International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y

Supplement 23

(11/2013)

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

ITU-T Y.2770-series – Supplement on DPI terminology

ITU-T Y-series Recommendations – Supplement 23

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.

Supplement 23 to ITU-T Y-series Recommendations

ITU-T Y.2770-series – Supplement on DPI terminology

Summary

Recommendation ITU-T Y.2770 introduced new terms in the area of deep packet inspection (DPI). Work on DPI terminology was an essential part during the development of this Recommendation. This Supplement 23 to the ITU-T Y-series provides complementary information on DPI terminology related to the flow and application descriptor, packet processing and layered protocol architectures, as defined by ITU-T Y.2770.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y Suppl. 23	2013-11-15	13	11.1002/1000/12101

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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/.

Table of Contents

Supplement 23 to ITU-T Y-series Recommendations

ITU-T Y.2770-series – Supplement on DPI terminology

1 Scope

This Supplement provides complementary information to DPI terminology, defined in [ITU-T Y.2770]. This Supplement is structured as follows:

DPI terminology:

- *relationship* and formal specification aspect of key DPI terms (clause 6);
- from perspective of *packet processing* (clause 7); and
- from perspective of *layered protocol architectures* (clause 8).

The purpose of this Supplement is to provide readers of [ITU-T Y.2770] with background information.

2 References

[ITU-T X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks*.

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[IETF RFC 1122] IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers*.

[IETF RFC 1123] IETF RFC 1123 (1989), *Requirements for Internet Hosts – Application and Support*.

[IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.

[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 Supplement 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);
- 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 above listed levels of applications.

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

Recommendation [ITU-T Y.2770] 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.

3.1.3 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.

3.1.4 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 policy rule 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.

3.1.5 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].

3.2 Terms defined in this Supplement

This Supplement defines the following term:

3.2.1 DPI for packets according to IETF-BRM protocol layering (abbreviated as $DPI_{IETF\text{-}BRM}$): The IETF basic reference model (BRM), given by [IETF RFC 791], relates to the OSI-BRM without protocol layers L5 and L6. The $DPI_{IETF\text{-}BRM}$ is thus based on an absolute protocol layering model. There is $DPI_{IETF\text{-}BRM}$ in case of policy rules for *deep* packet inspection with policy conditions primarily based on elements related to protocol layers *above the transport layer*.

NOTE – This does not exclude other indicated methods for DPI application identification as described in [ITU-T Y.2770].

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

ABNF Augmented Backus-Naur Form

AD Application Descriptor

BRM Basic Reference Model

CNF Conjunctive Normal Form

DCCP Datagram Congestion Control Protocol

DNF Disjunctive Normal Form

DPI Deep Packet Inspection

DPI-FE DPI Functional Entity

ERM Extended Reference Model

FD Flow Descriptor

F_D Flow dependent

F_I Flow independent

HTTP Hypertext Transfer Protocol

IANA Internet Assigned Numbers Authority

IE Information Element

IP Internet Protocol

IPFIX (IETF working group) IP Flow Information Export

L Lookup key

LX (Protocol) Layer X

L_YHI Header Inspection at protocol Layer Y

L_YPI Payload Inspection at protocol Layer Y

MPI Medium depth Packet Inspection

NGN Next Generation Network

OSI Open Systems Interconnection

PCI Protocol Control Information

PD Packet Descriptor

PDU Protocol Data Unit

PI	Packet Identification
RTP	Real-time Transport Protocol
SCTP	Stream Control Transmission Protocol
SD	Session Descriptor
SDU	Service Data Unit
SPI	Shallow Packet Inspection (DPI)
SSRC	(RTP) Synchronization Source
TRM	Tunnelled Reference Model

5 Conventions

None.

6 Formal specification of major terminology

6.1 Introduction

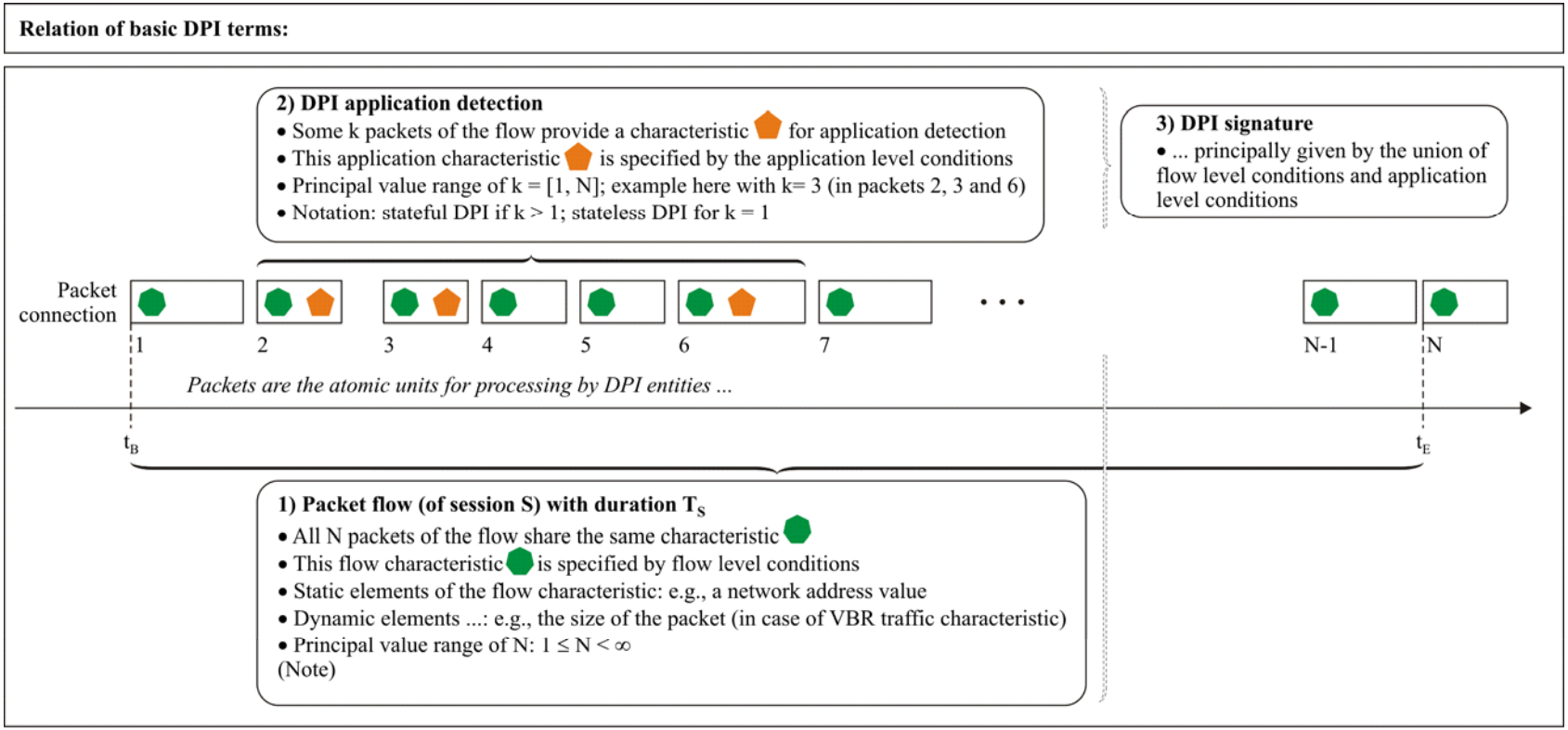
Terminology is defined in clause 3 of this Supplement. There are some crucial terms that are related to each other in the scope of deep packet inspection (DPI). The purpose of this clause is to highlight these principal relationships. This clause focuses on the terms *flow descriptor (flow level conditions)*, *application descriptor (application level conditions)* and *DPI Signature*.

Using a formal description of these terms allows for a more precise elaboration and indication of their differences.

Where there are discrepancies between this clause and clause 3 of [ITU-T Y.2770], [ITU-T Y.2770] takes precedence over this Supplement.

6.2 Summary and illustration of terms

Figure 6-1 provides a high-level summary and illustration of the underlying concepts and relationships of these terms.



t_B Arrival time of 1st packet (of a flow) at DPI entity
t_E Arrival time of last packet (of a flow) at DPI entity
t_S Session duration ($= t_E - t_B$)

NOTE – There will be a maximum value in practice due to the finite length of communication associations in reality.

Figure 6-1 – Illustration of the three major terms: *flow descriptor*, *application descriptor* and *DPI signature*

6.3 Using a formal description technique for the terms

The Augmented Backus–Naur Form (ABNF) is used as the formal language example in this clause.

6.3.1 Formal specification of flow descriptor (flow level conditions)

Table 6-1 provides a formal description of the flow level conditions, which is in line with the prose specification for *flow* (see clause 3.1.3 of [ITU-T Y.2770]); for flow descriptor/flow level conditions see clause 3.2.16 of [ITU-T Y.2770].

Table 6-1 – Formal specification of flow descriptor (flow level conditions)

ABNF (shortened)	Comments
`Flow Descriptor = CompoundCondition`	The flow descriptor relates to a logical function, which is effectively a set of rule conditions enforced for packet (flow) policing.
`CompoundCondition = DNF (*SimpleCondition) /` `CNF (*SimpleCondition)`	DNF Disjunctive Normal Form CNF Conjunctive Normal Form
`SimpleCondition = "(<Variable> MATCH <Value>)"`	Elementary condition structure.
`Variable = ...`	Flow-specific Information Element (e.g., according to the IANA registry (see: http://www.iana.org/assignments/ipfix/ipfix.xhtml) for IPFIX [IETF RFC 5101])
`MATCH = "=" / "<" / ...`	Match operator (the relationship between variable and value; Note).
`Value = ...`	Given by IE-specific defined value range
NOTE – Inclusive other operators, e.g., for heuristics, behavioural, or statistical relationships, e.g., "nearly match", "approximative match", etc.	

6.3.2 Formal specification of application descriptor (application level conditions)

Table 6-2 provides a formal description of the application level conditions, which is in line with the prose specification of clause 3.2.2 of [ITU-T Y.2770].

Table 6-2 – Formal specification of application descriptor (application level conditions)

ABNF (shortened)	Comments
`Application Descriptor = CompoundCondition`	Conceptually the same as the Flow Descriptor.
`CompoundCondition = DNF (*SimpleCondition) /` `CNF (*SimpleCondition)`	See Table 6-1.
`SimpleCondition = "(<Variable> MATCH <Value>)"`	See Table 6-1.
`Variable = ...`	Generic Information Element (Notes 1, 2)
`MATCH = "=" / "<" / ...`	See Table 6-1.
`Value = ...`	See Table 6-1.
NOTE 1 – The location (within the protocol data unit) of this IE may be additionally limited on a particular range of the packet (e.g., via a bit-offset). NOTE 2 – There could be also internal (state) variables in case of stateful DPI.	

6.3.3 Formal specification of DPI Signature

Table 6-3 provides a formal description for DPI signature, which is in line with the prose specification of clause 3.2.14 of [ITU-T Y.2770].

Table 6-3 – Formal specification of DPI Signature

ABNF (shortened)	Comments
`Signature = Application Descriptor AND 0*1Flow Descriptor`	Any signature comprises at least an *Application Descriptor* plus an optional *Flow Descriptor* (Note).
NOTE – Leading to the two principal scenarios of flow-dependent and flow-independent DPI.	

7 Illustration of terminology related to packet processing

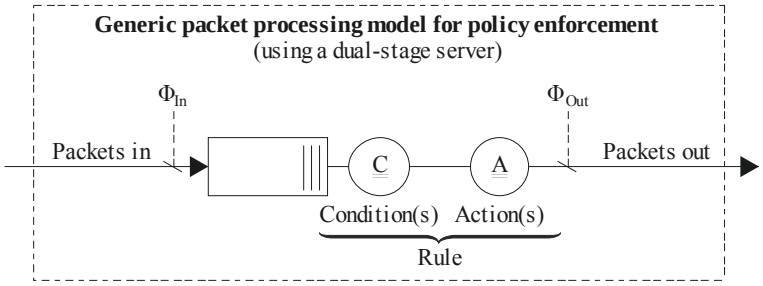
7.1 Introduction

Recommendation [ITU-T Y.2770] defines requirements for DPI. Some of these requirements refer to *identification* of packets (and aggregates like flow) and indicate possible *actions* after identification. The terms *filtering*, *classification*, *modification*, etc., of packets are used in this context. There are commonalities and differences between these terms and those used in the scope of [ITU-T Y.2770].

The purpose of this clause is to illustrate the underlying concept.

7.2 Rule-oriented packet processing

The consideration of *packet inspection* as *rule-based packet processing* allows for depicting the key differences between terms. Figure 7-1 shows the generic model, based on the rule definition according to clause 3.1.2 of [ITU-T Y.2770].



Legend:

Φ_{In}	Ingress packet rate
Φ_{Out}	Egress packet rate
A	Action(s) of a (policy) rule
C	Condition(s) of a (policy) rule (determine the packet identifier)
PDU	Protocol data unit ("packet")

Figure 7-1 – Generic model for Rule-oriented packet processing

The generic model uses a dual-stage server, given by the processing of *conditions* and *actions* as principal parts of a rule. Such a separation, for example, provides the indication that all basic requirements of DPI share the common characteristic of *packet identification* (PI).

The generic model may be applied to the DPI requirements (as specified in [ITU-T Y.2770]); see the next clause.

7.3 Major categories of packet policing

The large majority of DPI requirements may be mapped to five high-level categories of packet policing (see Figure 7-2).

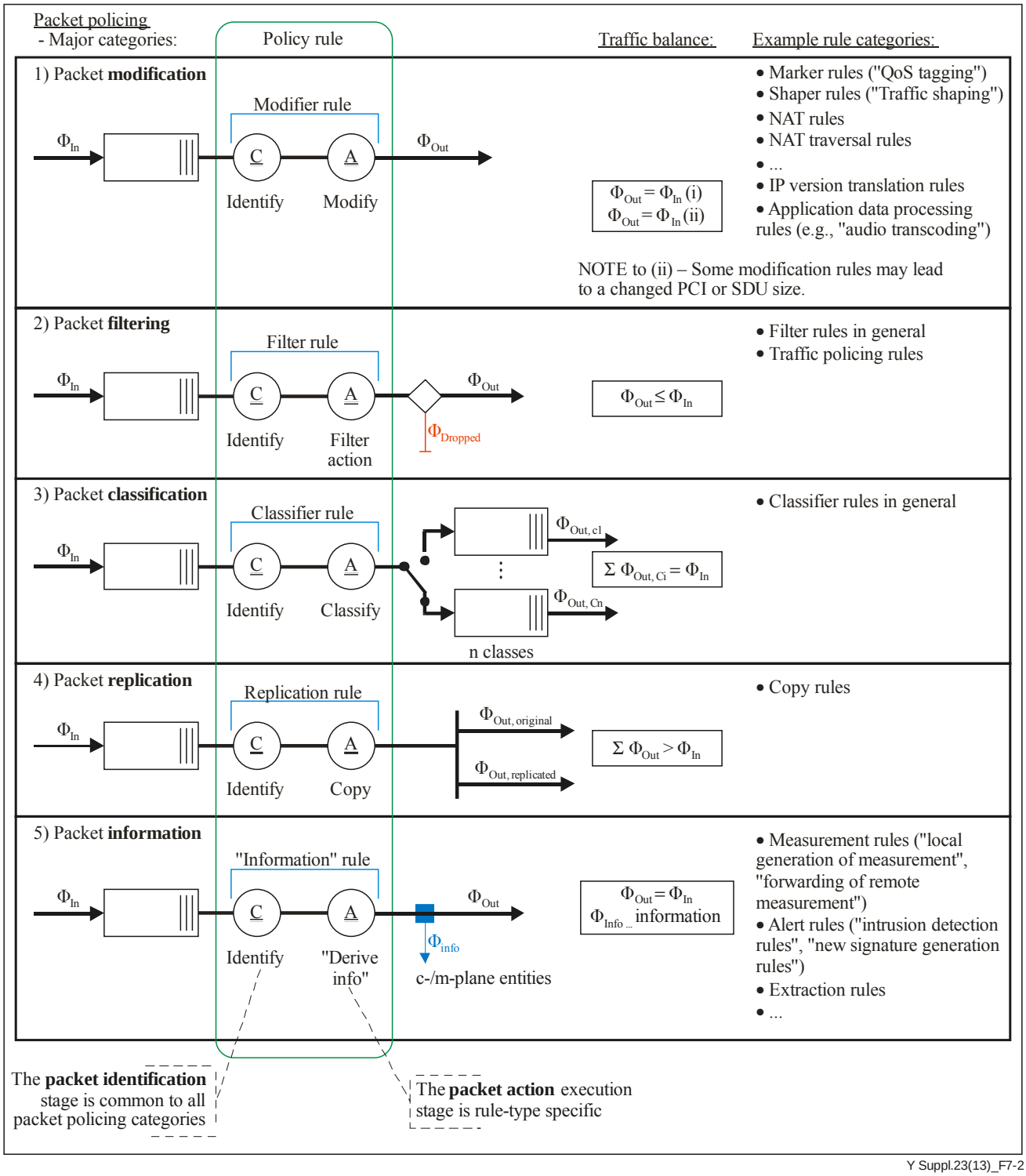


Figure 7-2 – Specific models for the major categories of packet policing

Similarities:

- each particular rule (and category) may be associated with the generic *policy rule* concept (clause 3.1.2 of [ITU-T Y.2770]);

- the *packet identification* stage is common to all rule categories.

Differences:

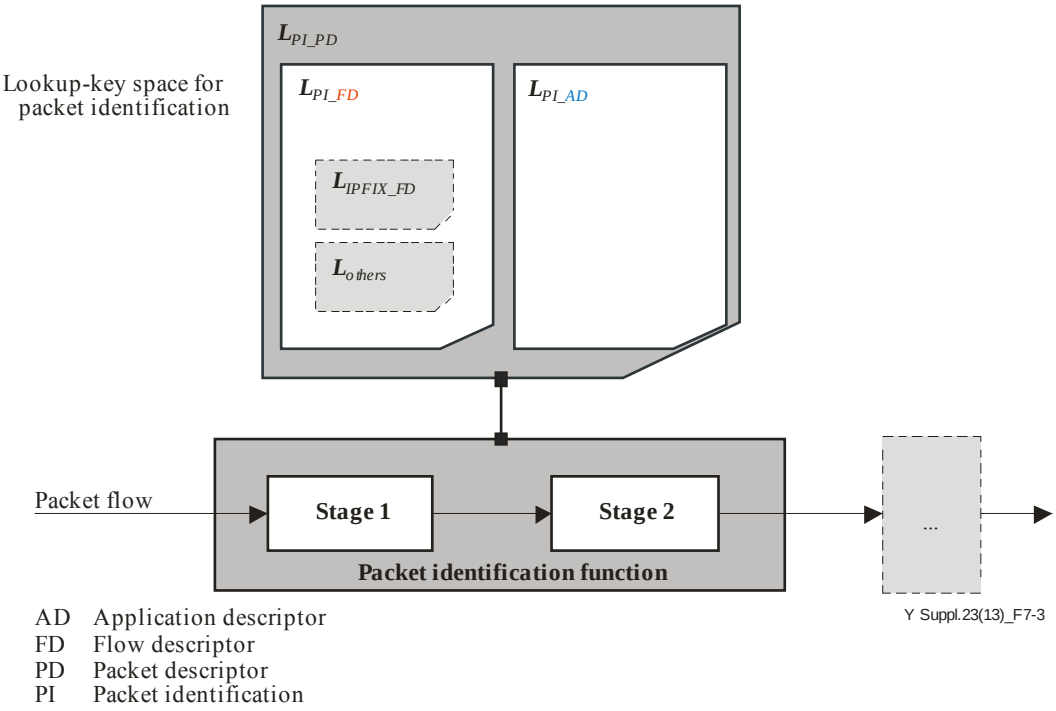
- the particular *action(s)* executed subsequently allow distinguishing different categories (e.g., packet *filtering* vs packet *classification*).

NOTE – It is worth repeating that some DPI requirements from [ITU-T Y.2770] indicate only principal actions, but without any detailed specification (which is beyond the scope of [ITU-T Y.2770]). For example, the generic "filter action" in the above model provides, in reality, a plethora of possible detailed actions (e.g., "silently discard", "discard plus alert", etc.).

It may be concluded that any (deep) *packet inspection* function may be considered as a packet policing function.

7.4 Packet descriptor

Packet identification (PI) is the first function executed (by the DPI functional entity (DPI-FE)) on an incoming packet (see clause 7.3). The identification is based on a lookup-key L_{PI_PD}, see Figure 7-3, which itself contains elements (conditions) for *application identification* (abbreviated as L_{PI_AD}) and optional *flow identification* (abbreviated as L_{PI_FD}).



NOTE 1 – Packet identification may be basically stateful or stateless. The identifiers may consequently contain elements for state information.

NOTE 2 – The identifier spaces of Flow Descriptor (FD) and Application Descriptor (AD) are typically disjoint, but may also overlap in some DPI scenarios.

NOTE 3 – Identification stages 1 and 2 represent the "Application Identification" and "Flow Identification" functions. The "Flow Identification" function is optional. If both identification functions are present, then any order is possible.

Figure 7-3 – Packet identification (as part of packet inspection) process, lookup-key for packet inspection (L_{PI})

The packet descriptor (PD) relates to the lookup-key used by the DPI-FE for identifying an incoming packet. Thus, the PD reflects the view of the DPI-FE as network element. From the network perspective ("end-to-end") there will be application level conditions and (optionally) flow

level conditions provided to the DPI-FE. Both application and flow descriptor spaces are typically disjoint because normally, there is no overlapping between application level conditions and flow level conditions (see Note). Thus, the concept of a packet descriptor may be used in order to structure the descriptor used for DPI:

PD = ***FD*** + ***AD***

FD = ***IPFIX-FD*** + ***Others-FD***

Others-FD = L2, L3 or/and L4 related information elements which are not (yet) in IPFIX registry (e.g., related to SCTP, DCCP)

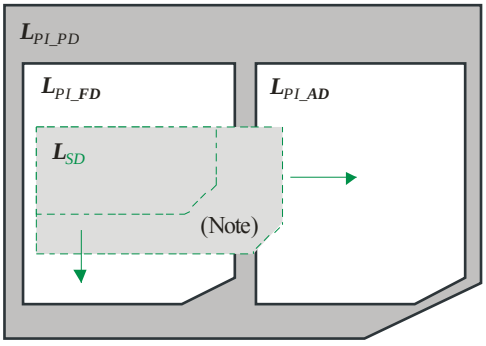
AD = NOT (FD)

It may be noted that the ***Others-FD*** may disappear in the future for the case where the extended IETF IPFIX registry covers all elements required for DPI-based flow identification.

NOTE – Overlapping descriptor spaces are not excluded and are not of concern in practice. Effectively this could mean, for example, the usage of the same *Variable* or even the same *SimpleCondition* in a flow descriptor and an application descriptor (see also clause 6.3).

7.5 Session descriptor

There are DPI requirements on *session identification* in clause 6 of [ITU-T Y.2770]. [ITU-T Y.2770] does not support a single session concept only, but rather a generic view. The correspondent session descriptor (SD) may not always be equated with a particular *FD* or *AD*, because the SD space may overlap both, see Figure 7-4.



NOTE – The lookup-key for session identification is typically based upon at least a flow identifier.

Figure 7-4 – Session descriptor

The SD may be a subset of the applied PD for a particular DPI service:

$$SD \subset PD$$

Example:

There might be an *audio session* within a multimedia IP call (e.g., peer-to-peer service). The audio session is allowed to use multiple, specific media formats (i.e., audio encodings). There may be a DPI policy rule for checking specific media encodings.

There may be the following conditions for the correspondent descriptors:

– *FD* = elements for identifying the end-to-end UDP transport connection

– *AD* = elements for RTP source identification (e.g., RTP SSRC) and a black or white list for media formats (e.g., RTP payload type identifiers)

– *SD* = FD plus RTP SSRC plus identifiers for allowed audio formats.

7.6 Terminology on identification, classification and filtering of packets, flows and traffic

[ITU-T Y.2770] uses terms related to operations executed on packets, but also higher-level traffic aggregates like flows, etc., in the scope of DPI functions. Such functions may be categorized as illustrated in this clause. Figure 7-5 provides a summary and the relationships between these terms. The terms identification, classification, filtering and others are sometimes used in a synonymous manner in [ITU-T Y.2770], due mainly to its more high-level consideration requirements.

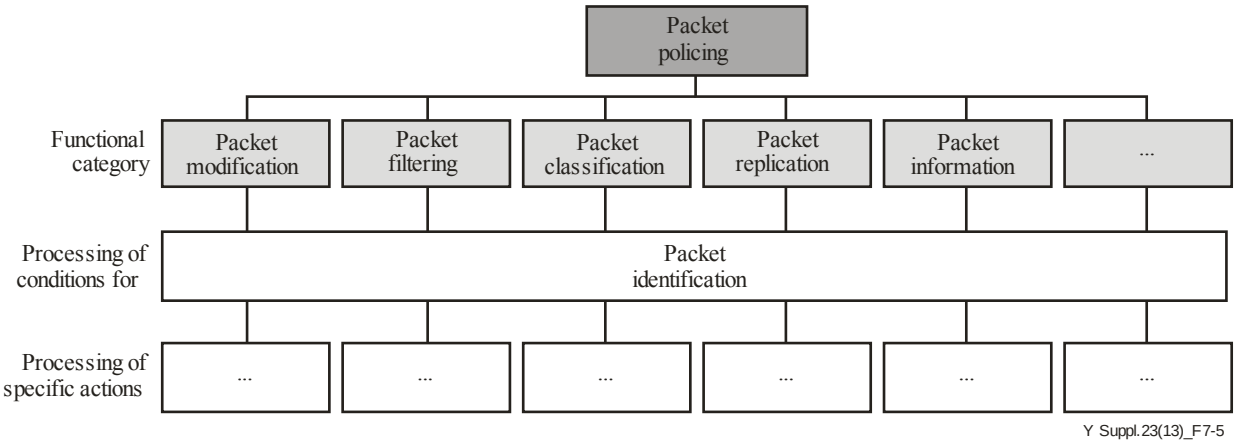
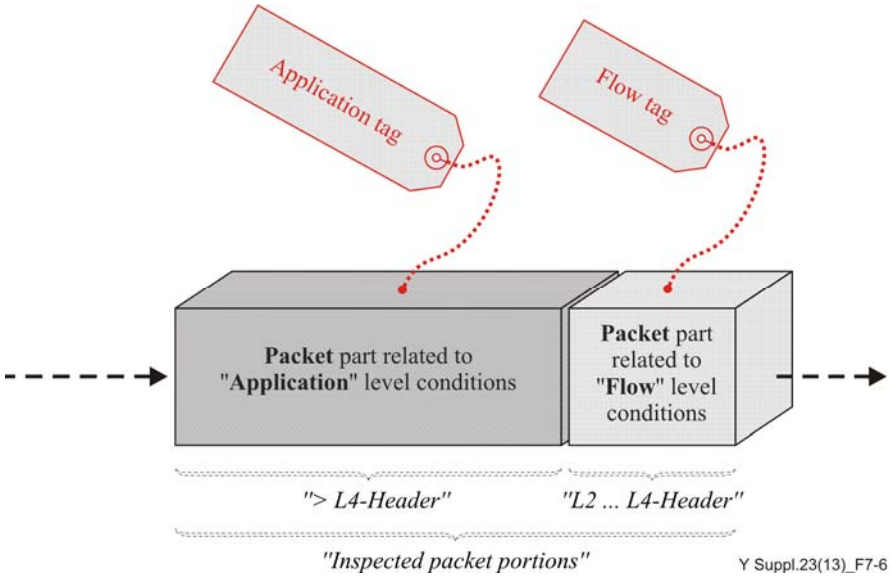


Figure 7-5 – Terminology overview related to packet policing

7.7 Application and flow tag

The DPI requirements sections of [ITU-T Y.2770] (e.g., clause 6 of [ITU-T Y.2770]) refer to the principles of *application identification* and *flow identification*. There are correlated naming, identifier and description principles which may be abstracted by correspondent *tags*, see Figure 7-6.



NOTE – This is an example only. This example uses an absolute protocol layering model such as OSI-BSM. The boundary between application and flow information may vary in other examples.

Figure 7-6 – Principal terms related to application identification and flow identification

Any successfully inspected packet could be "identified", at least by the mandatory "application tag". The optional "flow tag" leads to the discrimination of the two DPI modes of flow-dependent and flow-independent DPI (see Figure 7-7).

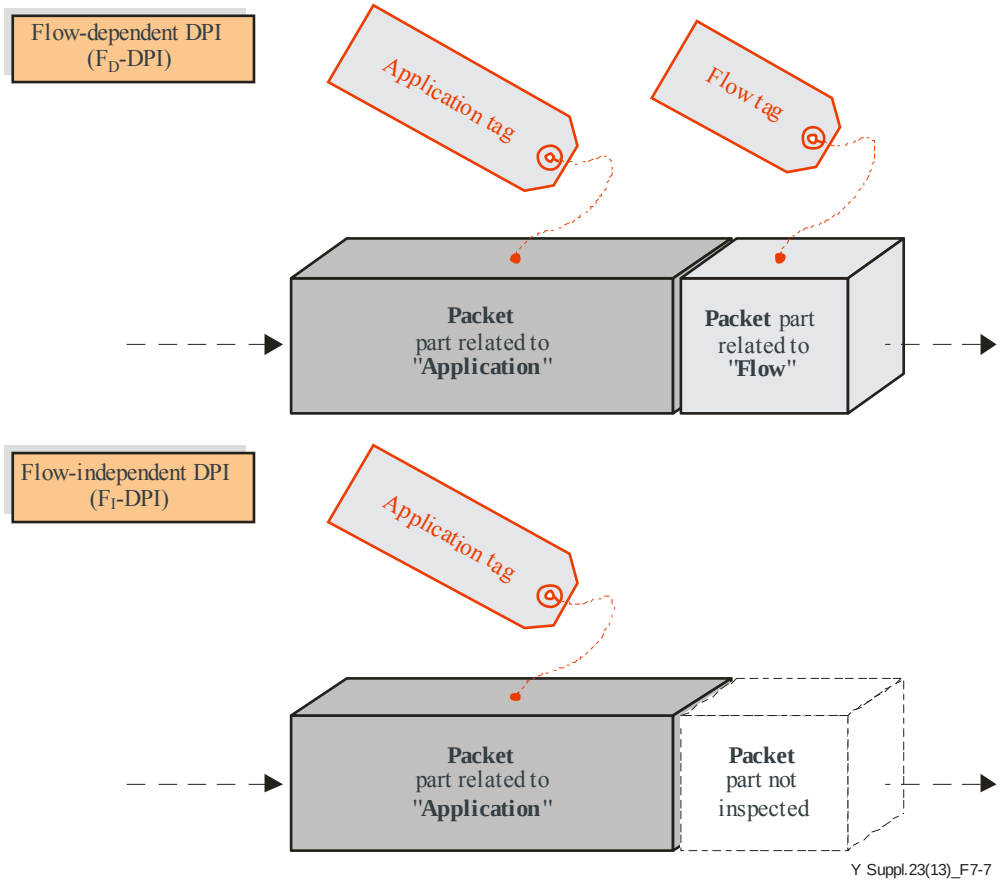


Figure 7-7 – Principal terms related to application identification and optional flow identification

Recommendation [ITU-T Y.2770] provides information about the application tag, but a detailed concept about flow tags has not yet been studied.

8 DPI in layered protocol architectures

8.1 DPI versus non-DPI

The elements for DPI may be subject to policy conditions, given by an overall policy rule concept for defining the functional behaviour of a DPI entity; see the example in Figure 8-1. It should be noted that DPI is applicable for all types of layered protocol architectures.

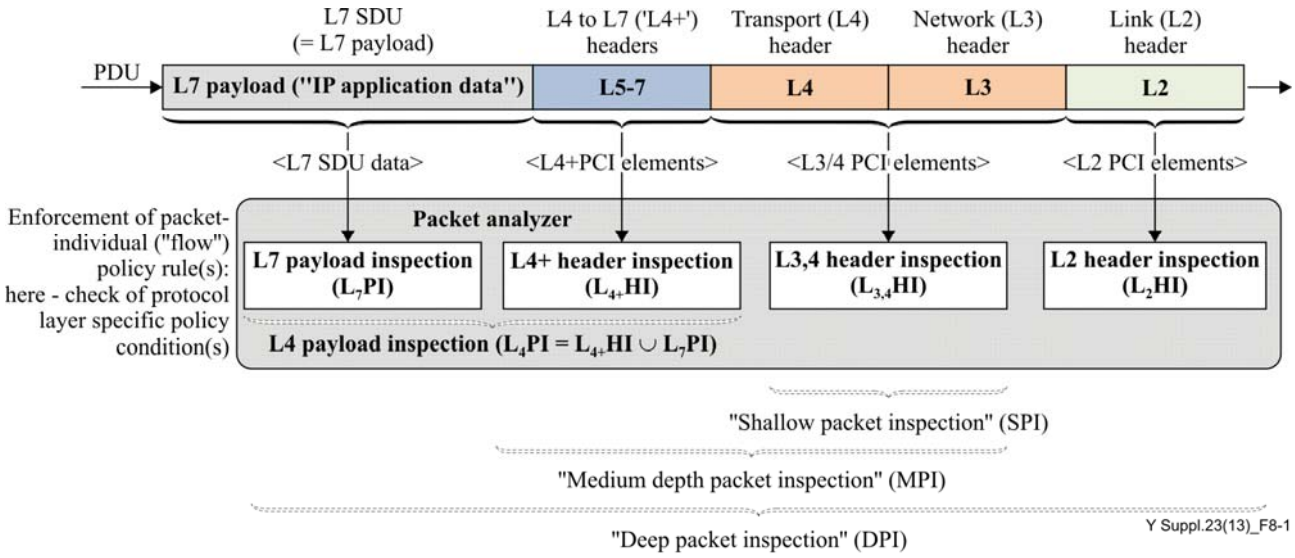
NOTE 1 – The information elements used by these identifiers are tied to a layered protocol architecture; see clause 3.2.16 of [ITU-T Y.2770] for flow level conditions. This concept allows the differentiation of DPI from non-DPI (see the example in Note 2).

NOTE 2 – Non-standard terms, often used in literature:

"Shallow Packet Inspection" (SPI) = $L_{3,4}HI$

"Medium Depth Packet Inspection" (MPI) = $L_{3,4}HI \cup L_{4+}HI$

"Deep Packet Inspection" (DPI) = $L_2HI \cup L_{3,4}HI \cup L_{4+}HI \cup L_7PI = L_2HI \cup L_{3,4}HI \cup L_4PI$



Legend:

LX	Protocol layer X
SDU	Service data unit ("packet payload")
PCI	Protocol control information ("packet header")
PDU	Protocol data unit ("packet")

Figure 8-1 – Packet inspection – illustration of terminology

8.2 Example reference models for some layered protocol architectures

8.2.1 DPI for packets according to IETF-BRM protocol layering

The generic DPI definition of clause 3.1.3 (which is identical to clause 3.2.5 of [ITU-T Y.2770]) may be adapted for network scenarios with concrete protocol layering models. Here, using the example of IETF IP network models, such a DPI service could be then qualified as $DPI_{IETF\text{-}BRM}$ (see definition in clause 3.2.1).

The IP protocol stacks in use may consider a refined reference model by, for example, including additional protocol layers between the application and transport layer. The application level framing protocol RTP in case of RTP traffic would be one such example (see Figure 8-2).

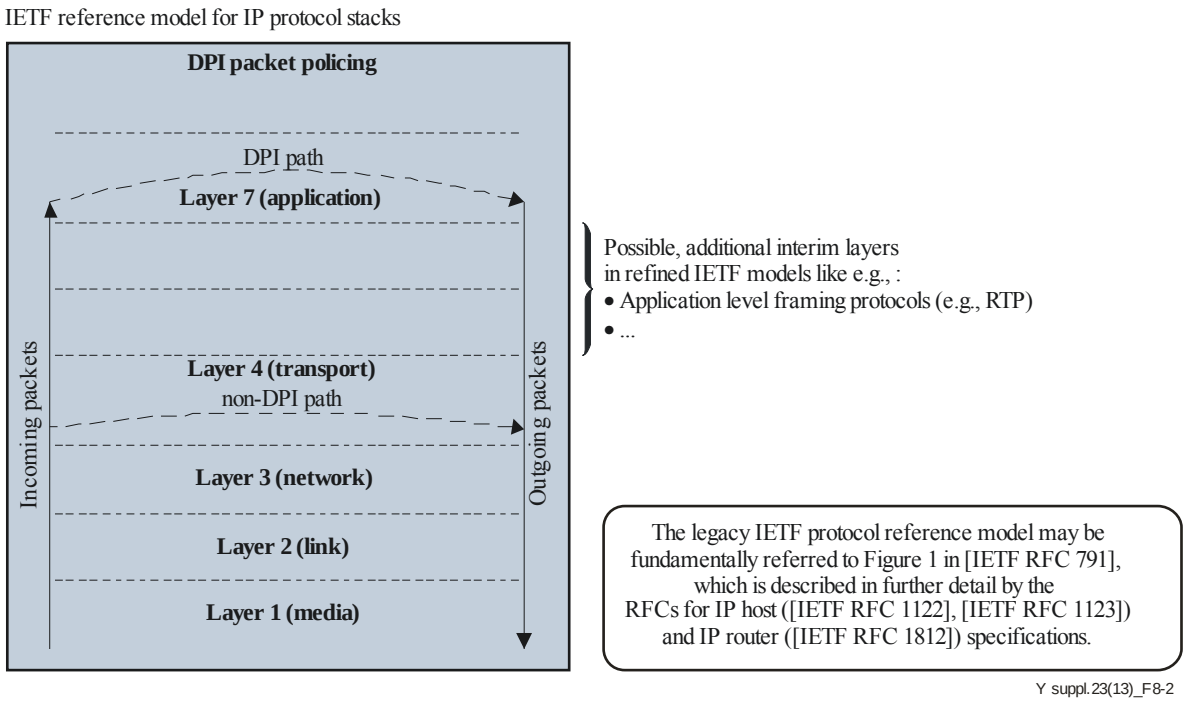


Figure 8-2 – IETF (basic and extended) reference model for IP

8.2.2 DPI for packets according to other IETF reference models

The reference model for IETF IP networks, shown in Figure 8-2, may be further refined. When considering current IP networks in pre-NGN and NGN solutions, more detailed protocol stack architectures are often found (e.g., access network type specific stacks, tunnelling methods, IPv4-to-IPv6 network transitioning scenarios or application specific framing and sub-layering). However, the vast majority of such heterogeneous IP stacks could be mapped to three example reference models: *basic*, *extended* and *tunnelled* reference model (i.e., BRM, ERM, TRM), see Figure 8-3.

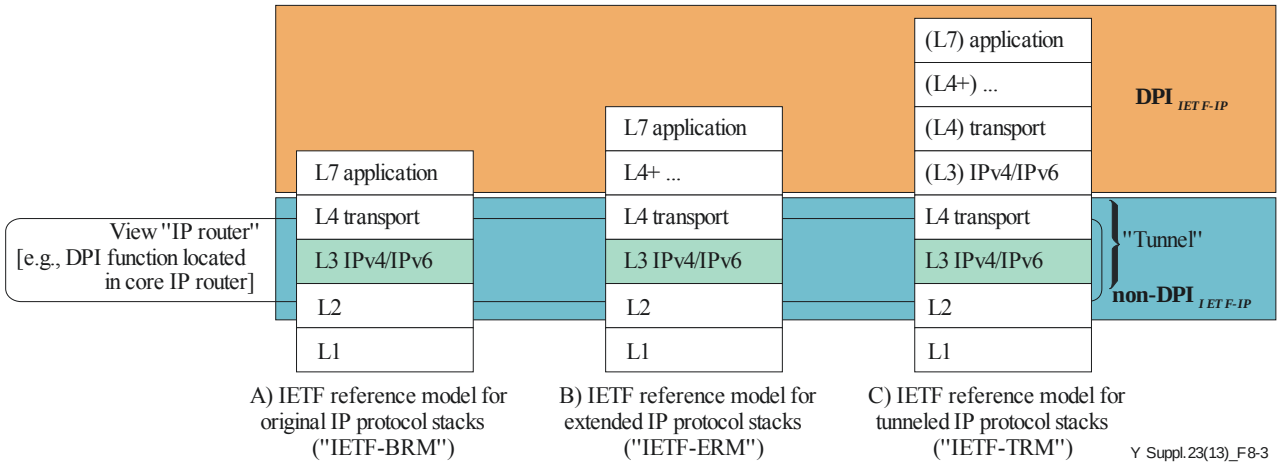


Figure 8-3 – DPI examples for packets according to other IETF reference models

It may be concluded then that the above definition for $DPI_{IETF\text{-}BRM}$ would still be valid for the other reference models, from the perspective of an IP hop entity (see Note).

NOTE – Whether a packet inspection is considered "deep" or not is thus dependent on the *location* of the DPI-FE. For example, the above distinction between DPI and non-DPI could be different for the case where a DPI-FE is integrated in an IP node that terminates a tunnelling protocol.

Bibliography

[b-ITU-T Y.2121] Recommendation ITU-T Y.2121 (2008), *Requirements for the support of flow-state-aware transport technology in NGN*.

[b-IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014