

International Telecommunication Union

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**Y.2771**

(07/2014)

SERIES Y: GLOBAL INFORMATION  
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS  
AND NEXT-GENERATION NETWORKS

Next Generation Networks – Security

---

## Framework for deep packet inspection

Recommendation ITU-T Y.2771

ITU-T Y-SERIES RECOMMENDATIONS

**GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-  
GENERATION NETWORKS**

**GLOBAL INFORMATION INFRASTRUCTURE**

|                                           |             |
|-------------------------------------------|-------------|
| General                                   | Y.100–Y.199 |
| Services, applications and middleware     | Y.200–Y.299 |
| Network aspects                           | Y.300–Y.399 |
| Interfaces and protocols                  | Y.400–Y.499 |
| Numbering, addressing and naming          | Y.500–Y.599 |
| Operation, administration and maintenance | Y.600–Y.699 |
| Security                                  | Y.700–Y.799 |
| Performances                              | Y.800–Y.899 |

**INTERNET PROTOCOL ASPECTS**

|                                                                    |               |
|--------------------------------------------------------------------|---------------|
| General                                                            | Y.1000–Y.1099 |
| Services and applications                                          | Y.1100–Y.1199 |
| Architecture, access, network capabilities and resource management | Y.1200–Y.1299 |
| Transport                                                          | Y.1300–Y.1399 |
| Interworking                                                       | Y.1400–Y.1499 |
| Quality of service and network performance                         | Y.1500–Y.1599 |
| Signalling                                                         | Y.1600–Y.1699 |
| Operation, administration and maintenance                          | Y.1700–Y.1799 |
| Charging                                                           | Y.1800–Y.1899 |
| IPTV over NGN                                                      | Y.1900–Y.1999 |

**NEXT GENERATION NETWORKS**

|                                                                   |               |
|-------------------------------------------------------------------|---------------|
| Frameworks and functional architecture models                     | Y.2000–Y.2099 |
| Quality of Service and performance                                | Y.2100–Y.2199 |
| Service aspects: Service capabilities and service architecture    | Y.2200–Y.2249 |
| Service aspects: Interoperability of services and networks in NGN | Y.2250–Y.2299 |
| Enhancements to NGN                                               | Y.2300–Y.2399 |
| Network management                                                | Y.2400–Y.2499 |
| Network control architectures and protocols                       | Y.2500–Y.2599 |
| Packet-based Networks                                             | Y.2600–Y.2699 |

**Security Y.2700–Y.2799**

|                                |               |
|--------------------------------|---------------|
| Generalized mobility           | Y.2800–Y.2899 |
| Carrier grade open environment | Y.2900–Y.2999 |

**FUTURE NETWORKS**

Y.3000–Y.3499

**CLOUD COMPUTING**

Y.3500–Y.3999

*For further details, please refer to the list of ITU-T Recommendations.*

# Recommendation ITU-T Y.2771

## Framework for deep packet inspection

### Summary

Recommendation ITU-T Y.2771 provides a framework for deep packet inspection (DPI). The primary purpose of this framework is to describe a structured approach for designing, defining and implementing DPI solutions in support of service/application awareness for facilitating interoperability in the evolving networks. It serves to identify and assist in understanding the network issues, from primarily an architectural viewpoint. This Recommendation also provides DPI framework aspects from modelling and performance.

The purpose of such frameworks is especially to outline possible relationships between a DPI function and other network functions, to assist in identifying requirements for DPI functions (which would be the subject of other ITU-T Recommendations like, e.g., Recommendation ITU-T Y.2770) and to help for terminology work (e.g., when a definition would be related to a functional model).

### History

| Edition | Recommendation | Approval   | Study Group | Unique ID*                                                                   |
|---------|----------------|------------|-------------|------------------------------------------------------------------------------|
| 1.0     | ITU-T Y.2771   | 2014-07-18 | 13          | <a href="http://handle.itu.int/11.1002/1000/11830-en">11.1002/1000/12178</a> |

---

\* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2014

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## Table of Contents

|     |                                                                                                           | <b>Page</b> |
|-----|-----------------------------------------------------------------------------------------------------------|-------------|
| 1   | Scope .....                                                                                               | 1           |
| 2   | References.....                                                                                           | 1           |
| 3   | Definitions .....                                                                                         | 2           |
| 3.1 | Terms defined elsewhere .....                                                                             | 2           |
| 3.2 | Terms defined in this Recommendation.....                                                                 | 3           |
| 4   | Abbreviations and acronyms .....                                                                          | 4           |
| 4.1 | General abbreviations and acronyms.....                                                                   | 4           |
| 4.2 | Mathematical symbols .....                                                                                | 6           |
| 5   | Conventions .....                                                                                         | 6           |
| 6   | Architectural framework.....                                                                              | 7           |
| 6.1 | Network architecture framework – High-level network scenarios.....                                        | 7           |
| 6.2 | Protocol architectural framework – Packet inspection level for some<br>example network applications ..... | 8           |
| 7   | Modelling framework .....                                                                                 | 16          |
| 7.1 | Functional models .....                                                                                   | 16          |
| 7.2 | Information and data models .....                                                                         | 30          |
| 7.3 | Traffic models .....                                                                                      | 31          |
| 7.4 | Identification of possible DPI-FE subcomponents.....                                                      | 37          |
| 7.5 | Fault tolerance models.....                                                                               | 38          |
| 8   | Performance framework .....                                                                               | 43          |
| 8.1 | Purpose and scope of performance considerations.....                                                      | 43          |
| 8.2 | Performance metrics .....                                                                                 | 44          |
| 8.3 | Performance of policy enforcement points, estimation of qualitative<br>performance behaviour .....        | 52          |
| 9   | Categorization of DPI functional entities .....                                                           | 55          |
| 9.1 | Categorization principles.....                                                                            | 55          |
| 9.2 | Capabilities in terms of conditions processing.....                                                       | 55          |
| 9.3 | Capabilities in terms of actions processing .....                                                         | 55          |
| 9.4 | DPI-FE types .....                                                                                        | 55          |
| 10  | Security considerations .....                                                                             | 56          |
|     | Appendix I Example functional architecture of probabilistic DPI based on the bloom<br>filter .....        | 57          |
|     | I.1 Introduction.....                                                                                     | 57          |
|     | I.2 Functional model of bloom filter based probabilistic DPI.....                                         | 58          |
|     | Bibliography.....                                                                                         | 59          |



# Recommendation ITU-T Y.2771

## Framework for deep packet inspection

### 1 Scope

This Recommendation provides a framework for deep packet inspection (DPI) in packet-based networks. The primary purpose of this Recommendation is to describe the fundamental concepts, functional components and capabilities of DPI that can be used to identify information flows in packet-based networks by DPI entities, to support the specification of DPI requirements and to guide structured solutions for packet-based networks (such as NGNs).

This Recommendation provides high-level system information with regard to some fundamental concepts as typically relevant when realizing DPI entities. However, it is not expected to present all-inclusive detailed specifications for the DPI. Rather, this Recommendation provides an high-level information (i.e., a framework) and is intended to be used as background material for use by ITU Study Groups and other expert groups outside the ITU, e.g., as input for their development of detailed standards for DPI functionalities.

The scope of this Recommendation includes:

- a) basic architectural principles that will be encountered in combining DPI in various network architectures;
- b) protocol architectural aspects from the perspective of DPI;
- c) example functional models and their application to DPI use case scenarios; and
- d) performance frameworks in order to assist in DPI performance discussions like the identification of key performance indicators related to DPI.

Implementers and users of this ITU-T Recommendation shall comply with all applicable national and regional laws, regulations and policies. The mechanism described in this Recommendation may not be applicable to international correspondence in order to ensure the secrecy and sovereign national legal requirements placed upon telecommunications providers, as well as the ITU Constitution and Convention.

### 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.

- [ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service*.
- [ITU-T G.602] Recommendation ITU-T G.602 (1988), *Reliability and availability of analogue cable transmission systems and associated equipments*.
- [ITU-T H.248.86] Recommendation ITU-T H.248.86 (2014), *Gateway control protocol: H.248 Support for deep packet inspection*.
- [ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

- [ITU-T X.731] Recommendation ITU-T X.731 (1992), *Information technology – Open Systems Interconnection – Systems management: State management function*.
- [ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.
- [ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks*.
- [ETSI TS 132 410] ETSI TS 132 410 (2012), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Key Performance Indicators (KPI) for UMTS and GSM (3GPP TS 32.410 version 11.0.0 Release 11*.
- [IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification*.
- [IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.
- [IETF RFC 5101] IETF RFC 5101 (2008), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

##### 3.1.1 **application** [ITU-T Y.2770]: A designation of one of the following:

- An *application protocol type* (e.g., IP application protocols ITU-T H.264 video, or session initiation protocol (SIP));
- A *served user instance* (e.g., VoIP, VoLTE, VoIMS, VoNGN, and VoP2P) of an application type, e.g., "voice-over-Packet application";
- A "*provider specific application*" for voice-over-Packet, (e.g., 3GPP provider VoIP, Skype VoIP); and
- an application embedded in another application (e.g., application content in a body element of a SIP or an HTTP message).

An application is identifiable by a particular identifier (e.g., via a bit field, pattern, signature, or regular expression as "application level conditions", see also clause 3.2.2 of [ITU-T Y.2770]), as a common characteristic of all the above listed levels of applications.

##### 3.1.2 **availability** [ITU-T E.800]: Availability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided.

##### 3.1.3 **application-descriptor (also known as application-level conditions)** [ITU-T Y.2770]: A set of rule conditions that identify the application (according to clause 3.2.1 of [ITU-T Y.2770]).

This Recommendation addresses the application descriptor as an object in general, which is synonymous with application-level conditions. It does not deal with its detailed structure, e.g., syntax, encoding and data type.

##### 3.1.4 **deep packet inspection (DPI)** [ITU-T Y.2770]: Analysis, according to the layered protocol architecture OSI-BRM [ITU-T X.200], of:

- payload and/or packet properties (see list of potential properties in clause 3.2.11 of [ITU-T Y.2770]) deeper than protocol layer 2, 3 or 4 (L2/L3/L4) header information, and
- other packet properties

in order to identify the application unambiguously.

NOTE – The output of the DPI function, along with some extra information such as the flow information is typically used in subsequent functions such as reporting or actions on the packet.

**3.1.5 DPI engine** [ITU-T Y.2770]: A subcomponent and central part of the DPI functional entity which performs all packet path processing functions (e.g., packet identification and other packet processing functions in Figure 6-1 of [ITU-T Y.2770]).

**3.1.6 DPI policy condition (also known as DPI signature)** [ITU-T Y.2770]: A representation of the necessary state and/or prerequisites that identify an application and define whether a policy rule's actions should be performed. The set of DPI policy conditions associated with a policy rule specifies when the policy rule is applicable (see also [b-IETF RFC 3198]).

A DPI policy condition must contain application level conditions and may contain other options such as state conditions and/or flow level conditions:

- 1) State condition (optional):
  - a) network grade of service conditions (e.g., experienced congestion in packet paths); or
  - b) network element status (e.g., local overload condition of the DPI-FE).
- 2) Flow descriptor/Flow level conditions (optional):
  - a) packet content (header fields);
  - b) characteristics of a packet (e.g., number# of MPLS labels);
  - c) packet treatment (e.g., output interface of the DPI-FE).
- 3) Application descriptor/application level conditions:
  - a) Packet content (application header fields and application payload).

NOTE – The condition relates to the "simple condition" in the formal descriptions of flow level conditions and application level conditions.

**3.1.7 DPI policy decision functional entity (DPI-PDFE)** [ITU-T Y.2770]: The function remote to the DPI-FE that decides the signature-based rules to be enforced in the DPI-FE. Some control and/or management functions may not necessarily be remote from the DPI-FE.

**3.1.8 flow descriptor (also known as flow level conditions)** [ITU-T Y.2770]: A set of rule conditions that is used to identify a specific type of flow (according to clause 3.1.3 of [ITU-T Y.2770]) from inspected traffic.

NOTE 1 – This definition of flow descriptor extends the definition in [b-ITU-T Y.2121] with additional elements as described in clause 3 of [ITU-T Y.2770].

NOTE 2 – For further normative discussion of the flow descriptor as used in [ITU-T Y.2770], see Annex A of [ITU-T Y.2770].

**3.1.9 reliability** [ITU-T E.800]: The probability that an item can perform a required function under stated conditions for a given time interval.

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 DPI analyser:** A subsequent entity in the DPI processing path (within a DPI policy enforcement function) with focus on comparison functions between the particular packet headers and payloads of preselected packet flows. The primary scope of the DPI analyser is related to the evaluation of DPI policy *conditions* against *preselected* incoming packets.

NOTE – The DPI analyser may be located after a DPI scanner (see clause 3.2.6). The DPI analyser may provide the functionality of an intrusion detection system (IDS) analyser.

**3.2.2 DPI node:** A network element or device that realizes the DPI related functions. It is thus a generic term used to designate the realization of a DPI physical entity.

NOTE – Functional perspective: the DPI node function (DPI-NF) comprises the DPI policy enforcement function (DPI-PEF) and the (optional) local policy decision function (L-PDF); hence, the DPI-NF is functionally equal to the DPI functional entity.

**3.2.3 DPI policy action (action in short):** Definition of what is to be done to enforce a policy rule, when the conditions of the rule are met. Policy actions may result in the execution of one or more operations to affect and/or configure network traffic and network resources; see also [b-IETF RFC 3198].

**3.2.4 DPI policy enforcement function (DPI-PEF):** A logical entity that enforces policy decisions, given by DPI policy rules.

**3.2.5 DPI scanner (also used as "DPI scan function"):** The first entity in the DPI processing path (within a DPI policy enforcement function) which provides a pre-selection (related to the subsequent DPI analyser, see clause 3.2.1) by checking *all* DPI policy *conditions* against *all* incoming packets.

**3.2.6 DPI "1+N" redundancy group:** The collection of DPI functional components (e.g., DPI node, DPI-PIB, DPI engine, etc.) following a "1+N" redundancy architecture (and  $N \geq 1$ ), given by a single working component and N protection components.

NOTE – The above collection is used to provide extra reliability and improve availability for a DPI node or network deployed with one or DPI nodes.

## 4 Abbreviations and acronyms

### 4.1 General abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

|                    |                                       |
|--------------------|---------------------------------------|
| A <sub>DPI</sub>   | DPI policy action                     |
| BRM                | Basic Reference Model                 |
| CAM                | Content Addressable Memory            |
| C <sub>DPI</sub>   | DPI policy condition                  |
| DAI                | Deep Application Identification       |
| DHI                | Deep Header Inspection                |
| DiffServ           | Differential Service                  |
| DPI                | Deep Packet Inspection                |
| DPI-AcEF           | DPI Action Execution Function         |
| DPI-AnF            | DPI Analyser Function                 |
| DPI-FE             | DPI Functional Entity                 |
| DPI <sub>InP</sub> | In-Path DPI                           |
| DPI-NF             | DPI Node Function                     |
| DPI <sub>OoP</sub> | Out-of-Path DPI                       |
| DPI-PDFE           | DPI Policy Decision Functional Entity |
| DPI-PE             | DPI Physical Entity                   |
| DPI-PEF            | DPI Policy Enforcement Function       |

|                    |                                                                   |
|--------------------|-------------------------------------------------------------------|
| DPI-PIB            | DPI Policy Information Base                                       |
| DPI-PIF            | DPI Packet Identification Function                                |
| DPI-ScF            | DPI Scan Function                                                 |
| DNNF               | Determining Next Node Function                                    |
| FIB                | Forwarding Information Base                                       |
| FTP                | File Transfer Protocol                                            |
| HTTP               | Hypertext Transfer Protocol                                       |
| HW                 | Hardware                                                          |
| IDS                | Intrusion Detection System                                        |
| IP                 | Internet Protocol                                                 |
| IPFIX              | IP Flow Information Export                                        |
| KPI                | Key Performance Indicator                                         |
| KPI <sub>DPI</sub> | Key performance indicators for DPI entities                       |
| L-PDF              | Local PDF                                                         |
| L2VPN              | Layer 2 Virtual Private Network                                   |
| L <sub>X</sub> HI  | Header Inspection of protocol Layer X                             |
| L <sub>X</sub> PI  | Payload Inspection of protocol Layer X                            |
| LX                 | (Protocol) Layer X                                                |
| LX+                | Higher (Protocol) Layer than LX                                   |
| MIB                | Management Information Base                                       |
| MPI                | Medium depth Packet Inspection                                    |
| MPLS               | Multi-Protocol Label Switch                                       |
| MTBF               | Mean Time Between Failures                                        |
| MTTR               | Mean Time To Repair                                               |
| NA(P)T             | Network Address (and Port) Translation                            |
| NGN                | Next Generation Network                                           |
| OSI-BRM            | Open System Interconnection-Basic Reference Model                 |
| PDF                | Policy Decision Function                                          |
| PEP                | Policy Enforcement Point                                          |
| PFF                | Packet Forwarding Function                                        |
| PIB                | Policy Information Base                                           |
| QoS                | Quality of Service                                                |
| RACF               | Resource and Admission Control Functions                          |
| R <sub>DPI</sub>   | DPI policy rule                                                   |
| R-PDF              | Remote PDF (i.e., PDF remotely located from DPI node perspective) |
| RTSP               | Real Time Streaming Protocol                                      |
| SDU                | Service Data Unit                                                 |

|                     |                                    |
|---------------------|------------------------------------|
| SIP                 | Session Initiation Protocol        |
| SPI                 | Shallow Packet Inspection          |
| S <sub>D</sub> -PDF | Session-dependent PDF              |
| S <sub>I</sub> -PDF | Session-independent PDF            |
| SW                  | Software                           |
| TCAM                | Ternary Content Addressable Memory |
| TCP                 | Transmission Control Protocol      |
| TOS                 | Type of Service                    |
| VoIP                | Voice over IP                      |
| VoLTE               | Voice over Long Term Evolution     |
| VoIMS               | Voice over Integrated Media System |
| VoNGN               | Voice over Next Generation Network |
| VoP2P               | Voice over Peer to Peer            |

## 4.2 Mathematical symbols

This Recommendation uses the following symbols (with name, unit and brief description):

|                              |                                                |                    |
|------------------------------|------------------------------------------------|--------------------|
| $\varepsilon_{\text{DPI}}$   | (DPI) error rate                               | —                  |
| $\varepsilon_{\text{f-n}}$   | (DPI) false-negative error rate                | —                  |
| $\varepsilon_{\text{f-p}}$   | (DPI) false-positive error rate                | —                  |
| $\phi_{\text{P,In}}$         | (DPI) processing rate of incoming packets      | [s <sup>-1</sup> ] |
| $\phi_{\text{P,Out}}$        | (DPI) packet rate in outgoing direction        | [s <sup>-1</sup> ] |
| $\phi_{\text{P,Node,Out}}$   | Packet node throughput                         | —                  |
| $\phi_{\text{P,Identified}}$ | Rate of successfully identified packets        | —                  |
| $P_{\text{Hit,BloomFilter}}$ | Estimated information certainty of probability | —                  |
| $N_{\text{db}}$              | The number of DPI policy rules                 | —                  |
| $S_{\text{p}}$               | The packet size                                | —                  |
| $N_{\text{DPIeng}}$          | The number of DPI engines                      | —                  |
| $\tau_{\text{TD}}$           | Node-internal transfer delay (of DPI node)     | [ns]               |
| $\underline{A}$              | Set of (DPI policy) rule actions               | —                  |
| $\underline{C}$              | Set of (DPI policy) rule conditions            | —                  |
| $\underline{R}$              | Set of (DPI policy) rules                      | —                  |

## 5 Conventions

None.

## 6 Architectural framework

### 6.1 Network architecture framework – High-level network scenarios

This framework outlines the major boundary conditions of a DPI deployment in a network infrastructure. Some principle DPI framework scenarios may be identified by consideration of criteria like:

- **Network location level** (i.e., the location of a DPI entity in a packet network domain)
  - at the edge ("**border DPI**"); or
  - within the network ("**core DPI**");
  - between peering networks ("**peering DPI**").
- **Network packet (path) types** (i.e., the kind of packet types are inspected)<sup>1</sup>
  - user plane (or transport stratum; e.g., IP data-path, IP media-path, IP bearer-path, tunnel, MPLS LSR, pseudo wire, etc.); or
  - control plane (or service stratum; e.g., IP signalling-path); or
  - management plane; or
  - combinations.
- **Alignment level with other network architectures** (i.e., the level how a DPI entity is coupled with the underlying packet network architecture)
  - **isolated DPI** entity (i.e., the DPI entity is hidden from the packet network),  
Examples:
    - a very few DPI entities located on selected points in the network (without the goal of "full coverage"; something like a probe-style in-path DPI);
    - Out-of-path DPI entities.
  - **overlay DPI** network (i.e., there is a dedicated DPI network infrastructure, overlayed to the underlying packet network; both network infrastructures are separated from an operational perspective),  
Examples:
    - generic example: a network of in-path DPI entities which share, e.g., the user plane paths, but use separate control and/or management interfaces;
    - specific example: e.g., a DPI function with the purpose of intrusion detection.
  - **embedded DPI** entity (i.e., the DPI functional entity is embedded in a physical network element together with other functional entities with regard to non-DPI packet processing; such a physical entity should provide, e.g., a single OAM interface from a cost-effective operational perspective, which implies consequently a harmonized management model across all functional entities),  
Examples:
    - generic example: a DPI entity with a management information base which is aligned with the management base of the other, non-DPI functional entities of the same physical network element;
    - specific example: a DPI functional entity within RACF and a common management capability, but without sharing any RACF control interfaces.
  - **integral DPI** (i.e., a DPI entity "fully integrated" in "the packet network"),

<sup>1</sup> The notion of "packet type" could be made specific by referring to a dedicated "protocol" or a "protocol stack". Though, that level of detail is not required here.

Examples:

- generic example: an SDO-defined network reference model (architecture) which takes into account DPI entities;
- specific example: ITU-T RACF extended by DPI entities which may use existing reference points (e.g., "Rw-controlled DPI" or an ITU-T H.248-based Rw extended by support of [ITU-T H.248.86]) or may introduce new reference points).

There are consequently numerous use cases from the perspective of the network integration scenario of a DPI entity.

## **6.2 Protocol architectural framework – Packet inspection level for some example network applications**

### **6.2.1 Principle**

There are various packet inspection levels. Table 6-1 provides an overview of typical network applications with respect to required involvement of "packet inspection levels". The packet inspection level may be denoted either:

- 1) according to a basic reference model (BRM) for layered protocol architectures, here columns  $L_{xHI}$  and  $L_{yPI}$ ; or
- 2) using "old" colloquial terms (which are described in clause 8.1 of [b-ITU-T Y-Sup.23]), here columns shallow packet inspection (SPI), medium packet inspection (MPI), deep header inspection (DHI) and deep application inspection (DAI).

See also clause 8 in [b-ITU-T Y-Sup.23] on the aspect of DPI in layered protocol architectures.

### **6.2.2 Distinction of cases DPI and non-DPI**

The concept of DPI, from the perspective of layered protocol architectures, is fairly wide and includes even all protocol layers above layer 1 (see clause 3.2.5 of [ITU-T Y.2770]). However, the scope of packet inspection could be basically limited in case of specific network application, such as primarily related on link, network and/or transport layers only.

Such a limitation is/was typically motivated by service-, historical- or/and implementation-related aspects, for instance, economical trade-off decisions with respect to an achievable DPI service versus state-of-the-art technique. Such a kind of limited packet inspection is/was also known as shallow packet inspection, and medium depth packet inspection (SPI, MPI; see also clause 8.1 in [b-ITU-T Y-Sup.23]).

The coarse granular distinction between DPI and non-DPI according to [ITU-T Y.2770] is sufficient and also followed by this Recommendation. The notion of 'DPI' here means (loosely) policy inspection rules as supported by this Recommendation, and 'non DPI' relates more to legacy packet inspection at protocol layers 2, 3 and/or 4 (i.e., SPI, MPI).

### **6.2.3 Examples**

Table 6-1 provides a list of example network applications versus packet inspection levels, as typically part of such network applications. It should be noted that the indications by Table 6-1 are only exemplary and not necessarily exhaustive.

**Table 6-1 – Packet inspection level for some example network applications**

| Network application<br>(example)               |                                                                                                                 | Packet inspection level                          |                                                 |                       |                                               | Comments                                                                              |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------|-------------------------------------------------|-----------------------|-----------------------------------------------|---------------------------------------------------------------------------------------|
|                                                |                                                                                                                 | "Deep packet inspection" (DPI)                   |                                                 |                       |                                               |                                                                                       |
|                                                |                                                                                                                 | (Note)                                           | "Deep header inspection" (DHI)                  |                       | "Deep application<br>identification"<br>(DAI) |                                                                                       |
|                                                |                                                                                                                 |                                                  | "Medium depth packet"                           |                       |                                               |                                                                                       |
|                                                |                                                                                                                 |                                                  | "Shallow<br>packet<br>inspection"<br>(SPI)      | "Inspection"<br>(MPI) |                                               |                                                                                       |
| L2 header<br>inspection<br>(L <sub>2</sub> HI) | L3,4 header<br>inspection<br>(L <sub>3,4</sub> HI)                                                              | L4+ header<br>inspection<br>(L <sub>4+</sub> HI) | L7 payload<br>inspection<br>(L <sub>7</sub> PI) |                       |                                               |                                                                                       |
| Security:                                      |                                                                                                                 |                                                  |                                                 |                       |                                               |                                                                                       |
| 1.1                                            | Network intrusion<br>detection                                                                                  | –                                                | X                                               | X                     | X                                             | There are different ID methods,<br>a) anomaly detection<br>b) misuse detection (here) |
| 1.2                                            | Security protection of<br>network resources<br>(network intrusion<br>prevention, security<br>attack prevention) | –                                                | X                                               | X                     | X                                             |                                                                                       |
| 1.3                                            | Other security-related<br>functions                                                                             |                                                  |                                                 |                       |                                               |                                                                                       |

Table 6-1 – Packet inspection level for some example network applications

| Network application<br>(example)               |                                                              | Packet inspection level                          |                                                 |                       |                                               | Comments                                                                                                   |
|------------------------------------------------|--------------------------------------------------------------|--------------------------------------------------|-------------------------------------------------|-----------------------|-----------------------------------------------|------------------------------------------------------------------------------------------------------------|
|                                                |                                                              | "Deep packet inspection" (DPI)                   |                                                 |                       |                                               |                                                                                                            |
|                                                |                                                              | (Note)                                           | "Deep header inspection" (DHI)                  |                       | "Deep application<br>identification"<br>(DAI) |                                                                                                            |
|                                                |                                                              |                                                  | "Medium depth packet"                           |                       |                                               |                                                                                                            |
|                                                |                                                              |                                                  | "Shallow<br>packet<br>inspection"<br>(SPI)      | "Inspection"<br>(MPI) |                                               |                                                                                                            |
| L2 header<br>inspection<br>(L <sub>2</sub> HI) | L3,4 header<br>inspection<br>(L <sub>3,4</sub> HI)           | L4+ header<br>inspection<br>(L <sub>4+</sub> HI) | L7 payload<br>inspection<br>(L <sub>7</sub> PI) |                       |                                               |                                                                                                            |
| Identification:                                |                                                              |                                                  |                                                 |                       |                                               |                                                                                                            |
| 2.1                                            | Subscriber, user                                             | –                                                | X                                               | –                     | –                                             | Identified by ...? (e.g., network address)                                                                 |
| 2.2                                            | Application type                                             | –                                                | –                                               | X                     | X                                             | Identified by ...? (e.g., application layer protocol type)                                                 |
| 2.3                                            | Session                                                      | –                                                | X                                               | –                     | –                                             | Identified by ...? (e.g., IP connection, IP transport connection). See also clause 7 in [b-ITU-T Y-Sup.23] |
| 2.4                                            | Application control protocol (e.g., SIP, RTSP, HTTP, FTP...) | –                                                | X<br>(dependent on well-known port)             | X                     | X                                             |                                                                                                            |
| Application data characteristics:              |                                                              |                                                  |                                                 |                       |                                               |                                                                                                            |
| 2.5                                            | Content                                                      | –                                                | –                                               | X                     | X                                             | For example, illegal content                                                                               |

Table 6-1 – Packet inspection level for some example network applications

| Network application<br>(example)               |                                                       | Packet inspection level                          |                                                 |                                               |   | Comments                                                    |
|------------------------------------------------|-------------------------------------------------------|--------------------------------------------------|-------------------------------------------------|-----------------------------------------------|---|-------------------------------------------------------------|
|                                                |                                                       | "Deep packet inspection" (DPI)                   |                                                 |                                               |   |                                                             |
|                                                |                                                       | (Note)                                           | "Deep header inspection" (DHI)                  | "Deep application<br>identification"<br>(DAI) |   |                                                             |
|                                                |                                                       |                                                  | "Medium depth packet"                           |                                               |   |                                                             |
|                                                |                                                       |                                                  | "Shallow<br>packet<br>inspection"<br>(SPI)      | "Inspection"<br>(MPI)                         |   |                                                             |
| L2 header<br>inspection<br>(L <sub>2</sub> HI) | L3,4 header<br>inspection<br>(L <sub>3,4</sub> HI)    | L4+ header<br>inspection<br>(L <sub>4+</sub> HI) | L7 payload<br>inspection<br>(L <sub>7</sub> PI) |                                               |   |                                                             |
| 2.6                                            | Media type<br>(Application data type)                 | —                                                | —                                               | X                                             | X |                                                             |
| 2.7                                            | Media format                                          | —                                                | —                                               | X                                             | X |                                                             |
| Modification (of protocol data units):         |                                                       |                                                  |                                                 |                                               |   |                                                             |
| 3.1                                            | Modification 'content':<br>Removing of viruses        | —                                                | —                                               | —                                             | X |                                                             |
| 3.2                                            | Modification 'header':<br>QoS marking                 | —                                                | X                                               | X                                             | — |                                                             |
| 3.3                                            | Modification 'header &<br>content':<br>"ALG function" | —                                                | X                                               | X                                             | — | Local NA(P)T function on L3<br>(& L4) and application layer |

Table 6-1 – Packet inspection level for some example network applications

| Network application<br>(example)               |                                                        | Packet inspection level                          |                                                 |                       |                                               | Comments                            |
|------------------------------------------------|--------------------------------------------------------|--------------------------------------------------|-------------------------------------------------|-----------------------|-----------------------------------------------|-------------------------------------|
|                                                |                                                        | "Deep packet inspection" (DPI)                   |                                                 |                       |                                               |                                     |
|                                                |                                                        | (Note)                                           | "Deep header inspection" (DHI)                  |                       | "Deep application<br>identification"<br>(DAI) |                                     |
|                                                |                                                        |                                                  | "Medium depth packet"                           |                       |                                               |                                     |
|                                                |                                                        |                                                  | "Shallow<br>packet<br>inspection"<br>(SPI)      | "Inspection"<br>(MPI) |                                               |                                     |
| L2 header<br>inspection<br>(L <sub>2</sub> HI) | L3,4 header<br>inspection<br>(L <sub>3,4</sub> HI)     | L4+ header<br>inspection<br>(L <sub>4+</sub> HI) | L7 payload<br>inspection<br>(L <sub>7</sub> PI) |                       |                                               |                                     |
| Usage parameter monitoring:                    |                                                        |                                                  |                                                 |                       |                                               |                                     |
| 4.1                                            | Service level agreements                               | –                                                | X                                               | X                     | X                                             |                                     |
| 4.2                                            | Traffic parameter control<br>Examples:                 | –                                                | X                                               | X                     | X                                             | Dependent on traffic parameter type |
|                                                | L3 byte rate policing<br>(peak rate, sustainable rate) | –                                                | X                                               | –                     | –                                             |                                     |
|                                                | L3 PDU size (min, max) policing                        | –                                                | X                                               | –                     | –                                             |                                     |
|                                                | L3 burst size policing                                 | –                                                | X                                               | –                     | –                                             |                                     |
|                                                | L7 SDU size policing<br>("application payload")        | –                                                | X                                               | X                     | –                                             |                                     |
|                                                | L7 byte rate policing                                  | –                                                | X                                               | X                     | –                                             |                                     |

Table 6-1 – Packet inspection level for some example network applications

| Network application<br>(example)               |                                                    | Packet inspection level                          |                                                 |                                               |   | Comments                                            |
|------------------------------------------------|----------------------------------------------------|--------------------------------------------------|-------------------------------------------------|-----------------------------------------------|---|-----------------------------------------------------|
|                                                |                                                    | "Deep packet inspection" (DPI)                   |                                                 |                                               |   |                                                     |
|                                                |                                                    | (Note)                                           | "Deep header inspection" (DHI)                  | "Deep application<br>identification"<br>(DAI) |   |                                                     |
|                                                |                                                    |                                                  | "Medium depth packet"                           |                                               |   |                                                     |
|                                                |                                                    |                                                  | "Shallow<br>packet<br>inspection"<br>(SPI)      | "Inspection"<br>(MPI)                         |   |                                                     |
| L2 header<br>inspection<br>(L <sub>2</sub> HI) | L3,4 header<br>inspection<br>(L <sub>3,4</sub> HI) | L4+ header<br>inspection<br>(L <sub>4+</sub> HI) | L7 payload<br>inspection<br>(L <sub>7</sub> PI) |                                               |   |                                                     |
|                                                | ("application volume")                             |                                                  |                                                 |                                               |   |                                                     |
|                                                |                                                    |                                                  |                                                 |                                               |   |                                                     |
| Quality of Service support:                    |                                                    |                                                  |                                                 |                                               |   |                                                     |
| 5.1                                            | Traffic shaping                                    | —                                                | X                                               | —                                             | — | See e.g., [b-ITU-T Y.1221] or<br>[b-ITU-T H.248.53] |
|                                                | L3 byte rate shaping                               | —                                                | X                                               | —                                             | — |                                                     |
|                                                |                                                    |                                                  |                                                 |                                               |   |                                                     |
| Network analysis:                              |                                                    |                                                  |                                                 |                                               |   |                                                     |
| 6.1                                            | User behaviour                                     | —                                                | X                                               | X                                             | X |                                                     |
| 6.2                                            | Usage patterns                                     | —                                                | X                                               | X                                             | X |                                                     |

**Table 6-1 – Packet inspection level for some example network applications**

| Network application<br>(example)                                |                                                    | Packet inspection level                          |                                                 |                       |                                               | Comments                                                                  |
|-----------------------------------------------------------------|----------------------------------------------------|--------------------------------------------------|-------------------------------------------------|-----------------------|-----------------------------------------------|---------------------------------------------------------------------------|
|                                                                 |                                                    | "Deep packet inspection" (DPI)                   |                                                 |                       |                                               |                                                                           |
|                                                                 |                                                    | (Note)                                           | "Deep header inspection" (DHI)                  |                       | "Deep application<br>identification"<br>(DAI) |                                                                           |
|                                                                 |                                                    |                                                  | "Medium depth packet"                           |                       |                                               |                                                                           |
|                                                                 |                                                    |                                                  | "Shallow<br>packet<br>inspection"<br>(SPI)      | "Inspection"<br>(MPI) |                                               |                                                                           |
| L2 header<br>inspection<br>(L <sub>2</sub> HI)                  | L3,4 header<br>inspection<br>(L <sub>3,4</sub> HI) | L4+ header<br>inspection<br>(L <sub>4+</sub> HI) | L7 payload<br>inspection<br>(L <sub>7</sub> PI) |                       |                                               |                                                                           |
| Performance measurements ("key performance indicators" (KPIs)): |                                                    |                                                  |                                                 |                       |                                               |                                                                           |
| 7.1                                                             | Collection of remote<br>measurements               | –                                                | X                                               | X                     | X                                             |                                                                           |
| 7.2                                                             | Generation of local<br>measurements                | –                                                | X                                               | X                     | X                                             |                                                                           |
|                                                                 |                                                    |                                                  |                                                 |                       |                                               |                                                                           |
| Charging/billing support:                                       |                                                    |                                                  |                                                 |                       |                                               |                                                                           |
| 8.1                                                             | Time-based<br>information                          | –                                                | X                                               | –                     | –                                             |                                                                           |
| 8.2                                                             | Traffic volume-based<br>information                | –                                                | X                                               | –                     | X                                             | Traffic volume related to IP<br>byte rate (L3) or/and<br>application data |
| 8.3                                                             | Event-based<br>information                         | –                                                | X                                               | X                     | X                                             | Dependent on event type (e.g.,<br>event may be associated to<br>content)  |

**Table 6-1 – Packet inspection level for some example network applications**

| Network application<br>(example)                                                                                                                                                                                                                                          |                                                                  | Packet inspection level                          |                                                 |                                               |   | Comments |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|--------------------------------------------------|-------------------------------------------------|-----------------------------------------------|---|----------|
|                                                                                                                                                                                                                                                                           |                                                                  | "Deep packet inspection" (DPI)                   |                                                 |                                               |   |          |
|                                                                                                                                                                                                                                                                           |                                                                  | (Note)                                           | "Deep header inspection" (DHI)                  | "Deep application<br>identification"<br>(DAI) |   |          |
|                                                                                                                                                                                                                                                                           |                                                                  |                                                  | "Medium depth packet"                           |                                               |   |          |
|                                                                                                                                                                                                                                                                           |                                                                  |                                                  | "Shallow<br>packet<br>inspection"<br>(SPI)      | "Inspection"<br>(MPI)                         |   |          |
| L2 header<br>inspection<br>(L <sub>2</sub> HI)                                                                                                                                                                                                                            | L3,4 header<br>inspection<br>(L <sub>3,4</sub> HI)               | L4+ header<br>inspection<br>(L <sub>4+</sub> HI) | L7 payload<br>inspection<br>(L <sub>7</sub> PI) |                                               |   |          |
|                                                                                                                                                                                                                                                                           |                                                                  |                                                  |                                                 |                                               |   |          |
| Link-oriented DPI:                                                                                                                                                                                                                                                        |                                                                  |                                                  |                                                 |                                               |   |          |
| 9.1                                                                                                                                                                                                                                                                       | DPI applications with possible layer 2-related policy conditions | X                                                | X                                               | X                                             | X | See Note |
| NOTE – There is a principal distinction between link-oriented DPI and network-oriented DPI. Link-oriented DPI is limited to a L2 network domain, and network-oriented DPI is related to DPI signatures which cover protocol information on network layer (L3) and higher. |                                                                  |                                                  |                                                 |                                               |   |          |