FireStorm Installation Guide

Release 8.20, Dec. 2016

Corporate Headquarters	Ixia Worldwide Headquarters 26601 W. Agoura Rd. Calabasas, CA 91302 USA +1 877 FOR IXIA (877 367 4942) +1 818 871 1800 (International) (FAX) +1 818 871 1805 sales@ixiacom.com	Web site: www.ixiacom.com General: info@ixiacom.com Investor Relations: ir@ixiacom.com Training: training@ixiacom.com Support: support@ixiacom.com +1 818 595 2599 For the online support form, go to: http://www.ixiacom.com/support/inquiry/
BreakingPoint Systems	Ixia BreakingPoint Systems 3900 N. Capital of Texas Hwy., Ste. 180 Austin, TX 78746 USA +1 512 821 6000 info@breakingpoint.com	Web site: www.breakingpoint.com General: http://www.ixiacom.com/products Support: support-bps@ixiacom.com + 1 818 595 2599
EMEA	Ixia Technologies Europe Limited Part 2nd floor, Clarion House, Norreys Drive Maidenhead, UK SL6 4FL +44 (1628) 408750 FAX +44 (1628) 639916 salesemea@ixiacom.com	Support: eurosupport@ixiacom.com +40 21 3015699 For the online support form, go to: http://www.ixiacom.com/support/inquiry/?location=emea
Asia Pacific	Ixia Pte Ltd 210 Middle Road #08-01 IOI Plaza Singapore 188994	Support: Support-AsiaPac@ixiacom.com +65 6332125 For the online support form, go to: http://www.ixiacom.com/support/inquiry/
Japan	Ixia Communications KK Nishi-Shinjuku Mitsui Bldg 11F 6-24-1, Nishi-Shinjuku, Shinjuku-ku Tokyo 160-0023 Japan	Support: Support-Japan@ixiacom.com +81 3 5326 1948 For the online support form, go to: http://www.ixiacom.com/support/inquiry/
India	Ixia Technologies Pvt Ltd Tower 1, 7th Floor, UMIYA Business Bay Cessna Business Park Survey No. 10/1A, 10/2, 11 & 13/2 Outer Ring Road, Varthur Hobli Kadubeesanahalli Village Bangalore East Taluk Bangalore-560 037, Karnataka, India +91 80 42862600	Support: Support-India@ixiacom.com +91 80 49396400 For the online support form, go to: http://www.ixiacom.com/support/inquiry/?location=india

For viewing the FAQs related to the product, go to Ixia Technical Support Online:
https://ebsoprod.ixiacom.com/OA_HTML/jtflogin.jsp

About This Guide

Product Overview

Getting Started

Site and Safety Regulations

Installation Guide

System Configuration

Accessing the Control Center

Frequently Asked Questions

Appendix

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 using your BreakingPoint device.

Purpose

To provide safety regulations, site requirements, and installation instructions for the 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 **Table I-1 on page i**.

Table I-1: Document Conventions

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

Table I-1: Document Conventions

Convention	Description	Example
Note:	Helpful suggestion or reference to additional information	**Note:** Racks must meet standard EIA-310-C requirements.
Link	Clickable link that references tables, figures, sections, and cross-references.	See **Table 12** for more information.

Related Documentation

Table I-2 on page ii lists all of the documentation related to the FireStorm. All documentation can be accessed through the Documentation area of the Ixia website.

Table I-2: Related Documentation

Documentation	Description
FireStorm Installation Guide	Provides installation instructions and information for the 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 you must complete in order to migrate from the BreakingPoint Storm to the 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 firmware updates as well as industry information.

- Obtain the latest firmware releases for the 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.

Support

If a solution to a problem has not been found after consulting the related section in this guide, please contact Customer Support using one of the methods in Table I-3 on page iii.

To expedite a support issue, please have the following information available:

- Customer Number – Located on the Customer Support Agreement and on the shipping invoice for the FireStorm.
- Serial Number – Located on the shipping invoice for the FireStorm.
- Firmware Versions – Located from the Help Menu in the Control Center (select Help > About).

Table I-3: Support Methods

Method	Contact Information
E-mail	support-bps@ixiacom.com
Telephone	1-818-595-2599

Documentation Feedback

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

1 Product Overview

This section covers:

- FireStorm Overview
- FireStorm Hardware Overview
- Control Center Overview

FireStorm Overview

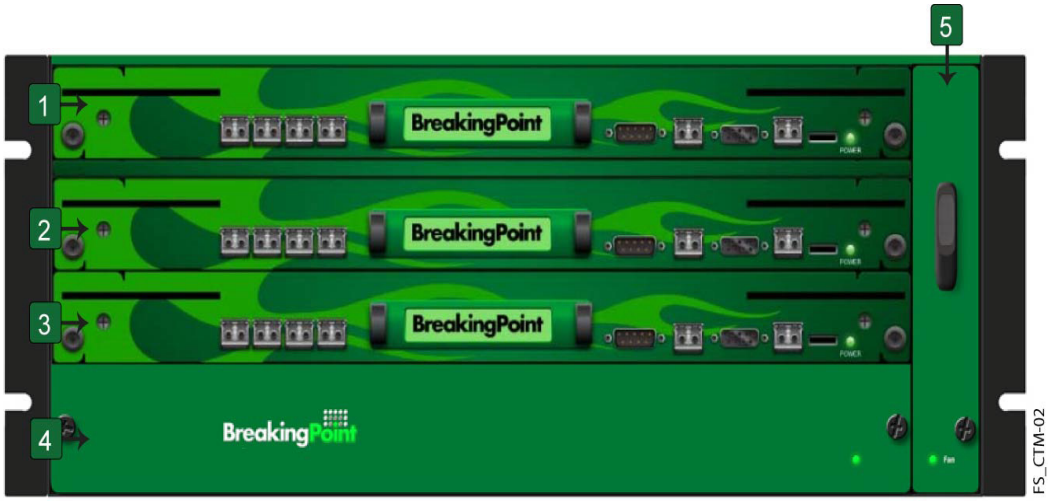
BreakingPoint Systems has developed a system that measures and hardens the resiliency of every component of your critical infrastructure against potentially crippling attacks and peak application traffic: the FireStorm. It is a 4 RU rack-mountable, modular system that can accurately recreate a live network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

The 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. The FireStorm can concurrently simulate TCP sessions, application traffic, and live security attacks, and ultimately, identify “breaking points” in your network devices.

FireStorm Hardware Overview

The FireStorm is comprised of five slots. **Figure 1-1 on page 1** highlights these slots with callouts.

Figure 1-1: FireStorm Slots



Callouts 1, 2 and **3** refer to the slots dedicated to high-speed data plane processors (or the blades) for the system. 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 system to a network and access it through an IP address. The target control ports allow you to automate testing for the device under test.

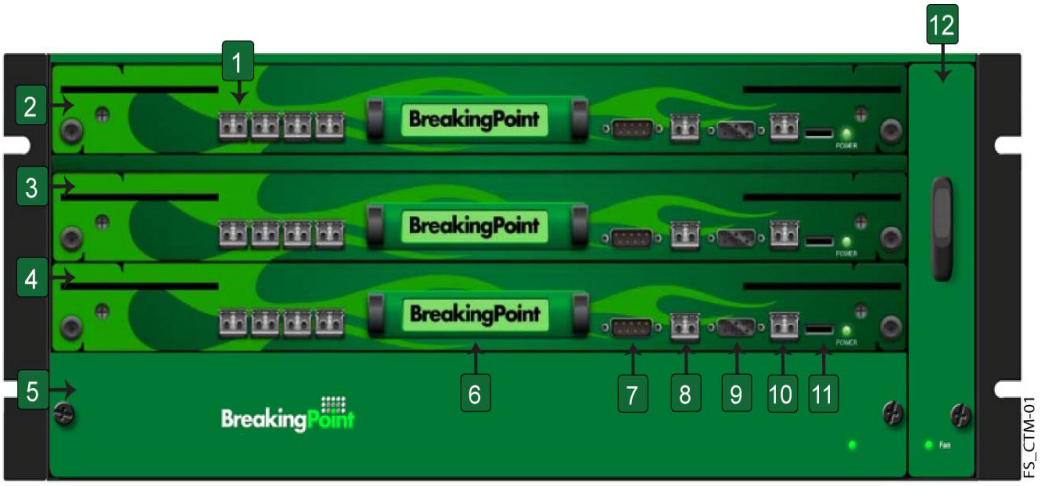
Callout 4 refers to the power tray, which contains the power supply for the system.

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

Front-view of the FireStorm

Figure 1-2 on page 2 illustrates the front of the FireStorm. Locate the corresponding callout in the table below for more information about each component.

Figure 1-2: FireStorm Front-view



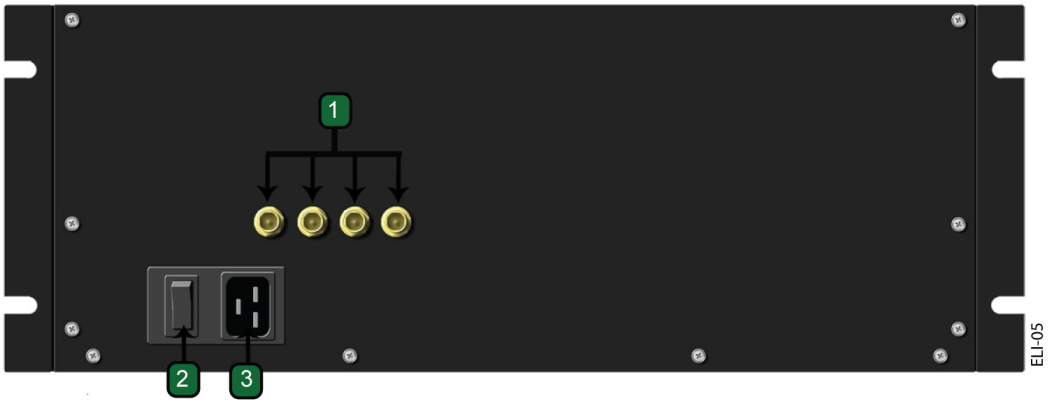
Callout	Component	Description
1	Data Ports	Transmits and receives traffic to and from the DUT.
2	Hard drive bay	Contains the hard drive enclosure.
3	Target Control Serial Port	Used to manage and configure settings for the DUT.
4	Target Control Ethernet Port	Used to manage and configure settings for the DUT.
5	BPS Management Serial Port	Manages the FireStorm configuration through a serial connection.

Callout	Component	Description
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 system.

Back-view of the FireStorm

The power inlet and power switch are located on the back of the chassis, as shown in **Figure 1-3 on page 3**. Additionally, there are BNC interfaces that you will be able to use in future releases to link together multiple chassis.

Figure 1-3: FireStorm Back-view



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 the FireStorm
3	Power Inlet	Power inlet for the FireStorm

Control Center Overview

The Control Center is a Web-based user interface where the testing environment can be created, tests can be run, and reports can be viewed. 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 enabled 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: BreakingPoint recommends that users of Internet Explorer use IE 10 or higher. IE 9 and earlier versions are not supported.

Enabling JavaScript

You must have JavaScript enabled to view the Control Center.

To enable JavaScript for Internet Explorer:

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

To enable JavaScript for Mozilla Firefox 2.0:

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

To enable JavaScript for Safari:

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

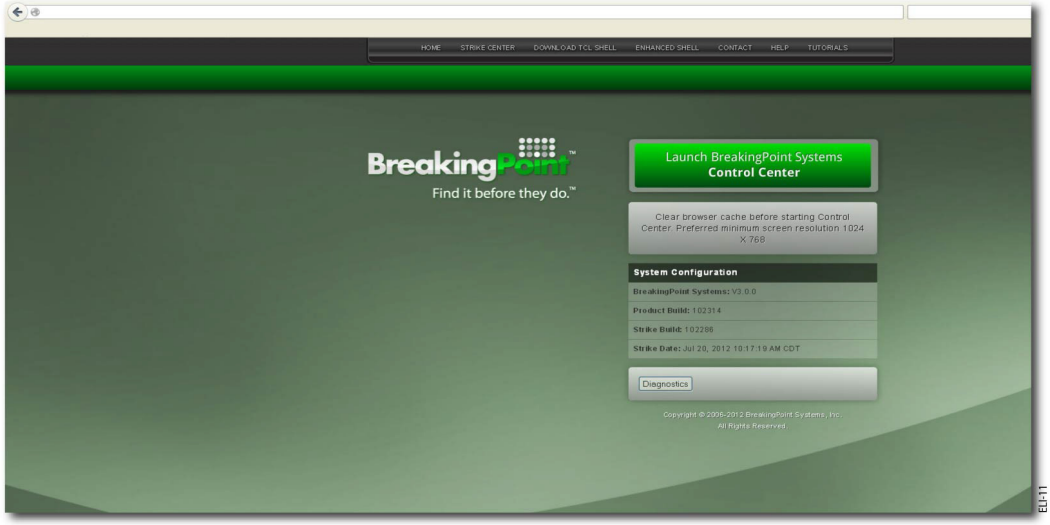
Accessing the Control Center

To access the Control Center, you must have a Web browser with the following items enabled or installed:

- Adobe Flash Player (version 11.6.602.171 or higher)
- 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.

Figure 1-4: BreakingPoint Start Page



To access the Control Center:

1. Open a Web browser.

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

   Note: The default address is http://10.10.10.10; however, the host address may have changed during the initial configuration of the system. You will need to contact the System Administrator for the current host address.

2. Enter the host address for the BPS Management port in the **Address** bar.
3. Click the **Launch BreakingPoint Systems Control Center** link on the Start Page.

   Note: The first time you attempt to login to the system, your browser will require you to verify a security exception in order to login. Follow the steps required by your browser to accept and verify the security exception. Once the security exception has been accepted and verified, you will be allowed to continue with the login process. A new window will open and display the Control Center login page.

4. Enter the login ID in the **Username** field.
5. Enter the password in the **Password** field.

   Note: Passwords are case sensitive.

6. Click the **Login** button.

The system allows three invalid logins. If invalid login information is entered on the fourth attempt, the login window will lock the user out. Users must refresh their browser to unlock their 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 **Figure 1-5 on page 6** for a tour of the interface.

Figure 1-5: Control Center Overview

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.

2 Getting Started

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

This section covers:
- Getting Started Overview
- 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 a User Account
- Task 6: Setting the Time and Date
- Task 7: Creating a Device Under Test Profile
- Task 8: Creating a Network Neighborhood
- Task 9: Making Port Reservations
- Task 10: Creating a Test

Getting Started Overview

Welcome to the Getting Started section of the *FireStorm Installation Guide*. This section will provide an overview of the tasks you must complete in order to install and configure the BreakingPoint device, as well as explain how to set up your test environment within the BreakingPoint Control Center.

Table 2-1 on page 7 lists the Getting Started tasks.

Table 2-1: 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 will briefly describe how to set up the BreakingPoint device.

To set up the BreakingPoint device:

1. Secure the chassis into an equipment rack. For more information on mounting the chassis, see the section **Mounting the BreakingPoint Storm into an Equipment Rack on page 32**.

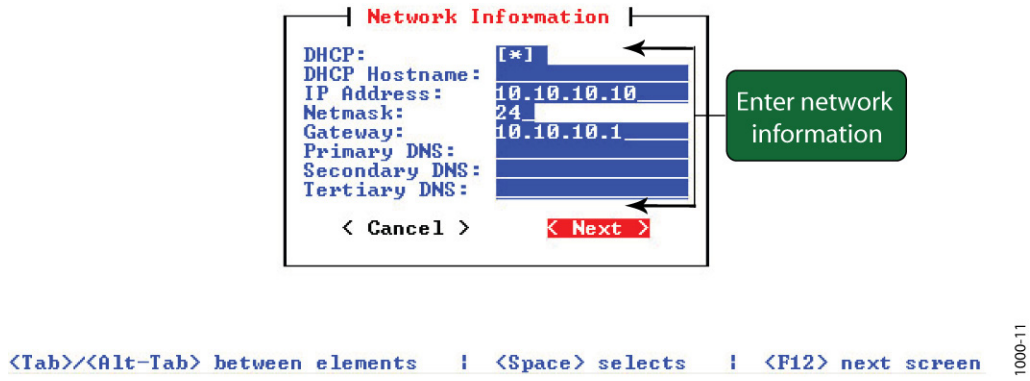
   Note: The chassis must be close enough to the device under test so that you can connect cables from the appliance to the device under test

2. Insert the system controller into the module above the power tray. For more information on installing the system controller, see the section **Installing the System Controller on page 34**.
3. Insert the blade(s) into the top two modules. For more information on installing the blade(s), see the section **Installing the Blade on page 34**.
4. Power the system. For more information on powering the system, see the section **Powering the System on page 35**.
5. Connect the device under test to the BreakingPoint device. For more information on connecting a device under test to the BreakingPoint device, see the section **Connecting a Device Under Test to the BreakingPoint Storm on page 35**.

Task 2: Configuring the BreakingPoint Device

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

Figure 2-1: Network Information Box



Telnet

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

To configure the BreakingPoint device using Telnet:

1. Open a telnet client (e.g., PuTTy, AlphaCom, etc.).
2. Telnet to the following host address: 10.10.10.10.
3. Specify your terminal emulation preference (e.g., ANSI, 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 disabled, users will be able to configure additional system routes from the BreakingPoint Control Center. If DHCP is enabled, the Routes area in the BreakingPoint Control Center will be disabled.

   - DHCP Hostname
   - IP Address
   - Netmask
   - Gateway

5. Select **Next**.
6. Enter 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 once it has been created.

7. Enter the password that will be used for the user account at the prompt.

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

The system will disconnect 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 into the BreakingPoint Control Center. You may create additional accounts through the Administration page in the BreakingPoint Control Center.

Text Console

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

To configure the BreakingPoint device using a text console:

1. Open a terminal emulation client (e.g., HyperTerminal).
2. Connect to the BPS Management serial port 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. Select **Next** when you are done inputting your network settings.
5. Enter the login ID that will be used for the user account at the prompt.
6. Enter the password that will be used for the user account at the prompt.

The system will disconnect 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 into 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. New user accounts can now be created and managed through the Ixia Web App user interface as well.

In order to establish a BreakingPoint session and operate in the BreakingPoint Control Center, you must first log into the Ixia Web App.

Note: 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 displays after you login.

To establish a BreakingPoint session:

1. Open a web browser.
2. In the URL field, 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.

   For example: 192.168.100.56:8080

   The Login page is displayed.

3. In the Username field, type your user ID.
4. In the Password field, type your password.
5. If you want the browser to automatically fill in the Username and Password field for future logins, check the Remember Me box.
6. Click Login.

The Sessions page displays.

7. Select the BreakingPoint New Session icon.

The BreakingPoint Control Center is displayed.

Task 4: Accessing the BreakingPoint Control Center

The BreakingPoint Control Center is a Web-based user interface where the testing environment can be created, tests can be run, and reports can be viewed. 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 enabled 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: BreakingPoint recommends that users of Internet Explorer use IE 10 or higher. IE 9 and earlier versions are not supported.

Viewing the BreakingPoint Control Center requires a Web browser with the following items either installed or enabled:

- Adobe Flash Player (version Version 11.6.602.171 or higher)
- Pop-ups
- JavaScript

Enabling JavaScript

You must have JavaScript enabled to view the BreakingPoint Control Center.

To enable JavaScript for Internet Explorer:

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

To enable JavaScript for Mozilla Firefox:

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

To enable JavaScript for Mozilla Firefox 23:

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 j**avascript.enabled** and click **Toggle**. JavaScript is now disabled.

To re-enable JavaScript, repeat these steps.

To enable JavaScript for Safari:

1. Open a Safari browser window.
2. Select **Preferences** from the Safari menu.
3. Click the **Security** option from the top of the window.
4. Select the **Enable JavaScript** option 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

Please note that 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 system. This is normal behavior for the BreakingPoint Control Center if multiple browser resources are being used.

Note: BreakingPoint recommends clearing your cache and refreshing your browser after upgrading or reverting to any release of the 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 Figure 2-2 on page 13 for a tour of the interface.

Figure 2-2: BreakingPoint Control Center Overview

Table 2-2 lists the elements of the BreakingPoint Control Center.

Table 2-2: BreakingPoint Control Center Overview

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:

1. Log in with an admin account.

2. Click Administration | Users.
3. Click New User.

The Create User Account window is displayed.

4. Configure the account. (See Table 2-3 for fields and parameter descriptions.)
5. Click OK to create the account.

Table 2-3, "Create/Edit Account Window," lists and describes the parameters of the Edit Account window.

Table 2-3: Create/Edit Account Window

Parameter	Description
Username	Name for the account.
Create Password / Confirm Password	Password for user name.
Full Name	Name identifying user.
Email	Email for user account. If this user chooses to receive test results by email (see Editing Your Account), 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 system 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 system 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: 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:

1. Log in with an admin account.
2. Click Administration | System Settings.
3. Click System time and date.

4. Configure the time and date. (See Table 2-4 for parameters and descriptions.)
5. Click Apply to set the time and date.

Table 2-4, "System Time and Date," lists and describes the parameters of the System time and date window.

Table 2-4: System Time and Date

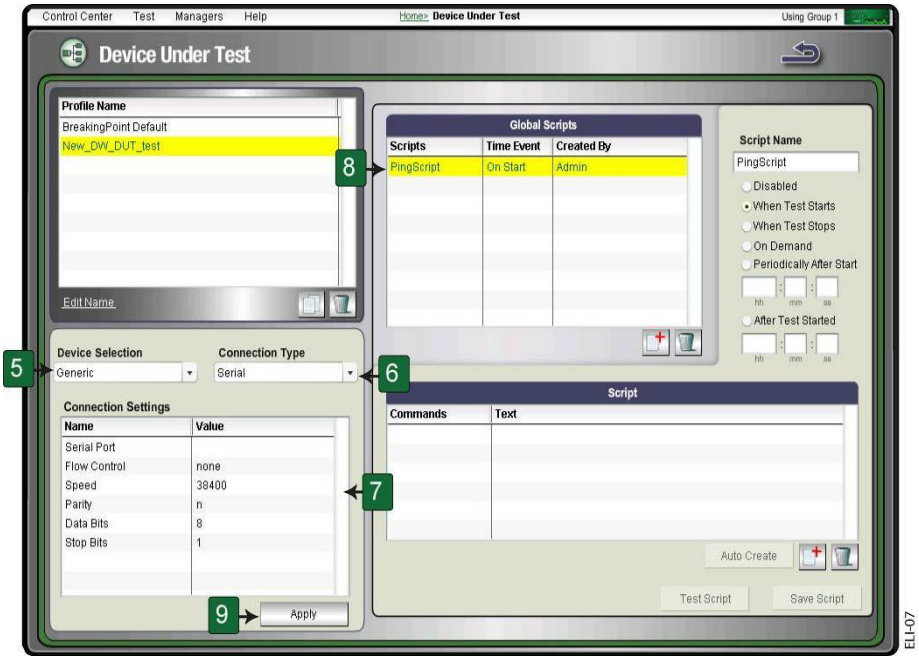
Parameter	Description
Time	Current time (hours:minutes) in 24-hour clock format.
Date	Today's date.
Time zone	Time zone where the chassis is located.

Task 7: Creating a Device Under Test Profile

This section will describe 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 section *DUT Profiles* 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.

Figure 2-3: Creating a DUT Profile



To create a DUT Profile:

1. Select **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 the **Clone the selected DUT** button.
4. Enter a name for the DUT Profile in the **Name** field and click the **OK** button.
5. Click the **Device Selection** dropdown button 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 the **Connection Type** dropdown button and select Telnet, SNMP, SSH, or Serial.

   Note: If you have selected **Serial**, the DUT must be plugged into the chassis through the BPS Management serial port. If you have selected 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 section *Connection Parameters* 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 will inherit the active global commands from its parent DUT Profile. For more information on commands, see the section *Commands* in the user guide.

9. Click the **Apply** button.

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/received by the interface.For each test component, you will need to specify the domain that the component will use to obtain the source and destination addressing for its traffic.

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

Note: The system 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.

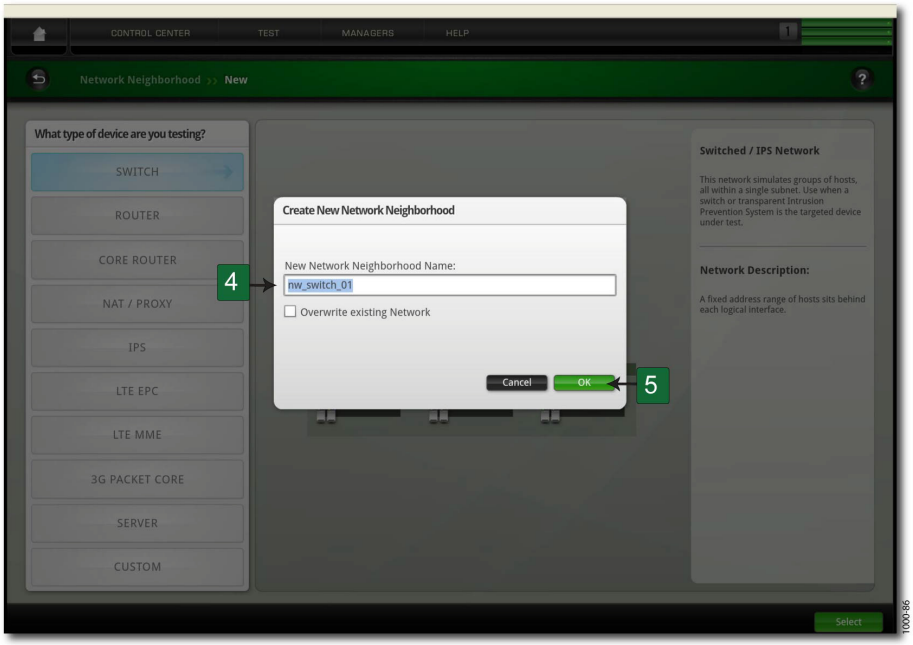
This task is broken into four parts:

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.

Figure 2-4: Creating a Network Neighborhood



To create a Network Neighborhood:

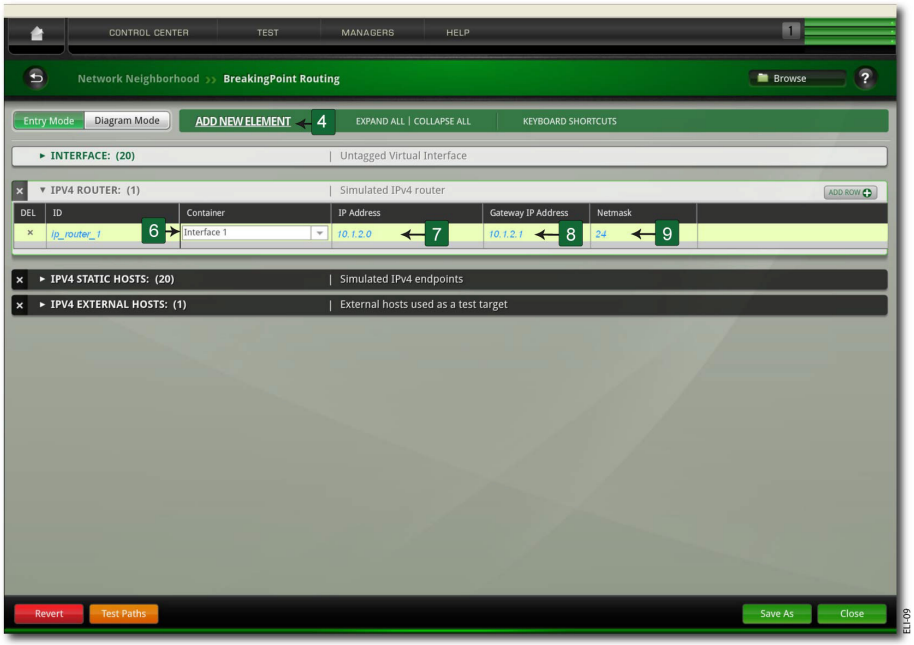
1. Select **Control Center > Network Neighborhood** from the BreakingPoint Control Center Menu bar.
2. Click the **Create a new network neighborhood ('+')** button located under the Network Neighborhoods list.
3. Enter a name for the Network Neighborhood in the **Name** field.
4. Click the **OK** button.

Note: Each interface will have a default domain with a preconfigured 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 section *External Interface Addressing* or *Defining a VLAN-Enabled Subnet* in the user guide.

Figure 2-5: Defining a Subnet



To define a non-VLAN subnet:

1. Select **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 the **Show the create new subnet form ('+')** button located under the Subnets list. The Create new subnet popup dialog box will appear.

   Note: If you are adding a subnet to an empty domain, then 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 the VLAN Tagging dropdown button and select a VLAN tag.
8. Select Use NAT for network address translation (if applicable).
9. Enter an IP address in the **Network IP Address** field. 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. Enter a mask for the network address in the **Netmask** field. For IPv6 addressing, enter the prefix in the Prefix field.
11. Enter a gateway address in the **Gateway IP Address** field. 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 the **Type** dropdown button.
13. Do one of the following:

- Select **Host** from the **Type** dropdown menu to use one MAC address per host.
- Select **Virtual Router** from the **Type** dropdown menu to use one MAC address for all hosts, and enter an IP address for the virtual router in the **Router IP Address** field.

Note: If an IPv6 router is present, the BreakingPoint device will generate at least one global address. You can discover the automatically generated IPv6 address via the SSH/telnet/serial interface, using the networkInfo command.

14. Enter an Ethernet address in the **Ethernet Address** field. Use the format xx:xx:xx:xx, where x is a valid hexadecimal value.
15. Enable or disable the **Use Address Range** option.
16. Enter a range of IP addresses using the **Minimum IP Address** and **Maximum IP Address** fields. Use the format x.x.x.x, where x is a number between 0-255.

    Note: If **Use Address Range** is disabled, you only need to enter an IP address in the **Minimum IP Address** field. The system will only use one IP address for the entire subnet.

17. Click the **Add Subnet** button.
18. Click the **Save Network** button.

Adding a Test Interface

By default, the system provides you with four transmitting and/or 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 system will automatically number the interface based on the order in which it was added.

If you delete any of the interfaces, the system will automatically resequence the interfaces. The succeeding interfaces (following the deleted interface) will be renumbered to the preceding interface's value (e.g., '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:

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

   Note: The interface will contain one domain with the default subnet.

Once you have added the interface to the Network Neighborhood, you can add subnets in the usual way. For more information on defining subnets, see the section **Defining a Subnet on page 18**.

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. However, in order to run all sixteen tests concurrently, you will need to assign each available port to a different Active Group.

In order to run tests on the BreakingPoint device, you must make port reservations. A port reservation occurs when you click on 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 on a port to reserve it, the system will lock the port reservation under your account. Locking a port reservation will also reserve all other ports under your account as well; however, only the ports with locked reservations can be used to run tests.

Note: In order 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 section called *Active Groups* 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 on the port you would like to reserve. This will lock the port reservation, as well as reserve all the ports on the blade under your account.

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

An important thing to remember when reserving your ports is the order in which you reserve them. Whenever you reserve a port, the system will automatically map that port to an interface on the chassis.

For example, if you reserve ports 0 and 1, then 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, then you cannot use that interface to run tests.

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

Note: Only reserved ports will can be mapped to interfaces.

To reserve ports on an unreserved blade:

1. Select **Control Center > Device Status** from the BreakingPoint Control Center Menu bar.

2. Click the **Active Group** dropdown menu.
3. Select the Active Group to which you would like to assign the ports.
4. Click on the port(s) you would like to reserve.

Note: A lock will appear over the reserved port. All other ports will be tagged with a small blue icon, denoting the port's Active Group. These ports, even though they have not been manually reserved by you, will be 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 on any of the ports. During a force reserve, the system will alert you that the ports are reserved by another user and ask if you want to force reserve all the ports on that blade. If you force reserve the port at this point, the system will reserve all the ports on that blade under your account.

Note: You cannot force reserve ports if there is a test or system process running on any of the ports on the blade. This system will alert 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 below 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 2 and 4 p.m. This may prevent other users from removing your port reservations.

To force-reserve ports

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

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

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

Note: The port(s) that you clicked on will show a locked icon, denoting that this port has been reserved by you. All other ports will be 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 on 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:

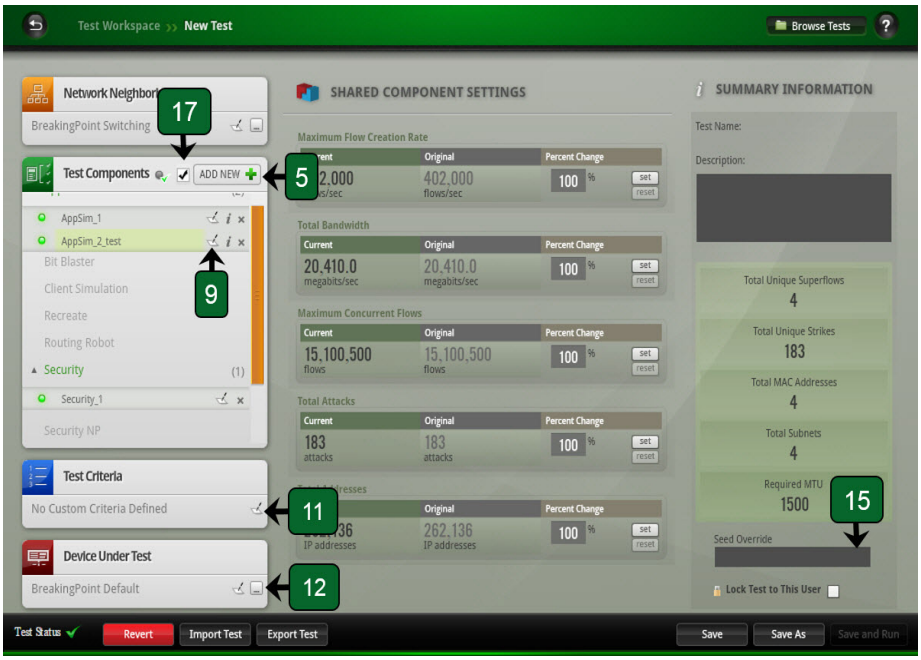
1. Select Control Center > Device Status from the BreakingPoint Control Center Menu bar.
2. Click the Active Group that you would like to use from the dropdown menu.
3. Right-click on the slot that has the ports you would like to reserve or unreserve.

4. Select the Reserve/Unreserve all ports on this slot option.

Task 10: Creating a Test

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

Figure 2-6: Creating a Test



To create a test:

1. Select **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 the **Open device under test screen** link to modify the DUT Profile. Once you have made your changes, click the **Return** button to go back to the DUT and Network Neighborhood selection screen. For more information on DUT Profiles, see the section **Task 7: Creating a Device Under Test Profile on page 15**.

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

Note: Click the **Open network neighborhood screen** link to modify the Network Neighborhood. Once you have made your changes, click the **Return** button to go back to the DUT and Network Neighborhood selection screen. For more information on Network Neighborhoods, see the section **Task 8: Creating a Network Neighborhood on page 17**.

5. Click the **Accept** button once 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 to be added to the test.
8. Do any of the following:

   - Click the **Information** tab.

     - Enter a new name for the test component in the **Name** field. (Optional)
     - Enter a new description for the test component in the **Description** field. (Optional)
     - Enable or disable the **Active** check box. (Optional)
     - Enable or disable the **Include in Report** check box. (Optional)
     - Click the **Apply Changes** button when done.

   - Click the **Interfaces** tab.

     - Select the interface(s) that will act as the client. The interface(s) you select must be mapped to a port.
     - Select the interface(s) that will act as the server. The interface(s) you select must be mapped to a port.
     - Click the **Apply Changes** button when done.

   - Click the **Presets** tab.

     - Select a Component Preset.
     - Click the **Apply Changes** button 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 the **Apply Changes** button when done.

9. Repeat Step 6-8 for each test component you want to add to the test.
10. Click the **Define Test Criteria** from the Test Quick Steps menu and create the pass/fail criteria for the test. For more information on pass/fail criteria, see the section *Test Pass/Fail Criteria* in the user guide.
11. Click the **Save As** button.
12. Enter a name for the test in the **Name** field.
13. Click **Save and Run** from the Test Quick Steps menu to run the test.

3 Site and Safety Regulations

This section covers:

- Site Requirements
- Safety Recommendations
- Safety Regulations

Site Requirements

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

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

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

Rack Requirements

The FireStorm chassis should be installed in a standard 19 inch EIA rack cabinet. Use of an equipment rack with side panels installed is not recommended due to the horizontal airflow requirements of the FireStorm.

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.

You should 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.

Note: 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 the section **Table 3-2 on page 28**.

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 3 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 system will shut down and the fan tray must be replaced. If this occurs, please contact BreakingPoint Support for further assistance.

Environmental Requirements

The 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

The FireStorm may be operated on 110VAC (nominal) or 220VAC (nominal) input power. However, there are some restrictions when operating on 110VAC. **Table 3-1, " Power Requirements,"** lists the configurations supported and the input current required for the chassis based on input voltage.

Table 3-1: Power Requirements

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

Note that the 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 FireStorm blade is installed with the system powered from a 110VAC source, the second blade will not power up. If two or more FireStorm blades are in a chassis, the input power must be 200-240VAC.

For North American shipments, power cords are provided with the system 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 system failure.

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

Note: Use proper ESD protection whenever handling any parts of the 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, be sure 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 the 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 the FireStorm.

Our recommended safety instructions for handling, operating, and maintaining the FireStorm are listed below:

- Keep the area around the chassis clear and dust-free during and after the installation.
- Only trained and qualified personnel should handle or service the 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 the FireStorm is powered on. Power the system off and wait until the fans have stopped running before removing the fan tray from the system.
- The chassis should be installed at least 2 feet above the ground.

Safety Regulations

Table 3-2 on page 28 lists the safety regulations to which the FireStorm is compliant.

Table 3-2: Safety Regulations

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 Web site.
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.

4 Installation Guide

This section covers:

- Shipping Package Contents Overview
- Installation Overview
- Powering the System

Shipping Package Contents Overview

The shipping packages for the FireStorm will contain 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 – 10Gb/1Gb SFP+ Optical Transceivers (short-reach or long-reach)
  - 6 – 1Gb 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:

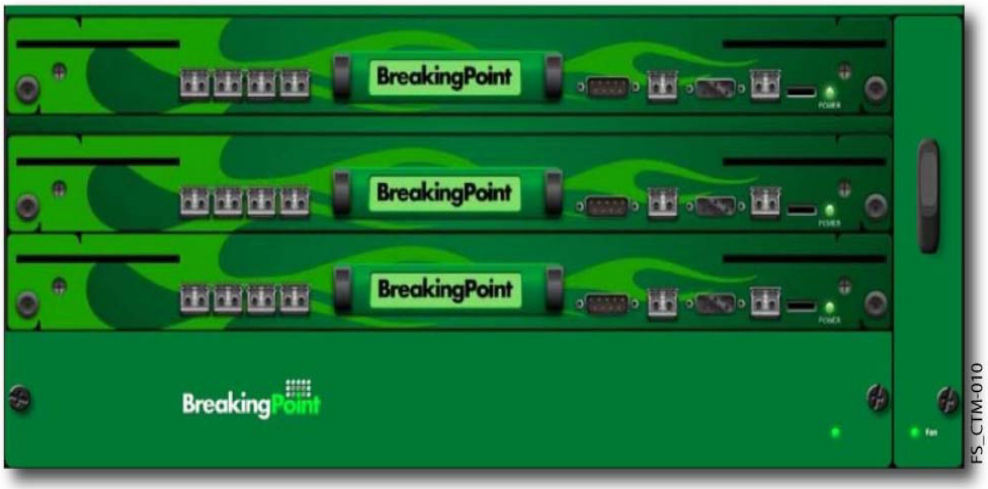
1. Mounting the chassis into an equipment rack.
2. Installing the blade(s) in the chassis.

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

Once 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.

Figure 4-1 on page 30 shows the chassis with blades installed in all three slots.

Figure 4-1: Chassis Modules



Mounting the FireStorm into an Equipment Rack

The following instructions will describe how to mount the FireStorm into a standard 19-inch equipment rack; if you require additional information for any other type of rack, you should refer to 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 the FireStorm into an equipment rack before installing the blade(s). Additionally, to avoid injury or damaging the chassis, three people are recommended to mount the chassis.

Guidelines to Keep in Mind

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

Generally, this includes:

- Mounting the chassis in an area where air can properly circulate (at least 3 inches of clearance around all ventilation openings)
- Ensuring that the chassis has at least 3 feet of clearance in the rear so you can easily access the system'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

In order 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 the FireStorm to a 19-inch equipment rack:

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 system.

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

   Note: The chassis should be placed at least 3 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 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

BreakingPoint recommends 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:

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 1 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 the FireStorm.
5. Push the blade into place once 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 System

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

- 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:

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.

Once you have turned on the power for the chassis, you can proceed to the initial configuration for the system. For more information, see section **Initial Configuration on page 35**.

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

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, make sure that your chassis is being powered by a BreakingPoint V2 Power Supply Tray.

Connecting a Device Under Test to the FireStorm

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

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

To connect a device under test to the chassis:

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 steps 1-3 for any additional optical data port connections.

5 System Configuration

This section covers:

- Initial Configuration
- Factory Revert

Initial Configuration

During an initial configuration, you will set up the IP address, netmask, and gateway for the FireStorm. Additionally, during this process, you will create a user account that will be used to log into the Control Center.

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

Management ports must be connected via a serial or Ethernet connection to your network. For a serial connection, use 115,200 8N1 on your terminal application. For an Ethernet connection, the FireStorm will attempt to obtain a DHCP address; if it cannot acquire an address, it will use the 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 system, FireStorm will guide you through the initial configuration.

To start the initial configuration:

1. Accept the end user license agreement.
2. Enter a fully qualified domain name in the FQDN field.
3. Enter the IP address you want to assign to your FireStorm in the IP Address field.
4. Enter a netmask in the Netmask field.
5. Enter the gateway address in the Gateway field.
6. Enter the primary DNS IP address in the Primary DNS field.
7. Enter the secondary DNS IP address in the Secondary DNS field.
8. Enter the tertiary DNS IP address in the Tertiary DNS field.
9. Tab to Next and press the Enter key.
10. Enter your user name in the Username field.
11. Enter your name in the Name field.
12. Enter your email address in the Email field.
13. Enter your password in the Password field.
14. Re-enter your password in the Confirm Password field.
15. Tab to Finish and press the Enter key. You will receive a message that the system is completing the configuration. Wait for the configuration process to complete.
16. To access the Control Center, enter the IP address you used in step **3** into the URL bar of your browser.

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

17. Click the Start BreakingPoint Systems Control Center button on the Start Page.
18. Enter the user name you created in step **10** in the Username field.
19. Enter the password you created in step **13** in the Password field.

    Note: Passwords are case sensitive.

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

20. Click the Login button.

    Note: The system allows three invalid logins. If invalid login information is entered on the fourth attempt, the login window will lock the user out. Users must refresh their browser to unlock their accounts.

Factory Revert

A factory revert will roll the system back to the build (factory build) that was initially installed on it and revert it back to its factory state. As a result, all settings, tests, and data stored on the system will be removed.

To perform a factory revert:

1. Locate the USB thumb drive 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 the Restore button.
4. Select ExternalDrive/USB/eSata, and click the Fetch Backups button.
5. Locate and click on the file named Factory Image.
6. Click the Restore button to start the factory revert.

Note: Note that all previous settings, stored tests, and reports will be wiped out by the factory revert process. The revert process typically takes 10 – 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 the FireStorm.
8. Wait for the status LED to turn green.
9. Press Return. The End User License Agreement screen will be displayed on the serial console. You can then go through the steps listed in the section **Initial Configuration on page 35**.

6 Accessing the Control Center

This section covers:

- Accessing the Control Center

Accessing the Control Center

You can access the Control Center after you have configured the FireStorm. When you access the Control Center, the first page that launches is the BreakingPoint Systems main page. From the main page, you can download the TCL shell, access from the Ixia Support Website, view the online Help, find BreakingPoint Systems contact information, and launch the Control Center user interface.

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

Note: BreakingPoint recommends clearing your cache and refreshing your browser after upgrading or reverting to any release of the FireStorm.

To access the Control Center:

1. Open a Web browser.

   Note: The browser must support Macromedia Flash version 10.0 or higher and have JavaScript enabled.

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

   Note: The default host address is http://10.10.10.10; however, if the host address was changed during the initial configuration, then you will use that address instead.

3. Click the **Start BreakingPoint Control Center** link located on the BreakingPoint Systems main page. A new window will open and launch the Control Center login page.
4. Enter your login ID in the **Login ID** field.

   Note: Login IDs are case sensitive.

5. Enter your password in the **Password** field.
6. Click **Login**.

   Note: The system allows three invalid login attempts. If invalid login information is entered on the fourth attempt, the login window will lock the user out. Users must clear their cache and refresh the browser to unlock their accounts.

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

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

Frequently Asked Questions

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

Account Questions

Question: I've had 4 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 into the Control Center to reset your password; you can log into the BPS Management port to reset the password; or you can telnet to the system's management IP address to reset the password.

Addressing Questions

Question: How do I configure the system 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" will use 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 will be 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 enabled. Any domain that has NAT enabled 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 disable the **Use Address Range** option and enter in the single IP address 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 enabled.

Bandwidth Questions

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

Answer: The maximum throughput is defined using the Data 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. The 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 system 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, then the corresponding Recreate test will estimate 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 will fluctuate between the data rate shared between both testing interfaces.

For example, if you have if a Session Sender test that uses 500 Mbps, then the test will never send more than 500 Mbps from an interface; however, the sum of traffic sent by both interfaces will fluctuate between 500 Mbps and 1000 Mbps.

System Questions

Question: What are the power requirements for the FireStorm?

Answer: See the table in the section titled **Power Requirements on page 26**.

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

Answer: 00:1A:C5

Question: Does the system 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 system?

Answer: Yes. Multiple users can be logged into the system 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 will roll the system back to the build that was initially installed on it (i.e., the factory build) and revert it back to its factory state; therefore, all settings, tests, and data stored on the system will be removed. A previous revert will roll the system back to the build that was previously installed on your system.

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 button on the Login Page?

Answer: Use the Preload for slower connections button 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 enabled, the system will alert you that an update has been downloaded to your system once you log into the Control Center. However, if you do not have automatic updates enabled, you will need to check the Ixia website at: https://support.ixiacom.com > **Software Downloads** > B**reakingPoint Software**.

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

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

Question: My system status says “System Not Operational”. What should I do?

Answer: There are two cases when this may occur: soon after a system has been rebooted, or after the system has not been rebooted for an extended period of time. Typically, after you reboot your system, you should wait at least 5 minutes before running a test. If you try to run a test before this time, the system may display this error. To resolve this error in either case, select **Control Center > Administration** from the Menu bar, click the **Restart** button to reboot your system, and wait at least 5 minutes before using the system.

Question: Where is the diagnostics file?

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

Troubleshooting Questions

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

Answer: First, power off the system. Once the system 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 system on. If this does not resolve your issue, please 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: All updates can be downloaded from the Ixia website at: https://support.ixiacom.com > **Software Downloads** > **BreakingPoint Software**.

Question: How will I know an update is available?

Answer: If you have automatic updates enabled, the system will alert you that an update file has been downloaded to your box. If you do not have automatic updates enabled, you will have to periodically visit https://support.ixiacom.com to check for new releases.

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

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

Question: How are the OS update files named?

Answer: Update files use the format X-N.bps. The X refers to the oldest version 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 will populate Smart Strike Lists with current strikes. Standard Strike Lists must be updated manually after applying any ATI upgrade.

Appendix

This section details the hardware and software specifications for the FireStorm.

Hardware Specifications

Table A-1 on page I details the hardware specifications for the FireStorm.

Table A-1: Hardware Specifications

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 (20.4kg) Rack Units: 4 RU
Dual Media Test Interfaces	4 - 10Gb/1Gb 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

Table A-2 on page II details the software specifications for the FireStorm.

Table A-2: Software Specifications

Software Component	Specification
Browser Client	Supported browsers: Adobe Flash- (Version 11.6.602.171 or higher) enabled browser (Internet Explorer 10 (or higher), Mozilla Firefox 18 (or higher), 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 the FireStorm.

See **Table A-3 on page II** for descriptions of each LED and what each LED color represents.

Table A-3: LED Statuses

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

Table A-3: LED Statuses

LED	Color	Status	Description
Power LED	Amber	Boot-up	System is booting up
	Green	Operational	System is powered on and operating
	Blinking Green	Busy	Insufficient power supply, a blade is not properly seated, or the system 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	System is powered on
	Off	Not powered	System 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

Table A-4 on page III lists the contents of the shipping container.

Table A-4: Shipping Container

Quantity	Item
1	FireStorm kit: 1 – FireStorm Blade 1 – 2500W V2 Power Supply 1 – Nameplate Label (upgrade kit only) 1 – 240VAC A/C Power Cable (110VAC A/C Power Cable for countries with primary 110VAC nominal power) 4 – SFP+ Optical Transceivers 6 – Copper 16b Transceivers 6 – Ethernet Cables 4 – 10GigE Fiber Optic Cables 1 – USB Thumb Drive

CLI Commands

Table A-5 on page IV lists the CLI commands available for the BPS Management port.

Table A-5: CLI Commands

Command	Description	Sample Syntax
?	Print a list of commands	`?`
? <cmd>	Print help for a command	`? addUser`
addUser	Add a user to the system	`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 into the BPS Management port	`passwd`
reboot	Reboot the system	`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 system'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 via firmware control. The following tables list the global scripts for available device types.

Dell PowerConnect 6024

Table A-6 on page V lists the global scripts for the Dell PowerConnect 6024 device type.

Table A-6: Dell PowerConnect 6024 Global Scripts Templates

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`

Table A-6: Dell PowerConnect 6024 Global Scripts Templates

Script	Template

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

Table A-7 on page VII lists the global scripts for the Extreme Summit 7i device type.

Table A-7: Extreme Summit 7i Global Scripts Templates

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

Table A-8 on page VIII lists the global commands available for the HP ProCurve 7500yl device type.

Table A-8: HP ProCurve 7500yl Global Scripts Templates

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 #`

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V