Test LTE/4G Network Performance, Security, and Stability at Massive Scale

Ixia BreakingPoint Products Emulate Millions of Users to Reduce Cost and Complexity of Validating LTE Network Infrastructure

Telecom carriers rolling out Long Term Evolution (LTE) and 4G networks must test mobile infrastructures efficiently and accurately under punishing real-world conditions, without spending a fortune to do so. Ixia BreakingPoint products answer this challenge with the industry’s most sophisticated and cost-effective Internet-scale LTE emulation.

These products allow carriers to test their networks and the devices within them against the behavior of millions of simulated users downloading rich media content, placing calls, purchasing music, browsing the Web, or unknowingly sharing the latest malware. A BreakingPoint module replaces racks of equipment and complicated setup processes with a single-chassis device and a single user interface (Figure 1).

Unprecedented Performance and Massive Scale in a Cost-Effective Device

Based on a patented breakthrough in network processor technology and backed by a team of network performance and security experts, only a BreakingPoint module produces the city-scale LTE network conditions needed to harden carrier-grade network resiliency.

With a BreakingPoint 4U chassis, you can:

- Measure and harden the performance, security, and stability of load balancers, firewalls, IPS devices, and other equipment with up to 120 gigabits per second of application, attack, and malformed traffic.
- Validate network and data center performance by recreating more than 220 application protocols, including AOL® IM, Yahoo® Mail and Messenger, Google® Gmail, Skype®, BitTorrent™, eDonkey, RADIUS, SIP, RTSP, RTP, HTTP, SSL, Facebook®, Twitter Mobile, YouTube®, and Apple® FaceTime®, as well as other mobile, social, and gaming protocols – with Multicast support.
- Stress network infrastructures with more than 35K+ security attacks and pieces of malware – including mobile malware – plus obfuscations and evasions.
- Find network problem areas sooner and prepare for the unexpected with the industry’s fastest protocol fuzzing capabilities.
- Emulate sophisticated, large-scale DDoS and mobile-initiated botnet attacks to uncover previously hidden weaknesses.
Figure 1. BreakingPoint Products Enable Configuration of Multi-Million-User LTE Infrastructure Tests from a Single-Screen Interface

The Solution for Simulating Multi-Million-User LTE Networks, with Additional 3G Capability

The unique architecture of BreakingPoint products delivers the huge performance numbers necessary to validate and harden even the largest LTE networks under the most realistic conditions, all from a turnkey solution, including:

- Up to 120 million concurrent TCP sessions, allowing emulation of thousands of eNodeBs connecting to millions of devices such as smartphones, tablet computers, and netbooks.
- Interactions among all the network elements involved in LTE communications, including user equipment (UE), eNodeBs, Service Gateways (SGWs), Packet Data Network Gateways (PGWs), and Mobility Management Entities (MMEs).
- A full Dynamic Host Control Protocol (DHCP) network, with support for both DHCP Client and DHCP Server processes.
- Support for both 3G and LTE environments with GTPv1 and GTPv2.
- Technological Breakthroughs from an Easy-to-Use Product that is Always Current
- BreakingPoint modules are designed for ease of use and rapid configuration in a variety of network environments. Because of their exclusive design, they evolve along with the frequent changes in the landscape for applications, attacks, and telecom standards. With a BreakingPoint, you will:
  - Receive frequent updates from the BreakingPoint Application and Threat Intelligence (ATI) research team, which is dedicated to keeping applications and attacks current and providing frequent feature and performance enhancements.
• Employ built-in network traffic profiles – created using data collected from top global telecom carriers – or easily customize these profiles to fit your own network’s unique conditions.

• Configure simulations in just minutes through a single user-friendly interface that features fully integrated reporting, even across multiple BreakingPoint modules.

• Leverage extensive automation and wizard-like labs that address many use-case scenarios, including validation of Lawful Intercept and Data Loss Prevention solutions with a digital storm of content in multiple languages.

• Eliminate the complexity of conventional testing approaches and replace it with the simplicity, power, and precision of the BreakingPoint modules.

**Performance Specifications**

From a single 4U chassis, a single BreakingPoint FireStorm chassis configured with 3 Firestorm blades provides unprecedented levels of scale & performance from a single 4U chassis, including:

• 120 Gbps of application traffic and up to 50 Gbps of GTP-encapsulated application traffic

• 120 million concurrent TCP sessions

• 4.5 million TCP sessions per second

• 1.5 million steady-state complete TCP sessions per second

• 120,000+ SSL sessions per second

• 9,000,000 concurrent GTP Tunnels

• 9,000,000 concurrent UEs

• 775,000 UE registrations/sec on S11 interface

• 5,400 UE registrations/sec on S1 interface

• 12,000 eNodeB’s

• 24 Gbps SSL encryption

• 24 Gbps IPsec encryption

• 65,000 concurrent IPsec tunnels

• 220+ stateful application protocols

• 35K+ live security attacks and pieces of malware

• Network latency down to 10-nanosecond resolution

• 12 universal 10GigE/1GigE interfaces

**3G/4G Operational Modes**

- eNodeBs + UEs
- PDN
- MME
- SGW + PGW + PDN
- eNodeBs + UEs + MME, SGW + PGW + PDN
- SGSN + UEs
- GGSN + PDN
- UE/eNB/MME/SGW
- PGW/PDN
- UE/eNB vs. MME/SGW/PGW/PDN
Interfaces Supported

- S1-U (eNodeB and SGW sides)
- S1-MME (eNodeB side)
- SGi (PDN side)
- S5/8 (SGW and PGW sides)
- S11 (MME and SGW sides)
- Gn (SSGN and GGSN sides)
- Wireless Protocols Supported:
  - S1AP
  - GTP-C v1, GTP-C v2, GTP-U v1
  - SCTP (over UDP or IP)

Predefined Mobility Application Profiles

- Mobile User
- European Wireless Carrier Daytime
- European Wireless Carrier Daytime with iPhone
- European Wireless Carrier Weekday
- European Wireless Carrier Weeknight
- European Wireless Carrier Weeknight with iPhone
- North American Wireless Carrier Weekday
- North American Wireless Carrier Weekday Daytime
- North American Wireless Carrier Weekday Daytime with iPhone
- North American Wireless Carrier Weekday with iPhone
- North American Wireless Carrier Weeknight
- North American Wireless Carrier Weeknight with iPhone
- Sandvine Mobile Internet Report – Caribbean/Latin America
- Sandvine Mobile Internet Report – Europe
- Sandvine Mobile Internet Report – North America

Wireless Reporting Statistics

- UE Attach Requests Sent/Accepted/Failed
- UE Detach Requests Sent/Succesess
- S1AP Setup Requests/Succcesses
- S1AP Reset Requests Received/Reset ACKs Sent
- SCTP Open Requests/Open Succcesses
- SCTP Close Requests/SCTP Close Succcesses
- GTP Create Requests Processed
- GTP Create Responses Processed
- GTP Delete Requests Processed
- GTP Delete Responses Processed
- GTP Client Side Tunnels
- GTP Client Side Sent/Received Data
- GTP Server Side Tunnels
- GTP Server Side Sent/Received Data
Other Features

- LTE specification supported: v9
- All security strikes and live malware supported over LTE and 3G
- Malformed application traffic over GTP
- Specific mobile malware support
- All application protocols supported
- Can emulate multiple device instances concurrently (MME, SGW, GGSN, SSGN)
- Automatic generation of IMSI, MSISDN, and UE secret keys

Example LTE Emulation Options