

Recommendation

ITU-T Y.2776 (07/2024)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Next Generation Networks – Security

Deep packet inspection – intelligent management and maintenance of policy information base

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	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.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999

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

Recommendation ITU-T Y.2776

Deep packet inspection – intelligent management and maintenance of policy information base

Summary

Recommendation ITU-T Y.2776 specifies intelligent management and maintenance aspects for policy information base (PIB) of deep packet inspection (DPI). The scope of this Recommendation includes the following aspects: problem analysis for PIB of DPI; the functional architecture of intelligent management and maintenance of PIB (PIB-IMM); implementation methods for PIB-IMM; functional requirements for PIB-IMM; performance aspects for PIB-IMM; considerations for the control plane of PIB-IMM; consideration for management and application of PIB-IMM; and security considerations.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.2776	2024-07-22	13	11.1002/1000/15894

Keywords

Deep packet inspection, intelligent management, policy information base.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2024

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
2	References.....	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	3
5	Conventions	4
6	Problem analysis for policy information base of DPI	4
7	Functional architecture of intelligent management and maintenance of PIB.....	6
	7.1 Overview of intelligent management and maintenance of PIB.....	6
	7.2 General functional model for intelligent management and maintenance of PIB.....	6
	7.3 Basic components necessary for intelligent management and maintenance of PIB.....	7
	7.4 Internal interfaces for intelligent management and maintenance of PIB	8
	7.5 External interfaces for intelligent management and maintenance of PIB	8
8	Implementation methods for intelligent management and maintenance of PIB.....	8
	8.1 Overview of feasible implementation methods.....	8
	8.2 Implementation method based on generative adversarial network	9
	8.3 Implementation method based on evolving algorithm	11
	8.4 Implementation method based on cluster algorithm	12
	8.5 Implementation method based on other methods.....	13
9	Functional requirements for intelligent management and maintenance of PIB	14
	9.1 Functional requirements for DPI entity	14
	9.2 Functional requirements for R-PDF+	15
	9.3 Functional requirements for L-PDF+	16
	9.4 Functional requirements for the DPI-Scf component.....	16
	9.5 Functional requirements for the DPI-Anf component.....	16
	9.6 Functional requirements for internal interfaces.....	17
	9.7 Functional requirements for external interfaces	17
10	Performance aspects for intelligent management and maintenance of PIB	17
	10.1 Process time for intelligent management and maintenance of PIB.....	17
	10.2 Storage usage for intelligent management and maintenance of PIB.....	18
	10.3 Process correct rate for intelligent management and maintenance of PIB.....	18
	10.4 Network traffic awareness correct rate.....	19
	10.5 Network traffic awareness volume	19

	Page
11 Control plane considerations	19
11.1 DPI-PIB control plane requirements	19
11.2 DPI-PIB control plane considerations	20
12 Management and application considerations.....	21
12.1 Overview requirements of management aspect.....	21
12.2 Requirements of management and configuration.....	21
12.3 Requirements of log management	21
12.4 Requirements of application.....	22
13 Security considerations.....	22
Bibliography.....	23

Recommendation ITU-T Y.2776

Deep packet inspection – intelligent management and maintenance of policy information base

1 Scope

This Recommendation specifies intelligent management and maintenance aspects for policy information base (PIB) of deep packet inspection (DPI). The scope of this Recommendation includes:

- a) Problem analysis for PIB of DPI;
- b) Functional architecture of intelligent management and maintenance of PIB;
- c) Implementation methods for intelligent management and maintenance of PIB;
- d) Functional requirements for intelligent management and maintenance of PIB;
- e) Performance aspects for intelligent management and maintenance of PIB;
- f) Consideration for control plane;
- g) Consideration for management and application;
- h) Security consideration.

Implementers and users of the described techniques shall comply with all applicable national and regional laws, regulations, and policies. The mechanisms described in this Recommendation may not be applicable to international correspondence, in order to ensure the secrecy and sovereign national legal requirements placed upon telecommunication networks, but implementers and users of the mechanisms shall comply with the Constitution and Convention of ITU, such as CS ARTICLE 33.

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 X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology. Open Systems Interconnection. Basic reference model: The basic model.*
- [ITU-T Y.2704] Recommendation ITU-T Y.2704 (2007), *Security mechanisms and procedures for NGN.*
- [ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks.*
- [ITU-T Y.2771] Recommendation ITU-T Y.2771 (2014), *Framework for deep packet inspection.*
- [ITU-T Y.2772] Recommendation ITU-T Y.2772 (2016), *Mechanisms for the network elements with support of deep packet inspection.*
- [ITU-T Y.2773] Recommendation ITU-T Y.2773 (2017), *Performance models and metrics for deep packet inspection.*



- [ITU-T Y.2774] Recommendation ITU-T Y.2774 (2019), *Functional requirements of deep packet inspection for future networks*.
- [ITU-T Y.2775] Recommendation ITU-T Y.2775 (2019), *Functional architecture of deep packet inspection for future networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

in order to identify the application unambiguously.

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

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

3.1.3 DPI policy [ITU-T Y.2770]: A policy as defined, for example in [b-IETF RFC 3198] (see clause 3.1.4), enforced in a DPI entity.

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

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

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

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

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

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

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

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

3.1.7 DPI analyser [ITU-T Y.2771]: A subsequent entity in the DPI processing path (within a DPI policy enforcement function) with focus on comparison functions between the particular packet headers and payloads of preselected packet flows. The primary scope of the DPI analyser is related to the evaluation of DPI policy conditions against preselected incoming packets.

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

3.1.8 DPI node [ITU-T Y.2771]: A network element or device that realizes the DPI related functions. It is thus a generic term used to designate the realization of a DPI physical entity.

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI	Artificial Intelligence
CA	Cluster Algorithm
CLI	Command Line Interface
DL	Deep Learning
DPI	Deep Packet Inspection
DPI-AcEF	Deep Packet Inspection Action Execution Function
DPI-AnF	Deep Packet Inspection Analyser Function
DPI-FE	DPI Functional Entity
DPI-FMF	DPI Feature Mining Function
DPI-PDFE	DPI Policy Decision Functional Entity
DPI-PE	DPI Physical Entity
DPI-PEF	Policy Enforcement Function
DPI-PIB	DPI Policy Information Base
DPI-SCF	Deep Packet Inspection Scan Function
EA	Evolving Algorithm
GAN	Generative Adversarial Network
L-IPRG	Local Intelligent Policy Rule Generator
L-PDF	Local PDF

L-PDF+	L-PDF updated for PIB-IMM
MIB	Management Information Base
ML	Machine Learning
NA	Network Awareness
Netconf	Network Configuration
NMS	Network Management System
NSA	Network Status Awareness
NTS	Network Traffic Simulator
PDF	Policy Decision Function
PIB	Policy Information Base
PIB-IMM	Intelligent Management and Maintenance of Policy Information Base
QoS	Quality of Service
R-IPRG	Remote Intelligent Policy Rule Generator
R-PDF	Remote PDF (i.e., PDF remotely located from DPI node perspective)
R-PDF+	R-PDF updated for PIB-IMM
SNMP	Simple Network Management Protocol
SSH	Secure Shell
YANG	Yet Another Next Generation

5 Conventions

In this Recommendation:

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

6 Problem analysis for policy information base of DPI

DPI is one of the basic technologies for implementing functions such as application and service awareness. DPI-related technologies and methods are beneficial to network management and control, quality of service (QoS) assurance, network security enhancement, value-added services, and so on.

At present, DPI-related technologies have been widely applied and played important roles in the network. Improvement and enhancement for DPI-related technologies are necessary anyway.

[ITU-T Y.2771] has depicted a generic model for the DPI entity, as shown in Figure 6-1.