International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2770

(11/2012)

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

Next Generation Networks – Security

Requirements for deep packet inspection in next generation networks

Recommendation ITU-T Y.2770

International Telecommunication Union

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
Numbering, naming and addressing	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.2770

Requirements for deep packet inspection in next generation networks

Summary

Recommendation ITU-T Y.2770 specifies the requirements for deep packet inspection (DPI) in next generation networks (NGNs). This Recommendation primarily specifies the requirements for deep packet inspection (DPI) entities in NGNs, addressing, in particular, aspects such as application identification, flow identification, inspected traffic types, signature management, reporting to the network management system (NMS) and interaction with the policy decision functional entity. Although aimed at the NGN, the requirements may be applicable to other types of networks.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2770	2012-11-20	13

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/.

Table of Contents

		Page
1	Scope	1
1.1	Applicability	1
1.2	Policy rules	2
2	References	3
3	Definitions	3
3.1	Terms defined elsewhere	3
3.2	Terms defined in this Recommendation	4
4	Abbreviations and acronyms	7
5	Conventions	8
6	DPI functional entity requirements	8
6.1	Flow and application identification	8
6.2	DPI signature management	9
6.3	Traffic inspection aspects	11
6.4	Reporting capability	14
6.5	Interaction with a policy decision function	16
6.6	Traffic control	16
6.7	Session identification	16
6.8	Inspection of encrypted traffic	17
6.9	Inspection of compressed traffic	18
6.10	Detection of abnormal traffic	19
7	Functional requirements from the network viewpoint	19
7.1	General requirements	19
7.2	Data plane, control plane and management plane in DPI node	20
8	Interfaces of the DPI-functional entity	21
8.1	External DPI-FE interfaces	22
8.2	Internal DPI-FE interfaces	22
8.3	Interface requirements	23
9	Security considerations and requirements	23
9.1	Security threats against DPI entities	23
9.2	Security requirements for DPI entities	24
Annex A – Specification of a flow descriptor		25
A.1	Protocol syntactical perspective	25
A.2	Specifying information element values	25
A.3	Relation between flow descriptor, IPFIX flow identifier and IPFIX flow key	26
Bibliography		28

Recommendation ITU-T Y.2770

Requirements for deep packet inspection in next generation networks

1 Scope

This Recommendation primarily specifies the requirements for deep packet inspection (DPI) entities in NGN, addressing in particular, aspects such as application identification, flow identification, inspected traffic types, signature management, reporting to the network management system (NMS) and interaction with the policy decision functional entity.

This Recommendation also identifies the requirements for DPI of traffic in non-native encoding formats (e.g., encrypted traffic, compressed data, and transcoded information).

Any DPI function may be generally described by the concept of policy rules (see clause 1.2).

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

This Recommendation does not address the specific impact of implementing a distributed DPI functionality. The requirements are primarily about functional aspects of DPI, but physical aspects are also covered. In the context of functional to physical mapping scenarios, only 1-to-1 mapping and N-to-1 mapping between a DPI-FE and a DPI-PE is within the scope of this Recommendation. In other words, no requirements cover distributed DPI-PEs.

1.1 Applicability

This Recommendation is applicable to the scenarios identified in Figure 1-1:

		Packet-based network type	
		NGN	non-NGN
Packet bearer technology	IP	Applicable	Possibly applicable
	non-IP	Possibly applicable	Possibly applicable

Y.2770(12)_F1-1

Figure 1-1 – Applicability of this Recommendation

The notion of "non-IP" refers to protocol stacks for packet bearer types without any IP protocol layer ([IETF RFC 791] and [IETF RFC 2460]).

Though this Recommendation mainly addresses the requirements of DPI for NGN, these requirements may be applicable to other types of networks. This further applicability is for further study.

1.2 Policy rules

This Recommendation assumes a generic high-level format for all policy rules. This high-level format applies to DPI rules as shown in Figure 1-2. The format distinguishes three basic blocks of:

i) rule identifier/name (with ranking/order indication due to possible multiple rules);

ii) DPI signature/conditions;

iii) actions.

There is a logical binding between action(s) and condition(s), see clause 3.1.2.

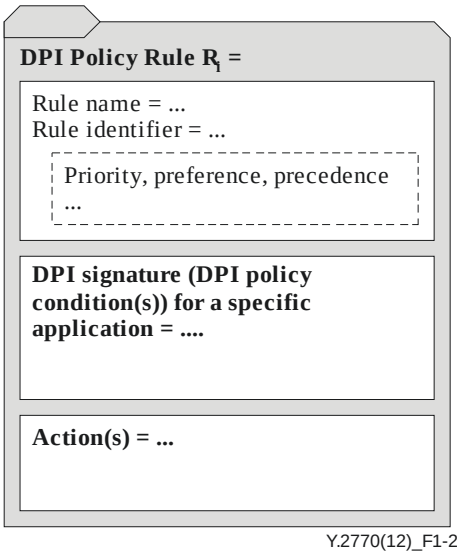


Figure 1-2 – Generic format of DPI policy rules

Note that the following aspects are within the scope of this Recommendation:

- the specification of requirements related to the DPI signature, (i.e., the DPI signatures used for application identification and flow identification);
- the specification of requirements related to the identification and naming of DPI policy rules; and
- the identification of possible scenarios involving policy actions as potential follow-up activities after the evaluation of DPI signatures.

In contrast, the following aspects are outside the scope of this Recommendation:

- the specification of requirements related to actions concerning the modification of inspected packet(s);
- the specification of explicit bindings between actions and conditions (Note);
- the specification of DPI policy rules in full;
- the specification of a language for DPI signatures; and
- the specifications of concrete DPI policy conditions (such as behavioural or statistical functions).

NOTE – For instance, there might be a specification for the action of discarding a packet, and the condition of searching for a packet signature, but there will *not* be any specification that associates an individual action to an actual condition.

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.107] Recommendation ITU-T E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS*.

[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 X.731] Recommendation ITU-T X.731 (1992) | ISO/IEC 10164-2:1993, *Information technology – Open Systems Interconnection – Systems management: State management function.*

[ITU-T Y.1221] Recommendation ITU-T X.1221 (2010), *Traffic control and congestion control in IP based networks*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in next generation networks*.

[ITU-T Y.2205] Recommendation ITU-T Y. 2205 (2011), *Next Generation Networks – Emergency telecommunications – Technical considerations*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.

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

[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 filter [b-IETF RFC 3198]: A set of terms and/or criteria used for the purpose of separating or categorizing. This is accomplished via single- or multi-field matching of traffic header and/or payload data. "Filters" are often manipulated and used in network operation and policy. For example, packet filters specify the criteria for matching a pattern (for example, IP or 802 criteria) to distinguish separable classes of traffic.

NOTE – In this Recommendation, the term "traffic header" is equivalent to "packet header".

3.1.2 filter/policy rule [b-IETF RFC 3198]: A basic building block of a policy-based system. It is the binding of a set of actions to a set of conditions, where the conditions are evaluated to determine whether the actions are performed.

NOTE – In this Recommendation, a filter rule is a specific policy rule with the purpose of separating traffic, e.g., in the main categories of "accepted" and "not-accepted".

3.1.3 flow [IETF RFC 5101]: A set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties. Each property is defined as the result of applying a function to the values of:

1) One or more packet header fields (e.g., destination IP address), transport header fields (e.g., destination port number), or application header fields (e.g., RTP header fields [b-IETF RFC 3550]).
2) One or more characteristics of the packet itself (e.g., number of MPLS labels, etc.).
3) One or more of fields derived from packet treatment (e.g., next hop IP address, the output interface).

A packet is defined as belonging to a flow if it completely satisfies all the defined properties of the flow.

This definition covers the range from a flow containing all packets observed at a network interface to a flow consisting of just a single packet between two applications. It includes packets selected by a sampling mechanism.

NOTE – The above numbered listed items indicate flow properties in the categories of (1) "Protocol Control Information (PCI) of packets", (2) "Protocol Data Unit (PDU) properties of packets" and (3) "Local packet forwarding information".

3.1.4 policy [b-IETF RFC 3198]: A set of rules to administer, manage, and control access to network resources.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 application: 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), as a common characteristic of all the above listed levels of applications.

3.2.2 application-descriptor (also known as application-level conditions): A set of rule conditions that identify the application (according to clause 3.2.1).

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.

3.2.3 application tag: A unique name for an application which is used to indicate the application semantics and is typically used for reporting scenarios.

Figure 3-1 outlines the relationship between the application tag and application descriptor.

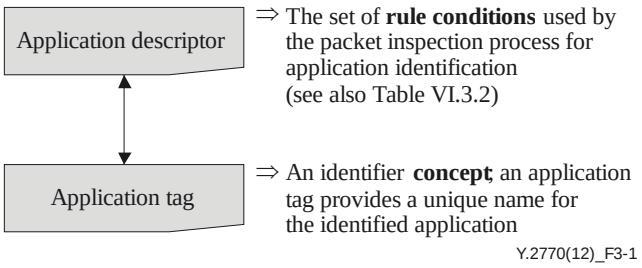


Figure 3-1 – Relationship between the application tag and application descriptor

3.2.4 bidirectional DPI: DPI that involves policy conditions concerning both traffic directions.

NOTE –There is at least one simple condition per traffic direction in the case of bidirectional DPI.

3.2.5 deep packet inspection (DPI): 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) 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.

3.2.6 DPI engine: 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).

3.2.7 DPI entity: The DPI entity is either the DPI functional entity or the DPI physical entity.

3.2.8 DPI functional entity (DPI-FE): A functional entity that performs deep packet inspection.

3.2.9 DPI physical entity (DPI-PE): The implemented instance of a DPI functional entity.

3.2.10 DPI policy: A policy as defined, for example in [b-IETF RFC 3198] (see clause 3.1.4), enforced in a DPI entity.

3.2.11 DPI policy condition (also known as DPI signature): 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.

3.2.12 DPI policy decision functional entity (DPI-PDFE): 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.

3.2.13 DPI policy rule: The policy rule pertinent to DPI (See also clause 3.1.2). In this Recommendation, a DPI policy rule is referred to simply as a rule.

3.2.14 DPI signature: A synonym to DPI policy condition(s) (see clause 3.2.11).

3.2.15 DPI signature library: A database consisting of a set of DPI signatures. It is also called a DPI protocol library because the signatures may be typically used for protocol identification.

3.2.16 flow descriptor (also known as flow level conditions): A set of rule conditions that is used to identify a specific type of flow (according to clause 3.1.3) 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.

NOTE 2 – For further normative discussion of the flow descriptor as used in this Recommendation, see Annex A.

3.2.17 IPFIX flow identifier (IPFIX flow ID): The set of values for the IPFIX flow keys, which is used in conjunction with the flow descriptor to identify a specific flow.

3.2.18 IPFIX flow key: Each of the information elements of the flow descriptor that is used in IPFIX-based flow identification processes (according to [IETF RFC 5101]).

NOTE – The IPFIX flow key definition is semantically consistent with the flow key definition specified in IPFIX [IETF RFC 5101]. The only difference between the two terms is that the definition in this document is scoped to the flow descriptor.

3.2.19 L3,4 header inspection ($L_{3,4}$HI): Processing of policy rule(s) with policy conditions involving only the protocol control information (PCI) elements of the network layer or/and transport layer.

3.2.20 L4+ header inspection (L_{4+}HI): Processing of policy rule(s) with policy conditions involving only the PCI elements above the transport layer.

3.2.21 L4 payload inspection (L_4PI): Processing of policy rule(s) with policy conditions involving only the transport payload which may be the "application data" for particular application protocols (e.g., SIP).

NOTE – L_4PI relates to the union of L_{4+}HI and L_7PI policy conditions.

3.2.22 L7 payload inspection (L_7PI): Processing of policy rule(s) with policy conditions based on the application data.

3.2.23 payload: The data unit following the header elements in a packet, and excluding optional elements at the end of a packet (e.g., padding, trailer, checksum elements).

NOTE 1 – Thus, the notion of payload is synonymous with the service data unit (SDU) in the OSI-BRM [ITU-T X.200], the packet is synonymous with the protocol data unit (PDU), and the protocol control information (PCI) covers all packet header and trailer elements. In summary, "PDU = PCI + SDU".

NOTE 2 – The notion of payload is specific to a particular protocol layer (i.e., Lx-Payload refers to the payload at protocol layer x). Ditto for Lx-SDU, Lx-PDU and Lx-PCI.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AH	Authentication Header
BRM	Basic Reference Model
DCCP	Datagram Congestion Control Protocol
DPI	Deep Packet Inspection
DPI-FE	DPI Functional Entity
DPI-PDFE	DPI Policy Decision Functional Entity
DPI-PE	DPI Physical Entity
DPI-PIB	DPI Policy Information Base
ESP	Encapsulating Security Payload
ET	Emergency Telecommunications
FPA	Full Payload area Analysis
FSL	Filter Specification Language
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IE	Information Elements
IP	Internet Protocol
IPFIX	IP Flow Information Export
IS	In-Service
L-PDF	Local PDF
MPLS	Multi-Protocol Label Switching
NGN	Next Generation Network
NMS	Network Management System
OGP	Open Game Protocol
OoS	Out-of-Service
OSI-BRM	Open Systems Interconnection – Basic Reference Model
P2P	Peer to Peer
PCC	Policy and Charging Control
PCI	Protocol Control Information
PDF	Policy Decision Function
PDU	Protocol Data Unit
PEL	Policy Expression Language
PFF	Packet Forwarding Function
PIB	Policy Information Base
PPA	Payload area Analysis
PSAMP	Packet Sampling

PSL	Policy Specification Language
RACF	Resource and Admission Control Functions
RACS	Resource and Admission Control Subsystem
R-PDF	Remote PDF (i.e., PDF remotely located from DPI node perspective)
RTP	Real-time Transport Protocol
SA	Security Association (IPsec)
SCTP	Stream Control Transmission Protocol
SDU	Service Data Unit
SigComp	Signalling Compression
SIP	Session Initiation Protocol
SPI	Security Parameter Index (IPsec)
TCP	Transmission Control Protocol
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
UDP	User Datagram Protocol

5 Conventions

This document provides a list of items, labelled as *R-x/y*, where *x* refers to the clause number and *y* a number within that clause. Such items use the following keywords with meanings as prescribed below:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 DPI functional entity requirements

6.1 Flow and application identification

R-6.1/1: The DPI functional entity is required to perform application identification.

R-6.1/2: The DPI functional entity is required to support various kinds of DPI policy rules.

R-6.1/3: The DPI-FE is required to identify an application by inspecting the application payload.

R-6.1/4: The DPI application level conditions (and optional flow level conditions) are required to allow application identification based on unidirectional traffic (unidirectional DPI) for all unidirectional applications and for bidirectional applications under the condition that one traffic direction allows an unambiguous identification.

R-6.1/5: The DPI application level conditions and (optional flow level conditions) can optionally allow application identification based on bidirectional traffic (bidirectional DPI).

R-6.1/6: The information element(s) used in the flow level conditions are recommended to comply with [b-IETF RFC 5102]**,** as registered with IANA [b-IETF IANA IPFIX]. In such a case IEs are recommended to include IPFIX information elements related to the link (L2), network (L3) and transport (L4) protocol layers, following the basic IETF layered protocol architecture.

NOTE – The IANA registry for IPFIX information elements can optionally be augmented to include additional elements (by the IETF). The present IANA registry (as of the end of year 2011) is missing information elements for L4 protocols other than UDP and TCP (e.g., for SCTP and DCCP).

R-6.1/7: The information element(s) can optionally be other L2, L3 or L4 related information elements outside the IPFIX registry (called enterprise specific information elements in the IPFIX protocol [IETF RFC 5101]).

6.2 DPI signature management

This clause defines the requirements concerning operations on the DPI signature library. Such operations may be locally initiated by the DPI-FE, or by a remote network entity (see Figure 6-1). All possible types of remote network entities may be abstracted as the DPI policy decision functional entity that decides the signature-based rules to be enforced in the DPI-FE.

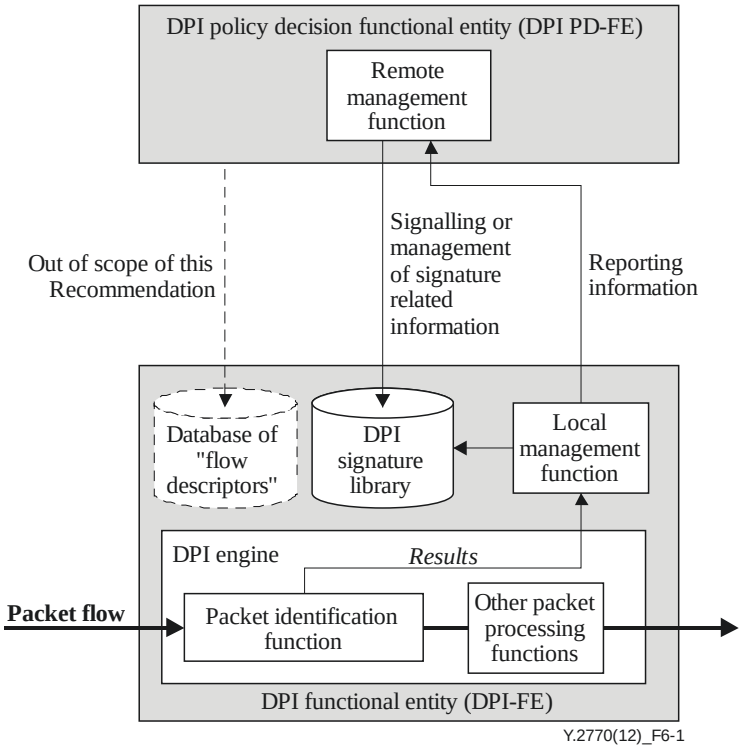


Figure 6-1 – DPI signature management within the scope of an example DPI functional entity architecture (see also Figure 8-2 with regards to the internal interfaces)

The DPI policy decision functional entity would be associated with the RACF (in case of an NGN with an RACF), but its specification is out of scope for this Recommendation. It is included in Figure 6-1 because it contains the remote management functions for the DPI-FE.

6.2.1 General signature requirements

R-6.2.1/1: DPI signatures are required to be stored in the *DPI signature library* which is a sub-entity of the DPI-FE.

NOTE – The rationale behind a local DPI signature library is the fact that the packet identification function requires immediate access on the database content.

The DPI signature may be used for:

- approximate identification (e.g., behavioural, heuristics, etc.); and
- exact identification (e.g., exact matching rules).

The language (formal or behavioural) used for specifying DPI policy rules in this library, as well as the matching rules themselves, are outside the scope of this Recommendation. This Recommendation only specifies that the DPI signature library exists, what a DPI signature (s) is/are, and the library management functions.

R-6.2.1/2: The DPI signature library is required to be securely maintained and not visible to unauthorized users.

6.2.2 Management of DPI signature library

This clause defines the requirements for management of the DPI signature library.

6.2.2.1 Adding new signatures

R-6.2.2.1/1: It is required to be able to add new DPI signatures to the DPI signature library.

6.2.2.2 Operations on existing signatures

R-6.2.2.2/1: It is required to be able to modify (update) existing signatures in the DPI signature library.

R-6.2.2.2/2: It is required to be able to enable and disable specific DPI signatures in the DPI signature library.

R-6.2.2.2/3: It is required to be able to delete (remove) specific DPI signatures in the DPI signature library.

6.2.2.3 The rule format exchanged through external interfaces

R-6.2.2.3/1: The DPI signature for application identification exchanged through external interfaces (i.e., *e1* and *e2* in Figure 8-1) can optionally follow any rule format (see also clause 1.2).

6.2.3 Location of management function

R-6.2.3/1: The DPI signature management actions specified in clause 6.2.2 are required to be performed locally from the DPI functional entity or remotely or both (see Figure 6-1).

6.2.4 Initiation of management actions

R-6.2.4/1: It is required to support the push mode regarding DPI signature operations, when the operations are remotely initiated (e.g., by the DPI-PDFE in Figure 6-1).

R-6.2.4/2: It is required to support the pull mode regarding the DPI signature operations, when the operations are locally initiated by the DPI-FE. The notion of pull means that the DPI-FE local management function requests the DPI-PDFE to perform a management action on a new or existing signature.

How a DPI-FE initiates a request is out of the scope of this Recommendation.

6.3 Traffic inspection aspects

This clause addresses the aspects concerning the types of traffic subject to DPI.

6.3.1 Flow identification aspects

R-6.3.1/1: The DPI functional entity is recommended to support the identification of applications, without a flow level inspection.

R-6.3.1/2: Any DPI scenario can optionally be initially flow-independent, i.e., the provided DPI policy rule to the DPI-FE would not contain a flow descriptor. However, the rule could request to collect interested flow information.

R-6.3.1/3: Such a request is required to provide an IPFIX flow key plus the optional completion of lacking flow information.

R-6.3.1/4: The DPI functional entity can optionally require a complete recognition of an IPFIX flow identifier based on a given IPFIX flow key and the inspection of multiple subsequent packets.

R-6.3.1/5: The reporting action of a complete or incomplete IPFIX flow identifier by the DPI-FE to a remote network entity can optionally be conditional (e.g., event-driven, timer-controlled, etc.).

6.3.2 Protocol-stack aware and protocol-stack agnostic DPI aspects

The DPI identification function (within a DPI-FE) is responsible for application identification and concerns the compare and search operations, based on the DPI signature, against an incoming packet (PDU). There are two options: the DPI-FE is either aware of the internal PDU structure (i.e., "protocol stack aware DPI-FE") or unaware of the structure ("protocol stack agnostic *DPI-FE*").

Both options may provide the same identification result and be functionally equivalent. The main difference is that the protocol stack aware identification logic may be more efficient.

It is useful to distinguish the following two types of analysis regarding operational efficiency (i.e., application identification and optional flow identification):

a) Predetermined payload area analysis (PPA): When packets (flow) correspond to a known application with a clearly defined payload structure, the DPI-FE may inspect the fixed predetermined location of the payload (i.e., the protocol-stack aware packet inspection mode).

b) Full payload area analysis (FPA): When packets (flow) do not correspond to a known application or the structure of the application payload is not clearly defined or known, the DPI-FE inspects the "entire payload area" (i.e., the protocol-stack agnostic packet inspection mode).

Both PPA and FPA can be applied to the same traffic flow.

R-6.3.2/1: The DPI-FE is recommended to support protocol stack aware application identification.

R-6.3.2/2: The DPI-FE is recommended to support protocol stack agnostic application identification.

R-6.3.2/3: The DPI-FE is required to identify applications running on IPv4 and IPv6 protocol stacks and can optionally identify applications running on other underlying protocol stacks.

R-6.3.2/4: The DPI-FE is recommended to identify applications in nested traffic, such as encapsulated or tunnelled traffic.

6.3.3 Aspects of DPI policy rule actions

6.3.3.1 Background

DPI policy actions may be performed on different hierarchical levels, e.g., DPI-FE, local and remote PDFs, and may include for instance the following:

1) Packet path level actions (by the DPI-FE):
   a) accept the packet and forward it to the packet forwarding function (PFF) (a conditional action for the "In-Path DPI" mode only);
   b) discard the packet (silently or otherwise);
   c) redirect the packet to other output interfaces;
   d) replicate/mirror the packet to other output interfaces;
   e) traffic classification, local measurements, and reporting of measurement data;
   f) prioritization, blocking, shaping and scheduling methods of individual packets.
2) Node level actions (by involvement of the local policy decision function (L-PDF)):
   a) dynamic building of new DPI policy rules and/or modification of existing rules (stored in the DPI policy information base (DPI-PIB));
   b) generation of logging/tracing data and reporting to policy management (see clause 2.11.2 of [b-IETF RFC 3871]);
   c) detecting and reporting of unidentifiable applications;
   d) notification of intrusion detection systems (e.g., by reporting traffic samples, suspicious packets).
3) Network level actions (via the remote policy decision function (R-PDF)):
   a) Resource management, admission control and high-level filtering (at the level of network subsystems (such as specified for RACF in [ITU-T Y.2111], ETSI TISPAN RACS [b-ETSI ES 282 003] and 3GPP PCC [b-ETSI TS 123 203]);
   b) content charging based on subscribers' application types (e.g., IETF RADIUS or Diameter).

Figure 6-2 further explains the above structuring principle through a detailed generic policy rule format (versus the one introduced in clause 1.2):

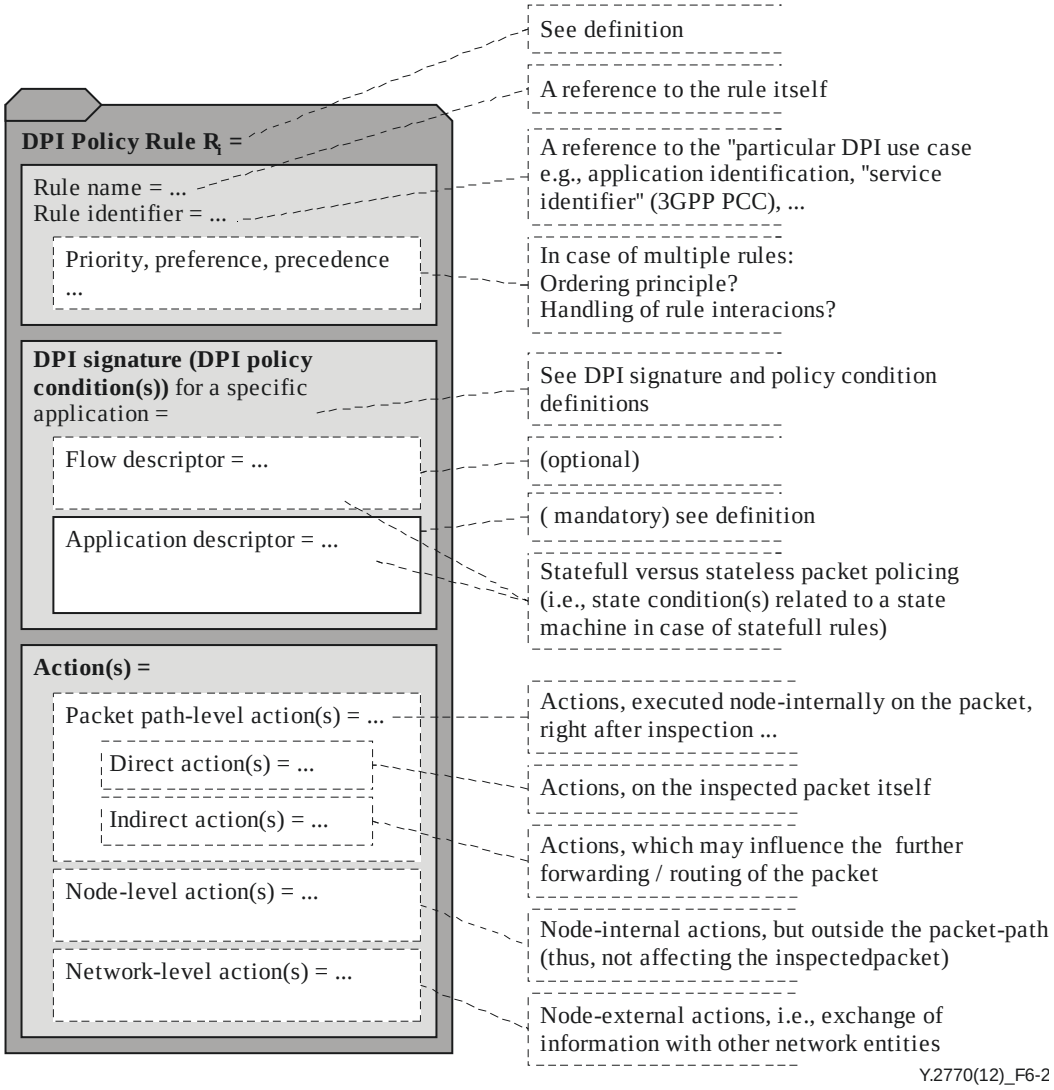


Figure 6-2 – An example of a detailed policy rule format (in comparison with Figure 1-2)

The mapping of specific actions to conditions is out of the scope of this Recommendation.

6.3.3.2 Requirements

R-6.3.3.2/1: Once an application has been identified by the DPI-FE, it can optionally be possible to extract application specific information.

For example, a URL in HTTP, a media format ("codec type") in the real-time transport protocol (RTP), or an RTP session identifier (e.g., SSRC for the RTP source endpoint).

R-6.3.3.2/2: The DPI-FE can optionally be able to work in conjunction with a flow metering function, such as the IPFIX metering process [IETF RFC 5101] and some filtering capabilities, such as [b-IETF RFC 5476].

NOTE – This metering process typically populates the following IPFIX information elements (used as flow keys): sourceIPv6Address and destinationIPv6Address, sourceIPv4Address and destinationIPv4Address, protocolIdentifier, sourceTransportPort, destinationTransportPort, etc. However, it is the DPI-FE's role to populate the application tag and the completion of the IPFIX flow identifier (based on the given IPFIX flow key, see also Figure A.1).

6.4 Reporting capability

Reporting concerns the notification (e.g., due to a particular event detected by the DPI-FE) to another functional entity, which is typically located in a remote network element (in the user, control or management plane). The DPI-FE may provide multiple reporting interfaces in support of the "different types of events".

6.4.1 Reporting to the network management system (NMS)

6.4.1.1 Interface and protocol for reporting

R-6.4.1.1/1: The export protocol is recommended to follow the IPFIX specification [IETF RFC 5101], and can optionally follow IPFIX extensions.

R-6.4.1.1/2: The export protocol can optionally follow the IPFIX specification [b-IETF RFC 5103] in case of bidirectional flows.

R-6.4.1.1/3: It is recommended that the IPFIX based export protocols use the external interface e2 (see Figure 8-1).

6.4.1.2 Reported information

R-6.4.1.2/1: DPI-FE is required to report inspection results (such as the application tag and potentially application specific information elements) along with the flow specific information to the DPI management plane. The locally updated flow key values (including the typical fields from the flow metering function) can optionally be exported to a policy decision function (e.g., PD-FE defined in [ITU-T Y.2111]).

R-6.4.1.2/2: The reported information is recommended to reuse the IPFIX information elements ([b-IETF IANA IPFIX]), which were initially specified in the IPFIX information model [b-IETF RFC 5102].

The flow specific information is specified in the IPFIX information model [b-IETF RFC 5102], for example:

1) Application specific information:
   - application tag; and
   - extracted fields such as RTP media format and RTP SSRC.
2) L3/L4 header fields corresponding to IP addresses, L4 ports (e.g., TCP or UDP, Note 1), and protocol type.
3) Performance information (like metrics, statistics) bytes count, packet count and maximum packet size (Note 2).
4) Time information: flow start time, flow end time.
5) Packet associated information: next hop and packet size (Note 3).

NOTE 1 – Some listed information elements are not (yet) part of the Internet Assigned Numbers Authority (IANA) IPFIX registry, but they are valid in the context of this Recommendation.

NOTE 2 – The flow specific information can be generated by a packet sampling (PSAMP) mechanism, but when exporting such results to the NMS, the application specific information is recommended to be added.

NOTE 3 – New information elements may have to be registered with the IPFIX IANA, according to section 7 "IANA Considerations" of [b-IETF RFC 5102].

6.4.2 Reporting of new, unknown or incorrect applications

6.4.2.1 Characteristics of such traffic

There are subtle differences between these application types. They may be characterized by following specific properties, resulting in different application level conditions for their detection:

– new application: e.g., a new version of an application, a new version of an application specific information element (e.g., a new game version within the open game protocol (OGP)), or a new protocol version; it may be noted that the notion of 'new' reflects the perspective of the DPI service (which may be based on a history of past DPI services);

– unknown application: e.g., an unknown packet type, unknown protocol, unknown "application";

– incorrect application: e.g., a packet carrying incorrect protocol grammar (Note), etc.

NOTE – Incorrect protocol syntax could be exploited for a security attack. Affected protocols are typically the ones which are terminated in user equipment (like signalling protocols).

6.4.2.2 Reporting requirements

R-6.4.2.2/1: The DPI-FE can optionally support reporting new, unknown or incorrect applications upon inspection of the traffic.

6.4.3 Reporting of abnormal traffic

R-6.4.3/1: The DPI-FE can optionally provide a reporting capability related to the detection of abnormal traffic upon detection of such traffic.

Abnormal traffic is defined to be the traffic not associated with normal traffic classes. A normal traffic class is a set of traffic that matches to existing statistical properties of well-defined applications, such as the packet inter-arrival time, arrival order, the size of the PDU of a specific protocol layer, the size of payload, or the traffic volume (at a specific protocol layer).

6.4.4 Reporting of events related to the DPI-PE

This clause describes the events concerning the operational state of the DPI entity and the related reporting requirements.

6.4.4.1 Failure events related to incorrect behaviour of the DPI-PE

The simplest way to depict the management state of the DPI-PE is in terms of two states: "In-Service" (IS) and "Out-of-Service" (OoS).

R-6.4.4.1/1: DPI management is recommended to be based on the state of art (e.g., [ITU-T X.731] and [b-IETF RFC 4268]) and is recommended to support at least the management states of IS and OoS.

R-6.4.4.1/2: Any failure of the DPI-PE, if not architected in a redundant manner, can optionally cause the IS-to-OoS state transition. Such events are recommended to be reported.

6.4.4.2 Events related to fault management of the DPI-PE

A DPI-PE provides network interfaces for ingress and egress traffic. Fault may occur on these interfaces.

R-6.4.4.2/1: The DPI-PE is recommended to support an alarm reporting function such as defined in [b-ITU-T X.734].

6.4.4.3 Events related to logging of the DPI functional entity

R-6.4.4.3/1: The DPI functional entity can optionally support a system logging capability according e.g., Syslog [b-IETF RFC 5424]. In such a case, the DPI functional entity is an originating point of Syslog messages.

It is worth noting that in the case when the inspected packet flow carries logging traffic, the DPI functional entity is neither an originating point nor a terminating point of logging messages. In other words, the lookup-key for such a packet flow may be based on an application descriptor (related to the syslog application layer) and an IPFIX flow descriptor (related to the selected syslog transport mode). Further information can be found in [b-IETF RFC 5424] and [b-IETF RFC 5426].

6.4.4.4 Events related to the load state and resource consumption of the DPI physical entity

A DPI-PE has limited resources for DPI processing. The resource specifics are implementation-dependent and out of the scope of this Recommendation.

R-6.4.4.4/1: The DPI physical entity is recommended to support the reporting of the load level of DPI resource components to the management plane.

For instance, in networks with Emergency Telecommunication traffic (see clause 7.1.1), the DPI process must be able to forward ET traffic through congested network nodes; therefore it is desirable that the network management system be aware of the load level.

6.5 Interaction with a policy decision function

R-6.5/1: DPI-FE can optionally act as a part of the policy enforcement functional entity as defined in [ITU-T Y.2111] and provide the related transport function.

R-6.5/2: The interface between the DPI-FE and RACF can optionally be Rw as defined in [ITU-T Y.2111].

R-6.5/3: The information between DPI-FE and the RACF PD-FE can optionally be exchanged via existing (e.g., the *Rw* interface) or new RACF interfaces depending on the specific DPI use case.

NOTE – In this case, the RACF needs to be enhanced to cover DPI information (e.g., a protocol signature within a DPI policy rule); the RACF as defined in [ITU-T Y.2111] supports primarily flow-identification based policy rules. The specific RACF reference point would be dependent on the specific DPI use case.

6.6 Traffic control

The following high-level requirements may be derived:

R-6.6/1: The DPI functional entity may optionally be involved in network scenarios with the purpose of traffic control (e.g., traffic control functions as defined by [ITU-T Y.1221]). The DPI-FE is recommended to support corresponding traffic control capabilities.

R-6.6/2: The DPI-FE can optionally support traffic control natively. Nevertheless, the detailed functional requirements for traffic control are out of the scope of this Recommendation.

R-6.6/3: The DPI-FE can optionally support interactions with external traffic control functions. The related functional requirements are out of the scope of this Recommendation.

6.7 Session identification

There are many terms related to session in this Recommendation. All traffic of a session can be unambiguously identified by the DPI-FE as the "session descriptor" is either equal to or a subset of the flow and/or application descriptor.

6.7.1 Requirements for session identification

R-6.7.1/1: The DPI-FE is required to be able to analyse session (e.g., RTP session, HTTP session, IM session, VoIP SIP session) behaviour.

R-6.7.1/2: The DPI-FE is required to be able to track session state.

6.7.2 DPI actions at 'session level'

R-6.7.2/1: The DPI-FE can optionally extract or generate measurement data at the session level (e.g., for monitoring performance metrics concerning a subscriber's quality of experience.

6.8 Inspection of encrypted traffic

There is a common view that DPI signatures can be applied only to unencrypted traffic. Nevertheless, DPI signatures could be applicable to encrypted traffic depending on:

- the level of encryption (see clause 6.8.1)
- local availability of the decryption key (see clause 6.8.2)
- inspection conditions based on encrypted information (see clause 6.8.3).

6.8.1 Extent of encryption

Any 'packet' as protocol data unit (PDU) consists of protocol control information (PCI) and service data units (SDU) at various protocol layers. When encryption is applied on the inspected communication path, then encryption may be applied:

- either to the entire protocol stack or only to a part of the protocol stack (Note 1), and,
- within a protocol layer, either to the PDU of a layer x (Lx) (i.e., complete Lx-PDU) or only partially (e.g., just the Lx-PCI or Lx-SDU part).

NOTE 1 – Example: an RTP-over-IP packet service may provide encryption on:

a) network layer (e.g., via IPsec transport mode or IPsec tunnel mode);

b) transport layer (e.g., via DTLS); or/and

c) application layer (e.g., via SRTP).

DPI can be performed on any unencrypted part of the packet.

R-6.8.1/1: Awareness of encrypted traffic (from the DPI signature perspective): DPI can optionally be performed on all unencrypted information elements of the inspected traffic, dependent on the extent of encryption (Note 2).

NOTE 2 – Example: an SRTP-over-IP packet flow may still be inspected in the case of DPI signatures, based on information elements on RTP PCI ("RTP header"), UDP PCI ("UDP header"), IP PCI ("IP header"), etc., if just the RTP SDU (containing the IP application data) is encrypted.

R-6.8.1/2: Unawareness of encrypted traffic (from the DPI signature perspective): DPI can optionally be performed as a partial DPI (because parts of the DPI signatures could be related to unencrypted packet information elements).

Such a "partial DPI" on encrypted traffic may lead to "limited DPI services", but already enough for specific use cases (e.g., if a "coarse granular" identification of an application or protocol would be already sufficient).

6.8.2 Availability of decryption key

R-6.8.2/1: DPI can optionally be applied in the case of local availability of the used encryption key(s). Any DPI enforcement will then imply an initial decryption of (a local copy) the inspected packet.

6.8.3 Conditions for inspections based on encrypted information

R-6.8.3/1: DPI can optionally be supported on encrypted traffic, in the case of policy conditions applicable for inspections based on encrypted information (Note).

NOTE – Example: a bit pattern (which unambiguously identifies a particular packet flow) may be derived by the observation (inspection) of partially encrypted traffic (see clause 6.8.1). The bit pattern as part of subsequent DPI signatures would then be already available in the encrypted encoding.

6.8.4 IPsec-specific DPI requirements

The requirements stated in clauses 6.8.1 to 6.8.4 are also valid for IPsec encrypted packets. This Recommendation is focusing on the flow identification aspects of IPsec encrypted traffic. The aspects related to application identification are for further study.

6.8.4.1 General requirements

R-6.8.4.1/1: The DPI-FE can optionally be able to support, at the least flow identification for IPsec encrypted traffic. The corresponding flow descriptor n-tuple can optionally be limited to only the L2 and L3 based elements.

R-6.8.4.1/2: A flow can optionally correspond to the traffic of a single IPsec security association (SA), or can optionally span multiple SAs.

R-6.8.4.1/3: The SA-based flow identification implies that the 32-bit IPsec security parameter index (SPI) can optionally be part of the flow descriptor.

6.8.4.2 IPsec tunnel and transport mode

The IPsec protocols (AH and ESP, see below) can be used to protect either an entire IP payload (i.e., the tunnel mode) or the upper-layer protocols of an IP payload (i.e., the transport mode).

R-6.8.4.2/1: The DPI-FE can optionally be able to detect IPsec encrypted traffic in the tunnel mode.

R-6.8.4.2/2: The DPI-FE can optionally be able to detect IPsec encrypted traffic in the transport mode.

6.8.4.3 IPsec AH-protected traffic

The authentication header (AH) provides data integrity, data origin authentication and limited optional anti-replay services.

R-6.8.4.3/1: The DPI-FE can optionally be able to detect AH-protected traffic based on the corresponding IP protocol number.

6.8.4.4 IPsec ESP-protected traffic

The encapsulating security payload (ESP) additionally provides confidentiality.

R-6.8.4.4/1: The DPI-FE can optionally be able to detect ESP-protected traffic based on the corresponding IP protocol number.

6.9 Inspection of compressed traffic

The purpose of compression is to reduce the amount of traffic. For example:

- "ZIP"-based compression [b-IETF RFC 1950] reduces file sizes (relevant to FTP-over-TCP/IP flows);
- "SigComp"-based compression [b-IETF RFC 3320] reduces the size of SIP messages (relevant to SIP-over-L4/IP flows).

6.9.1 Awareness of compression method

R-6.9.1/1: DPI can optionally be supported when local information on the applied compression scheme would be available (e.g., if DPI node is aware that the inspected SIP signalling path is encoded according to clause 8 of [b-ETSI TS 124 229]). Any DPI enforcement would then imply an initial decompression of (a local copy) the inspected packet.

R-6.9.1/2: DPI can optionally be also supported if it is possible to derive the applied compression scheme from the inspected traffic flow (e.g., the particular zip compression method can optionally be derived from file header information elements).

6.10 Detection of abnormal traffic

6.10.1 Requirements for detection of abnormal traffic

R-6.10.1/1: The DPI-FE is required to be able to support detection of abnormal traffic. Namely, the DPI signatures are required to be able to characterize normal and abnormal traffic (e.g., either as a black or white list).

NOTE – DPI policy rule aspects: This capability could imply the check of many metrics with regards to traffic and/or packet characteristics, as well as possibly maintaining a decision tree for the final conclusion concerning normal or abnormal traffic classes.

7 Functional requirements from the network viewpoint

7.1 General requirements

7.1.1 Emergency telecommunications

The overall design, implementation, deployment and use of DPI functions have to include appropriate measures to prevent negative impacts to the performance and security of emergency telecommunications (ET). ET [ITU-T Y.2205] means any emergency related service that requires special handling relative to other services (i.e., priority treatment over regular services). This includes government authorized emergency services, e.g., emergency telecommunication services [ITU-T E.107] and public safety services.

This Recommendation is based on the use of an application tag to identify different application semantics such as application protocol type (e.g., ITU-T H.264 video, or SIP as an example IP application protocol) in a generic manner. The same application types (e.g., SIP) are used to support both regular services and ET application services. However, this Recommendation does not specify any unique application tag to identify ET application services. Therefore, appropriate precautions would be necessary to prevent negative implications on ET application services.

R-7.1/1: It is required to not interfere with the priority treatment of ET application services traffic over ordinary services.

R-7.1/2: It is required that the overall design, implementation, deployment and use of DPI functions include appropriate measures to prevent negative impacts to the performance of ET application services (e.g., introducing unnecessary delays).

R-7.1/3: It is required that the overall design, implementation, deployment and use of DPI functions include appropriate measures to prevent introduction of security compromises to the integrity, confidentiality or availability of ET communications/sessions.

NOTE – This Recommendation does not provide any stipulations as to how the above requirements are to be met. The requirements could be achieved through the use of functional capabilities, operational measures or a combination of both.

7.2 Data plane, control plane and management plane in DPI node

7.2.1 Traffic planes and traffic types from DPI node perspective

Following the network model of user, control and management plane (see [b-ITU-T Y.2011]), a DPI node deals with a data path and local decision path (see Figure 7-1). The data path can work either in the unidirectional or bidirectional mode.

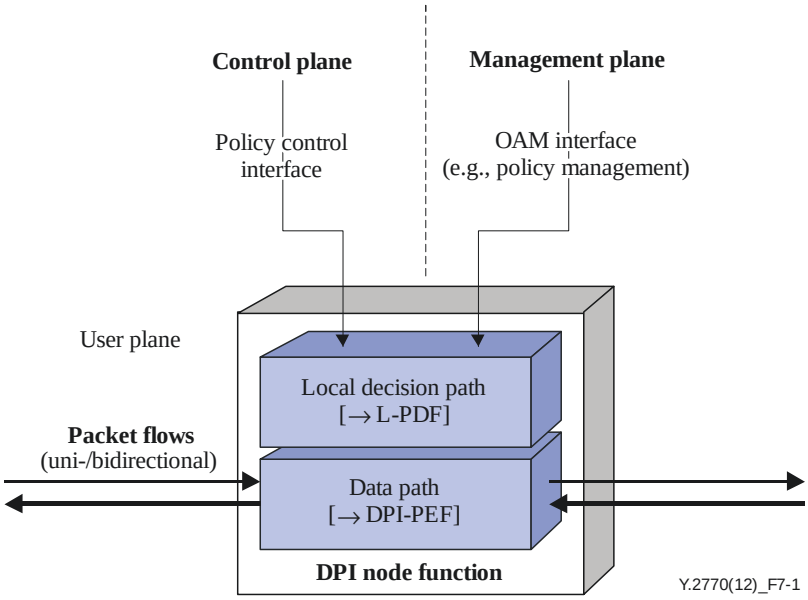


Figure 7-1 – External and internal traffic planes of a DPI node

NOTE 1 – The packet flows are routed/switched along the packet paths, which are often called data paths in IP networks (see e.g., [b-IETF RFC 4778]); therefore, the term data plane is synonymous with user plane.

NOTE 2 – The IP data path is also known as IP media path (or bearer path) in the case of IP application data traffic, or IP signalling path in the case of IP application control traffic [b-ITU-T X.1141].

R-7.2.1/1: A DPI node is required to support the management plane interface for policy management and can optionally support the control plane interface for policy control.

The *Local Decision Path* entity provides the node-internal control and management capabilities.

R-7.2.1/2: A DPI node is required to recognize two kinds of packets (see Figure 7-2):

a) data packets, which belong to customers and carry customer traffic (called "traffic THROUGH", see [b-IETF opsec]); and

b) control and management packets, which belong to the network provider and relate to network operations (called "traffic TO"; see [b-IETF opsec]).

The two kinds of packets traverse a "common pipe" (or are "in-band") or traverse different channels that logically separate data from "out-of-band" control packets (see also [b-IETF RFC 4778], clause 2.2 for an example of management traffic).

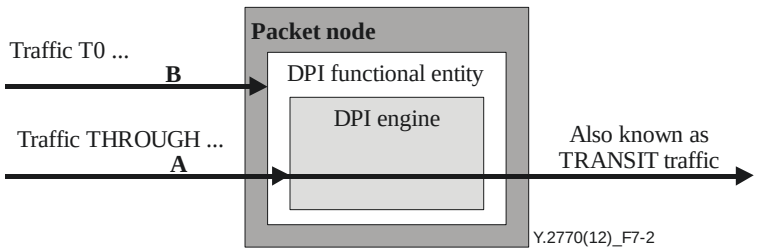


Figure 7-2 – Traffic THROUGH (A) and TO (B) a DPI node

7.2.2 Requirements related to management plane

R-7.2.2/1: DPI-FE is required to support management protocols for configuration management of DPI policy rules.

R-7.2.2/2: DPI-FE is recommended to support the management of a user's identity information and the relationship between the user and user's applications.

R-7.2.2/3: DPI-FE is recommended to support the management of applications and services:

- generate, modify and publish application templates;
- maintain the relationship between applications and strategies; and
- provide and manage reservation of user's service.

R-7.2.2/4: DPI-FE is recommended to support the management of strategies predefined or generated dynamically. (These strategies can optionally relate to application identification, application control, and user management.)

R-7.1.2/5: DPI-FE is recommended to support the management of administration authority. To support hierarchical management, different administrators have different management authorities.

7.2.3 Requirements related to control plane

R-7.2.3/1: DPI-FE can optionally support policy control protocols (like [b-ITU-T H.248.1] for the ITU-T *Rw* reference point as defined in [ITU-T Y.2111]) for control and signalling of DPI policy rules.

7.2.4 Requirements related to user (data) plane

The data (user) plane meets the following optional requirements:

R-7.2.4/1: DPI-FE can optionally support different packet technologies (e.g., xDSL, UMTS, CDMA2000, cable, LAN, WLAN, Ethernet, MPLS, IP, ATM).

7.2.5 Requirements across planes

R-7.2.5/1: DPI-FE can optionally support an aligned protocol grammar for the specification of DPI policy rules. The syntax used at the policy control interface (control plane) and policy management interface (management plane) is recommended to be preferably identical. This does not imply the use of the same protocol, but concerns the specification language for (DPI) policy rules (often called Filter Specification Language (FSL), or Policy Specification Language (PSL); see Note).

NOTE – Example script languages are SIEVE [b-IETF RFC 5228] or PERL, or XML or XACML (eXtensible Access Control Markup Language).

An aligned protocol grammar allows the use of a common data/object model in the policy enforcement path within a DPI node, which is a prerequisite for efficient and fast rule execution as well as the interruption-less update operations on the DPI signature library.

8 Interfaces of the DPI-functional entity

The requirements described in the previous clauses entail the following interfaces:

- between the DPI-FE and remote network entities (see clause 8.1), and
- between DPI-FE internal components (see clause 8.2).

8.1 External DPI-FE interfaces

Figure 8-1 depicts the external interfaces of the DPI-FE:

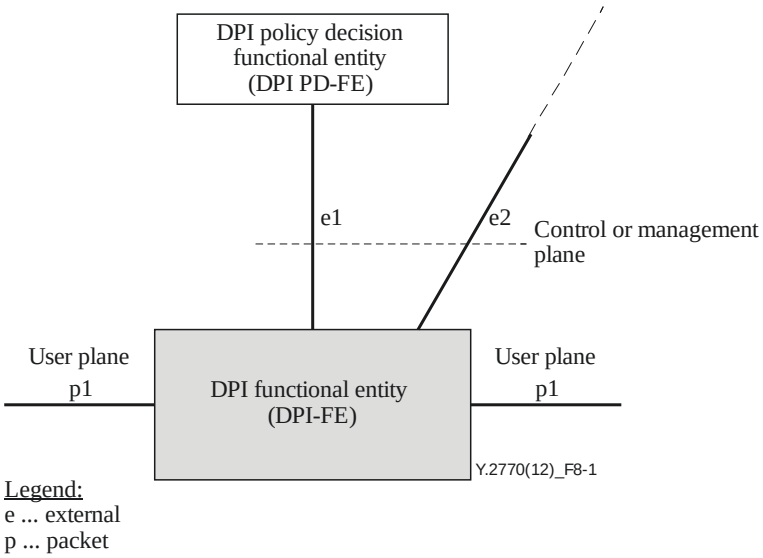


Figure 8-1 – External DPI-FE interfaces

8.1.1 Inspected traffic (p1)

The DPI-FE exchanges packets with remote packet nodes via *p1*. The packet path topology is point-to-point for a DPI-FE acting in the In-Path DPI mode. Multipoint topologies are not supported. Interface p1 covers bidirectional packet paths.

The packet path topology for a DPI-FE acting in the Out-of-Path DPI mode is related to an endpoint.

8.1.2 Control/management of traffic inspection (e1)

The DPI policy decision functional entity (DPI-PDFE) aims to control or manage the DPI-FE. The information exchanged via e1 thus concerns the commands for controlling/configuring the packet handling behaviour of the DPI-FE. Such commands could be described in a DPI policy.

Interface e1 could also support the reporting and notification from the DPI-FE to the DPI-PDFE.

8.1.3 Reporting to other network entities (e2)

Interface e2 encompasses all possible communication interfaces with remote network entities other than the DPI-PDFE. This interface primarily supports reporting.

8.2 Internal DPI-FE interfaces

Figure 8-2 shows the possible internal interfaces based on the DPI requirements:

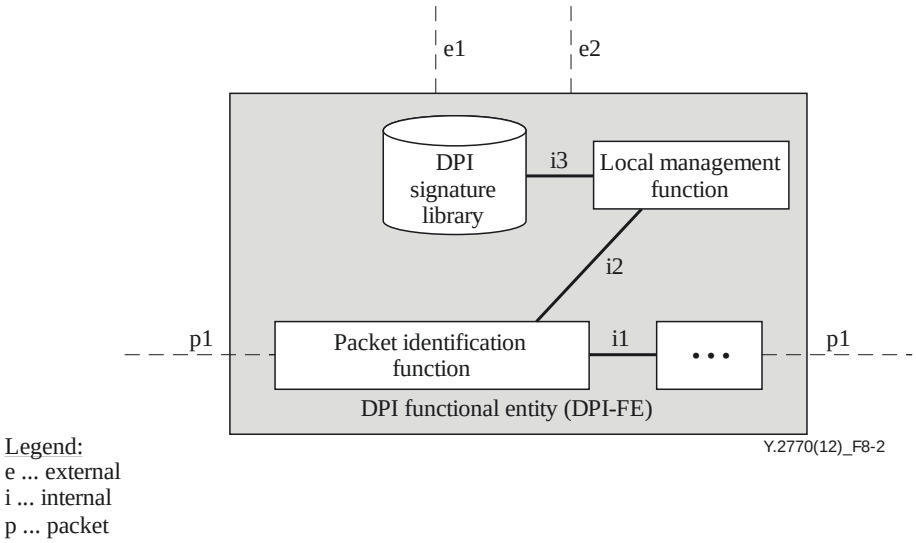


Figure 8-2 – Internal DPI-FE interfaces

There might be further DPI-FE internal functional components and internal interfaces. The internal interfaces are for further study.

8.3 Interface requirements

R-8.3/1: It is recommended that interface e1 follow the requirements in clause 6.5.

R-8.3/2: It is recommended that interface e2 follow the requirements in clause 6.4.1.

9 Security considerations and requirements

This clause describes security threats and defines security requirements for DPI entities in NGN.

9.1 Security threats against DPI entities

The functional entities associated with DPI may be typically located within an NGN operator's trusted zone or trusted but vulnerable zone as defined in [ITU-T Y.2701]. This Recommendation identifies the security threats to NGN and defines the requirements for protection against the threats. Since the DPI-related entities are a part of NGN, the conclusions of [ITU-T Y.2701] are applicable to them. Based on [ITU-T Y.2701], the security threats related to the DPI entities are identified as follows:

- destruction of DPI-related information
- corruption or modification of DPI-related information
- theft, removal or loss of DPI-related information
- disclosure of DPI-related information
- interruption of services.

The information pertaining to the DPI operations include DPI policy rules with their signatures and DPI exported flow and application information. Destruction, corruption or modification, theft, removal or loss of such information may make it unusable for DPI operations. In many countries, such information is recommended to be treated according to the national regulatory and policy requirements and must not be disclosed.

The interruption of services may be as result of denial of service (DoS) attacks. Any entity receiving data can be a target of a DoS attack. For example, an attacker can indirectly flood a DPI

entity with a large volume of traffic causing degradation or interruption of the DPI services for the legitimate users.

9.2 Security requirements for DPI entities

The major security requirements for DPI entities are:

R-9.2/1: The DPI-related information residing in DPI entities is required to be protected.

R-9.2/2: If the information is exchanged beyond the NGN operator's trusted zone, the DPI-related information is required to be protected between DPI entities and the remote functional entities (e.g., DPI PD-FE, NMS).

R-9.2/3: Mechanisms can optionally be required to mitigate the flooding attack against the DPI FE.

R-9.2/4: Vendors, operators and service providers are required to take into account national regulatory and policy requirements when implementing this Recommendation.

R-9.2/5: The implementers are recommended to employ the existing well-tested mechanisms for meeting the security requirements of this Recommendation. For example, as specified in [ITU-T Y.2704].

Annex A

Specification of a flow descriptor

(This annex forms an integral part of this Recommendation.)

A.1 Protocol syntactical perspective

The flow descriptor relates to a data structure (data object), which may be modelled *as k-Tuple* (see Figure A.1). The data structure consists of *k* information elements (IE) (Note). The value of k is variable and greater than zero[1], but constant for a particular flow. The information elements are the ones as contained in the IANA IPFIX registry. There is a value associated with each information element. The association is typically mathematical equality ('='), but other mathematical relations are not excluded.

NOTE – The IETF IPFIX information elements may be attributed as "key field" or "non-key field".

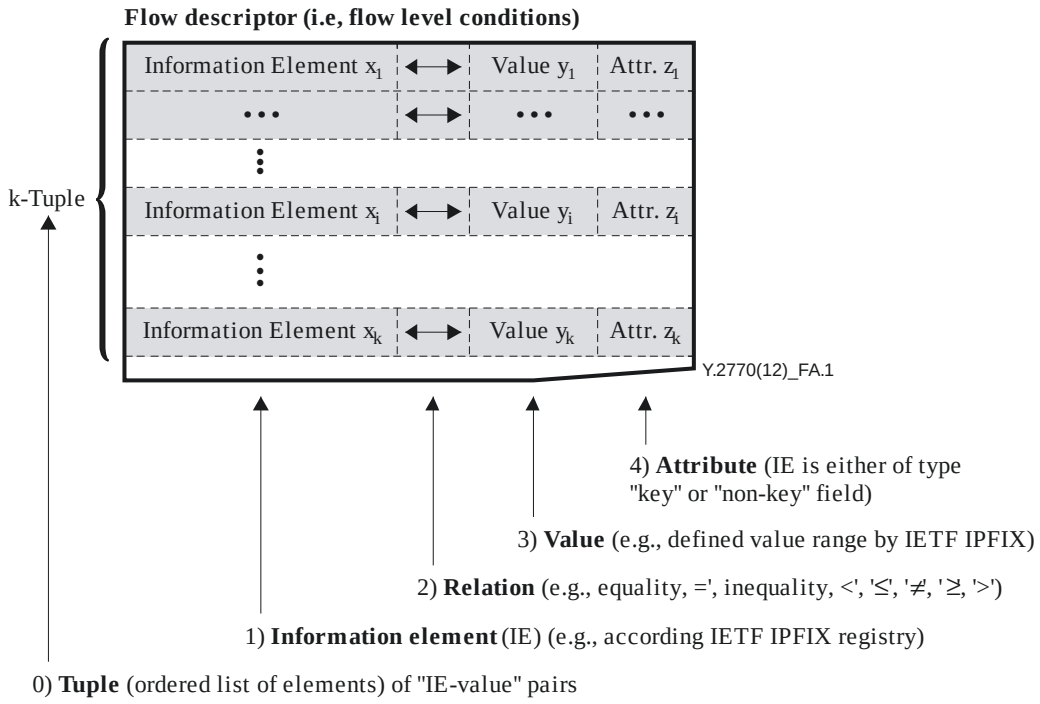


Figure A.1 – The flow descriptor (flow level conditions) from a protocol syntactical point of view

The flow level descriptor as a k-tuple represents consequently a list of k "name-value pairs" (NVP); here a sequence of "< *IE* ↔ *value* >" pairs)[2].

A.2 Specifying information element values

In the flow level conditions, the value of an IE may be:

- fully specified

  Full specification represents the case of a complete name-value setting.

---

1 Note: N = 0 indicates "Flow-independent".

2 Similar to other structures like AVP (<attribute name, value>), parameter-value pair (<parm=value>), etc.

- not specified

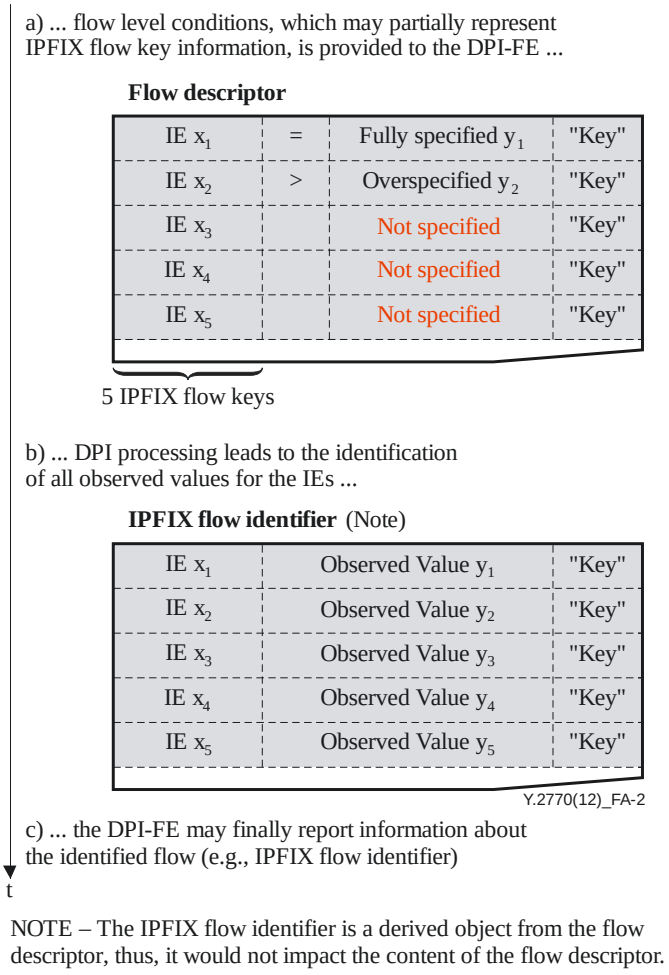
  "*Not specified*" represents the case when there is *not yet any value* assigned to an IE.
- overspecified or

  Overspecification indicates there are multiple possible values for a specific IE.
- underspecified

  Underspecification indicates wildcarding (e.g., all possible values, or choose value).

A.3 Relation between flow descriptor, IPFIX flow identifier and IPFIX flow key

The example in Figure A.2 provides a 5-tuple flow descriptor and contains 5 IFPIX flow keys. In order to identify a particular flow, the flow descriptor imposes some conditions on the values of these flow keys as defined in clause A.2: the first flow key IE x_1 is "fully specified", the second flow key IE x_2 is "overspecified", while the other IEs are "not specified", as displayed in part a) of Figure A.2.



NOTE – The IPFIX flow identifier is a derived object from the flow descriptor, thus, it would not impact the content of the flow descriptor.

Figure A.2 – Flow descriptor, IPFIX flow identifier and IPFIX flow key example

Note that the flow descriptor does not impose conditions on the IPFIX flow keys only: indeed, in some circumstances, flow descriptors on non-flow keys might be required, for example when a condition of the TCP flags of the first packet of the flow is required. The fundamental difference between the flow descriptor and the IPFIX flow identifier in the example Figure A.2, is that the flow descriptor contains a "superior than" condition on the IE x_2, ("IE x_2 > value y_2"), while the IPFIX flow identifier contains the observed value for the IE x_2, i.e., value yy_2. The IPFIX flow identifier is composed of the set of observed values for the flow keys, once the DPI functional entity has processed the packets and classified them into a flow.

Note that if the exported information (e.g., via an IPFIX flow record) contains each IE along with the associated observed values, and whether or not the IE is an IPFIX flow key, then there is no need to assign a specified IPFIX flow identifier, as the IPFIX flow identifier is the sum of all this information.

Bibliography

[b-ITU-T H.248.1] Recommendation ITU-T H.248.1 v3 (2005), *Gateway Control Protocol: Version 3*.

[b-ITU-T X.734] Recommendation ITU-T X.734 (1992), *Information technology – Open Systems Interconnection – Systems Management: Event report management function*.

[b-ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

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

[b-ETSI ES 282 003] ETSI ES 282 003 (2011), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture*.

[b-ETSI TS 123 203] ETSI TS 123 203 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture (3GPP TS 23.203 version 10.4.0 Release 10)*.

[b-ETSI TS 124 229] ETSI TS 124 229 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE;IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 version 9.4.0 Release 9)*.

[b-IETF IANA IPFIX] IETF IANA IPFIX (2007), IP Flow Information Export (IPFIX) Entities.
<http://www.iana.org/assignments/ipfix/ipfix.xhtml>

[b-IETF opsec] IETF draft-ietf-opsec-filter-caps (2007), *Filtering and Rate Limiting Capabilities for IP Network Infrastructure*.
<http://tools.ietf.org/html/draft-ietf-opsec-filter-caps-09>

[b-IETF RFC 1950] IETF RFC 1950 (1996), *ZLIB Compressed Data Format Specification version 3.3*.

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

[b-IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp)*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[b-IETF RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*.

[b-IETF RFC 4268] IETF RFC 4268 (2005), *Entity State MIB*.

[b-IETF RFC 4778] IETF RFC 4778 (2007), *Operational Security Current Practices in Internet Service Provider Environments*.

[b-IETF RFC 4867] IETF RFC 4867 (2007), *RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs.*

[b-IETF RFC 5102] IETF RFC 5102 (2008), *Information Model for IP Flow Information Export*.

[b-IETF RFC 5103] IETF RFC 5103 (2008), *Bidirectional Flow Export Using IP Flow Information Export (IPFIX).*

[b-IETF RFC 5228] IETF RFC 5228 (2008), *Sieve: An Email Filtering Language.*

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.

[b-IETF RFC 5426] IETF RFC 5426 (2009), *Transmission of Syslog Messages over UDP*.

[b-IETF RFC 5476] IETF RFC 5476 (2009), *Packet Sampling (PSAMP) Protocol Specifications*.

[b-PacketTypes] McCann, P.J., and Chandra S. (2000), *Packet Types: Abstract Specification of Network Protocol Messages*; in SIGCOMM '00: Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 321-333, ACM Press, New York.

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, 2013