. PROTECTION PDUs sent by sub-stack to active-stack over helper linkagg.
4. Active-stack sends trap indicating stack split.

③ Recovery

Helper switch.
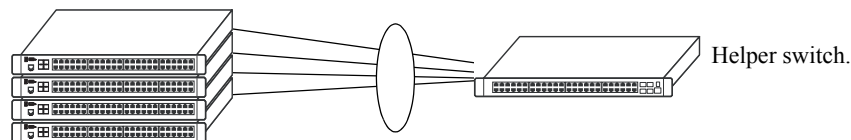
1. Stacking link recovers, new elements detected by Primary.
2. Manual Recovery - Administrator disables/enables SSP to clear PROTECTION state.
3. Automatic Recovery - After guard-timer expiration, Primary will bring up elements one at a time.
4. Once stack is functioning, Primary will send trap indicating stack recovery.

Stack Split Example

Monitoring the Stack

As shown in the previous sections, monitoring the current status and operation of all elements in a stack can help users avoid unexpected stack conditions. The table below includes CLI commands that are useful in monitoring stack conditions.

CLI Commands Used for Monitoring a Stack	
show stack topology	Displays the current operating topology of switches within a stack.
show stack status	Displays the current redundant stacking cable status.
show running-directory	Displays the directory from where the switch was booted. This command also shows important information, including whether the software across the stack is synchronized.
show chassis	Displays basic configuration and status information for the switch chassis.
show cmm	Displays basic hardware and status information for primary and secondary management modules operating in the stack.
show ni	Displays basic hardware and status information for modules currently operating in the stack.
show module	Displays basic information for modules installed in the stack. Modules include primary and secondary management modules and any modules operating in idle status.
show module long	Displays detailed information for modules installed in the stack. Modules include primary and secondary management modules and any modules operating in idle status.
show module status	Displays basic status information for modules installed in the stack. Modules include primary and secondary management modules and any modules operating in idle status.
show power	Displays hardware information and current status for chassis power supplies. This includes the status of backup power supplies, if applicable.
show fan	Displays the current operating status of each of the six fans operating in each chassis.
show temperature	Displays the current operating chassis ambient temperature, as well as current temperature threshold settings for each of the modules in the stack.

Visually Monitoring the Stack

Users can also monitor many stack operations by viewing the front panel LEDs on all elements in the stack. Refer to "OmniSwitch 6350 LED Status" on page 3-21 for detailed information on LEDs and stack status.

CLI Commands Supported on Both Primary and Secondary Management Modules

Although most CLI commands are executed when logged into the switch with the primary management role, there is a group of commands that is supported when logged in to either the primary or secondary management module. For a list of these commands, refer to the tables below.

Note. For detailed information on these commands, including command syntax options and definitions, refer to the *OmniSwitch AOS Release 6 CLI Reference Guide*.

CMM Commands

reload	**debug chassis auto-reboot**	**show microcode**
takeover	**show running-directory**	
install	**show reload**	

Chassis Management and Monitoring Commands

show system	**show module**	**show cmm**
show hardware info	**show module long**	**show ni**
show chassis	**show module status**	

File Management Commands

cd	**delete**	**ed**
pwd	**cp**	**vi**
mkdir	**mv**	**view**
rmdir	**move**	**tty**
ls	**chmod**	**show tty**
dir	**attrib**	**rz**
rename	**fsck**	**more**
rm	**newfs**	**install**

Switch Logging and Monitoring Commands

swlog	**debug ktrace**	**debug systrace show**
swlog appid level	**debug ktrace appid level**	**debug systrace show log**
swlog output	**debug ktrace show**	**debug memory monitor**
show log swlog	**debug systrace**	**debug memory monitor show log**
show swlog	**debug systrace appid level**	

Memory Monitoring Commands

show log pmd

A Regulatory Compliance and Safety Information

This appendix provides information on regulatory agency compliance and safety for OmniSwitch 6350 switches.

Declaration of Conformity: CE Mark

This equipment is in compliance with the essential requirements and other provisions of Directive 2004/108/EC (EMC), 2006/95/EC (LVD), 91/263/EEC (Telecom Terminal Equipment, if applicable), 1999/5/EC (R&TTE, if applicable).

Français: Cet équipement est conforme aux exigences essentielles et aux autres provisions de la Directive 2004/108/EC (EMC), 2006/95/CE (LVD), 91/263/CEE (équipements terminaux de télécommunications, le cas échéant), 1999/5/EC (R&TTE, le cas échéant).

Deutsch: Diese Ausrüstung erfüllt die wesentlichen Anforderungen und sonstigen Bestimmungen der Richtlinien 2004/108/EG (EMV-Richtlinie), 2006/95/EG (Niederspannungsrichtlinie), 91/263/EWG (Telekommunikationsendeinrichtungen, falls zutreffend), 1999/5/EG (Funkanlagen und Telekommunikationsendeinrichtungen, falls zutreffend).

Español: Este equipo cumple los requisitos esenciales y otras disposiciones de las directivas 2004/108/CE (EMC), 2006/95/CE (LVD), 91/263/CEE (equipos terminales de telecomunicación, si procede), 1999/5/CE (R&TTE, si procede).

China RoHS: Hazardous Substance Table

部件名称 Part Name	有毒和危险品 Toxic and Hazardous Substances or Elements					
	铅 (Pb)	水银 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴化苯 (PBB)	多溴化二苯醚 (PBDE)
电路模块 (Circuit Boards)	X	O	O	O	O	O
电缆及电缆组件 (Cables & Cable Accessories)	X	O	O	O	O	O
金属部件 (Metal Parts)	X	O	O	O	O	O
塑料和聚合物部件 (Plastic and Polymeric parts)	O	O	O	O	O	O
可插拔模块 (Pluggable modules)	X	O	O	O	O	O
电池 (Batteries)	O	O	O	O	O	O

本表格依据 SJ/T 11364 的规定编制

O = 表示该有害物质在该部件所有均质材料中的含量均在 GB/T 26572 规定的限量要求以下 (indicates that the content of the toxic and hazardous substance in all the Homogeneous Materials of the part is below the concentration limit requirement as described in GB/T 26572).

X = 表示该有害物质至少在该部件的某一均质材料中的含量超出 GB/T 26572 规定的限量要求 (indicates that the content of the toxic and hazardous substance in at least one Homogeneous Material of the part exceeds the concentration limit requirement as described in GB/T 26572).

Taiwan RoHS: Hazardous Substance Table

<table>
<tr><td colspan="7" align="center">设备名称：交换机和路由器產品</td></tr>
<tr><td rowspan="2">单位</td><td colspan="6" align="center">受限物质及其化学符号</td></tr>
<tr><td>铅
(Pb)</td><td>汞
(Hg)</td><td>镉
(Cd)</td><td>六价铬
(Cr+6)</td><td>多溴联苯 (PBB)</td><td>多溴二苯醚
(PBDE)</td></tr>
<tr><td>電路板
(Circuit Boards)</td><td>-</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td></tr>
<tr><td>電纜及電纜配件
(Cables & Cable Accessories)</td><td>-</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td></tr>
<tr><td>金屬部件
(Metal Parts)</td><td>-</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td></tr>
<tr><td>塑料和聚合物部件
(Plastic and Polymeric Parts)</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td></tr>
<tr><td>可插拔模塊
(Pluggable modules)</td><td>-</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td></tr>
<tr><td>電池
(Batteries)</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td></tr>
<tr><td colspan="7">注 1: "○" 表示该项受限物质的含量百分比未超过百分比含量基准值。
注 2: "-" 表示该项受限物质为排除项目。</td></tr>
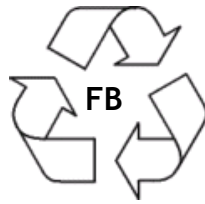</table>

California Proposition 65 Warning

WARNING: This product can expose you to chemicals including Pb and Pb compounds, which is known to the State of California to cause cancer and birth defects or other reproductive harm. For more information go to www.P65Warnings.ca.gov.

Products are packaged using one or more of the following packaging materials:
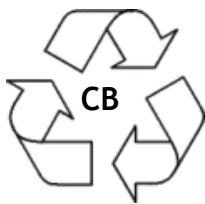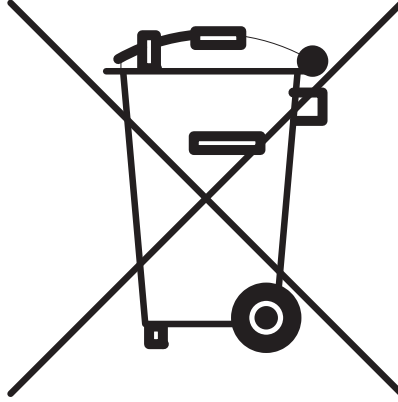

Corrugated Cardboard   Corrugated Fiberboard   Low-Density Polyethylene

Waste Electrical and Electronic Equipment (WEEE) Statement

The product at end of life is subject to separate collection and treatment in the EU Member States, Norway and Switzerland and therefore marked with the symbol:

Treatment applied at end of life of the product in these countries shall comply with the applicable national laws implementing directive 2002/96EC on waste electrical and electronic equipment (WEEE).

Standards Compliance

Safety Standards

- UL 60950-1, 2nd Edition
- CAN/CSA-C22.2 No. 60950-1-07, 2nd Edition
- EN 60950-1 with Amendment II
- IEC 60950-1 2nd Edition
- AS/NZS TS-001 and 60950, Australia
- UL-AR, Argentina
- TUV,UL-GS Mark, Germany
- NOM-019 SCFI, Mexico
- EN 60825-1 Laser
- EN 60825-2 Laser
- CDRH Laser
- CB Certification per IEC 60950-1, Second Edition

EMC Standards

- FCC Part 15 (CFR 47) Class A
- ICES-003 Class A
- EN 55022 Class A
- CISPR 22 Class A
- AS/NZS 3548 Class A
- VCCI Class A; A1 and A2
- EN 55024 (Immunity)
- EN 61000-3-2
- EN 61000-3-3
- EN 61000-4-2
- EN 61000-4-3
- EN 61000-4-4
- EN 61000-4-5
- EN 61000-4-6
- EN 61000-4-8
- EN 61000-4-11

Environmental Standards

- ETS 300 019 Storage Class 1.1
- ETS 300 019 Transportation Class 2.3
- ETS 300 019 Stationary Use Class 3.1

FCC Class A, Part 15

This equipment has been tested and found to comply with the limits for 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 instructions in this guide, may cause 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.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.It is suggested that the user use only shielded and grounded cables to ensure compliance with FCC Rules.

If this equipment does cause interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

• Reorient the receiving antenna.

• Relocate the equipment with respect to the receiver.

• Move the equipment away from the receiver.

• Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions.

Canada Class A Statement

This equipment does not exceed Class A limits per radio noise emissions for digital apparatus, set out in the Radio Interference Regulation of the Canadian Department of Communications.

Avis de conformitè aux normes du ministère des Communications du Canada

Cet èquipement ne dèpasse pas les limites de Classe A d íèmission de bruits radioèlectriques pour les appareils numèriques,telles que prescrites par le RÈglement sur le brouillage radioèlectrique ètabli par le ministère des Communications du Canada.

JATE

This equipment meets the requirements of the Japan Approvals Institute of Telecommunications Equipment (JATE).

CISPR22 Class A Warning

This is a Class A product. In a domestic environment, this product may cause radio interference. Under such circumstances, the user may be requested to take appropriate countermeasures.

Korea Emissions Statement

A 급 기기 (업무용 방송통신 기자재)

이 기기는 업무용 (A 급) 전자파적합기기로서 판

매자 또는 사용자는 이 점을 주의하시기 바라

며 , 가정외의 지역에서 사용하는 것을 목적으

로 합니다 .

Class A Equipment (Business equipment)

This equipment is registered for Electromagnetic Conformity Registration as business equipment (A), not home equipment. Sellers or users are required to take caution in this regard.

VCCI

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Class A Warning for Taiwan and Other Chinese Markets

This is a Class A Information Product. When used in a residential environment, it may cause radio frequency interference. Under such circumstances, the user may be requested to take appropriate counter-measure.

Network Cable Installation Warning

Never install exposed network cables outdoors. Install network cables per manufacturer requirements.

Translated Safety Warnings

Chassis Lifting Warning

Two people are required when lifting the chassis. Due to its weight, lifting the chassis unassisted can cause personal injury. Also be sure to bend your knees and keep your back straight when assisting with the lifting of the chassis.

Français: Le châssis doit être soulevé par deux personnes au minimum. Pour éviter tout risque d'accident, maintenez le dos droit et poussez sur vos jambes. Ne soulevez pas l'unité avec votre dos.

Deutsch: Sicherheitshinweise
Hinweise zur Anhebung des Chassis

Zum Anheben des Chassis werden zwei Personen benötigt. Aufgrund des Gewichts kann das Anheben ohne Unterstützung zu Personenschäden führen. Heben Sie das Chassis aus den Knien und halten Sie den Rücken gerade wenn Sie beim Anheben des Chassis assistieren.

Español: Se requieren dos personas para elevar el chasis. Para evitar lesiones, mantenga su espalda en posición recta y levante con sus piernas, no con su espalda.

Electrical Storm Warning

To avoid a shock hazard, do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.

Français: Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage.

Deutsch: Hinweise bei Unwetter
Um elektrische Schläge zu vermeiden dürfen während eines Gewitters and diesem Gerät keine Kabel angeschlossen oder gelöst werden, sowie keinerlei Installationen, Wartungen oder Konfigurationen vorgenommen werden.

Español: Para evitar peligro de descargas, no conecte o desconecte ningun cable, ni realice ninguna instalación, maintenimiento o reconfiguración de este producto durante una tormenta eléctrica.

Installation Warning

Only personnel knowledgeable in basic electrical and mechanical procedures should install or maintain this equipment.

Français: Toute installation ou remplacement de l'appareil doit être réalisée par du personnel qualifié et compétent.

Deutsch: Installationshinweise
Dieses Gerät soll nur von Personal installiert oder gewartet werden, welches in elektrischen und mechanischen Grundlagen ausgebildet ist.

Español: Estos equipos deben ser instalados y atendidos exclusivamente por personal adecuadamente formado y capacitado en técnicas eléctricas y mecánicas.

Invisible Laser Radiation Warning

Lasers emit invisible radiation from the aperture opening when no fiber-optic cable is connected. When removing cables do not stare into the open apertures. In addition, install protective aperture covers to fiber with no cable connected.

Français: Des radiations invisibles à l'œil nu pouvant traverser l'ouverture du port lorsque aucun câble en fibre optique n'y est connecté, il est recommandé de ne pas regarder fixement l'intérieur de ces ouvertures. Installez les caches connecteurs prévus à cet effet.

Deutsch: Hinweise zur unsichtbaren Laserstrahlung
Die Laser strahlen an der Blendenöffnung unsichtbares Licht ab, wenn keine Glasfaserkabel angeschlossen sind. Blicken Sie nicht in die Öffnungen und installieren Sie unverzüglich die Abdeckungen über den Glasfaseranschlüssen.

Español: Debido a que la apertura del puerto puede emitir radiación invisible cuando no hay un cable de fibra conectado, procurar no mirar directamente a las aperturas para no exponerse a la radiación.

Power Disconnection Warning

Your switch is equipped with multiple power supplies. To reduce the risk of electrical shock, be sure to disconnect all power connections before servicing or moving the unit.

Français: Il se peut que cette unité soit équipée de plusieurs raccordements d'alimentation. Pour supprimer tout courant électrique de l'unité, tous les cordons d'alimentation doivent être débranchés.

Deutsch: Hinweise zur Spannungsfreischaltung
Ihr Gerät ist mit mehreren Netzteilen ausgerüstet. Um die Gefahr des elektrischen Schlages zu verringern, stellen sie sicher, daß alle Netzverbindungen getrennt sind bevor das Gerät gewartet oder bewegt wird.

Español: Antes de empezar a trabajar con un sistema, asegurese que el interruptor está cerrado y el cable eléctrico desconectado.

Proper Earthing Requirement Warning

To avoid shock hazard:

- The power cord must be connected to a properly wired and earth receptacle.

- Any equipment to which this product will attached must also be connected to properly wired receptacles.

- Use 22AWG solid copper conductor for ground leads connecting the frame to ground and DC return.

- Cleaning and dressing of grounding points during installation is strongly recommended. Also, do not forget the antioxidant.

- To ground the equipment properly, connect a Panduit Corporation UL listed Lug, P/N: LCD8-10A-L to the two threaded holes located on the rear using 8AWG copper conductors. Use Panduit Corporation, P/N: CT-940CH for crimping.

Français:

Pour éviter tout risque de choc électrique:

- Ne jamais rendre inopérant le conducteur de masse ni utiliser l'équipement sans un conducteur de masse adéquatement installé.

- En cas de doute sur la mise à la masse appropriée disponible, s'adresser à l'organisme responsable de la sécurité électrique ou à un électricien.

Deutsch: Hinweise zur geforderten Erdung des Gerätes

Aus Sicherheitsgründen:

- darf das Netzkabel nur an eine Schutzkontaktsteckdose angeschloossen werden.

- dürfen für den Anschluß anderer Geräte, welche mit diesem Gerät verbunden sind, auch nur Schutzkontaktsteckdosen verwendet werden.

Español:

Para evitar peligro de descargas:

- Para evitar peligro de descargas asegurese de que el cable de alimentación está conectado a una toma de alimentación adecuadamente cableada y con toma de tierra.

- Cualquier otro equipo a cual se conecte este producto también debe estar conectado a tomas de alimentación adecuadamente cableadas.

Read Important Safety Information Warning

This guide contains important safety information about which you should be aware when working with hardware components in this system. You should read this guide before installing, using, or servicing this equipment.

Français: Avant de brancher le système sur la source d'alimentation, consultez les directives d'installation disponibles dans ceci guide.

Deutsch: Bitte lesen - Sicherheitshinweise
Dieses guide enthält wichtige Sicherheitsinformationen, über die sie sich beim Arbeiten mit den Hardwareeinheiten bewußt sein sollten. Sie sollten diese Hinweise lesen, bevor sie installieren, reparieren oder die Anlage verwenden.

Español: Esto guide contiene información importante de seguridad sobre la cual usted debe estar enterado al trabajar con los componentes de dotación física en este sistema. Usted debe leer esta guía antes de instalar, usar o mantener este equipo.

Restricted Access Location Warning

This equipment should be installed in a location that restricts access. A restricted access location is one where access is secure and limited to service personnel who have a special key, or other means of security.

Français: Le matériel doit être installé dans un local avec accès limité ou seules les personnes habilitées peuvent entrer.

Deutsch: Hinweis zu Umgebungen mit beschränktem Zutritt
Die Anlage sollte an einem Standort mit beschränktem Zutritt installiert sein. Ein Standort mit beschränktem Zutritt stellt sicher, daß dort nur Servicepersonal mit Hilfe eines Schlüssels oder eines anderen Sicherheitssystems Zugang hat.

Español: Este equipo se debe instalar en un sitio con acceso restrinjido. Un sitio con el acceso restrinjido es uno seguro y con acceso limitado al personal de servicio que tiene una clave especial u otros medios de seguridad.

Wrist Strap Warning

Because electrostatic discharge (ESD) can damage switch components, you must ground yourself properly before continuing with the hardware installation. For this purpose, Alcatel-Lucent provides a grounding wrist strap and a grounding lug located near the top-right of the chassis. For the grounding wrist strap to be effective in eliminating ESD, the power supplies must be installed in the chassis and plugged into grounded AC outlets.

Français: L'électricité statique (ESD) peut endommager les composants du commutateur. Pour cette raison Alcatel-Lucent joint à l'envoi du châssis un bracelet antistatique à brancher sur la prise mise à la terre située en bas à droite du commutateur. Vous devrez mettre ce bracelet avant toute intervention hardware.

Deutsch: Hinweise zur ESD (Elektrostatischen Aufladung)
Weil elektrostatische Aufladung (ESD) Teile der Anlage beschädigen könnten, müssen sie sich selbst erden, bevor sie mit der Hardware Installation beginnen. Zu diesem Zweck stellt Alcatel-Lucent ein Erdungsarmband und eine Erdungsöse an der oberen rechten Seite des Chassis zur Verfügung. Um eine sichere Erdungsfunktion des Erdungsarmbandes sicherzustellen, müssen die Netzteile installiert und mit dem Schutzleiter des Versorgungsstromkreises verbunden sein.

Español: La descarga electrostática (ESD) puede dañar componentes eletrónicos. Usted debe asegurarse que está en contacto con tierra antes de hacer la instalación del equipo. Con este fin, Alcatel-Lucent proporciona una pulsera de muñeca para conectar al chasis en la toma de tierra situada en la parte superior derecha del chasis. Para que la correa de muñeca sea eficaz en la eliminación de ESD, las fuentes de alimentación deben estar instaladas en el chasis y conectadas a enchufes CA con tierra adecuada.

Instrucciones de seguridad en español

Advertencia sobre el levantamiento del chasis

Se requieren dos personas para levantar el chasis. Debido a su peso, la elevación del chasis sin ayuda puede causar daños corporales. También es seguro doblar sus rodillas y guardar su espalda derecho al ayudar a levantar el chasis.

Advertencia de las tapaderas en blanco

Porque regulan la circulación de aire y ayudan a proteger componentes internos del chasis, las tapaderas en blanco deben seguir instaladas en las ranuras vacías del módulo y la fuente de alimentación siempre.

Advertencia en caso de tormenta eléctrica

Para evitar peligro de descargas, no conecte o desconecte ningun cable, ni realice ninguna instalación, maintenimiento o reconfiguratión de este producto durante una tormenta eléctrica.

Advertencia de instalación

Solamente el personal bien informado en procedimientos eléctricos y mecánicos básicos debe instalar o mantener este equipo.

Advertencia de radiación láser invisible

Los lasers emiten radiación invisible de la apertura abierta cuando no se conecta ningún cable de fibra óptica. Al quitar los cables no mire fijamente en las aberturas abiertas. Además, instale las cubiertas protectoras de la abertura a las salidas de la fibra sin el cable conectado.

Advertencia de la batería de litio

Hay un peligro de la explosión si la batería del litio en su chasis se substituye incorrectamente. Substituya la batería solamente por el mismo o el equivalente de tipo de batería recomendado por el fabricante. Deseche las baterías usadas según las instrucciones del fabricante. Las instrucciones del fabricante son como sigue: Devuelva el módulo con la batería del litio a Alcatel-Lucent. La batería del litio será substitu- ida en la fábrica de Alcatel-Lucent.

Advertencia sobre la tensión de operación

Para reducir el riesgo del choque eléctrico, matenga sus manos y dedos fuera de la fuente de alimentación y no toque la placa madre mientras que el interruptor está funcionando.

Advertencia sobre la desconexión de la fuente

Su interruptor esta equipado por fuentes de alimentación múltiples. Para reducir el riesgo de choque eléc- trico, asegúrese desconectar todas las conexiones de alimentación antes de mantener o de mover la unidad.

Advertencia sobre una apropiada conexión a tierra

Para evitar peligro de descargas:

- El cable de alimentación debe estar conectado a una toma de alimentación adecuadamente cableada y con toma de tierra.

Cualquier equipo al cual se conecte este producto debe estar también conectado a tomas de alimentación adecuadamente cableadas.

Leer "información importante de seguridad"

La *Guía de "Comenzando a Usar"* que acompaña este equipo contiene información importante de seguridad sobre la cual usted debe saber al trabajar con los componentes de dotación física en este sistema. Usted debe leer esta guía antes de instalar, de usar, o de mantener este equipo.

Advertencia de acceso restringido

Este equipo se debe instalar en una ubicación que restrinja el acceso. Una ubicación con acceso restringido es una donde está seguro y limitado el acceso al personal de servicio que tiene un clave especial, u otros medios de la seguridad.

Advertencia de pulsera antiestática

Debido a que la descarga electrostática (ESD) puede dañar componentes del interruptor, usted debe conectarse a tierra correctamente antes de continuar con la instalación del equipo. Para este propósito, Alcatel-Lucent proporciona una pulsera antiestática y un terminal que pone a tierra situados cerca de la parte superior derecha del chasis. Para que la pulsera antiestática sea eficaz en la eliminación de ESD, las fuentes de alimentación se deben instalar en el chasis y enchufar en las salidas de CA con descarga a tierra.

Clase de seguridad

Cumple con 21CFR 1040.10 y 1040.11 ó sus equivalentes.