OmniSwitch® 9000 Series

Getting Started Guide

ALCATEL

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. The Lithium battery will be replaced at Alcatel's factory.**

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

Table of Contents

OmniSwitch 9000 Series

Features

Alcatel's OmniSwitch 9000 Series switches offer high performance Gigabit Ethernet and 10-Gigabit Ethernet capabilities, as well as open standards for enterprise requirements.

Refer to "Chassis Types" on page 2 for additional details on OS9800, OS9700 and OS9600 switches.

Full duplex is supported on Gigabit Ethernet and 10-Gigabit Ethernet ports.

Availability Features

Availability ensures that your switch is consistently operational for your day-to-day networking needs. This added reliability is provided through redundant components for critical hardware and software subsystems. OmniSwitch 9000 Series switches provide a broad variety of Availability features, including:

- Hardware-based resiliency for CMMs, PSUs, and fans
- Distributed architecture with Smart Continuous Switching allows NIs forward even during CMM takeover
- Hot-swappable hardware for CMMs, NIs, transceivers, fans, and PSUs
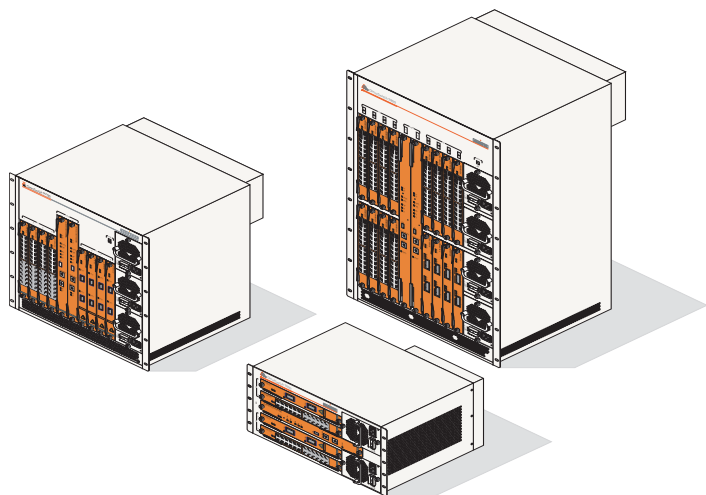
- Spanning Tree, VRRP, and other routing protocols with Graceful Restart provide software-based redundancy
- Flash with dual images (working & certified) enables rollback capability during image and configuration updates

For more information on Availability features, refer to the *OmniSwitch 9000 Series Hardware Users Guide*, *OmniSwitch 6800/6850/9000 Switch Management Guide*, and *OmniSwitch 6800/6850/9000 Network Configuration Guide.*

Chassis Types

OmniSwitch 9800

The OmniSwitch 9800 is a 16-slot large enterprise core switch. The OmniSwitch 9800 offers up to 384 Gigabit Ethernet ports and can also be equipped with up to 96 10-Gigabit Ethernet ports.

The OmniSwitch 9800 chassis contains the following major components:

- Sixteen Network Interface (NI) module slots
- Two Chassis Management Module (CMM) slots
- Power supply bay holding up to four power supplies
- Fan tray with three fans
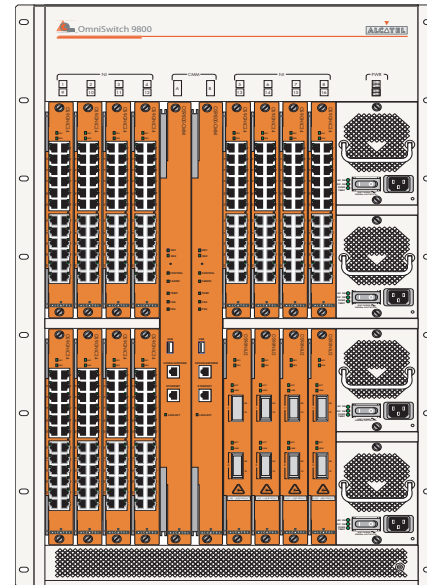
OmniSwitch 9700

The OmniSwitch 9700 is a 10-slot large enterprise core switch. The OmniSwitch 9700 offers up to 192 Gigabit Ethernet ports and can also be equipped with up to 48 10-Gigabit Ethernet ports.

The OmniSwitch 9700 chassis contains the following major components:

- Eight Network Interface (NI) module slots
- Two Chassis Management Module (CMM) slots
- Power supply bay holding up to three power supplies
- Fan tray with three fans
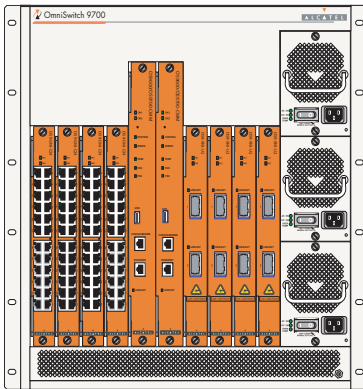
OmniSwitch 9600

The OmniSwitch 9600 is a 5-slot large enterprise core switch. The OmniSwitch 9600 offers up to 96 Gigabit Ethernet ports and can also be equipped with up to 24 10-Gigabit Ethernet ports.

The OmniSwitch 9600 chassis contains the following major components:

- Four Network Interface (NI) module slots
- One Chassis Management Module (CMM) slots
- Power supply bay holding up to two power supplies
- Fan tray with four fans
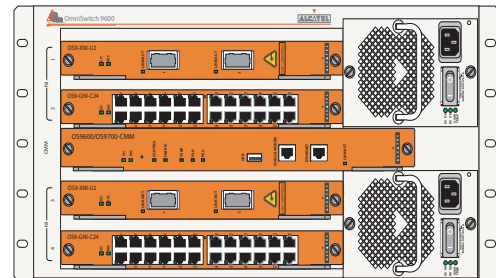
Installing the Hardware

Items Required

- Grounding wrist strap (included)

- Phillips screwdriver

- Flat-blade screwdriver

- Serial cable

Site Preparation

Environmental Requirements

OmniSwitch 9000 Series 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 "Mounting the Switch" on page 7 for minimum clearance requirements. No clearance is necessary at the top or bottom of the chassis.

Electrical Requirements

OmniSwitch 9000 Series switches have the following general electrical requirements:

- Each switch requires one grounded electrical outlet for each power supply installed in the chassis (up to four for OS9800 switches; up to three for OS9700 switches; up to two for OS9600 switches). OmniSwitch 9000 Series switches offer both AC and DC power supply support. Refer to the *OmniSwitch 9000 Series 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 *OmniSwitch 9000 Series Hardware Users Guide* for more information, including installation guidelines.

Weight Considerations

OS9800

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

OS9700

When fully populated (i.e., with all CMM and NI modules and power supplies installed), the OmniSwitch 9700 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 weighs approximately 66 lbs (30 Kgs).

Items Included

Your OmniSwitch 9800/9700/9600 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

- MiniGBICs 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 *OmniSwitch 9000 Series Getting Started Guide*

- Documentation CD containing a complete set of user guides for the switch and switch software. Refer to "User Documentation on CD" on page 61 for a complete list of included documentation.

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 marked "OPEN HERE FIRST".

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 *OmniSwitch 9000 Series 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.
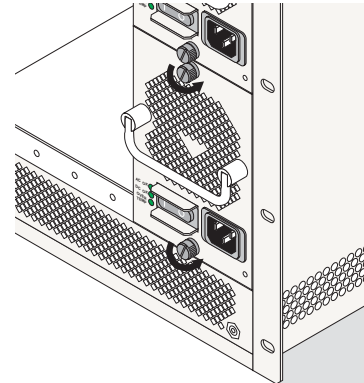
Note. Alcatel provides factory-installed blank cover plates for empty module slots. Do not remove these cover plates as they play an important role in chassis ventilation.

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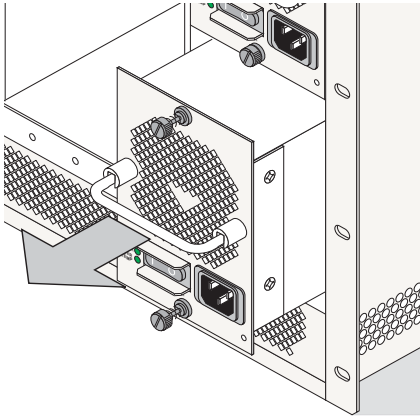
9 When the power supply is pulled out far enough (about 10"), place your other hand under the power supply casing to support its weight.

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 9000 Series 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:

Rear. 6 inches minimum at rear of chassis fan unit.

Sides. 2 inches minimum at left and right sides.

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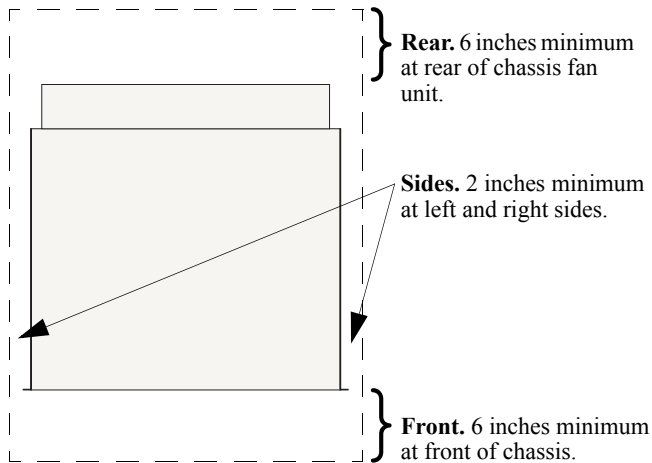
Chassis Top View

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 for information on optional rack-mounting hardware.

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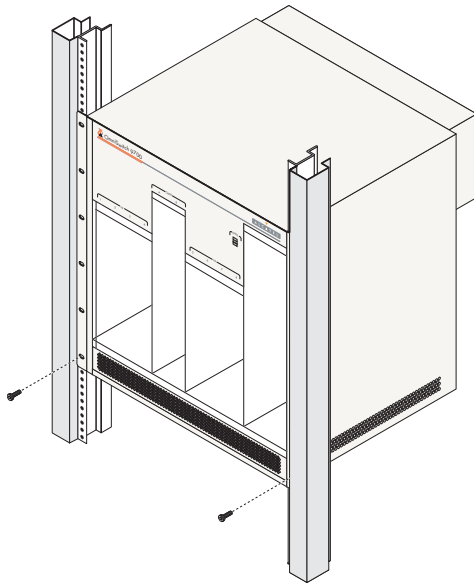
Note. Be sure to install the screws in the *bottom hole* of each flange, as shown, before proceeding.

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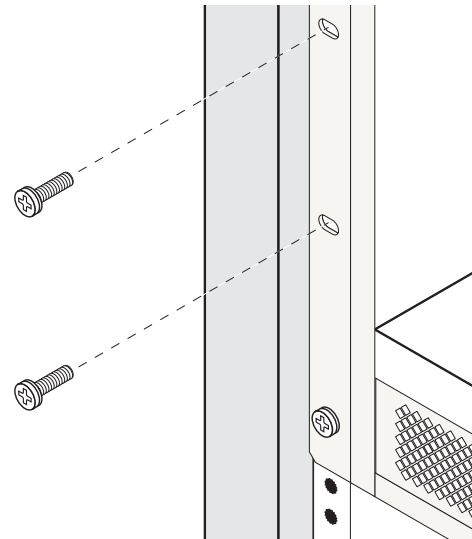
Optional Rack-Mounting Hardware

All OmniSwitch 9000 Series switches 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 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 representative.

Standalone

The OmniSwitch 9000 Series switches 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. A fully-populated OmniSwitch 9800 weighs approximately 188 lbs (85 Kgs); a fully-populated OmniSwitch 9700 weighs approximately 128 lbs (58 Kgs) and a fully-populated OmniSwitch 9600 weights approximately 66 lbs (30 Kgs).

Note. OmniSwitch 9000 Series switches 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 . For environmental and electrical requirements, refer to .

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.
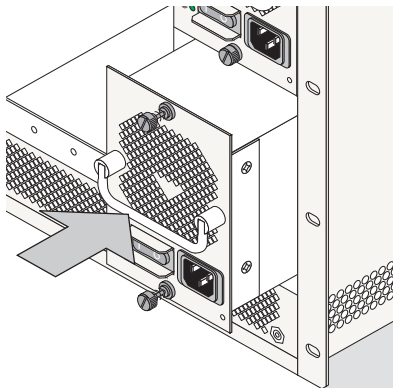
4 Continue sliding the power supply back until the front panel meets the front of the chassis. *Do not force the*

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.*
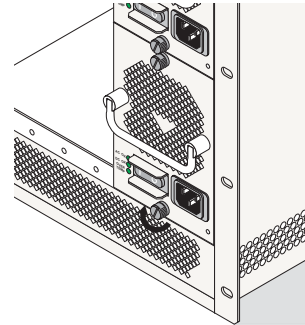
6 Verify that the power supply's on/off switch is in the off (O) position.

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 OS9000 series 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 *OmniSwitch 9000 Series 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 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.

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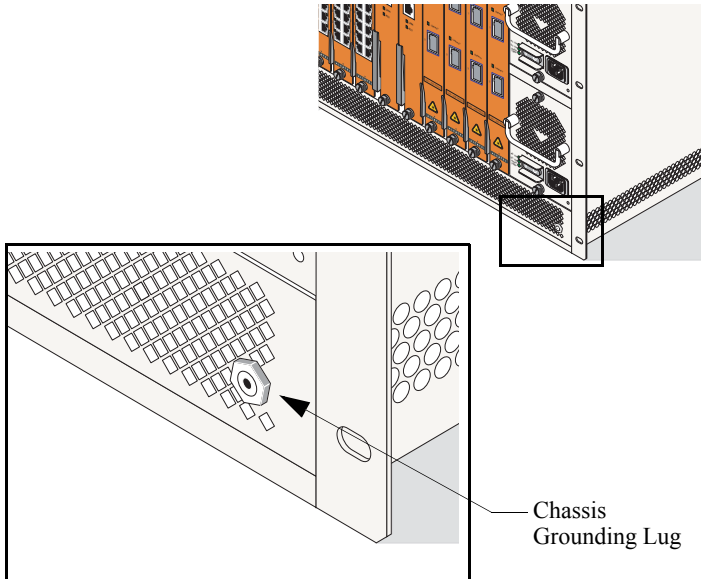
Note. The grounding lug diagram on the left is a general diagram only. It is intended to show the location of the grounding lug. No NI modules or CMMs should be installed in your chassis at this time.

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 .

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 9000 Series CMMs and NIs are colored orange to distinguish them from OmniSwitch 7700/7800 CMMs and NIs that are colored white. Do not install OmniSwitch 9000 Series and OmniSwitch 7700/7800 CMMs and NIs in the same chassis.

NI Modules

NI modules may be installed in any slot position from 1 through 16 in OS9800 switches, 1 through 8 in OS9700 switches and 1 through 4 in OS9600 switches.

CMMs

On OmniSwitch 9000 Series switches, a minimum of one CMM is required for switch operations. On OmniSwitch 9700/9800 switches, the second CMM provides redundancy. CMMs may be installed either in slot A or slot B in OmniSwitch 9700/9800 switches.

> **Note.** CMM redundancy is not supported on OmniSwitch 9600 switches because OS9600 switches contain only one CMM slot.

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 more information on redundancy, refer to page 50 or for detailed information, refer to the *OmniSwitch 9000 Series Hardware Users Guide*.

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

> **More Information on Slot Numbering.** For a diagram showing the chassis layout and slot positions, refer to "Chassis Slot Numbering" on page 48.

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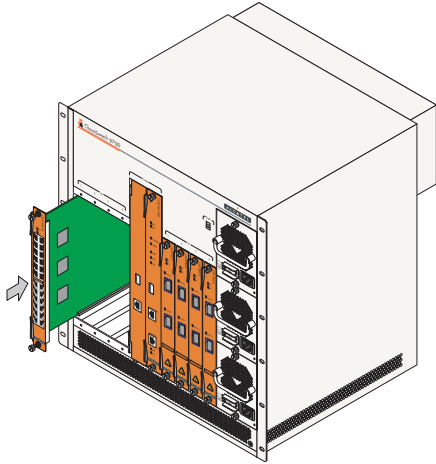
2 The module should slide in easily. Do not force the module into the slot. If any resistance is encountered, ensure that the module is aligned properly in the card guide. Also, see the important note regarding chassis card guides on .

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.

Chassis Attachment Rail

Notch in Extractor Lever
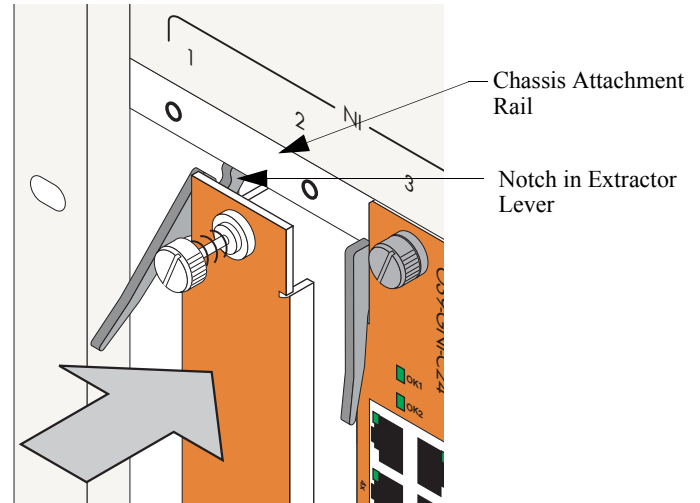
4 Once the module is firmly seated, secure the module to the chassis by tightening the two captive screws. *Be sure not to overtighten the captive screws. If you use a screw-driver, the torque used to tighten the screws must not exceed 2.3 foot pounds.*
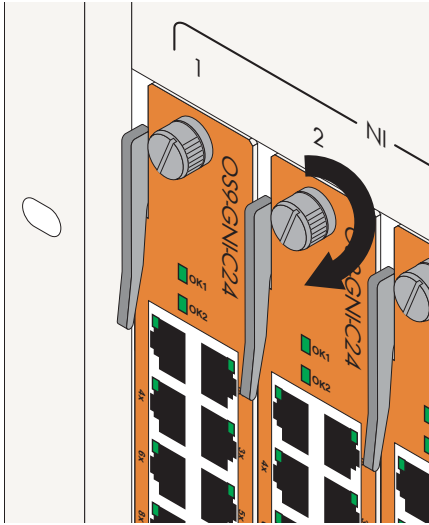
5 Install all remaining modules by repeating steps 1 through 4 for each module.

Installing XFP Connectors

If you are installing an OS9-XNI-U2 or OS9-XNI-U6 module, you must install 10 Gbps Small Form Factor Pluggables (XFPs) as required. OS9-XNI-U2 modules provide ports for up to two XFPs. OS9-XNI-U6 modules provide ports for up to six XFPs. These XFPs are packaged separately.

To install an XFP follow the steps below:

1 Be sure you have eliminated ESD by using the grounding wrist strap that has been provided. Refer to "Using the Grounding Wrist Strap and Chassis Grounding Lug" on page 13 for more information.

2 Note that there is an alignment groove used to keep the XFP from being installed backward or upside-down. Orient the XFP with the slot located on the OS9-XNI-U2 or OS9-XNI-U6 module and carefully slide the XFP into place until the tabs lock.

Caution. Do not force the XFP into the slot. If the XFP does not slide easily into position, verify that the XFP grooves are aligned properly. Forcing the XFP into the slot can damage the unit as well as the components on your XNI module.

Installing MiniGBIC Connectors

If you are installing an OS9-GNI-U24 module, you must install Miniature Gigabit Interface Converters (MiniGBICs) as required. OS9-GNI-U24 modules provide ports for up to 24 MiniGBICs. These MiniGBICs are packaged separately.

To install a MiniGBIC follow the steps below:

1 Be sure you have eliminated ESD by using the grounding wrist strap that has been provided. Refer to "Using the Grounding Wrist Strap and Chassis Grounding Lug" on page 13 for more information.

2   When inserting a MiniGBIC, be sure that the hinged face is closed.

3   Slide the MiniGBIC straight into the slot until the module clicks firmly into place.

Note. The diagram below is a representation only; the physical appearance of the actual MiniGBIC may vary.
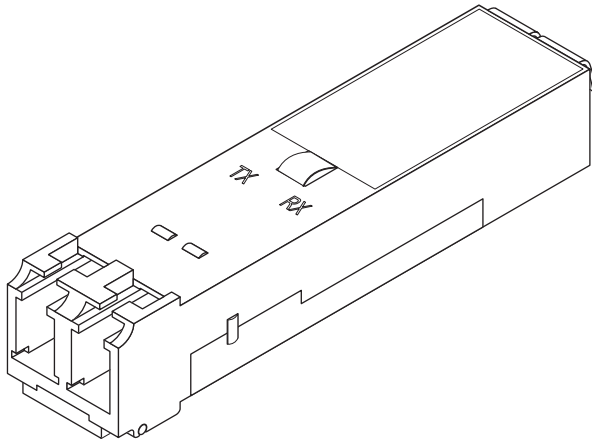
Caution. The MiniGBIC should slide in easily. Do not force it into the slot. If any resistance is encountered, ensure the MiniGBIC is aligned properly. Forcing the MiniGBIC into the slot can damage the unit as well as components on your GNI module.

Note. To remove a MiniGBIC, you must first open the MiniGBIC's hinged face to approximately 90°. Then, grasp the hinged face and carefully pull the MiniGBIC straight out of the slot.

Note. For further details regarding supported SFP and XFP transceivers, refer to the *OmniSwitch 9000 Series Hardware Users 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 26.

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 module descriptions on page 53 through page 59.

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 (|) 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 Customer Support.

For descriptions of CMM and NI LED states, see page 53 through page 59. For information on power supply LED states, refer to the *OmniSwitch 9000 Series 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 20.

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 OmniSwitch 9000
Software Version 6.1.1.350.R01: September 15, 2005.

Copyright(c), 1994-2003 Alcatel Internetworking, Inc.
All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel Internetwork-
ing, Inc. registered 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 *OmniSwitch 9000 Series 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 OmniSwitch 9000 switches. 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
```

How Many Sessions are Allowed?

Once a session type has been unlocked, the following number of sessions are allowed for each type:

Telnet sessions allowed	4 concurrent sessions
FTP sessions allowed	4 concurrent sessions
HTTP (Web browser) sessions allowed	4 concurrent sessions
Secure Shell and Secure Shell FTP sessions allowed	8 concurrent sessions
Total sessions (Telnet, FTP, HTTP, Secure Shell and Secure Shell FTP, console)	21 concurrent sessions
SNMP sessions allowed	50 concurrent sessions

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).

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 *engr*. A better password might be *engr2735*.

---

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 on OS9000 switches 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.

User Accounts. The switch allows a maximum of 50 user accounts in the local user database. For information on creating additional user types and assigning individual passwords, refer to the *Switch Management Guide*.

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 time-zone** 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 06/27/2004
```

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 of up to 254 characters. 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 description of up to 254 characters. 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 description of up to 254 characters. 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 36.

> **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 page 38 for important information on these directories.

Modifying the Serial Connection Settings

The switch's serial connection defaults are listed on page 18. 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 serialstop-bits**, 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 9000 switch 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.

CLI Basics

Command Line Interface (CLI) allows you to configure and monitor your switch by entering single-line commands. The CLI can be accessed through terminal or Telnet sessions.

> **Note.** Configuring the switch by using the CLI is also referred to as "online configuration."

The following section provides basic information on CLI assistance features. For detailed information on the CLI, including syntax conventions, usage rules, command documentation, and a quick reference card, refer to the *OmniSwitch CLI Reference Guide* and the *Switch Management Guide*.

CLI Assistance Features

The CLI provides inbuilt features that assist you while entering commands. These features include:

- Syntax checking
- Command line help
- Partial keyword completion
- Deleting and inserting characters
- Previous command recall
- Prefix recognition
- Prefix prompt
- Command history and command logging

> **Note.** The software supports vt100 terminal emulation; CLI assistance features may be limited if your terminal emulation software is using a setting other than vt100.

Syntax Checking

If you make a mistake while entering command syntax, the CLI provides clues about how to correct the error. Whenever a command error is entered, two indicators are displayed:

- An Error message describing the type of error.
- A carat (^) character indicating where the error occurred.

For example, the syntax

```
-> show vlan router port mac status
```
results in the following error:

```
-> show vlan router port mac status
                        ^
ERROR: Invalid entry: "port"
```

Because **port** is not valid syntax for the command, the error message shows it as an invalid entry and the carat indicates where the problem has occurred. For this example, the valid command syntax is

```
-> show vlan router mac status
```

Command Line (?) Help

The CLI provides additional help in the form of the question mark (**?**) character. The **?** character provides information that helps you build your command syntax. For example, if you enter

```
-> show vlan router
```

at the command line and are unsure of the next keyword, you can enter the **?** character for additional options (be sure to include a space between the last keyword and the **?** character):

```
-> show vlan router ?
                     ^

                  MAC
      (Vlan Manager Command Set)
```

The carat character (^) indicates the point where you invoked the command line help. Possible keyword options along with the corresponding command set are displayed. Here, you can continue building the command by entering **mac**.

Some command completion options may indicate user-defined information. For example: **<string>**, **<slot/port>**, **<hh:mm:ss>**, etc. The option **<cr>** indicates that the command can be completed by pressing **Enter**.

> **Note.** The **?** character can be entered at any time. In addition, you can type the **?** character alone at the CLI prompt to display root keywords for *all* command sets.

Partial Keyword Completion

The CLI has a partial keyword recognition feature. Instead of typing an entire keyword, you can type only the minimum number of characters needed to uniquely identify the keyword, and then press the **Tab** key. The CLI will complete the keyword and place the cursor at the end of the command line.

If you do not enter enough characters to uniquely identify the keyword, pressing the **Tab** key will have no effect.

If you enter characters that do not belong to an applicable keyword, pressing the **Tab** key will remove the characters and place the cursor back in its previous position.

Deleting Characters

You can delete CLI command characters by using the **Backspace** key or the **Delete** key. The **Backspace** key deletes each character in a line, one at a time, from right to left.

To change incorrect syntax with the **Delete** key, use the **Left Arrow** key to move the cursor to the left of the character to be deleted, and then use the **Delete** key to remove characters to the right of the cursor.

Inserting Characters

To insert a character between characters that are already typed, use the **Left** and **Right Arrow** keys to place the cursor into position, and then type the new character. Once the syntax is correct, execute the command by pressing **Enter**. In the following example, the user enters incorrect syntax to execute a command. The result is an error message.

```
-> show micrcode
         ^
ERROR: Invalid entry: "micrcode"
```

To correct the syntax without retyping the entire command line, use the **!!** command to recall the previous syntax. Then, use the **Left Arrow** key to position the cursor between the "r" and the "c" characters. To insert the missing character for this example, type "o" as shown:

```
-> !!
-> show microcode
```

Previous Command Recall

To recall the last command executed by the switch, press the **Up Arrow** key at the prompt. The previous command will be displayed on your screen. You can execute the command again by pressing **Enter**, or you can edit it first by deleting or inserting characters.

Prefix Recognition

Prefix recognition is a CLI feature that reduces redundant command line entry by storing commonly-used prefix information for certain commands. The CLI assumes this stored prefix information when the next command is entered. For example, if you enter

```
-> vlan 32
```

at the command line, the CLI will store the **vlan 32** prefix information.

The following command families support prefix recognition:

- AAA

- Interface

- Link Aggregation

- Quality of Service (QoS)

- Spanning Tree

- VLAN Management

Prefix Prompt

You can set the CLI to display the current command prefix *as the command prompt* by entering the following command:

```
-> prompt prefix
```

After entering this command, your command prompt will include current stored prefix information until a new prompt is specified. For example, the following is a prompt for a user who has begun configuring VLAN 32:

```
-> vlan 32
```

To set the prompt back to the default arrow (**->**), enter the following syntax, exactly as shown, at the prefix prompt:

```
-> prompt
```

Command History

You can view a list of up to 30 of the most recently executed commands via the **show history** command. For example:

```
-> show history
1 show cmm
2 show fan
3 show sensor
4 show temperature
5 ip load dvmrp
6 show arp
7 show cmm
8 show fan
9 show sensor
10 show temperature
11 ip load dvmrp
12 show arp
13 show history
```

Note that the most recent commands are displayed *lower* in the list. For this reason, the **show history** command will always be listed last.

You can recall commands from the history list by entering an exclamation point (**!**). For example:

```
-> !4
-> show temperature
```

The CLI prints the fourth command from the history list (in this case, **show temperature**) at the CLI prompt.

You can also recall the *last* command in the history list by entering two exclamation points (**!!**). For example:

```
-> !!
-> show history
```

To specify the number of commands displayed in the history list (1 - 30), use the **history size** command. For example:

```
-> history size 10
```

To view the current history list settings, use the **show history parameters** command. For example:

```
-> show history parameters
History size: 30
CurrentSize: 10
Index Range: 1-10
```

Command Logging

OmniSwitch 9000 switches provide command logging. This feature allows users to record up to 100 of the most recent commands entered via Telnet and console sessions. In addition to a list of commands entered, the results of each command entry are recorded. Results include information such as whether a command was executed successfully, or whether a syntax or configuration error occurred.

> **Note.** The **command history** feature differs from the **command logging** feature in that the command history buffers up to 30 of the most recent commands. The command information is *not* written to a separate log file. Also, the command history feature includes only general keyword syntax (i.e., it does not record full syntax, date and time, session IP address, and entry results). For more information on command history, refer to page 32.

Refer to the sections below for more information on configuring and using CLI command logging. For detailed information related to command logging commands, refer to the *OmniSwitch CLI Reference Guide*.

Enabling Command Logging

By default, command logging is *disabled*. To enable command logging on the switch, enter the following command:

```
-> command-log enable
```

When command logging is enabled via the **command-log enable** syntax, a file called **command.log** is automatically created in the switch's **/flash** directory. Once enabled, configuration commands entered at the command line are recorded in this file until command logging is disabled.

The **command.log** file has a 66402 byte capacity. This capacity allows up to 100 of the most recent commands to be recorded. Because all CLI command logging information is archived to the **command.log** file, command history information will be lost if the file is deleted.

> **Note.** The **command.log** file cannot be deleted while the command logging feature is enabled. Before attempting to remove the file, be sure to disable command logging.

For detailed information on command logging, refer to "Using the CLI" in the *Switch Management Guide*.

Common CLI Commands

The following table lists some basic CLI commands that will help you get acquainted with the CLI interface. Enter each command exactly as shown. For complete descriptions of these commands, refer to your *CLI Reference Guide*.

write memory	Saves current configuration changes to the **/flash/working** directory's **boot.cfg** file. For more information, refer to .
show running-directory	Displays the current running directory. For more information, refer to .
vlan	Creates a new VLAN.
show vlan	Displays a list of VLANs configured on the switch.
ip interface	Configures an IP interface to enable IP routing on a VLAN.
show chassis	Displays basic configuration and status information for the switch chassis.
show module	Displays basic information for switches in a stacked configuration.
show ni	Displays basic hardware and status information for a stand-alone switch, or for all switches installed in a stacked configuration.
show cmm	Displays basic hardware and status information for a stand-alone switch, or for the primary or secondary switches installed in a stacked configuration.
show system	Displays basic information about the switch.
show microcode	Displays the version of software currently installed on the switch.
session timeout	Modifies the amount of time before Telnet and console sessions time out.
who	Displays all active login sessions (e.g., Console, Telnet, FTP, HTTP, Secure Shell, and Secure Shell FTP)
exit	Ends the current Telnet or console session.

Offline Configuring

You can configure OmniSwitch 9000 switches by using an ASCII-based text file. This is referred to as *offline configuring*. With offline configuring, CLI commands may be typed into a text document (referred to as a *text-based configuration file*) and then uploaded and applied to the switch.

An ASCII-based configuration file can be viewed or edited at any time by using a standard text editor (e.g., WordPad). The switch also offers its own text editing buffer. This enables editing of files in the flash file directory without having to download them to a workstation.

Because they are portable, stand-alone documents, configuration files allow users to clone switch configurations easily. Moreover, the ability to store a broad range of network information in a single text file facilitates troubleshooting, testing, and overall network readability.

Syntax Checking

Offline configuration includes a syntax check feature. This function reports syntax errors or typos that might cause a command to be rejected by the switch when a configuration file is applied.

Scheduling a Configuration File to be Applied at a Later Time

You can apply a file to the switch immediately, or you can schedule a file to be applied either at a specific date and time or after a specific amount of time has passed. Timer sessions can greatly facilitate maintenance tasks, such as synchronized batch updates.

Generating Snapshots of the Current Configuration

A generated snapshot captures the switch's current configuration settings in a single text file. The captured configuration settings can then be viewed or edited offline at any time. Troubleshooting is greatly facilitated, because aggregate network information can be read at a glance.

Snapshot files can be used as configuration files for a single switch or for multiple switches. This allows easy cloning of switch configurations for networks requiring multiple, similarly-configured switches. Simply place the snapshot file in the appropriate directory of the switch(es) you want to configure and use the CLI to apply the file.

For detailed information on offline configuring and the features described above, refer to the *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 38 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 execut-able 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 direc-tory 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 Customer Support for replacements. There-fore, it is recommended that you keep backup copies on your computer's hard drive or a locally-accessible server.

For a complete list of OmniSwitch 9000 Series image files along with their functions, refer to the table below.
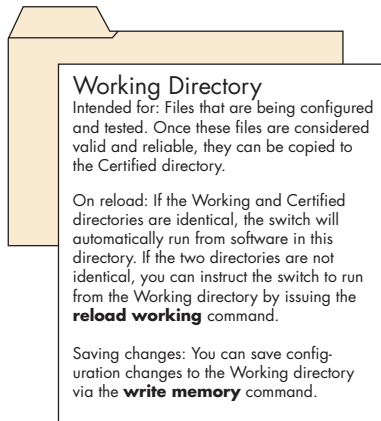
Jos.img	Contains the OmniSwitch 9000 Series operating system software.
Jbase.img	Contains base code for the switch.
Jeni.img	Provides support for 10/100, Fast Ether-net, and Gigabit Ethernet.
Jdiag.img	Provides enhanced hardware diagnostics for the switch.
Jadvrout.img	Alcatel's Advanced Routing software package. Optional.

Working and Certified Directories

Switches are shipped with 128 MB of 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

Working Directory
Intended for: Files that are being configured and tested. Once these files are considered valid and reliable, they can be copied to the Certified directory.

On reload: If the Working and Certified directories are identical, the switch will automatically run from software in this directory. If the two directories are not identical, you can instruct the switch to run from the Working directory by issuing the **reload working** command.

Saving changes: You can save configuration changes to the Working directory via the **write memory** command.
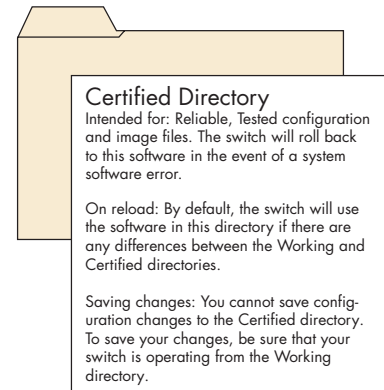
The **/flash/working** directory is intended for software that is still being configured for your network. Changes made while configuring your switch are saved to the **boot.cfg** file in the **/flash/working** directory.

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

Certified Directory
Intended for: Reliable, Tested configuration and image files. The switch will roll back to this software in the event of a system software error.

On reload: By default, the switch will use the software in this directory if there are any differences between the Working and Certified directories.

Saving changes: You cannot save configuration changes to the Certified directory. To save your changes, be sure that your switch is operating from the Working 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.

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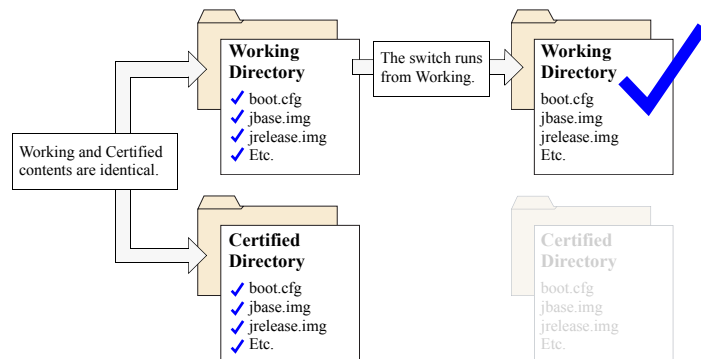
When the switch is running from the **/flash/working** directory software, configuration changes can be saved via the **write memory** command.

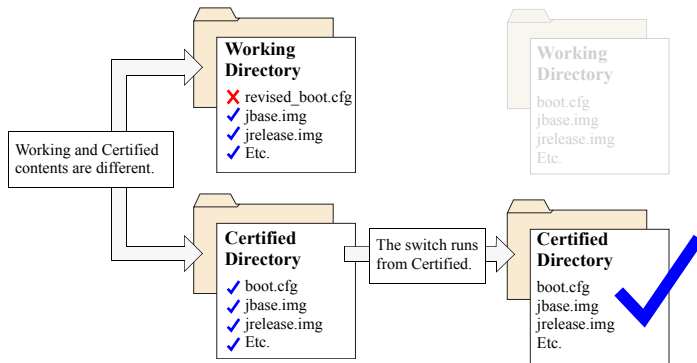## Working and Certified Are Different

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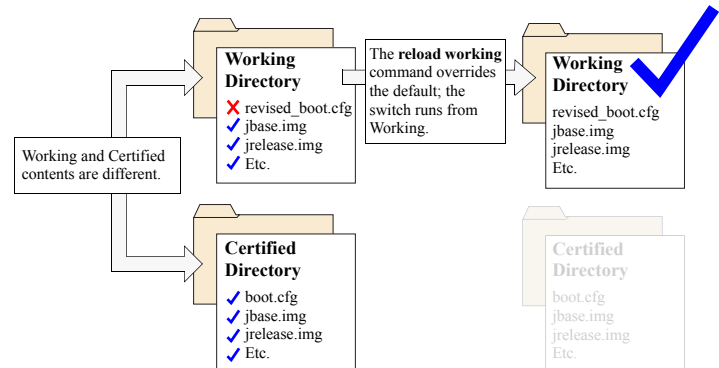
Note. For detailed information on using directories, refer to the *Switch Management Guide*.

Loading Software

The following section describes the procedure for loading new release software to your switch. Note that the procedure varies slightly for non-redundant (single CMM) and redundant (dual CMM) configurations. Follow the steps that apply to your system.

Note. For detailed information on loading software and working with directories in both non-redundant and redundant CMM configurations, refer to the *Switch Management Guide*.

Non-Redundant Configurations

1 Verify that all required image files from the new software release are located on your computer's hard drive or a *locally accessible* server.

2 Establish an FTP session to the switch, and then access the **/flash/working** directory.

Note. Before attempting to establish an FTP session, be sure that you have first unlocked the FTP session type via the **aaa authentication** command. Otherwise, an FTP login error will occur. See "Unlocking Session Types" on page 22 for more information.

---

3 Using your FTP client or the CLI's **rm** command, delete all **.img** files from the **/flash/working** directory. You can use the asterisk (*****) wildcard to delete all **.img** files at once. For example:
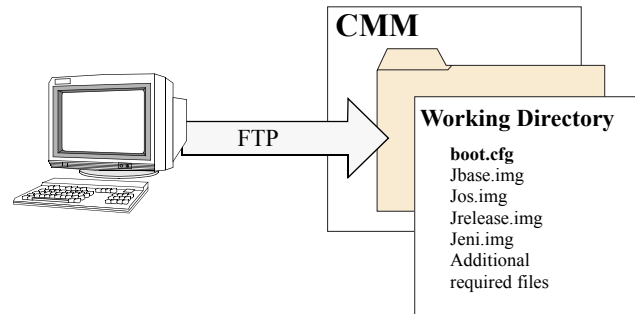
```
-> rm working/*.img
```

Important. Do not delete the **boot.cfg** file. Otherwise, any configuration changes you have saved will be lost. Also, do not delete files from the **/flash/certified** directory.

---

4 Using your FTP client, upload all required **.img** files from the new software release to the **/flash/working** directory.

5 Use the **install** command after the software files have been transferred to the switch via FTP. For example:

```
-> install /flash/working/*.img
```

Note. For more information on the **install** command, refer to the *Switch Management Guide* or the *CLI Reference Guide*.

6 Reload the switch from the **/flash/working** directory. To do this, enter

```
-> reload working no rollback-timeout
```

at the CLI prompt.

Note. This reload process will take a few moments to complete.

Following the reload, the switch will come up running from the **/flash/working** directory (i.e., the new release software) until the next system reboot. Meanwhile, the software in the **/flash/certified** directory remains unchanged and available as a last known good version if an error should occur with the new software.

Once the release software is considered valid and reliable with your network configuration, the contents of the **/flash/working** directory can be copied to the **/flash/certified** directory via the **copy working certified** command.

Redundant Configurations

1 Verify that the OK1 LED is solid green and the OK2 LED is flashing green on both the primary and secondary CMM modules.

2 Next, verify that all required image files from the new software release are located on your computer's hard drive or a *locally accessible* server.

3 Establish an FTP session to the switch, and then access the **/flash/working** directory.

Note. Before attempting to establish an FTP session, be sure that you have first unlocked the FTP session type via the **aaa authentication** command. Otherwise, an FTP login error will occur. See for more information.

4 Using your FTP client or the CLI's **rm** command, delete all **.img** files from the **/flash/working** directory on the *primary* CMM. (To determine whether you are logged into the primary CMM, use the **show running-directory** command.) You can use the asterisk (*****) wildcard to delete all **.img** files at once. For example:

```
-> rm working/*.img
```

Important. Do not delete the **boot.cfg** file. Otherwise, any configuration changes you have saved will be lost. Also, do not delete files from the **/flash/certified** directory.

5 Using your FTP client, upload all required **.img** files from the new software release to the primary CMM's **/flash/working** directory.

6 Use the **install** command after the software files have been transferred to the switch via FTP. For example:

```
-> install /flash/working/*.img
```

Note. For more information on the **install** command, refer to the *Switch Management Guide* or the *CLI Reference Guide*.

---

7 Reload the switch from the **/flash/working** directory. To do this, enter

```
-> reload working no rollback-timeout
```

at the CLI prompt.

Note. This reload process will take a few moments to complete.

During this reload, the secondary CMM takes over the primary role and the switch runs from the **/flash/working** directory (i.e., the new release software) until the next system reboot. Meanwhile, the software in the **/flash/certified** directory remains unchanged and available as a last known good version if an error should occur with the new software.

Once the release software is considered valid and reliable with your network configuration, the contents of the **/flash/working** directory can be copied to the **/flash/certified** directory of each CMM by entering the following command:

```
-> copy working certified flash-synchro
```

This command provides two functions. It copies all contents from **/flash/working** to the **/flash/certified** directory on the primary CMM, *and* it copies all directory contents from the primary CMM to the secondary CMM synchronizing the two modules. This helps to ensure effective CMM redundancy.

Note. The process initialized by the **copy working certified flash-synchro** command will take a few moments to complete.

Using WebView

OmniSwitch 9000 switches can be configured and monitored using WebView, Alcatel'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 22 for more information.

Browser Compatibility

WebView has been tested on the following Web browsers:

- Internet Explorer 6.0 for Windows 2000, Windows NT, and Windows XP

- Netscape 4.79 for Solaris 2.8, and HP-UX 11.0

- Netscape 7.1 for Windows 2000, Windows NT, and Solaris 2.8

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 22 for more information.

To access WebView and log in to a switch:

1 Open any Alcatel-tested Web browser (see page 44).

2 Enter the switch's IP address in the browser's "Address" text field ("Location:" for Netscape users). The login screen displays:
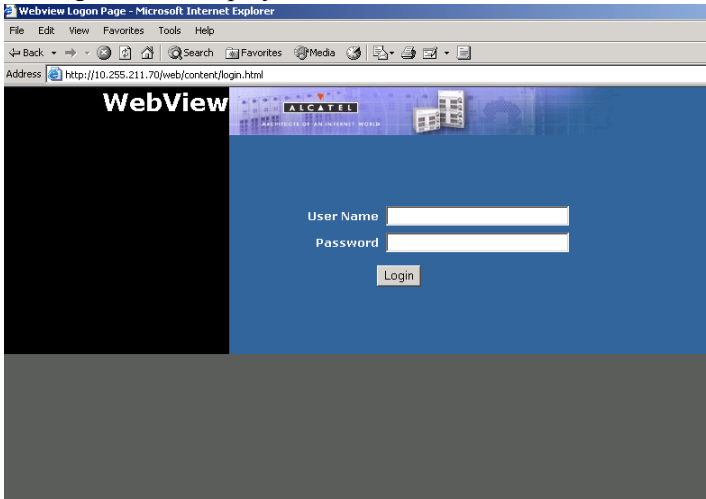
3 Enter the user name and password at the login prompt.

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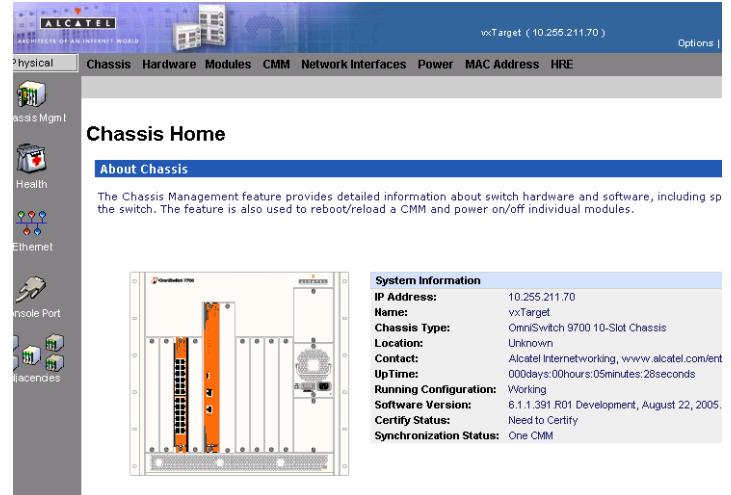
The Chassis Management home page provides a physical representation of the switch as well as basic system information. This is the main launching point for WebView.

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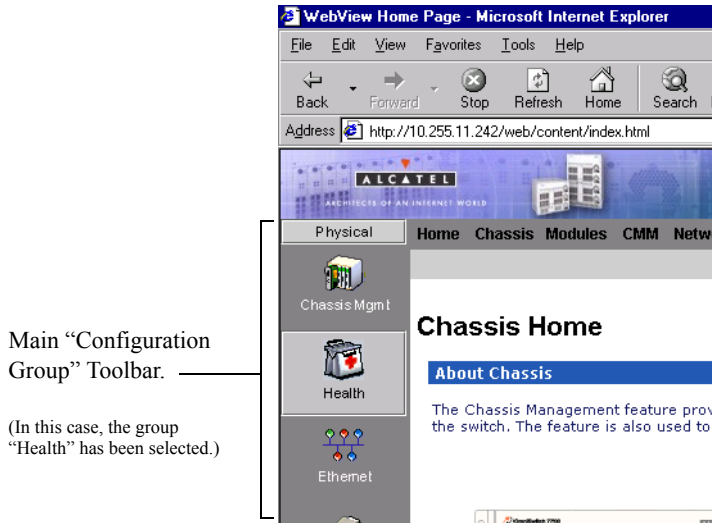
Refine your navigation by selecting "Configuration Options" for each group from the items displayed in the grey, horizontal navigation bar.

"Configuration Options" Toolbar.

(In this case, the option "Device" has been selected.)
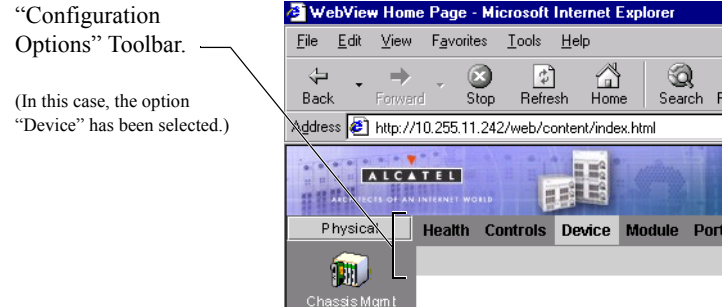
Site Maps. WebView also provides site maps for each configuration group. Site maps allow you to view complete page contents under each feature. By providing quick, easy access to specific pages, site maps can reduce time spent searching through the WebView application. To access site maps, click the "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

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

VLAN Administration

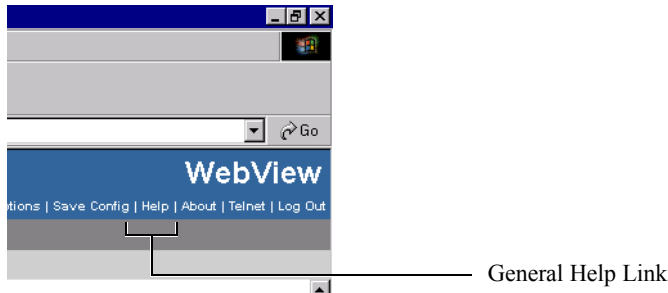|	VLAN ▼	Description	Admin Status	Operational Status	Flat STP Status	1x1 STP Status	IP	IPX
☐	1	VLAN 1	Enabled	Active	Enabled	Enabled	On	Off

[Expanded View]

Add   Modify   Delete   Refresh   Help

Context-specific Help button.

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

Additional Information

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

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 21 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
  ```

See page 22 for information on unlocking session types.

Hardware Basics

Chassis Slot Numbering

The term "slot" refers to the position at which a module is installed in the chassis. CMM slot positions are designated as Slots A and B. For the OS9800, NI slot numbers range from 1 to 16. For the OS9700, NI slot numbers range from 1 to 8. For the OS9600, NI slot numbers range from 1 to 4.

Power supply bays are also given specific slot numbers. For the OS9800, slot numbers are designated PS-1 through PS-4, from top to bottom. For the OS9700, slot numbers are designated PS-1 through PS-3, from top to bottom. For the OS9600, slot numbers are designated PS-1 and PS-2, from top to bottom.
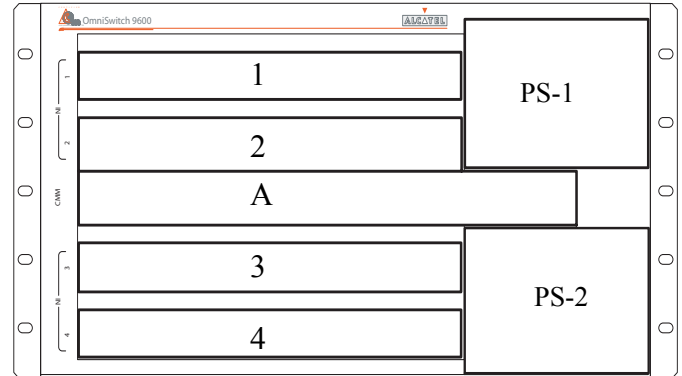
OmniSwitch 9600 Slot Numbering
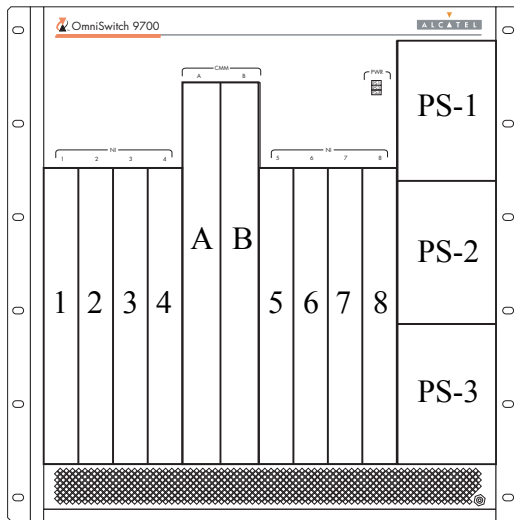
OmniSwitch 9700 Slot Numbering
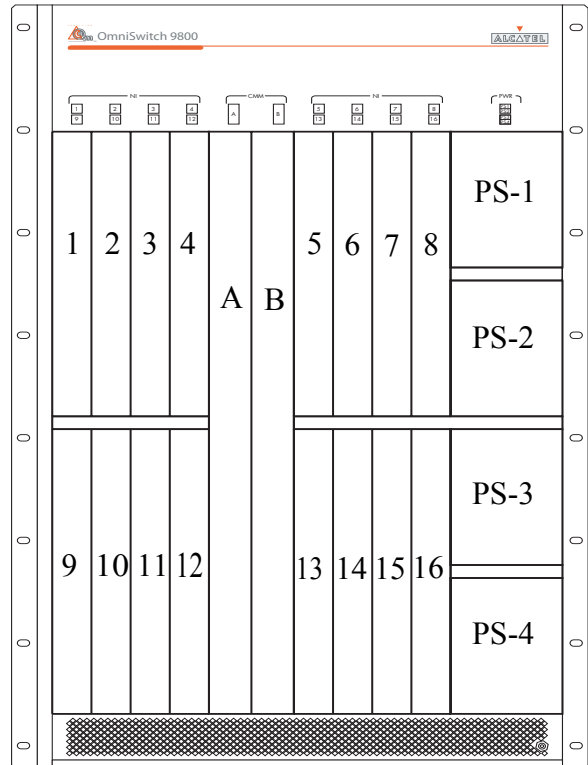
OmniSwitch 9800 Slot Numbering

Chassis Management Module (CMM)

The Chassis Management Module (CMM) is the management unit for OmniSwitch 9000 Series switches. In its role as the management unit, the CMM provides key system services, including:

- Console, modem, and Ethernet management port connections to the switch

- Software and configuration management, including the Command Line Interface (CLI)

- Web-based management (WebView)

- SNMP management

- Power management

- Temperature management

- Switch diagnostics

- Important availability features, including redundancy (when used in conjunction with another CMM) and image rollback

CMM Redundancy

CMM redundancy is an important resiliency feature. For CMM redundancy, two fully-operational CMM modules must be installed in the chassis at all times.

> **Note.** CMM redundancy is not supported on OmniSwitch 9600 switches because OS9600 switches contain only one CMM slot.

When two CMMs are running in the switch, one CMM has the primary role and the other has the secondary role at any given time. The primary CMM manages the current switch operations, while the secondary CMM provides backup (also referred to as "failover").

> **Note.** By default, the CMM in slot A automatically assumes the primary role. Refer to page 48 or page 51 for CMM slot A and B positions.

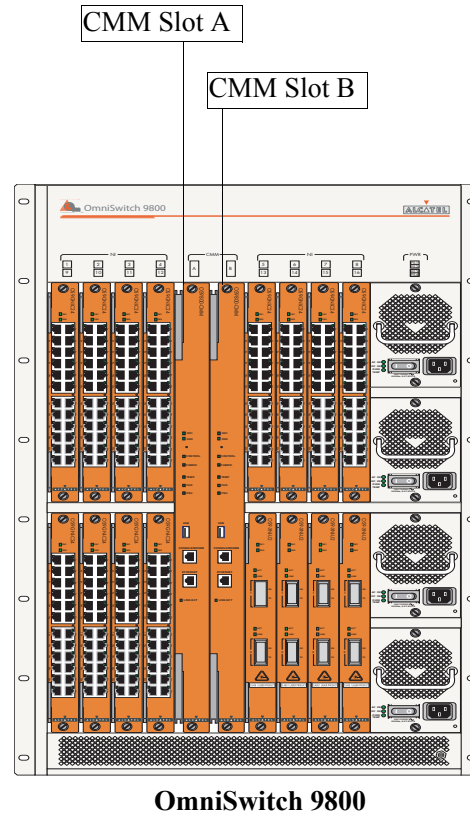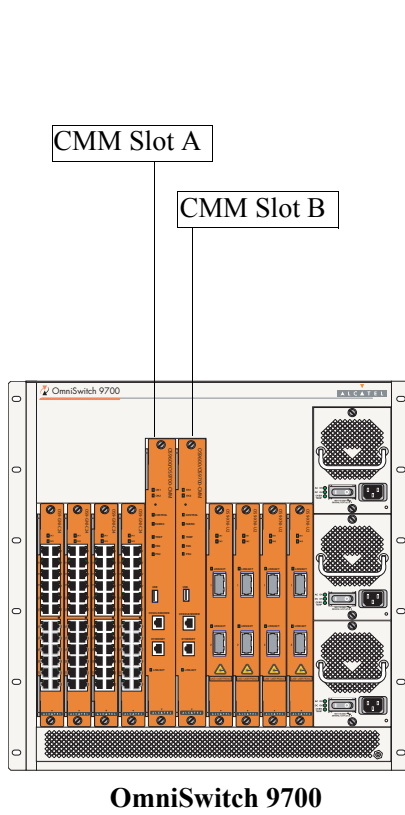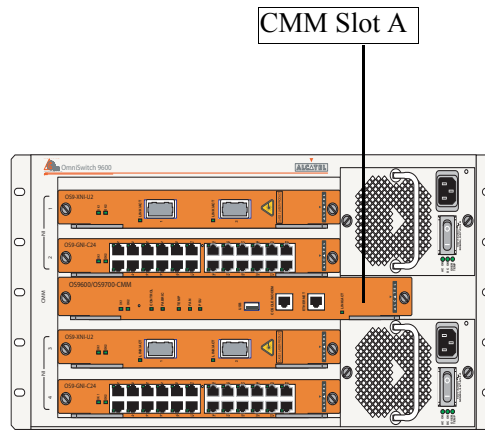If the primary CMM fails or goes offline for any reason, the secondary CMM is notified. The secondary CMM then automatically assumes the primary role.

For important information on CMM redundancy, refer to the *OmniSwitch 9000 Series Hardware Users Guide*.

CMM Slot Locations

CMM Slot A

CMM Slot B

CMM Slot A

CMM Slot B

OmniSwitch 9700

OmniSwitch 9800

CMM Slot A

OmniSwitch 9600

CMM Front Panel

Module Status LEDs
OK1. Hardware Status. Displays solid green when powered on, and the CMM has passed hardware diagnostic tests. Displays solid amber when powered on, and the CMM has failed hardware diagnostic tests.

OK2. Software Status. Blinks green when the CMM is operational. Displays solid amber when a system software failure occurs. Blinks amber when the software is in a transitional state (e.g., when software is being downloaded to the switch).

Control/FabricsPSU/Temperature/Fan status LEDs
CONTROL. Dislays solid green when the CMM is active, blinking green when on standby mode, amber when malfunctioning, and blinking amber for upgrade.

FABRIC. Displays solid green when the fabric is active, blinking amber or steady amber for different fabric malfunctions.

PSU. Displays green when power is OK, blinking amber when one PSU is bad but the chassis has enough power, and solid amber when the chassis does not have enough power.

TEMP. Displays green at 0-40°C, blinking amber at 40-45°C, and solid amber at over 45°C.

FAN. Displays solid green when all fans in the fan tray are running at normal speed. Displays solid amber if a fan error occurs (i.e., one or more fans are not running at normal speed).

Ethernet Management Port LEDs
LINK. Link/Activity Status. Displays solid green when an Ethernet cable connection exists at the CMM's Ethernet Management Port. Flashes green as data is transmitted or received.

USB Port. High speed (480 Mbps) USB 2.0 port, which can be used for quick upgrades.
Note: USB port is not supported in this release.

Console Port. The CMM's front panel provides one RJ45 port for console connections. By default, this connector provides a DCE console connection.

Ethernet Management Port (EMP). The CMM's front panel also provides one Ethernet 10/100/1000BaseT port (copper RJ-45). This port provides out-of-band network management and can be used for Telnet sessions, switch diagnostics, and for downloading software to the switch.

This 10/100/1000BaseT port supports all three ports 10BaseT, 100BaseT, and 1000BaseT with auto-negotiation through the RJ-45 connector.

Note: In redundant CMM configurations, the EMP is only operational on the *primary* CMM.

CMM Front Panel (OS9600/0S9700-CMM version shown)

Network Interface (NI) Modules

The following section outlines front panel information for Network Interface (NI) modules, including LED and port descriptions. For detailed information on all modules, refer the *OmniSwitch 9000 Series Hardware Users Guide*.

GNI Modules

The Gigabit Ethernet Network Interface (GNI) modules provide up to twenty-four 1000 Mbps (1 Gbps) connections per module. GNI modules can be used for backbone connections in networks where Gigabit Ethernet is used as the backbone media. GNI modules can also be used in the wiring closet for connections to workstations and other devices.

- **OS9-GNI-C24**. Provides 24 auto-sensing twisted-pair ports, auto-negotiating *and* individually configurable as 10BaseT, 100BaseTX, or 1000BaseT.

- **OS9-GNI-U24**. Provides 24 connectors for use with hot-swappable SFP MSAs. Refer to "Miniature Gigabit Interface Converters (SFP MSA)" on page 54 for information on connections supported by SFP MSAs.

- **OS9-GNI-P24**. Provides 24 auto-sensing twisted-pair ports with Power over Ethernet (PoE) support *and* individually configurable as 10BaseT, 100BaseTX, or 1000BaseT.

XNI Modules

The 10-Gigabit Network Interface (XNI) modules provide up to two (OS9-XNI-U2) and six (OS9-XNI-U6) 10, 000 Mbps (10 Gbps) connections per module, respectively. In addition, XNI modules can be used in enterprise applications including backbone connections in networks where 10-Gigabit Ethernet is used as the backbone media.

OS9-XNI-U2. Provides two connectors for use with hot-swappable XFPs. Refer to "10 Gbps Small Form Factor Pluggables (XFP MSAs)" on page 55 for information on connections supported by XFPs.

OS9-XNI-U6. Provides six connectors for use with hot-swappable XFPs. Refer to "10 Gbps Small Form Factor Pluggables (XFP MSAs)" on page 55 for information on connections supported by XFPs.

Miniature Gigabit Interface Converters (SFP MSA)

The OS9-GNI-U24 module provides 24 SFP MSA connectors. A SFP MSA is a Gigabit Ethernet port module that is hot-pluggable; i.e., it can be installed or removed while the GNI is powered on and operating without the risk of damage to the SFP MSA module or the host circuitry.

When a SFP MSA is installed, the switch automatically gathers basic SFP MSA information via the connector's serial E2PROM interface. This information includes the SFP MSA's capabilities, standard interfaces, manufacturer, and other information.

Customers should use only Alcatel-provided SFP MSA modules. Third party SFP MSA modules not provided by Alcatel are not guaranteed to work properly.

> **Note.** For a list of supported Gigabit Ethernet Transceivers (SFP MSA), refer to the *OmniSwitch 9000 Series Hardware Users Guide*.

> **Note.** For information on installing SFP MSA modules, refer to "Installing MiniGBIC Connectors" on page 16.

10 Gbps Small Form Factor Pluggables (XFP MSAs)

The OS9-XNI-U2 module provides two XFP MSA connectors and OS9-XNI-U6 module provides six XFP MSA connectors. An XFP MSA is a 10 Gbps small form factor pluggable module that is hot-pluggable; i.e., it can be installed or removed while the XNI is powered on and operating without the risk of damage to the XFP MSA module or the host circuitry.

Customers should use only Alcatel-provided XFP MSA modules. Third party XFP MSA modules not provided by Alcatel are not guaranteed to work properly.

> **Note.** For a list of supported 10 Gigabit Ethernet Transceivers (XFP MSA), refer to the *OmniSwitch 9000 Series Hardware Users Guide*.

> **Note.** For information on installing XFP MSA connectors, refer to "Installing XFP Connectors" on page 16.

OS9-GNI-U24 Front Panel

Module Status LEDs

OK1. Hardware Status. Displays solid green when powered on and the GNI has passed hardware diagnostic tests. Displays solid amber when powered on and the GNI has failed hardware diagnostic tests.

OK2. Software Status. Blinks green when the GNI is operational and has successfully loaded software. Displays solid amber when powered on and the GNI has failed to load software.

Gigabit Ethernet Port LEDs

Each fiber-based Gigabit Ethernet port has a corresponding LED. This LED indicates the link and activity status for each Gigabit Ethernet port. The LED displays green when a valid Gigabit Ethernet cable connection exists. Flashes green as data is transmitted or received on the port.

Module Status LEDs

Gigabit Ethernet Ports

The OS9-GNI-U24 module provides 24 MiniGBIC slots. For a list of supported Gigabit Ethernet Transceivers (SFP MSA), refer to the *OmniSwitch 9000 Series Hardware Users Guide.*
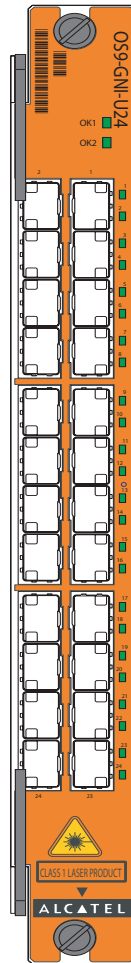
OS9-GNI-P24 Front Panel

Module Status LEDs

OK1. Hardware Status. Displays solid green when powered on and the GNI has passed hardware diagnostic tests. Displays solid amber when powered on and the GNI has failed hardware diagnostic tests.

OK2. Software Status. Blinks green when the GNI is operational and has successfully loaded software. Displays solid amber when powered on and the GNI has failed to load software.

PoE. PoE Status. This LED will be off if PoE is not available on this module and will be solid green if PoE is enabled on this module.

Ethernet Port LEDs

Each Gigabit Ethernet port has two built-in corresponding LEDs. The top LED indicates 10/100 Mbps link and activity status for the port while the bottom LED indicates 1 Gigabit link and activity status for the port. The appropriate LED displays solid green when a valid Ethernet cable connection exists and there is no PoE. Flashes green as data is transmitted or received on the port and there is no PoE. If PoE is present, the appropriate LED displays solid amber when a valid Ethernet cable connection exists. And flashes amber as data is transmitted or received on the port if PoE is present.

Module Status LEDs

Ethernet Ports

The OS9-GNI-P24 module provides 24 10/100/1000 Power over Ethernet (PoE) ports. These ports are twisted-pair and are individually configurable as 10BaseT, 100BaseTX, or 1000BaseT. The ports use RJ-45 connectors.

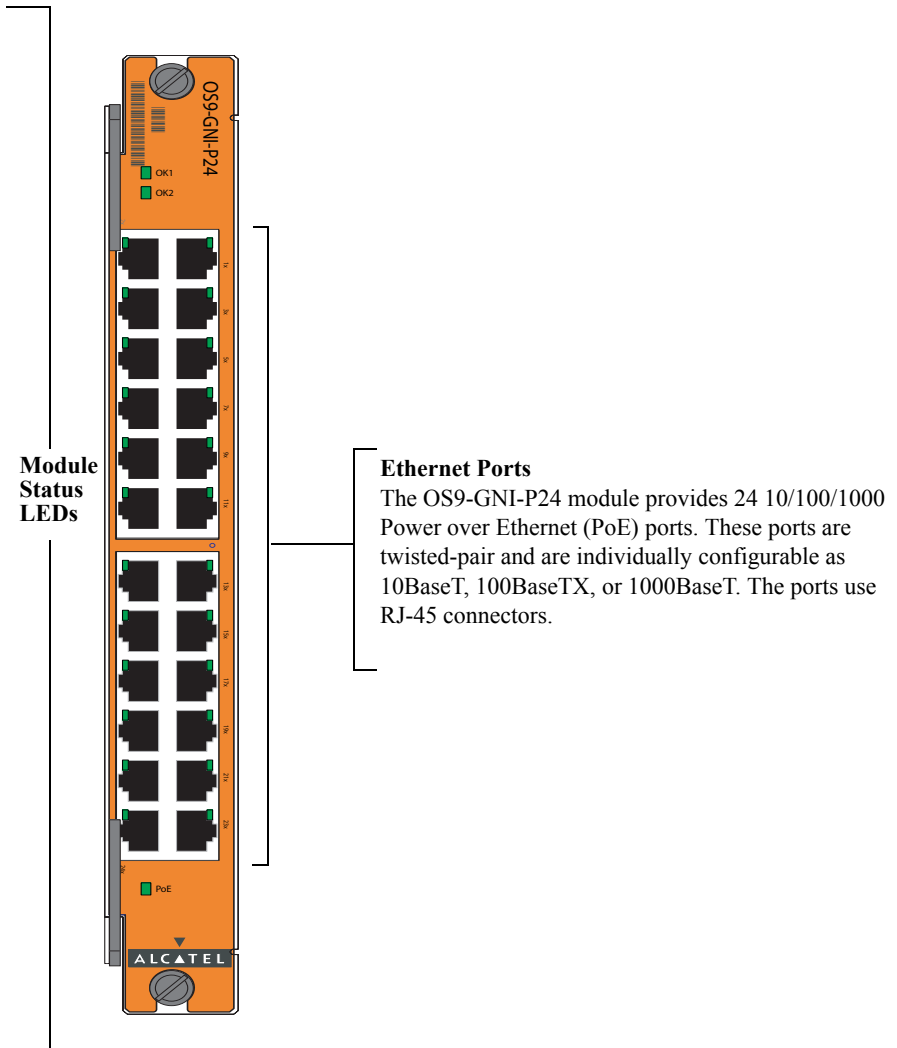# OS9-GNI-C24 Front Panel

Module Status LEDs

OK1. Hardware Status. Displays solid green when powered on and the GNI has passed hardware diagnostic tests. Displays solid amber when powered on and the GNI has failed hardware diagnostic tests.

OK2. Software Status. Blinks green when the GNI is operational and has successfully loaded software. Displays solid amber when powered on and the GNI has failed to load software.

Module Status LEDs

Ethernet Port LEDs

Each fiber-based Ethernet port has a corresponding LED. This LED indicates the link and activity status for each Ethernet port. The LED displays solid green when a valid Ethernet cable connection exists. Flashes green as data is transmitted or received on the port.

Ethernet Ports

The OS9-GNI-C24 module provides 24 10/100/1000 Ethernet ports. These ports are twisted-pair and are individually configurable as 10BaseT, 100BaseTX, or 1000BaseT. The ports use RJ-45 connectors.
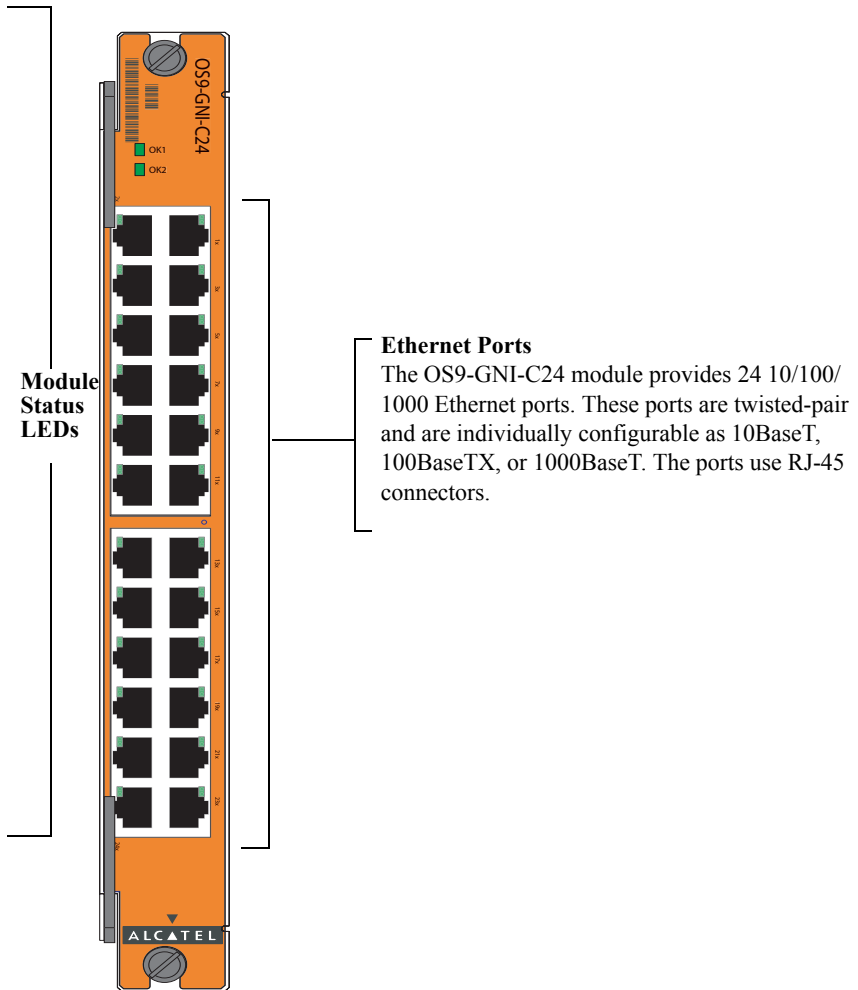
OS9-XNI-U2 Front Panel

Module Status LEDs

OK1. Hardware Status. Displays solid green when powered on and the XNI has passed hardware diagnostic tests. Displays solid amber when powered on and the 10GNI has failed hardware diagnostic tests.

OK2. Software Status. Blinks green when the XNI is operational and has successfully loaded software. Displays solid amber when powered on and the XNI has failed to load software.

LINK/ACT LEDs

Each 10 Gigabit port has a single LED for monitoring XFP link status and activity. The LED displays solid green when the port is up; the LED blinks green when the port is transmitting or receiving packets in a link-up state. The LED is off when no link is detected.

Module Status LEDs

10-Gigabit Ethernet Ports

The OS9-XNI-U2 module provides 2 XFP slots. For a list of supported 10 Gigabit Ethernet Transceivers (XFP MSA), refer to the *OmniSwitch 9000 Series Hardware Users Guide*.

OS9-XNI-U2

OK1
OK2

LINK/ACT

1

LINK/ACT

2

CLASS 1 LASER PRODUCT

ALCATEL

OS9-XNI-U6 Front Panel

Module Status LEDs

OK1. Hardware Status. Displays solid green when powered on and the XNI has passed hardware diagnostic tests. Displays solid amber when powered on and the 10GNI has failed hardware diagnostic tests.

OK2. Software Status. Blinks green when the XNI is operational and has successfully loaded software. Displays solid amber when powered on and the XNI has failed to load software.

Module Status LEDs

LINK/ACT LEDs

Each 10 Gigabit port has a single LED for monitoring XFP link status and activity. The LED displays solid green when the port is up; the LED blinks green when the port is transmitting or receiving packets in a link-up state. The LED is off when no link is detected.

10-Gigabit Ethernet Ports
The OS9-XNI-U6 module provides 6 XFP slots. For a list of supported 10 Gigabit Ethernet Transceivers (XFP MSA), refer to the *OmniSwitch 9000 Series Hardware Users Guide*.

User Documentation on CD

The CD that accompanies this *Getting Started Guide* contains comprehensive Alcatel user documentation, including the following manuals:

- *OmniSwitch 9000 Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 9000 up and running. Also provides information on fundamental aspects of OmniSwitch hardware components and software architecture.

- *OmniSwitch 9000 Hardware Users Guide*

  Complete technical specifications and procedures for all OmniSwitch 9000 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 9000. Includes syntax definitions, default values, examples, usage guidelines, and CLI-to-MIB variable mappings.

- *OmniSwitch 6800/6850/9000 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 6800/6850/9000 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 and IPX), security options (authenticated VLANs), Quality of Service (QoS), link aggregation, and server load balancing.

- *OmniSwitch 6800/6850/9000 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. Chapters cover multicast routing (DVMRP and PIM-SM) and OSPF.

General Information

To load the CD and access the user documentation, refer to the instructions printed on the CD packaging.

All documentation is in PDF format and requires the Adobe Acrobat Reader program for viewing. Acrobat Reader freeware is available at www.adobe.com.

Global Search. To take advantage of the documentation CD's global search feature, it is recommended that you select the option for *searching PDF files* when downloading Acrobat Reader freeware from the Adobe Web site.

To verify that you are using Acrobat Reader with the global search option, look for the following button on the toolbar:

If you cannot locate a button with the document image behind the binoculars (as shown), then the global search feature is *not*

available in the version of Acrobat Reader you are currently using.

Printing PDFs. While printing pages from the documentation PDFs, de-select Fit to Page if it is selected in your print dialog. Otherwise, pages with slightly smaller margins will be printed.