Draft baseline text of Y.dpireq "Requirements of DPI in packet-based networks and NGN environment"

Abstract

This is the output of draft Recommendation Y.dpireq (Requirements of DPI in packet-based networks and NGNenvironment) from the January 2009 meeting of SG13. It includes the initial baseline text for the draft Recommendation.

1. Scope

The scope of this draft Recommendation is targeted primarily at the service requirements, capability requirements and functional requirements of the Deep Packet Inspection (DPI), including: (1) to provide real-time service awareness and control by scanning partial or the whole packet for service awareness and control based on static/dynamic rules in packet-based networks and NGN environment; (2) to identify and define, if necessary, standard interfaces to interconnect with other components, taking into account the migration from non-NGN environment into NGN environment.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.
[1] ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, Information technology. Open Systems Interconnection. Basic reference model: The basic model.

TBD

3. Definition

This Recommendation defines the following terms:

3.1 Deep Packet Inspection (DPI): an method of packet filtering that functions at Layer 2-7 (Open Systems Interconnection) reference model[1]. The use of DPI makes it possible to find, identify, classify, or control packets with specific data or code payloads that conventional packet filtering, which examines only packet headers, cannot detect.

3.2 DPI node: a network node device with DPI function. Note: This network node device could be a router, switch, bridge, border gateway, or any other kind of access devices, telecom transmission device or system, etc.

3.3 DPI engine: a DPI processing element including a scan function, analyzer, rule action, rules table.

3.4 A rule entry: one of a set of rules (or N-octet string) which are statically predefined or dynamically generated and used to compare the particular overhead or contents octets of the real-time packet flows with a set of the rules (strings) to determine if the string matching is successful or not.

3.5 A DPI analyzer: a functional implementation to perform comparison functions between the particular overhead or contents octets of the real-time packet flows and a set of the rules (strings) to determine what the results are.

3.6 A rule action: an action after analyzing according to the related rule actions, which include at least the following:

- •Traffic classification, measurement, and reporting and management
- •Resource management, admission control and filtering
- •Policy-based prioritization, blocking, shaping and scheduling
- •Dynamic rule building and modification

3.7 Rules table: a database including the multiple rule entries. These rules are defined and classified at the different levels (layer2-layer7), and the different functions at the same layer to meet the carrier class interworking requirements.

3.8 Mediation Unit: a mediation functional unit performing the bi-directional DPI. This unit is connected to each Rules table, rule action and analyzer to deal with the end-to-end association between outgoing stream and the relevant incoming stream.

4. Abbreviations

This Recommendation uses the following abbreviations and acronyms:

TBD

5. Conventions

TBD

6. Service requirements

(TBD)

7. Capability requirements

7.1 Scanning Packet Payloads at all layers

In order to monitor and control traffic, DPI is required to support the mechanism to scan packets from the first bit to the last when required. For maximum applicability, payload-scanning capabilities include applications and transactions that traverse multiple packets.

7.2 Application Classification, Measurement, and Reporting

DPI is required to support the mechanism to classify applications, measure performance, and generate reports. This provides network managers with the visibility essential for strategic traffic planning and policy based charging, etc.

7.3 Set Policies for Controlling Traffic

Based on packet payload scans, application classification, and a set of policies for managing traffic, DPI is capable to support mechanisms to prioritize and control traffic. This function provides one of the fundamental controls that used for offering tiered services and for controlling applications.

7.4 Session Identification

DPI is capable to analyze session behaviour, track session state change if necessary, monitor individual subscribers' quality of experience, end-to-end KPIs (Key Performance Indicators) in real-time on a complete session-by-session basis from Layer 2 to Layer 7.

7.5 Modification of the Packet Envelope

It is optional that DPI be capable of modifying packet envelopes in order to enable new services and prevent attacks. It is optional that this capability be configurable, programmable, and sufficiently granular to allow maximum flexibility in packet processing.

7.6 Modification of Packet Payload Content

DPI is required to support the mechanisms to modify payload content. Based on dynamic packet and session monitoring, DPI packet content modification can carry out functions such as removing viruses

7.7 Generating Packets

DPI is required to support the mechanisms to generate packets with all the appropriate content and envelope information to be sent to the network manager.

8. Functional requirements

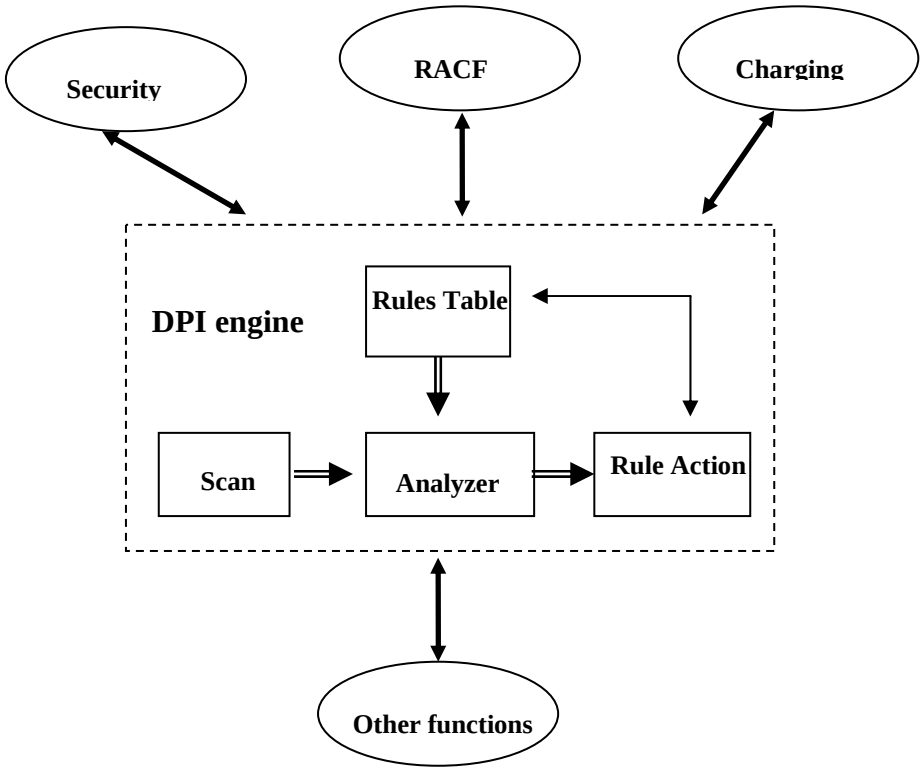

Figure 1. DPI within the packet-based networks and NGN environment

Figure 1 illustrates the relationship between DPI and other components within the packet-based networks and NGN environment.

TBD

Bibliography

[ITU-T Y.2011] ITU-T Recommendation Y.2011 (2004), General principles and

general reference model for Next Generation Networks.

[ITU-T Y.2001] ITU-T Recommendation Y.2001 (2004), General overview of NGN.
[ITU-T Y.2021] ITU-T Recommendation Y.2021 (2006), IMS for Next Generation Networks.
[ITU-T Y.2091] ITU-T Recommendation Y.2091 (2007), Terms and definitions for Next Generation Networks.
ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, Information technology . Open Systems Interconnection . Basic reference model: The basic model.
ITU-T X.211 (1995) | ISO/IEC 10022:1996, Information technology . Open Systems Interconnection . Physical service definition.
IETF RFC 791 (1981), Internet Protocol . DARPA Internet Program . Protocol Specification.
IETF RFC 2460 (1998), Internet Protocol, Version 6 (IPv6). Specification.

Appendix I

Architectural Framework of DPI

(This Appendix does not form an integral part of this Recommendation.)

This Appendix describes the framework of DPI within packet-based networks and NGN environment.

The IPv4/v6/NGN access and metro networks are primarily built with the packet switching and routing technologies, which are opaque for the details of the upper layers of the protocol stack and devoid of service control capabilities. While these technologies can determine source and destination IP addresses and TCP ports of each packet, they could hardly determine the behaviour of the application, the user, the content, or other aspects of the upper layer protocols and applications. As a result, a NGN and Ipv4/v6 service provider hires an opaque or black broadband pipe at a cheaper price, it is likely that subscribers will change to rent upper value-added services with content awareness from other Internet content providers. This is an insufferable problem for network service providers that the more investments in their broadband infrastructure, the less return from the service income.

The better method to address this issue is to change an opaque and black broadband pipe into a transparent broadband pipe, which provides service providers visibility using the networks, traffics and applications, visibility implementing service management and control. This offers network operators complete visibility of network applications, flexible traffic control through the real-time comparison and string matching between the particular overhead or contents octets of the packet flows and a set of the octets predefined rules.

The string matching is one of the most important functions in applications such as IP address lookup in routers. In a DPI node, it allows for the node to scan into both the headers and the actual content flowing. Figure 1 illustrates the DPI Dataflow Window for matching the rule (N-octet string). If a string is identified as a rule member of DPI function, the system can declare the string as a matching signature. Such strings are then sent to a DPI analyzer to determine if the string matching is successful or not. The DPI analyzer uses a particular string-matching algorithm and gives a query result per clock cycle. The tens of thousands of strings can be scanned at gigabit per second rates.

The basic DPI function and architecture are presented in Figure 2. As the packet passes through the pipeline, the extracted ingress packets from incoming link enter the input queue and are scanned in different window lengths for signatures of different lengths by DPI engine, which is a real-time processing functionality and ability of traffic management based on the particular overhead or content of packet. DPI operates with content awareness on information contained at all layers of the protocol stacks, including the application layer to satisfy new emerging requirements. The DPI engine illustrated in Figure 2 contains a scan function, analyzer, rule action, and rules table. A DPI analyzer performs comparison function between the particular overhead or contents octets of the real-time packet flows and a set of the predefined rules (strings) to determine what the result is.

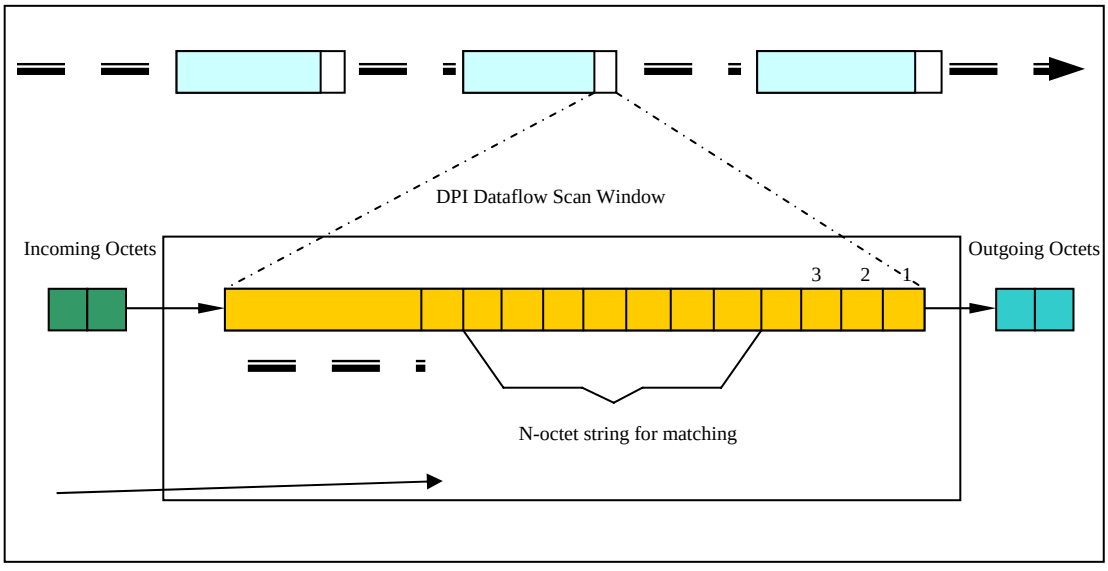

Figure 1 – DPI Dataflow Window

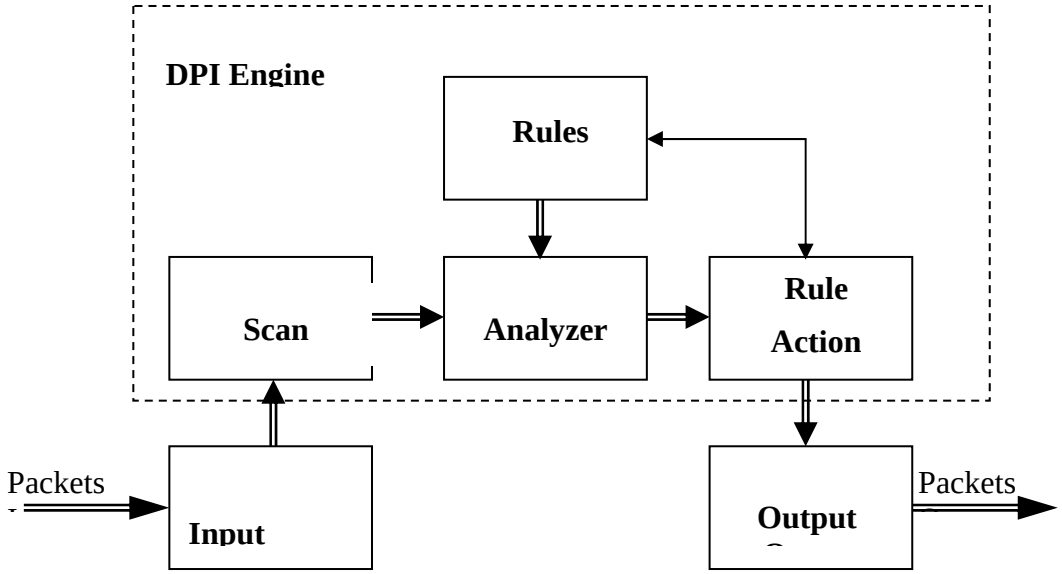

Figure 2 – The basic DPI function and architecture

A rule action is the most critical and reflects the enforcement of the related rule requirements, this action includes at least the following (for release 1):

•Traffic classification, measurement, and reporting and management

•Resource management, admission control and filtering

•Policy-based prioritization, blocking, shaping and scheduling

•Dynamic rule building and modification

The important characteristics of DPI are a direct traffic management in the real-time. As an example, if a rule action detects a match occurred, the related content can be blocked and an alert message is generated, or the related content can be modified and a schedule or action is produced.

Rules table in the DPI engine presents a table database including the multiple rule members. These rules are defined and classified as the different levels (including L2, L3, L4, L5, L6, L7 and content), and the different functions at the same layer to meet the carrier class interworking requirements.

Data leaves the content pipeline after the DPI engine processing, flows to the output queue, and then packets are re-injected into the network.

Figure 3 illustrates the bi-directional DPI function and architecture. The Mediation Unit is targeted at a mediation function unit of performing the bi-directional DPI. This unit interfaces to the bi-directional rules table, rule action and analyzer to align and deal with the end-to-end pertinences between outgoing stream and the relevant incoming stream.

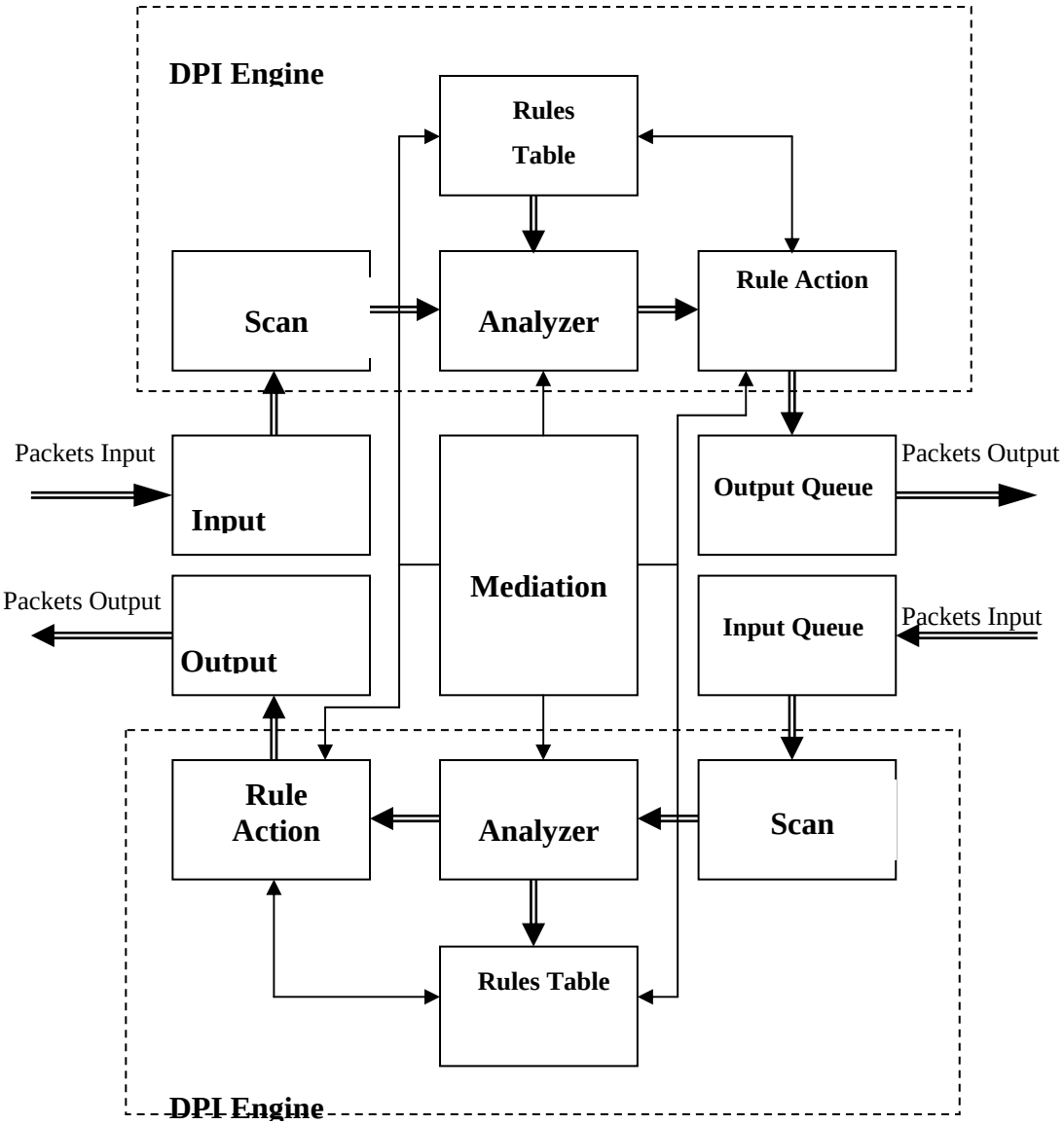

Figure 3 – The bi-directional DPI function and architecture