Cisco SCE8000

Peer-to-Peer Monitoring and Filtering Test Report

Introduction

Cisco commissioned EANTC to independently verify the Peer-to-Peer monitoring and control capabilities of their SCE8000 Series Service Control Engine. The tests were conducted at EANTC's lab in Berlin in January 2009.

The Cisco SCE8000 (Service Control Engine) implements a range of features such as applications- and quota-based billing, traffic optimization based on applications and usage analysis. Our tests focused on one major aspect of the SCE8000 – its ability to detect and regulate peer-to-peer traffic. We specifically tailored our tests to typical Internet Service Provider (ISP) deployment scenarios, validating the accuracy of the P2P monitoring reports and the detection and filtering performance of the SCE8000.

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.

Cisco
SCE8000

☑ Detection and Regulation
>99% accurate for popular P2P (BitTorrent, eDonkey, Gnutella)

☑ Performance
Passed mixed P2P traffic up to test generator max. 12.8 Gbit/s and 15.6 Gbit/s throughput at a L3 test

Test Period: January 2009
SCE8000 Version 3.1.6 build 014s
© 2009 EANTC AG

Tested by EANTC 2009

Executive Summary

Our tests confirmed Cisco’s functionality and performance claims for the SCE8000. The Service Control Engine demonstrated an excellent detection and regulation implementation, identifying all 13 peer-to-peer applications under load. A single unit showed more than 95% accuracy in detection while passing up to 12.8 Gbit/s of maximum test generator application-layer P2P traffic. In a Layer3 test, the device showed 15.6 Gbit/s throughput.

We tested the SCE8000 in the three main operational modes — P2P detection, regulation and blocking — to find a very well engineered implementation. Out of the wide range of P2P protocols we threatened the SCE8000 with, it interpreted all protocols correctly with only one minor exception: SoulSeek traffic was correctly classified as a P2P application, but mapped to a different P2P protocol.

SCE8000 reliably blocked more than 95% of the P2P traffic. »False positives« (accidentally blocking HTTP traffic) were not seen.

Most notably, the SCE8000 was able to detect so-called »encrypted« BitTorrent, Ares, eDonkey and Filetopia file exchanges successfully.

In the “Network Operations Constraints” test group, we skipped the Asymmetrical Routing Test due to time constraints. The SCE8000’s performance and detection accuracy was not influenced in any way by the presence of VLAN tags.

Cisco SCE8000

Test Bed

The Device Under Test (DUT), the SCE8000 was operated in *transparent bridging mode* where the DUT is transparently configured into the Ethernet link, forwarding, limiting 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.

EANTC used the following test equipment to emulate ISP conditions. An Ixia XM12 with IxNetwork and IxLoad software generated IP flows, emulated HTTP and a range of Peer-to-Peer protocols. In addition two Windows XP workstations were integrated into the test bed to allow functional verification tests using real P2P clients. The PCs were connected to the Internet, whereas the IxLoad application replay worked between emulated instances between tester ports.

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.

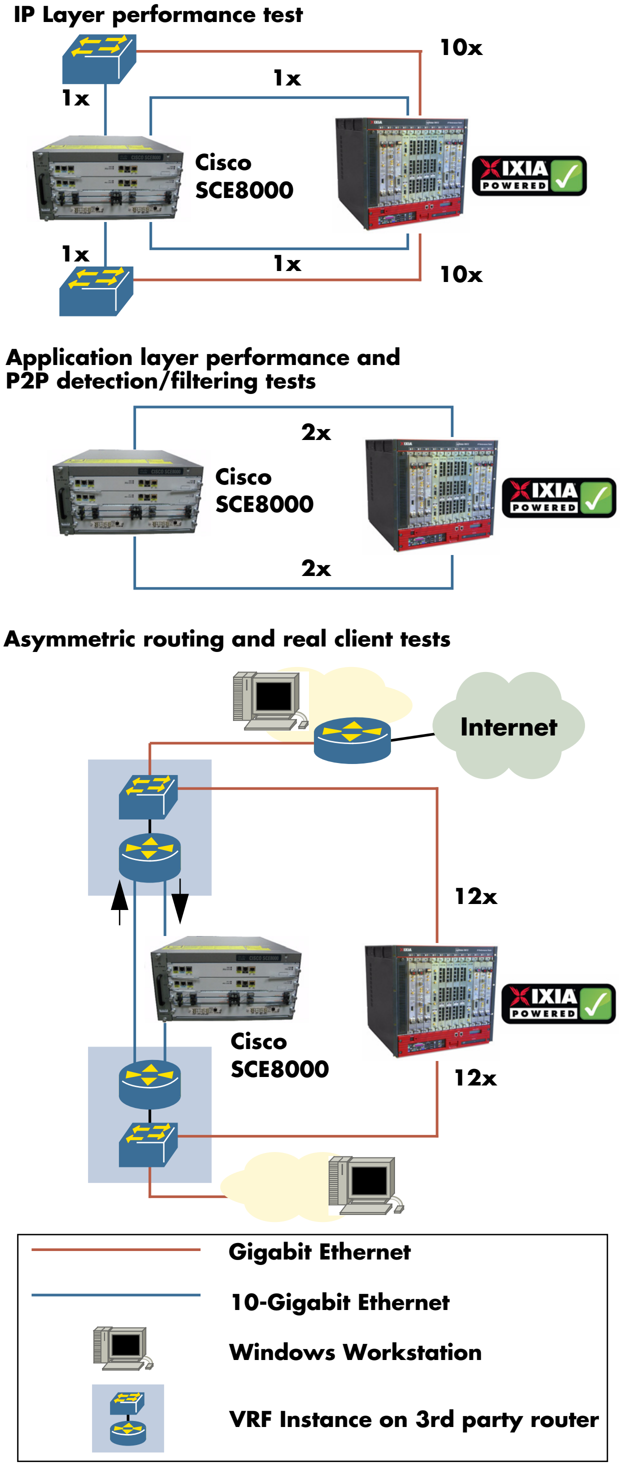
For the application performance, detection and filtering tests, as well as for the VLAN encapsulation tests, we connected the application load modules directly to the DUT using 10 Gigabit Ethernet links. We configured a third party router to set-up the asymmetrical routing scenario and to attach workstation 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 on this page show the three test bed configurations.

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.


IP Layer performance test

Application layer performance and P2P detection/filtering tests

Asymmetric routing and real client tests

Once we had measured the maximum throughput for SCE8000 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 SCE8000 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 Tests

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 analyze. 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.

Cisco claimed that the SCE8000 should reach a throughput performance of 15.6 Gbit/s in the version tested. We were able to confirm Cisco's claim, using the following ISP-MIX.

% of Sent Packets	**IP Frame Size**
40	46
20	522
40	1500
Average Size	**728.8**

Application Traffic Forwarding

With this test we aimed to determine the DPI engine analysis performance. Using the Ixia XM12 emulator, 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 20,000 concurrent TCP connections with a total bandwidth of 12.8 GBit/s (test bed limit). After the test we collected the traffic analysis statistics of the DUT and compared them with the analyzer statistics.

The SCE8000 demonstrated a total throughput of 12.8 Gbit/s for application traffic while reporting, with 97.4% accuracy, all used protocols. It is possible that the SCE8000 layer 7 forwarding detection would have matched the Layer 3 test, however, due to traffic aggregation limitations, we could not generate more than 12.8 Gbit/s.

Detection and Regulation Tests

The following group of tests investigated Cisco's SCE8000 capabilities to detect, regulate and filter peer-to-peer traffic under load. The table below 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 different clients of some of the same protocols.

Category	**Protocol**	**Appli-cation**	**Encrypted**	**Target Bandwidth, Mbit/s**
Non-P2P	HTTP	IxLoad		6000
P2P Functional	BitTorrent	µTorrent		125
	eDonkey	AMule		125
	MP2P	Manolito		125
	Soulseek	Soulseek		125
	BitTorrent	Azureus	x	125
	eDonkey	EMule	x	125
	Ares	Ares	x	125
	Filetopia	Filetopia	x	125
P2P Performance	BitTorrent	Azureus		1000
	eDonkey	EMule		1000
	Gnutella1	Limewire		1000
	Gnutella2	Shareasa		1000
	DirectConnect	DC++		1000
Total				12000

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. The total bandwidth of the L7 traffic used in the tests was approximately 12 Gbit/s with 18,000 concurrent connections.

Peer-to-Peer Detection

First we examined the capability of the SCE8000 to detect and accurately report traffic volumes of peer-to-peer protocols. The DUT was running in observation mode and hat to accurately report the traffic statistics on each of the P2P protocols we transmitted.

The SCE8000 successfully detected all configured Peer-to-Peer protocols with only one minor exception: Soulseek traffic was correctly classified as a P2P application but reported as a different P2P protocol PPlive.

Some of the encrypted protocols went partially undetected. However, for encrypted BitTorrent and eDonkey, and also Ares we could show that it was caused by the less realistic behavior of the synthetic traffic - SCE8000 was able to correctly and completely detect these protocols when exposed to real P2P clients. The detection of Ares could be improved to 100% by a slight adjustment of the detection algorithm parameters.

For all correctly identified protocols, SCE8000 reported a slightly higher traffic volume than expected. By analysis of the raw statistics data, we could identify this as a minor mistake with unit translation (when translating bytes to megabytes), which was fixed in a later releases.

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 throttle the peer-to-peer traffic to a specific bandwidth.

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 total traffic volume of the P2P traffic transferred in the test was close to the desired 50% of the reference test.

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.

We monitored that the SCE8000 was able to nearly completely block Peer-to-Peer traffic without affecting the HTTP streams.

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.

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 and filtered even though the DUT monitors only one direction of the flow. Due to time constraints we were not able to run the Asymmetrical Routing Test

Detection of VLAN-tagged Traffic

It is a common deployment practice, specifically for DSL networks, to encapsulate user traffic in service VLAN tag (as defined by the IEEE 802.1Q). The test aimed to verify that even when the peer-to-peer traffic is being encapsulated using VLAN tags, the SCE8000 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 SCE8000 were not affected by the addition of the VLAN header to the Ethernet frames.

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/