PCI-based High-speed Internet Control and Analysis Platform for Application Monitoring and Control

Sang-Kil Park[1], **Sang-Sik Yoon**[1], **and Joon-Kyung Lee**[1]
[1]Computing Network Research Department, ETRI, Daejeon, Republic of Korea

Abstract – *Smart TV, Smart-Phone and other hand-held device makes tremendous traffic on network year by year. Most ISP managers want to regulate specific application traffic which makes their network busy. They want to do traffic analyzing for identifying the traffic mixture of the network. Several different approaches co-exist in the literature, but none of them performs well for all different application traffic types present in the Internet. Therefore, one approach is to combine the advantages of different identification methods, in order to improve the completeness and accuracy of classification. We adopt application traffic classification on Traffic Control Platform. Deep Packet Processing engine can more efficient application inspection on classified application traffic for inspection.*

Keywords: Application Traffic Classification, Traffic Control, Traffic Monitoring, Multi-core, Network Processor.

1 Introduction

With its amazing growth in the uptake of mobile broadband, operators now face the challenge of handling data traffic from multiple devices and applications. To stand out from the crowd, operators will need to offer a widespread, high-quality user experience and a range of differentiated services to attract different subscriber types. With the growth in cloud computing, not only are connectivity and affordability important, latency is critical. Latency, which is the end-to-end measurement of time delay, plays a critical role for time sensitive applications. For a gaming environment, the ability to control the character to evade or attack within a short period of time would determine if the user wins or loses the game.

Smart TV, Smart-Phone and other hand-held device makes tremendous traffic on network year by year. Most ISP manager want to which application's traffic makes their network busy. They want to do traffic analyzing for identifying the traffic mixture of the network. Internet Traffic volume is larger than a few years ago. Mobile Internet traffic from mobile handset device makes network bandwidth exhausted. Basically, traffic analysis aims at identifying the traffic mixture of the network.

Several different approaches co-exist in the literature, but none of them performs well for all different application traffic types present in the Internet. Therefore, one approach is to combine the advantages of different identification methods, in order to improve the completeness and accuracy of classification. Internet Service Provider and Telecommunication Service Provider want to view detailed packet information. They want to discard some packet data from their network so they want make clean internet circuit for stable network status. Most Internet traffics are composed of web traffic and specific application traffic. If traffic throttle device in network can inspect only interest traffic which should be investigated deeply, ISP or TSP manager can detect hostile traffic or high-volume usage traffic from their network. This paper describes multi-stage traffic control platform which is composed of 2 type of functional Block.

2 Application Traffic Classification and Deep Packet Inspection

Ofcom in UK think it is helpful to think of traffic management techniques as a continuum as figure 1[1].

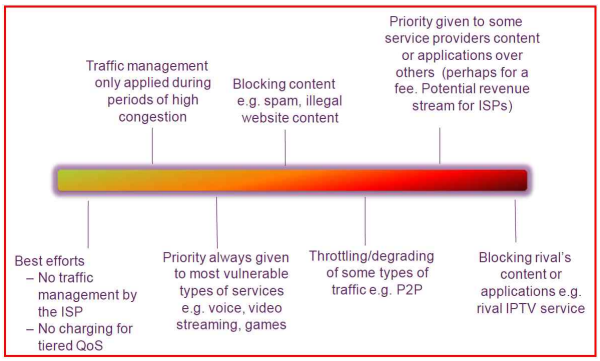


Figure 1 Traffic Management Continuum

With the evolution of mobile systems, the bandwidth capabilities of the packet switched services improved significantly. Currently, the access rates of 3G networks are comparable with the low segment of the access rates observed in fixed networks. As a consequence, applications that were present only in fixed broadband networks earlier are also appearing in mobile traffic. The change in the composition of

traffic mixture may have high impact on the operation of the mobile access as well as the mobile core networks

Most internet device like a firewall, IDS, IPS has some weakness when very high PPS(Packet Per Second) packets are incoming their device. If packet inspection system can view volume-tuned classified traffic which are filtered from network, it can support the full functionality which is implemented on it.

2.1 Signature based Classification

The signature based classification method has an up-to-date byte signature database of the protocols we can identify. The packet payloads are processed by searching predefined byte signatures in them. It should be kept in mind that the byte signature database needs to be maintained up-to-date and the byte signatures have to be tested before the usage if they are too common among other packet payloads.

2.2 Port based Classification

Port based classification differentiates traffic by destination port number. It is a common method of classification which operates by associating a well-known port number to a given traffic type[2].

2.3 Application Traffic Classification

Accurate traffic classification is the heart of the traffic control system, with the result becoming the basis of the security policy[3][4][5]. Traditional network appliance identify/classify traffic by port and protocol, which, at one point, was a satisfactory mechanism for clarifying the network. Today, application can easily bypass a port-based network system; hopping ports, using SSL and SSH, sneaking across port 80, or using non-standards ports.

2.4 Common Network device vs. DPI device

In Figure 2, Host/Server can see all packet header and payload data which is received from network.

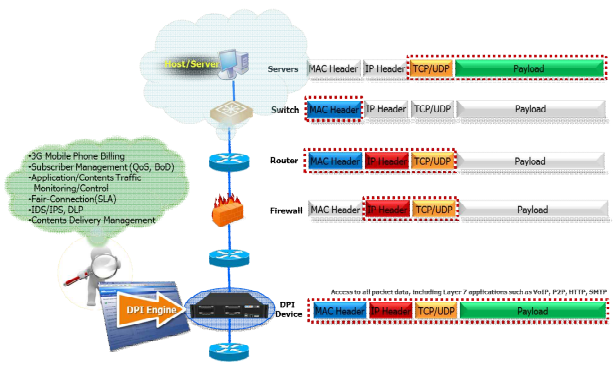


Figure 1 Network Device Visibility Layer and DPI

Traditional network devices like a switch, firewall, router can see L2~L4 Packet Layer(MAC, IP Address, Port, Protocol, Header), but DPI(Deep Packet Inspection) technology enable full visibility of packet payload ,what is more, including application payload[6][7][8].

3 Composition of Multi-stage Traffic Control Platform

HITCAP(High-speed Internet Traffic Control and Analysis Platform)is mainly composed of two-stage traffic processing like figure 3.

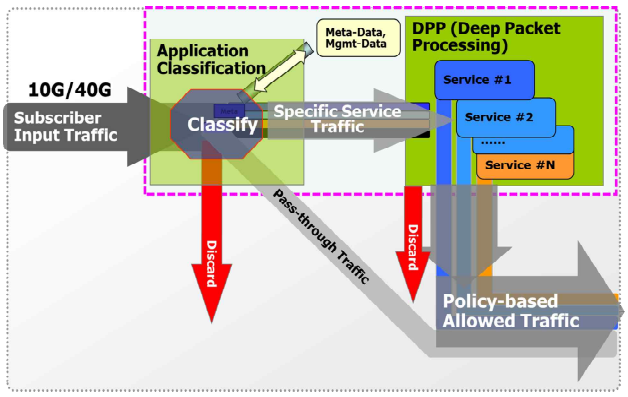


Figure 2 Concept of Two-stage Traffic Control Platform

First step is Intelligent DPI function for high-speed traffic classification and filtering. If Intelligent DPI engine select specific services packet from input traffic, it send specific services traffic to second Smart DPP engine for Deep Packet Processing. If Intelligent DPI engine decide specific service traffic to drop from input traffic, it discard the packet from the network. In other case, Intelligent DPI engine forward input traffic to the network lines. If input packet is classified by applications(specific services), as an interested traffic then Intelligent DPI engine send specific service packet to second Smart DPP(Deep Packet Processing) engine.

As usual upper model could be one hardware board. But we implement 2-type of PCI-NIC type card for flexibility, functionality, economical reasons. PCI NIC can be installed COTS server without additional cost. First NIC(HITCAP-HX) mainly do the packet classification and second NIC(HITCAP-TG) do the deep packet processing.

3.1 HITCAP-HX for application classification

Figure 4 shows an prototype of HX330[10] based high-speed traffic classification card. It uses the systolic type NPU, HX330 of Xelerated[9] as network processor(Xelerated is merged by Marvell Networks). Below are the main functionality of HITCAP-HX.

It can support state-machine based high-performacne packet processing(parsing, filtering, dropping, forwarding) on 4*10Gbps high-speed traffic interfaces. It's high-speed packet classificationi engine classify a service traffic by 7-tuple datas(Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol, Input Interface, Signature) on 40Gbps traffic.

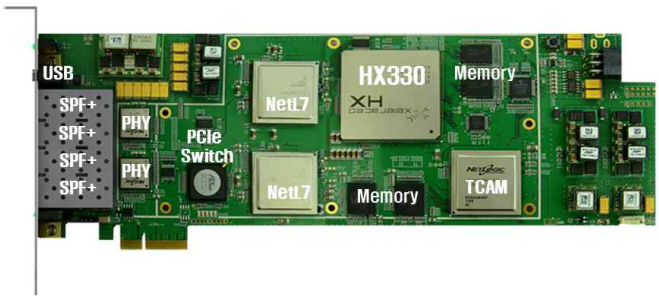


Figure 3 HX330 based High-speed traffic classification Card

HITCAP-HX card has four 10GbE SFP+ type interface and 1 debug console port. HX330 receives input packet data form PHY chipset and if some packet needs do the pattern matching, it sends packet data to Layer 7 Inspection chipset(NetL7) and return the matching result.

We adopt some types of action like drop, transmit, forward, modify, redirect, log, replicate.

3.2 HITCAP-TG for Deep Packet Processing

Figure 5 shows Tile-GX36 based deep packet processing card(HITCAP-TG). User can program c-like syntax and API.

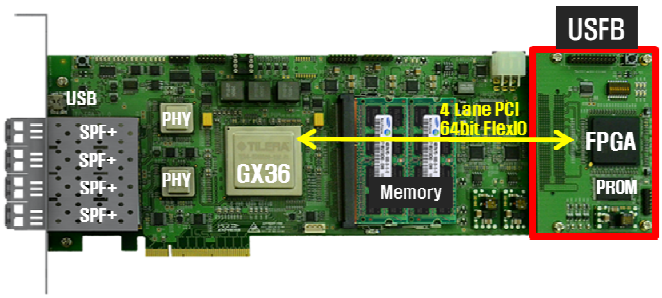


Figure 4 Tilera-GX 36 based Deep Packet Processing Card

HITCAP-TG card has four 10GbE SFP+ type interface and 1 miniUSB port for debug. Tile-GX manage flow and policy data on 8Gb DDR3 memory. Tile-GX has 36core for high-speed processing, we programmed the snort for IDS on tile-GX using 26cores. We adopt some types of action like transmit, drop, forward, modify, redirect, log, replicate.

Tile-GX chipset has only MICA engine for compression/decompression and chiper. So we design and implement USFB(User Specific Functionial daughter board) for some critical high-speed processing like a crypto/codec/PCRE engine. We connect 4lane(x4) PCIe bus and 64bit FlexIO signals between Tile-GX36 and USFB.

3.3 Platform Management Sever (PMS)

Traffic Control Platform is managed by the Platform Management Sever(PMS). All received policy and configuration data are collected by PMS. PMS receive policy from policy server and PMS enforce policy to the adequate Hardware.

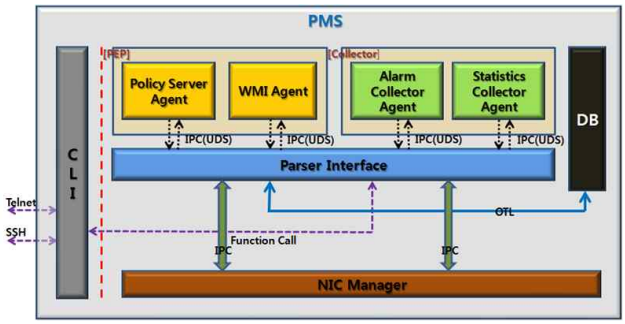


Figure 5 PMS(Platform Management Server)

There are some cases of policy enforcement. If the policy handles only L2~L4 headers of packet, this policy mainly enforced to HITCAP-HX card. But if the policy handles from L2 to L7 siganture fields, L2~L4 header related subset rule is enforced to HITCAP-HX card with send 2nd board forward action command. Hole policy is installed into HITCAP-TG .

3.4 Policy Server(PS)

Policy server manages policy rules between applications and policy enforcement points like HITCAP-hardware.

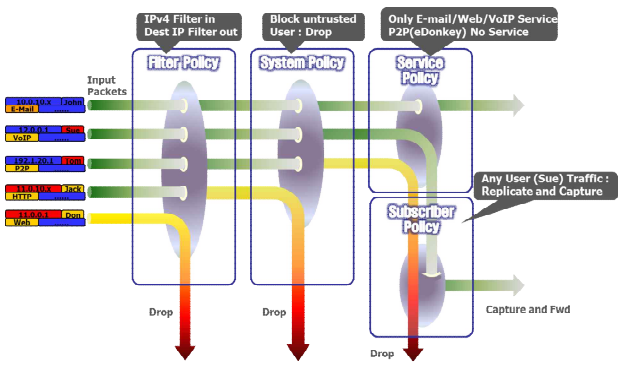


Figure 6 Subscriber base Policy structure of Policy Server

Manager can easily add and re-configure policies to manage and control Quality of Service(QoS), charging,

optimization and admission control. A wide variety of interfaces make it easy for manager to integrate the policy server into any type of network service.

4 Performance testing of HITCAP

We install our 2-type PCI-e NIC into HITCAP proprietary chassis server and connect HITCAP platform and AX4000 using 4 port of SPF+. We make 4 x 10Gbps traffic into HITCAP Platform.

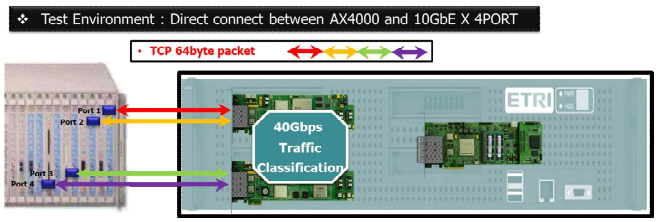
In this test we installed two HITCAP-HX cards and one HITCAP-TG card on HITCAP proprietary chassis server. Mainly all 10Gbps circuit is connected to HITCAP-HX card from AX4000. HITCAP-HX handles each packet and only some services traffics classified by HITCAP-HX are sent to HITCAP-TG board for Deep Packet Processing.

4.1 High-speed Traffic Classification

We make 64byte TCP packet from packet generator (AX4000) into HITCAP for high-speed traffic classification.

4.1.1 40Gbps Packet Forwarding Test

First we generate 40Gbps TCP Traffic from AX4000 into HITCAP. HITCAP receives 4 x 10Gbps traffic. HITCAP-HX card classify each packet by look-up TCAM memory, if action of input packet is forwarding input packet is forwarded but input packet is not matched the input packet is discarded like figure 10. In this test HITCAP-HX handle 4 x 14,880,952pps on real time without packet loss by in-line mode.



Packet Processing	Packet Size	Traffic volume	IP Address Information
FWD and DPP	64 Byte	40 Gbps	Random packet Generation
Packet Forwarding by Identification and Classification	TCP 64 Byte	❖40Gbps(4port x 10Gbps) ✓4 x 14,880,952pps	-Port 1 : TCP Stream . Src IP : 10.0.0.1 ~ 10.0.0.65 . Dst IP : 20.0.0.1 ~ 20.0.0.65 -Port 2 : TCP Stream . Src IP : 30.0.0.1 ~ 30.0.0.65 . Dst IP : 40.0.0.1 ~ 40.0.0.65 -Port 3 : TCP Stream . Src IP : 50.0.0.1 ~ 50.0.0.65 . Dst IP : 60.0.0.1 ~ 60.0.0.65 -Port 4 : TCP Stream . Src IP : 70.0.0.1 ~ 70.0.0.65 . Dst IP : 80.0.0.1 ~ 80.0.0.65

Figure 7 Test Scenario of High-speed Traffic Classification

Figure 8 shows the result of packet forwarding test(figure 7). Port 2 and Port 3 is connected rx and tx port each other. All sent packet from port 2 is received in port 3 and all sent packet from port 3 is received in port 2. Port 4 and Port 5 is connected rx and tx port each other. All sent packet from port 4 is received in port 5 and all sent packet from port 5 is received in port 4.

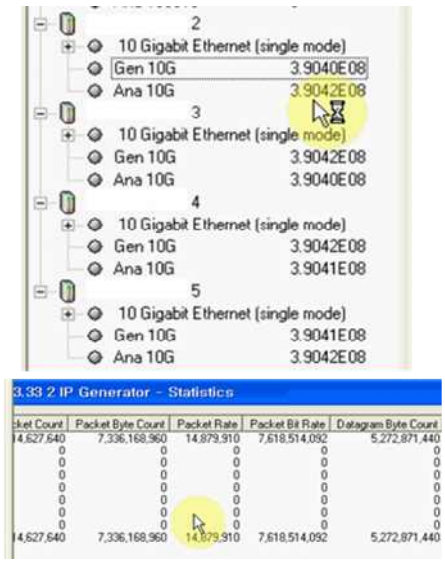
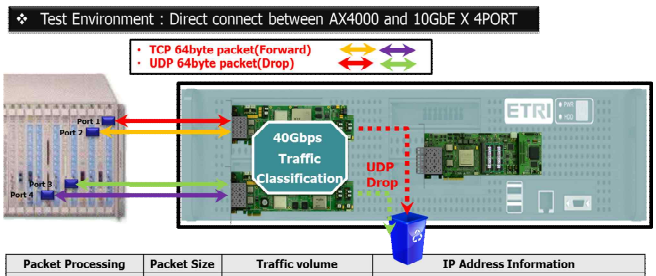


Figure 8 Test Result of High-speed Traffic Classification

Each interface on AX4000 send packet to HITCAP directly at 14,879,910 Packet Rate(PPS). This test result shows that HITCAP platform guarantee good through result of packet processing evenly minimum size packet without loss.

4.1.2 40Gbps Packet Forwarding and Filtering Test

We generate 20Gbps TCP traffic and 20Gbps UDP traffic from AX4000 into HITCAP. HITCAP receives 4 x 10Gbps traffic. HITCAP-HX card classify each packet by look-up TCAM memory. If input packet is TCP, HITCAP forward this traffic to network. But if input packet is UDP traffic HITCAP discard this traffic from network.



Packet Processing	Packet Size	Traffic volume	IP Address Information
FWD and DPP	64 Byte	40 Gbps	Random packet Generation
Forwarding & Drop by Identification and Classification • Forwarding ✓ TCP(20Gbps) • Drop : ✓ UDP(20Gbps)	TCP/UDP 64 Byte	❖40Gbps(4port x 10Gbps) ✓ 4 x 14,880,952pps	-Port 1 : TCP Stream . Src IP : 10.0.0.1 ~ 10.0.0.65 . Dst IP : 20.0.0.1 ~ 20.0.0.65 -Port 2 : TCP Stream . Src IP : 30.0.0.1 ~ 30.0.0.65 . Dst IP : 40.0.0.1 ~ 40.0.0.65 -Port 3 : TCP Stream . Src IP : 50.0.0.1 ~ 50.0.0.65 . Dst IP : 60.0.0.1 ~ 60.0.0.65 -Port 4 : TCP Stream . Src IP : 70.0.0.1 ~ 70.0.0.65 . Dst IP : 80.0.0.1 ~ 80.0.0.65

Figure 9 Test Scenario of Packet Forwarding and Filtering

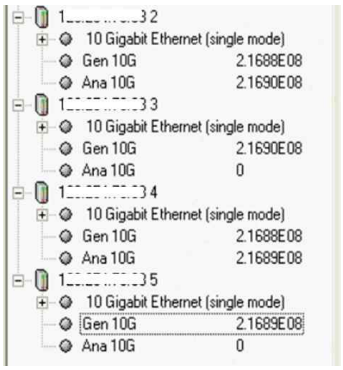
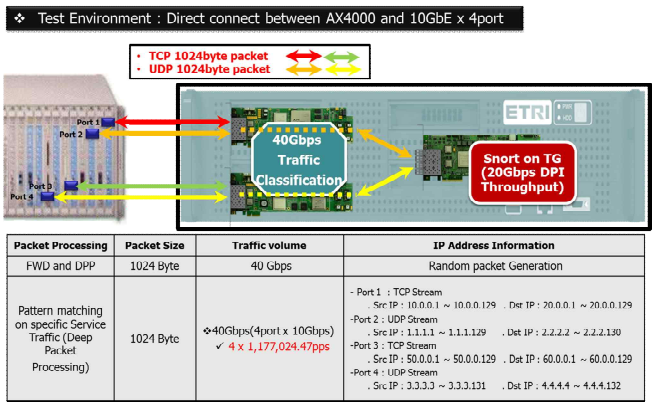


Figure 10Test Resultof Packet Forwarding and Filtering

Figure 10 shows the result of packet forwarding and filtering test(figure 9). Port 2 and Port 3 is connected rx and tx port each other. All sent packet from port 2 is blocked in port 3 and all sent packet from port 3 is received in port 2. Port 4 and Port 5 is connected rx and tx port each other. All sent packet from port 4 is blocked in port 5 and all sent packet from port 5 is received in port 4.

4.2 Deep Packet Inspection

In case of test for pattern matching on payload area, we make 1024 size packet into HITCAP chassis server. If TCP packet is received the HITCAP-HX do the packet forwarding for adequate port. If UDP packet is arrived, HITCAP-HX send it to HITCAP-TG card for Deep Packet Processing. Snort program which is implemented 25core of Tile-GX chip(A1) on HITCAP-TG show all area of payload data in packet. In our test Snort can handle 20Gbps traffic successfully.



Packet Processing	Packet Size	Traffic volume	IP Address Information
FWD and DPP	1024 Byte	40 Gbps	Random packet Generation
Pattern matching on specific Service Traffic (Deep Packet Processing)	1024 Byte	❖40Gbps(4port x 10Gbps) ✓ 4 x 1,177,024.47pps	- Port 1 : TCP Stream . Src IP : 10.0.0.1 ~ 10.0.0.129 . Dst IP : 20.0.0.1 ~ 20.0.0.129 -Port 2 : UDP Stream . Src IP : 1.1.1.1 ~ 1.1.1.129 . Dst IP : 2.2.2.2 ~ 2.2.2.130 -Port 3 : TCP Stream . Src IP : 50.0.0.1 ~ 50.0.0.129 . Dst IP : 60.0.0.1 ~ 60.0.0.129 -Port 4 : UDP Stream . Src IP : 3.3.3.3 ~ 3.3.3.131 . Dst IP : 4.4.4.4 ~ 4.4.4.132

Figure 11 Test Scenario of High-speed Deep Packet Processing

Figure 11 shows the test traffic and the configuration of HITCAP Card. All input traffic classified on HITCAP-HX, if the input traffic is TCP this traffic is sent to network and if input traffic is UDP traffic then HITCAP-HX send this traffic to HITCAP-TG(2nd Board) for Deep Packet Processing.

In this test we use tilera GX pre-release chipset(A1) nowadays stable A2 chipset is supported from Tilera corporation. In view of HITCAP-TG all input traffic from AX4000 is received on xgbe1 and xgbe3 like figure 12.

We run Snort program with 25core of tiles from tile-GX chipset. It can handle almost 2*10Gbps traffic on real time.

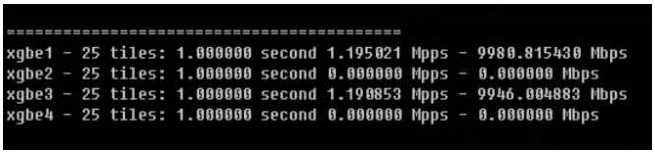


Figure 12 Test Result of High-speed Deep Packet Processing

5 Conclusions

Mobile devices like a smart-phone, are more and more wide spread all of network. So the tele-communication provider wants to see the payload of each app and each application. User wants to know current the billing information of him. It can be done by rapid policy enforcement. This is we will design and implement 4-port 10Gbps NIC for Network redundancy. It is needed to improve the stability and long-term safety for applying in commercial area.

Acknowledgements

This work has been funded by KCC(Korea Communication committee)

6 References

[1] Traffic Management and ‘net neutrality’ A Discussion Document, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutra lity.pdf ‚June. 2010.

[2] Karagiannis, T., Broido, A., Brownlee, N., Claffy, K.C., Faloutsos, M.: Is p2p dying or just hiding In: IEEE Globecom (2004)

[3] Paxson, V.: Bro: A system for detecting network intruders in real-time. In: Computer Networks, pp. 23~24 (1999)

[4] L7-filter, Application Layer Packet Classifier for Linux, http://l7-filter.sourceforge.net

[5] Cisco systems. Blocking Peer-to-Peer File Sharing Programs with the PIX Firewall, http://www.cisco.com/application/pdf/paws/42700/block_p2p_pix.pdf

[6] ″Deep Packet Inspection”, Wikipedia

[7] ″Deep Security : DISA Beefs up security with Deep packet Inspection of IP Transmissions”, dpacket.org. 2008

[8] ″Deep Packet Inspection : The end of the Internet As We now it”, www.freepress.net, 2009

[9] Xelerated homepage, http://www.xelerated.com

[10] HX Family of Network Processors, 100Gbps NPU with Integrated Traffic Manager, Switch, Programmable Pipeline and Ethernet MACs, http://www.xelerated.com/ Uploads/Files/68.pdf, 2011.