International Journal on Emerging Technologies (Special Issue on NCRIET-2015) **6**(2): 262-265(2015)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Deep Packet Inspection Technology

Nagashetty B Kolar

Department of Computer Science and Engineering REC Bhalki, Karnataka, INDIA

(Corresponding author: Nagashetty B Kolar)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: **DPI expanded is "deep packet inspection" however what is often asked for is not DPI, but the capabilities DPI enables such as traffic shaping, admission, content access restrictions, information extraction about subscribers from their packet traffic, and soon and at a higher level the DPI applications which form the basis of useful services to a subscriber or capabilities to a service provider. • DPI can be broadly defined as the ability to collect information and optionally take action based on the information in or that can be inferred from the content of the communication. The applications running over IP increasingly, 1) are Dynamic and Distributed. They change, are stateful and operate from multiple sources, 2) involve Protocols, require the ability to understand not just a packet but the communication and syntax across multiple packets and ports, and 3) may need Intervention, such as blocked if unauthorized, or shaped to provide reasonable throughput overall.**

I. INTRODUCTION

Deep Packet Inspection (DPI, also called complete packet inspection and Information eXtraction or IX) is a form of computer network packet filtering that examines thedata part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, or, for the purpose of collecting statistical information. There are multiple headers for IP packets; network equipment only needs to use the first of these (the IP header) for normal operation, but use of the second header (TCP, UDP etc.) is normally considered to be shallow packet inspection (usually called Stateful Packet Inspection) despite this definition.

II. DEEP PACKET INSPECTION (DPI) - REQUIREMENTS AND ARCHITECTURES

DPI is a technique with many different use cases, delivering information about packet flows and content as well as allowing network operators and service providers to ensure quality of service at an application level. As more and more DPI use cases are being implemented in the market, a common set of requirements has developed. These requirements have driven a set of architectures that deliver the level of performance, throughput and statistical data collection required to fulfill the respective task at hand. There are multiple building blocks, consisting of both software and hardware, which enable developers to create solutions that not only support their specific approach to solving the problem of packet inspection, but that also enable developers to take advantage of a pre-validated platform, thus de-risking large projects.

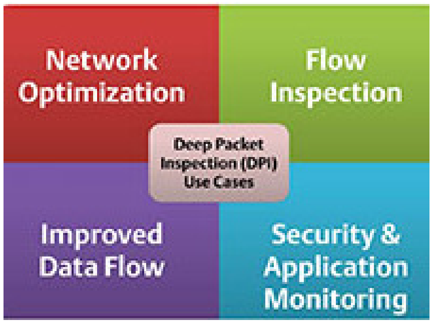
Network Optimization
Flow Inspection
Deep Packet Inspection (DPI) Use Cases
Improved Data Flow
Security & Application Monitoring

Fig. 1.

This white paper will analyze use cases, define a set of common requirements for DPI applications and outline several architectures and building blocks that simplify the creation of scalable, reliable DPI appliances.

III. SIMPLIFIED VIRTUALIZATION

DPI (Deep Packet Inspection) allows an Operator to analyze the contents inside the packet header and to classify the type of data going inside any packet. The DPI engine reports the usage as part of a flow and classifies each into a group of available application classes.

PCRF can then be used to evaluate rules that inform the PCEF in the DPI to enforce the policies and charging as guided by the PCEF.

Following use cases can be realized by putting a DPI engine in the policy framework.

Peering Control:

Control can be exercised over Peer to Peer traffic which is causing a major portion of Internet traffic today. PCRF may block all P2P traffic or allow it based on Operator's policy. It also allows the operator to limit P2P traffic during specific times of day and also allows to upsell P2P traffic only to user specifically paying for it as part of their subscriptions.

Layer 7 shaping and firewalling: Any other protocol or application category can be gated (blocked), throttled or passed with full bandwidth. This allows the operator to exercise control over the consumed bandwidth in terms of more granular application level controls.

QoS Assurance: DPI also enables an operator to assure QoS for some types of traffic e.g. Skype calls or other VoIP /Video telephony. Like all other such features it gives the service provider an option to monetize and offer as a value added service on top of flat Internet access.

OTT Monetization: OTT (Over the Top) monetization is a broad use case covering many aspects of the service but they all start with a DPI engine in place. Once the DPI is reporting each flow separately to the PCRF, the PCRF can be used to enforce operator's policies. Operators can think of innovative ways then to monetize their bandwidth and capacity in different ways.

Security Threats: Looking deeply inside packets, the PCRF is also in a position to proactively alert the customers of any rogue application consuming more data than what is considered normal. This will help minimize security threats in the network.

Putting a DPI engine allow an operator to exercise more granular control over the flow of data and PCRF plays a vital role in analyzing that information and processing it to realize the business use cases by the operator in terms of policy control and charging.

IV. TESTING TDF/DPI APPLICATIONS WITHIN AN EXISTING PDN TEST ENVIRONMENT

In order to test the TDF within an existing PDN environment, the gateway node can obtain an IP address via the external DHCP server during the packet bearer establishment procedures, such as PDP Context activation or default bearer establishment. The GGSN, or other PDN gateway, acts as a DHCP client towards the DHCP server or uses a DHCP relay agent to request the information. The DHCP Server offers a set of IP addresses from a pool maintained by the SPR. Within the PDN, a DHCP client or relay agent function allows routing of DHCP requests and replies between the nodes and the DHCP server. The DHCP agent relays the requests received from the DHCP client to the DHCP server, and the replies received from the server to the corresponding client. When the IP address has been negotiated, the PCRF emulator sends the IP address as part of the policy rules to the TDF via the Sd interface. A TDF-Session-Request (TSR) command is sent by the PCRF to the TDF in order to establish the TDF session and to provision the ADC rules. The TDF acknowledges the TSR with a TDF-Session-Answer (TSA) message.

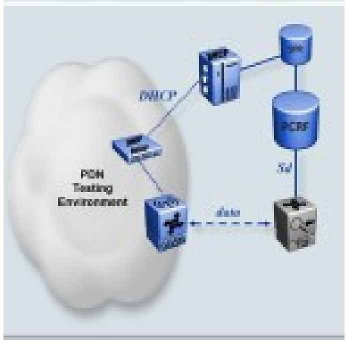

Fig. 2.

A media bearer session is established between the PDN gateway node (GGSN in this example, but could be any media gateway type node). Data then flows between the PDN and the TDF. At this point, DPI applications within the TDF can be evaluated.

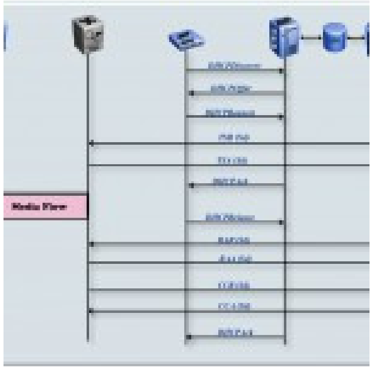

Fig. 3.

When the media session is complete, the DHCP client releases the IP address, and the TDF session closes via the Sd interface. The Re-Auth-Request (RAR) command is sent by the PCRF to request the TDF session termination, and the Re-Auth-Answer (RAA) is sent by the TDF to the PCRF in response.

V. EFFECTIVELY DELIVER ADVANCED SERVICES TO YOUR SUBSCRIBERS

To support use cases that your network requires, you need a deeper understanding of your traffic and powerful traffic recognition capabilities achieved with a DPI Deep Packet Inspection appliance to answer top of mind questions:

Fig. 4.

- What applications are on my network?
- Which devices are subscribers using on my network?
- What are the subscriber behaviors on my network? (usage patterns, favorite applications, roaming)
- Are my network resources being used effectively and efficiently?

You need a DPI Deep Packet Inspection product with leading traffic classification to provide the highest accuracy, largest breadth of completeness, and most comprehensive measurements. Everyone invests the most in traffic classification and in turn has the industry's best measurements among deep packet inspection vendors. Service providers worldwide choose DPI deep packet inspection solution to power business intelligence, revenue generation, traffic optimization and network security use cases to improve QoE for their most important customer, subscribers.

VI. TRAFFIC CLASSIFICATION FOR ACTIONABLE DATA

Traffic classification is powered by DPI technology, acting as the foundation of all our network policy control and business intelligence solutions. Traffic Classification examines Internet traffic and reads meta-information to determine the type of network traffic, the device with which it is associated, the content delivery network (CDN) from which it came, and other important characteristics which enable operators to implement and execute different network policy control use cases.

VII. UNIFIED NETWORK POLICY CONTROL USING SANDVINE

Policy Engine The Policy Engine is the world’s most versatile and powerful network policy control platform, and is the foundation of all solutions. There are couple of organizations provide silutions like sandvine. Which can provide policy engine.

Policy Engine can be thought of as a black box:

into which information about measured conditions and provisioned subscriber entitlements flow from our traffic classification technology, and

out of which charging updates, management actions, and business intelligence emerge from our powerful freeform policy languages.

The Policy Engine spans both the data plane and control plane, embedded within PCEF/TDF and PCRF elements, and interacts with the B/OSS plane and remote enforcement points using standard interfaces. we predict that policy engine as a field will continue to rapidly evolve in software shift away from the model based on a more traditional physical network. also moving the dpi from physical world to virtual world is the hot topic in technology.

VIII. FUTURE

The Policy Engine spans both the data plane and control plane, embedded within PCEF/TDF and PCRF elements, and interacts with the B/OSS plane and remote enforcement points using standard interfaces. we predict that policy engine as a field will continue to rapidly evolve in software shift away from the model based on a more traditional physical network. also moving the dpi from physical world to virtual world is the hot topic in technology.

A new approach to data inspection is needed that incorporates thorough analysis to address the undetected and emerging threats, Deep Content Inspection (DCI) is an advanced form of network filtering that functions as a fully transparent device at a comprehensive level. DCI examines the entire object and detects any malicious or non-compliant intent, instead of solely checking the body or header of data packets circling through a network. DCI reconstructs, decompresses and/or decodes network traffic packets into their constituting application level objects, often referred to as the MIME objects.

IX. CONCLUSION

People and organizations concerned about privacy or network neutrality find inspection of the content layers of the Internet protocol to be offensive, saying for example, "the 'Net was built on open access and non-discrimination of packets!" Critics of network neutrality rules, meanwhile, call them "a solution in search of a problem" and say that net neutrality rules would reduce incentives to upgrade networks and launch next-generation network services. Deep packet inspection is considered by many to both undermine the infrastructure of the internet and is considered illegal under United States constitution. of the virtual clusters.

REFERENCE

[1] Wiki :
http://en.wikipedia.org/wiki/Deep_packet_inspection
[2] “Sandvine policy engine”
https://www.sandvine.com/
[3] White papers
http://www.intel.in/content/dam/www/public/us/en/documents/white-papers/communications-qosmos-paper.pdf