

ipoque PRX-10G Traffic Manager

Peer-to-Peer Monitoring and Filtering Test Report

Introduction

ipoque GmbH commissioned EANTC to independently verify the peer-to-peer monitoring and control capabilities of their PRX-10G Traffic Manager device. The tests were conducted at EANTC's lab in Berlin in January 2009.

The goal of this test was to verify the functionality and performance of ipoque's PRX-10G Traffic Manager with regard to Deep Packet Inspection. We focussed on peer-to-peer traffic detection and policing and the suitability of deployment in Internet Service Provider (ISP) environments.

In order to demonstrate to ISPs that P2P detection and control solutions will integrate smoothly into their existing networks and will not harm the network performance and operations, we emulated ISP conditions in our peer-to-peer test lab environment. The P2P applications used during our tests were selected according to their popularity, difficulty in recognition and foreseeable future trends.

Executive Summary

In our tests we were able to verify ipoque's PRX-10G Traffic Manager performance claims to handle up to 60 Gbit/s of traffic. The PRX-10G was able to correctly detect all peer-to-peer application protocols up to the limits of the test bed (around 25 Gbit/s) and measured the traffic volume for each of the P2P protocols with 98.5% accuracy. In addition, PRX-10G was threatened with up to 60 Gbit/s of plain IP traffic which it forwarded without any packet loss. According to ipoque's explanation of the system architecture, the P2P application layer throughput should reach 60 Gbit/s equivalently.

We achieved also very good results for the P2P detection tests with 97.6% accuracy. Only 0.006% of the traffic was not blocked as expected.

Our test of an asymmetrical routing scenario — a somewhat typical challenge in a service provider backbone — showed a detection and filtering ratio of only around 50% of the emulated P2P traffic. The PRX-10G's performance and detection accuracy was not influenced in any way by the presence of VLAN tags.

ipoque
PRX-10G Traffic Manager

- ✓ **Performance**
Passed mixed P2P traffic at 25 Gbit/s; IP traffic up to 60 Gbit/s (test bed limit)
- ✓ **Detection and Regulation**
99% accurate for all popular P2P protocols

Test Period: January 2009
DUT with Firmware Version 2.8
© 2009 EANTC AG

Tested by
EANTC
2009



Tested Device & Test Equipment

ipoque's PRX-10G Traffic Manager is a carrier-grade bandwidth management solution scalable up to six Gigabit Ethernet or six 10Gigabit Ethernet links, enabling operators to monitor and control network traffic per application and per subscriber. According to ipoque, the PRX-10G version we tested offers the following features:

- Load balancing and high availability with automatic hardware-based failover,
- Application detection with a combination of layer 7 deep packet inspection (DPI) and behavioral traffic analysis
- Support of all major protocols used for peer-to-peer file sharing (P2P), instant messaging (IM), media streaming, Internet telephony (VoIP), tunneling and online gaming,
- Integrated QoS management and accounting features.

We operated the Device Under Test (DUT) PRX-10G Traffic Manager in a transparent mode, forwarding or blocking the traffic without intervening with the higher protocol stack layers. The adjacent switches and routers see the DUT as no more than a wire.

In the test, EANTC used several devices to emulate ISP conditions. An Ixia XM12 analyzer with IxNetwork and IxLoad software generated IP flows, emulated HTTP and a range of peer-to-peer protocols. The Ixia emulated very large number of simultaneous BitTorrent, eDonkey, Gnutella and other P2P protocol sessions by replaying previously captured live application layer traffic from a variety of popular P2P clients.

In addition, two Windows XP workstations were integrated into the test bed to allow verification with real P2P clients. The PCs had a real connection to the public Internet, whereas the IxLoad application replay worked between emulated instances between the tester ports.

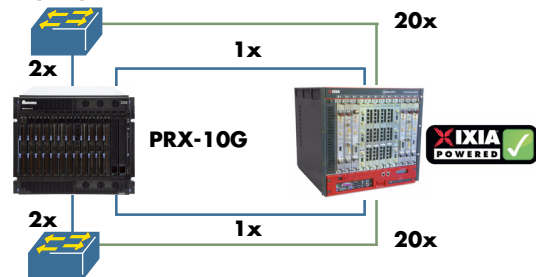
Test Setup

In our tests we used different setups of the test bed for each specific aspect. For the IP layer performance tests, we connected the IP load modules of the analyzer to the DUT directly and via separate third party aggregation switches.

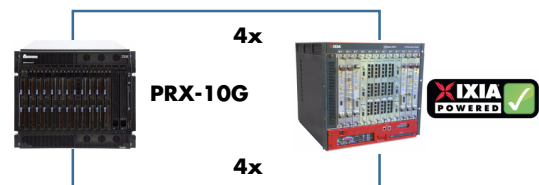
For the application performance, detection and filtering tests, as well as for the VLAN encapsulation tests, we connected the application load modules directly to the DUT using 10 Gigabit Ethernet links. We configured a third party router to set-up the asymmetrical routing scenario and to attach workstation PCs and a DSL router to the test bed. With the latter, we were able to perform tests with the real P2P clients.

The figures below show the three test bed configurations.

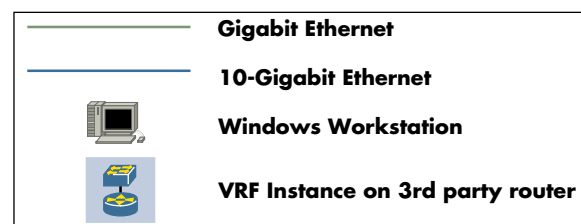
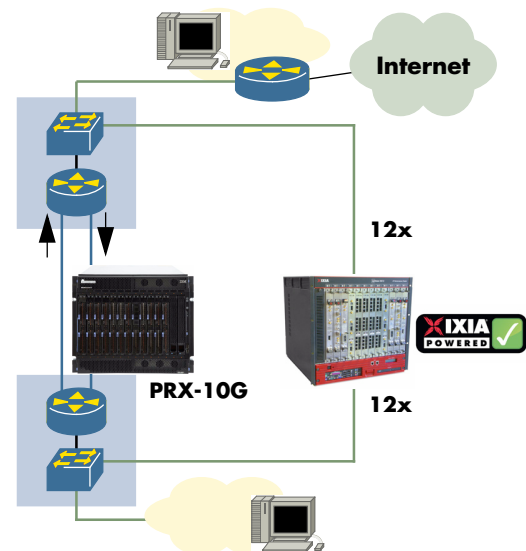
IP Layer performance test



Application layer performance and P2P detection/filtering tests



Asymmetric routing and real client tests



Test Methodology

Following up EANTC's test of P2P solutions as published in Internet Evolution (http://www.internetevolution.com/document.asp?doc_id=148803) in March 2008 we massively increased the bandwidth of the test bed connecting to the DUT for this second testing campaign

We performed the test in three phases. First we verified the performance characteristics of the DUT for both IP layer and application layer traffic. In the second phase we focused on detection, regulation and filtering accuracy under load. In the third test phase we emulated special ISP traffic conditions such as asymmetric routing and encapsulated traffic.

Once we had measured the maximum throughput for PRX-10G Traffic Manager we used this value for the peer-to-peer detection, regulation and filtering tests. We verified the detection accuracy by comparing the analyzer's send and receive statistics with the statistics produced by PRX-10G Traffic Manager.

To ensure a realistic service providers traffic scenario, we added background traffic to the protocol test traffic. This background traffic consisted of stateful HTTP traffic and was aimed to mimic typical load scenarios of ISP links.

Performance Test Results

IP Layer Throughput

In this test we measured the raw IP throughput performance for traffic without peer-to-peer application content. We sent plain IP traffic without any higher protocols (UDP or TCP) in order to give the DUT the theoretically simplest traffic to analyse. However since these packets will still have to pass through the DUT's DPI engine, the forwarding capability is additionally stressed. Compared to a simple switch, a DPI device will at least have to store the packets in memory and prepare them for the analysis. According to ipoque, PRX-10G Traffic Manager analyzes all packets, regardless of the detected upper layer protocol.

ipoque claimed that PRX-10G Traffic Manager is able to handle at least 60 Gbit/s of total traffic. In this test we were able to verify this throughput performance using the following traffic mix which reflects well the typical distribution of packet sizes in ISP networks:

% of Sent Packets	IP Frame Size [Byte]
40	46
20	522
40	1500
Average Packet Size	728.8

Forwarding Performance for peer-to-peer Application Traffic

With this test we aimed to determine the DPI engine analysis performance. Using the Ixia XM12 analyzer, we generated a mix of HTTP traffic and the three most popular P2P protocols: Unencrypted BitTorrent, eDonkey and Gnutella in a proportion typically observed in the Internet. In total, we emulated 40,000 concurrent TCP connections with a total bandwidth of 25 Gbit/s. After the test we collected the traffic analysis statistics of the DUT and compared them with the analyzer statistics.

The DUT was able to correctly detect all protocols used and measured the traffic volume for each of them with 98.5% accuracy.

In order to calculate the performance limits of the device, we repeated the tests with a reduced number of processing modules (blades). We observed a linear dependency of the throughput from the number of installed modules. Taking this linearity into account, we can extrapolate that PRX-10G is able to handle up to 75Gbit/s of traffic in a full P2P configuration.

Peer-to-peer Detection and Regulation Test Results

The following group of tests investigated ipoque's PRX-10G Traffic Manager capabilities to detect, regulate and filter peer-to-peer traffic under load.

The following table shows the composition of the application layer traffic we used for all P2P detection and regulation tests.

The P2P traffic bandwidth was distributed into two categories of P2P protocols depending on their popularity and prevalence in the Internet traffic. The protocols in the "functional" category served the verification of general capabilities of the DUT to detect and/or block different P2P protocols and were assigned a small fixed bandwidth. This category included relevant

cases of encrypted protocols and multiple clients for some major protocols.

Category	Protocol	Application	Encrypted	Target Bandwidth, Mbit/s
Non-P2P	HTTP	lXload		12000
P2P Functional	BitTorrent	µTorrent		250
	eDonkey	AMule		250
	MP2P	Manolito		250
	Soulseek	Soulseek		250
	BitTorrent	Azureus	x	250
	eDonkey	EMule	x	250
	Ares	Ares	x	250
	Filetopia	Filetopia	x	250
P2P Performance	BitTorrent	Azureus		2000
	eDonkey	EMule		2000
	Gnutella1	Limewire		2000
	Gnutella2	Shareaza		2000
	DirectConnect	DC++		2000
Total				24000

The protocols in the “performance” category included the most popular P2P protocols and were assigned a larger fixed bandwidth. This category served the verification of the detection capabilities of the DUT under stress.

In total, the DUT was exposed to an offered load of 24 Gbit/s of traffic and 36000 concurrent connections, based on the results of the application throughput test.

Peer-to-peer Detection

First we examined the capability of PRX-10G to detect and accurately report traffic volumes of peer-to-peer protocols. The DUT was running in observation mode and had to accurately report the traffic statistics on each of the P2P protocols we transmitted.

PRX-10G showed a 97.6% detection accuracy across all protocols mentioned in the table above. However, a significant deviation was observed in case of the encrypted BitTorrent and encrypted eDonkey protocols. According to ipoque’s explanation, these protocols are detected with the help of heuristic analysis based on behavior of real clients. ipoque explained that the analysis algorithm may produce inaccurate

results for synthetic traffic generated in the tests, which lacks characteristics of the real client behavior, for example a variation in the number of connections set-up by certain P2P clients.

Peer-to-peer Regulation

In this test we examined the capability of the DUT to limit peer-to-peer flows to a specified amount of traffic volume while at the same time not affecting other user traffic such as HTTP. We modified the methodology of the previous test: The device was now set to shape the amount of peer-to-peer traffic.

The DUT was able to reduce the amount of peer-to-peer traffic transported during the test, while HTTP traffic was not significantly affected. The regulation of the traffic was unbalanced between the different protocols – some were accurately regulated where others showed high deviation. Nonetheless, the total bandwidth regulated was close to the desired value.

Peer-to-peer Filtering

Finally, in this test we verified that the device is able to completely block the P2P traffic, while continuing to forward HTTP without any packet loss or quality of service impairment. We used the same test setup and protocol mix as in the two previous tests.

The PRX-10G showed outstanding performance by completely blocking all P2P protocols present in the mix. In terms of figures, no more than 0.006% of the P2P traffic was able to slip through.

Test Results: Network Operations Constraints

In this series of tests we analyzed the DUT’s behavior in the face of more challenging conditions as are encountered in a typical ISP infrastructure. The two conditions emulated were asymmetric routing and VLAN encapsulated user traffic. Both are common in service provider networks and are transparent to the end user, however, they present challenges to the peer-to-peer control devices to be integrated in this infrastructure.

Peer-to-peer Detection in Asymmetrical Routing Scenarios

Bidirectional traffic could traverse different routes between source and destination. For any peer-to-peer monitoring hardware the challenge to identify correctly a unidirectional flow as peer-to-peer increases as only one direction of the conversation will

pass through the device. The goal of this test was to verify that peer-to-peer traffic is still being detected if the DUT monitors only one direction of the flow.

In this case, the PRX-10G showed highly inaccurate results and failed to detect several protocols. In total, only approximately 55% of the expected P2P traffic volume was reported. According to ipoque's analysis, Gnutella traffic is incorrectly classified as HTTP, when only one direction is monitored.

Further, the device recognized only a minority of the BitTorrent traffic presented, with regard to the connections established from the customer side. ipoque confirmed that in the case of asymmetrical traffic PRX-10G Traffic Manager applies different BitTorrent detection methods depending on which side the connection was established from. In the synthetic traffic conditions of our test, the DUT did not have access to the additional communication between clients and failed to reliably classify BitTorrent peers if many simultaneous connections were present.

Peer-to-peer Filtering in Asymmetrical Routing Scenarios

Similarly, we tested the blocking functionality of the device under asymmetric routing conditions. Technically, a DPI device will be able to fully suppress a TCP connection if a P2P protocol is recognized on the monitored direction.

As expected from the results of the detection test above, PRX-10G was able to block only approximately 50% of the P2P traffic.

Peer-to-peer Detection of VLAN-tagged Traffic

It is a common deployment practice, specifically for DSL networks, to encapsulate user traffic in service VLAN tags (as defined in IEEE 802.1Q). The test aimed to verify that even when the peer-to-peer traffic is being encapsulated using VLAN tags, the PRX-10G Traffic Manager can still detect the traffic.

We used the same traffic profile as in the previous two test cases with the sole exception of adding a VLAN tag to each frame (peer-to-peer and HTTP). The detection accuracy and performance of the PRX-10G Traffic Manager were not affected by the addition of the VLAN header to the Ethernet frames.

About Ixia

Ixia provides IP network users around the world with industry-leading test equipment that they need to ensure secure, reliable, high-performance equipment and networks.

info@ixiacom.com, <http://www.ixiacom.com>

About EANTC



The European Advanced Networking Test Center (EANTC) offers vendor-neutral network test services for manufacturers, service providers and enterprise customers. Primary business areas include interoperability, conformance and performance testing for IP, MPLS, Mobile Backhaul, VoIP, Carrier Ethernet, Triple Play, and IP applications.

EANTC AG
Einsteinufer 17, 10587 Berlin, Germany
info@eantc.com,
<http://www.eantc.com/>