



The authoritative, unbiased source for IT certification, research and testing



WHITE PAPER

August 2005

**A white paper
commissioned by
Shenick Network
Systems**

Document #205122

Test Tool Evolution Keeps Pace with Network Operator Needs

*Integration of Shenick diversifEye
Pushes Up the Stack to Drive True
Measurement of the User Experience*

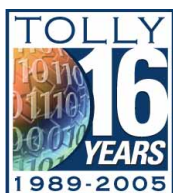
Terms of Usage



Entire contents © 2005 The Tolly Group, Inc. All rights reserved.

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 can occur.



The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, this 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. The Tolly Group provides a fee-based service to assist users in understanding the applicability of a given test scenario to their specific needs. Contact us for information. When foreign translations exist, this English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.



Tolly Group Vendor Service



With more than 16 years experience validating leading-edge Information Technology products and services; [The Tolly Group](#) has built a global reputation for producing accurate and unbiased evaluations and analysis. We employ time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy.

Launched in 2003, The Tolly Group's "Tolly Verified" service provides in-depth, vendor-neutral certification of an array of features, functions and performance characteristics in technology disciplines as diverse as WLAN Switching and Anti-spam. See our ["Tolly Verified" Home Page](#).

Our "Up-to-Spec" service provides the custom testing complement to the "standard", granular tests offered in "Tolly Verified". See our ["Up-to-Spec" Home Page](#).

Plus, unlike narrowly focused testing labs, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure.

This document
was authored by:

- Kevin Tolly,
President/CEO
The Tolly Group
- Charles Bruno,
Executive Editor
The Tolly Group

Table of Contents

- 4 Focus Turns to 'Triple Play'
- 6 Tightly Integrated Architecture
- 7 Performance Matters
- 8 Driving Traffic
- 9 Real-World Performance Under DDoS Attacks
- 9 DDoS Test Validation
- 11 Nimda Test Validation
- 11 Layer 2 to 7 Flexibility
- 12 Flexibility Put to the Test
- 13 Going with the Flows
- 14 Per-Flow QoS Testing
- 17 Bringing It All Together

List of Figures

- 5 Figure 1: Network Test Bed
- 7 Figure 2: Layer 2 throughput and frame rates
- 8 Figure 3: Distribution of HTTP server response times
- 10 Figure 4: Snapshot of HTTP throughput and DDoS attack test.
- 13 Figure 5: Aggregate IDS throughput with stateless and stateful traffic mix.
- 14 Figure 6: Application response times over a link that was rate limited to 40 Mbps.
- 15 Figure 7: Application response times over a link that was rate limited to 5 Mbps.
- 15 Figure 8: Per-flow bandwidth allocation test results.
- 16 Figure 9: Per-flow performance of traffic shaper tool.
- 18 Figure 10: Multitasking traffic generation and test reporting.
- 19 Figure 11: Delay and Jitter Measurements for an Emulated VoIP Client

Test Tool Evolution Keeps Pace with Network Operator Needs

Focus Turns to 'Triple Play'

Service provider networks are evolving rapidly. Today, it is imperative for network operators to support the so-called "triple play" scenario of voice, data and video riding the same network, contending for the same bandwidth.

Even the mainstream press is recognizing that broadband networks are evolving. CNN reported recently that broadband Internet access via cable TV will hit 100 Mbps as early as next year, more than 50 times faster than the average broadband speeds now offered to homes. Some service providers in the Far East already are offering field trials of such services on a "best-efforts" basis. And Europe is close behind.

Such a rich traffic landscape, supporting triple play traffic focuses the need for dynamic network simulation and traffic generation. The advent of 'triple play' networks drives the requirement for tightly integrated test tools that employ a single user interface up and down the protocol stack to deliver rich analysis and performance insights.

This new emphasis on application-level guarantees is the catalyst for test tools moving up the protocol stack. While service providers traditionally have tested at Layer 2/3, the focus now is to show that application performance is acceptable even under periods of network congestion. At the end of the day, what is important to customers is the way that their applications actually behave on service provider networks. So, being able to emulate and measure performance with real, live application traffic is becoming vitally important.

Shenick Network Systems commissioned The Tolly Group in July 2005 to examine the company's diversifEye™ integrated network, application and security performance test system. The diversifEye platform offers a high degree of granular control over each application flow and individual network services to measure Quality of Service (QoS) and Quality of Experience (QoE) with a high degree of accuracy.

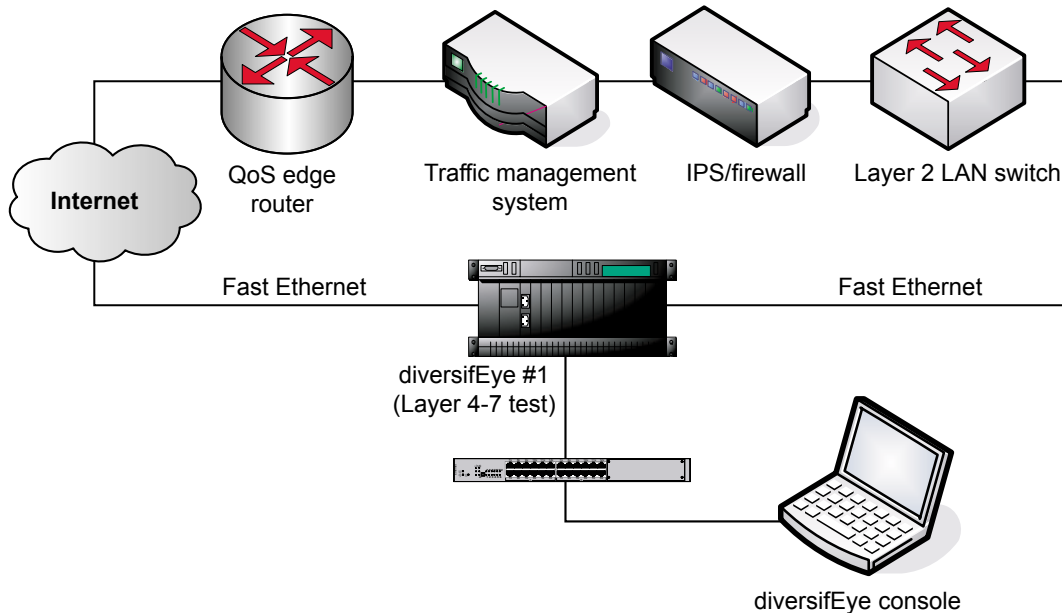
QoE is a higher-level abstraction of network measurements. While engineers may capture throughput, latency and delay rates, such results often are meaningless to end users. Instead, QoE equates to the time required to change a channel in an IP TV application, for instance, or for a Web page to download; QoE identifies the performance measurement that is most meaningful to end users.

It is QoE that is particularly important in the context of 'triple play' networks, security and traffic-shaping applications, since this type of benchmark reveals precisely what the user is experiencing.

The objective of the diversifEye testing was to test an access network with triple-play traffic mixed with Distributed Denial of Service (DDoS) traffic which attempts to overwhelm the network with invalid traffic and thus deny service to valid users and P2P that consumes too much service provider bandwidth. Such triple play traffic represents revenue generating "value-added" services like VoIP and video.

The test network had a variety of service levels policed by the traffic manager and security policies implemented by the firewall. Since these devices use Deep Packet Inspection they affect application performance. Therefore, the services are tested by diversifEye to test Class of Service performance for triple-play traffic and the user-experience, before and during attacks and various volumes of P2P. Overall, this is achieved by first testing the performance of individual elements and then as a complete system.

Figure 1: Network Test Bed



Tightly Integrated Architecture

Shenick's diversifEye platform represents a tightly integrated set of test tool functions that meld traffic generation, emulation, simulation and reporting/analysis capabilities into a single unit that pulls together functions that users previously would assemble from multiple devices.

The company describes the diversifEye platform as "an integrated network and application layer (Layer 2-7) end-to-end QoS test system that enables a per-client view of Quality of Experience (QoE). diversifEye achieves this by emulating real-world applications and measuring the statistics that constitute quality on a per-application basis, providing a network, service and user view of network and application server performance."

Although The Tolly Group tested the diversifEye 8400, the company also markets a diversifEye 4200 chassis. Both testers utilize the same Java client and the test modules are interchangeable between chassis. See <http://www.shenick.com/products.htm>.

What is unique about diversifEye is that it delivers integrated Layer 2-7 testing in a single chassis. A single test port on the diversifEye platform can emulate both a back-end server (to which requests are channeled through the DUT), as well as emulate multiple front-end, load-generating clients. The test tool also supports per-flow testing, which enables users to drill down on an IP address level to gather performance data that can be analyzed to assess the QoE.

This is important for service providers who may wish to assess 'triple-play' services on an application-by-application basis, since each typically has a different performance objective and variable traffic class. Likewise, network operators concerned with security can evaluate the efficiency of security policies and determine the affect of attacks on normal traffic – well before attacks occur.

Finally, QoE data is important for organizations that perform traffic shaping since service providers need a per-subscriber analysis to determine that the shaper is doing its job with regards to applicable policies and that the shaper is accurately identifying the volume of traffic, by application type, traversing the net.

The diversifEye platform also is based upon a full RFC-compliant TCP stack that gives users a high degree of control over TCP stack parameters. And the tool furnishes extensive real-time and post analysis reporting with full access to recorded data.

Performance Matters

Performance Attributes:

Shenick Network Systems claims the diversifEye 8400 chassis delivers:

- Support for 2,000,000 simultaneously open application flows or virtual clients
- Generation of up to > 2 Gbps of server-side application traffic
- Creation of 75,000 transactions per second with a transaction equal to the TCP session open, data transfer and session close
- Units are stackable and one Java client can control several systems as one logical tester

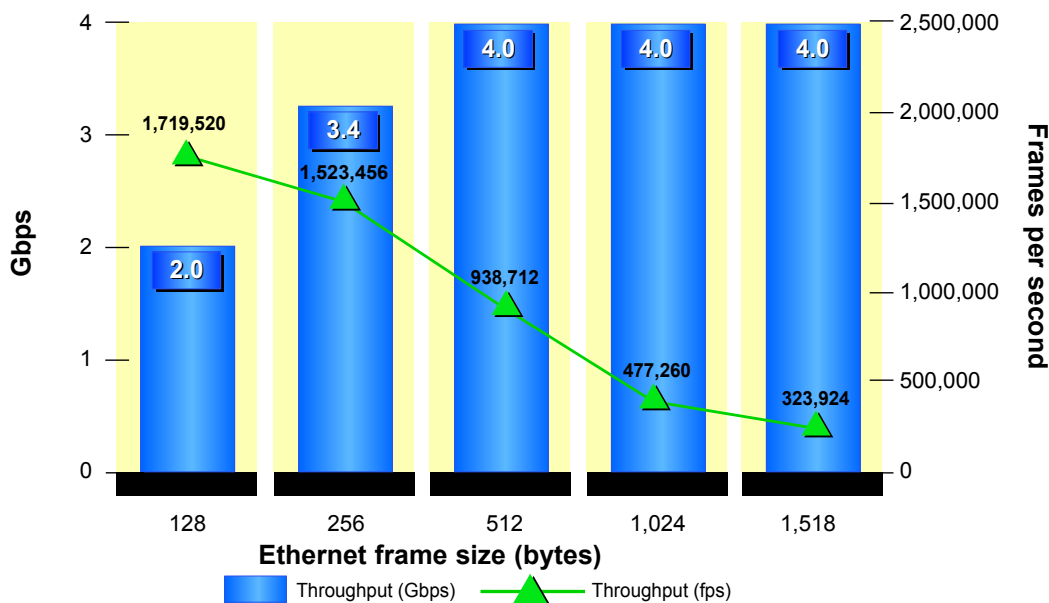
While Shenick's philosophy is that the importance of today's network testing lies at the upper protocol stack levels, the company recognizes the continuing need to validate lower stack performance as well, instead of investing separately in a load generator for Layer 2/3 testing and another platform for Layer 4-7 testing.

First, The Tolly Group examined the diversifEye 8400's ability to generate Layer 2 traffic and measure aggregate Layer 2 throughput across a representative industry firewall. (As the focus of the paper is the testing solution "tested" infrastructures will be referred to only generically.)

For this test, Tolly Group engineers connected the Shenick diversifEye 8400 to the firewall under test and configured it to execute an aggregate Layer 2 throughput test at the appropriate load, on Ethernet frame sizes of 128, 256, 512, 1,024 and 1,518 bytes for a 60-second test duration. Engineers configured the Shenick diversifEye 8400 to send and receive the test traffic through the firewall in a two-segment configuration in which four ports on the tested device were utilized. They recorded the throughput as the Layer 2 received bps reported by the diversifEye 8400 and reported actual throughput on the Ethernet link. (See Figure 2, below.)

Figure 2: Layer 2 throughput and frame rates

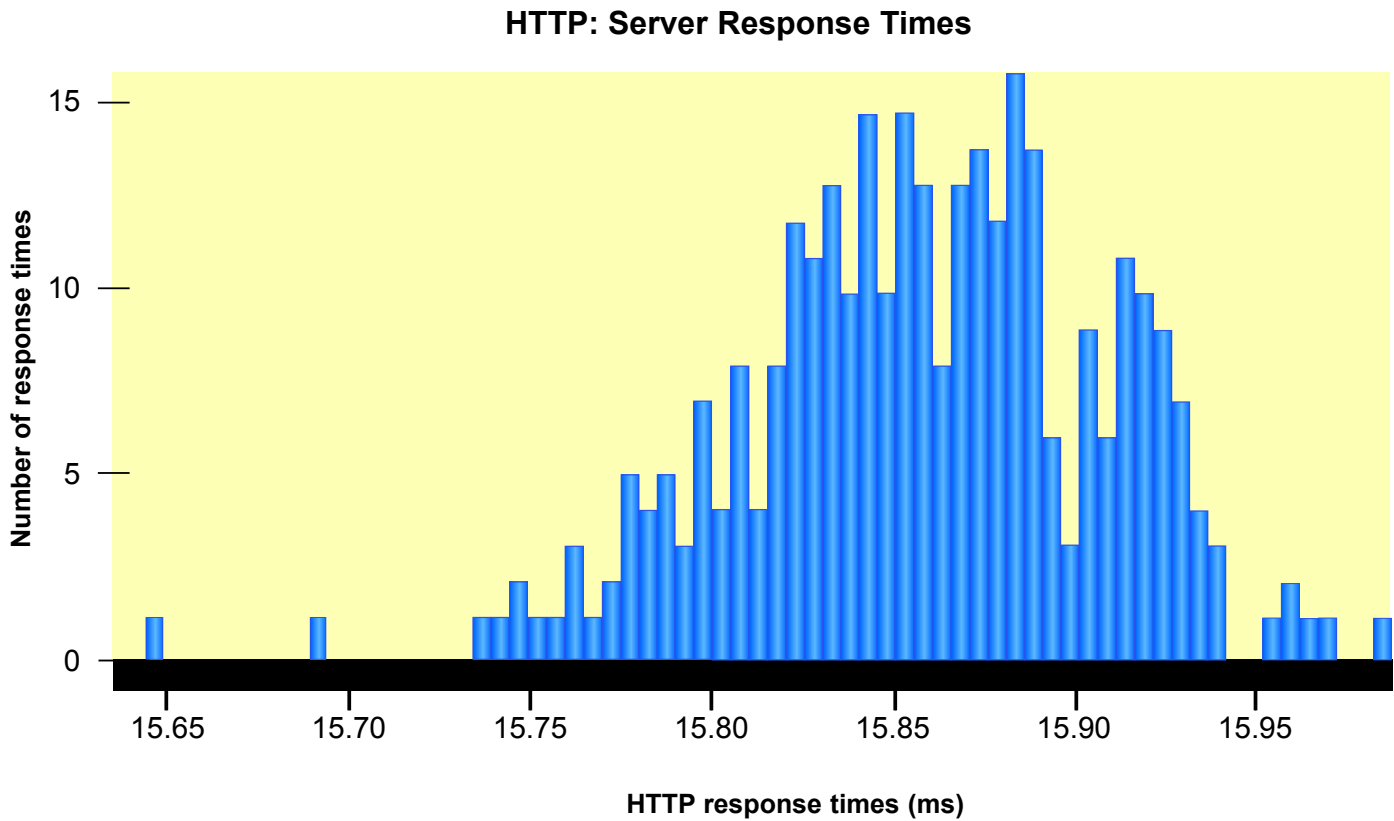
Zero-loss ($\leq 0.001\%$) Layer 2 Aggregate Throughput in a Dual-Segment or Four-Segment GbE Port Configuration as Reported by Shenick diversifEye 8400



Engineers also measured the HTTP throughput of the firewall when the simulated HTTP 1.1 clients retrieved 10K fixed objects from four emulated HTTP servers. For the TCP handshaking, a three-way open and three-way close option was selected.

Tests show the diversifEye 8400 was able to drive 1,232 Mbps of HTTP traffic through the firewall with exceptional HTTP server response times. (See Figure 3.) During the test the firewall handled 273,410 packets per second (pps) of traffic sent to it by the diversifEye 8400. This test proves that the diversifEye 8400 generates real HTTP traffic and measures the resulting HTTP throughput in Mbps and in pps, and also reports the HTTP server response time in milliseconds. (See Figure 3, below.)

Figure 3: Distribution of HTTP server response times



Driving Traffic

Stateless packet tests provide important data, but it is increasingly important to understand the behavior of "stateful," session-oriented traffic as well.

Increasingly, it is important to drive stateful test traffic across a firewall, intrusion system, or other device to ascertain the connection per second rate and the aggregate number of connections the tested device can handle. Security and shaping can affect device performance and it is best to find that out under controlled conditions - and prior to deployment.

In this test, Tolly Group engineers established the connections between a representative firewall tested and the diversifEye 8400 in a four-segment configuration. They also configured the diversifEye 8400 to test for the maximum open connections, the maximum connection rate and the maximum throughput. For the open connection and the connection rate tests, four diversifEye 8400 ports were configured to emulate 600 HTTP clients and send HTTP/1.1 GET requests to retrieve 50-byte fixed objects from the other four diversifEye 8400 ports which emulated four HTTP servers. For these tests, a three-way open and RESET close option was selected. Engineers verified that the firewall tested was able to achieve a connection rate of 37,828 connections per second and support 1,500,712 established open connections.

This test proves that the diversifEye 8400 generates real HTTP traffic and measures the maximum open HTTP connections and aggregate established open connections. The key point is that the diversifEye 8400 can drive traffic at an exceptionally high level to meet the demands of large enterprises and service providers.

It is important to note that the diversifEye product line (both the 8400 and 4200 models) can emulate a specified amount of Layer 4-7 traffic to mirror the traffic observed on a typical enterprise or service provider network. For instance, a given test can be run with 60% P2P traffic, 20% HTTP traffic and 10% IPTV streams. This demonstrates that the diversifEye product line not only can scale to 1.5 million+ open connections, but it can recreate specific network environments to simulate actual network conditions.

Real-World Performance Under DDoS Attacks

With Denial of Service (DoS) attacks and other pernicious security threats prevalent on the Internet and in private networks, test tools need to help users understand the effect on customer QoE under attack conditions. Crippling Distributed Denial of Service (DDoS) attacks during virus attacks can cause havoc.

Shenick's diversifEye platform offers attack throughput testing on an 'end-to-end' basis for DDoS attacks, worm propagation, viruses and spam. The diversifEye platform enables service providers to benchmark the performance of a network device with regular IP traffic flows, while simultaneously introducing disruptive IP events like mail-borne viruses, DDoS attacks, etc.

The diversifEye's integrated client and server mode of operation provides both an attacker and a victim view. Reflective DDoS attacks are also fully supported in diversifEye with emulation of attackers, unwitting participants and victims. Shenick diversifEye also can generate both real viruses as E-mail attachments and also safe-mode 'defused' viruses. Every E-mail can have a different attachment to emulate a real-world mix of regular message attachment traffic, virus/worm and spam E-mails.

DDoS Test Validation

For this test of a SYN Flood attack with simulated real-world traffic, engineers made the necessary connections between a representative intrusion detection system (IDS) and the diversifEye 8400 traffic generator in a four-segment configuration. All segments were configured to generate both HTTP traffic and the SYN Flood attack traffic. The HTTP traffic generation was the same as the previous HTTP throughput test.

In addition to background HTTP traffic, engineers introduced the SYN Flood DoS traffic in four incremental steps. That is, the diversifEye 8400 was configured to emulate a distributed DoS attack, where attack

DDoS Attack Update

Shenick says that diversifEye attacks include the following DDoS types and enhancements to the list are made with every release:

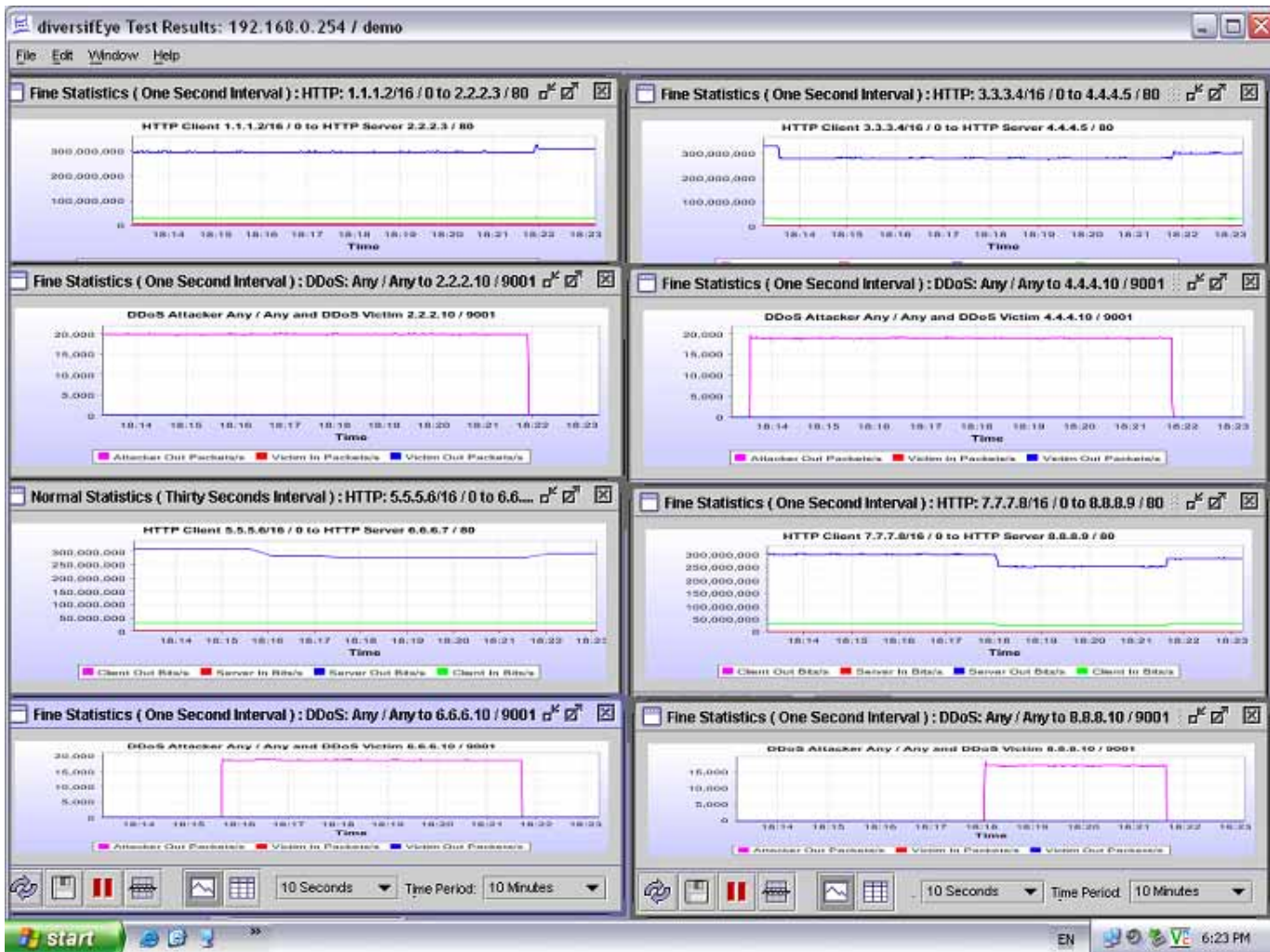
- ARP Flood
- Ping Sweep
- Ping of Death
- Reflective DDoS attacks
- Reset floods
- "Smurf" attacks
- SYN Flood attacks
- TCP port scans
- Teardrop attacks
- UDP port scans
- UDP Flood
- XmasTree

packets were issued with unique IP addresses. Each DDoS entry generated 20,000 SYN PPS. While background traffic was flowing across the DUT, engineers initiated one DoS attacker and monitored the changes in the performance. After two minutes, engineers introduced another DoS attacker and so on. Finally, engineers recorded the performance variations in the background HTTP traffic with the presence of four DoS attackers which generated 80,000 SYN pps. Engineers measured the performance in Mbps.

Tests show that the diversifEye 8400 generated real HTTP and DoS attack traffic from the same or different interfaces simultaneously and measured the DoS attack block rate as well as the HTTP throughput performance in Mbps and in pps.

In a 10-minute window when DoS attack traffic bombarded the test network, the intrusion detection system tested was able to sustain between 1,154 Mbps and 1,258 Mbps of aggregate throughput.

Figure 4: Snapshot of HTTP throughput and DDoS attack test.



The importance of this test is that it demonstrates that the diversifEye platform not only enables users to generate common network traffic types and flow, but also introduce disruptive IP traffic events from the same test tool.

Until now, users have had to use a mix of tools to generate normal network traffic types, and invoke specialized test procedures to introduce DDoS and other attacks signature traffic onto the test network.

Additionally, diversifEye enables users to incrementally increase the attack traffic rate and bring attacks in and out of service on the fly. This enables users to gauge the precise point at which a network device reaches the threshold of maximum performance while under a sustained DDoS attack.

Compared to other DDoS emulation methods, diversifEye can support a DDoS attack by putting an attacker on one physical interface, locating several thousand legitimate IP addresses on another interface (the unwitting participants to the attack) and the victim on a third interface. Since diversifEye collects statistics on each interface, users can identify if the attack is being stopped between the attacker and the intervening clients, or between the clients and the victim.

Nimda Test Validation

For the Nimda attack test, engineers made the necessary connections between the DUT (a representative industry intrusion detection system) and the diversifEye 8400 in a single-segment configuration. They configured the test tool to generate Nimda attacks using the packet replay option across the IDS. For this test, one diversifEye 8400 port acted as a Nimda attacker and the other port as a victim. Engineers recorded the throughput and connection rate for the Nimda attack block accuracy rate.

Tests show that between 5 Mbps to 8 Mbps of Nimda traffic was injected to the IDS box and was all blocked by the DUT.

One of the primary attributes of the diversifEye platform is its ability to capture and replay attack traffic. This test demonstrates the diversifEye's ability to capture and playback Nimda traffic on one port, while also measuring the effectiveness of an IDS at blocking the traffic from reaching a victim located on a second port.

Layer 2 to 7 Flexibility

The performance of a firewall, switch or other network device depends on the application mix, the security settings and other parameters that may introduce overhead or otherwise come into play. A useful set of per-

Per-flow Analysis

In a typical scenario, one flow may propagate the worm while a second does not. Per-flow analysis shows the performance of the good traffic and the efficacy of the firewall blocking the attack.

formance tests for one company may well be pointless for another. Many vendors issue performance metrics of their products but users are aware these benchmarks often are meaningless in certain environments.

That means network operators need a test tool that delivers a fair degree of traffic flexibility, especially in generating the traffic and measuring the performance as experienced by an end-user.

The diversifEye is an integrated Layer 2 to Layer 7 test platform, which means that each test port can generate 1 Gbps of stateless TCP traffic. However, a combination of stateless TCP and Layer 4-7 stateful applications is required to sufficiently evaluate network devices, stress test switching platforms and examine the impact of multiple application types of network performance.

Network operators who deploy test tools need a device that can offer a flexible mix of stateless and stateful traffic to model network traffic with a degree of realism. Any test tool platform should empower the user to fine-tune application streams to precisely model the traffic usually found in local networks.

The diversifEye is a unique test tool platform that integrates stateless and stateful traffic generation into a single box.

Flexibility Put to the Test

For this test, the objective was to use the diversifEye 8400 to generate a variable mix of stateless and stateful traffic to pass across the test network and then use the test tool to measure the throughput of a representative IDS.

Tolly Group engineers made the necessary connections between the IDS and the diversifEye 8400 in a four-segment configuration. The first three segments were configured to generate stateful HTTP traffic and the last segment was used to generate stateless Layer 2 traffic. Engineers configured the test tool to generate the gigabit-rated stateful traffic and stateless traffic in the mix of 100:0, 90:10, 80:20 and 70:30.

For the stateful traffic, three diversifEye 8400 ports were configured to emulate 300 HTTP clients and send HTTP 1.1 GET requests to retrieve variable requested data sizes from the other three diversifEye 8400 ports which emulated three HTTP servers. Engineers changed the requested data sizes to adjust the stateful HTTP throughput for 1,000 Mbps, 900 Mbps, 800 Mbps and 700 Mbps. For the stateless traffic, engineers configured the test tool to generate the bidirectional Layer 2 traffic (256-byte Ethernet frames) at the rate of 100 Mbps, 200 Mbps and 300 Mbps.

diversifEye Flexibility

diversifEye enables traffic shaping, concurrent connection and rate-limiting configuration of stateful traffic.

Test results show that the representative IDS was able to handle over a Gigabit of stateful traffic, as well as a mix of stateless and stateful traffic that exceeded 1 Gbps. (See Figure 5 below.)

What struck testers here is the relative ease with which the diversifEye 8400 is able to dial-up and deliver both traffic types. Engineers recall

Figure 5: Aggregate IDS throughput with stateless and stateful traffic mix.

Layer 2 Throughput with a Variable Mix of Stateless and Stateful Traffic		
Traffic Mix	Stateful (HTTP traffic)	Stateless (Ethernet traffic)
	Aggregate Mbps	
Stateful (100%) : Stateless (0%)	1,006	0
Stateful (90%) : Stateless (10%)	907	100
Stateful (90%) : Stateless (20%)	819	200
Stateful (60%) : Stateless (30%)	725	300

the days of manually interacting with real applications to generate the desired traffic. This often was very painful because it took a fair amount of trial-and-error runs to reach the desired traffic level.

Engineers were impressed with the relative ease and simplicity delivered by the diversifEye 8400 to realistically model and generate stateless and stateful test traffic.

Going with the Flows

In today's networks, where application flows constantly contend for available bandwidth, it is essential for a network test tool to be able to benchmark the performance of application data on a flow-level basis.

Flow-level testing is critical to such key initiatives as the so-called 'triple play' of voice, video and data all sharing a common network framework. Each application has unique performance objectives and requires specific QoS treatment as it traverses the network.

Service providers often want triple play services to deliver performance tailored specifically for the application type, to maximize bandwidth and deliver the QoE users come to expect of an application service.

Finally, any network operator or service provider intent on performing per-subscriber analysis will need a test tool that can perform per-flow testing to determine if traffic shapers in use are observing set policies/SLA agreements and can accurately identify the volume of traffic passing across the network under test.

Per-Flow QoS Testing

There were two different tests in this section. One was a Per-Flow test focusing on QoS delivered by an application-aware traffic management system which provides bandwidth limitation and QoS based on assigned policy and application type. The other test was a Per-Protocol-based test.

A pair of diversifEye 8400 ports were used for both tests. One port emulated a group of clients and the other emulated a group of servers across the DUT.

Each client and server was assigned a different MAC/IP address. For the Per-Flow test, one diversifEye port emulated four HTTP clients retrieving 3,500 bytes of data from a single emulated server across the DUT. Engineers configured the traffic shaper to provide the different bandwidth limitation for four traffic flows which were based on the source and destination IP addresses. With this configuration, the DUT limited the bandwidth of flow #1 by 5 Mbps, implemented a bandwidth ceiling of 10 Mbps on flow #2 and restricted bandwidth on flow #3 to 20 Mbps and flow #4 to 40 Mbps.

Figure 6: Application response times over a link that was rate limited to 40 Mbps. (Note the subsecond response times.)

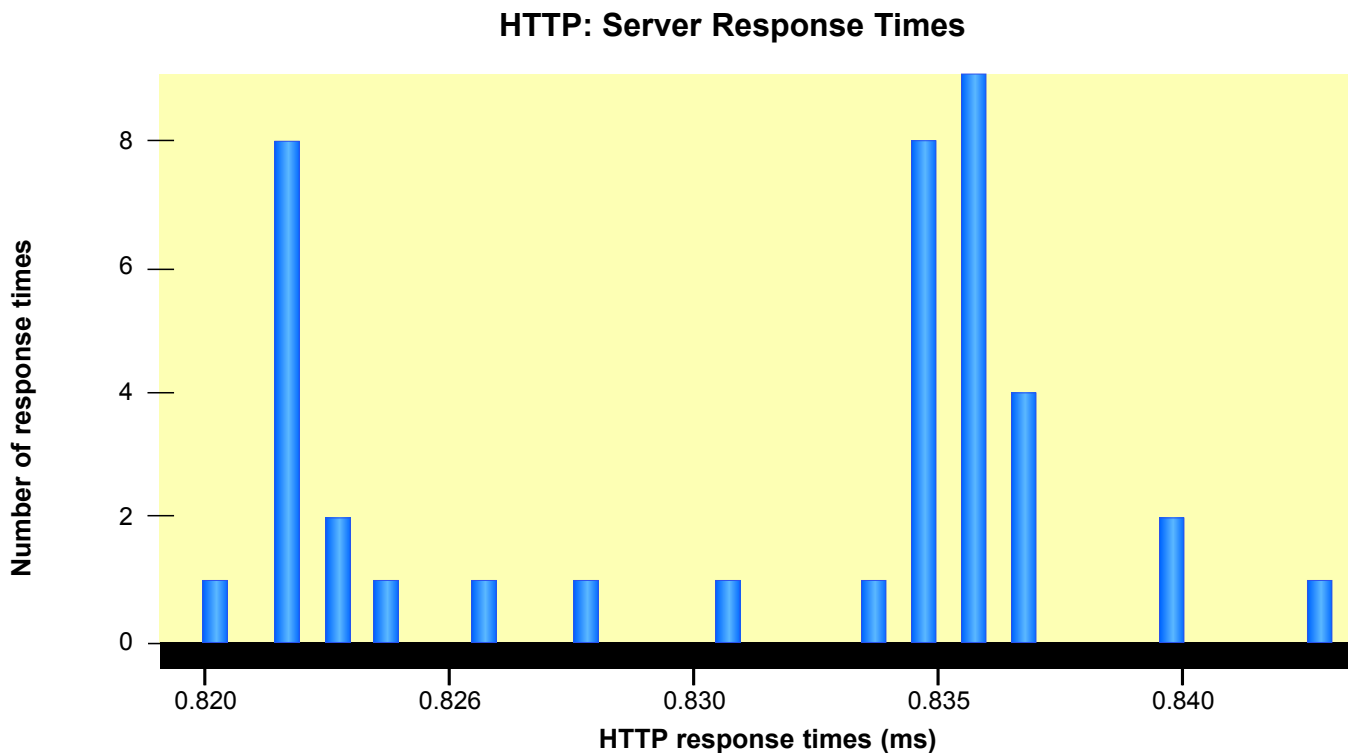
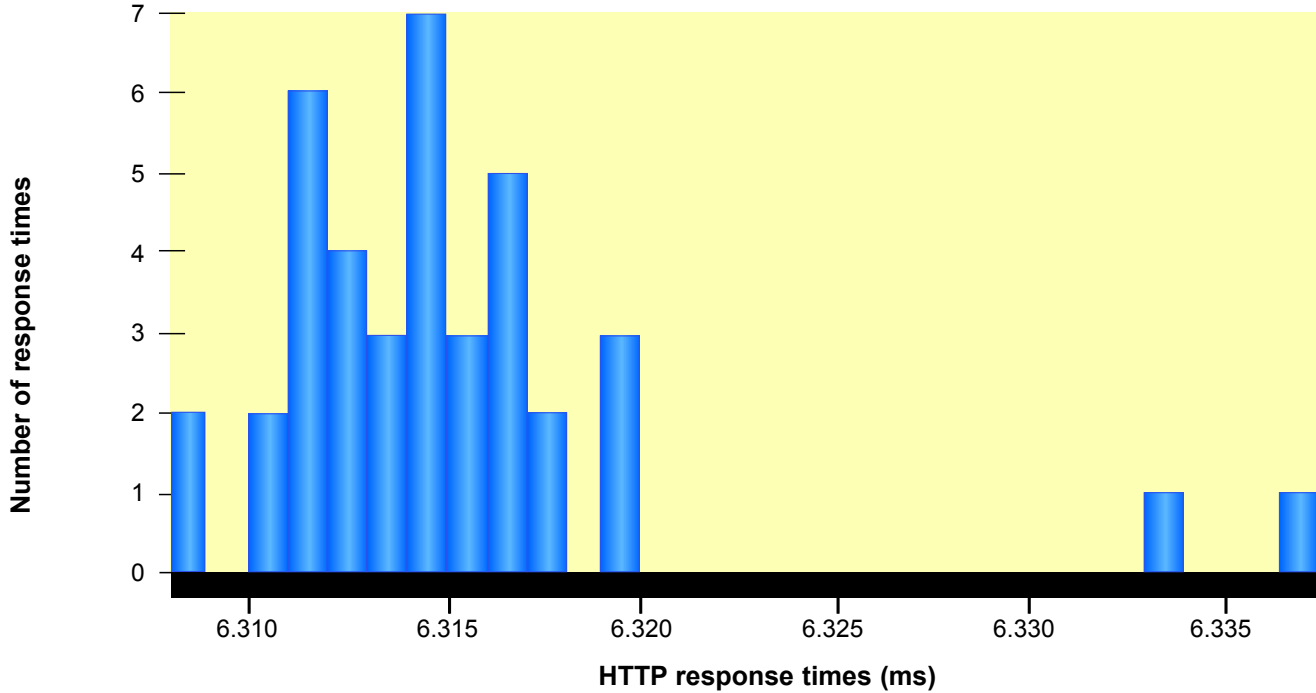


Figure 7: Application response times over a link that was rate limited to 5 Mbps. (Note the significant increase in response times due to greater contention for a smaller amount of available bandwidth.)

HTTP: Server Response Times



Engineers recorded the throughput for each flow reported by the diversifEye 8400.

In the Per-Protocol test, one diversifEye 8400 port emulated four Web/HTTP clients, four SMTP clients, four POP3 clients, one multicast client and two P2P nodes. A second port emulated one Web/HTTP server, one SMTP server, one POP3 server, one multicast client and two P2P nodes.

Figure 8: Per-flow bandwidth allocation test results.

Layer 2 Throughput with a Variable Mix of Stateless and Stateful Traffic			
	Client (Mbps)	Client (pps)	Client established connections per second
Flow #1 (Rate limited to 5 Mbps)	4.6	654	16
Flow #2 (Rate limited to 10 Mbps)	9.0	1,292	31
Flow #3 (Rate limited to 20 Mbps)	17.5	2,502	60
Flow #4 (Rate limited to 40 Mbps)	34.1	4,866	116

The detail configuration for each protocol was as follows: The four SMTP clients sent a 1K E-mail object to the SMTP server. The four POP2 clients received a 240-byte message from the POP3 server. The multicast server transmitted a 1-Kbyte payload file at the rate of 2 Mbps to the multicast clients. For this test, only one client joined the multicast group. The first P2P peers emulated the Gnutella P2P communication by sending and receiving 4 Mbytes of file

continuously. The second P2P peers emulated a Kazaa P2P communication by sending and receiving 24 Kbytes of file continuously. Engineers configured the DUT to limit the bandwidth based on the source/destination IP addresses and TCP/UDP port numbers such that the DUT limited the bandwidth of the HTTP traffic in the same way as the previous Per-Flow test. Besides, the DUT rate-limited the multicast traffic and Gnutella by 1 Mbps and 40 Mbps respectively.

Figure 9: Per-flow performance of traffic shaper tool.

Traffic Shaper Per-Protocol Performance				
Traffic type	Client out (Mbps)	Server in (Mbps)	Server out (Mbps)	Client in (Mbps)
HTTP (Unlimited bandwidth)	1.7	1.7	54.2	54.2
SMTP (Unlimited bandwidth)	3.5	3.5	0.3	0.3
POP3 (Unlimited bandwidth)	0.3	0.3	3.7	3.7
GMP/Multicast (Rate limited to 1 Mbps)	0	0	2.0	0.9
	Peer 1 out (Mbps)	Peer 2 in (Mbps)	Peer 2 out (Mbps)	Peer 1 in (Mbps)
P2P-Gnutella (Rate limited to 40 Mbps)	0.7	0.7	37.3	37.3
P2P-Kazaa	0.6	0.6	0.7	0.7

Results of the Per-Protocol test show that the traffic shaper tested can rate limit according to per-protocol attributes. More importantly, the Per-Protocol test proves that the diversifEye 8400 delivers client and/or server emulation for Multicast, Web, E-mail and assesses the QoS attributes for each, along with the user experience as measured by the per-flow emulation and quality analysis.

It is important to note here that the per-flow tests demonstrate the ability of

the diversifEye 8400 to generate multiple flows from one physical port, a rarity among test tools. Each flow represents a single client, be it Web, SMTP, or other client type. By simulating multiple flows from the same port, users can achieve more realistic traffic emulation. Additionally, diversifEye 8400 enables users to track performance metrics on a per-flow basis. Users get info on application-specific statistics, network and transmission statistics and byte/packet stats.

Further, the detail provided by the diversifEye 8400 reporting facilities enables network operators to identify a more refined understanding of performance. For instance, while the network may yield high packet throughput, closer inspection of TCP statistics shows the 'goodput' revealed by Layer 4 statistics usually in the form of TCP retransmissions or the number of failed connections or out-of-sequence packets.

It is this type of performance detail that enables network operators and service providers to identify QoE characteristics and help service providers define their SLAs.

Bringing It All Together

Tolly Group testing focused on individual capabilities delivered by the diversifEye 8400, somewhat analogous to listening to different sections of an orchestra play solo. However, we capped our comprehensive examination of the diversifEye 8400 with a final test in which we brought all of the testing facilities together, into one test bed. In effect, this was our "stress test" of the diversifEye 8400, forcing it to multitask on different fronts.

The network under test included an edge router, a traffic management system, an IPS/firewall and a LAN switch. Two Fast Ethernet ports of the edge router were configured to route the traffic from two subnets and prioritize the traffic based on assigned DSCP values.

Engineers took the opportunity to exercise the diversifEye 8400 to generate HTTP traffic and measure throughput of a representative firewall. HTTP traffic represented the "data" traffic. In total, 10 HTTP clients sent HTTP 1.1 GET requests to retrieve 10 KB of data from the server for each direction. The HTTP traffic had a DSCP value of 0.

At the same time the test tool was pumping out streaming video (IPTV) and measuring the flow of the video feed from the server to the client. In all, 10 streaming clients received 2 Mbps of traffic from the server for each direction. The streaming traffic had DSCP value of 32.

While all that was happening, engineers configured the diversifEye 8400 to generate P2P traffic and directed it through the traffic shaper that rate limited Gnutella traffic to 2 Mbps, and blocked all Kazaa traffic it encountered. But that's not all, either. Engineers also dialed up a DoS attack, flooding almost 5 Mbps of DoS attack traffic on to the network with the aim that an attached IPS would block it. And while all of this was happening, the diversifEye 8400 directed delay-sensitive voice traffic onto the network, measuring the degree of latency and the one-way trip time across the network. The delay-sensitive VoIP traffic had a DSCP value of 48.

Engineers monitored the real-time statistics and recorded the performance results based on the application, the service and the port.

Figure 10 shows how the diversifEye 8400 reported about the performance of the various concurrent tests.

Here we see that the diversifEye 8400 generated 1.5 Mbps of on the server side, and the server responding with 134.1 Mbps of simulated traffic from the server-side interface of the diversifEye 8400.

Simultaneously, the diversifEye 8400 was streaming 39.3 Mbps of IPTV traffic out of its server-side interface, and an equal amount of traffic was received on the client-side interface.

Application Support

In addition to a wide range of supported protocols, diversifEye enables replay of captured network traffic to emulate esoteric or non-standard applications such as Skype.

Tests show that the diversifEye 8400 generated 1.8 Mbps of Gnutella traffic and received an equal amount of the peer-in side. Also, even though the P2P peers were sending 24K-byte Kazaa files continuously, we see that the attached traffic manager blocked the traffic according to preset policies.

Also, diversifEye 8400 reports that 4.8 Mbps of DoS attack traffic left an attacker interface, but none of it got through to the intended victim interface.

Figure 10: Multitasking traffic generation and test reporting.

diversifEye 8400 Multitasking Test				
Traffic type	Client out (Mbps)	Server in (Mbps)	Server out (Mbps)	Client in (Mbps)
HTTP (Data)	1.5	1.5	134.1	134.1
Streaming (Video)			39.3	39.3
P2P-Gnutella (Rate limited to 2 Mbps)	Peer out (Mbps)			Peer in (Mbps)
	1.8			1.8
P2P-Kazaa (Firewall blocks Kazaa)	Kazaa traffic blocked, no connections			
DoS (IPS blocks DoS attack)	Attacker out (Mbps)	Victim in (Mbps)		
	4.8	0.0		
Delay-sensitive voice	Client mean latency (milliseconds)	Client - Min. one-way trip time (milliseconds)	Client - Max one-way trip time (milliseconds)	
	2.0	0.046	9.702	

Finally, delay-sensitive voice traffic traversing the network incurred latency of just 2 milliseconds.

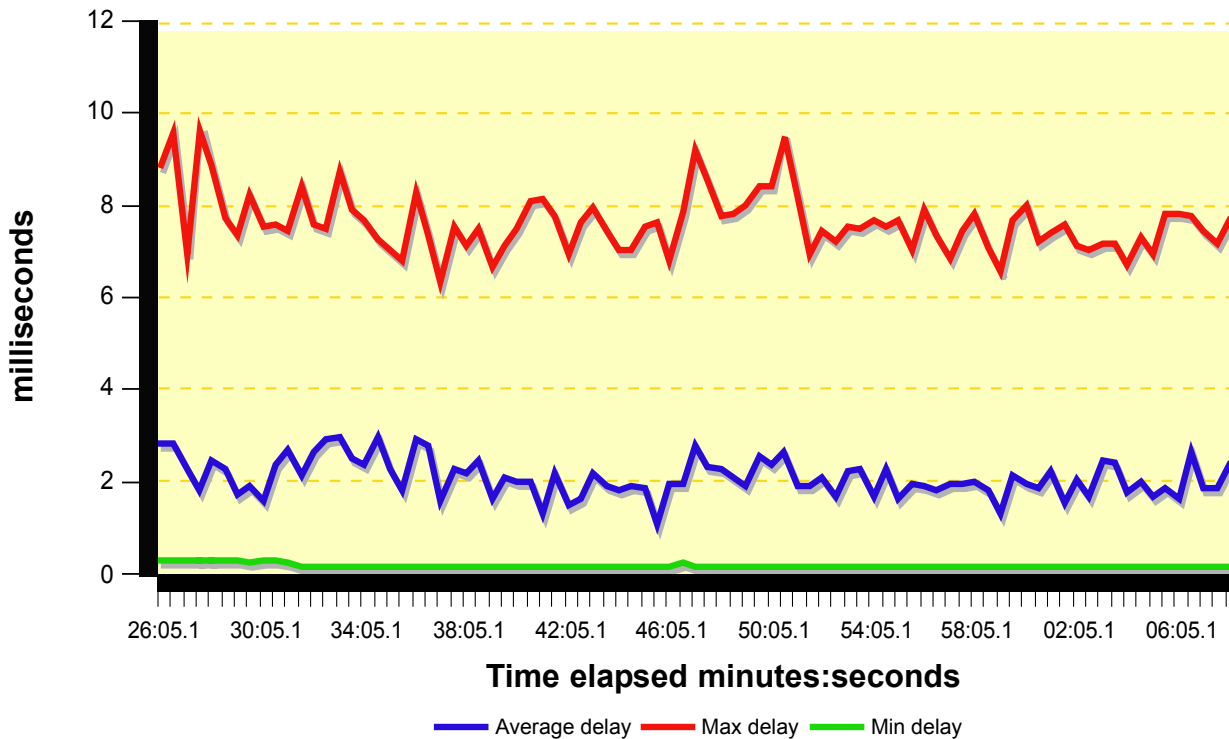
The key point of this test is that the diversifEye 8400 successfully emulated multiple mixed applications over the large-scale and complex enterprise/service network environments, and also was able to report in fine detail about the performance of those traffic types.

In effect, by bringing together the sum of the individual tests conducted on the diversifEye 8400, Tolly Group testers were able to obtain a composite of the various functions that enables users to assess the QoS and QoE on the network. Finally, it is important to note that in these tests

the diversifEye 8400 generated the traffic volumes as observed by our "imaginary" service provider and also emulated real IPTV, P2P and other applications.

Figure 11: Delay and Jitter Measurements for an Emulated VoIP Client

**Delay and Jitter Measurements for an Emulated VoIP Client
as Reported by Shenick diversifEye 8400**



Turning the Triple Play

Today's multiprotocol networks have been designed to support the "triple play" of voice, data and video. However, service providers and other network operators still need the tools that enable them to perform accurate traffic modeling and assess network conditions and anticipate the impact of changing conditions so they do not adversely impact service quality.

Shenick Network Systems diversifEye platform has demonstrated that it is an able platform for Layer2/3 testing, and has been designed specifically to handle the rigors of Layer 4-7 testing.

The test tool's support of per-flow testing makes it possible to gather the data required for service providers and others to assess the quality of the user experience. This will prove to be an indispensable function for enter-

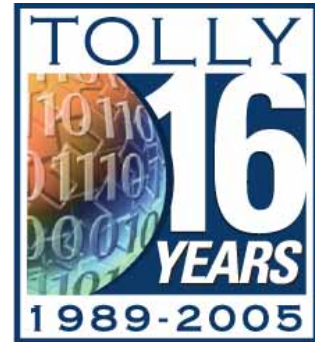
prise and service provider users who need the type of detailed data to model the user experience and meet the expectations of customers.

Moreover, Shenick has demonstrated that it has taken into account the needs of a wide spectrum of users - from engineers who need lower-level performance data, to security experts who need to model what impact network disturbances will have on existing or new equipment, to application providers who need credible information about the performance they can expect in certain network conditions.

Tests confirm that Shenick has a deep understanding for the needs of service providers and other network operators. The diversifEye network test tool is an ideal device for 'triple play' network measurement. The diversifEye tool is likely to become an indispensable tool for measuring performance up and down the protocol stack.

###

Information technology is an area of rapid growth and constant change. The Tolly Group conducts engineering-caliber testing in an effort to provide the internetworking industry with valuable information on current products and technology. While great care is taken to assure utmost accuracy, mistakes 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. All trademarks are the property of their respective owners.



The Tolly Group, Inc.
3701 FAU Blvd. Suite 100
Boca Raton, FL 33431
Phone: 561.391.5610
Fax: 561.391.5810
<http://www.tolly.com>
info@tolly.com

