

OmniSwitch[®] 9000/9000E Series

Getting Started Guide

060210-10, Rev. E
August 2009

Alcatel-Lucent 

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

Lithium Batteries Caution. There is a danger of explosion if the Lithium battery in your chassis is incorrectly replaced. Replace the battery only with the same or equivalent type of battery recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. The manufacturer's instructions are as follows:

Return the module with the Lithium battery to Alcatel-Lucent. The Lithium battery will be replaced at Alcatel-Lucent's factory.

The features and specifications described in this guide are subject to change without notice.

Copyright © 2008 by Alcatel-Lucent. All rights reserved. This document may not be reproduced in whole or in part without the express written permission of Alcatel-Lucent.

Alcatel-Lucent® and the Alcatel-Lucent logo are registered trademarks of Alcatel-Lucent. Xylan®, OmniSwitch®, OmniStack®, and Alcatel-Lucent OmniVista® are registered trademarks of Alcatel-Lucent.

OmniAccess™, Omni Switch/Router™, PolicyView™, RouterView™, SwitchManager™, VoiceView™, WebView™, X-Cell™, X-Vision™, and the Xylan logo are trademarks of Alcatel-Lucent.

This OmniSwitch product contains components which may be covered by one or more of the following U.S. Patents:

- U.S. Patent No. 6,339,830
- U.S. Patent No. 6,070,243
- U.S. Patent No. 6,061,368
- U.S. Patent No. 5,394,402
- U.S. Patent No. 6,047,024
- U.S. Patent No. 6,314,106
- U.S. Patent No. 6,542,507

Alcatel-Lucent 

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

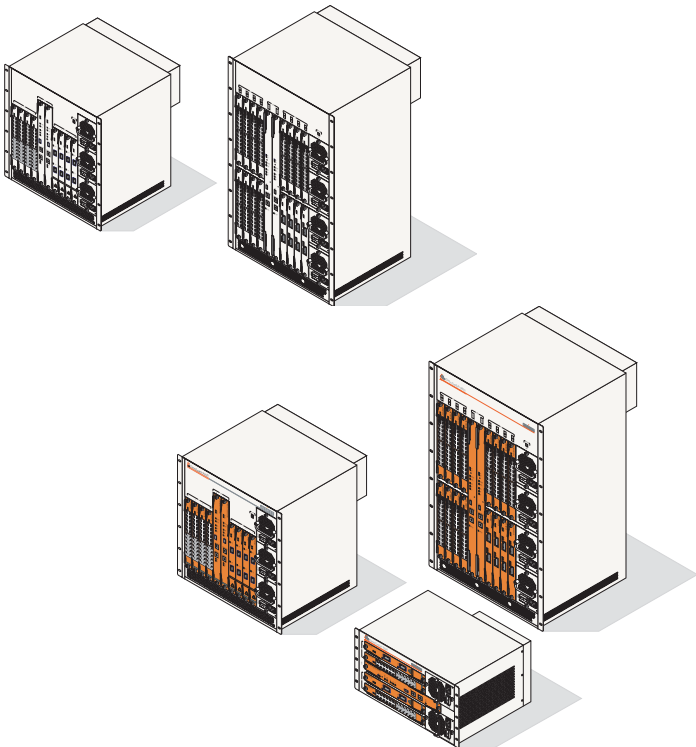
US Customer Support: (800) 995-2696
International Customer Support: (818) 880-3500
Internet: service.esd.alcatel-lucent.com

Table of Contents

OmniSwitch 9000 / 9000E Series . . .	1	Management Modules (CMMs)	12
Related Documentation	2	NI Modules	12
Installing the Hardware	3	CMMs	12
Items Required	3	Installing SFP and XFP Transceivers	15
Site Preparation	3	Blank Cover Plates	15
Environmental Requirements	3	Connections and Cabling	16
Electrical Requirements	3	Serial Connection to the Console Port	16
Chassis Weight Considerations	4	Serial Connection Default Settings	16
OS9800	4	Ethernet Management Port (EMP)	
OS9700/9702	4	Cable Requirements	17
OS9600	4	Booting the Switch	18
Items Included	4	Component LEDs	18
Unpacking and Installing the Switch	5	Your First Login Session	19
Unpacking the Chassis	5	Logging In to the Switch	19
Recommendations	5	Setting IP Address Information for the EMP	20
Instructions	5	Unlocking Session Types	21
Lifting the Chassis	7	Unlocking All Session Types	21
Mounting the Switch	7	Unlocking Specified Session Types	22
Airflow Considerations	7	Changing the Login Password	22
Rack-Mounting	8	Setting the System Time Zone	23
Optional Rack-Mounting Hardware	9	Setting the Date and Time	23
Standalone	9	Setting Optional System	
Installing Power Supplies	10	Information	24
Using the Grounding Wrist Strap and Chassis			
Grounding Lug	11		
Installing the Network Interface (NI) and Chassis			

Specifying an Administrative Contact	24	Troubleshooting	37
Specifying a System Name	24	The WebView login screen	
Specifying the Switch's Location	24	does not display.	37
Viewing Your Changes	25	The login screen displays, but my login	
Saving Your Changes	25	attempt fails.	37
Modifying the Serial Connection Settings	25		
Files and Directories	28		
Boot and Image Files	28		
boot.params File	28		
boot.cfg File	28		
Image Files	29		
Working and Certified Directories	30		
Working Directory	30		
Certified Directory	30		
Which directory is the switch currently using?	31		
Can I save changes to the Certified directory?	31		
What happens when the switch boots?	31		
Working and Certified Are Identical	31		
Working and Certified Are Different	32		
My Working and Certified Directories are			
different.Can I force a reboot from the Working direc-			
tory?	32		
Using WebView	33		
Browser Compatibility	33		
Logging In to WebView	33		
Navigating WebView	34		
Online Help	36		
Additional Information	36		

OmniSwitch 9000 / 9000E Series



OmniSwitch 9000/9000E Series Switches

The OmniSwitch 9000 and 9000E Series switches are designed to meet the needs of today's networks by supporting high availability, wire-speed performance and services that address the Enterprise Datacenter and Core as well as Campus networks. The OmniSwitch Series incorporates multiple chassis and module configurations designed to meet those needs.

The latest generation OmniSwitch chassis, modules, and CMMs provide all the functionality of the original OmniSwitch 9000 along with the addition of key features such as increased throughput, multi-VRF support with wire-rate performance, additional QoS & ACLs with more granular rate limiting and support of increased IPv4/IPv6 multicast flows, hosts, and routes.

Refer to the User Manual CD or Product Documentation Card for additional hardware and software OmniSwitch documentation.

Related Documentation

The following are the titles and descriptions of all the OmniSwitch 9000/9000E user documentation available:

- *OmniSwitch 9000/9000E Getting Started Guide*

Describes the basic steps for installing and mounting hardware and getting an OmniSwitch up and running. Also provides information on fundamental aspects of OmniSwitch hardware components and software architecture.

- *OmniSwitch 9000/9000E Hardware Users Guide*

Complete technical specifications and procedures for all OmniSwitch chassis, power supplies, fans, Chassis Management Modules (CMMs), and Network Interface (NI) modules.

- *OmniSwitch CLI Reference Guide*

Complete reference to all CLI commands supported on the OmniSwitch. 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, applications), security options (authenticated VLANs), Quality of Service (QoS), link aggregation, and server load balancing.

- *OmniSwitch AOS Release 6 Advanced Routing Configuration Guide*

Includes network configuration procedures and descriptive information on all the software features and protocols included in the advanced routing software package such as multicast routing (DVMRP and PIM-SM), OSPF and BGP.

- *OmniSwitch Transceivers Guide*

Includes information on Small Form Factor Pluggable (SFPs) and 10 Gbps Small Form Factor Pluggables (XFPs) transceivers.

Installing the Hardware

Items Required

- Grounding wrist strap (included)
- Phillips screwdriver
- Flat-blade screwdriver
- Serial cable

Site Preparation

Environmental Requirements

The OmniSwitch has the following environmental and airflow requirements:

- The installation site must maintain an appropriate temperature and humidity as specified in the Hardware Users Guide.
- Be sure to allow adequate room for proper air ventilation at the front, back, and sides of the switch. Refer to [“Mounting the Switch” on page 7](#) for minimum clearance requirements. No clearance is necessary at the top or bottom of the chassis.

Electrical Requirements

The OmniSwitch has the following general electrical requirements:

- Each switch requires one grounded electrical outlet for each power supply installed in the chassis. The OmniSwitch offers both AC and DC power supply support. Refer to the *Hardware Users Guide* for more information.
- For switches using AC power connections, each supplied AC power cord is 2 meters (approximately 6.5 feet) long. Do not use extension cords.

Redundant AC Power. It is recommended that each AC outlet resides on a separate circuit. With redundant AC, if a single circuit fails, the switch’s remaining power supplies (on separate circuits) are likely to remain unaffected and can, therefore, continue operating.

- For switches using DC power, refer to the *Hardware Users Guide* for more information, including installation guidelines.

Chassis Weight Considerations

OS9800

When fully populated (i.e., with all CMM and NI modules and power supplies installed), the OmniSwitch 9800 chassis weighs approximately 188 lbs (85 Kgs).

OS9700/9702

When fully populated (i.e., with all CMM and NI modules and power supplies installed), the OmniSwitch 9700/9702 chassis weighs approximately 128 lbs (58 Kgs).

OS9600

When fully populated (i.e., with CMM and all NI modules and power supplies installed), the OmniSwitch 9600 chassis weighs approximately 66 lbs (30 Kgs).

Items Included

Your OmniSwitch order includes the following items:

- OmniSwitch chassis with factory-installed power supplies per order
- CMM module(s) per order
- NI modules per order
- XFPs per order, if applicable
- SFPs per order, if applicable
- Blank cover panels, if applicable
- Grounding wrist strap
- RJ45-to-DB9 console adapter
- Power cord(s) per order, if applicable
- Hard copy of the *Getting Started Guide*
- Documentation CD containing a complete set of user guides for the switch and switch software. Refer to [“Related Documentation” on page 2](#) for a complete list of included documentation.
- Product Documentation Card with information on downloading the latest user guides.

Unpacking and Installing the Switch

Unpacking the Chassis

To protect your switch components from electrostatic discharge (ESD) and physical damage, read all unpacking recommendations and instructions carefully before beginning.

Recommendations

- Unpack your OmniSwitch chassis as close as possible to the location where it will be installed.
- Network Interface (NI) modules are packaged in separate boxes. In order to reduce significantly the exposure to electrostatic discharge (ESD) and physical damage, *do not* unpack these boxes until the NI modules are ready to be installed.

Instructions

- 1** Begin by carefully cutting the tape along the seam.
- 2** Lift the box's top flaps. Remove the smaller boxes that are enclosed and set them aside. These smaller boxes contain the Ship Kit and the switch's Chassis Management Modules (CMMs).
- 3** Next, completely remove the white plastic handle inserts from the sides of the box. Removing these handles allows the overpack to be removed.

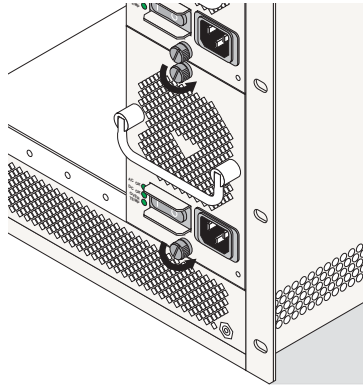
4 The overpack is the outer shell of the packaging. Lift the overpack straight up until it slides free from the rest of the packaging. This allows easy access to the chassis.

5 Carefully remove the protective plastic from the switch chassis.

6 In order to reduce the weight of the chassis, it is recommended that you remove all factory-installed power supplies prior to lifting it from the packaging. Steps 7 through 12 below provide instructions for removing power supplies.

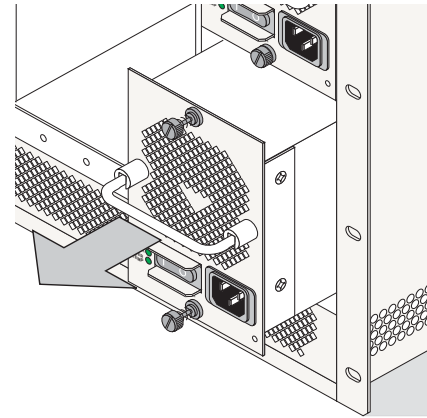
Note. Steps 7 through 12 apply to power supplies that are newly shipped in the switch chassis. They have no power cords attached and the on/off switches are in the off (O) position. For instructions on removing power supplies that are currently operating in an existing switch, refer to the *Hardware Users Guide*.

7 Loosen the two captive screws, located at the top and bottom of the power supply's front panel. If necessary, use a flat-blade screwdriver to loosen the screws. Be sure that both captive screws are completely disengaged from the threaded holes in the chassis before continuing.



Note. Alcatel-Lucent provides factory-installed blank cover plates for empty module slots. Do not remove these cover plates as they play an important role in chassis ventilation.

8 With one hand, grasp the handle at the front of the power supply and slowly pull the power supply out of the power supply bay. *Do not pull the power supply completely out of the bay with one hand.*



9 When the power supply is pulled out far enough (about 10”), place your other hand under the power supply casing to support its weight.

10 Continue pulling the power supply out until it is removed from the chassis.

11 Set the power supply aside on a clean, static-free surface. You will need to re-install it later.

12 Remove all remaining power supplies by repeating steps 7 through 11.

13 Continue to “Lifting the Chassis” below.

Lifting the Chassis

Once its weight has been reduced by removing the power supplies, the chassis can be lifted from the packaging material and moved to the location where it is to be installed (see important note below).

Important. Two people are required to lift the chassis. Due to its weight, lifting the chassis unassisted can cause personal injury.

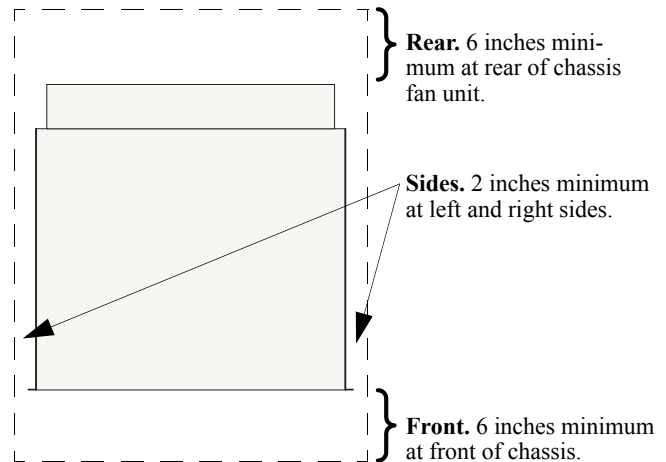
Once the chassis has been removed from the packaging, continue to “Mounting the Switch” below.

Mounting the Switch

Note. Due to their weight and airflow requirements, OmniSwitch chassis-based switches cannot be wall-mounted.

Airflow Considerations

Be sure that your switch is placed in a well-ventilated, static-free environment. Always allow adequate clearance at the front and sides of the switch, as well as behind the switch’s fan unit (located at the top-rear of the chassis). The following top-view diagram shows recommended minimum clearances for adequate airflow:



Chassis Top View

Never obstruct the air intake vents located at the bottom-front and bottom-sides of the chassis or the fan unit’s air output vents located at the rear of the chassis.

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

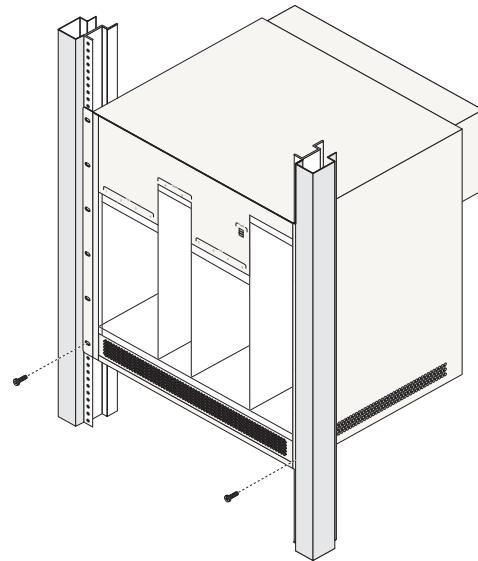
Rack-Mounting

Refer to the important guidelines below before installing the OmniSwitch chassis in a rack.

- Rack-mounting the chassis requires three people—two people to hold the chassis and position it in the rack and a third person to secure the chassis to the rack by using the attachment screws.
- The chassis has two integral rack-mount flanges that support standard 19” rack mount installations. Refer to [page 9](#) for information on optional rack-mounting hardware.
- 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.
- If you are installing the switch in a relay rack, be sure to install and secure the rack per the rack manufacturer’s specifications.
- Refer to [page 7](#) for important chassis airflow recommendations before installing.

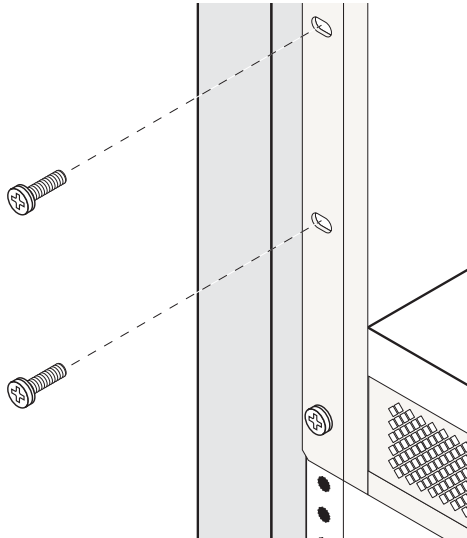
To rack-mount the switch, follow the steps below:

- 1** Mark the holes on the rack where the chassis is to be installed.
- 2** Using two people, 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 you marked in step 1.
- 4** Once the holes are aligned, use a third person to insert a screw through the *bottom hole on each flange*. Tighten both screws until they are secure.



Note. Be sure to install the screws in the *bottom hole* of each flange, as shown, before proceeding.

5 Once the screws at the bottom of each flange are secure, install the remaining screws. Be sure that all screws are securely tightened.



Optional Rack-Mounting Hardware

All OmniSwitches are shipped with integral front rack-mount flanges. These flanges support standard 19" rack mount installations. If you have non-standard rack-mount requirements, Alcatel-Lucent offers optional hardware for the following applications:

- 23" rack installations
- Side-mount hardware for additional support

For information on this optional rack mounting hardware, contact your Alcatel-Lucent representative.

Standalone

The OmniSwitch can be installed unmounted as a standalone unit. Be sure that the installation location is a stable, flat surface that can accommodate the *fully-populated* weight of all switches being installed. For detailed information on weight considerations, refer to [“Chassis Weight Considerations” on page 4](#).

Note. The OmniSwitch must be installed “right side up”. Never attempt to operate a switch while it is lying on its side.

To install the switch as a standalone unit, follow the steps below:

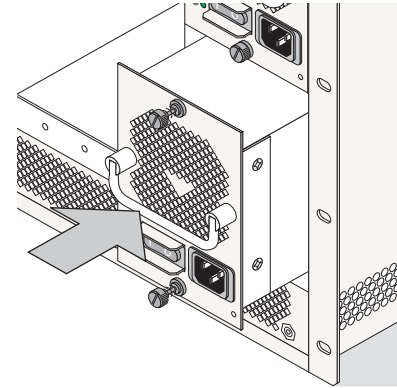
- 1 Use two or more people to move and position the unpopulated chassis upright on the floor or bench where it is to be installed.
- 2 Be sure that adequate clearance has been provided for chassis airflow and that you have placed the chassis within reach of all required electrical outlets. For recommended airflow allowances, refer to [page 7](#). For environmental and electrical requirements, refer to [page 3](#).

Installing Power Supplies

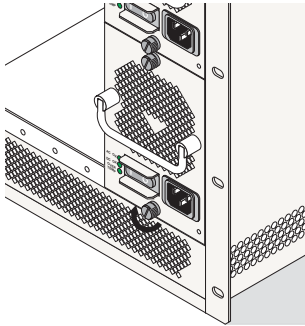
Next, re-install the power supplies in the chassis power supply bays by following the steps below:

- 1 First, be sure that you do not install the power supply upside down. While orienting the power supply, note that the on/off switch and power cord socket are located at the *bottom* of the power supply and the fan is located at the *top* of the power supply.
- 2 With one hand, grasp the handle at the front of the power supply. Place your other hand under the power supply casing to support its weight.

- 3 Carefully insert the rear of the casing into the power supply bay and slide the power supply back until its connector meets the chassis backplane connector.



- 4 Continue sliding the power supply back until the front panel meets the front of the chassis. *Do not force the power supply into the bay. Otherwise you can damage the connectors.*
- 5 Tighten the two captive screws located at the top and bottom of the power supply's front panel. *Be sure not to overtighten the captive screws. If you use a screwdriver, the torque used to tighten the screws must not exceed 2.3 foot-pounds.*



- 6** Verify that the power supply's on/off switch is in the off (O) position.
- 7** Loop the AC power cord (provided) once through the cable retainer located on the power supply's front panel and secure the retainer by using the butterfly fastener. By looping the power cord through this retainer, the cord cannot be accidentally pulled from the socket.
- 8** Once the power cord is looped through the retainer, plug the power cord connector into the power supply's socket and then plug the power cord into an easily-accessible, *properly grounded* outlet. *Do not use an extension cord.*

Note. For switches using DC power, the power cord connector snaps into the connector socket. A cable retainer is not used. For more information, refer to the *Hardware Users Guide*.

Important. *Do not* turn on the power supplies at this time.

- 9** Install all remaining power supplies by repeating steps 1 through 8 for each power supply.

Using the Grounding Wrist Strap and Chassis Grounding Lug

As electrostatic discharge (ESD) can damage switch components, such as the Network Interface (NI) and CMMs, 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 bottom-right of the chassis.

To ground yourself properly, follow the steps below:

- 1** Fasten the provided grounding strap to your wrist.
- 2** Insert the wrist strap's connector pin (located at the end of the strap's tether) into the grounding lug near the bottom-right of the chassis, as shown:

Installing the Network Interface (NI) and Chassis Management Modules (CMMs)

Once you are properly grounded, you may begin installing the Network Interface (NI) and CMM(s).

Note. OmniSwitch 9000E Series CMMs and NIs are colored with a purple line to distinguish them from OmniSwitch 9000 Series CMMs and NIs that are colored orange. Do not install OmniSwitch 9000E Series and OmniSwitch 9000 Series CMMs and NIs in the same chassis.

NI Modules

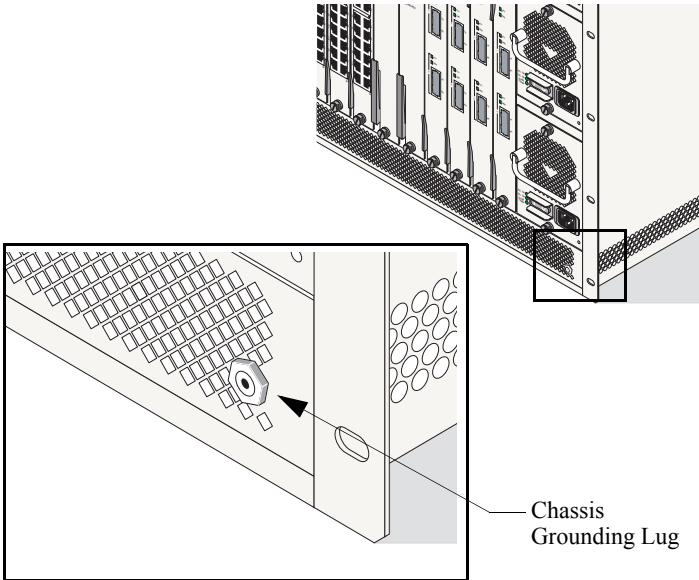
NI modules may be installed in any slot position except for the CMM slots.

CMMs

An OmniSwitch requires a minimum of one CMM for switch operations. The second CMM provides redundancy and may be installed either in slot A or slot B.

In non-redundant configurations, the CMM may be installed in either slots A or B. In redundant configurations, the CMM installed in slot A will be designated *primary* by default. For detailed information, refer to the *Hardware Users Guide*.

NI modules cannot be installed in CMM slots A or B; likewise, CMMs cannot be installed in any NI slot position.



Note: The grounding lug diagram on the left is a general diagram only. It is intended to show the location of the grounding lug. No NI modules or CMMs should be installed in your chassis at this time.

Important. For the grounding wrist strap to be effective in eliminating ESD, the power supplies must be installed in the chassis and plugged into grounded electrical outlets as described on [page 11](#).

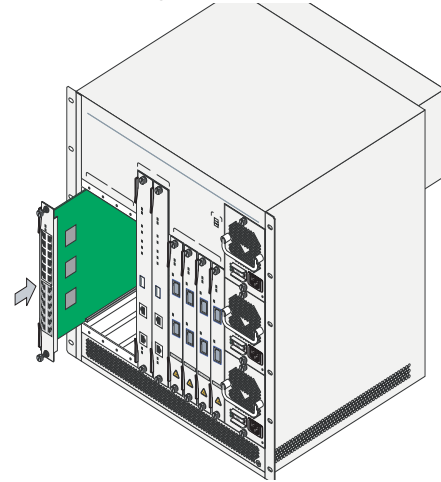
More Information on Slot Numbering. For a diagram showing the chassis layout and slot positions, refer to *Hardware Users Guide*.

To install an NI or CMM module, follow the steps below:

Note. To further reduce exposure to electrostatic discharge (ESD) and physical damage, do not remove more than one module at a time from the factory packaging. Unpack one module, immediately install the module in the chassis, then repeat the sequence for another module.

Important. Before beginning, note that the CMM modules and NI modules slide into the chassis card guides differently. CMMs have a sheet metal tray that slides into the guides; with NIs, the edges of the module's printed circuit slide into the guides.

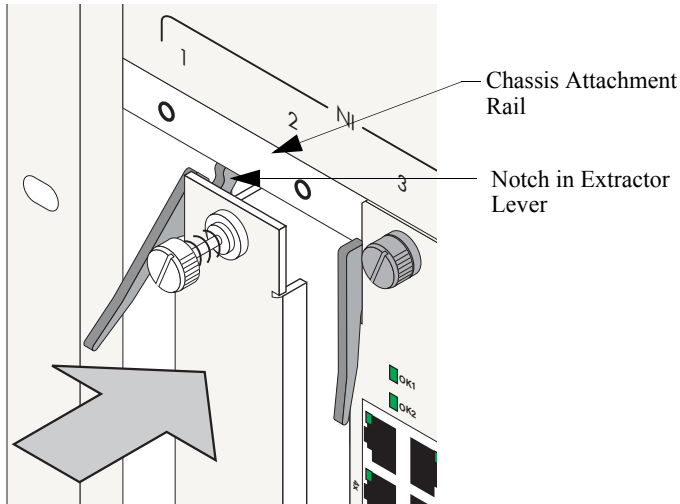
1 Holding the module in both hands, slide it carefully into the chassis card guide. The component side of the board should face right.



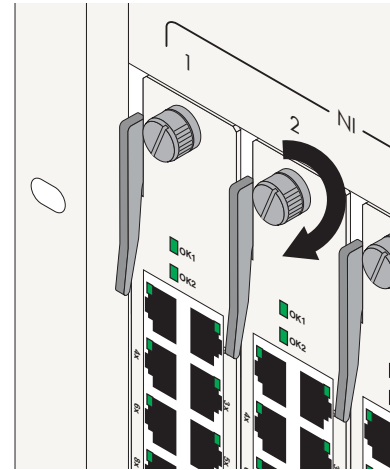
2 The module should slide in easily. Do not force the module into the slot. If any resistance is encountered, ensure that the module is aligned properly in the card guide. Also, see the important note regarding chassis card guides on [page 13](#).

3 When the module is nearly seated in the slot, be sure that the two extractor levers—one on top of the module and one at the bottom—are slightly opened (approximately 30°). This allows the notch on each extractor lever to grasp the rail on the chassis. Once the notches

have grasped the rail, press both extractor levers simultaneously until the module is firmly seated.



4 Once the module is firmly seated, secure the module to the chassis by tightening the two captive screws. *Be sure not to overtighten the captive screws. If you use a screwdriver, the torque used to tighten the screws must not exceed 2.3 foot-pounds.*



5 Install all remaining modules by repeating steps 1 through 4 for each module.

Installing SFP and XFP Transceivers

For information on installing XFPs and SFPs, refer to the *OmniSwitch Transceivers Guide*.

Blank Cover Plates

Blank cover plates are factory-installed in the chassis and are used to cover empty CMM and NI slots as well as empty power supply bays.

These cover plates play an important role in chassis airflow and temperature management. They also provide protection for module processor boards and other sensitive internal switch components by closing off a chassis that is not fully populated.

Because they regulate airflow and help protect internal chassis components, blank cover plates should remain installed at empty module slots and power supply bays at all times.

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:

- Serial cable to the console port
- Ethernet cable to the Ethernet Management Port (EMP) on the CMM
- Gigabit cables to all required XFPs or MiniGBICs
- Ethernet cables to all required Ethernet Network Interface (ENI) ports

Serial Connection to the Console Port

The console port, located on the CMM module, provides a serial connection to the switch and is required when logging into the switch for the first time. By default, this RJ-45 connector provides a DCE 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

For information on modifying these settings, refer to [“Modifying the Serial Connection Settings”](#) on page 25.

Ethernet Management Port (EMP) Cable Requirements

There are specific cable type requirements (i.e., straight-through or crossover) based on the location of the Ethernet Management Port (EMP) and the type of device to which it is connecting. Refer to the information below:

EMP to a Switch	Straight-through
EMP to a Computer or Workstation	Crossover

Note. For information on manually configuring Ethernet ports for cabling requirements, refer to “Configuring Ethernet Ports” in the *Network Configuration Guide*.

For detailed information on all port types, including console, EMP, Gigabit Ethernet, and 10 Gigabit Ethernet, refer to the *Hardware Users Guide*.

Booting the Switch

Now that you have installed the switch components and connected all required cables, you can boot the switch. To boot the switch, simply turn the on/off switch for all installed power supplies to the on (I) position.

Note. If you have more than one power supply installed, be sure to turn on each power supply in rapid succession, (i.e., within a few seconds of each other). This ensures that there will be adequate power for all NI modules when they boot.

Component LEDs

The boot process takes a few moments to complete. During this process, the LEDs on the CMM and NI modules may flash and change color, indicating different stages of the boot.

Following a successful boot, the LEDs on all switch components, including power supplies, should display as follows:

CMM OK1	Solid Green
CMM OK2	Blinking Green
CMM CONTROL	Solid Green
CMM FABRIC	Solid Green
CMM FAN	Solid Green

CMM TEMP	Green
CMM PSU	Green
NI OK1	Solid Green
NI OK2	Blinking Green
Power Supply AC OK	Solid Green
Power Supply DC OK	Solid Green
Power Supply OVER TEMP	Off

If the LEDs do not display as indicated, make sure the boot process is completed. Again, the boot process takes several moments to complete. If the LEDs do not display as indicated following a complete boot sequence, contact Alcatel-Lucent Customer Support.

For information on power supply LED states, refer to the *Hardware Users Guide*.

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 19](#).

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
- Set IP address information for the Ethernet Management Port (EMP)
- 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 (i.e., *user*) name and password. During this first login session, only one user name option and one password option is available:

- Login (i.e., user name)—**admin**
- Password—**switch**

To log in to the switch, enter **admin** at the login prompt:

```
login: admin
```

Next, enter the factory default password, **switch**, at the password prompt:

```
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 9000E
Software Version 6.4.1.281.R01 Development, March 16,
2009.
```

```
Copyright (c), 1994-2007 Alcatel-Lucent All Rights
reserved.
```

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

```
->
```

More Information On User Accounts. 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 and user privileges, refer to the *Switch Management Guide*.

Setting IP Address Information for the EMP

The Ethernet Management Port (EMP) is located on the CMM module. The EMP allows you to bypass the Network Interface (NI) modules and manage the switch over the network directly through the CMM.

In order to ping the switch through the EMP Ethernet connection, you must change the port's default IP and gateway addresses.

To change the default IP and gateway addresses, refer to the following steps:

Note. You must be connected to the switch via the console port before attempting to change IP address information. Otherwise, an error message will display.

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

```
Boot >
```

2 At the boot prompt, enter **boot empipaddr**, followed by the new default IP address for the EMP. For example:

```
Boot > boot empipaddr 168.22.2.120
```

3 Next, enter **boot empgatewayipaddr**, followed by the new default gateway address for the EMP. For example:

```
Boot> boot empgatewayipaddr 168.22.2.254
```

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

```
Boot > show
Edit buffer contents:
EMP IP Address           : 168.22.2.120
EMP Gateway IP Address   : 168.22.2.254
```

(additional table output not shown)

Subnet Mask. The default subnet mask is Class C (255.255.255.0). If you must change this default value, use the **boot empnetmask** command at the boot prompt.

Access to the EMP. By default, only devices in the same subnet as the EMP will be able to manage the switch through that port. For information on allowing devices in other subnets to manage the switch via the EMP, refer to the *Hardware Users Guide*.

5 Save these changes to the switch's running memory by entering **commit system** at the boot prompt:

```
Boot > commit system
```

This will immediately enable your changes and allow users to ping the EMP. However, note that these changes have not yet been saved to the switch's **boot.params** file and will be lost if the switch is rebooted.

6 To permanently save these changes to the **boot.params** file, enter **commit file** at the boot prompt:

```
Boot > commit file
```

Changes will be preserved following a switch reboot.

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

Important. Although you have configured the EMP with valid IP address information, you will not be able to access the switch through this port for Telnet, FTP, WebView, or SNMP sessions until you have unlocked these remote session types. See “[Unlocking Session Types](#)” for more information.

Unlocking Session Types

Security is a key feature on the OmniSwitch. As a result, 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
```

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 19).
- 2** Enter the keyword **password** and press **Enter**.
- 3** Enter your new password at the prompt (refer to the note below).

Note. Typically, the password should be a string of non-repeating characters. The CLI uses the first occurrence of the character series to uniquely identify the password. For example, the password *engrengr* is the same as *enr*. A better password might be *enr2735*.

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

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

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.

Setting the System Time Zone

The switch's default time zone is UTC (also referred to as Greenwich Mean Time).

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 example, to set the system clock to run on Pacific standard time, enter the following command:

```
-> system timezone pst
```

To enable Daylight Savings time, enter the following command:

```
-> system daylight savings time enable
```

Many other time zone variables are supported. For detailed information on configuring a time zone for the switch, refer to your *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*. For example:

```
-> system time 18:35:00
```

The switch uses a 24-hour clock; the time value shown in the above example would set the time to 6:35 PM.

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

```
-> system date 06/27/2009
```

Setting Optional System Information

This section provides information on configuring optional system parameters, including:

- the switch's administrative contact
- a system name
- the switch's physical location

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, enter **system contact**, followed by a text string. If you include spaces between words in the text string, be sure to enclose the string in quotes (“ ”).

For example:

```
-> system contact "JSmith X477 js@company.com"
```

Specifying a System Name

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

To specify a system name, enter **system name**, followed by a text string. If you include spaces between words in the text string, be sure to enclose the string in quotes (“ ”).

For example:

```
-> system name "Engineering Switch 3"
```

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, enter **system location**, followed by a text string. If you include spaces between words in the text string, be sure to enclose the string in quotes (“ ”).

For example:

```
-> system location "NMS Lab--NE Corner Rack"
```

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.

When the **write memory** command is entered, changes are automatically saved to the main configuration file (**boot.cfg**) and placed in the **/flash/working** directory. For more information on the **boot.cfg** file, refer to [page 28](#).

Note. If the switch reboots following a **write memory** command entry, the switch will run from the **/flash/certified** directory. As a result, subsequent configuration changes cannot be saved using the **write memory** command until the switch is once again running from the **/flash/working** directory. See [page 30](#) for important information on these directories.

Modifying the Serial Connection Settings

The switch's serial connection defaults are listed on [page 16](#). 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 be displayed.

1 Enter **modify boot parameters** 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 while 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.

This completes the initial setup process. Your OmniSwitch is now ready for additional configuration and network operation. Refer to the following sections for more information on using your switch, as well as additional built-in features.

For more information on using the CLI, refer to “Using the CLI” in the *OmniSwitch AOS Release 6 Switch Management Guide*.

Files and Directories

Boot and Image Files

Although the switch's flash memory can contain many file types (e.g., log and snapshot files), there are three specific file types that provide key switch and network functions. These files include the **boot.cfg** file, the **boot.params** file, and image (.img) files.

boot.params File

The **boot.params** file provides IP address, gateway, and mask information for the switch's Ethernet Management Port (EMP). This information is required for direct Ethernet connections to the switch's primary CMM.

This file also contains default console port parameters (baud rate, etc.) and can be modified via the **modify boot parameters** CLI command.

To be read by the switch, the **boot.params** file must be placed in the **/flash** directory. If the file is deleted for any reason, a new **boot.params** file will be generated automatically on the next system boot. However, all user-configured information, such as IP address, gateway, and mask information, will be lost. Therefore, it is recommended that you keep a backup copy of this file at all times.

boot.cfg File

The **boot.cfg** file stores your network configuration parameters. When you first boot the switch, the **boot.cfg** file is not present. This file is automatically generated when you first issue a **write memory** command to save your configuration changes. The file is then automatically placed in the **/flash/working** directory.

Important. Your switch must be running from the **/flash/working** directory in order to save changes to the **boot.cfg** file. Refer to [“Working and Certified Directories” on page 30](#) for more information.

Once the configuration parameters stored in the **boot.cfg** file are considered tested and reliable, the file can be copied to the **certified** directory and become part of the “last known good” software for the switch.

If all copies of this file are deleted and a system boot occurs, your network configuration will be lost. Therefore, it is recommended that you keep a backup copy of this file at all times.

Image Files

Image files (those files with **.img** extensions) contain executable code that provides support for the system, NI modules, and network functions. In other words, they serve as essential drivers for switch and network operations.

Although these files may be backed up to the root flash directory or any user-defined subdirectory, they must be present in the **/flash/working** and **/flash/certified** directories for the switch to operate and pass traffic.

If you delete all copies of an image file, you will be required to contact Alcatel-Lucent Customer Support for replacements. Therefore, it is recommended that you keep backup copies on your computer's hard drive or a locally-accessible server.

For a complete list of image files along with their functions, refer to the *Switch Management Guide*. See below for a list of the more common image files.

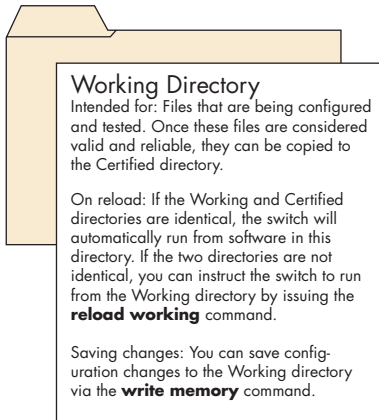
Jos.img	Contains the operating system software.
Jbase.img	Contains base code for the switch.
Jeni.img	Provides Ethernet support.
Jdiag.img	Provides enhanced hardware diagnostics for the switch.
Jadvrout.img	Alcatel-Lucent's Advanced Routing software package.
Jrelease.img	Contains release information for image downloads.
Jdni.img	Provides enhanced hardware diagnostics for the installed modules.
Jsecu.img	Alcatel-Lucent's security software package.

Working and Certified Directories

Switches are shipped with flash memory. This memory is used to store files, including boot and image files that are used for switch operations.

The **/flash** directory contains two subdirectories: **/working** and **/certified**. These directories work together to provide the *image rollback* resiliency feature. Image rollback allows the switch to return to a prior “last known good” version of software in the event of a system software problem.

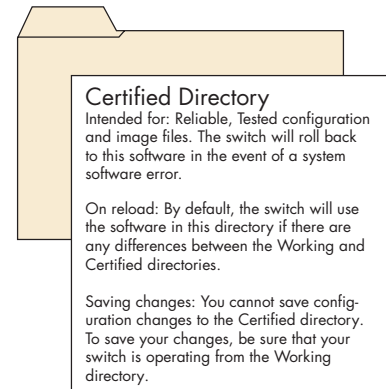
Working Directory



The **/flash/working** directory is intended for software that is still being configured for your network. Changes made while configuring your switch are saved to the **boot.cfg** file in the **/flash/working** directory.

Once the **/flash/working** directory’s configuration and image files are road-tested and considered valid and reliable for your network, they can be copied to the **/flash/certified** directory.

Certified Directory



The software in the **/flash/certified** directory should be treated as the “gold master” for the switch. When you place configuration and image files in this directory, you are “certifying” them as tested and reliable. If the switch is running from the **/flash/working** directory and experiences a software problem, it will “roll back” to the last known good software in the **/flash/certified** directory on the next reboot.

Which directory is the switch currently using?

When you first boot the switch, the **/flash/working** directory is used; this allows you to save your initial configuration changes to the **boot.cfg** file. However, subsequent boots may result in your switch running from the **/flash/certified** directory. Therefore, verifying the current running directory is a key step any time you are configuring or monitoring the switch.

View the current directory by entering the **show running-directory** command. For example:

```
-> show running-directory

CONFIGURATION STATUS
  Running CMM                : PRIMARY,
  CMM Mode                   : DUAL CMMs,
  Current CMM Slot           : A,
  Running configuration      : WORKING,
  Certify/Restore Status     : CERTIFY NEEDED
SYNCHRONIZATION STATUS
  Flash Between CMMs        : NOT SYNCHRONIZED,
  Running Configuration     : SYNCHRONIZED,
  NIs Reload On Takeover    : ALL NIs
```

In this example, the switch is using the **/flash/working** directory.

Can I save changes to the Certified directory?

No. The **/flash/certified** directory is intended to store only tested, reliable configuration and image files. Configuration changes must be saved to the **boot.cfg** file in the **/flash/working** directory. Once those changes have been road-tested, the contents of the **/flash/working** directory can be

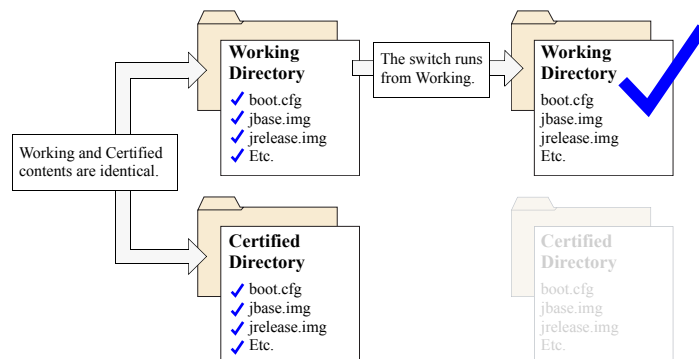
copied to the **/flash/certified** directory via the **copy working certified** command.

What happens when the switch boots?

During the boot process, the switch compares the contents of the **/flash/working** and **/flash/certified** directories. Based on this comparison, the switch determines which directory to use as its running software.

Working and Certified Are Identical

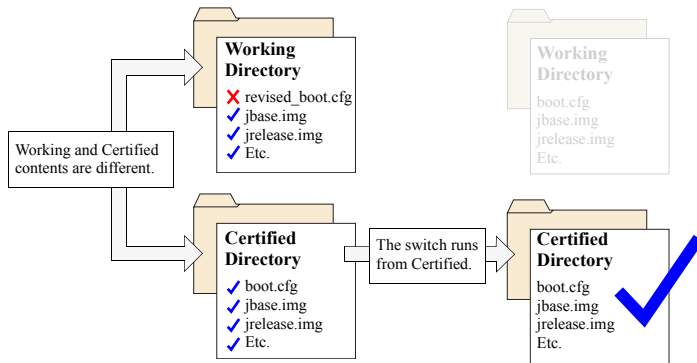
If the software in the **/flash/working** and **/flash/certified** directories is identical, the switch considers the software in both directories to be equally reliable. In this case, the switch will run from the **/flash/working** directory.



When the switch is running from the **/flash/working** directory software, configuration changes can be saved via the **write memory** command.

Working and Certified Are Different

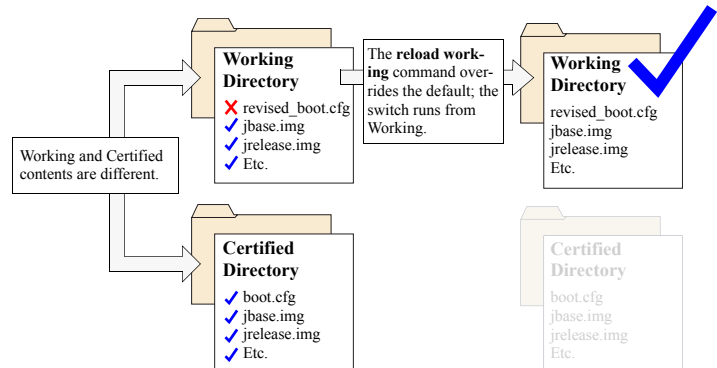
If the software in the `/flash/working` directory differs *even slightly* from the software in the `/flash/certified` directory, the switch will automatically run from the `/flash/certified` directory.



When the switch runs from the `/flash/certified` directory, configuration changes *cannot* be saved via the **write memory** command.

My Working and Certified Directories are different. Can I force a reboot from the Working directory?

Yes. If its configuration and image files are known to be reliable, you can override the default and initiate a reboot from the `/flash/working` directory. This is done via the **reload working** command. For more information, refer to your *CLI Reference Guide*.



Note. For detailed information on using directories, refer to the *Switch Management Guide*.

Using WebView

OmniSwitches can be configured and monitored using WebView, Alcatel-Lucent's Web-based device management tool. WebView software is pre-installed in the switch; you are not required to load additional software.

Note. Although WebView software is pre-installed, you must first enable HTTP sessions for your switch before you can log in. Refer to [“Unlocking Session Types” on page 21](#) for more information.

Browser Compatibility

WebView is supported on the following Web browsers:

- Internet Explorer 6.0 or greater for Windows 2000, Windows NT, Windows XP and Windows Vista
- Firefox 2.0 for Windows and Sun Solaris.

Logging In to WebView

Note. Before attempting to establish a WebView session, be sure that you have first unlocked the HTTP session type via the **aaa authentication** command. Otherwise, a login error will occur. See [“Unlocking Session Types” on page 21](#) for more information.

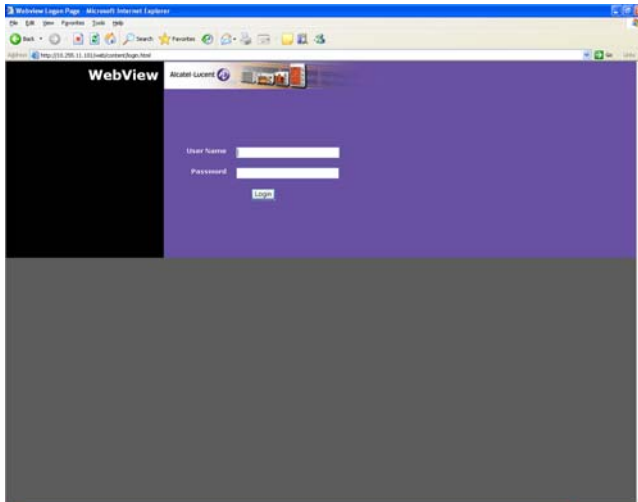
To access WebView and log in to a switch:

- 1** Ensure web-management is globally enabled on the switch by issuing the following:

```
-> http server
```

- 2** Open any Alcatel-Lucent supported Web browser.

- 3 Enter the switch's IP address in the browser's URL field. The login screen displays.

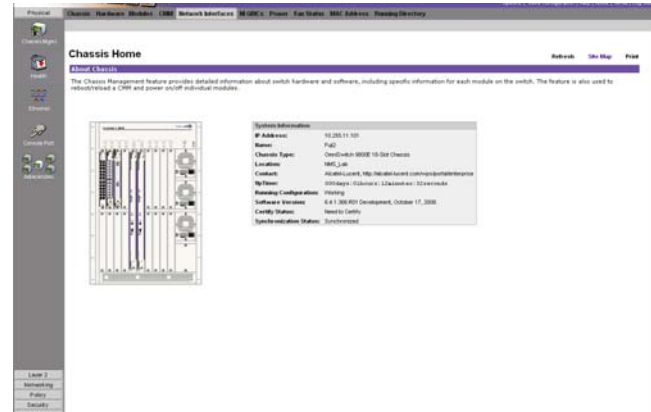


- 4 Enter the user name and password at the login prompt.

If you have already changed the user name and password for your switch, be sure to use the new information. If you have not changed your user name or password, the factory defaults are **admin** and **switch**, respectively. Refer to the *Switch Management Guide* for information on modifying the default user name and password.

Navigating WebView

After you have successfully logged in, the Chassis Management home page displays.



The Chassis Management home page provides a physical representation of the switch as well as basic system information. This is the main launching point for WebView.

Navigate the application by clicking the “Configuration Group” buttons on the left-hand toolbar.

Main “Configuration Group” Toolbar.

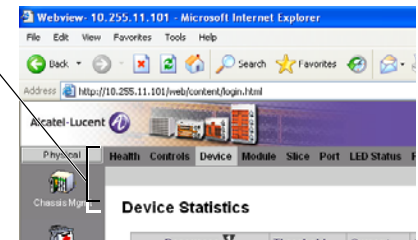
(In this case, the group “Health” has been selected.)



Refine your navigation by selecting “Configuration Options” for each group from the items displayed in the grey, horizontal navigation bar.

“Configuration Options” Toolbar.

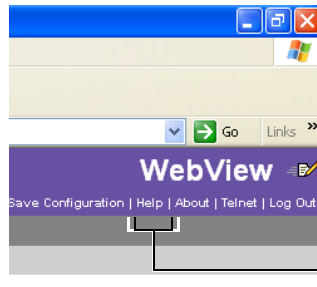
(In this case, the option “Device” has been selected.)



Site Maps. WebView also provides site maps for each configuration group. Site maps allow you to view complete page contents under each feature. By providing quick, easy access to specific pages, site maps can reduce time spent searching through the WebView application. To access site maps, click the “Site Map” link included on each configuration group Home page (e.g., Health).

Online Help

General online help is available through the main Help link located at the top of the WebView banner.

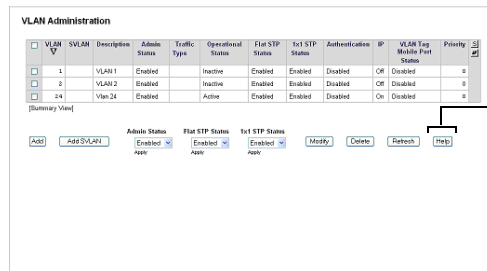


General Help Link

Additional Information

For more information on using WebView, refer to “Using WebView” in the *Switch Management Guide*.

Detailed, context-based help is provided for each status table and configuration dialog window.



Context-specific Help button.

(In this case, for the VLAN Administration table.)

Troubleshooting

The WebView login screen does not display.

This suggests either a physical or network connection issue. Try the following options:

- Be sure that you have a good physical Ethernet cable connection to the Ethernet port used for managing the switch (EMP or NI port).
- Be sure your computer has a valid Ethernet connection and IP address. See [page 20](#) for information on configuring the IP address for the EMP.

The login screen displays, but my login attempt fails.

This suggests either a user name and password or Authenticated Switch Access error. Try the following options:

- Check that you are using the correct user name and password. If you have already changed the user name and password for your switch, be sure to use the new information. If you have not changed the user name and password, the factory defaults are **admin** and **switch**, respectively.
- Be sure that you have “unlocked” HTTP sessions on the switch. To unlock HTTP sessions, enter the following command:

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

Note: See [page 21](#) for information on unlocking session types.
