ixia
A Keysight Business

FireStorm

Installation Guide

Notices

Copyright Notice

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at http://www.keysight.com/find/sweula or https://support.ixiacom.com/support-services/warranty-license-agreements. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b) (2) (November 1995), as applicable in any technical data.

Safety Information

Do not proceed beyond a hazard notice until the indicated conditions are fully understood and met.

A **CAUTION** notice denotes a hazardous situation that, if not avoided, could result in minor or moderate injury.

A **WARNING** notice denotes a hazardous situation that, if not avoided, could result in death or serious injury.

Contact Us

Ixia headquarters

26601 West Agoura Road
Calabasas, California 91302
+1 877 367 4942 – Toll-free North America
+1 818 871 1800 – Outside North America
+1.818.871.1805 – Fax
www.ixiacom.com/contact/info

Support

Global Support	+1 818 595 2599	support@ixiacom.com
APAC Support	+91 80 4939 6410	support-asiapac@ixiacom.com
EMEA Support	+40 21 301 5699	support-emea@ixiacom.com
Greater China Region	+400 898 0598	support-china@ixiacom.com
Hong Kong	+86 10 5732 3932	support-china@ixiacom.com
India Office	+91 80 4939 6410	support-india@ixiacom.com
Japan Head Office	+81 3 5326 1980	support-japan@ixiacom.com
Korea Office	+82 2 3461 0095	support-korea@ixiacom.com
Singapore Office	+656 494 8910	support-asiapac@ixiacom.com

CONTENTS

Product Safety Information

Before installing the unit, read all product safety instructions contained in this document. These instructions contain specific safety messages that will alert you to any hazards associated with the installation and proper operations of the equipment. Failure to follow those instructions can result in serious injury or death.

This page intentionally left blank.

CHAPTER 1 About This Guide

This section explains the purpose, audience, and organization of this guide. It also defines conventions used to present instructions and information throughout this guide and includes information on how to get support for issues encountered while you use your BreakingPoint device.

Purpose

The purpose of this guide is to provide safety regulations, site requirements, and installation instructions for FireStorm.

Target Audience

The intended audience is users of all skill levels.

Organization

This guide is organized into the following sections:

- About This Guide
- Product Overview
- Site and Safety Requirements
- FireStorm Installation
- System Configuration
- Accessing the Control Center
- Frequently Asked Questions
- Appendix
- Index

Conventions

This guide uses the conventions listed in the following table:

Convention	Description	Example
Bolded text	Commands, keywords, or buttons	Press the **Enter** key.
`Courier New font`	User input	Type `GET` in the **Method Request** box.

Note:	Helpful suggestion or reference to additional information	**Note:** Racks must meet standard EIA-310-C requirements.

Related Documentation

The following table lists all the documentation related to FireStorm. You can access all documentation through the Documentation area of the Ixia support website.

Documentation	Description
FireStorm Installation Guide	Provides installation instructions and information for FireStorm.
FireStorm User Guide	Provides information on how to use the Control Center to set up, customize, and run traffic through devices under test.
FireStorm Migration Guide	Provides an overview of the tasks that you must complete to migrate from BreakingPoint Storm to FireStorm.
BreakingPoint Online Help	Online documentation for all BreakingPoint products. Requires Internet Explorer 10.0 or Firefox 18.0 for proper viewing.

Ixia Support Website

The Ixia Support website is an online portal for security and software updates as well as industry information. You can use the Ixia support website to do the following:

- Obtain the latest software releases for BreakingPoint FireStorm.
- Download the most up-to-date ATI Updates (formerly known as StrikePacks), which includes the latest Strikes, test capabilities, and application protocols.
- Download PDFs of documentation.
- Find contact information for Customer Support, Sales, and corporate facilities.
- Access blogs and technical articles related to vulnerabilities, exploits, and recent updates to any BPS product.

Documentation Feedback

Please send any feedback or suggestions regarding this documentation to techpub@breakingpoint.com.

CHAPTER 2 Product Overview

This section covers the following:

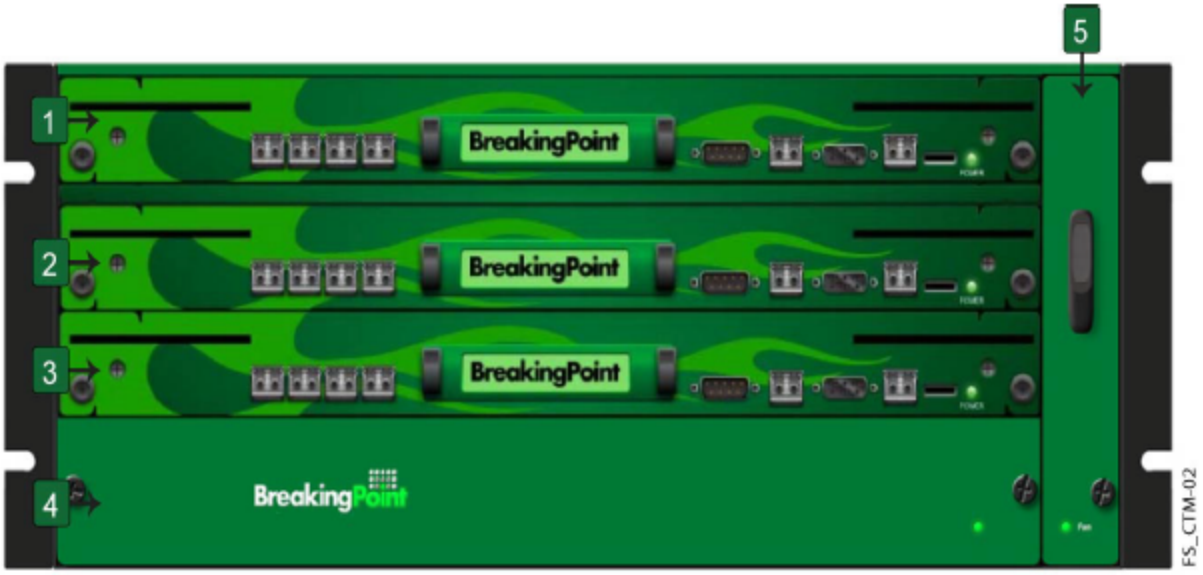
FireStorm Overview

BreakingPoint Systems has developed a product that measures and hardens the resiliency of every component of your critical infrastructure against potentially crippling attacks and peak application traffic: the FireStorm. It is a 4 RU rack-mountable and modular system that can accurately recreate a live network environment.

FireStorm consists of the chassis and the user interface called the Control Center. Both components work together to create a comprehensive and user-friendly test solution for all network devices. FireStorm can concurrently simulate TCP sessions, application traffic, and live security attacks, and ultimately, identify 'breaking points' in your network devices.

FireStorm Hardware Overview

FireStorm is comprised of five slots. The following image highlights these slots with callouts:



Callouts 1, 2, and 3 refer to the slots dedicated to high-speed data plane processors (or the blades) for the computer. When you initially receive the FireStorm chassis, these slots will not contain any blades. You will need to install the blade(s) into the chassis.

Each blade provides four 10 GigE fiber-optic data ports that support up to Gbps per blade. The fiber-optic connections between the ports on your device under test and the test ports on the chassis establish the transmitting and receiving interfaces for your tests.

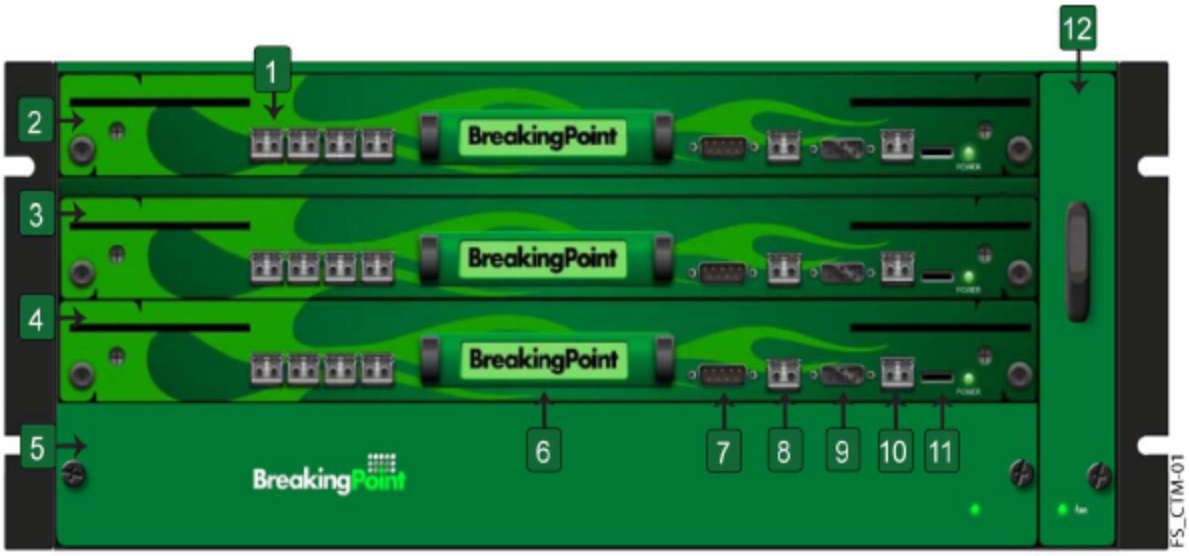
The BPS management ports (serial and ethernet) allow you to connect your computer to a network and access it through an IP address. The target control ports allow you to automate testing for the device under test.

Callout 4 refers to the power tray, which contains the power supply for the computer.

Callout 5 refers to the removable fan tray that is vertically mounted on the right-side of the chassis.

Front view of FireStorm

The following image illustrates the front view of FireStorm. Locate the corresponding callout in the following table for more information about each component.

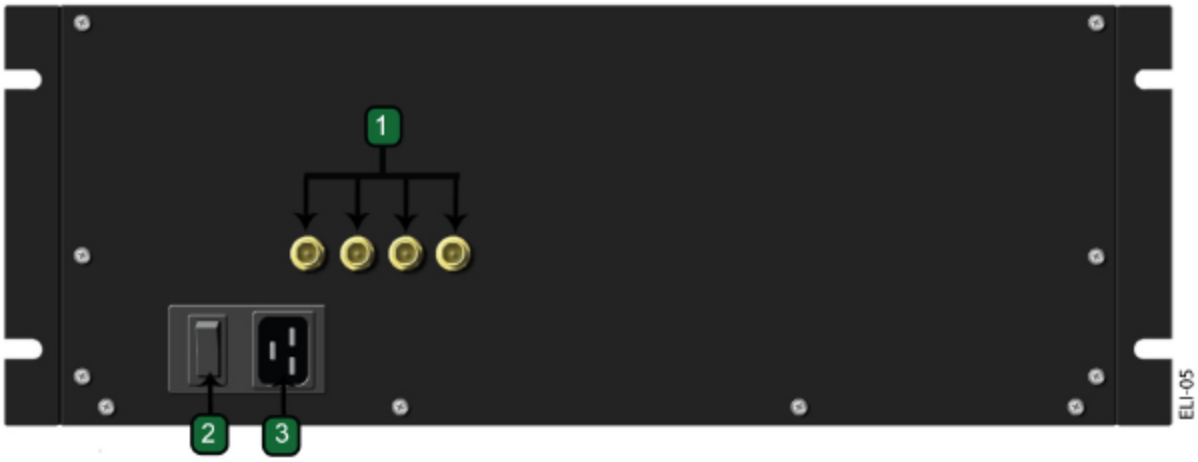


Callout	Component	Description
1	Data Ports	Transmits and receives traffic to and from the DUT.
2	Hard drive bay	Contains the hard drive enclosure.
3	Target Control Serial Port	Used to manage and configure settings for the DUT.
4	Target Control Ethernet Port	Used to manage and configure settings for the DUT.

5	BPS Management Serial Port	Manages the FireStorm configuration through a serial connection.
6	BPS Management Ethernet Port	Manages the FireStorm configuration through an ethernet connection.
7	USB Port	Provides a USB connection for an external memory device.
8	System Fan Tray	Holds the fan tray for the computer.

Back view of FireStorm

The power inlet and power switch are located on the back of the chassis, as shown in the following image. Additionally, there are BNC interfaces that you can use in future releases to link together multiple chassis.



Callout	Component	Description
1	BNC Interfaces	Interfaces that are used to connect multiple chassis together (for clock I/O and trigger I/O).
2	Power Switch	Power breaker switch for FireStorm.
3	Power Inlet	Power inlet for FireStorm.

Control Center Overview

The Control Center is a web-based user interface where you can create the testing environment, run tests, and view reports. The Control Center is accessible through a Flash-enabled web browser, such as Internet Explorer, Mozilla Firefox, Safari, and Opera. You must also have JavaScript turned on to view the Control Center.

Note: Safari 6.0.2 on Mac OS 10.8.2 and Safari for Windows are not supported. Mac users with OS 10.8.2 can use Firefox or Chrome as their browser.

Note: We recommend that users of Internet Explorer use IE 10. IE 9 and earlier versions are not supported.

Enabling JavaScript

You must have JavaScript turned on to view the Control Center.

To turn on JavaScript for Internet Explorer, do the following:

1. Open an Internet Explorer browser window.
2. Click **Tools** > **Internet Options** from the menu bar.
3. Click the **Security** tab.
4. Click **Custom Level**.
5. Scroll down to the **Scripting** section.
6. Find the category called **Active Scripting**.
7. Click **Enable** for this category.
8. Click **Yes** when the confirmation window appears.
9. Click **OK** to close the **Internet Options** window.

To turn on JavaScript for Mozilla Firefox 2.0, do the following:

1. Open a Mozilla Firefox browser window.
2. Click **Tools** > **Options** from the menu bar.
3. Click **Content** located at the top of the window.
4. Click **Enable JavaScript**.
5. Click **OK** to close the **Options** window.

To turn on JavaScript for Safari, do the following:

1. Open a Safari browser window.
2. Click **Preferences** from the Safari menu.
3. Click **Security** from the top of the window.
4. Click **Enable JavaScript** located under the Web Content section.
5. Close the **Security** window.

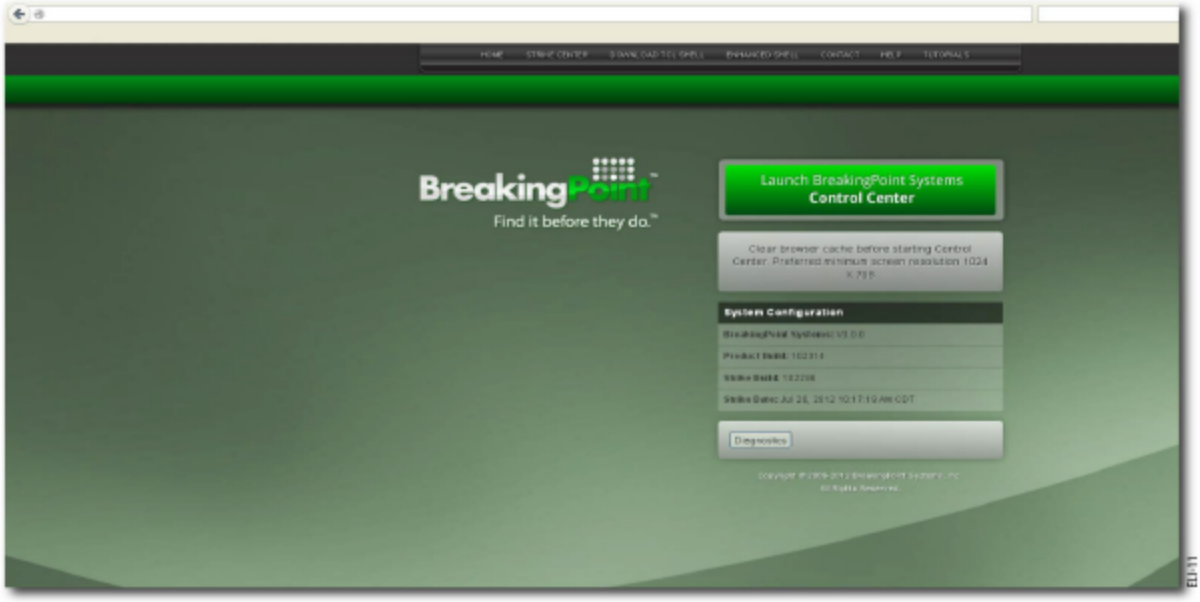
Accessing the Control Center

To access the Control Center, you must have a web browser with the following items turned on or installed:

- Adobe Flash Player (version 11.6.602.171)
- Pop-ups
- JavaScript

Additionally, you must have the host address that has been set for the BPS Management Port and the Control Center login information.

The chassis must already be installed and configured before the Control Center can be accessed.



To access the Control Center, do the following:

1. Open a Web browser.

   Note: After upgrading or reverting to any release of the BreakingPoint Firmware, clear your cache and refresh your browser.

2. Type the host address for the BPS Management port in the **Address** bar.

   Note: The default address is http://10.10.10.10, however, the host address may have changed during the initial configuration of the computer. Contact the System Administrator for the current host address.

3. Click **Launch BreakingPoint Systems Control Center** in the **Start** page.

   Note: The first time you attempt to log on to the computer, your browser will require you to verify a security exception to login. Follow the steps required by your browser to accept and verify the security exception. After the security exception has been accepted and verified, you will be allowed to continue with the login process. A new window opens and shows the Control Center login page.

4. Type the login ID in the **Username** box.
5. Type the password in the **Password** box.

   Note: Passwords are case sensitive.

6. Click **Login**.

> **Note:** The computer allows three invalid logins. If you type invalid login information on the fourth attempt, the login window will lock you out. Refresh the browser to unlock your accounts.

Navigational Overview

This section provides an overview of the navigational areas in the Control Center. The Control Center is divided into two main areas: the menu bar and the navigational buttons. See the following image for a tour of the interface:

Callout	Name	Description
1	Menu Bar	Provides point and click access to the main areas of the user interface.
2	Device Status	Provides access to the Device Status area so that you can reserve ports while no tests are running or the Real Time Statistics screen if there is a running test.
3	Navigational Buttons	Provides access to areas within the user interface.

CHAPTER 3 Getting Started

Note: You can also reference the BreakingPoint User Guide for the most current information on performing the tasks described in this topic.

This section covers the following:

Getting Started Overview

This section provides an overview of the tasks that you must complete to install and configure the BreakingPoint device, as well as explain how to set up your test environment within the BreakingPoint Control Center.

The following table lists the Getting Started tasks:

Task	Description
Task 1	Installing the BreakingPoint Device.
Task 2	Configuring the BreakingPoint Device.
Task 3	Establishing a BreakingPoint Session.
Task 4	Accessing the BreakingPoint Control Center.
Task 5	Creating user accounts.
Task 6	Setting the time and date.

Task 7	Creating a DUT Profile.
Task 8	Creating a Network Neighborhood.
Task 9	Making Port Reservations.
Task 10	Creating a test.

Task 1: Installing the BreakingPoint Device

This section describes how to set up the BreakingPoint device.

To set up the BreakingPoint device, do the following:

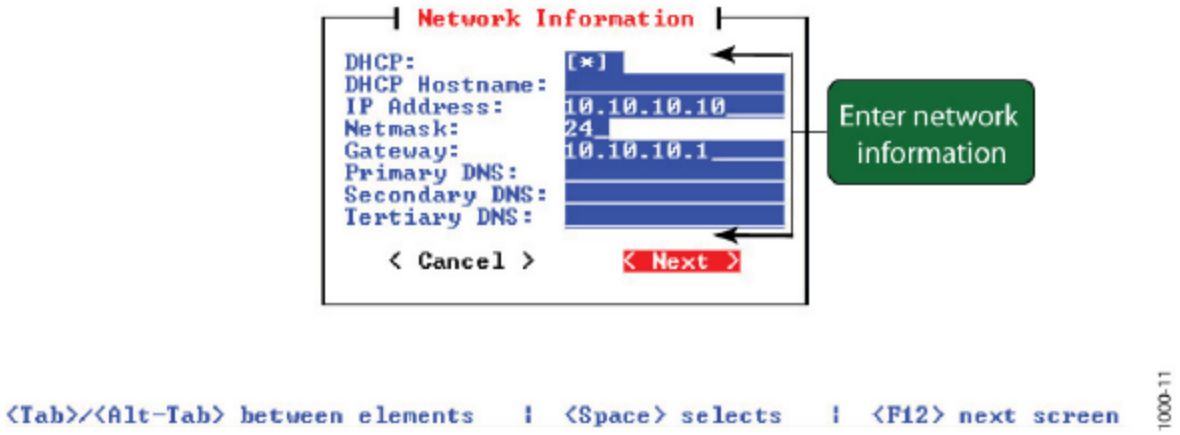
1. Secure the chassis into an equipment rack.

   Note: The chassis must be close enough to the device under test so that you can connect cables from the appliance to the device under test.

2. Insert the computer controller into the module over the power tray.
3. Insert the blade(s) into the top two modules.
4. Power the computer.
5. Connect the device under test to the BreakingPoint device.

Task 2: Configuring the BreakingPoint Device

You will need to use either a telnet client or text console to configure the network settings for the BreakingPoint device. The following sections provide instructions for configuration through a telnet client or a text console.



Telnet

This section describes how to configure the host address, netmask, and gateway for the BreakingPoint device by using either a telnet client or a text console.

To configure the BreakingPoint device by using Telnet, do the following:

1. Open a telnet client (for example, PuTTy or AlphaCom).
2. Telnet to the following host address: 10.10.10.10.
3. Specify your terminal emulation preference (for example, ANSI or xterm) at the prompt and press **Enter**.
4. Specify the following information for your BreakingPoint device in the Network Information box:
   - DHCP Enable/Disable

     Note: If DHCP is turned off, you can configure additional computer routes from the **Routes** tab in the **Administration** area of the Control Center. If DHCP is turned on, the **Routes** area will be unavailable.

   - DHCP Hostname
   - IP Address
   - Netmask
   - Gateway
5. Click **Next**.
6. Type the login ID for the user account at the prompt.

   Note: The login ID must use alphanumeric characters and consist of 1-15 characters. The first character of the login ID must be a letter. Login IDs cannot solely consist of numbers. The login ID cannot be changed after it has been created.

7. Type the password for the user account at the prompt.

   Note: The password can consist of up to 15 alphanumeric and special characters.

The computer disconnects while the new network settings are applied and your account is created. Document the network IP address and user account information. You will need this information to access and log on to the BreakingPoint Control Center. You may create additional accounts through the **Administration** page in the BreakingPoint Control Center.

Text Console

This section describes how to configure the host address, netmask, and gateway for the BreakingPoint device by using a text console.

To configure the BreakingPoint device by using a text console, do the following:

1. Open a terminal emulation client (for example, HyperTerminal).
2. Connect to the BPS management serial port by using the following settings:
   - Baud Rate: 115200 bps
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None

3. Specify the following information in the **Network Information** box:
   - DHCP Enable/Disable
   - DHCP Hostname
   - IP Address
   - Netmask
   - Gateway
4. Click **Next** when you are done inputting your network settings.
5. Type the login ID that you will use for the user account at the prompt.
6. Type the password for the user account at the prompt.

The computer disconnects while the new network settings are applied and your new account is created. Document the network IP address and user account information. You will need this information to access and log on to the BreakingPoint Control Center. You may create additional accounts through the **Administration** page in the Ixia web app.

Task 3: Establishing a BreakingPoint Session

The Breaking Point (BPS) application has been integrated into Ixia's web app. This integration enables you to access the BreakingPoint Control Center from the Ixia web app user interface. You can also configure certain BreakingPoint chassis properties through the Ixia web app user interface. You can now create new user accounts and manage them through the Ixia web app user interface.

To establish a BreakingPoint session and operate in the BreakingPoint Control Center, you must first log on to the Ixia web app.

Note: A session is an individual instance of a running test. You can run multiple sessions at one time, and manage all your current sessions from a single window. You manage sessions on the **Sessions** page, which appears after you log on.

To establish a BreakingPoint session, do the following:

1. Open a web browser.
2. In the **URL** box, type the IP address or hostname of the Ixia chassis where the Ixia web app server components are installed, followed by the port number that the Ixia web app server is listening on (the default is 8080), and then press **Enter**.

   Example: 192.168.100.56:8080

   The **Login** page appears.
3. In the **Username** box, type your user ID.
4. In the **Password** box, type your password.
5. If you want the browser to automatically fill in the Username and Password field for future logins, select the **Remember Me** check box.
6. Click **Login**. The **Sessions** page appears.
7. Click the **BreakingPoint New Session** icon. The BreakingPoint Control Center appears.

Task 4: Accessing the BreakingPoint Control Center

The BreakingPoint Control Center is a web-based user interface where you can create the testing environment, run tests, and view reports. The BreakingPoint Control Center is accessible through an Adobe Flash-enabled web browser, such as Internet Explorer, Mozilla Firefox, Safari, and Opera. You must also have JavaScript turned on to view the BreakingPoint Control Center.

Note: Safari 6.0.2 on Mac OS 10.8.2 and Safari for Windows are not supported. Mac users with OS 10.8.2 can use Firefox or Chrome as their browser.

Note: We recommend users of Internet Explorer to use IE 10. IE 9 and earlier versions are not supported.

Viewing the BreakingPoint Control Center requires a web browser with the following items either turned on or installed:

- Adobe Flash Player (version 11.6.602.171)
- Pop-ups
- JavaScript

Enabling JavaScript

You must have JavaScript turned on to view the BreakingPoint Control Center.

To turn on JavaScript for Internet Explorer, do the following:

1. Open an Internet Explorer browser window.
2. Click **Tools** > **Internet Options** from the BreakingPoint Control Center menu bar.
3. Click the **Security** tab.
4. Click **Custom Level**.
5. Scroll down to the **Scripting** section.
6. Find the category called **Active Scripting**.
7. Click **Enable** for this category.
8. Click **Yes** when the confirmation window appears.
9. Click **OK** to close the **Internet Options** window.

To turn on JavaScript for Mozilla Firefox, do the following:

1. Open a Mozilla Firefox browser window.
2. Click **Tools** > **Options** from the BreakingPoint Control Center menu bar.
3. Click **Content** located at the top of the window.
4. Click **Enable JavaScript**.
5. Click **OK** to close the **Options** window.

To turn on JavaScript for Mozilla Firefox 23, do the following:

1. In the address bar, type `about:config` and press **Enter**.
2. Click **"I'll be careful, I promise"**.

3. In the search bar, search for **javascript.enabled**.
4. Right click the result named **javascript.enabled** and click **Toggle**. JavaScript is now turned off.

To turn on JavaScript, repeat these steps.

To turn on JavaScript for Safari, do the following:

1. Open a Safari browser window.
2. Click **Preferences** from the Safari menu.
3. Click **Security** from the top of the window.
4. Click **Enable JavaScript** located under the Web Content section.
5. Close the **Security** window.

You must also have the host address that has been set for the BPS management port and the BreakingPoint Control Center login information.

Note: The chassis must already be installed and configured before the BreakingPoint Control Center can be accessed. For more information on installing and configuring your BreakingPoint device, see your BreakingPoint device's installation guide.

Browser Resources

If you have several browser windows open simultaneously, or if you have multiple instances of the BreakingPoint Control Center open, this may cause lagging or delayed responses from the computer. This is normal behavior for the BreakingPoint Control Center if multiple browser resources are being used.

Note: We recommend clearing your cache and refreshing your browser after upgrading or reverting to any release of BreakingPoint.

Navigational Overview

This section provides an overview of the navigational areas in the BreakingPoint Control Center. The BreakingPoint Control Center is divided into two main areas: the BreakingPoint Control Center menu bar and the navigational buttons. See the following image for a tour of the interface:

The following table lists the elements of the BreakingPoint Control Center:

Callout	Name	Description
1	Menu Bar	Provides point and click access to the main areas of the user interface.
2	Device Status Icon	Provides access to the Device Status area so that you can reserve ports while no tests are running or the Real-Time Statistics screen if there is a running test.
3	Navigational Buttons	Provides access to areas within the user interface.
4	Firmware Version Information	Provides firmware version and update information.

Task 5: Creating a User Account

Only admin users can create user accounts or edit all the properties of a user account. If you are a non-admin user, the only change you can make to your own account is to change your password.

To create or edit a user account, do the following:

1. Log on with an admin account.
2. Click **Administration** > **Users**.
3. Click **New User**. The **Create User Account** window appears.
4. Configure the account. (See the following table for fields and parameter descriptions.)
5. Click **OK** to create the account.

The following table lists and describes the parameters of the **Edit Account** window:

Parameter	Description
Username	Name for the account.
Create Password/Confirm Password	Password for the user name.
Full Name	Name identifying the user.
Email	Email for the user account. If this user chooses to receive test results by email, this is the email address that will be used.
Assigned to Groups	Group that the user account will belong to: • Admin: Administrators have authority over all user accounts. • Regular Users: Standard users can change some aspects of their accounts and run the applications that administrators have authorized for them.
Permissions to Use	Applications that this user account will be allowed to run.

Task 6: Setting the Time and Date

To set the computer time and day, go to the **System Settings** tab of the **Ixia Administration** page. The controls on this window set the time and date on the chassis. The computer time and date appears in test results and system logs. The time and date are not set by default. You need to set it when you install a new chassis.

Note: The time and date do not automatically adjust for Daylight Savings Time. You must manually change the time to account for Daylight Savings Time.

To set the time and date, do the following:

1. Log on with an admin account.
2. Click **Administration** > **System Settings**.
3. Click **System time and date**.
4. Configure the time and date. (See the following table for parameters and descriptions.)
5. Click **Apply** to set the time and date.

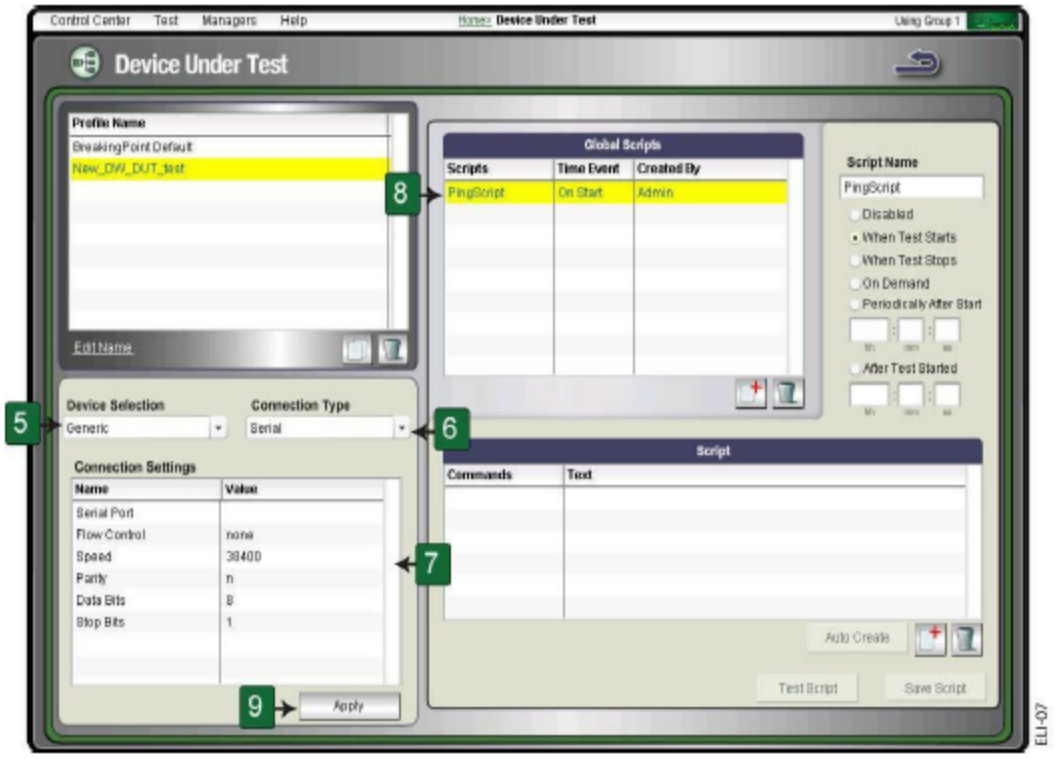
The following table lists and describes the parameters of the **System time and date** window:

Parameter	Description
Time	Current time (hours:minutes) in 24-hour clock format.
Date	Today's date.
Time zone	Time zone where the chassis is located.

Task 7: Creating a Device Under Test Profile

This section describes how to create a DUT profile. A DUT profile defines the connection settings for the device under test, such as the device's connection type, connection parameters, link type, and global commands. The BreakingPoint device uses these settings to connect to the device under test for remote scripting. For more information on DUT Profiles, see the DUT Profiles section in the user guide.

Note: The BreakingPoint device provides a default DUT profile called BreakingPoint Default. This DUT profile cannot be modified or deleted, however, it can be cloned and customized for your device.



To create a DUT profile, do the following:

1. Click **Control Center** > **Device Under Test** from the BreakingPoint Control Center menu bar.
2. Select a profile from the **Profile Name** list to clone.
3. Click **Clone the selected DUT**.
4. Type a name for the DUT profile in the **Name** field and click **OK**.

5. Click **Device Selection** and select a device type (optional).

   Note: Each device type has its own set of global commands. Select the device type that best fits your device.

6. Click **Connection Type** and select Telnet, SNMP, SSH, or Serial.

   Note: If you select **Serial**, the DUT must be plugged into the chassis through the BPS management serial port. If you select Telnet or SSH, the DUT must be plugged into the chassis through the BPS management ethernet port.

7. Define the connection parameters for the DUT under the **Connections Settings** area. For more information on connection parameters, see the Connection Parameters section in the user guide for a list of valid parameter values.
8. Enable or disable any global commands from the **Global Commands** list.

   Note: All cloned DUT profiles inherit the active global commands from its parent DUT profile. For more information on commands, see the Commands section in the user guide.

9. Click **Apply**.

Task 8: Creating a Network Neighborhood

A Network Neighborhood consists of all the domains for each test interface. The domains consist of subnets, which set the range of source and destination addresses for the test traffic sent or received by the interface. For each test component, specify the domain that the component uses to obtain the source and destination addressing for its traffic.

Each domain consists of a single subnet, or it can have multiple subnets depending on whether or not the domain supports VLANs. All VLAN-enabled domains have more than one subnet. Any other type of domain can only have one.

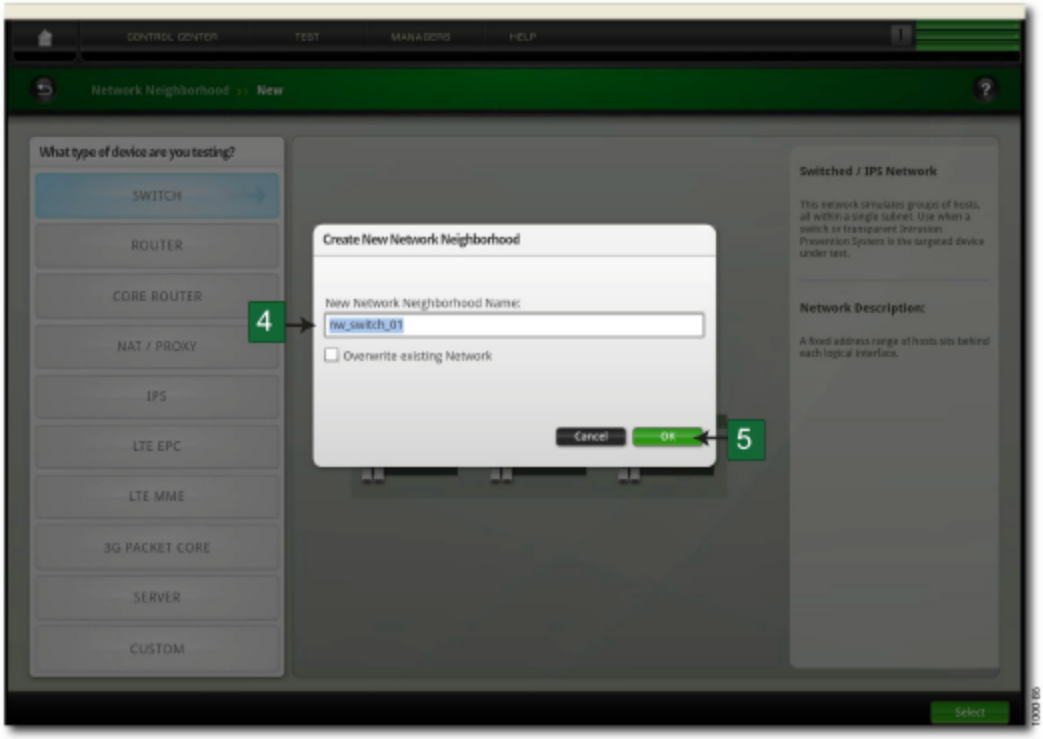
Note: The computer randomly selects VLAN IDs from the Network Neighborhood. Therefore, some VLAN IDs may be used multiple times, whereas others may not be used at all.

This task is broken into four parts:

1. Creating a Network Neighborhood.
2. Adding a domain to the Network Neighborhood.
3. Defining the subnet for the domain.
4. Adding additional interfaces to the Network Neighborhood (for two-blade chassis).

Creating a Network Neighborhood

This section describes how to create a Network Neighborhood.



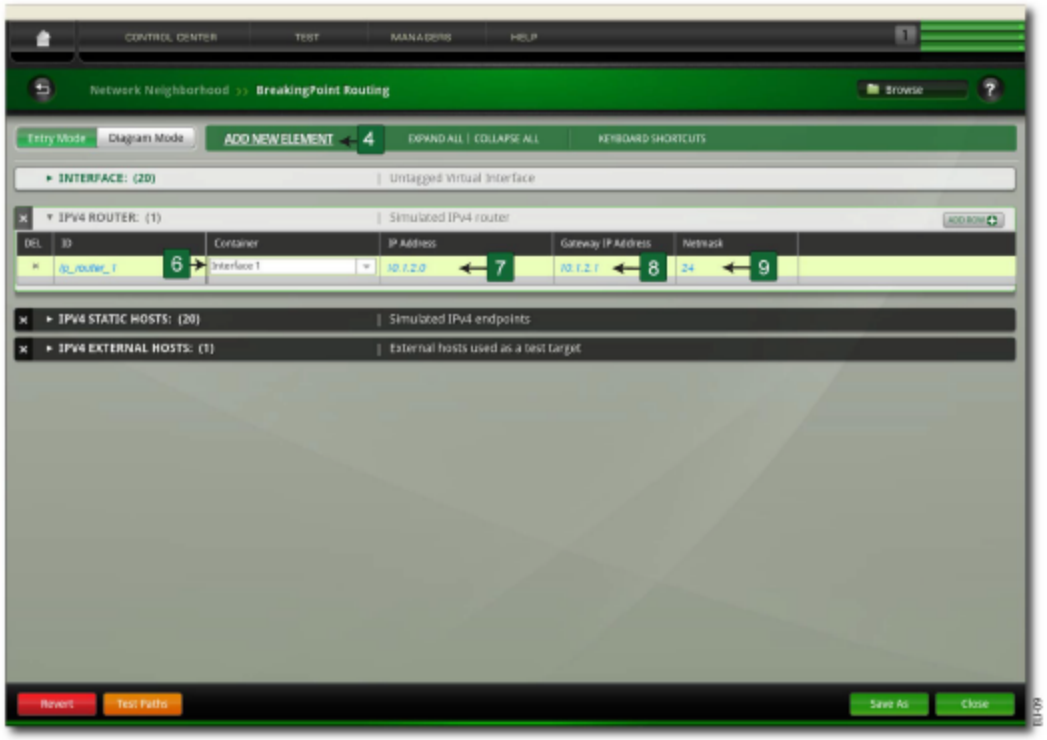
To create a Network Neighborhood, do the following:

1. Click **Control Center** > **Network Neighborhood** from the BreakingPoint Control Center menu bar.
2. Click **Create a new network neighborhood ('+')** located under the Network Neighborhoods list.
3. Type a name for the Network Neighborhood in the **Name** box.
4. Click **OK**.

Note: Each interface has a default domain with a reconfigured subnet.

Defining a Subnet

This section describes how to add a subnet to a non-VLAN tagging subnet on a non-external interface. For information on external device addressing or VLAN-enabled addressing, see the External Interface Addressing or Defining a VLAN-Enabled Subnet section in the user guide.



To define a non-VLAN subnet, do the following:

1. Click **Control Center** > **Network Neighborhood** from the BreakingPoint Control Center menu bar.
2. Select a Network Neighborhood from the **Network Neighborhoods** list.
3. Select a test interface to modify by clicking the **Interface** tab.
4. Select a domain from the **Domains** list.
5. Click **Show the create new subnet form ('+')** located under the Subnets list. The **Create new subnet** dialog box appears.

   Note: If you are adding a subnet to an empty domain, you can skip this step. The Subnet form will already be blank and ready for you to input addressing information.

6. Select IPv4 or IPv6 addressing.
7. Click **VLAN Tagging** and select a VLAN tag.
8. Select Use NAT for network address translation (if applicable).
9. Type an IP address in the **Network IP Address** box. To assign an IPv4 address, use the format x.x.x.x, where x is a number between 0-255. To assign an IPv6 address, use the format x:x:x:x, where x is a valid hexadecimal value.
10. Type a mask for the network address in the **Netmask** box. For IPv6 addressing, type the prefix in the **Prefix** field.
11. Type a gateway address in the **Gateway IP Address** box. To assign an IPv4 address, use the format x.x.x.x, where x is a number between 0-255. To assign an IPv6 address, use the format x:x:x:x, where x is a valid hexadecimal value.

12. Click **Type**.
13. Do one of the following:
    - Click **Host** from the **Type** list to use one MAC address per host.
    - Click **Virtual Router** from the **Type** list to use one MAC address for all hosts, and type an IP address for the virtual router in the **Router IP Address** box.

    Note: If an IPv6 router is present, the BreakingPoint device generates at least one global address. You can discover the automatically generated IPv6 address through the SSH/telnet/serial interface, by using the networkInfo command.
14. Type an ethernet address in the **Ethernet Address** box. Use the format xx:xx:xx:xx, where x is a valid hexadecimal value.
15. Turn on or turn off the **Use Address Range** option.
16. Type a range of IP addresses by using the **Minimum IP Address** and **Maximum IP Address** box. Use the format x.x.x.x, where x is a number between 0-255.

    Note: If **Use Address Range** is turned off, you only need to type an IP address in the **Minimum IP Address** box. The system only uses one IP address for the entire subnet.
17. Click **Add Subnet**.
18. Click **Save Network**.

Adding a Test Interface

By default, the computer provides you with four transmitting and receiving interfaces and one external interface (for SSL testing). So, if you have a two blade chassis, you will need to add additional interfaces to your Network Neighborhood.

Each test interface in the Network Neighborhood corresponds to a data port on the chassis. When you add an interface to a Network Neigbhorhood, the computer automatically numbers the interface based on the order in which it was added.

If you delete any of the interfaces, the computer automatically sequences the interfaces again. The succeeding interfaces (following the deleted interface) will be renumbered to the preceding interface's value (for example, '6' will become '5').

Note: There can be up to eight test interfaces in a Network Neighborhood and one external interface.

To add a test interface to a Network Neighborhood, do the following:

1. Click **Control Center** > **Network Neighborhood** from the BreakingPoint Control Center menu bar.
2. Select a Network Neighborhood from the **Network Neighborhoods** list.
3. Click **Add New Interface ('+')**.

   Note: The interface contains one domain with the default subnet.

After you have added the interface to the Network Neighborhood, add subnets in the usual way. For more information on defining subnets, see Defining a Subnet.

Task 9: Making Port Reservations

The number of tests that you can run concurrently depends on the number of available ports that the BreakingPoint device has. For example, a single-blade BreakingPoint device with four available ports can only run four tests at a time. A two-blade chassis with sixteen total available ports can run sixteen tests simultaneously. To run all sixteen tests concurrently, however, you will need to assign each available port to a different Active Group.

To run tests on the BreakingPoint device, you must make port reservations. A port reservation occurs when you click a port to reserve it under your account. No other users can run tests or system processes on that port while it is reserved under your account.

When you click a port to reserve it, the computer will lock the port reservation under your account. Locking a port reservation also reserves all other ports under your account as well, however, only the ports with locked reservations can be used to run tests.

Note: To run two tests concurrently, each set of blades must be assigned to a different Active Group. For more information on Active Groups, see the Active Groups section in the user guide.

There are three ways to reserve a blade:

- Reserving an unreserved blade.
- Force reserving a reserved blade.
- Simultaneously reserving or unreserving a blade.

Reserving an Unreserved Blade

Unreserved blades may be reserved simply by selecting the Active Group to which you would like to assign the blade, and then clicking the port that you would like to reserve. This locks the port reservation, as well as reserves all the ports on the blade under your account.

Note: A lock containing the Active Group appears on all the ports on the blade.

When reserving your ports, remember the order in which you reserve them. Whenever you reserve a port, the computer automatically maps that port to an interface on the chassis. For example, if you reserve ports 0 and 1, port 0 will map to interface 1 and port 1 will map to interface 2. You can use these interfaces to run tests. If an interface is not mapped to a port, you cannot use that interface to run tests.

If you want to remap the ports to different interfaces, click **Port Mapping**, located on the **Device Options** screen, and manually remap the ports.

Note: You can map only reserved ports to interfaces.

To reserve ports on an unreserved blade, do the following:

1. Click **Control Center** > **Device Status** from the BreakingPoint Control Center menu bar.
2. Click **Active Group**.
3. Select the Active Group to which you would like to assign the ports.
4. Click the port(s) that you would like to reserve.

Note: A lock appears over the reserved port. All other ports are tagged with a small blue icon, denoting the port's Active Group. These ports, even though they have not been manually reserved by you, are reserved under your account.

Force Reserving a Blade

If another user has reserved the ports on a blade, you can force reserve all the ports on that blade by clicking any of the ports. During a force reserve, the computer alerts you that the ports are reserved by another user and asks if you want to force reserve all the ports on that blade. If you force reserve the port at this point, the computer reserves all the ports on that blade under your account.

Note: You cannot force reserve ports if there is a test or computer process running on any of the ports on the blade. This computer alerts you that there is a process running on that module.

You should check the port notes before you force reserve the port(s) because other system users may not want you to remove their port reservations. If available, the port notes will appear as a yellow note icon located next to the port.

As a best practice recommendation, you should add a port note to your reserved ports. For example, you may want to note that you will be running tests on these ports everyday between 14:00 and 16:00. This may prevent other users from removing your port reservations.

To force-reserve ports, do the following:

1. Click **Control Center** > **Device Status** from the BreakingPoint Control Center menu bar.
2. Click the port(s) that you would like to reserve.

   Note: You can only force reserve ports that do not have tests or computer processes running on them.

3. Click **Yes** when the dialog window appears, asking if you would like to force reserve all the ports in the module.

   Note: The port(s) that you clicked will show a locked icon, denoting that this port has been reserved by you. All other ports are tagged with a blue note icon, showing the active group to which the ports belong.

Simultaneously Reserving or Unreserving All Ports On A Blade

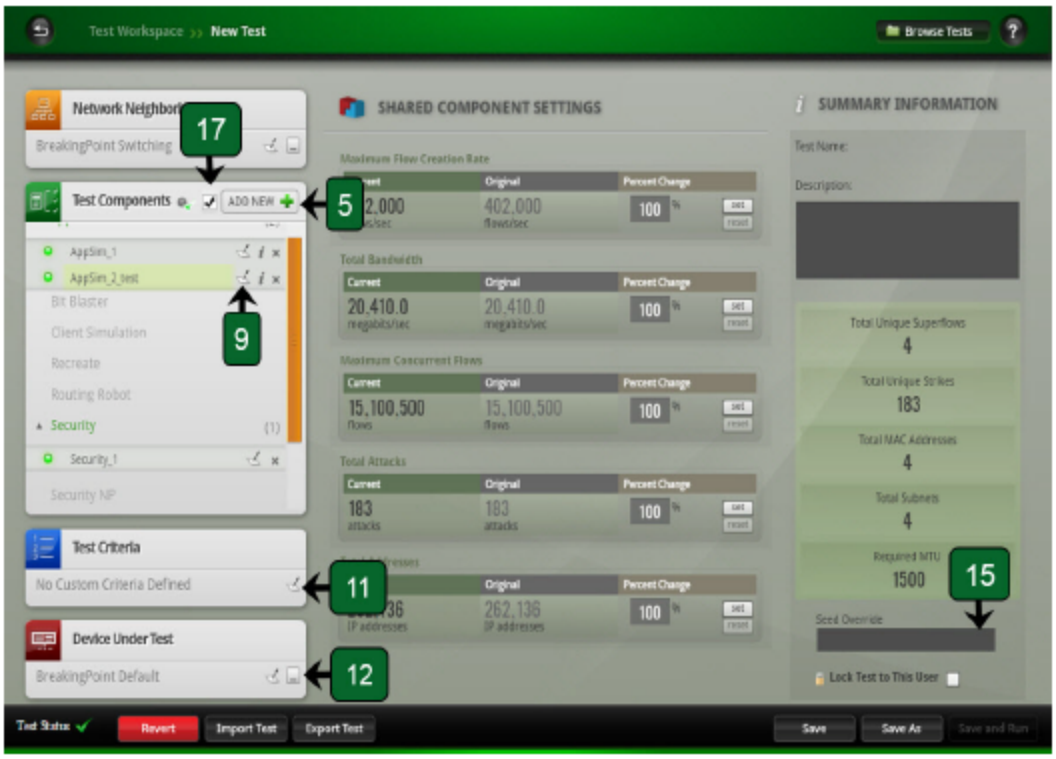
When you right-click a port, you can conveniently reserve or unreserve all ports on that slot without having to individually select them.

To simultaneously reserve or unreserve all ports on a blade, do the following:

1. Click **Control Center** > **Device Status** from the BreakingPoint Control Center menu bar.
2. Click the Active Group that you would like to use from the list.
3. Right-click the slot that has the ports, which you would like to reserve or unreserve.
4. Click **Reserve/Unreserve all ports on this slot**.

Task 10: Creating a Test

This section describes how to create a test from start to finish, which includes selecting the Network Neighborhood and DUT profile, adding a test component, configuring the test component, and running the test.



To create a test, do the following:

1. Click **Test** > **New Test** from the BreakingPoint Control Center menu bar.
2. Click **Select the DUT/Network** from the Test Quick Steps menu.
3. Select a DUT profile from the **Device Under Test(s)** list.

   Note: Click **Open device under test screen** to modify the DUT profile. After you have made your changes, click **Return** to go back to the DUT and Network Neighborhood selection screen. For more information on DUT profiles, see Task 7: Creating a Device Under Test Profile.

4. Select a Network Neighborhood from the **Network Neighborhood(s)** list.

   Note: Click **Open network neighborhood screen** to modify the Network Neighborhood. After you have made your changes, click **Return** to go back to the DUT and Network Neighborhood selection screen. For more information on Network Neighborhoods, see Task 8: Creating a Network Neighborhood.

5. Click **Accept** after you have made selections for the DUT profile and Network Neighborhood.
6. Click **Add a test component** from the Test Quick Steps menu.

7. Select the test component that you want to add to the test.
8. Do any of the following:

- Click the **Information** tab.
  - Type a new name for the test component in the **Name** box (optional).
  - Type a new description for the test component in the **Description** box (optional).
  - Select or clear the **Active** check box (optional).
  - Select or clear the **Include in Report** check box (optional).
  - Click **Apply Changes** when done.
- Click the **Interfaces** tab.
  - Select the interface(s) that will act as the client. The interface(s) that you select must be mapped to a port.
  - Select the interface(s) that will act as the server. The interface(s) that you select must be mapped to a port.
  - Click **Apply Changes** when done.
- Click the **Presets** tab.
  - Select a Component Preset.
  - Click **Apply Changes** when done.
- Click the **Parameters** tab.
  - Adjust any parameters for the test component.
  - Edit the Evasion Profile settings (optional, for the security component only).
  - Click **Apply Changes** when done.

9. Repeat the preceding three steps for each test component that you want to add to the test.
10. Click **Define Test Criteria** from the Test Quick Steps menu and create the pass and fail criteria for the test. For more information on pass and fail criteria, see the Test Pass/Fail Criteria section in the user guide.
11. Click **Save As**.
12. Type a name for the test in the **Name** box.
13. Click **Save and Run** from the Test Quick Steps menu to run the test.

This page intentionally left blank.

CHAPTER 4 Site and Safety Regulations

This section covers the following:

Site Requirements

Site requirements must be met before any type of electrical equipment can be installed at your location. Site requirements include the following:

- Rack Requirements
- Ventilation Requirements
- Environmental Requirements
- Power Requirements
- System Grounding Requirements
- Fiber-Optic Connection Requirements

Review the following site requirements before proceeding with the installation and configuration of FireStorm.

Rack Requirements

The FireStorm chassis should be installed in a standard 19 inch EIA rack cabinet. We do not recommend use of an equipment rack with side panels installed because of the horizontal airflow requirements of BreakingPoint 20.

If the weight of the equipment on the rack is not evenly distributed, there is a chance that the rack may tip over. Therefore, the rack needs to be properly anchored to an unmovable support system to prevent it from tipping over.

Load the rack from the bottom up, filling the lower racks with the heaviest components and the higher racks with the lightest components. This stabilizes the rack by evenly distributing the weight of the equipment on the rack.

The vertical spacing on the rack rails must meet the standard EIA-310C spacing requirements of 1 inch (2.54 cm). For more information on EIA-310C regulations, see Safety Regulations.

Ventilation Requirements

The FireStorm chassis contains a removable fan tray that pulls in cool air from the right side of the chassis and exhausts hot air on the left. There must be at least three inches of clearance at all of the ventilation openings to ensure that the chassis is properly ventilated.

Note: The FireStorm chassis will not power up without the fan tray installed. If one or more fans on the fan tray fail to operate at full speed, the computer will shut down and the fan tray must be replaced. If this occurs, contact BreakingPoint Support for further assistance.

Environmental Requirements

FireStorm must operate under the following environmental requirements:

- Operating environment: 15°C to 35°C (59°F to 95°F)
- Non-operating environment: -20°C to 70°C (-4°F to 158°F)
- Relative Humidity: 5 to 95%, non-condensing
- Altitude: No degradation up to 13,000 feet above sea level

Power Requirements

FireStorm may be operated on 110VAC (nominal) or 220VAC (nominal) input power. However, there are some restrictions when operating on 110VAC. The following table lists the configurations supported and the input current required for the chassis based on input voltage.

Input Voltage	Configuration	Input Current
90 – 120VAC	One 20 Blade	5.0A
90 – 120VAC	One 20 Blade + two 10Gb or 1Gb Blades	9.0A
200 – 240VAC	One 20 Blade	3.0A
200 – 240VAC	Two 20 Blades	5.7A
200 – 240VAC	Three 20 Blades	8.4A

Note that FireStorm may be operated on a 110VAC nominal power source as long as only one FireStorm blade is installed. Up to two BreakingPoint Storm blades may also be installed in this configuration. If a second 20 blade is installed with the computer powered from a 110VAC source, the second blade will not power up. If two or more 20 blades are in a chassis, the input power must be 200-240VAC.

For North American shipments, power cords are provided with the computer for both 110VAC and 220VAC connections. The 220VAC power cord includes a NEMA L6-20P plug and an adapter for NEMA L6-20P to NEMA 6-20P. International shipments include country-specific power cords.

System Grounding Requirements

Electrostatic Discharge (ESD) can occur if electronic components are improperly handled. ESD can cause intermittent or complete computer failure.

To prevent ESD from occurring, you should eliminate static generators (for example, plastic) and static conductors (for example, metal) from all areas that house electronic equipment or highly charged materials.

Note: Use proper ESD protection whenever handling any parts of FireStorm.

Fiber-Optic Connection Requirements

The SFP+ optical transceivers and fiber-optic connections are classified as Class 1 lasers. This means that exposure to the laser will not cause eye injury and are generally considered safe, however, we recommend that you do not look directly into the connectors.

The SFP+ optical transceivers from the Accessories Kit come with protective dust covers. You should install the protective dust covers over the transceivers to protect the optical data ports whenever they are not in use. If you remove the dust covers later on, ensure to properly store them so that you can easily find them again.

Note: Do not remove the SFP optical transceivers from the data ports. When these ports are not in use, keep the protective dust covers in them.

Safety Recommendations

This section covers the safety recommendations that you must read before installing or operating FireStorm. Keep in mind that any electronic equipment, like the chassis, can create a dangerous environment for employees and surrounding equipment if it is installed improperly.

By following the safety recommendations outlined in this section, you can reduce the likelihood of accidents and ensure the proper installation of FireStorm.

Our recommended safety instructions for handling, operating, and maintaining FireStorm are listed as follows:

- Keep the area around the chassis clear and dust-free during and after the installation.
- Only trained and qualified personnel should handle or service FireStorm.
- Wear safety glasses when working under any conditions that may be considered hazardous to your eyes.
- Use proper electrostatic discharge (ESD) protection when handling the blades or the chassis.
- Only trained and qualified personnel, who have thoroughly reviewed the FireStorm Installation Guide, should install, perform maintenance, or request service for the chassis.
- Do not touch uninsulated wires or terminals unless all cables and connections have been disconnected from the chassis.
- Do not remove the fan tray while FireStorm is powered on. Power the computer off and wait until the fans have stopped running before removing the fan tray from the computer.
- The chassis should be installed at least two feet above the ground.

Safety Regulations

The following table lists the safety regulations to which FireStorm is compliant:

Regulation	Description
CE Mark Certification	The CE mark certification indicates that a product meets the European Union's (EU) health, safety, and environmental requirements.
FCC Rules: Part 15, Class A	Part 15 of the FCC Rules stipulates that devices must not cause harmful interference to any radio services, and it describes the technical specifications and administration requirements for Part 15 devices. For more information on Part 15 of the FCC Rules, visit the FCC's website.
EIA-310-C Requirements	These requirements define the industry specifications for standard 19-inch equipment racks. The height is measured in units and each unit (U) on the rack is 1.75 inches.
UL-60950-1	This regulation describes the safety standards for low voltage information technology equipment. This standard specifies requirements intended to reduce risks of fire, electric shock, or injury to the operator or layman who may come into contact with the equipment.

CHAPTER 5 Installation Guide

This section covers the following:

Shipping Package Contents Overview

The shipping packages for FireStorm contains the following items:

- FireStorm Chassis Kit
  - 1 – Fan tray
  - 1 – Power tray
  - 1 – AC input cable
  - 4 – 10-32 x .75 pan screws
- FireStorm Blade Kit(s)
  - 4 – 10 Gb/1 Gb SFP+ optical transceivers (short-reach or long-reach)
  - 6 – 1 Gb copper SFP transceivers
  - 4 – 10’ short-reach or long-reach fiber optic cables (depending on transceiver selection)
  - 6 – 10’ CAT6 ethernet cables
  - 2 – DB9 serial cables
  - 1 – USB thumb drive containing the factory software image

Installation Overview

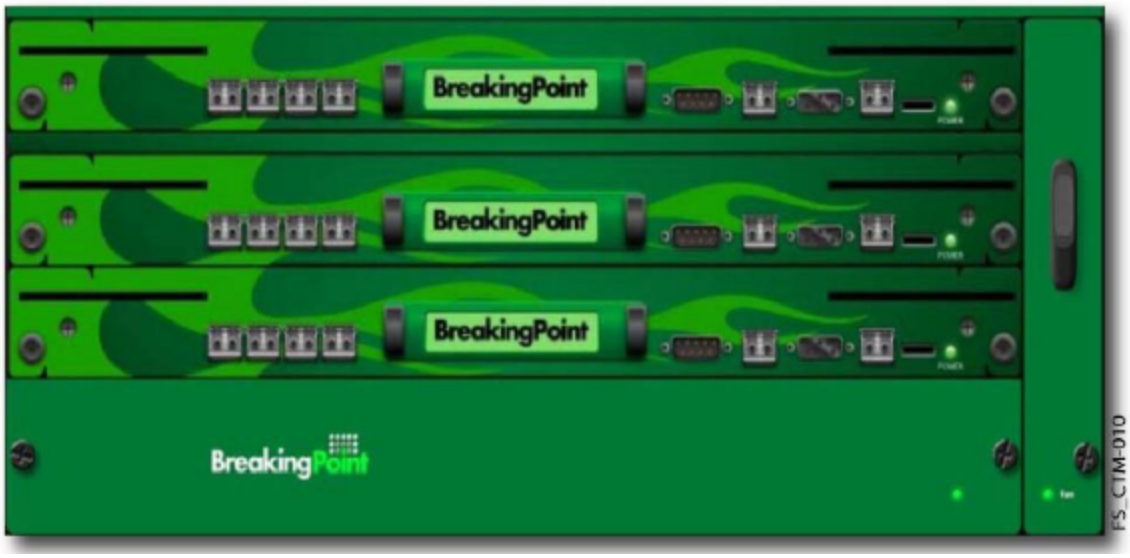
There are two parts to installing the chassis:

1. Mounting the chassis into an equipment rack.
2. Installing the blade(s) in the chassis.

Before installing the blade(s) into the chassis, we recommend that you mount the chassis into an equipment rack first.

After you have mounted the chassis into a rack, you can install the blade(s). The first blade must be installed into the bottommost slot of the chassis.

The following image shows the chassis with blades installed in all three slots:



Mounting FireStorm into an Equipment Rack

The following instructions describe how to mount FireStorm into a standard 19-inch equipment rack. If you require additional information for any other type of rack, see your rack vendor's documentation.

A rack unit (RU) is an industry-standard measurement for rack-mountable equipment. Each rack unit is equal to 1.75 inches and is comprised of three mounting holes. If you look at the rack's mounting rails, you will notice small markers that indicate each rack unit. For the FireStorm chassis, you will need 4 RU of rackspace.

Typically, you will need to count mounting holes upward, from the first mounting hole in the range of rack units needed to install the chassis.

Note: For safety purposes, we recommend that you mount FireStorm into an equipment rack before installing the blade(s). Additionally, to avoid injury or damaging the chassis, we recommend you to use three people to mount the chassis.

Guidelines to Keep in Mind

Before you mount the chassis to the equipment rack, ensure that the operating environment meets the criteria listed in the Site and Safety Regulations section.

Generally, this includes the following:

- Mounting the chassis in an area where air can properly circulate (at least three inches of clearance around all ventilation openings).
- Ensuring that the chassis has at least three feet of clearance in the rear so you can easily access the computer's power switch and inlet.
- Engaging the rack's stabilizers to keep it stable before mounting the chassis to the rack.
- Placing the chassis in a dry and dust-free area.
- Loading the equipment rack from the bottom up.
- Ensuring that the operating environment is 15°C to 35°C (59°F to 95°F)

Required Tools and Mounting Steps

To mount the FireStorm chassis, you will need the following tools:

- Phillips screwdriver

Use the following instructions to mount the FireStorm chassis to the 19-inch equipment rack from the front. This process requires at least three people.

To install FireStorm to a 19-inch equipment rack, do the following:

1. Using two people, one on each side of the chassis, lift the chassis.

   Note: With one hand, hold the bottom of the chassis, with the other, hold the back of the chassis for complete support of the computer.

2. Raise the chassis to the desired height in the equipment rack.

   Note: The chassis should be placed at least three feet above the ground to prevent dust particles from collecting inside the chassis.

3. Insert the chassis between the rack rails.
4. Align the four mounting holes on the chassis to the four mounting holes on the equipment rack.
5. Secure the unit by using the 10-32 x .75 supplied rack screws through the holes on the chassis and into the mounting rails on the equipment rack.

   Note: This step must be done by the third person, while the two other people are holding the chassis.

Installing the Blade

We recommend that you install the first blade into the bottommost slot of the chassis. If only one blade is installed in the chassis, it must be installed in the bottommost slot.

To install the blade, do the following:

1. Locate the card guide rails.
2. Place the blade onto the card guide rails.
3. Slide the card slowly into the slot until the front panel of the blade is about one inch from the chassis.

   Note: You may experience some resistance when you slide the blade into place, however, this is normal behavior.

4. Verify that the ejectors and thumb fasteners are aligned with the inner mounting rails on FireStorm.
5. Push the blade into place after you have verified that the ejectors and thumb fasteners are properly aligned.
6. Push the ejectors so that they lock the blade into place.
7. Tighten the thumb fasteners by turning them in a clockwise direction.
8. Insert an SFP+ optical transceiver into each data port.

9. Insert a copper SFP Ethernet transceiver into the management port of the blade in the bottommost slot.

> **Note:** Any unused optical transceiver must be covered with the rubber dust cover. This will prevent the optical data port from damage and protect your eyes from the Class 1 lasers.

Powering the Computer

Before connecting any power cables to the chassis, verify the following:

- The chassis has been securely fastened into an equipment rack.
- There is an AC power disconnect installed for the equipment rack, and it is easily accessible.
- The main AC power disconnect for the rack is properly labeled.
- All of the installation steps have been followed and all site and safety requirements have been met.
- All the power switches are in the off position.
- The chassis is being powered by a BreakingPoint V2 Power Supply Tray if there are multiple FireStorm blades in the chassis.

After you have verified all of this information, you may proceed to the instructions for powering the chassis.

To connect the power cables to the chassis, do the following:

1. Insert the female end of the supplied power cable into the power inlet, which is located on the back of the chassis.
2. Insert the male end of the cable into an AC outlet.
3. Turn the power switch to Reset.

After you have turned on the power for the chassis, you can proceed to the initial configuration for the computer. For more information, see Initial Configuration.

> **Note:** Do not remove the fan tray while FireStorm is powered on. Power the computer off and wait until the fans have stopped running before removing the fan tray from the computer.

> **Note:** A flashing Power Supply LED indicates that you do not have the proper power configuration to power the blades in slot 1 or slot 2. Multiple FireStorm blades in a single chassis require a BreakingPoint V2 Power Supply Tray. If you are installing multiple FireStorm blades into a single chassis, ensure that your chassis is being powered by a BreakingPoint V2 Power Supply Tray.

Connecting a Device Under Test to FireStorm

After mounting and configuring FireStorm, you can connect your device(s) under test to the computer.

> **Note:** The computer can be powered on when you connect the device under test to FireStorm.

To connect a device under test to the chassis, do the following:

1. Locate a free data port on the chassis.
2. Connect one end of a supplied fiber-optic cable to the data port.
3. Connect the other end of the fiber-optic cable to a port on the device under test.
4. Repeat the preceding three steps for any additional optical data port connections.

This page intentionally left blank.

CHAPTER 6 System Configuration

This section covers the following:

Initial Configuration

During an initial configuration, set up the IP address, netmask, and gateway for BreakingPoint 20. Additionally, during this process, create a user account that you can use to log on to the Control Center.

Note: FireStorm does not assign privilege levels to any accounts. Therefore, all accounts have the same access rights.

Connect the management ports through a serial or ethernet connection to your network. For a serial connection, use 115,200 8N1 on your terminal application. For an ethernet connection, FireStorm attempts to obtain a DHCP address. If it cannot acquire an address, it uses FireStorm's default settings: IP address 10.10.10.10, netmask 255.255.255.0, and default gateway 10.10.10.1.

When you first access the computer, FireStorm guides you through the initial configuration.

To start the initial configuration, do the following:

1. Accept the end user license agreement.
2. Type a fully qualified domain name in the **FQDN** box.
3. Type the IP address that you want to assign to FireStorm in the **IP Address** box.
4. Type a netmask in the **Netmask** box.
5. Type the gateway address in the **Gateway** box.
6. Type the primary DNS IP address in the **Primary DNS** box.
7. Type the secondary DNS IP address in the **Secondary DNS** box.
8. Type the tertiary DNS IP address in the **Tertiary DNS** box.
9. Press **Tab** to move to **Next** and press the **Enter** key.
10. Type your user name in the **Username** box.
11. Type your name in the **Name** field.
12. Type your email address in the **Email** box.
13. Type your password in the **Password** box.
14. Type your password again in the **Confirm Password** box.

15. Press **Tab** to **Finish** and press the **Enter** key. You will receive a message that the computer is completing the configuration. Wait for the configuration process to complete.
16. To access the Control Center, type the IP address that you used in step 3 into the URL bar of your browser.

    Note: After upgrading or reverting to any release of FireStorm, you must clear your cache and refresh your browser.

17. Click **Start BreakingPoint Systems Control Center** in the **Start** Page.
18. Type the user name that you created in step 10 in the **Username** box.
19. Type the password that you created in step 13 in the **Password** box.

    Note: Passwords are case sensitive.

    Note: Access may require installation of the latest Adobe Flash player.

20. Click Login.

    Note: The computer allows three invalid logins. If invalid login information is entered on the fourth attempt, the login window will lock you out. Refresh your browser to unlock your accounts.

Factory Revert

A factory revert rolls the computer back to the build (factory build) that was initially installed on it and reverts it back to its factory state. As a result, all settings, tests, and data stored on the computer are removed.

To perform a factory revert, do the following:

1. Locate the USB thumb drive that was included with the FireStorm accessory kit.
2. Insert the thumb drive into the USB port of the blade installed in the bottommost slot of the chassis.
3. Go to the Administration screen and click **Restore**.
4. Click ExternalDrive/USB/eSata, and then click **Fetch Backups**.
5. Locate and click the file named Factory Image.
6. Click **Restore** to start the factory revert.

   Note: All previous settings, stored tests, and reports are wiped out by the factory revert process. The revert process typically takes 10 to 15 minutes.

7. Using one of the provided serial cables, connect a computer running a terminal interface program to the DB9 management port on the front of FireStorm.
8. Wait for the status LED to turn green.
9. Press **Return**. The End User License Agreement screen appears on the serial console. You can then go through the steps listed in Initial Configuration.

CHAPTER 7 Accessing the Control Center

This section describes how to access the Control Center.

You can access the Control Center after you have configured FireStorm. When you access the Control Center, the first page that opens is the BreakingPoint Systems **Start** page. From the **Start** page, you can download the TCL shell, view the online Help, find BreakingPoint Systems contact information, and open the Control Center user interface.

Note: To access the Control Center, you must have a web browser with Adobe Flash installed and pop-ups turned on as well as the host address of the BPS Management Port.

Note: We recommend clearing your cache and refreshing your browser after upgrading or reverting to any release of FireStorm.

To access the Control Center, do the following:

1. Open a Web browser.

   Note: The browser must support Adobe Flash version 10.0 and have JavaScript turned on.

2. Type the host address for the BPS Management port in the **Address** bar.

   Note: The default address is http://10.10.10.10, however, the host address may have changed during the initial configuration of the computer. Contact the System Administrator for the current host address.

3. Click **Start BreakingPoint Control Center** in the BreakingPoint Systems main page. A new window appears and opens the Control Center login page.
4. Type the login ID in the **Login ID** box.

   Note: Login IDs are case sensitive.

5. Type the password in the **Password** box.
6. Click **Login**.

   Note: The computer allows three invalid logins. If you type invalid login information on the fourth attempt, the login window will lock you out. Refresh the browser to unlock your accounts.

   Note: The email address can use the following special characters: underscores, hyphens, periods, and spaces.

7. Click **Add User ('+')**.

This page intentionally left blank.

CHAPTER 8 Frequently Asked Questions

This section provides answers to some of the most frequently asked questions. If you have any questions that you would like added to this section, send them to techpubs@breakingpoint.com.

Account Questions

Question: I have had four invalid login attempts to the Control Center, and my account is now locked. How do I unlock my account?

Answer: Close the **Control Center** window and open a new browser window.

Question: How do I reset my Control Center account password?

Answer: You can have another user log on to the Control Center to reset your password. You can log on to the BPS management port to reset the password, or you can telnet to the computer's management IP address to reset the password.

Addressing Questions

Question: How do I configure the computer to use one MAC address per host?

Answer: If you edit the Network Neighborhood selected for your test, you can select 'Host' as the type for the domain. This will allot one MAC address per host. Selecting 'Virtual Router' uses one MAC address total for all traffic from that subnet.

Question: Why would I want to use one MAC address for all hosts?

Answer: A device has limited memory dedicated to its ARP table. If it takes too long for the ARP table to populate, the device may run out of buffer packets for that host and drop packets. So, you will want to use the 'Virtual Router' option when using more addresses than the device's ARP table is capable of handling. Otherwise, entries are dropped before they need to be used.

Question: Can NAT be used across multiple test components?

Answer: No. Only one test component can use a domain that has NAT turned on. Any domain that has NAT tuned on cannot be shared between test components.

Question: How many subnets can I add to a domain?

Answer: The number of subnets that can be added depends on the type of subnet you are defining. Each domain can contain one non-VLAN subnet. Each additional subnet must have a VLAN ID assigned to it. So, theoretically, the limit is 4,095, because you can assign VLAN IDs from 1-4,095.

Question: How do I assign one IP address per subnet?

Answer: If you edit the Network Neighborhood selected for your test, you can turn off the **Use Address Range** option and type the single IP address that you want to use in the **Minimum Range** field.

Question: What type of Network Address Translation (NAT) is supported?

Answer: Source NAT, also known as Traditional NAT, Outbound NAT, or Unidirectional NAT.

Question: Do you support Destination NAT?

Answer: No.

Question: Can I send and receive traffic on the same interface?

Answer: Yes. You can send and receive traffic on the same interface if you assign the interface a domain that has VLAN-tagging turned on.

Bandwidth Questions

Question: How do I define the maximum throughput for each test interface?

Answer: The maximum throughput is defined by using the **Date Rate** parameters. This parameter is defined per test component, and it is the upper-bound rate for each interface, which means that the interface will never send more traffic than the value specified. For the session-based components, you can define the scope of the data rate, which enables you to set the maximum data rate per interface, or set the aggregate data rate for the entire test component.

Question: What is the maximum throughput for each interface?

Answer: The maximum throughput is determined by the link speed of the device connected to the appliance. FireStorm allows up to 10 Gbps on the 10 Gb blades and 1 Gbps on the 1 Gb blades.

Question: How do I determine how much bandwidth each test component is using?

Answer: The computer has a test status verification feature that tells you whether or not the test components have exceeded the maximum allowed bandwidth for each interface. For example, if you capture 500 Mbps of traffic on Interface 1, the corresponding Recreate test estimates that the data rate

is 500 Mbps for both the transmitting and receiving interfaces. To set the data rate to be an aggregate sum for the test component, set the **Data Rate Scope** parameter to **Limit Aggregate Throughput**.

Question: What is the maximum bandwidth usage for a test interface?

Answer: For test components that send bidirectional traffic, such as Session Sender, Application Simulator, and Recreate, the value defined for Frame Rate Distribution sets the upper bound limits for bandwidth usage per interface. However, the aggregate sum of the traffic sent by each interface fluctuates between the data rate shared between both testing interfaces. For example, if you have a Session Sender test that uses 500 Mbps, the test never sends more than 500 Mbps from an interface, however, the sum of traffic sent by both interfaces fluctuates between 500 Mbps and 1000 Mbps.

System Questions

Question: What are the power requirements for FireStorm?

Answer: See the table in Power Requirements.

Question: What is the manufacturer MAC address for the BPS Management port?

Answer: 00:1A:C5

Question: Does the computer support ephemeral ports or application specification modifications that are required to match the application data to the IP and TCP/UDP headers?

Answer: No. This functionality is currently not supported.

Question: Can multiple users use the computer?

Answer: Yes. Multiple users can be logged on to the computer at the same time and multiple tests, Tcl scripts, and packet captures can be run simultaneously.

Question: What is the difference between a factory revert and a previous revert?

Answer: A factory revert rolls the computer back to the build that was initially installed on it (that is, the factory build) and reverts it back to its factory state. Therefore, all settings, tests, and data stored on the computer are removed. A previous revert rolls the computer back to the build that was previously installed on your computer.

Question: What is the difference between a soft reboot and a restart?

Answer: A soft reboot will restart the software processes, whereas restart will power-cycle the box.

Question: When would I use the **Preload for slower connections** command on the **Login** page?

Answer: Use the **Preload for slower connections** command if your connection is slow. Pressing this button prefetches the application assets and places them into the browser's cache. This reduces the amount of time it takes for the application to load. When you clear your browser's cache, press the **Preload for slower connections** button again on subsequent logins.

Question: How do I know when an OS update or ATI Update is available?

Answer: If you have automatic updates turned on, the computer alerts you that an update has been downloaded after you log on to the Control Center. However, if you do not have automatic updates turned on, you will need to check the Ixia support website at: https://support.ixiacom.com > **Software Downloads** > **BreakingPoint Software**.

Question: What ports do I need to be open to allow me to manage the computer?

Answer: You will need to have the following ports available: 80, 443, 8880, and 843.

Question: My computer status says 'System Not Operational.' What should I do?

Answer: There are two cases when this may occur: soon after a computer has been rebooted, or after the computer has not been rebooted for an extended period of time. Typically, after you reboot your computer, you should wait at least five minutes before running a test. If you try to run a test before this time, the computer may show this error. To resolve this error in either case, click **Control Center** > **Administration** from the menu bar, click **Restart** to reboot your computer, and wait at least five minutes before using the computer.

Question: Where is the diagnostics file?

Answer: You can download the diagnostics file from the **Start** page. If you click **Diagnostics**, you are prompted to save a ZIP file to your computer. The zip file contains the diagnostics files for the computer.

Troubleshooting Questions

Question: What should I do if the fan stops running?

Answer: First, power off the computer. After the computer is completely off, remove the fan tray from its module, and reseat the fan by reinserting it into the module again. After you have reseated the fan tray, power the computer on. If this does not resolve your issue, contact BreakingPoint Support.

Question: When should I remove the power tray?

Answer: You can remove the power tray if you are experiencing problems with the power supply and need to ship the power tray to BreakingPoint Systems.

Update Questions

Question: I just installed the latest OS update, however, I could not reconnect. What should I do?

Answer: Clear your cache and refresh the browser.

Question: Where can I download the latest software updates and ATI updates?

Answer: You can download all updates from the Ixia website at: https://support.ixiacom.com > **Software Downloads** > **BreakingPoint Software**.

Question: How will I know that an update is available?

Answer: If you have automatic updates turned on, the computer alerts you that an update file has been downloaded to your box. If you do not have automatic updates turned on, you will have to periodically visit the Ixia support website to check for new releases.

Question: I have automatic updates turned on. Does this install the update for me?

Answer: No. Automatic updates only downloads the update file. You will need to log on to the Control Center to install the update.

Question: How are the OS update files named?

Answer: Update files use the format X-N.bps. The X refers to the oldest version that you can upgrade from, and the N refers to the update file's version.

Question: Will ATI updates update my existing Strike Lists with the latest Strikes?

Answer: All ATI updates populate Smart Strike Lists with current strikes. You must manually update Standard Strike Lists after applying any ATI upgrade.

This page intentionally left blank.

APPENDIX A Safety Instructions

This appendix describes the various unit safety instructions in English and French.

SAFETY INSTRUCTIONS (English)

 **CAUTION: Safety Instructions**

Use the following safety guidelines to help ensure your own personal safety and to help protect your equipment and working environment from potential damage.

SAFETY: General Safety

 **CAUTION**

The power supplies in your system may produce high voltages and energy hazards, which can cause bodily harm. Only Ixia service technicians are authorized to remove the cover and access any of the components inside the system.

 **CAUTION**

To reduce the risk of electrical shock, a trained service technician must disconnect all power supply cables before servicing the system.

Note: The installation of your equipment and rack kit in a rack cabinet has not been approved by any safety agencies. It is your responsibility to ensure that the final combination of equipment and rack complies with all applicable safety standards and local electric code requirements. Ixia disclaims all liability and warranties in connection with such combinations. Rack kits are intended to be installed in a rack by trained service technicians.

When setting up the equipment for use:

- Place the equipment on a hard, level surface.
- Leave 5.1 cm (2 in) minimum clearance on all vented sides of the equipment to permit the airflow required for proper ventilation. Restricting airflow can damage the equipment.
- Ensure that nothing rests on your equipment's cables and that the cables are not located where they can be stepped on or tripped over.

- Keep your equipment away from radiators and heat sources.

  Keep your equipment away from extremely hot or cold temperatures to ensure that it is used within the specified operating range.
- Do not stack equipment or place equipment so close together that it is subject to re-circulated or preheated air.

When operating your equipment:

 **CAUTION**: Do not operate your equipment with the cover removed.

- Use this product only with approved / certified equipment. Operate this product only with approved /certified redundant power supplies.
- Operate the equipment only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- Use only approved power cable(s). If you have not been provided with a power cable for the equipment or for any AC-powered option intended for the equipment, purchase a power cable that is approved for use in your country. The power cable must be rated for the equipment and for the voltage and current marked on the equipment's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the equipment.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- To help prevent electric shock, plug the equipment's power cable into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Ensure that the total ampere rating of all equipment plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- If any of the following conditions occur, unplug the equipment from the electrical outlet and replace the part or contact Ixia:
  - The power cable, extension cable, or plug is damaged.
  - An object has fallen into the equipment.
  - The equipment has been exposed to water.
  - The equipment has been dropped or damaged.
  - The equipment does not operate correctly when you follow the operating instructions.
- Do not operate the equipment within a separate enclosure unless adequate intake and exhaust ventilation are provided on the enclosure that adheres to the guidelines listed above.
- Do not restrict airflow into the equipment by blocking any vents or air intakes.
- Do not push any objects into the air vents or openings of your equipment. Doing so can cause fire or electric shock by shorting out interior components.

 **CAUTION**:

Only Ixia trained service technicians are authorized to replace the battery. Should the battery need to be replaced, please contact Ixia to arrange for the replacement of the battery. Incorrectly installing or using an incompatible battery may increase the risk of fire or explosion. Replace the battery only with the same or equivalent type recommended by the manufacturer, carefully following installation instructions. Dispose of used batteries properly.

SAFETY: Battery Disposal


Your system uses a lithium coin-cell battery. These batteries are long-life batteries, and it is very possible that you will never need to replace them. However, should you need to do so, please contact Ixia to arrange for the replacement of the battery.

Do not dispose of the battery along with ordinary waste. Contact your local waste disposal agency for the address of the nearest battery deposit site.

Handle batteries carefully. Do not disassemble, crush or puncture batteries. Do not short external contacts, dispose of batteries in fire or water, or expose batteries to temperatures higher than 60 degrees Celsius (140 degrees Fahrenheit). Do not attempt to open or service batteries. Replace batteries only with batteries designated for the equipment.

SAFETY: Risk of Electrical Shock


CAUTION:

Opening or removing the cover of this equipment may expose you to risk of electrical shock. Components inside these compartments should be serviced only by an Ixia service technician.

Allow the equipment to cool before removing add-in modules. Add-in modules may become very warm during normal operation. Use care when removing add-in modules after their continuous operation.

To help avoid the potential hazard of electric shock, do not connect or disconnect any cables or perform maintenance or reconfiguration of your equipment during an electrical storm.

SAFETY: Equipment with Laser Devices


CAUTION:

Do not look directly into a fiber-optic transceiver or into the end of a fiber-optic cable. Fiber-optic transceivers contain laser light sources that can damage your eyes.

This equipment may contain optical communications transceivers which have built-in laser devices. To prevent any risk of exposure to laser radiation, do not disassemble or open any optical transceiver assembly for any reason.

Protecting Against Electrostatic Discharge

 **CAUTION**:

Disconnect product from mains power source in accordance with product-specific safety information located in this manual.

Electrostatic discharge (ESD) events can harm electronic components. Under certain conditions, ESD may build up on your body or an object and then discharge into another object, such as your add-in modules. To prevent ESD damage, you should discharge static electricity from your body before you handling add-in modules.

You can protect against ESD and discharge static electricity from your body by touching a metal grounded object before you interact with anything electronic. When connecting other devices to this equipment, you should always ground both yourself and the other device before connecting it to this equipment.

You can also take the following steps to prevent damage from electrostatic discharge:

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component. Just prior to unwrapping the antistatic package, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all electrostatic sensitive components in a static-safe area. If possible, use antistatic floor pads and work bench pads.

SAFETY INSTRUCTIONS (French)

 **AVERTISSEMENT**: Instructions relatives à la sécurité

Veuillez suivre les directives de sécurité suivantes afin d’assurer votre sécurité personnelle et de protéger votre équipement et votre environnement de travail contre les dommages potentiels.

SÉCURITÉ : Sécurité générale

 **AVERTISSEMENT**:

les sources d’alimentation de votre système peuvent produire une tension élevée et des dangers électriques qui peuvent causer des blessures corporelles. Seuls les techniciens de service d’Ixia sont autorisés à retirer le couvercle et à accéder aux composants à l’intérieur du système.

 **AVERTISSEMENT**:

Afin de réduire le risque de choc électrique, un technicien de service formé devra débrancher tous les câbles d'alimentation avant d'effectuer l'entretien sur le système.

REMARQUE:

'l'installation de votre équipement et de votre ensemble de bâti dans une armoire n'a été approuvée par aucune agence de sécurité. Il vous incombe d'assurer que la combinaison finale d'équipements et de bâtis soit conforme à toutes les normes de sécurité applicables et aux exigences du code local en matière d'électricité. Ixia décline toute responsabilité et toutes les garanties relatives à de telles combinaisons. Les ensembles de bâtis sont prévus pour être installés par un technicien de service formé.

Lors de l'installation de l'équipement aux fins d'utilisation:

- Placer l'équipement sur une surface dure et à niveau.
- Laisser un espace d'au moins 5.1 cm (2 po) sur tous les côtés de l'équipement dotés de fentes d'aération afin de permettre la circulation d'air nécessaire à une bonne ventilation. L'entrave à la circulation d'air peut endommager l'équipement.
- S'assurer que rien ne se trouve sur les câbles de l'équipement et que les câbles ne se trouvent pas dans un endroit où on pourrait marcher ou trébucher sur eux.
- Tenir l'équipement éloigné des radiateurs et autres sources de chaleur.
- Ne pas exposer l'équipement à des températures extrêmement chaudes ou froides afin d'assurer qu'il soit utilisé dans la plage de fonctionnement spécifiée.
- Ne pas empiler l'équipement ni placer ses composants si près les uns des autres qu'ils risquent d'être exposés à de l'air de recirculation ou préchauffé.

Lors de l'utilisation de votre équipement:

AVERTISSEMENT: ne pas utiliser votre équipement avec le couvercle retiré.

- Utiliser ce produit uniquement avec des équipements approuvés/certifiés. Faire fonctionner ce produit uniquement avec des 'alimentations redondantes approuvées/certifiées.
- Faire fonctionner l'équipement uniquement avec le type d'alimentation externe indiqué sur l'étiquette des caractéristiques électriques. 'En cas de doute quant au type d'alimentation requis, consulter votre prestataire de services ou la compagnie d'électricité locale.
- Utiliser uniquement des câbles d'alimentation approuvés. Si on ne vous a pas fourni de câble d'alimentation pour l'équipement ou pour toute autre option alimentée au CA prévue pour l'équipement, acheter un câble d'alimentation approuvé pour utilisation dans votre pays. Le câble d'alimentation doit être conforme aux caractéristiques nominales de l'équipement, ainsi qu'aux valeurs nominales de tension et de courant indiquées sur l'étiquette des caractéristiques électriques de l'équipement. Les valeurs nominales de tension et de courant du câble doivent être supérieures à celles indiquées sur l'équipement.
- Ne pas modifier les câbles d'alimentation ou les fiches. Consulter un électricien agréé ou votre compagnie d'électricité pour toute modification du site. Systématiquement respecter les règles locales/ nationales en matière de câblage.

- Pour prévenir les chocs électriques, brancher les câble d'alimentation de l'équipement dans des prises électriques mises à la terre correctement. Ces câbles sont dotés de fiches à trois branches afin d'assurer une mise à la terre adéquate. Ne pas utiliser de fiches d'adaptation ni retirer la broche de mise à la terre d'un câble. Si 'une rallonge doit absolument être utilisée, utiliser un câble à trois fils doté de fiches de mise à la terre adéquates.
- Respecter les caractéristiques nominales 'de la rallonge et de la barrette d'alimentation. S'assurer que l'ampérage nominal total de tous les équipements branchés 'à la rallonge ou à la barrette d'alimentation n'excède pas 80 pour cent de l'ampérage nominal maximal 'de la rallonge ou de la barrette d'alimentation.
- Si l'une des situations suivantes se produit, débrancher l'équipement de la prise de courant et remplacer la pièce ou contacter Ixia:
  - Le câble d'alimentation, 'la rallonge ou la fiche est endommagé.
  - Un objet est tombé dans l'équipement.
  - L'équipement a été exposé à de l'eau.
  - L'équipement est tombé ou a été endommagé.
  - L'équipement ne fonctionne pas correctement quand vous suivez les consignes d'utilisation.
  - Ne pas utiliser l'équipement dans une enceinte séparée à moins qu'une ventilation d'entrée et de sortie d'air adéquate soit fournie sur cette enceinte en conformité avec les directives indiquées ci-dessus.
  - Ne pas "entraver l'arrivée d'air dans l'équipement en bloquant les fentes d'aération ou les entrées d'air.
  - Ne pas introduire d'objets dans les fentes 'd'aération ou ouvertures de votre équipement au risque de causer un incendie ou un choc électrique à la suite d'un court-circuit des composants internes.

 **AVERTISSEMENT**:

seuls les techniciens de service formés d'Ixia sont autorisés à remplacer la pile. Si la pile doit être remplacée, contacter Ixia pour prendre les dispositions nécessaires au remplacement de la pile. L'installation incorrecte ou l'utilisation d'une pile incompatible peut augmenter le risque d'incendie ou d'explosion. Remplacer la pile uniquement par un type de pile identique ou équivalent conformément aux recommandations du fabricant et suivre les consignes d'installation à la lettre. Correctement éliminer les piles usées.

SÉCURITÉ : Élimination des piles

 Votre système utilise une pile bouton au lithium. Ces piles sont à longue durée et il est très possible que vous n'ayez jamais à les remplacer. Toutefois, si jamais vous deviez le faire, veuillez contacter Ixia pour prendre les dispositions nécessaires au remplacement de la pile.

Ne pas éliminer la pile avec les ordures ménagères. 'Contacter l'agence locale chargée de l'élimination des déchets pour obtenir l'adresse du site de collecte de piles le plus proche.

Manipuler les piles avec précaution. Ne pas démonter, écraser ou percer les piles. Ne pas court-circuiter les contacts externes, éliminer les piles dans le feu ou l'eau, ni exposer les piles à des températures supérieures à 60 degrés Celsius (140 degrés Fahrenheit). Ne pas essayer d'ouvrir ou de 'réparer les piles. Remplacer les piles uniquement avec les piles désignées pour l'équipement.

SÉCURITÉ : Risque de choc électrique

 **AVERTISSEMENT**:

ouvrir ou retirer le couvercle de cet équipement peut vous exposer à un risque de choc électrique. Les composants à l'intérieur de ces compartiments doivent être entretenus exclusivement par un technicien de service Ixia.

- Laisser l'équipement refroidir avant de retirer les modules additionnels. Les modules additionnels peuvent devenir très chauds lors du fonctionnement normal. Faire preuve de prudence lors du retrait de modules additionnels après un fonctionnement continu.
- Pour éviter le risque potentiel de choc électrique, ne pas connecter ou déconnecter les câbles, ni effectuer l'entretien ou la reconfiguration de votre système durant une tempête électrique.

SÉCURITÉ : Équipement doté de dispositifs laser

 AVERTISSEMENT:

ne jamais regarder directement dans un émetteur-récepteur à fibres optiques ou dans l'extrémité d'un câble à fibres optiques. Les émetteurs-récepteurs à fibres optiques contiennent des sources de lumière laser qui peuvent endommager vos yeux.

Cet équipement peut contenir des émetteurs-récepteurs de communication par fibre optique qui comportent des dispositifs laser intégrés. Pour prévenir tout risque d'exposition au rayonnement laser, ne jamais démonter ou ouvrir un émetteur-récepteur à fibres optiques.

Protection contre les décharges électrostatiques

 AVERTISSEMENT:

débrancher le produit de la source principale d'alimentation conformément aux informations de sécurité spécifiques au produit fournies dans ce manuel.

Les décharges électrostatiques peuvent endommager les composants électroniques. Dans certaines conditions, les décharges électrostatiques peuvent s'accumuler sur votre corps ou sur un objet, puis se décharger dans un autre objet comme vos modules additionnels. Pour prévenir les dommages dus aux

décharges électrostatiques, vous devez décharger l’électricité statique de votre corps avant de manipuler un module additionnel.

Vous pouvez assurer la protection contre les décharges électrostatiques et décharger l’électricité statique de votre corps en touchant un objet en métal mis à la terre avant ’de toucher quoi que ce soit d’électronique. Lors de la connexion d’autres dispositifs à cet équipement, vous devez toujours assurer votre mise à la terre et celle de l’autre dispositif avant de le connecter à cet équipement.

Vous pouvez aussi suivre les étapes suivantes afin de prévenir les dommages causés par les

décharges électrostatiques:

- Lors du retrait d’un composant sensible à l’électricité statique de son carton d’expédition, ne pas retirer le composant de son matériau d’emballage antistatique ’avant d’être prêt à installer ce composant. Juste avant de retirer l’emballage antistatique, ’veiller à décharger l’électricité statique de votre corps.
- Lors du transport d’un composant sensible, le placer préalablement dans un contenant ou un emballage antistatique.
- Manipuler tous les composants sensibles à ’l’électricité statique dans une zone à protection antistatique. Si possible, utiliser des tapis antistatiques pour le sol et la surface de travail.

APPENDIX B Hardware Specifications

This section details the hardware and software specifications for FireStorm.

Hardware Specifications

The following table details the hardware specifications for FireStorm:

Hardware Component	Specification
Model	FireStorm
Dimensions	Height: 7 inches (17.8 cm) Width: 17.4 inches (44.2 cm) Depth: 19.5 inches (49.8 cm) Shipping Weight: 45 lbs (20.4 kg) Rack Units: 4 RU
Dual Media Test Interfaces	4 - 10 Gb/1 Gb ethernet ports
Target Control Ports	1 - 10/100/1000 ethernet interface 1 - DB9 serial interface
BPS Management Ports	1 - 10/100/1000 ethernet interface 1 - DB9 serial interface
Power Requirements	100-240 V, 50/60 Hz Maximum power consumption: 1,800 Watts
Temperature Requirements	Operating: 15° C to 35° C (59° F to 95° F) Non-operating: -20° C to 70° C (-4° F to 158° F)
Humidity Requirements	Humidity: 5% to 95% relative humidity, non-condensing
Altitude Requirements	No degradation up to 13,000 feet

Software Specifications

The following table details the software specifications for FireStorm:

Software	Specification

Component	
Browser Client	Supported browsers: Adobe Flash (version 11.6.602.171) enabled browser (Internet Explorer 10), Mozilla Firefox 18, Chrome, and Safari (Mac) Not supported: Safari for Windows, and Safari 6.0.2 on Mac OS 10.8.2 Recommended minimum screen resolution: 1024 x 768 Minimum 2 Gb RAM
Telnet Client	Telnet client running VT100 emulation
Serial Client	Serial client running 115200/8/n/l/none

Light-Emitting Diodes

The light-emitting diodes (LEDs) status indicators are located on the front of FireStorm. See the following table for descriptions of each LED and what each LED color represents:

LED	Color	Status	Description
Link LED	Green	Operational	Link is present.
Active LED	Blue	Operational	Indicates that the link is ready to send and receive traffic.
	Blinking blue	Operational	Link is present and traffic is on the bus.
User LED	Multicolor	Operational	This LED indicates the user who has reserved the port.
Reserved LED	Multicolor	Operational	This LED indicates the port group to which the user belongs.
Power LED	Amber	Boot-up	Computer is booting up.
	Green	Operational	Computer is powered on and operating.
	Blinking Green	Busy	Insufficient power supply, a blade is not properly seated, or the computer is in update mode. Do not remove the hard drive when the Power LED is blinking.
	Blinking (Red/Green)	Busy	Insufficient power source to power on multiple FireStorm units. Disconnect one FireStorm or upgrade power source.
Power Tray LED	Green	Powered	Computer is powered on.
	Off	Not powered	Computer is powered off.
	Red	Boot-up	Power tray is booting up.

Fan LED	Green	Operational	Fan is on.
	Off	Not powered	Fan is powered off.
	Red	Boot-up	Fan is booting up.

Shipping Container Contents

The following table lists the contents of the shipping container:

Quantity	Item
1	FireStorm kit: 1 – FireStorm blade 1 – 2500 W V2 power supply 1 – Nameplate label (upgrade kit only) 1 – 240 VAC A/C power cable (110 VAC A/C power cable for countries with primary 110 VAC nominal power) 4 – SFP+ optical transceivers 6 – Copper 16b transceivers 6 – ethernet cables 4 – 10 GigE fiber optic cables 1 – USB thumb drive

CLI Commands

The following table lists the CLI commands available for the BPS Management port:

Command	Description	Sample Syntax
?	Print a list of commands	`?`
? <cmd>	Print help for a command	`? addUser`
addUser	Add a user to the computer	`addUser Joe Smith -name Joe -email joe@email.com`
exit	Exit the shell	`exit`
help	Print the list of commands with descriptions	`help`
help <cmd>	Print help for a command	`help addUser`
networkInfo	Retrieve network setup information	`networkInfo`

passwd	Change the password for the account logged on to the BPS Management port	`passwd`
reboot	Reboot the computer	`reboot`
removeUser	Delete a user account	`removeUser Joe`
updateNetwork	Configure a network interface	`updateNetwork -dhcp yes - hostname test.bpointsys.int - ip 10.10.10.123 - netmask 24 - gw 10.10.10.1`
updateNetwork	Switch ports on and off	`updateNetwork -http_ off value HTTP Off: <true> turns port 80 OFF`
updateUser	Modify a user account	`updateUser joe -name Joseph Smith -email joeS@email.com`
uptime	Display the computer's uptime	`uptime`
userInfo	Query a user's information	`userInfo joe`
version	Display the software version	`version`

Global Scripts Templates

Global scripts allow you do things like reboot your device, monitor DUT statistics, and create VLANs through firmware control. The following tables list the global scripts for available device types.

Dell PowerConnect 6024

The following table lists the global scripts for the Dell PowerConnect 6024 device type:

Script	Template

VLAN Trunk Create	Expect > Send enable\r Expect # Send conf \r Expect # Send vlan database\r Expect # Send vlan 1-12\r Expect # Send exit\r Expect # Send interface eth g2\r Expect # Send switchport mode trunk\r Expect # Send switchport trunkallowed vlan add 1-12\r Expect # Send exit\r Send exit\r
VLAN Create	Expect > Send enable\r Expect # Send conf \r Expect # Send vlan database\r Expect # Send vlan 1-12\r Expect # Send exit\r Expect # Send exit\r Expect #
VLAN Delete	Expect > Send enable\r Expect # Send conf \r Expect # Send vlan database\r Expect # Send no vlan 1-12\r Expect # Send exit\r Expect # Send exit\r Expect #

Extreme Summit 7i

The following table lists the global scripts for the Extreme Summit 7i device type:

Script	Template
VLAN Create	Send amdin\r Expect password: Send password\r Expect # Send create vlan test\r Expect # Send configure vlan test ipaddress 192.168.1.1/16\r Expect # Send exit\r Expect # Send exit\r Expect #
VLAN Delete	Send amdin\r Expect password: Send password\r Expect # Send delete vlan test\r Expect # Send exit\r Expect # Send exit\r Expect #
Trunk Create	Send amdin\r Expect password: Send password\r Expect # Send config dot1q ethertype 9100\r Expect # Send config jumbo-frame size 1530\r Expect # Send config vlan test tag 50\r Expect # Send config vlan test add port 1-4 untag\r Expect # Send config vlan test add port 31,32 tagged\r Expect # Send exit\r Expect # Send exit\r Expect #

HP ProCurve 7500yl

The following table lists the global commands available for the HP ProCurve 7500yl device type:

Script	Template
VLAN Delete	Send r\r Expect Password: Send password\r Expect # Send config t\r Expect # Send no vlan 2\r Expect # Send exit\r Expect # Send exit\r Expect #
VLAN Create	Send r\r Expect Password: Send password\r Expect # Send config t\r Expect # Send vlan 2\r Expect # Send exit\r Expect # Send exit\r Expect #

This page intentionally left blank.

INDEX

Ixia, a Keysight Business
26601 West Agoura Road
Calabasas, California 91302