Document # 207251

Content Awareness Drives Next-Generation Test Tool

BreakingPoint Systems' BPS-1000 Enables Multilayer Emulation Testing at Multi-gigabit Speeds

A white paper commissioned by BreakingPoint Systems Inc.

THE TOLLY GROUP

White Paper

December 2007

Table of Contents

Before using this document you must agree to the terms of usage.
These terms are listed on the final page.

THE TOLLY GROUP

Table of Contents

Before using this document you must agree to the terms of usage.
These terms are listed on the final page.

THE TOLLY GROUP

Table of Contents

Before using this document you must agree to the terms of usage.
These terms are listed on the final page.

Executive Summary

Reaching the "Breaking Point"

The BPS-1000 enables companies to evaluate new or soon-to-be-deployed equipment and discover "breaking points" by creating repeatable, adaptable and scalable traffic.

BreakingPoint Systems, Inc. commissioned The Tolly Group to evaluate its BPS-1000 network test tool. The BPS-1000 can create traffic scenarios from Layer 2 through Layer 7. It can simultaneously generate TCP sessions, application traffic and attack traffic to test a product's performance and security coverage effectively.

The Tolly Group conducted a comprehensive hands-on examination of the BPS-1000 from September through October 2007. Engineers ran a battery of tests and feature validation exercises on the BPS-1000 to understand with greater depth the capabilities that the system provides to users.

BreakingPoint Systems believes users need to concurrently send live attacks while running high-speed application traffic through a device to provide an accurate summarization of a device's effectiveness.

Tolly Group engineers conducted focused examinations of the seven major components of the BPS-1000 test tool: Bit Blaster, Routing Robot, Session Sender, Security, App Sim, Stack Scrambler and Recreate.

The Tolly Group's hands-on evaluation revealed that the test tool delivers a complete toolbox that enables enterprise users and developers alike to simulate TCP session traffic, generate a wide array of application traffic and inject security threats through the device under test and determine its effectiveness at providing security coverage. Tests also show that the BPS-1000 supports 500,000 TCP requests per second, and supports as many as 5 million simultaneous TCP sessions.

Tests also revealed that the BPS-1000 is able to generate application traffic that conforms to protocols such as HTTP, FTP, DNS, SMTP, SMB, IMAP, POP3, RTSP, NFS, SIP, Telnet and more. On the security front, the test tool can perform dozens of evasion techniques, generate thousands of attacks, including SYN Floods.

Tolly Group engineers brought all of the BPS-1000 components together in a heavily loaded scenario to determine how many sessions it could gener-

ate across four Gigabit Ethernet ports. Engineers also set out to determine how this scenario would affect the test tool's internal processing.

Tests show that the BPS-1000 delivered optimal performance under stress. It was able to service all seven components without bogging down due to processing overhead. This underscores BreakingPoint's hardware design of multiple field programmable gate arrays (FPGAs), network processors and a array of embedded processors for generating traffic. BreakingPoint also designed the BPS-1000 with a separate control processor that runs the reporting and test creation functions.

Tolly Group tests indicate that the BPS-1000 offers a variety of functions normally requiring several separate test tools while consolidating them into a single unit. This single unit offers the traffic generation performance and reporting capabilities needed for testing enterprise-class and service provider-class equipment. In the sections that follow, The Tolly Group reports on core functions of the BPS-1000.

Session Sender Advanced Options

- Data rate
- Source and destination addressing
- Session behavior
- Session duration
- Maximum simultaneous sessions
- And more...

TCP Session Generation

The purpose of this test was to verify the BPS-1000 Session Sender's ability to build TCP sessions to a rate of 500,000 sessions/second and a maximum of 5 million simultaneous TCP sessions. In order for the BPS-1000 to pass the Session Sender test, the total number of sessions opened and the session set-up rate must reach the specific target within an alloted period of time.

Session Sender and Its Role

Session Sender measures a device's ability to handle a specified ramp rate and/or a specified number of concurrent TCP sessions.

The Session Sender test component allows users to control:

- The total number of TCP sessions that are open simultaneously
- The rate at which the sessions are opened and closed
- The duration of each TCP session

BreakingPoint Systems

BPS-1000

Performance and Functionality Validation

Product Specifications

Vendor-supplied information not necessarily verified by The Tolly Group

BreakingPoint Systems
BPS-1000

Dimensions
5.25"Hx17.5"Wx22.4"D

Weight
40 lbs.

Power Requirements
100-240V, 50/60 Hz.

Maximum Power Consumption
350 Watts

Automation
Built-in power receptacle for power cycle testing
Built-in serial and Ethernet ports

Application Layer
5 million simultaneous TCP sessions
500,000 TCP sessions per second
Dozens of application protocols supported including HTTP, FTP, DNS, SMTP, IMAP, POP3 RTSP, NFS, NFS, SIP and Telnet

Attack Generation
3,100+ security strikes
Dozens of evasion techniques
Automatic StrikePack updates
StrikeCenter

For more information contact:
BreakingPoint Systems
10535 Boyer Blvd, Suite 300
Austin, Texas 78758
Email: info@bpointsys.com
Phone: 512.821.6000
Fax: 512.997.9861

Test Methodology

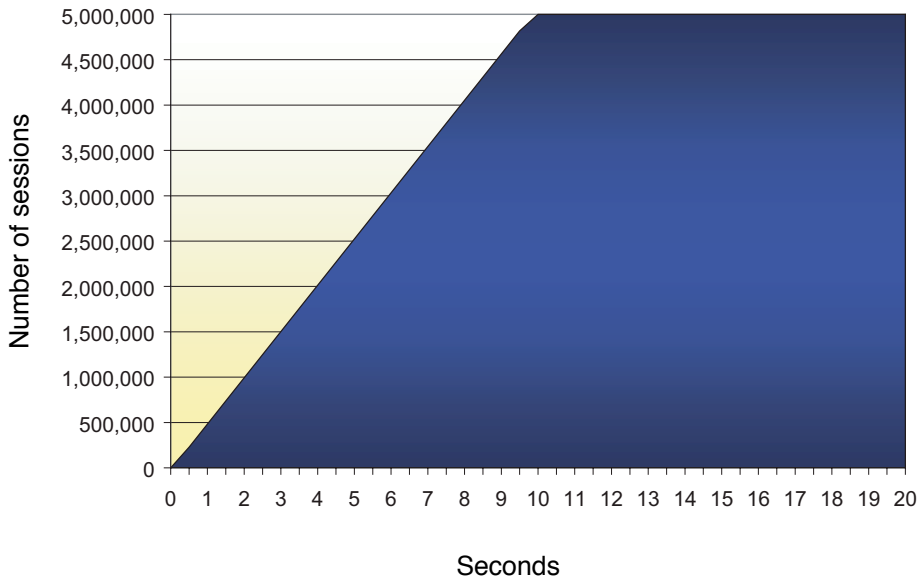
Engineers set up traffic across two ports on the BPS-1000 in a back-to-back configuration with a single Category 6 cable. Normally, the test tool would sit between these ports.

Tolly Group engineers noted the flexibility of the 30 Session Sender parameters that can be modified to fine-tune session generation characteristics. For the purpose of this test, engineers left many of the values in their default modes, but set the Maximum Simultaneous Sessions to 5,000,000 and the Maximum Sessions per Second to 500,000. The test duration was set to 300 seconds (five minutes) and the session ramp up/ramp down time was set to 10 seconds.

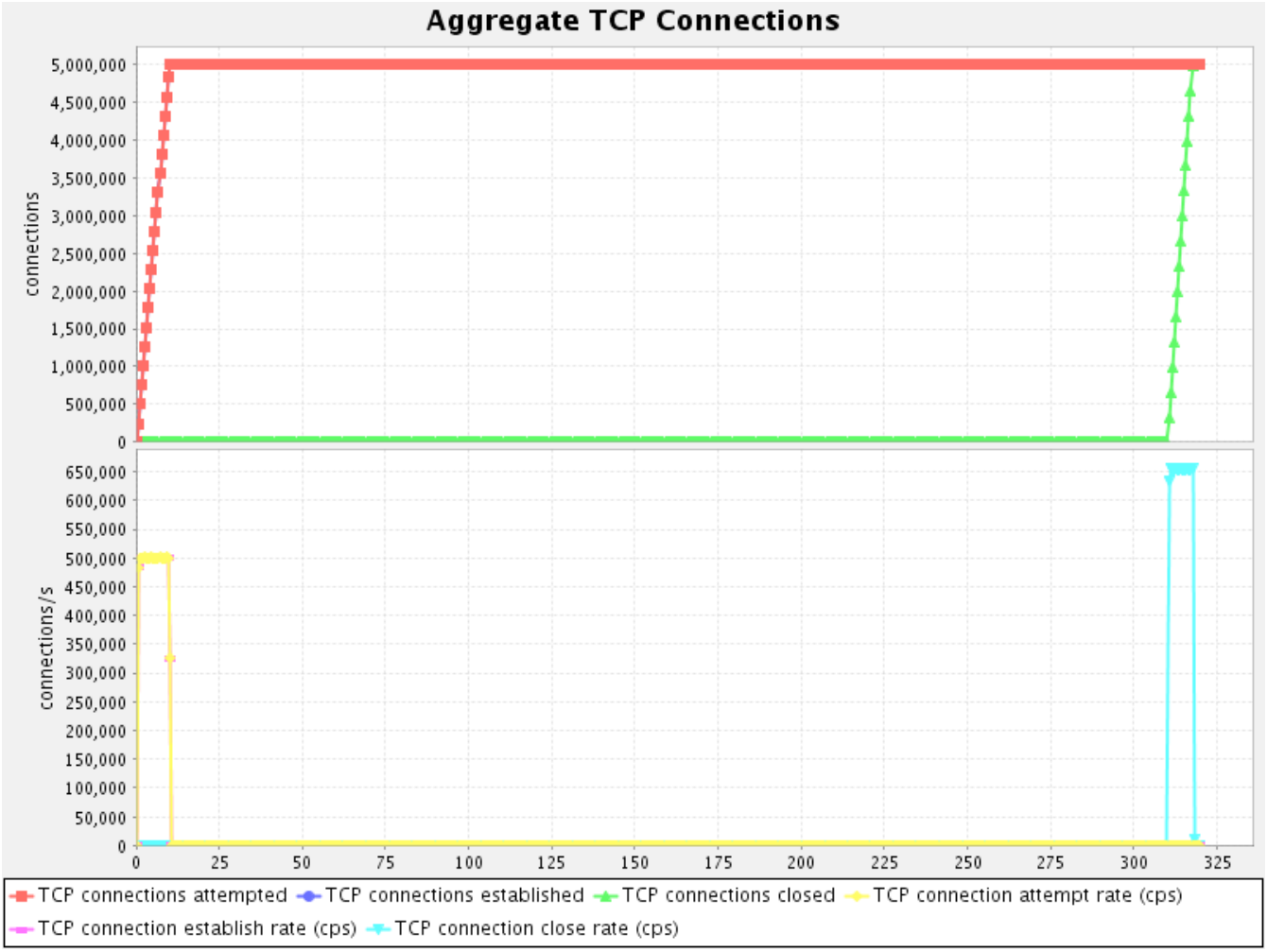
Session Sender Test Results

Tests show that the BPS-1000 was able to generate a maximum of 5 million sessions —verifying the company's claim of a maxi-

Average Concurrent TCP Sessions Supported



Source: The Tolly Group; October 2007 Figure 1



NOTE: The above image represents a graph generated for a report by the BPS-1000 and illustrates the manner in which the test tool delivers report info.

Source: The Tolly Group; October 2007

Figure 2

mum of 5 million sessions. The BPS-1000 reached its maximum session state 10.19 seconds into the test and held that session for five minutes, after which it gracefully ramped down sessions. See Figures 1 and 2.

Application Traffic Generation

The purpose of this test was to verify the BPS-1000 and its ability to create different types of simulated application traffic via the test tool's App Sim component.

App Sim and Its Role

The App Sim test component simulates real-world traffic based on application usage, and it is typically used in conjunction with other test components. Unlike other test components where the payload is created from a set of dummy data, the App Sim test component allows users to define the contents of the payload. If more than 5% of the traffic is dropped, the App Sim test will fail.

Using App Sim, users define basic and advanced parameters. Basic parameters include the maximum number of simultaneous sessions, the session ramp up duration, and the duration of each session.

The App Sim component enables users to create application traffic based on protocols such as HTTP, FTP, DNS, SMB, SMTP, IMAP, POP3, PostgreSQL, NFS, SIP, DHCP, Telnet, RTSP, NTP, SNMP and AOL.

Application Protocols

- AOL
- DHCP
- DNS
- FTP
- HTTP
- IMAP
- LDAP
- NETBIOS
- NFS
- PostgreSQL
- RTSP
- SIP
- SMB
- SMTP
- Telnet

Test Methodology

Engineers connected the BPS-1000 to a single port on a 24-port 3Com Switch 4500G--PWR switch and generated upstream application traffic to the switch. Traffic crossed the switch backplane and exited a second switch port where it was returned to the BPS-1000.

Engineers mirrored one of the two switch ports and redirected the mirrored application traffic to a Wireshark network protocol analyzer (running version 0.996a).

Engineers configured the App Sim component to generate a traffic mix of 19 application types (See Figure 3) and transmit the data through the

switch back to a receiving port of the BPS-1000. Even though the BPS-1000 is capable of much higher session rates, engineers used defaults parameters to ensure the largest variety of traffic by allocating at least 5% of each type of traffic Tolly Group engineers configured the test for 50,000 maximum simultaneous session, at a session setup rate of 125,000 sessions/second.

Application Generation Results

Tests show that the BPS-1000 successfully generated 19 application types with no detection of internal errors such as session disruptions.

Verification of Application Traffic Generation by Type

Application Traffic Type	Percentage of Traffic Mix	Verified
HTTP	10%	✓
FTP	5%	✓
DNS	5%	✓
SMTP	5%	✓
SMB	5%	✓
IMAP	5%	✓
POP3	5%	✓
PostgreSQL	5%	✓
NFS	5%	✓
SIP	5%	✓
DHCP	5%	✓
Telnet	5%	✓
RTSP	5%	✓
NTP	5%	✓
SNMP	5%	✓
AOL	5%	✓
LDAP	5%	✓
NETBIOS	5%	✓
DCERPC	5%	✓

Source: The Tolly Group, Sept. 2007 Figure 3

Attack Generation

The purpose of this test was to verify that the BPS-1000's Security component can generate valid threat packets and to assess the maximum number of threat strikes it can send. Additionally, Tolly Group engineers identified the different security (intensity) levels of attacks generated by the BPS-1000, and validated that the BPS-1000 can manipulate attack traffic to take on certain evasion characteristics.

BreakingPoint maintains that its BPS-1000 is capable of launching 3,000+ unique attacks and more than 60 evasion types. Tolly Group engineers validated the large base of evasion techniques available from the BPS-1000.

Attack Types

Two types of attacks may be launched from the Security screen: A basic attack and a targeted attack. In a basic attack, you send strikes using groups of pre-selected attacks. With a targeted attack, you select the attack series you want and any evasion options to be used.

Security and Its Role

The Security test component can be used to test network security appliances, such as intrusion prevention systems (IPS), intrusion detection systems (IDS), VPNs and firewalls. It measures a security device's

BPS-1000 Strike Levels Supported for Various Attack Scenarios

Strike Level	Description
1	Targets high-risk vulnerabilities in services that are exposed to the Internet.
2	Targets all high-risk vulnerabilities.
3	Targets all high-risk vulnerabilities, worms, and backdoors.
4	Targets all vulnerabilities, worms, and backdoors.
5	Targets all vulnerabilities, worms, backdoors, probes, and Denial of Service flaws.

Source: The Tolly Group, September 2007 Figure 4

ability to protect a network by sending “strikes,” or attacks, and verifying that the device successfully blocks the threats.

Test Methodology

The BPS-1000’s Security component offers five levels of security testing. Level 1 provides the lowest level of security testing, while Level 5 provides the most comprehensive and intense level of security testing. Additionally, besides the five levels of security testing, the BPS-1000 offers several other Attack Series that target other areas of security.

Tolly Group engineers chose the All Strikes Attack Series. This is the most serious type of Attack Series that can be sent by the BPS-1000. This Attack Series targets all vulnerabilities, including worms, backdoors, probes and Denial of Service flaws. Currently, this attack includes 3,131 strikes.

Engineers ran the security test twice. They sent traffic out on Port 3 and received traffic on Port 4. Engineers used a Wireshark analyzer to capture and verify the attack packets.

Security Test Results

Tests show that the BPS-1000 successfully generated valid IP packets according to each type of strike. Engineers also observed that the BPS-1000 allows users to pre-configure a wide array of options to evade threat or strike detection. Finally, Tolly Group engineers validated that the BPS-1000 is capable of launching a maximum of 3,131 strikes.

Application Traffic and Threat Generation

In this test,. The Tolly Group set out to verify that the generation of application traffic will not be adversely slowed by the simultaneous creation of strike/attack traffic. Tolly Group engineers measured the number of attempted applications flows attempted versus the number of established application flows to verify that the presence of threat traffic did not impede the application traffic.

Test Methodology

Engineers set the BPS-1000 App Sim and Security components to both transmit from Port 3 and receive at Port 4 using a back-to-back connection with a Category 6 cable.

For the Security component, engineers used Security Level 5. This attack series uses all strikes that are available and default evasion options.

For the App Sim component, engineers set the maximum number of simultaneous sessions to 5 million and the maximum number of sessions per second to 500,000. These values represent the maximum values supported by the BPS-1000 across all test components. In addition to setting up these sessions engineers also defined 19 application protocols to run in the background. These included: HTTP, FTP and POP3 traffic, to Telnet, SNMP, LDAP and NetBIOS traffic and more.

App Sim and Security Test Results

The test results show that the BPS-1000 is able to generate significant threat-based traffic without any adverse impact on the generation of high volume application traffic. This shows that the multiple, independent network processors at the heart of the BPS-1000 are able to handle application traffic generation separately from threat traffic generation and deliver both simultaneously to the transmitting port.

Application Traffic Flows Established in Presence of Attack Traffic			
Flow type	**Attempted**	**Established**	**Percent of Flows Completed**
HTTP	1,556,179	1,556,179	100%
POP3	692,342	692,342	100%
Telnet	345,995	345,995	100%
DNS	807,354	807,354	100%
IMAP	576,473	576,473	100%
PostgreSQL	230,916	230,916	100%
FTP	460,935	460,935	100%
SMTP	460,639	460,639	100%
SIP	922,270	922,270	100%
DHCP	345,818	345,818	100%
SMB	461,043	461,043	100%
NFS	345,649	345,649	100%
RTSP	691,077	691,077	100%
NTP	633,682	633,682	100%
SNMP	461,203	461,203	100%
AOL IM	691,931	691,931	100%
LDAP	345,310	345,310	100%
NETBIOS	691,197	691,197	100%
DCERPC	693,298	693,298	100%

Source: The Tolly Group, September 2007

Figure 5

Layer 2 Traffic Generation

The purpose of this test was to verify the BPS-1000's ability to generate standard Ethernet frames via the test tool's Bit Blaster component for Layer 2 traffic tests.

Engineers measured the aggregate Layer 2 traffic yielded across four Gigabit Ethernet ports, verified that it generates Layer 2 frames and identifies the performance metrics (throughput, latency, etc.).

Bit Blaster Selectable Features

Users may define a pool of IP addresses from which packets may obtain their destination addresses. Users may also set a variety of time parameters and payload options, as well as throughput settings and frame/packet sizes.

Bit Blaster and Its Role

The Bit Blaster test component analyzes a target device's ability to handle high volumes of traffic by identifying whether the tested device receives and sends packets without corrupting or dropping them.

The Bit Blaster identifies:

- The amount of time (latency) a DUT holds onto a packet before forwarding it to its destination
- The number of corrupt packets sent by the DUT
- The number of packets dropped by the DUT

Test Methodology

Engineers followed the Test Methodology approach used in the Application Traffic Generation test scenario. Engineers connected the BPS-1000 to a single port on a 24-port 3Com Switch 4500G--PWR switch and generated upstream Layer 2 application traffic to the switch for 10 seconds. Traffic crossed the switch backplane and exited a second switch port where it was returned to the BPS-1000.

Engineers mirrored one of the two switch ports and redirected the mirrored application traffic to a Wireshark network protocol analyzer (running version 0.996a).

Engineers also verified the Layer 2 throughput over back-to-back connections (Port 1 to Port 2, Port 3 to Port 4) using two Category 6 cables and sending 1,024-byte default frames for 60 seconds.

Bit Blaster Test Results

Test results show that the BPS-1000 yields 4 Gbps of aggregate Layer 2 traffic across the four available GbE ports, equaling 1 Gbps of traffic on a per-port basis. Engineers validated that 100% of the GbE port bandwidth was utilized by the Layer 2 traffic generated by the Bit Blaster. In effect, each of the four GbE interfaces sent 1 Gbps of Layer 2 traffic simultaneously. Engineers used a Wireshark traffic analyzer to verify that the Bit Blaster generated frame traffic.

Finally, tests show that the BPS-1000 identifies the latency, throughput number of corrupted frames sent, and frame count of devices tested. For a 30-second Layer 2 test, the BPS-1000 transmitted an average of 1 Gbps of frame data, and received 1 Gbps of frame data with zero latency and zero dropped frames. This frame rate equates to wire-speed performance.

Layer 3 Traffic Generation

Engineers set out to verify the BPS-1000's ability to generate standard Ethernet packets via the test tool's Routing Robot component for Layer 3 traffic tests.

Engineers measured the aggregate Layer 3 traffic across four Gigabit Ethernet ports, verified that it generates Layer 3 packets and identifies the performance metrics it is capable of reporting (throughput, latency, etc.).

Routing Robot and Its Role

The Routing Robot test component if a DUT routes traffic properly by sending UDP traffic from one interface and monitoring the receiving interface to determine if the traffic is received properly.

The Routing Robot uses three metrics to determine if a packet is received successfully:

- The packet is not dropped
- The packet is not corrupt
- The packet is not modified

Test Methodology

Engineers employed a methodology similar to the Layer 2 test, but instead used 64-byte packets (which the BPS-1000 sends automatically via UDP). Packets were transmitted for 60 seconds.

Routing Robot Test Results

Test results show that the BPS-1000 yields 4 Gbps of aggregate Layer 3 packet traffic across four 1-Gbps interfaces.

Transmitting 64-byte packets, the BPS-1000 achieved a packet transmit rate of just over 1,480,000 pps. Since 64-byte packets is the smallest packet size the test tool handles, the 1.49 million UDP packets achieved represents the highest amount of unidirectional packets the BPS-1000 can generate on a 1-Gbps full-duplex connection, based on handling the smallest packet size available.

A traffic capture by a Wireshark analyzer revealed that the BPS-1000 did, in fact, send UDP packets at the specified 64-byte packet size.

Finally, tests show that the BPS-1000 identifies the latency, throughput number of corrupted packets sent, and packet count of devices tested. For a 60-second Layer 2 test, the BPS-1000 transmitted an average of 1 Gbps of packet data, and received 1 Gbps of packet data with zero latency and zero dropped packets. This packet rate equates to wire-speed performance.

Protocol "Fuzzing"

It is a requisite that any traffic generation test tool create normal application traffic such as HTTP, FTP, and other application-related traffic, it is equally imperative for traffic generators to serve up intentionally flawed or corrupted data for test purposes.

In this test scenario, Tolly Group engineers used the Stack Scrambler to generate corrupted data (or fuzz) and transmitted it from one port to another.

Stack Scrambler and Its Role

The Stack Scrambler component of the BPS-1000 uses a "fuzzing" technique to modify a part of the packet traffic (including the checksum, protocol options, etc.) to generate corrupt data.

Users can employ the Stack Scrambler to test a device's ability to transmit packets so they arrive at the correct destination and continues to work properly while it simultaneously handles the malformed packets.

Test Methodology

Engineers used the Stack Scrambler to generate data traffic from Port 3 to Port 4 while the traffic was simultaneously captured by a Wireshark analyzer. As in other test scenarios, traffic sent from Port 3 traveled through the 3Com switch back to Port 4 on the BPS-1000. All optional parameters were left in "default" mode.

Stack Scrambler Test Results

From the data capture on the Wireshark analyzer, engineers validated that the BPS-1000 generated corrupt packets.

Scrambled Packets

The BPS-1000's Stack Scrambler sends ICMP echo requests to a device under test to validate that the device is working properly. At the end of the test, a burst of packets is sent to the DUT; if all packets successfully arrive at their destinations, then the DUT is successful in handling invalid packets.

Traffic Recreation

A content-aware network test tool should be able to assist users in modeling traffic to create a test scenario with speed and ease. In this test, The Tolly Group assessed the Recreate component of the BPS-1000 to capture traffic from an actual application and use that snapshot to recreate the traffic for a test scenario.

Recreate and Its Role

The Recreate component builds traffic based on data from a capture file. It rewrites capture file data to match parameters specified for a domain. The payload is the only portion of the capture file that is not modified.

This can be useful to users that want to capture traffic and then multiply it, such as a single VoIP call that can be “recreated” and played back as multiple calls and transmitted onto the network for testing purposes.

Test Methodology

To create traffic, engineers initiated a capture file, went to Firefox and opened the browser to its home page. They then visited google.com, searched on a keyword, “test” and pasted a link to a malware Hotbar in the address bar. Engineers then downloaded malware Hotbar.exe and visited ftp.microsoft.com where they downloaded a random 1-MB file. Once complete, they ended the capture.

The data capture was handled via WireShark due to its bidirectional capturing capability. The capture file (.pcap) was then loaded directly into the BPS-1000. A Recreate component was added to a test and was then run.

Recreate Test Results

The Recreate component was able to reproduce all of the frames captured. All of the recreated fames were then transmitted to and received at the destination port.

Reporting Features

Reporting Detail

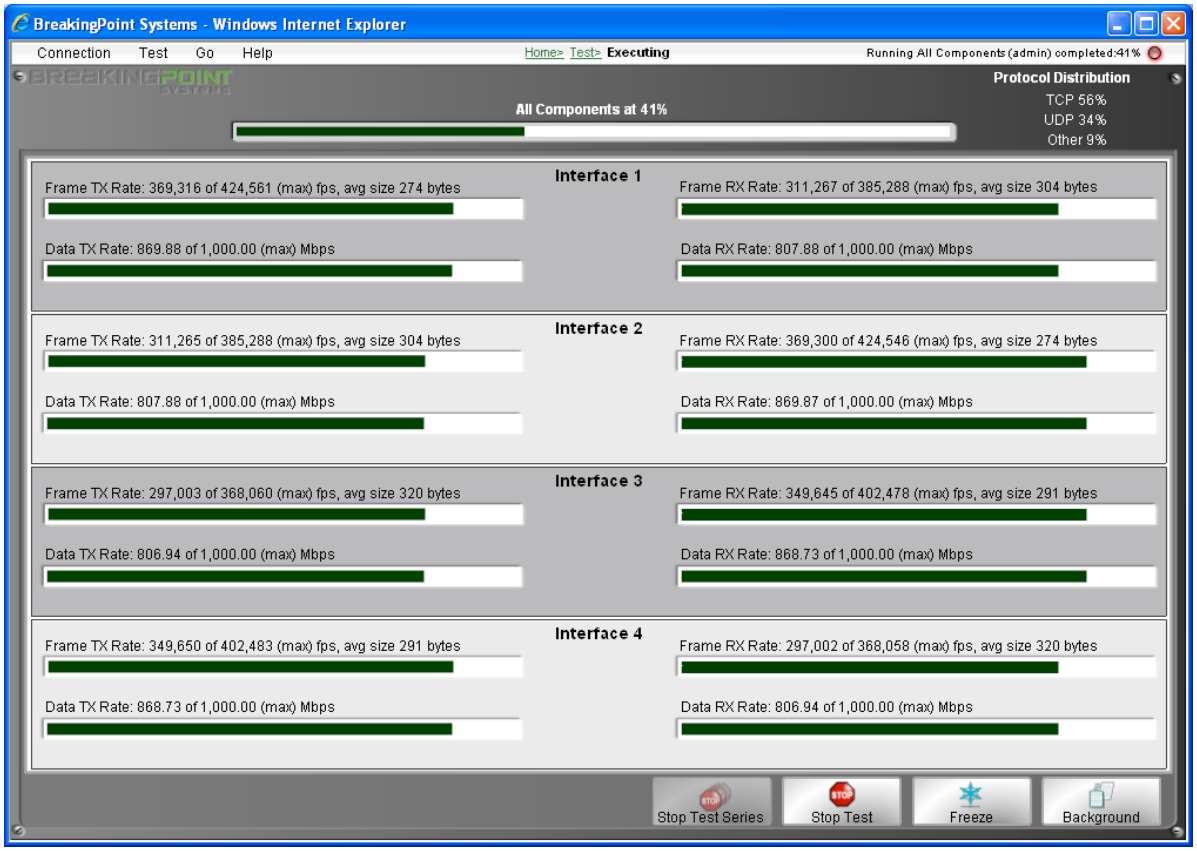
By default, all of the BPS-1000's reports include data on:

- Test environments
- Test purpose
- Traffic appearance
- Test criteria
- Test results

Tolly Group engineers examined the breadth of reporting capabilities offered by the BPS-1000. Engineers observed that BPS-1000 offers real-time reporting capabilities. Data, frame transmit and receive rates are displayed for every port, including an average frame size. Information on traffic by protocol distribution is also available in percentages showing the TCP, UDP or other traffic running at any given time during the test. A progress bar displays the test's progress. (See Figure 6.)

Reports are available in PDF, HTML, CSV and XML formats. Users have the ability within the BPS-1000 to set report characteristics by default. Test results also can be E-mailed to an admin or other person upon test completion.

BPS-1000 Real-Time Reporting Capabilities



Source: The Tolly Group, September 2007

Figure 6

Maximum Performance Under Stress

For the final test, Tolly Group engineers created a heavily loaded scenario designed to push the BPS-1000 to deliver its maximum performance under load.

For this test, engineers ran multiple instances of the Bit Blaster, Routing Robot, Security, Stack Scrambler, Application Sim and Recreate components across four available GbE ports.

The aim was to understand what impact, if any, the heavy loading and processing overhead would have on taxing the BPS-1000.

Test Methodology

Engineers configured all BPS-1000 components to support default settings. Next, they created 5 million sessions, balanced between the Session Sender, Application Simulator and Recreate components. Then they ran all seven BPS-1000 components for 300 seconds (five minutes) to determine what impact, if any, the components would have on the BPS-1000's processing engine.

Performance Under Stress Results

This test reveals that BPS-1000 components, when used in tandem to support a heavy traffic generation load, do not overtax the hardware architecture of the test tool. It continues to support seven different components as each transmits generated traffic unidirectionally, or bidirectionally, across the four available ports. Tests show that the processing load from all seven BPS-1000 components utilized from 75% to 95% of available bandwidth. This demonstrates that all components can run and interoperate with each other at the full capacity offered by each interface. Ultimately, the bandwidth utilization achieved depends on the protocol type in the test component, since some protocols do not stream data continuously.

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.

This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental and consequential damages which may result from the use of information contained in this document

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.

When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

All trademarks are the property of their respective owners.

The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services.

The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at http://www.tolly.com, sales@tolly.com

THE TOLLY GROUP