Platform Guide: 1500, 3400, 6400, and 6800

MAN-0183-00

Product Version

This manual applies to hardware platforms 1500, 3400, 6400, and 6800 created by F5 Networks, Inc.

Publication Date

This guide was published on August 16, 2006.

Legal Notices

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

VCCI Class A Compliance

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take corrective actions. VCCI-A

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with "386BSD" and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to "NetBSD," "FreeBSD," "Mach" (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

Table of Contents

6
Configuring and Maintaining a FIPS Security Domain

7
Working with Environmental Guidelines for the IP Application Switch Platform

8
Reviewing Hardware Specifications

Glossary

Index

1

Introducing the IP Application Switch Platform

- Working with the IP Application Switch platform
- Getting started
- Familiarizing yourself with the IP Application Switch
- About this guide
- Finding help and technical support resources

Working with the IP Application Switch platform

The IP Application Switch™ platforms are powerful systems capable of managing traffic for any size of enterprise.

Externally, the IP Application Switch platforms look similar. However, there are internal differences and some minor external differences.

- **1500 platform**
  This platform is designed for the best performance at the price. This switch can manage all the capabilities of F5 Networks traffic management software. The 1500 platform (Figure 1.1) provides the power of two SFP GBICs (LC connector type) and four (10/100/1000) interfaces, with SSL processing available as an additional add-on through the software license.
- **3400 platform**
  The 3400 platform is available with two SFP GBICs (LC connector type) and eight (10/100/1000) interfaces (Figure 1.2).
- **6400 and 6800 platforms**
  The 6400 and 6800 platforms are available with four SFP GBICs (LC connector type and sixteen (10/100/1000) interfaces (Figure 1.3).

WARNING

Only optics modules provided by F5 Networks are supported in this platform.

For detailed specifications of each platform, see *Reviewing hardware specifications*, on page 8-1.

Figure 1.1 *This is an external view of the 1500 platform*

Figure 1.2 *This is an external view of the 3400 platform*

Figure 1.3 *This is an external view of the 6400 or 6800 platform*

Getting started

There are several basic tasks you must complete to get the IP Application Switch platform installed and set up.

- Review the hardware requirements. For more information about the hardware requirements, read the following sections, *Components provided with the IP Application Switch*, and *Peripheral hardware that you provide*.
- Understand the environmental guidelines. For more information, see *Environmental requirements*, on page 7-1.
- Familiarize yourself with the IP Application Switch hardware. For more information, see *Familiarizing yourself with the IP Application Switch*, on page 1-6.

- Connect the IP Application Switch to the network, and optionally connect the peripheral hardware. For more information on mounting the hardware and attaching cables, see *Installing and connecting the hardware*, on page 2-1.

The IP Application Switch comes with the hardware that you need for installation. However, you must also provide standard peripheral hardware, such as a serial terminal, if you want to administer the IP Application Switch directly.

Components provided with the IP Application Switch

When you unpack the IP Application Switch, you should make sure that the following components, shown in Figure 1.4, are included:

- One power cable
- One serial fail-over cable
- Four rack-mounting screws

The power cable included with this unit is for exclusive use with this unit and should not be used with other electrical appliances.

If you purchased a hardware-based redundant system, you also received one fail-over cable to connect the two IP Application Switch units together (network-based redundant systems do not require a fail-over cable).

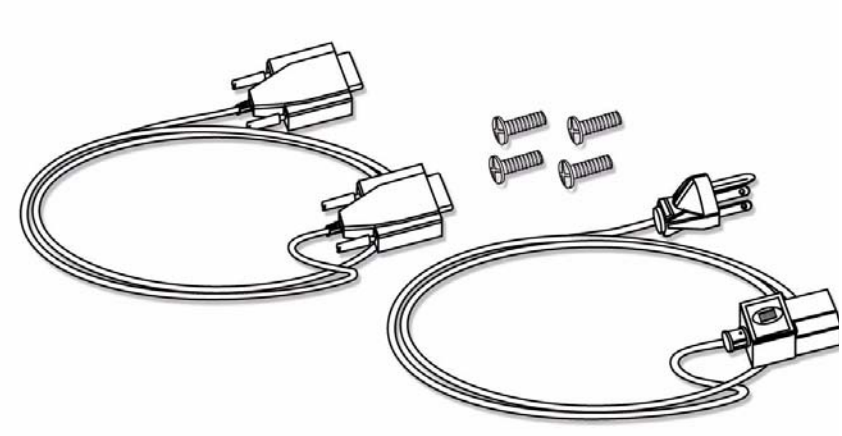


Figure 1.4 *Components included with the IP Application Switch*

Peripheral hardware that you provide

For each IP Application Switch in the system, you need to provide the following peripheral hardware:

- If you plan to use direct administrative access to the IP Application Switch, you need standard input/output hardware. This requires a serial terminal and a null modem cable.
- If you want to use the default IP Application Switch configuration, you must have an administrative workstation on the same IP network as the IP Application Switch.
- You also need network hubs, switches, or concentrators to connect to the IP Application Switch network interfaces. The devices you select must be compatible with the network interface cards installed in the IP Application Switch. The devices can support 10/100 Ethernet or Gigabit Ethernet.
  - Ethernet requires either a 10 Mbps or 100 Mbps hub or switch.

    - Gigabit Ethernet requires a compatible Gigabit Ethernet switch.

- You can use a USB drive compatible with the system for installing upgrades and for system recovery. You can perform an upgrade or system recovery with almost any non-CDRW USB drive. Even though most USB CD-ROMS should work, we cannot guarantee compatibility with all makes and models.

If you plan on doing remote administration from your own PC workstation as most users do, we recommend that you have your workstation already in place on the same subnet to which the management interface is connected.

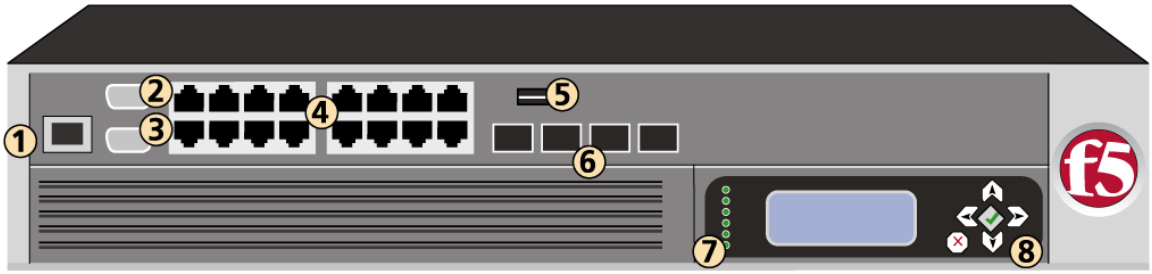
Familiarizing yourself with the IP Application Switch

The IP Application Switch comes in several different hardware configurations. Before you begin to install the IP Application Switch, you may want to quickly review the following figures that illustrate the controls and ports on both the front and the back of an IP Application Switch.

Using the IP Application Switch hardware

You need to be familiar with both the front and back layout of an IP Application Switch. Figure 1.5 illustrates the front of a 6400 or 6800 series IP Application Switch. Figure 1.6 illustrates the front view of the 1500 series. The front of the 3400 platform is very similar to the front of the 1500 series. On the front of the unit, you can turn the unit off and on, or you can reset the unit. You can also view the indicator lights for hard disk access.

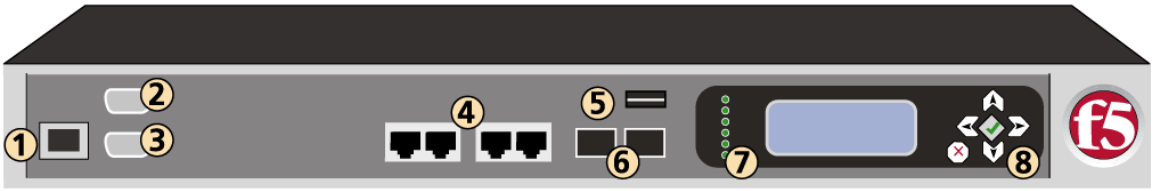
The interfaces on every IP Application Switch are labeled, so it should be clear what each port is, no matter which hardware configuration you have purchased.



1. Management interface
2. Console port
3. Hard-wired fail-over port
4. 10/100/1000 interfaces
5. USB port
6. SFP Gbics
7. Status LEDs
8. LCD control buttons

Figure 1.5 *Front view of a 6400/6800 series IP Application Switch*

Figure 1.6 illustrates the front of the 1500 platform. The front of the 3400 platform is very similar to the front of the 1500 platform.

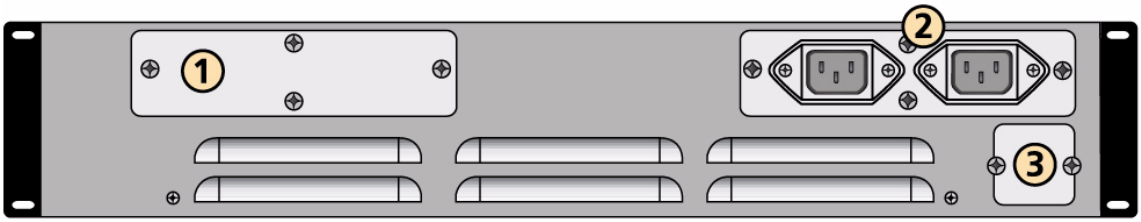


1. Management interface
2. Console port
3. Hard-wired fail-over port
4. 10/100/1000 interfaces
5. USB port
6. SFP Gbics
7. Status LEDs
8. LCD control buttons

Figure 1.6 *Front view of the 1500 series IP Application Switch*

If you have physical access to the unit, you can use the front-panel LEDs to assess the condition of the unit. For details about the behavior of the LEDs, see *Understanding LED behavior*, on page 4-1.

Figure 1.7, following, illustrates the back of a IP Application Switch. Note that all ports are labeled.



1. Unused bay
2. Power input panel
   Power 1 (right receptacle)
   Power 2 (left receptacle, optional)
3. Access panel

Figure 1.7 *Back view of the 2U IP Application Switch*

About this guide

This guide describes the features of the 1500, 3400, 6400, and 6800 IP Application Switch platforms. This guide contains the following information about these platforms.

- **Installing the hardware**
  You can learn how to install the hardware in a rack.
- **Understanding the ports and interfaces**
  You can understand the intended use of the ports and interfaces on each platform.
- **Using the LCD panel**
  You can learn how to understand and use the LCD panel.
- **Understanding LED behavior**
  You can learn how to decipher what conditions are signaled by the LEDs.
- **Replacing a fan tray and filter**
  You can learn how to replace a fan tray and filter.
- **Understanding the environmental guidelines**
  This chapter includes detailed environmental guidelines for each platform.
- **Learning the hardware specifications**
  This chapter provides details about the hardware specifications for each platform.

Additional information

In addition to this guide, there are other sources of the documentation you can use in order to work with the BIG-IP system. The information is organized into the guides and documents described below. The following printed documentation is included with the BIG-IP system.

- **Configuration Worksheet**
  This worksheet provides you with a place to plan the basic configuration for the BIG-IP system.
- **BIG-IP Quick Start Instructions**
  This pamphlet provides you with the basic configuration steps required to get the BIG-IP system up and running in the network.

The following guides are available in PDF format from the CD-ROM provided with the BIG-IP system. These guides are also available from the first Web page you see when you log in to the administrative web server on the BIG-IP system.

- **Installation, Licensing, and Upgrades for BIG-IP Systems**
  This guide provides detailed information about installing upgrades to the BIG-IP system. It also provides information about licensing the BIG-IP system software and connecting the system to a management workstation or network.

- **Configuration Guide for Local Traffic Management**
  This guide contains any information you need for configuring the BIG-IP system to manage local network traffic. With this guide, you can perform tasks such as creating virtual servers and load balancing pools, configuring application and persistence profiles, implementing health monitors, and setting up remote authentication.
- **Network and System Management Guide**
  This guide contains any information you need to configure and maintain the network and system-related components of the BIG-IP system. With this guide, you can perform tasks such as configuring VLANs, assigning self IP addresses, creating administrative user accounts, and managing a redundant system.

Stylistic conventions

To help you easily identify and understand important information, our documentation uses the stylistic conventions described below.

Using the solution examples

All examples in this documentation use only private class IP addresses. When you set up the solutions we describe, you must use valid IP addresses suitable to your own network in place of our sample addresses.

Identifying new terms

To help you identify sections where a term is defined, the term itself is shown in bold italic text. For example, a ***virtual server*** is a specific combination of a virtual address and virtual port, associated with a content site that is managed by a BIG-IP system or other type of host server.

Identifying references to objects, names, and commands

We apply bold text to a variety of items to help you easily pick them out of a block of text. These items include web addresses, IP addresses, utility names, and portions of commands, such as variables and keywords. For example, with the **bigpipe pool <pool_name> show** command, you can specify a specific pool to show by specifying a pool name for the **<pool_name>** variable.

Identifying references to other documents

We use italic text to denote a reference to another document. In references where we provide the name of a book as well as a specific chapter or section in the book, we show the book name in bold, italic text, and the chapter/section name in italic text to help quickly differentiate the two.

Identifying command syntax

We show complete commands in bold Courier text. Note that we do not include the corresponding screen prompt, unless the command is shown in a figure that depicts an entire command line screen. For example, the following command shows the configuration of the specified pool name:

```
bigpipe pool <pool_name> show
```

or

```
b pool <pool_name> show
```

Table 1.1 explains additional special conventions used in command line syntax.

Item in text	Description
****	Indicates that the command continues on the following line, and that users should type the entire command without typing a line break.
< >	Identifies a user-defined parameter. For example, if the command has **<your name>**, type in your name, but do not include the brackets.
|	Separates parts of a command.
[ ]	Indicates that syntax inside the brackets is optional.
...	Indicates that you can type a series of items.
::=	Means **is defined as**. Indicates that an argument is followed by the description of the elements that you can use for the argument.

Table 1.1 *Command line syntax conventions*

Finding help and technical support resources

You can find additional technical documentation and product information in the following locations:

- **Online help for local traffic management**
  The Configuration utility has online help for each screen. The online help contains descriptions of each control and setting on the screen. Click the Help tab in the left navigation pane to view the online help for a screen.
- **Welcome screen in the Configuration utility**
  The Welcome screen in the Configuration utility contains links to many useful web sites and resources, including:
  - The F5 Networks Technical Support web site
  - The F5 Solution Center
  - The F5 DevCentral web site
  - Plug-ins, SNMP MIBs, and SSH clients
- **F5 Networks Technical Support web site**
  The F5 Networks Technical Support web site, **http://tech.f5.com**, provides the latest documentation for the product, including:
  - Release notes for the BIG-IP system, current and past
  - Updates for guides (in PDF form)
  - Technical notes
  - Answers to frequently asked questions
  - The Ask F5 natural language question and answer engine.

  To access this site, you need to register at **http://tech.f5.com**.

2

Installing the IP Application Switch Platform

- Installing and connecting the hardware

Installing and connecting the hardware

After you have reviewed the hardware requirements and become familiar with the IP Application switch, as described in *Getting started*, on page 1-2, you can install the unit.

There are two basic tasks required to install the hardware. You simply need to install the IP Application Switch in a rack, and then connect the peripheral hardware and the interfaces.

General recommendations for mounting a unit in a rack

We recommend that all units have 1U spacing between them when mounted in a rack to allow for a rack mounting shelf, and to provide additional air circulation for cooling the unit.

Although not required, a 1U space between units makes it easier for you to remove the unit from the rack in the event that the unit requires service. A 1U space between units also provides additional cable routing options.

We recommend 100mm spacing from the front panel of the unit to the rack front or rack door. This provides enough room for you to route the cables without bending them excessively.

WARNING

This product is sensitive to electrostatic discharge (ESD). We recommend that when you install or maintain the unit, you use proper ESD grounding procedures and equipment.

WARNING

Do not turn on an IP Application Switch until the management serial console and/or the management network is connected to the unit.

A shelf or similar device is required to support the unit if a single person is installing the unit. To prevent personal injury or damage to the unit, we recommend that at least two people perform the installation.

To install the hardware in a rack

1. Lift the unit into place.
2. Secure the unit using the four rack-mounting screws that are provided.
   The unit must be securely fastened to the rack to provide adequate stability and to prevent the unit from falling out of the rack.
   Securing the rack with the screws also provides adequate grounding.

If the rack you have does not provide adequate support for the unit, you may need a shelf kit. We recommend that you use a shelf kit created by the rack manufacturer. For example, some rack manufacturers provide shelf kits for their racks.

Figure 2.1 shows the orientation of the IP Application Switch and the mounting screws for installation in a standard 19" rack. Figure 2.2 shows the IP Application Switch installed in the rack.

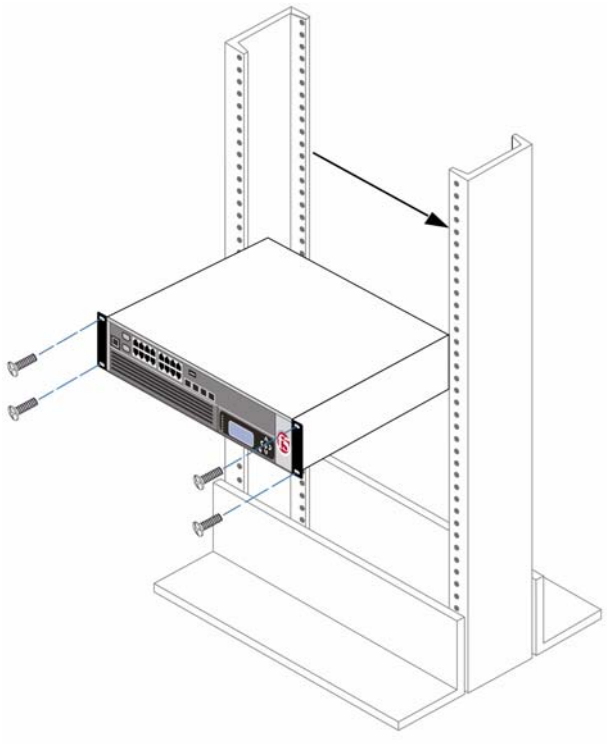


Figure 2.1 *Platform orientation for rack mounting*

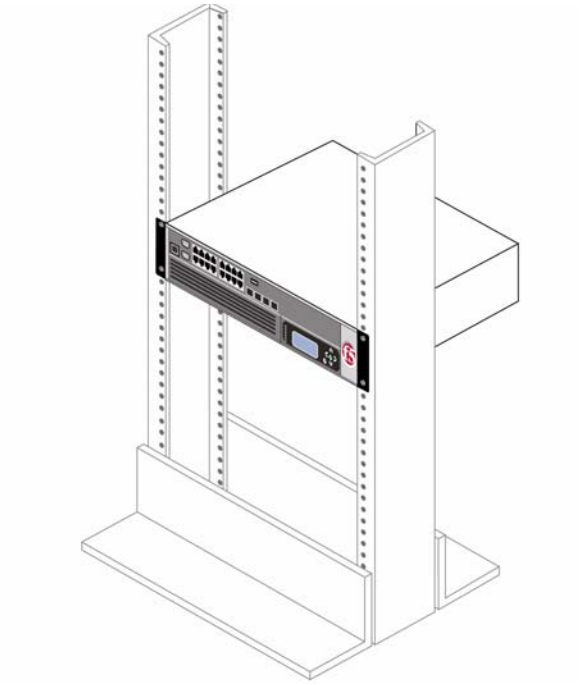


Figure 2.2 *Platform installed in a 19" rack*

To connect the cables and hardware for input/output

1. Connect the hardware that you have chosen to use for input/output. For details about connecting the system to a management workstation or network, see Chapter 2, *Connecting a Management Workstation or Network*, in ***Installation, Licensing, and Upgrades for BIG-IP Systems***.
   - If you are using a serial terminal as the console, connect the serial cable supplied by F5 Networks to the console port (number 2 in Figure 1.5, on page 1-6).
   - If you are using an Ethernet connection, connect a management workstation to the management interface (number 1 in Figure 1.5, on page 1-6).
2. If you have a hardware-based redundant system, connect the fail-over cable to the fail-over port on each unit (number 3 in Figure 1.5, on page 1-6).
3. Connect the power cable to the power input panel (number 2 in Figure 1.7, on page 1-8), and then connect it to the power source.
4. Turn on the unit and begin licensing the system. For details about licensing the BIG-IP system, see Chapter 3, *Licensing and Configuring the BIG-IP System*, in ***Installation, Licensing, and Upgrades for BIG-IP Systems***.

3

Operating the LCD Panel

- Introducing the LCD panel
- Using the LCD panel
- Navigating through the LCD menus

Introducing the LCD panel

The liquid crystal display, or LCD panel, provides the ability to control the unit without attaching a serial or network cable. The following menus are available on the LCD panel.

- **Information menu**
  Use the Information menu to find information about using the LCD and its functionality.
- **System menu**
  Use the System menu to reboot, netboot, or halt the unit. This menu also has options for setting the properties of the management interface (MGMT) and the serial port
- **Screens menu**
  Use the Screens menu to set up the informational screens you would like the LCD to cycle through. The information screens include system status, statistics, and system alerts.
- **Options menu**
  Use the Options menu to configure the properties of the LCD panel.

This chapter describes how to use the LCD panel and its menus. It does not describe each function available in each menu.

Figure 3.1 *An example of the LCD panel and control buttons*

Using the LCD panel

You can configure the LCD panel to meet your needs. The following section describes how to perform a number of tasks with the LCD panel:

- Pause on a screen
- Use the LCD menus
- Power up the unit
- Halt the unit
- Power down the unit
- Reboot the unit

Pausing on a screen

Normally, the screens cycle on the LCD at a constant rate. However, push the Check button to toggle the LCD between Hold and Rotate modes. In Hold mode, a single screen is displayed. The Rotate mode changes the screen displayed on the LCD every 4 seconds.

Using LCD menus

Pressing the **X** button puts the LCD panel in Menu mode. The buttons Left Arrow, Right Arrow, Up Arrow, and Down Arrow are only functional when the LCD is in Menu mode.

Powering up the unit

When you want to power on a unit that is shut down, press the Check button to turn the power on.

Halting the unit

We recommend you halt the unit before you power it down or reboot it using the LCD menu options.

To halt the unit

1. Press the **X** button, then use the arrow keys to navigate to the System menu.
2. Press the Check button. Navigate to the Halt menu.
3. Press the Check button. Press the Check button again at the confirmation screen.
4. Wait 30 seconds before powering the machine off or rebooting it.

Powering down the unit

Hold the **X** button for 4 seconds to power down the unit. We recommend that you halt the system before you power down the system in this manner.

Rebooting the unit

Hold the Check button for 4 seconds to reboot the unit. You should only use this option after you halt the unit.

Clearing alerts

Press the Check button to clear any alerts on the LCD screen. You must clear any alerts on the screen before you can use the LCD.

Navigating through the LCD menus

To use the LCD menus, you must first put the LCD in Menu mode. To put the LCD in menu mode, press the **X** button.

After you put the LCD in menu mode, use the Left Arrow, Right Arrow, Up Arrow, and Down Arrow buttons to select menu options. There are four menu options:

- Information
- System
- Screens
- Options

The following tables describe each LCD menu option.

Information menu

You can use the Information menu to access help pages about using the LCD panel functionality. You can also find more information on what different LED activity means and the failover state of the unit in a redundant system. The following table, Table 3.1, shows the options available on the Information menu.

Option	Description
How to use the LCD	Displays a vertical scrolling text description on how to use the LCD panel.
Front Panel LEDs	Displays a vertical scrolling text description of what the front panel LEDs mean.
Port Indicators	Displays a vertical scrolling text description of what the lights above the ports mean.
Console and Failover serial port information	Displays a vertical scrolling text description of the console and failover serial ports.

Table 3.1 *The Information menu*

System menu

The System menu provides various options for rebooting, halting, or netbooting the hardware. This menu also provides options for configuring the network on the management interface. The following table, Table 3.2, lists the options available in the System menu.

Option	Description
Reboot	Select this option to reboot the unit.
Halt	Select this option to halt the unit.
Netboot	Select this option if you are installing software from a PXE server.
IP address	Type the management interface IP address. You can use only an IPv4 address.
Netmask	Set the netmask for the management interface IP address.
Default route	Type in the default route for the management interface. This route is necessary if you plan to manage the unit from a different subnetwork.
Commit	Select this option to commit your changes.
Serial port	Use this option to change the baud rate of the serial port. The following options are available: 9600 19200 38400 115200

Table 3.2 *The System menu*

Screens menu

You can use the Screens menu options to view various statistics and information about the system. The following table, Table 3.3, lists all the general information screens. You can use the Check button to place a check mark next to the name of the screens you would like to appear when the screens cycle.

Option	Description
VersionScreen (Version screen)	Displays the product version information.
InfoScreen (Information screen)	Displays the information screen menu.
DateScreen (Date and Time screen)	Displays the date and time.
MACscreen (MAC addresses screen)	Displays the MAC addresses on the unit.
SysinfoScreen (System information screen)	Displays system information.
TMMCPUScreen (CPU usage)	Displays the CPU usage percentage.
TMMMemoryScreen (Memory usage)	Displays the memory usage.
TMMAuthScreen (Auth requests)	Displays the number of authentication requests being processed.
TMMStatScreen (Statistics)	Displays simple statistics, such as bytes and packets in and out of the system.

Table 3.3 *The general screen information menu*

Options menu

You can use the Options menu to adjust the display properties of the LCD panel. The following table, Table 3.4, lists the options available on the Options menu.

Option	Description
Heartbeat	Use the Check button to turn on (checked) or off (unchecked) the heartbeat displayed on the LCD screen. This heartbeat displays if the SCCP is running on the system. This heartbeat does not affect the failover mechanism of the system.
Contrast	Use the Left and Right arrow keys on the LCD to set the contrast of the LCD.
On Brightness	This setting provides the ability to adjust the LCD backlight brightness.
Off Brightness	This setting controls the brightness of the LCD panel when the backlight is off. Use the Left and Right arrow keys to set the brightness of the LCD panel.

Table 3.4 *The Options menu*

4

Using Additional IP Application Switch Functionality

- Understanding LED behavior
- Working with interfaces
- Hardware acceleration

Understanding LED behavior

This section describes the LED behavior of the BIG-IP software, version 9.0 and later, on BIG-IP 1000, 2400, and 5100 platforms and the BIG-IP 1500, 3400, 6400, and 6800 platforms

Important

Installing BIG-IP version 9.0 on the 1000, 2400, and 5100 platforms changes the way the front-panel LEDs work on these systems. The LEDs do not function in the manner described in the BIG-IP version 4.x documentation. After you install BIG-IP version 9.0, these systems will function in the manner described in this document.

LED indicator actions

The behavior, or action, of each of LED indicates the status of the system. The LED indicator actions are defined in Table 4.1.

Action	Description
Off (none)	The LED is not lit and does not display any color.
Solid	The LED is lit and does not blink.
Blinking	The LED turns on and off at a regular frequency.
Intermittent	The LED turns on and off with an irregular frequency and may sometimes appear solid.

Table 4.1 *LED indicator actions*

Standard operating states

When the unit is in a standard operating state, the LEDs behave in a defined manner. The standard operating states are defined in Table 4.2.

System State	Alarm LED	Activity LED	Status LED
Power is off	off/none	off/none	off/none
Standby mode	off/none	green or yellow intermittent	yellow solid
Active mode	off/none	green or yellow intermittent	green solid

Table 4.2 *Standard operating states of the LEDs*

Alert conditions indicated by the Alarm LED

When there is an alert condition on the unit, the Alarm LED behaves in a specific manner.

System Situation	Alarm LED behavior
Emergency	The LED blinks red.
Alert or Critical	The LED is lit red.
Error	The LED is blinks yellow.
Warning	The LED is lit yellow.

Table 4.3 *LED indicator functions*

Alerts that cause the indicators to change are defined in the **/etc/alertd/alert.conf** and **/config/user_alert.conf** files on the BIG-IP system. You should only edit **/config/user_alert.conf** to add new alerts. The **/etc/alertd/alert.conf** defines standard system alerts.

To configure LED indicators to display node status

1. Display a command-line prompt on the BIG-IP system.
2. Type the following command:
   ```
   cd /config
   ```
3. Using a text editor, such as **vi** or **pico**, open the file **user_alert.conf**.
4. Add the lines shown in Figure 4.1 to the end of the file.
5. Save the file and exit the text editor.
   The front panel LEDs now indicate when nodes are marked down

.

```
alert BIGIP_MCPD_MCPDERR_POOL_MEMBER_MON_DOWN "Pool member (.*?):(.*?) monitor status
down." {
        snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.10";
                    lcdwarn description="Node down"  priority="1"
}
alert BIGIP_MCPD_MCPDERR_NODE_ADDRESS_MON_DOWN "Node (.*?) monitor status down." {
         snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.12";
                     lcdwarn description="Node address down"  priority="1"
}
alert BIGIP_MCPD_MCPDERR_POOL_MEMBER_MON_UP "Pool member (.*?):(.*?) monitor status
up." {
         snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.11"
}
alert BIGIP_MCPD_MCPDERR_NODE_ADDRESS_MON_UP "Node (.*?) monitor status up." {
         snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.13"
}
```

Figure 4.1 *The user_alert.conf file*

Specific status indicated by the LEDs

This section includes some specific conditions that are not covered in the definition tables in the **/etc/alertd/alert.conf**. These conditions include:

- Yellow intermittent Activity LED indicator
- Green intermittent Activity LED indicator
- Green solid Status LED indicator

Yellow intermittent Activity LED indicator

A yellow intermittent Activity LED indicates that host traffic is present. Also, while the kernel is loading, the Activity LED indicator flashes yellow intermittently when the disk is accessed. This condition is normal and occurs only during boot up.

Green intermittent Activity LED indicator

When the Activity LED indicator flashes green intermittently, it indicates Ethernet traffic leaving the switch subsystem and going to the CPU subsystem. Because internal traffic may cause this indicator to be active, you may see the Activity indicator flicker green even though there is no external client/server traffic.

Green solid Status LED indicator

When the Status LED indicator is solid yellow or green, it indicates that the BIG-IP unit is in a Standby state (yellow) or an Active state (green).

Working with interfaces

You can perform configuration tasks such as displaying interface status and settings, setting the media type, and setting the duplex mode using the **bigpipe** command.

When using **bigpipe**, and a command calls for a list of interfaces, the list may consist of one or more interfaces, with multiple interfaces separated by spaces. For example:

```
1.1 1.2 2.1 2.2
```

Displaying status and settings for interfaces

From the command line interface, use the following syntax to display the current status and the settings for all installed interfaces:

```
b interface show
```

Figure 4.2 shows an example of the output you see when you issue this command on an active/standby unit in active mode.

```
interface  speed   pkts   pkts   pkts   pkts   bits   bits errors trunk STP
             Mb/s     in    out   drop   coll     in    out
  1.1 UP  100 HD      0    213      0      0      0  74.2K      0
  1.2 UP  100 HD     20     25      0      0  28.6K  33.9K      0
```

Figure 4.2 *The **bigpipe interface show** command output*

Use the following syntax to display the current status and the setting for a specific interface:

```
b interface <if_name> show
```

Media type and duplex mode

Properties that you can configure on the interfaces include media type and duplex mode, as shown in Table 4.4.

Interface Properties	Description	Default
media	You may specify a media type or use **auto** for automatic detection.	auto
duplex	Use **auto** for automatic selection.	auto

Table 4.4 *Attributes you can configure for an interface*

Setting the media type

All interfaces on the BIG-IP system default to auto-negotiate speed and duplex settings. We recommend that you configure any network equipment that you plan to use with the BIG-IP system to auto-negotiate speed and duplex settings. If you connect the BIG-IP system to network devices with forced speed and duplex settings, you must force the speed and duplex settings of the BIG-IP system to match the settings of the other network device.

WARNING

If the BIG-IP system is attempting to auto-negotiate interface settings with an interface that has the speed and duplex settings forced, you will experience severe performance degredation.

Use the following syntax to set the media type:

```
b interface <if name list> media <media type> | auto
```

The valid media types for this command are:

- 10baseT <duplex>
- 100baseTX <duplex>
- 1000baseFX full
- 1000baseT <duplex>
- 1000baseSX full
- 1000baseLX full |
- 10GbaseSR full
- 10GbaseLR full |
- 10GbaseER full | auto

To view the valid media types for an interface, type the following command:

```
b interface <if name list> media show
```

Important

In all Gigabit Ethernet modes, the only valid duplex mode is full duplex.

Setting the duplex mode

You can set duplex mode to full or half duplex. If the media type does not accept the duplex mode setting, an onscreen message indicates this. If media type is set to **auto**, or if the interface does not accept the duplex mode setting, the duplex setting is not saved to **/config/bigip_base.conf**.

Use the following syntax to set the duplex mode:

```
b interface <if_name> duplex  full | half
```

Hardware acceleration

The Packet Velocity ASIC® 2 optimizes application performance, and reduces application wait times. An ***ASIC*** is an Application Specific Integrated Circuit. The Packet Velocity ASIC is designed to accelerate Layer 4 decisions. Off-loading the Layer 4 decisions enables the BIG-IP system to increase performance and throughput for basic routing functions (Layer 4) and application switching (Layer 7).

5

Changing the Fan Tray and Filter

- Changing the fan tray and filter

Changing the fan tray and filter

The 6400 and 6800 series platforms have a removable fan tray and filter. You can change or replace the fan tray and filter as part of the routine maintenance of the unit, or in the event of a fan failure. The air filter in the BIG-IP unit is designed to remove airborne contaminants and requires replacement during the life of the product. The fans in the fan tray run constantly while the unit is on. Over time, the fans will wear out, requiring you to replace the fan tray.

Note

We recommend that you inspect the fan tray and filter every four months. Replace the fan tray if any of the fans are not functional. Replace the filter when you replace the fan tray.

Replacing the fan tray and filter

You do not need special tools to replace the fan tray and filter. You can perform this maintenance while the unit is running.

However, we recommend that you perform the fan tray and filter replacement only on the standby unit in a redundant system while the unit is powered down. After you install the fan tray and filter in the standby system, power up the unit, then force the active system to fail over and install the fan tray and filter replacement in the other unit of the redundant system.

To replace the fan tray and filter

1. Start by opening the front panel of the BIG-IP unit running in standby mode.
2. The fan tray is held on the chassis by a knurled fastener. Loosen the knurled fastener by turning it counter-clockwise.
3. Pull the old fan tray and filter out of the system.
4. Slide the new fan tray and filter into the fan tray and filter slot. The tray is automatically turned on when you slide the tray completely into the chassis.
5. Tighten the knurled fastener into place by turning it clockwise.
6. Close the front panel of the unit.

WARNING

You should not leave the unit running longer than 90 seconds without the fan tray installed.

Figure 5.1 *The removable fan and filter tray*

Figure 5.1 shows an example of the fan and filter tray assembly partially removed from a BIG-IP system (your hardware may appear slightly different). You can also replace the filter without replacing the fan tray. This requires you to remove the fan tray, and take out the old filter, and insert a new one.

To replace the filter only

1. Start by opening the front panel of the BIG-IP unit running in standby mode.
2. The fan tray is held on the chassis by a knurled fastener. Loosen the knurled fastener by turning it counter-clockwise.
3. Pull the old fan tray and filter out of the system.
4. Slide the old filter out of the fan tray filter slot. Slide the new filter into the filter slot.
5. Push the fan tray and filter back into the system.
   The tray is automatically turned on when you slide the tray completely into the chassis.
6. Tighten the knurled fastener into place by turning it clockwise.

Close the front panel of the unit.

6

Configuring and Maintaining a FIPS Security Domain

- Understanding the FIPS implementation
- Installing the BIG-IP systems and connecting a serial console
- Creating the FIPS security domain
- Running the Configuration utility
- Running the fipscardsync utility to synchronize the FIPS HSMs
- Generating and managing FIPS keys
- Planning for system recovery
- Recovering FIPS information after a system failure

Understanding the FIPS implementation

The BIG-IP® system includes the option to install a FIPS hardware security module (HSM). Currently, the FIPS HSM is available in the BIG-IP 6400 and 6800 platforms. With this release, the HSM and the BIG-IP key management software provide FIPS-140 level 2 support. This level of support provides the following security benefits.

- Keys are stored in the HSM where they are protected from physical and software attacks.
- Keys can never be extracted in plain text format.

This chapter describes how to configure a redundant system from the factory with one FIPS HSM installed in each unit. To implement a FIPS solution in a BIG-IP redundant system, you must perform the following tasks.

- Install the BIG-IP systems and connect a serial console.
- Create the FIPS security domain from the console.
- Run the Configuration utility.
- Run the **fipscardsync** utility to synchronize the FIPS HSMs from the console.

Some of these tasks are described in other documents. When a section in this document has tasks described in other documents, it contains links or pointers to the related documentation.

Installing the BIG-IP systems and connecting a serial console

The first two tasks that you need to complete when setting up a FIPS configuration on a redundant system are to install the systems and connect a serial console. For details about performing these tasks, refer to the following documentation:

- For details about installing the hardware, in this guide see the *Installing and connecting the hardware*, on page 2-1.
- For information on connecting a serial console, see ***Installation, Licensing, and Upgrading for BIG-IP Systems***, Chapter 2, *Connecting a Management Workstation or Network*.

After the systems are set up, and you have configured a serial console, you can create the FIPS security domain.

Creating the FIPS security domain

The first task in creating a FIPS security domain is to initialize the FIPS HSM and create a security officer (SO) password. The SO password is required to re-initialize the HSM. When you are configuring a redundant system, you need to initialize the security domain on one unit, and then initialize the card on the peer unit using the same security domain name you used on the first unit.

To create a FIPS security domain, you must perform the following tasks:

- Initialize the first unit in the redundant system.
- Initialize the peer system.

Note

You can initialize the FIPS HSM and create the security domain before you license the system and create a traffic management configuration.

Initializing the first unit in a redundant system

To initialize the first unit in a redundant system and create a security domain, you must use the **fipsutil** utility. To initialize the HSM and create an SO password, type the following command:

```
fipsutil -f init
```

After the utility starts, you are prompted to create a security officer password, and then confirm the password. After you create a password and confirm it, you are prompted for the security domain name. Remember the security domain name you use. You need the domain name when you initialize the HSM on the peer unit. The domain name cannot be extracted or displayed by the software or hardware once you use it.

After you complete the initialization process on the first unit, you can initialize the peer system.

Initializing the peer system

To initialize the peer unit in the redundant system and add it to the security domain of the first unit, you must use the **fipsutil** utility. Type the following command:

```
fipsutil -f init
```

After the utility starts, you are prompted to create a security officer (SO) password. You can use the SO password that you created on the first unit; however, you are not required to use it.

When you are prompted for the security domain name, you must type the security domain name you created on the first unit.

After you initialize the HSMs in both units, you can log into each unit and run the Configuration utility.

Running the Configuration utility

After you complete the initialization of the HSMs and create a security domain on the redundant system, you need to run the Configuration utility.

The Configuration utility provides the ability to license the system, configure the management interface, configure failover, and create a base network configuration. After you configure failover properly, and after you have run the **fipscardsync** utility you are synchronizing card and key information for the security domain every time you synchronize the configuration of the redundant system. The following section describes how to run the **fipscardsync** utility.

For details about running the Configuration utility and creating a base network configuration, see the ***BIG-IP Quick Start Instructions***. These instructions are included in the BIG-IP Resource Kit shipped with each unit. You can also access these instructions at **http://tech.f5.com**.

Running the fipscardsync utility to synchronize the FIPS HSMs

After you set up the system with the Configuration utility, you can synchronize the FIPS HSMs with the **fipscardsync** utility. Synchronizing the HSMs provides the ability to exchange keys. To run the **fipscardsync** utility, type the following command at the console.

```
fipscardsync peer
```

After you synchronize the HSMs, you can create a traffic management configuration.

The remainder of this chapter describes additional FIPS system maintenance tasks, including:

- Generating and managing FIPS keys
- Planning for system recovery
- Recovering FIPS information after a system failure

Generating and managing FIPS keys

The web-based Configuration utility provides a key management interface. You can use the Configuration utility to create FIPS keys, convert existing keys to FIPS keys, and import existing keys into the system.

◆ Note

Once a key is converted to FIPS, the process cannot be reversed.

To create FIPS keys using the Configuration utility

1. On the Main tab of the navigation pane, expand **Local Traffic**, and click **SSL Certificates**.
   This opens the SSL Certificates screen which lists all certificates installed on the LTM system.
2. On the upper-right portion of the screen, click **Create**.
   The New SSL Certificates screen opens.
3. In the **Name** box, type a unique name for the certificate.
4. Using the **Issuer** setting, specify the type of certificate you want to use:
   - For a self-signed certificate, select **Self**.
   - To request a certificate from a CA, select **Certificate Authority**.
5. Configure the **Common Name** setting, and any other settings you want.
6. In the Key Properties section, select the security type **FIPS**, and a key size.
7. Click **Finished**.

To convert existing keys using the Configuration utility

1. On the Main tab of the navigation pane, expand **Local Traffic** and click **SSL Certificates**.
   This opens the SSL Certificates screen which lists all certificates installed on the LTM system.
2. Click a certificate name.
   This displays the properties of that certificate.
3. If you want to see information about the key that is associated with that certificate, click **Key** on the menu bar.
   This displays the type and size of the key.
4. To convert the key to a FIPS key, click the **Convert to FIPS** button.
   The key is converted. Once the key is converted, this process cannot be reversed.

To import existing keys using the Configuration utility

1. On the Main tab of the navigation pane, expand **Local Traffic** and click **SSL Certificates**.
   This displays the list of existing certificates.
2. In the upper right corner of the screen, click **Import**.
3. Select the type of import **Key**.
4. Select the import method (**File** or **Text**).
5. In the **Certificate** box, type the name of the key.
   You can click the **Browse** button and browse for the key and select it.
6. Click **Import**.

   After you import the key, you can convert it to FIPS using the procedure *To convert existing keys using the Configuration utility*, on page 6-4.

Planning for system recovery

There are three different ways you can plan for a system recovery.

- You can maintain a redundant system. In the event of a failure, the standby unit becomes active and handles incoming traffic.
- Another option is to configure a third unit with the same configuration, and store it in a safe place.
- A last option, that is not FIPS approved, is to copy the keys to a disk and put the disk in a safe place.

Each of these options is described, following.

Configuring a redundant system

The first option is to maintain a redundant system. In the event of a failure, the standby unit becomes active and handles the incoming traffic. This chapter describes how to create a redundant system configuration as part of the initial configuration. After you configure failover properly, every time you synchronize the configuration of the redundant system, you are synchronizing card and key information for the security domain.

Configuring an additional unit for recovery

For additional system backup, you can take a third unit, fully configure it, add it to the security domain, and synchronize the configurations. Remove the unit from the network and store it in a safe location. If the BIG-IP system in production is damaged or destroyed, you can take the backup unit from storage, and reconstitute the security domain.

Saving keys on a disk

Another possible method for preserving the keys is not FIPS-approved. With this option, you generate your keys in software. Copy the keys to a disk and put the disk in a secure place. Then you can import the keys into the FIPS HSM. If there is a catastrophic system failure, you can use these backup keys to create the security domain. This is not a FIPS-compliant method for backup.

Recovering FIPS information after a system failure

If one unit of a redundant system fails, the failover unit becomes active and maintains FIPS information. However, after you replace the failed unit in a redundant system, you need to restore FIPS information on the replacement unit.

To copy FIPS information from the currently active original system to a new replacement system

1. Ensure that current BIG-IP software is configured, and install your saved UCS on the new replacement system.
   See **http://tech.f5.com** for information on backup and recovery of a BIG-IP UCS file.
2. Connect the currently active unit to new replacement unit.
3. On the new replacement unit, run the **fipsutil -f init** command.
   Ensure that you use the exact same security domain that you specified when you initially set up the currently active unit.
4. On the currently active unit, run the **fipssync peer** command.
   This copies the information in the FIPS module from the currently active unit to the new replacement unit.

   WARNING: *Ensure that you run the* ***fipssync peer*** *command from the currently active unit. If you run the* ***fipssync peer*** *command from the new replacement unit, you will lose the original FIPS information.*
5. On the currently active unit, run **configsync** to copy the full configuration to the replacement system.
   The new replacement system is now ready to function as the failover device in a redundant pair configuration.

7

Working with Environmental Guidelines for the IP Application Switch Platform

- Environmental requirements

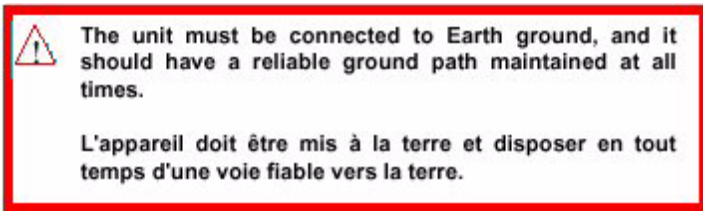
Environmental requirements

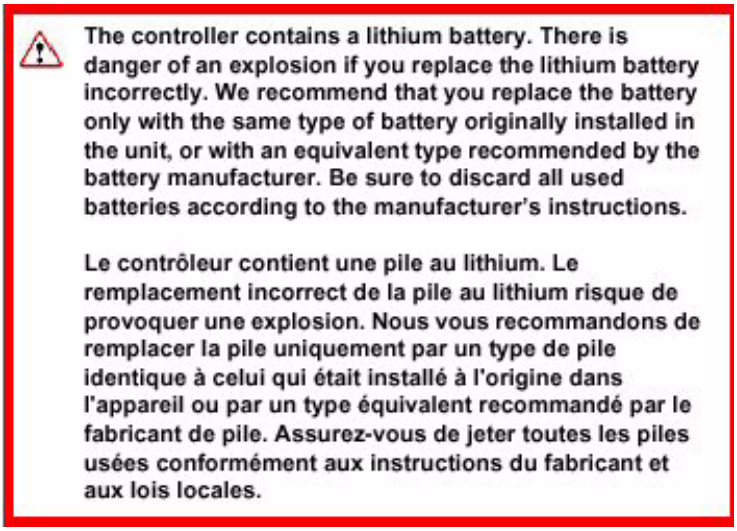
Before you install the IP Application Switch, review the following guidelines to make sure that you are installing and using the IP Application Switch in the appropriate environment.

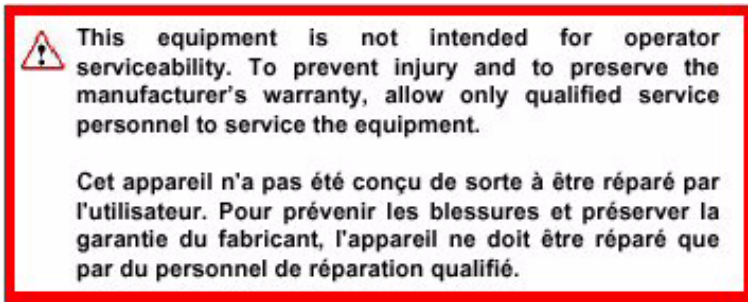
General environmental guidelines

An IP Application Switch is an industrial network appliance, designed to be mounted in a standard 19-inch rack. To ensure safe installation and operation of the unit:

- Install the rack according to the manufacturer's instructions, and check the rack for stability before placing equipment in it.
- Build and position the rack so that once you install the IP Application Switch, the power supply and the vents on both the front and back of the unit remain unobstructed. The IP Application Switch must have adequate ventilation around the unit at all times.
- Do not allow the air temperature in the room to exceed 40° C.
- Do not plug the unit into a branch circuit shared by more electronic equipment than the circuit is designed to manage safely at one time.
- This product is sensitive to electrostatic discharge (ESD). We recommend that when you install or maintain the unit you use proper ESD grounding procedures and equipment.



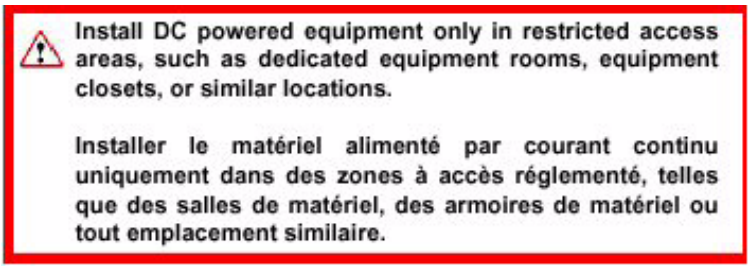




Guidelines for DC-powered equipment

A DC-powered installation must meet the following requirements:

- Install the unit using a 20 Amp external branch circuit protection device.
- For permanently connected equipment, incorporate a readily accessible disconnect in the fixed wiring.
- Use only copper conductors.



8

Reviewing Hardware Specifications

- Reviewing hardware specifications
- 1500 specifications
- 3400 specifications
- 4100 specifications
- 6400 specifications
- 6800 specifications
- Additional acoustic, airflow, and altitude specifications

Reviewing hardware specifications

The following section contains additional information about the IP Application Switch hardware platforms.

Item	Specification
Server/Node Operating System Compatibility	Load balancing of any TCP/IP OS, including Windows NT, Windows 95, all UNIX platforms, and Mac/OS
Internet/Intranet Protocol Support	All TCP services, UDP, SIP, and SSL; nearly all IP-based protocols
Administrative Environment Support	DNS proxy, SMTP, SSH, SNMP, dynamic/static network monitoring, scheduled batch job processing, system status reports, and alarms event notification
Network Management & Monitoring	Secure SSL browser-based interface, remote encrypted login and file transfer using SSH monitor, BIG-IP system network monitoring utilities and additional contributed software; SNMP gets and traps iControl API using CORBA & SOAP/XML
Dynamic Content Support	ASP (active server pages),VB (visual basic script), ActiveX, JAVA,VRML, CGI, Cool Talk, Net Meeting, Real Audio, Real Video, Netshow, Quick Time, PointCast, any HTTP encapsulated data
Device Redundancy	Watchdog timer, fail-safe cable (primary & secondary)
SFP hot swap	These devices support hot swap of the SFP modules
Web Server Application Compatibility	Any IP-based web or application server
Routing Protocols	RIP, OSPF, and BGP with optional ZebOS Advanced Routing Modules
Operating Temperature	23° to 122° F (-5° to 50° C) per Telcordia GR-63-CORE 5.1.1 and 5.1.2
Relative Humidity	10 to 90% @ 40º C, per Telcordia GR-63-CORE 5.1.1 and 5.1.2
Safety Agency Approval	UL 60950 (UL1950-3) CSA-C22.2 No. 60950-00 (Bi-national standard with UL 60950) CB TEST CERTIFICATION TO IEC 950 EN 60950
Electromagnetic Emissions Certifications	EN55022 1998 Class A EN55024 1998 Class A FCC Part 15B Class A VCCI Class A
Non-operational specification	Temperature -40º to 149º F (-40º to 65º C) Humidity 10 to 95% at 40º non-condensing

Table 8.1 *General IP Application Switch specifications*

1500 specifications

The following specifications apply to only the 1500 platform.

Item	Specification
Dimensions	1.75"H x 19"W x 20"D (per unit) 1U industry standard rack-mount chassis
Weight	19 lbs. (per unit)
Processor	Single 2.5 GHz Celeron
Network Interface	4x10/100/1000 2xFiber Gigabit Ethernet interface (SFP GBIC) 1000BASE-SX - 850nm (LC Connector 1000BASE-LX - 1310nm (LC Connector, optional) 1x10/100 Ethernet Management port
Hard Drive Capacity	80 GB hard drive
RAM	768 MB (expandable to 2 GB)
Power supply	300W 100/240 +/- 10% VAC AUTO Switching
Typical power consumption	143W
Heat generated	488 BTU/hour

Table 8.2 *The 1500 IP Application Switch platform specification*

Important

Specifications are subject to change without notification.

3400 specifications

The following specifications apply to only the 3400 platform.

Item	Specification
Dimensions	1.75"H x 19"W x 24"D (per unit) 1U industry standard rack-mount chassis
Weight	24 lbs. (per unit)
Processor	Single Pentium IV 2.8 GHz
ASIC	Packet Velocity ASIC™ 2
Network Interface	8x10/100/1000 with 2xFiber Gigabit Ethernet interfaces (SFP GBIC) 1000BASE-SX - 850nm (LC Connector) 1000BASE-LX - 1310nm (LC Connector) 1x10/100 Ethernet Management port
Hard Drive Capacity	512 MB flash with 80 Gigabyte hard drive
RAM	1 GB (expandable to 2 GB)
Power supply	300W 100/240 +/- 10% VAC AUTO Switching
Typical power consumption	231W
Heat generated	788 BTU/hour

Table 8.3 *The 3400 IP Application Switch platform specification*

Important

Specifications are subject to change without notification.

4100 specifications

The following specifications apply to only the 4100 IP Application Switch platform.

Item	Specification
Dimensions	3.5"H x 19"W x 24"D (per unit) 2U industry standard rack-mount chassis
Weight	40 lbs. (single power), 43 lbs. (dual power) per unit
Processor	Dual Opteron 1.6 GHz
Power Supply	Optional redundant power supply
ASIC	Packet Velocity ASIC™ 2
Network Interface	4x10/100/1000
	2xFiber Gigabit Ethernet interfaces (SFP GBIC) 1000BASE-SX - 850nm (LC Connector) 1000BASE-LX - 1310nm (LC Connector)
	1x10/100 Ethernet Management port
Hard Drive Capacity	512 MB flash with 80 Gigabyte hard drive
RAM	2 GB (expandable to 4 GB)
Power supply	400W 90/240 +/- 10% VAC AUTO Switching
Typical power consumption	275W
Heat generated	939 BTU/hour

Table 8.4 *The 4100 IP Application Switch platform specification*

Important

Specifications are subject to change without notification.

6400 specifications

The following specifications apply to only the 6400 IP Application Switch platform.

Item	Specification
Dimensions	3.5"H x 19"W x 24"D (per unit) 2U industry standard rack-mount chassis
Weight	40 lbs. (single power), 43 lbs. (dual power) per unit
Processor	Dual Opteron 1.6 GHz
Power Supply	Optional redundant power supply
ASIC	Packet Velocity ASIC™ 2
Network Interface	16x10/100/1000
	4xFiber Gigabit Ethernet interfaces (SFP GBIC) 1000BASE-SX - 850nm (LC Connector) 1000BASE-LX - 1310nm (LC Connector)
	1x10/100 Ethernet Management port
Hard Drive Capacity	512 MB flash with 80 Gigabyte hard drive
RAM	2 GB (expandable to 4 GB)
Power supply	400W 90/240 +/- 10% VAC AUTO Switching
Typical power consumption	275W
Heat generated	939 BTU/hour

Table 8.5 *The 6400 IP Application Switch platform specification*

Important

Specifications are subject to change without notification.

6800 specifications

The following specifications apply to only the 6800 IP Application Switch platform.

Item	Specification
Dimensions	3.5"H x 19"W x 24"D (per unit) 2U industry standard rack-mount chassis
Weight	40 lbs. (single power), 43 lbs. (dual power) per unit
Processor	Dual Opteron 2.4 GHz
Power Supply	Optional redundant power supply
ASIC	Packet Velocity ASIC™ 2
Network Interface	16x10/100/1000
	4xFiber Gigabit Ethernet interfaces (SFP GBIC) 1000BASE-SX - 850nm (LC Connector) 1000BASE-LX - 1310nm (LC Connector)
	1x10/100 Ethernet Management port
Hard Drive Capacity	512 MB flash with 80 Gigabyte hard drive
RAM	2 GB (expandable to 4 GB)
Power supply	400W 90/240 +/- 10% VAC AUTO Switching
Typical power consumption	285W
Heat generated	973 BTU/hour

Table 8.6 *The 6800 IP Application Switch platform specification*

Important

Specifications are subject to change without notification.

Additional acoustic, airflow, and altitude specifications

This section describes additional specifications such as acoustic levels, airflow movement, and operational altitude for the BIG-IP 1500, 3400, 6400, and 6800 chassis.

	Detail	Units	1500	3400 [4]	6400	6800
Acoustic [1]						
	Front face	db	57	58	65	65
	Left face	db	61	59	64	64
	Right face	db	58	65	68	68
	Rear face	db	59	63	65	65
Altitude [2]						
	Operational	Feet	5905	5905	5905	5905
	Non-operational	Feet	40000	40000	40000	40000
Airflow						
	Entire chassis	cfm	32.1	52.6	117.6	117.6

Table 8.7 *Acoustic, altitude, and airflow specifications*

[1] All measurements taken at 1 meter - A-weighting

[2] Per BELCORE GR-63-CORE, section 4.1.3. 60m (197ft) below sea level to 1800m (5905 ft) above sea level.

[3] Calculated

[4] New platforms shipped as of 6/26/2005

Glossary

bigpipe

The **bigpipe** utility provides command line access to the BIG-IP software.

BIOS

BIOS stands for Basic Input/Output System. The BIOS is software that is built-in to the computer and determines what the computer can do without accessing programs from a disk.

Configuration utility

The Configuration utility is the browser-based application that you use to configure the software.

DHCP

DHCP stands for Dynamic Host Configuration Protocol. It is a protocol used to assign dynamic IP addresses to network devices. When using DHCP, a network device can have a different IP address each time it connects to the network.

DNS

DNS stands for Domain Name System. It is a service that translates domain names into IP addresses. For example, the domain name **www.sample.com** might translate to **101.102.103.104**.

LCD

LCD stands for liquid crystal display. An LCD panel is available on the front of the 1500, 3400, 6400, and 6800 platforms. You can use the LCD and its associated controls to configure the management port on the unit and view basic statistics.

NIC

NIC stands for Network Interface Card. It is an expansion board used to connect a computer to a network.

port

A port is represented by a number that is associated with a specific service supported by a host. Refer to the Services and Port Index for a list of port numbers and corresponding services.

PXE

PXE stands for Pre-Boot Execution Environment, a network boot method. It allows you to boot a computer from a server on a network before you boot the operating system on the local hard drive.

SFP GBIC

SFP GBIC stands for small form factor pluggable (SFP) gigabit interface converter (GBIC).

SSH

SSH is a protocol for secure remote login and other secure network services over a non-secure network.

SSL

SSL stands for Secure Sockets Layer. It is a protocol that uses a public key to encrypt data transmitted through the Internet over an SSL connection. URLs using an SSL connection start with **HTTPS:** instead of **HTTP:**.

subnetwork

The portion of a network that shares a common address component. For instance, on TCP/IP networks, a subnetwork is all devices whose IP addresses have the same prefix segment.

Telnet

Telnet is a terminal emulation program for TCP/IP networks. Telnet runs on your computer and connects it to a server on the network. It then allows you to enter and execute commands as though you were directly connected to the server console.

terminal emulator

A terminal emulator is a program that mimics a terminal.

virtual server

Virtual servers are a specific combination of virtual address and virtual port, associated with a content site that is managed by BIG-IP system or other type of host server.

Index