

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

Document Sharing Hub

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/>.

© ITU 2013

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

Table of Contents

		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

Downloaded from ITU-T Y.2770 2012

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.

Copyright International Telecommunication Union/ITU Telecommunication Sector

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.

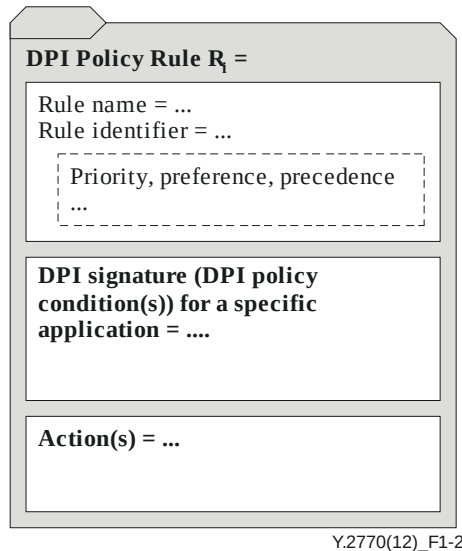


Figure 1-2 – Generic format of DPI policy rules

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.

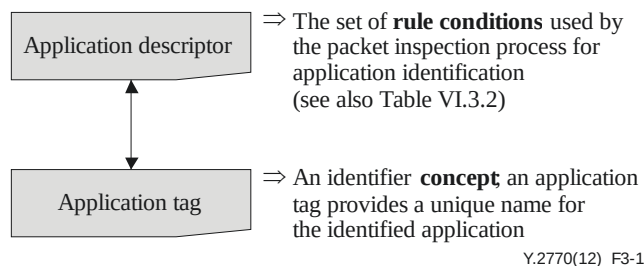


Figure 3-1 – Relationship between the application tag and application descriptor

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 L_{3,4} 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 (L₄+HI): Processing of policy rule(s) with policy conditions involving only the PCI elements above the transport layer.

3.2.21 L₄ payload inspection (L₄PI): 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 – L₄PI relates to the union of L₄+HI and L₇PI policy conditions.

3.2.22 L₇ payload inspection (L₇PI): 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., L_x-Payload refers to the payload at protocol layer x). Ditto for L_x-SDU, L_x-PDU and L_x-PCI.