International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.86

(01/2014)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Gateway Control Protocol: ITU-T H.248 support for deep packet inspection

Recommendation ITU-T H.248.86

International Telecommunication Union

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	**H.240–H.259**
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Interoperability compliance testing of personal health systems (HRN, PAN, LAN and WAN)	H.820–H.849
Multimedia e-health data exchange services	H.860–H.869

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

Recommendation ITU-T H.248.86

Gateway Control Protocol: ITU-T H.248 support for deep packet inspection

Summary

Recommendation ITU-T H.248.86 has in scope ITU-T H.248 media gateways with support of packet inspection capabilities. This Recommendation describes the relation of deep packet inspection (DPI) to existing ITU-T H.248 protocol capabilities concerning packet processing, and defines new ITU-T H.248 packages with the specific scope of DPI.

The proposed ITU-T H.248 packages serve various different network-level use cases and provide inherent flexibility due to the core design concept that separates encoding and transport of DPI policy rules.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.248.86	2014-01-13	16	11.1002/1000/12069

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T H.248.86

Gateway Control Protocol: ITU-T H.248 support for deep packet inspection

1 Scope

An ITU-T H.248 media gateway (MG) provides operations on packet traffic in general, related to the ephemeral (and root) termination type. Several existing ITU-T H.248 packages include packet inspection as part of the overall defined service (such as gate management and packet filtering services according to [ITU-T H.248.43]).

This Recommendation defines additional ITU-T H.248 capabilities for so-called deep packet inspection (DPI) related services. Understanding and definition of DPI in this Recommendation follows principally [ITU-T Y.2770]. The "DPI concept" is fundamentally coupled with the architecture of layered protocol stacks, as expressed by the acronym words 'deep' and 'packet'. Figure 1 depicts DPI in an example of an ITU-T X.200 layered protocol architecture, and also illustrates the historical evolution from *shallow packet inspection* (SPI) over *medium depth packet inspection* (MPI) towards DPI. It should be noted that SPI and MPI are colloquial terms, whereas clause 3.2.5 of [ITU-T Y.2770] defines DPI. Further, the notion of 'packet' is used in the broadest sense, typically nowadays focusing on IP packets [IETF RFC 791], [b-IETF RFC 2460], but covering non-IP traffic as well (see also clause 1.1 of [ITU-T Y.2770]).

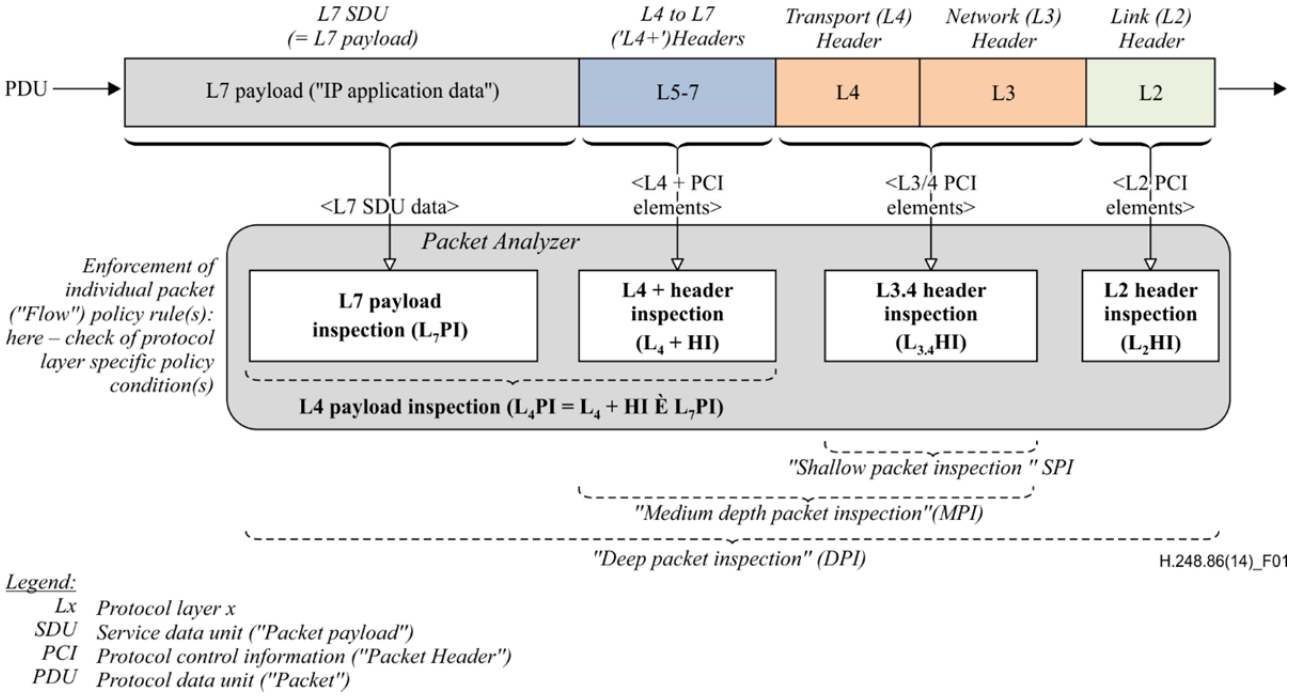


Figure 1 – Packet Inspection – Example of DPI, using a layered protocol architecture according to OSI-BRM [ITU-T X.200] where DPI covers also layer 2

This Recommendation:

– clarifies the understanding of DPI versus non-DPI in context of the ITU-T H.248.x-series of Recommendation (clause 5.2);

– describes the relation of "policy rule" support by existing ITU-T H.248 packages (clause 6); and

– defines new ITU-T H.248 packages for flexible DPI support in various network scenarios (clauses 7 to 9).

This Recommendation provides several appendices that provide complementary information on various aspects of ITU-T H.248-supported DPI.

1.1 Applicability statements

As outlined by Figure 1, DPI is not a new technology, it is rather a continuous evolution of existing packet processing functions. Interactions with existing packet inspection technologies needs to be considered when using this Recommendation.

1.1.1 This Recommendation with other ITU-T H.248.x-series Recommendations with policy rule support

See clause 6.2.

1.1.2 This Recommendation with non-H.248 policy specification languages

The usage of non-H.248 policy specification languages (PSL) is a fundamental concept behind the ITU-T H.248 capabilities for DPI support defined by the ITU-T H.248 packages of this Recommendation. See also clause 6.4, Appendix III and Appendix IV.

However, any normative guidance for the usage of such PSLs is out of scope of this Recommendation.

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 H.248.1] Recommendation ITU-T H.248.1 (2013), *Gateway control protocol: Version 3*.

[ITU-T H.248.37] Recommendation ITU-T H.248.37 (2008), *Gateway control protocol: IP NAPT traversal package*.

[ITU-T H.248.40] Recommendation ITU-T H.248.40 (2013), *Gateway control protocol: Application data inactivity detection package*.

[ITU-T H.248.43] Recommendation ITU-T H.248.43 (2008), *Gateway control protocol: Packages for gate management and gate control*.

[ITU-T H.248.48] Recommendation ITU-T H.248.48 (2012), *Gateway control protocol: RTCP XR block reporting package*.

[ITU-T H.248.53] Recommendation ITU-T H.248.53 (2009), *Gateway control protocol: Traffic management packages*.

[ITU-T H.248.61] Recommendation ITU-T H.248.61 (2013), *Gateway control protocol: Packages for network level ITU-T H.248 statistics*.

[ITU-T H.248.68] Recommendation ITU-T H.248.68 (2009), *Gateway control protocol: Package for removal of digits and tones*.

[ITU-T H.248.69] Recommendation ITU-T H.248.69 (2009), *Gateway control protocol: Packages for interworking between MSRP and H.248*.

[ITU-T H.248.76] Recommendation ITU-T H.248.76 (2010), *Gateway control protocol: Filter group package and guidelines*.

[ITU-T H.248.78] Recommendation ITU-T H.248.78 (2013), *Gateway control protocol: Bearer-level application level gateway*.

[ITU-T H.248.79] Recommendation ITU-T H.248.79 (2012), *Gateway control protocol: Guidelines for packet-based streams*.

[ITU-T H.248.84] Recommendation ITU-T H.248.84 (2012), *Gateway control protocol: NAT traversal for peer-to-peer services*.

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

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

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

[IETF RFC 3986] IETF RFC 3986 (2005), *Uniform Resource Identifier (URI): Generic Syntax.*

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 policy rule [ITU-T Y.2770]: The policy rule pertinent to DPI (see also clause 3.1.2 in [ITU-T Y.2770]). In this Recommendation, a DPI policy rule is referred to simply as a rule.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

A Address *or* Action

ADC Application Detection and Control

ALG Application Level Gateway

AMR Adaptive-Multi Rate (codec)

API Application Programmable Interface

ASIC Application Specific Integrated Circuit

Bp Bucket size of peak token bucket [ITU-T H.248.53]

Bs Bucket size of sustainable token bucket [ITU-T H.248.53]

BT	(RTCP) Block Type
C	Condition
CLI	Command Line Interface
Cz	ITU-T H.248 Context
CPU	Central Processing Unit
DA	(IP) Destination Address
DPI	Deep Packet Inspection
DS	Differentiated Services
F_j	Media or Control Flow
FIB	Forwarding Information Base
FPGA	Field Programmable Gate Array
FSL	Filter Specification Language
GBRA	Generic Byte Rate Algorithm
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identifier
IM	Instant Messaging
IP	Internet Protocol
IWF	Interworking Function
LD	Local Descriptor (ITU-T H.248 protocol) *or* Local Destination (ITU-T H.248 bearer connection endpoint)
L_x	Layer *x*
L_xHI	Layer *x* Header Inspection (see also clause 3.2.19 of [ITU-T Y.2770])
L_yPI	Layer *y* Payload Inspection (see also clauses 3.2.21 to 3.2.23 in [ITU-T Y.2770])
Lz+	Layer(s) above *z* (e.g., L4+)
MG	Media Gateway
MGC	Media Gateway Controller
MIME	Multipurpose Internet Mail Extensions
MMI	Man-Machine Interface
MPI	Medium depth Packet Inspection
MSRP	Message Session Relay Protocol
NAT	Network Address Translation
OGP	Open Game Protocol
P	(L4) Port *or* Protocol
P2P	Peer-to-Peer
PCI	Protocol Control Information
PDP	Policy Decision Point

PDU	Protocol Data Unit
PEL	Policy Expression Language
PIB	Policy Information Base
PSL	Policy Specification Language
PT	(RTP) Payload Type *or* (RTCP) Packet Type
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RD	Remote Descriptor (ITU-T H.248 protocol) *or* Remote Destination (ITU-T H.248 bearer connection endpoint)
Rp	Rate of peak token bucket [ITU-T H.248.53]
Rs	Rate of sustainable token bucket [ITU-T H.248.53]
RS	Remote Source (ITU-T H.248 bearer connection endpoint)
Rx	Policy Rule
RTCP	RTP Control Protocol
RTCP XR	RTCP Extended Report
RTP	Real-time Transport Protocol
SA	(IP) Source Address
SDP	Session Description Protocol
SDU	Service Data Unit
Si	Stream
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SP	(IP) Source Port
SPI	Shallow Packet Inspection
Ta	Termination
TC	(IPv6) Traffic Class
TCP	Transmission Control Protocol
TDF	Traffic Detection Function
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
ToS	(IP) Type of Service
TTL	(IP) Time To Live
UDP	User Datagram Protocol
URI	Universal Resource Indicator
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

5 Conventions

5.1 Connection endpoint naming

The reader should be familiar with the connection endpoint naming scheme according to clause 5.2 of [ITU-T H.248.1].

5.2 Distinction of DPI and non-DPI cases

The concept of packet inspection, from the perspective of layered protocol architectures, is fairly wide and includes all protocol layers above layer 1. However, the scope of packet inspection may be limited, mainly related to link, network and/or transport layers. Such a limitation is/was typically motivated by service-, historical- or implementation-related aspects. This kind of limited packet inspection is also known as shallow and medium depth packet inspection (SPI, MPI; see also clause 8.1 in [b-ITU-T Y.Sup 23]).

The distinction between DPI and non-DPI according to [ITU-T Y.2770] is followed by this Recommendation. Thus, in the context of this Recommendation, 'DPI' means policy inspections rules using protocol information elements higher than layer 4. This is in contrast to 'non-DPI', which relates to packet inspection at protocol layers 2, 3 and/or 4 (i.e., SPI, MPI).

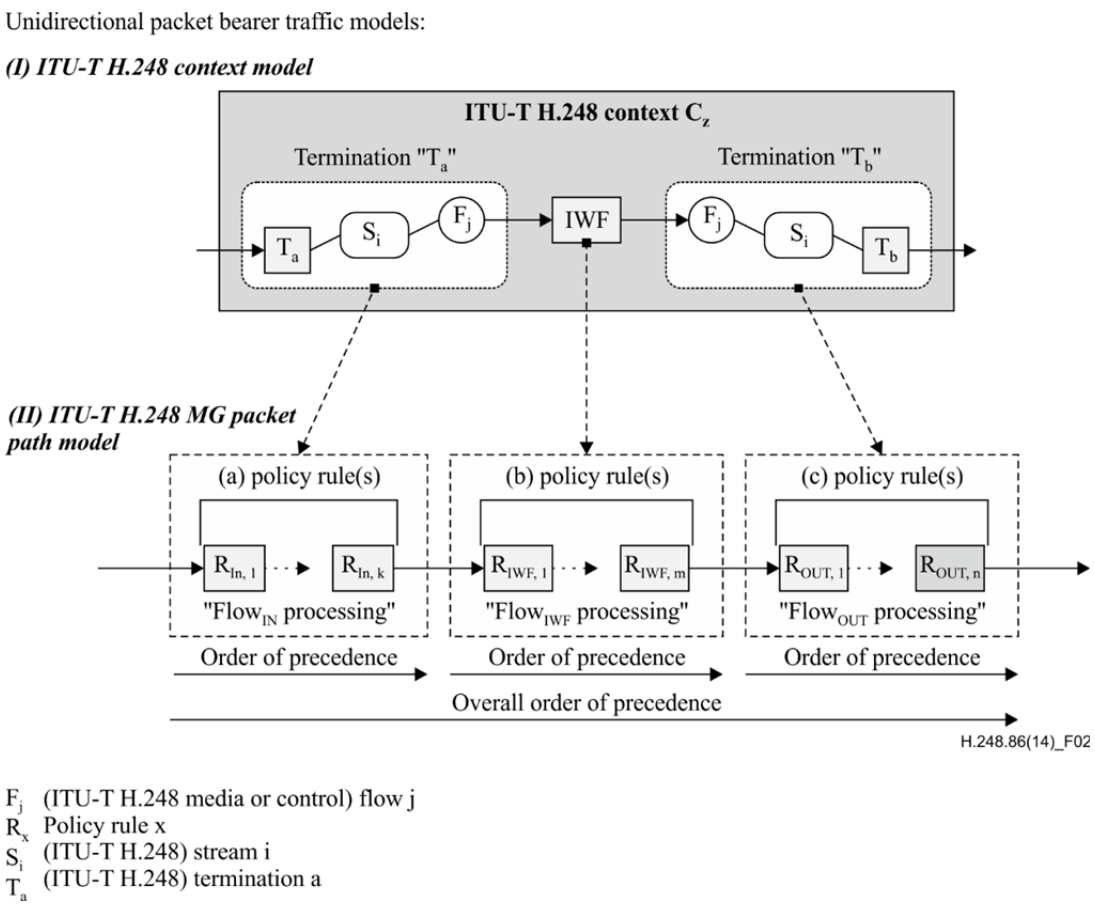
NOTE – Clause 6.2 provides a rough classification of existing ITU-T H.248.x-series of Recommendations in DPI and non-DPI cases.

6 Overview

6.1 Policy rule model

6.1.1 Basic model

DPI relates to the processing of policy rules by the MG, hence the generic policy rule model (see Figure 2) according to [ITU-T H.248.79] is also applicable for this Recommendation. A DPI policy rule is typically associated with termination "Ta" in this model, because the "inspection function" is normally executed on incoming traffic as soon as packets enter the MG.



F_j (ITU-T H.248 media or control) flow j
R_x Policy rule x
S_i (ITU-T H.248) stream i
T_a (ITU-T H.248) termination a

Figure 2 (copy of Figure 4 of [ITU-T H.248.79]) – Order of operations (within a layer) – Unidirectional packet bearer traffic models using the concept of policy rules

6.1.2 Extended models

Similar to existing ITU-T H.248 MG functions, rules could be associated with individual contexts or at the higher entire MG (e.g., DPI policy rules assigned to the root termination).

6.2 Relation to other ITU-T H.248.x-series of Recommendations

This clause provides a non-exhaustive inventory of the relation of DPI functions to existing ITU-T H.248 services.

6.2.1 ITU-T H.248.79 on general guidelines for packet-based streams

[ITU-T H.248.79] is related to filtering TCP traffic. See overview in clause 9 of [ITU-T H.248.79].

6.2.2 ITU-T H.248.37 on policy rules for NAT-T support

The MG inspects transport address information in incoming IP packets (rule condition) and possibly modifies that information (rule action) ([ITU-T H.248.37]).

NOTE – This is an example of SPI due to L4/L3 related rule conditions.

6.2.3 ITU-T H.248.40 on policy rules for application data inactivity detection

The MG inspects the packet inter-arrival or/and inter-departure rate at IP transport endpoints (rule condition) and possibly notifies the MGC (rule action) ([ITU-T H.248.40]).

NOTE – This is an example of SPI due to L4/L3 related rule conditions.

6.2.4 ITU-T H.248.43 on policy rules for basic gate management

See e.g., the two examples in clauses II.2.1.3 and II.2.1.4. The illustrated policy rules are entirely based on [ITU-T H.248.43] signalling.

NOTE – This is related to SPI due to L4/L3 related rule conditions, and to MPI in case of the "upper layer protocol type" filter element (see clause 9.6.3 of [ITU-T H.248.43]).

6.2.5 ITU-T H.248.48 on policy rules for RTCP report filtering

The kind of policy rules given by the example in clause II.2.2.5 are supported by [ITU-T H.248.48].

NOTE – This is an example of MPI due to additional L4+ related rule conditions (by inspection of RTP header elements plus possibly RTCP XR report structures).

6.2.6 ITU-T H.248.53 on policy rules for traffic volume policing

See e.g., the two examples of "packet size range policing" and "flow-level byterate policing" in clauses II.2.1.1 and II.2.1.2. The illustrated policy rules are entirely based on [ITU-T H.248.53] signalling.

NOTE – This is an example of SPI due to L4/L3 related rule conditions (in case of IP traffic policing).

6.2.7 ITU-T H.248.61 on policy rules for IP traffic measurements

The MG identifies incoming IP packets according to a wide variety of lookup-keys according to Appendix II of [ITU-T H.248.61] (rule condition) and possibly updating statistics (rule action).

NOTE – This is an example of SPI due to L4/L3(/L2) related rule conditions.

6.2.8 ITU-T H.248.68 on policy rules for removal of in-band information

The MG inspects incoming media-over-packets for digit and/or tone signals (rule condition) and possibly removes that information (rule action) ([ITU-T H.248.68]).

NOTE – This is an example of MPI or even DPI, dependent on the protocol layer and encoding of tone/digit information.

6.2.9 ITU-T H.248.69 on policy rules for message filtering

The Messaging Filtering package (clause 13 of [ITU-T H.248.69]) defines a policy rule based behaviour (based on "Sieve" as defined by [b-IETF RFC 5228]) for inspecting e-mail traffic (i.e., e-mail over SMTP/L4/IP packets) with the purpose of message filtering (rule actions).

NOTE – This is an example of DPI.

6.2.10 ITU-T H.248.76 on policy rules for general filtering

[ITU-T H.248.76] allows generating multiple, combined policy rules with regards to packet filtering, called "filter groups".

NOTE – This is an example of SPI and MPI (same as clause 6.2.3).

6.2.11 ITU-T H.248.78 on policy rules for NAT-T support

In case of the MG autonomous bearer-level ALG mode (clause 6.2 of [ITU-T H.248.78]) the MG inspects address information at protocol layers L4+, L4 and L3 in incoming IP packets (rule condition) and possibly modifies the L4+ address information (rule action).

NOTE – This is an example of MPI/DPI, dependent on the protocol layer and encoding of address information.

6.2.12 ITU-T H.248.84 on policy rules for NAT-T support

The MG inspects TCP header protocol control information in incoming IP packets (rule condition) and possibly forwards TCP packets including the modified TCP header protocol control information (rule action) ([ITU-T H.248.84]).

NOTE – This is an example of SPI due to L4/L3 related rule conditions.

6.3 Control and management of DPI policy rules

The notion of "policy control" refers to the network *control* plane, i.e., the signalling of (DPI) policy rules by the MGC to the MG via ITU-T H.248. ITU-T H.248 as a gateway control protocol may be then considered as policy control protocol. The notion of "policy management" refers to the network *management* plane, i.e., the provisioning of (DPI) policy rules by the network/element management system in the MG via configuration management (policy management) protocol(s). See also clause 7.2.1 of [ITU-T Y.2770].

This Recommendation focuses on DPI policy control, however, the provisioning option of some package elements (e.g., via package usage detail specifications by ITU-T H.248 profiles) covers some DPI policy management capabilities (see also Figure II.2).

The possible MGC involvement in DPI policy control is further outlined in Appendix I.

6.4 Package design philosophy

There are several different models relating to how DPI could be supported by ITU-T H.248 gateways (see e.g., Appendix III). The variety of models is reflected in the design of the *inspection rule base package* (clause 7). The concept in differentiating between basic and augmented DPI services is satisfied by the *inspection rule operational package* (clause 8), as an extension to the base package, and a future *inspection rule group package* (clause 9) (see also Figure 3).

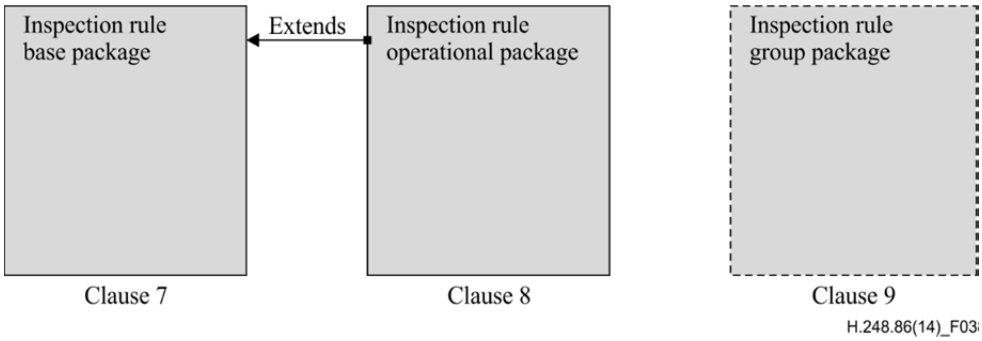


Figure 3 – Overview of ITU-T H.248 packages

7 Inspection rule base package

Package name: Inspection rule base package

Package ID: irb (0x0112)

Description: This package allows the MGC to indicate to the MG DPI policy rules. The DPI policy rules and behaviour are out of scope of this Recommendation. Such rules could be e.g., based on "SNORT" (see Appendix IV) as a typical policy rule specification language for DPI.

This package defines a minimum service by two properties, representing two principle rule signalling variants (see more in Appendix III). The properties may be associated with Root and non-Root terminations. Possible interactions should be considered (see clause 7.6.3).

Property values may be either signalled by the MGC or provisioned via management actions.

Usage of this package implies

– that there is a prior agreement between MGC and MG about the used policy specification language(s) (PSL; see e.g., Table IV.1); and

– that the PSL(s) are not changed during the lifetime of the ITU-T H.248 Control Association.

The base package capabilities allow therefore a basic mechanism to communicate rules to the MG.

Example: A very minimum DPI service support (from MGC perspective) might be the provisioning of an *irb* package property via the management plane (i.e., configuration management action for DPI policy rule(s)) with rule-embedded management plane reporting only. Such an application is also known as "overlay DPI".

Version: 1

Extends: None

7.1 Properties

7.1.1 Pointer to rule conditions

Property name: Pointer to rule conditions

Property ID: ptr (0x0001)

Description: This property allows the MGC to indicate which rule conditions should be used for inspection of incoming packets by referring to a pointer to a data object which contains DPI policy rule conditions.

The pointer is in a URI format which includes also a generic name (which may represent a globally or locally unique identifier).

The applied pointer scheme is subject of an ITU-T H.248 profile specification. E.g., the URI format could follow a URI scheme such as "file", "ftp", "https", etc.

NOTE – The concept of a "pointer to a local or remote data object" is also supported by [ITU-T H.248.9] and [ITU-T H.248.69] (see e.g., clause 13.1.2, property "*Incoming Message Filters by reference*") with pointers data object types "media" and "message" [ITU-T H.248.9] and "SIEVE script" [ITU-T H.248.69] respectively.

Type: String

Possible values: The string is of type "URI". [IETF RFC 3986]

See: http://www.iana.org/assignments/uri-schemes/

Default: None

Defined in: LocalControl (in case of non-root termination),
TerminationState (in case of root termination)

Characteristics: Read/Write

7.1.2 Container for rule

Property name: Container for rule

Property ID: cfr (0x0002)

Description: This property contains a DPI policy rule that is applied to incoming packets.

Appendices I, II and III provide complementary information about such DPI policy rules. Such a DPI policy rule object could internally be structured as simple, compound, hierarchical, etc DPI policy rules. Syntax and semantics of such DPI policy rule objects are out of scope of this Recommendation.

NOTE 1 – Appendix IV indicates possible examples of policy rules for packet inspection.

NOTE 2 – The concept of a "container for a rule data object" is also supported by [ITU-T H.248.69] (see e.g., clause 13.1.1, property "*Incoming Message Filters*") with concrete data object type "SIEVE script".

Type: String

Possible values: As per the grammar of the applied policy rule specification language(s).

Default: An empty string

Defined in: LocalControl (in case of non-root termination),
TerminationState (in case of root termination)

Characteristics: Read/Write

7.2 Events

None.

7.3 Signals

None.

7.4 Statistics

None.

7.5 Error codes

None.

7.6 Procedures

7.6.1 Enforcement of policy rules for packet inspection

Based on a user profile, service profile or/and MGC policy, the MGC may set packet level inspection rules at an individual stream level or the root termination.

7.6.1.1 Via explicit rule signalling in native ITU-T H.248 syntax

This method is out of scope of this package, and relates rather to existing ITU-T H.248 tools as indicated by clause 6.2.

7.6.1.2 Via explicit rule signalling using container method

The MGC enforces packet inspection by transferring DPI policy rules to the MG via the *cfr* property.

7.6.1.3 Via pointer to rule signalling and MG-locally stored rules

The MGC enforces packet inspection by referring correspondent DPI policy rules via the *ptr* property.

7.6.1.4 Via pointer to rule signalling and MG-remotely stored rules

The MGC enforces packet inspection by referring to the corresponding DPI policy rules via the *ptr* property.

7.6.1.5 Parallel usage of explicit and pointer based rule signalling

The MGC may use both methods in parallel, taking into account possible rule interactions (see clause 7.6.3).

7.6.2 Unsuccessful packet inspection process

The enforcement of policy rules for packet inspection might be principally not successful. For example: The MG may not be able to parse or apply the rules indicated via the *ptr* and/or *cfr* properties. The base package does not provide any means for detailed feedback and diagnosis support. The MG should rather reply with existing ITU-T H.248 error codes.

Applications with requirements for more detailed feedback information from the packet inspection process should additionally use the *inspection rule operational* package (see next clause 8).

NOTE – Unsuccessful packet inspection operations could also lead to management plane reporting events (e.g., fault management) besides MGC notifications, but this is out of scope of this Recommendation.

7.6.3 Guidelines in order to address possible rule interaction problems

This package offers some flexibility, with regards to:

1. support of multiple signalling variants (see Appendix III)
2. support of Root and Context-level DPI and
3. support of multiple DPI policy specification languages (see Appendix IV) due to decoupling of DPI policy rule specification from the ITU-T H.248 protocol.

Such degrees of freedom could lead to interaction problems in the MG when enforcing DPI policy rules. E.g., different rules' semantics could overlap or even be contradictory.

In order to mitigate interaction risks, a network application (as defined by an ITU-T H.248 profile) could e.g.,:

– select just one signalling variant,
– separate the root and non-root DPI policy rules into two disjoint sets,
– support only one DPI policy specification language,
– and/or many other restrictions, which limit the likelihood of interactions.

8 Inspection rule operational package

Package name: Inspection rule operational package

Package ID: iro (0x0113)

Description: This package allows the MGC to receive information related to the operation of enforced DPI policy rules in the MG.

The scope of this package version is limited on operational information concerning principal feedback from packet inspection process with focus on:

1. whether packets are successfully identified (and if, by which policy rule);
2. possible rule errors; and
3. high level performance metrics related to some basic packet handling events.

Version: 1

Extends: irb v1

8.1 Properties

None.

8.2 Events

8.2.1 Satisfied policy rules

Event name: Satisfied policy rules

Event ID: spr (0x0001)

Description: This event allows the MGC to be notified about satisfied policy rule conditions, as part of an enforced DPI policy rule. It is assumed that DPI policy rules contain an embedded rule identifier (see e.g., Figure II.1).

8.2.1.1 EventsDescriptor parameters

8.2.1.1.1 Policy rule filter

Parameter name: Policy rule filter

Parameter ID: prf (0x0001)

Description: This parameter allows the MGC to select the list of DPI policy rules. The MG will check *all* enforced DPI policy rules according the *inspection rule base* package usage. The MG reporting is limited to successfully checked DPI policy rules according the specified *prf* filter.

Semantic of "successfully checked DPI policy rule":

> At least one packet could be *identified* which *matched* the DPI policy rule *condition(s)*

(NOTE – This implies that the MG was successful in parsing that DPI policy rule).

Type: Sub-list of String

Optional: Yes

Possible values: The possible values are determined according to the applied DPI policy rule specification language(s) (PSL). The MG should be inherently aware of that grammar.

Default: Empty list (i.e., the MGC shall not be notified)

8.2.1.2 ObservedEventsDescriptor parameters

8.2.1.2.1 Detected policy rules

Parameter name: Detected policy rules

Parameter ID: dpr (0x0001)

Description: This parameter indicates the list of successfully checked DPI policy rules.

Type: Sub-list of String

Optional: No

Possible values: Same value range as in clause 8.2.1.1.1

Default: None

8.2.2 Inspection runtime error

Event name: Inspection runtime error

Event ID: ire (0x0002)

Description: This event allows the MG to send a notification to the MGC indicating that an error has occurred during the execution of DPI policy rule(s) against incoming packet flows.

8.2.2.1 EventsDescriptor parameters

None.

NOTE – The scope of runtime error observations is considered to be global across *all* enforced DPI policy rules.

8.2.2.2 ObservedEventsDescriptor parameters

8.2.2.2.1 Unsuccessful policy rule

Parameter name: Unsuccessful policy rule

Parameter ID: upr (0x0001)

Description: There might be one or multiple DPI policy rules enforced at the MG. This parameter indicates which particular DPI policy rule(s) generated an error.

Type: Sub-list of String

Optional: Yes

Possible values: same value range as in clause 8.2.1.1.1

Default: None

8.3 Signals

None.

8.4 Statistics

8.4.1 Identified packets

Statistic name: Identified packets

Statistic ID: idpa (0x0001)

Description: Provides the number of successfully identified packets (from the ingress traffic flow) on the termination or stream since the statistic was set. The packets represent the ingress protocol data units (PDU) of all packet flows of an ITU-T H.248 Stream (or root termination).

The semantic of "packet" is related to the applied "packet inspection" process, which is given by the enforced DPI policy rule(s). This statistic is therefore inherently accumulative across all applied rules.

The semantic of "successfully identified packet" relates to a *match* event of the DPI policy rule *condition(s)*.

NOTE – The notion of "packet identification" is described in clauses 7.3 and 7.4 in [b-ITU-T Y.Sup 23].

Example: "IP packet" in case of policy rule conditions related to IP traffic. Statistic *idpa* may be then used in conjunction with the "IP packets received" statistics (clause 7.4.2 of [ITU-T H.248.61]), e.g., when the packet ratio of successfully identified packets would be interesting.

Type: Double

Possible values: Any 64-bit integer 0 and up

Level: Either

8.4.2 Discarded packets

Statistic name: Discarded packets due to rule actions

Statistic ID: dipa (0x0002)

Description: Provides the number of packets discarded on the termination or stream since the statistic has been set. The packets represent the ingress protocol data units (PDU) of all packet flows of an ITU-T H.248 Stream (or root termination).

The semantic of "packet" is related to the applied "packet inspection" process, which is given by the enforced DPI policy rule(s).

The event of packet discard would be the result of correspondent DPI policy rule actions.

Type: Double

Possible values: Any 64-bit integer 0 and up

Level: Either

8.4.3 Modified packets

Statistic name: Modified packets due to rule actions

Statistic ID: mopa (0x0003)

Description: Provides the number of packets modified on the termination or stream since the statistic has been set. The packets represent the ingress protocol data units (PDU) of all packet flows of an ITU-T H.248 Stream (or root termination).

The semantic of "packet" is related to the applied "packet inspection" process, which is given by the enforced DPI policy rule(s).

The event of packet modification would be the result of correspondent DPI policy rule actions. Packet modification could related to packet header and/or payload information. Excluded is the packet destination address information, because subject of statistic *repa* (clause 8.4.4).

Type: Double

Possible values: Any 64-bit integer 0 and up

Level: Either

8.4.4 Redirected packets

Statistic name: Redirected packets due to rule actions

Statistic ID: repa (0x0004)

Description: Provides the number of packets modified for redirection on the termination or stream since the statistic has been set. The packets represent the ingress protocol data units (PDU) of all packet flows of an ITU-T H.248 Stream (or root termination).

The semantic of "packet" is related to the applied "packet inspection" process, which is given by the enforced DPI policy rule(s).

The event of *packet redirect* would be the result of correspondent DPI policy rule actions, which relates typically to a change of the packet destination address information.

Type: Double

Possible values: Any 64-bit integer 0 and up

Level: Either

8.5 Error codes

None.

8.6 Procedures

8.6.1 General operation

This package should be used in conjunction with the *inspection rule base* (irb) package (clause 7) due to the precondition of enabled DPI policy rules in the MG.

8.6.2 Results of policy rule enforcement

8.6.2.1 Notification about policy rule detections

The MGC subscribes to this notification service by arming the *src* event. The list of policy rules could be qualified by the MGC via event parameter *prf*. In order to uniquely identify the relevant stream when the *src* event is used at termination level and there is a multiple-stream-per-termination structure, the StreamID should be used with the ObservedEvent.

8.6.2.2 Performance monitoring of policy rule enforcement process

Related to the processing of rule conditions:

– Number of successfully identified packets are counted by statistic *idpa*.

Related to the processing of rule actions:

– Number of discarded packets are counted by statistic *dipa*.

– Number of modified packets are counted by statistic *mopa*.

– Number of redirected packets are counted by statistic *repa*.

8.6.3 Runtime errors

The MGC should also set the "inspection runtime error" (iro/ire) event on the applicable stream or termination in order to determine if there are any errors when running DPI policy rules against incoming packet traffic. In order to uniquely identify the relevant stream when the *src* event is used at termination level and there is a multiple-stream-per-termination structure, the StreamID should be used with the ObservedEvent.

9 Inspection rule group package

The previous packages allow a basic support for DPI. This service may be augmented in future by e.g., an *inspection rule group* package, similar to the constellation between [ITU-T H.248.43] ("basic filter service") and [ITU-T H.248.76] ("advanced filter service by filter rule grouping"). A future *inspection rule group* package could then provide similar properties (as [ITU-T H.248.76]) with respect to the introduction of a "*inspection rule context*" concept, an "*inspection rule group identifier*" and a "*relative rule order*" capability.

Such an advanced DPI support service is out of scope of the initial release of this Recommendation.

Appendix I

MGC aspects of DPI policy rules

(This appendix does not form an integral part of this Recommendation.)

I.1 Introduction

Policy rules enforced in a MG are basically related to an associated communication instance, such as a call, session, application, service, dialogue, etc., which may be abstracted as "context" (Note). There are consequently context-dependent policy rules, whether of type DPI or non-DPI. Context-independent policy rules would be associated with the ITU-T H.248 Root termination in MGs.

The MGC may principally enforce both, – context-aware and context-unaware policy rule processing, – however, typically the MGC's prime responsibility is the control of context-aware MG behaviour.

This general background is also valid with regards to DPI policy rule enforcement.

NOTE – The general context concept is here identical to the ITU-T H.248 (protocol) context element. The "context awareness" of MGs (and MGCs) is synonym to the correspondent capability according to clause 3.2.5 of [b-ITU-T Y.2201].

I.2 MGC-locally vs MGC-remotely generated DPI policy rules

DPI policy rules signalled to the MG by the MGC via ITU-T H.248 could be either completely produced by the MGC itself, or prepared and provided by other network elements. Figure I.1 illustrates these two options of MGC-locally and MGC-remotely generated DPI policy rules. The applied model in a specific network environment may impact the question on the used policy rule format or which signalling option ("container" versus "pointer") at the ITU-T H.248 interface.

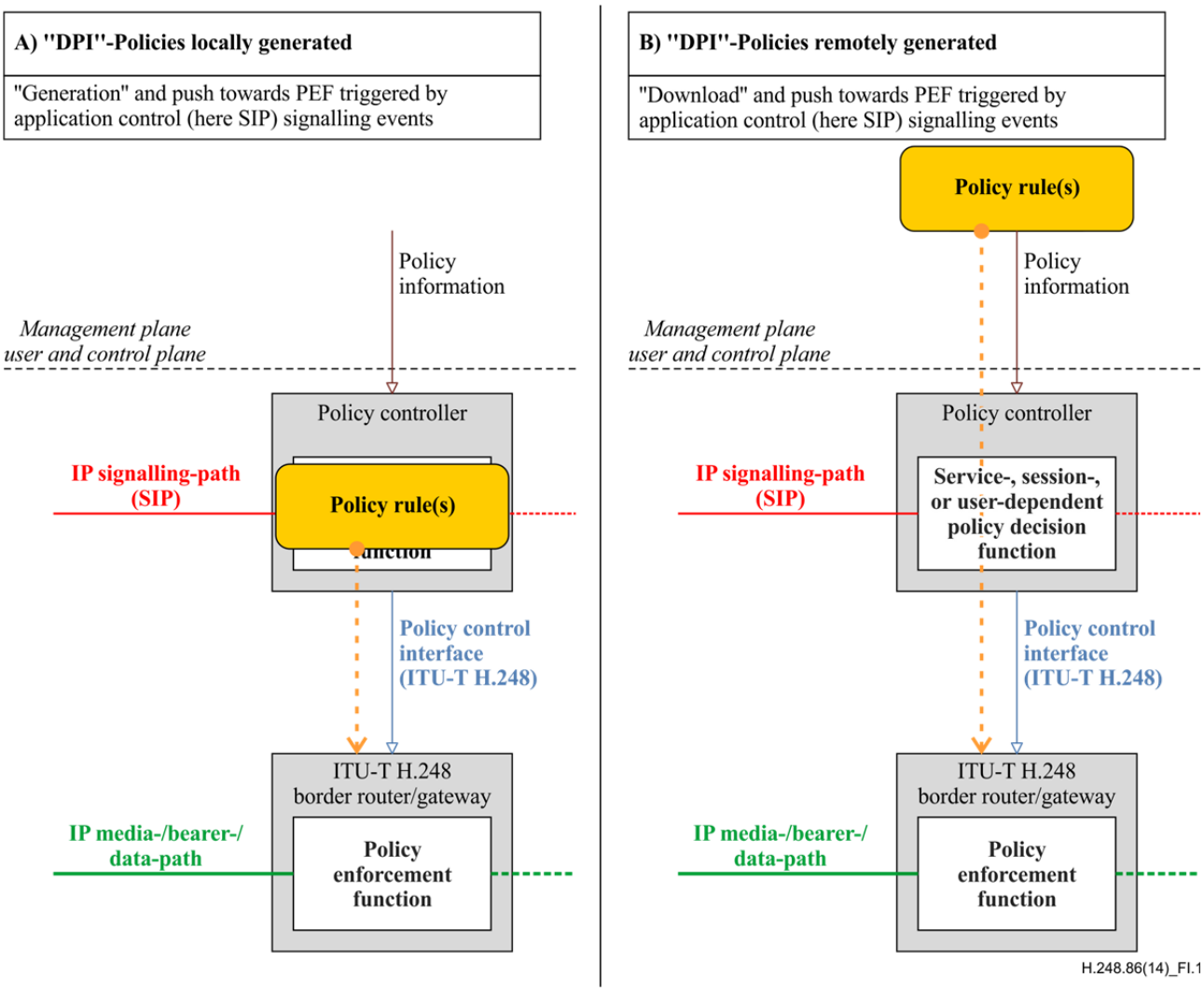


Figure I.1 – Possible roles of a policy control server (with embedded MGC entity) – MGC-locally (A) vs MGC-remotely (B) generated DPI policy rules (Example with SIP as an application control protocol at MGC level)

There might be a mix of both (A and B) in real networks, and even the additional policy rule enforcement in MGs via management plane actions (see also Figure II.2).

Appendix II

Examples of DPI and non-DPI Policy Rules

(This appendix does not form an integral part of this Recommendation.)

II.1 Introduction

II.1.1 Purpose and overview

This appendix provides accompanying material for the illustration of typical DPI use cases. Table II.1 provides an overview of illustrated example policy rules.

Table II.1 – Overview of examples in this appendix

No.	Name	Clause
a) Non-DPI scenarios:		
I	Packet size range policing	II.2.1.1
II	Flow-level byterate policing	II.2.1.2
III	Well-known port SIP message policing	II.2.1.3
IV	General IP 5-tuple policing	II.2.1.4
V	Extensive filtering	II.2.1.5
b) DPI scenarios:		
VI	Media type/media format policing	II.2.2.1
VII	Detect application X of an "application-agnostic" bearer	II.2.2.2
VIII	Detect application X = 'BitTorrent'	II.2.2.2.1
IX	Detect application X = 'Skype'	II.2.2.2.2
X	Detect application X = 'Open Game Protocol'	II.2.2.2.3
XI	Detect application X = 'audio channel in a multi-channel media application'	II.2.2.2.4
XII	Detect & measure application X = 'greek Jabber traffic'	II.2.2.2.5
XIII	TCP attack detection	II.2.2.3
XIV	Remove invalid MIME attachments from Instant Messaging	II.2.2.4
XV	RTCP Block Type Filtering	II.2.2.5
XVI	Application-specific traffic handling	II.2.2.6
XVII	Abnormal packet size detection	II.2.2.7
XVIII	Delete old packets of application X	II.2.2.8

II.1.2 Specification level of rules

Packet inspection may be considered as a packet *policing function* in general. The particular "inspection function" may be formulated as policy rule (see also [ITU-T H.248.79]). The specification depth may differ in various respects:

– High-level

– Low-level rules (using informal specification language, like a prose language)

– Low-level rules (using formal specification grammar)

This appendix describes ITU-T H.248 protocol elements for either transporting complete DPI policy rules embedded in ITU-T H.248 messages ("*container principle*"), or a reference method ("*pointer principle*"). The particular encoding of DPI policy rules in either case is out of scope.

Thus, the policy rule examples of this appendix are inherently generic, i.e., using a kind of pseudo policy specification language.

II.1.3 Generic rule format

In order to use a common description format for (DPI and non-DPI) policy rules, the examples below follow a generic rule format (see Figure II.1), comprised of

– a *rule header* (name, identifier, precedence, etc.), and

– a *rule body* (for conditions, actions).

NOTE – The examples focus on the condition/action part only.

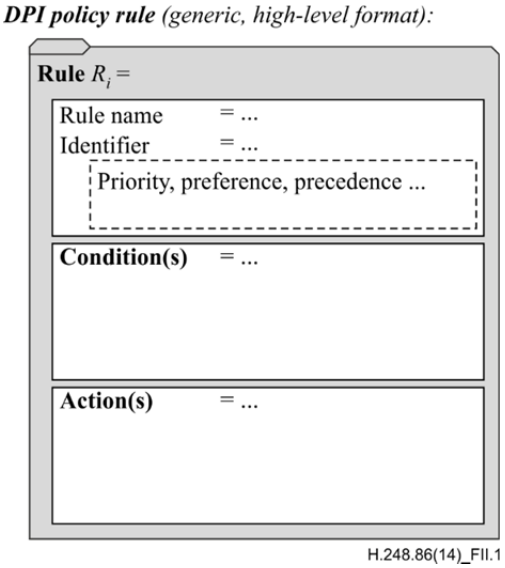


Figure II.1 – Generic high-level format of a (DPI and non-DPI) policy rule

Such a generic format is independent of ITU-T H.248 and is suited for all existing policy control and policy management protocols.

NOTE – A *filter rule* is a dedicated type of a *policy rule*. In scope of this appendix, the terms filter rule and policy rule are synonymous (however, in general there are also other policy actions different from filtering (of packets, flows, traffic, etc.)).

Figure II.2 illustrates the principle: Policy rules are assigned to ITU-T H.248 contexts, terminations (non-Root or Root) or/and streams. Policy rules may be signalled, but correspondent ITU-T H.248 property values may be also provisioned. There is thus a signalling and management aspect (or policy control and policy management), see also clause 6.3.

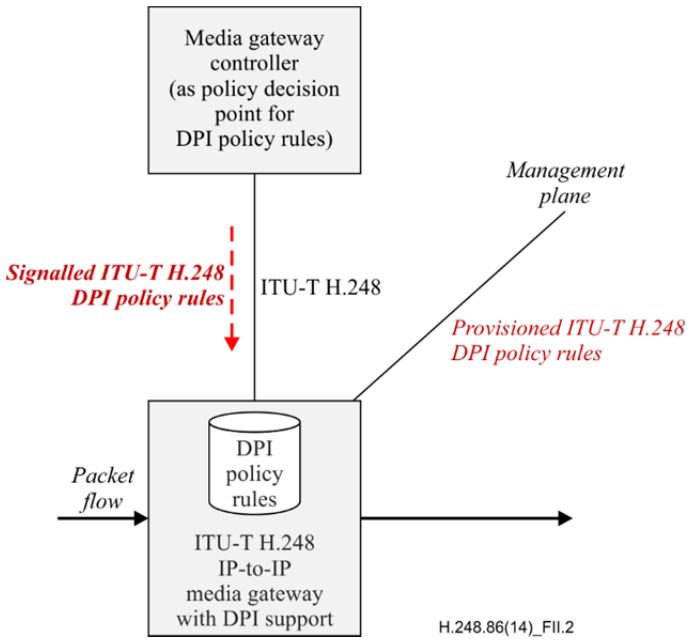


Figure II.2 – General principle for (DPI) policy rules

II.2 Examples of generic DPI and non-DPI policy rules

II.2.1 Non-DPI scenarios

This category refers to "legacy packet inspection" use cases (classified as non-DPI policing scenarios in clause 5.2).

II.2.1.1 Example I: "Packet size range policing"

This example illustrates *packet size range policing (Table II.2)*:

Table II.2 – "Non-DPI" Example I – "Packet size range policing"

Policy Rule ("Packet size range policing") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If: C_1: "L3 DA = (*H.248 LD(A)*)?" AND { C_2: "L3 PDU size > (*H.248 pacs/m*)?" OR C_3: "L3 PDU size < (*H.248 pacs/mpu*)?"}	Then: A_1: "discard IP packet" AND A_2: "Update Statistic *H.248 pacs/dp*"

The policy rule is classified as non-DPI because only layer 3 packet header and payload properties needs to be "inspected". This example supposes a wildcard *ALL* L4 port value (thus *LD(P) = ALL*; see clause 6.11 of [b-ITU-T H.248.39]). The received ITU-T H.248 IP packets must match a particular range concerning a given packet size distribution function, which is bounded by a maximum and minimum size value (using the [ITU-T H.248.53] packet size (*pacs*) package). Violating packets are not silently discarded, rather counted by the *pacs/dp* statistic.

It should be reminded that such a policy rule could be already achieved solely on basis of [ITU-T H.248.53].

II.2.1.2 Example II: "Flow-level byterate policing"

This example, also fully based on [ITU-T H.248.53], illustrates *flow-level byterate policing (Table II.3)*. The notion of 'flow' relates to the ITU-T H.248 'flow', i.e., a traffic level above the ITU T H.248 stream (see clause 6.6.2 of [ITU-T H.248.53]).

Table II.3 – "Non-DPI" Example II – "Flow-level byterate policing"

Policy Rule ("Flow-level byterate policing") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If: C_1: "L3 DA = (*H.248 LD(A)*)?" AND C_2: "L4 DP = (*H.248 LD(P)*)?" AND C_3: "L3 SA = (*H.248 RD(A)*)?" AND C_4: "L4 SP = (*H.248 RD(P)*)?" AND { C_5: "GBRA(*Rp*, *Bp*) = not OK?" OR C_6: "GBRA(*Rs*, *Bs*) = not OK?"}	Then: A_1: "discard IP packet" AND {/** if peak-rate violation $A_{2,1}$: "Update Statistic *H.248 tmanr/pvp*" $A_{2,2}$: "Update Statistic *H.248 tmanr/pvo*" } {/** if sustainable-rate violation $A_{3,1}$: "Update Statistic *H.248 tmanr/svp*" $A_{3,2}$: "Update Statistic *H.248 tmanr/svo*" }
NOTE – Package identifier *tmanr* refers to the [ITU-T H.248.53] *traffic policing statistics* package.	

This example supposes incoming IP traffic on a *local* transport connection endpoint (given by transport address LD(A,P)) plus the inspection of the *remote source* transport address (i.e., RS(A,P)). RS(A,P) which is equal here to the *remote destination* transport address (i.e., RD(A,P)) due to a symmetry assumption.

A 2-stage policing shall be enforced (peak- and sustainable rate level; see e.g., model in clause I.2.1.3.1 of [ITU-T H.248.53]).

The traffic policer conditions (for GBRA algorithm) are derived from *tman v2* properties: e.g., the first list item values for flow 1.

Violating packets are counted by the correspondent *tmanr* statistics, on packet and byte level.

II.2.1.3 Example III: "Well-known port SIP message policing"

This example is based on clause III.1.1 of [ITU-T H.248.43] (see Table II.4):

Table II.4 – "Non-DPI" Example III – "Well-known port SIP message policing"

Policy Rule ("Well-known port SIP message policing") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If NOT: C_1: "L3 DA = (*H.248 LD(A)*)?" AND C_2: "IP PCI 'protocol' = 'UDP' OR 'TCP'?" AND C_3: "L4 DP = well known port for 'SIP' OR 'SIP-TLS'?"	Then: A_1: "discard IP packet"

This example uses *compound* policy conditions, i.e., a combination of multiple simple policy conditions (see also [ITU-T H.248.43]). However, this aspect is minor (because every compound condition may be equally transformed to a number of simple conditions).

II.2.1.4 Example IV: "General IP 5-tuple policing"

The considered 5-tuple relates here to the 4-tuple of the IP transport connection endpoints plus the 1-tuple of protocol type. [ITU-T H.248.43] supports "general IP 5-tuple policing" by specifying a set of such 5-tuples in parallel. The example here is based on clause III.1.3 of [ITU-T H.248.43] (see Table II.5):

Table II.5 – "Non-DPI" Example IV – "General IP 5-tuple policing"

Policy Rule ("General IP 5-tuple policing") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If NOT: C_1: "L3 SA = [101.0.*.0]?" /* wildcard IPv4 OR C_2: "L4 DP = 23 OR 14 OR [1442-1490] OR 19999 OR 25000?" /* port range OR C_3: "IP 'protocol' = 'FTP' OR 'TELNET' OR 'SMTP' OR 'TFTP' OR 'FINGER' OR 'SIP' OR 'SIP-TLS'?"	Then: A_1: "discard IP packet"
If: C_1: "L3 DA = "[12.8.3.0]/12?" /* wildcard AND C_2: "L4 DP = 153 OR 155 OR 157 OR 159 OR 161 OR [732-789]?" /* port range AND C_3: "IP 'protocol' = '…' OR '…' … OR '…'?"	Then: A_1: "discard IP packet"

The policy rule is classified as "non-DPI" because the policy conditions are based on L3 and L4 PCI information elements only (see also clause 5.2).

II.2.1.5 Example V: "Extensive filtering"

[ITU-T H.248.76] provides a tool for defining an extensive set of filter rules per context.

II.2.2 DPI scenarios

Scenarios which contain at least one policy rule condition related to higher protocol layers above the transport layer.

II.2.2.1 Example VI: "Media type/media format policing"

There are ITU-T H.248 profile definitions for IP-to-IP gateways which support media type/media format policing. Such kind of policy rules may be addressed by specifying allowed SDP values (in the ITU-T H.248 profile section on SDP information elements).

For instance, the profile could not allow a particular list of RTP payload type values (related to a specific RTP profile type (like e.g., 'RTP/AVP' [b-IETF RFC 3551])). The ITU-T H.248 MG must then inspect the RTP header field "payload/packet type" against correspondent values. Unsupported media formats shall lead to the blocking of such RTP packets (see Table II.6). That is an example of an implicit policy rule because it is not explicitly signalled over the ITU-T H.248 interfaces, but enforced due to the successful registration of this ITU-T H.248 profile by the MG.

Table II.6 – "DPI" Example VI – "Media type/media format policing"

Policy Rule ("Media type/media format policing") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If: C_1: "L4+ protocol = RTP?" AND { C_2: "RTP PT = NOT {…*allowed values*…}?"	Then: A_1: "silently discard IP (= RTP) packet"

II.2.2.2 Example VII: "Detect application *X* of an "application-agnostic" bearer"

Figure II.3 abstracts the general framework. The created context may be e.g., transport protocol type aware, but also application agnostic according to the ITU-T H.248 signalling information (from MGC to MG) for "regular IP user plane processing".

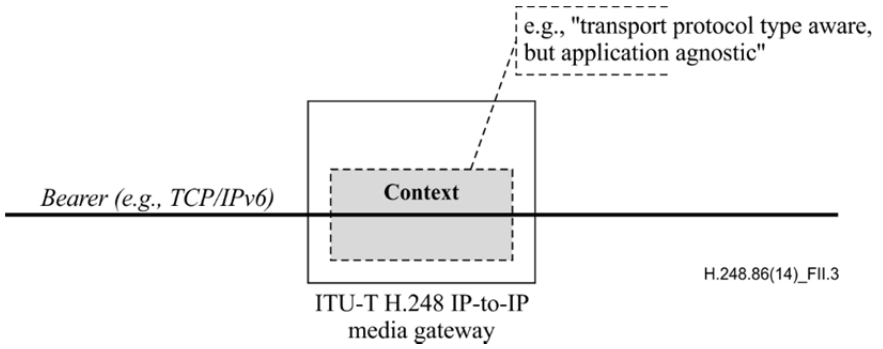


Figure II.3 – General framework for rule category of "Detect application X of an "application-agnostic" bearer"

Such a context could then be overlaid by a policy rule for the inspection of a particular application or a number of applications. Such as policy can be justified e.g., by security concerns, or to check whether users are really using that IP transport connection for the initially requested application.

The principle rule is just denoted, but not detailed in Table II.7:

Table II.7 – "DPI" Example VII – "Detect application *X* of an "application-agnostic" bearer"

Policy Rule ("Detect application *X* of an "application-agnostic" bearer") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If: C_1: "… *IP transport connection endpoint values* = 4-tuple {…}?" AND { C_2: "… *transport protocol* = …?" AND { C_3: "'application' = *X*?"	Then: A_1: "…" + possibly other actions

It may be noted that the notion of "application" shall be not limited to (IP) application protocol types only, rather every kind of "application" which may be unambiguously detected based on correspondent conditions (Note).

NOTE – Such an understanding of "application" is consistent with [ITU-T Y.2770]).

Random examples for '*X*':

a. BitTorrent

b. Skype

c. Open Game Protocol (OGP)

d. Media format (e.g., video layer)

e. Extensible Messaging and Presence Protocol (XMPP)

The chosen application types are related to peer-to-peer (P2P) file sharing (a), proprietary conversational service (b), multi-user distributed P2P (c) and e.g., an HTTP-based streaming service (d).

More, detailed policy rules for the above scenarios are indicated in clauses II.2.2.2.1 to II.2.2.2.5), which illustrate that the underlying policy conditions may be multifaceted, e.g.

– "simple" by searching for a particular bit pattern,

– "complex" by executing a regular expression on each packet,

– deterministic versus stochastic (e.g., heuristic) rule type,

– stateless versus stateful.

II.2.2.2.1 Example VIII: "Detect application *X* = 'BitTorrrent'"

This is a HTTP/TCP-based application, which may be roughly detected by looking for specific keywords (e.g., control commands), see Table II.8.

Table II.8 – "DPI" Example VIII: "Detect application *X* = 'BitTorrrent'"

Policy Rule ("Detect application *X* = 'BitTorrrent") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If: C_1: "… *IP transport connection endpoint values* = 4-tuple {…}?" AND C_2: "IP PCI 'protocol' = 'TCP'?" AND C_3: "L4+ protocol type = HTTP?" AND C_4: "http control = GET request header?" AND C_5: "http message content contains element *uploaded* with a value > 0?" AND C_6: "…"	Then: A_1: "…" + possibly other actions

II.2.2.2.2 Example IX: "Detect application *X* = 'Skype'"

Table II.9 presents an example for a bidirectional, stateful DPI policy rule. The attribute 'bidirectional' indicates that the packet flows of each communication direction needs to be inspected.

NOTE – The used rule itself illustrates just the proceeding principal, but is not necessarily sufficient for a real deployment. There are some policy rule proposals for detecting this application. This is just one out of many.

The details of the rule are minor. Relevant here is the fact that this application has an inherent session concept in terms of a state machine. The DPI policy rule here is related to that state model and associated to the session establishment phase.

Table II.9 – "DPI" Example X: "Detect application *X* = 'Skype'"

DPI Policy Rule ("Detect Skype session establishment") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
State S1: If: $C_{1,1}$: "L4 protocol = UDP?" AND $C_{1,2}$: "L4 payload size = 18?" AND $C_{1,3}$: "3rd payload byte = 0x02?"	Then: $A_{1,1}$: "save source IP transport address" $A_{1,2}$: "save destination IP transport address" $A_{1,3}$: "save first two bytes of L4 payload" Comment: The *FlowID* is based here on the 5-tuple for the UDP/IP transport connection and locally stored.
State S2: If: $C_{2,1}$: "FlowID in *reverse* direction = … (see $A_{1,1}$ / $A_{1,2}$)?" AND $C_{2,2}$: "L4 payload size = 11?" AND $C_{2,3}$: "first two bytes of L4 payload = … (see $A_{1,3}$)?" AND $C_{2,4}$: "3rd payload byte: lower nibble = 7?"	Then: none
State S3: If: $C_{3,1}$: "FlowID in *initial* direction = … (see $A_{1,1}$ / $A_{1,2}$)?" AND $C_{3,2}$: "L4 payload size = 23?" AND $C_{3,3}$: "first two bytes of L4 payload = … (see $A_{1,3}$)?" AND $C_{3,4}$: "3rd payload byte: lower nibble = 3?"	Then: none
State S4: If: $C_{4,1}$: "FlowID in *reverse* direction = … (see $A_{1,1}$ / $A_{1,2}$)?" AND $C_{4,2}$: "L4 payload size = 18?" AND $C_{4,3}$: "3rd payload byte = 0x02?"	Then: $A_{4,1}$: "report " Skype successfully detected"

II.2.2.2.3 Example X: "Detect application *X* = 'Open Game Protocol'"

This is a UDP-based application, which may be simply detected by L4+ header inspection (L_{4+}HI), see Table II.10.

Table II.10 – "DPI" Example X: "Detect application *X* = 'Open Game Protocol'"

Policy Rule ("Detect application *X* of an "application-agnostic" bearer") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If: C_1: "… *IP transport connection endpoint values* = 4-tuple {…}?" AND C_2: "IP PCI 'protocol' = 'UDP'?" AND C_3: "L4-SDU 1st 32-bit-Word = '0xFF…F'?" AND C_4: "L4-SDU 2nd 32-bit-Word = '"OGP"'?"	Then: A_1: "…" + possibly other actions

II.2.2.2.4 Example XI: "Detect application *X* = 'audio channel in a multi-channel media application'"

Chosen example: Detect second audio channel in a multi-channel AMR application and remove channel, see Table II.11.

Table II.11 – "DPI" Example XI: "Detect application *X* = 'audio channel in a multi-channel media application'"

Policy Rule ("Detect application *X* = 'audio channel in a multi-channel media application'") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If: C_1: "…" AND C_2: "…" AND C_3: "Packet contains the hexadecimal string = "0x2321414d525F4D43312E300a"?"[1] AND C_4: "next 32-bit word contains the hexadecimal string = "0x00000002"?"[2]	Then: A_1: "Discard Audio Frame within SDU" A_2: "Update Statistic" + possibly other actions

II.2.2.2.5 Example XII: "Detect & measure application *X* = 'greek Jabber traffic'"

This is a XMPP/TCP-based application, which may be simply detected by looking for XML specific control elements, see Table II.12.

---

1 = ASCII character string: "#!AMR_MC1.0\n" (see [b-IETF RFC 4867], the *magic number* for multi-channel AMR).

2 = 32 bit channel description field (see [b-IETF RFC 4867]).

Table II.12 – "DPI" Example XII: "Detect & measure application *X* = 'greek Jabber traffic'"

Policy Rule ("Detect & measure application *X* = 'greek Jabber traffic'") R_x: "…", Id = …, precedence = …	
Condition(s)	**Action(s)**
If: C_1: "… *IP transport connection endpoint values* = 4-tuple {…}?" AND C_2: "IP PCI 'protocol' = 'TCP'?" AND C_3: "L4+ header type = XMPP stream header" AND C_4: "XMPP message content contains XML element = "`xml:lang='gr'`"	Then: A_1: "…" + possibly other actions

For the subsequent examples, the DPI policy rule indications are omitted.

II.2.2.3 Example XIII: "TCP attack detection"

There are existing ITU-T H.248 profiles for IP-to-IP gateways which support TCP-based applications (e.g., with [ITU-T H.248.84] NAT traversal support for TCP traffic). Such a gateway may principally located at the edge of a security domain, and then requested to enforce some policy rules for well-known TCP attack scenarios (see also clause 9 of [ITU-T H.248.79]).

This is not necessarily a DPI scenario ("the very majority of TCP threat scenarios are related to L3/L4 header inspection, thus rather "non-DPI""), but the correspondent policy conditions are typically "statefull" (because the inspection may cover multiple TCP/IP packets and the MG may need to execute through the TCP connection state machine).

II.2.2.4 Example XIV: "Remove invalid MIME attachments from Instant Messaging"

A user may be subscribed to an Instant Messaging (IM) service, realized here as the "MSRP-over-TCP" application. The IM service allows the transmission of "attachments", which may be encapsulated via MIME ("the low level details are not important here"). The user may be not allowed to issue via his IM client dedicated attachment types. The IM service may be "end-to-end", i.e., without a MSRP relay or switch node. The ITU-T H.248 MG may be thus requested to inspect MIME attachment types (because e.g., the only "IP hop" instance where all bearer traffic is routed across).

This example relates to a DPI policy rule because besides the TCP header verification, there might be policy conditions related to the

– MSRP header,
– MSRP body 'text',
– MSRP body embedded MIME attachment types,
– etc. ("e.g., MIME itself is recursive, which allows to consider MIME-over-MIME …")

II.2.2.5 Example XV: "RTCP Block Type Filtering"

With [ITU-T H.248.48] based network applications RTCP block type filtering may be needed (see clause 3.2.1 of [ITU-T H.248.48]). Appendix I in [b-ITU-T H.248.RTCPPROF] illustrates a number of example use cases with "RTCP filtering". E.g., provider *A* wants to block the distribution of own RTCP-based measurement data to other, peering provider partners.

Such DPI policy conditions for measurement data filtering may look like:

– RTCP report: PT = x_1, BT = x_2, Field = "..."

In other words, firstly the packet type value is checked, then block type value, then a particular field within a block, and if all conditions are true, then the action may be to remove the correspondent metric or to reset the value to default, and to recalculate PCI on all affected protocol layers (e.g., UDP checksum recalculation).

II.2.2.6 Example XVI: "Application-specific traffic handling"

The notion of 'handling' shall indicate other possible action types like just "packet accept" or "packet discard" actions.

For instance, action types like:

– create packet copy and …;

– send alert (e.g., ITU-T H.248 Notify to MGC);

– modify IP header DS/ToS/TC values ("[b-ITU-T H.248.52] like");

– etc.

A principal classification of DPI policy rule actions is described in clause 6.3.3 in [ITU-T Y.2770], which are all relevant as well for this appendix.

II.2.2.7 Example XVII: "Abnormal packet size detection"

This example is similar to example I (clause I.2.1.1), but the difference may be related to another protocol layer (above L4). E.g., multiple application layer PDUs may be assembled in a single IP packet.

The example may be generalized to "abnormal traffic detection", with correspondent policy conditions for specific traffic characteristics. Related information is provided by [b-ITU-T X.Sup18] and clause 6.4.3 of [ITU-T Y.2770].

II.2.2.8 Example XVIII: "Delete old packets of application *X*"

The notion of 'old' shall be related to the IP header TTL value. The specific example here may illustrate that the condition

"*IP PCI "TTL" < y?*"

would be tied to a pre-condition of

"*'application' = X?*".

It may be observed that policy rules themselves may be hierarchical, like e.g., conditions embedded in another condition, or an action may refer again to another policy rule, etc.

Appendix III

ITU-T H.248 aspects for signalling DPI policy rules

(This appendix does not form an integral part of this Recommendation.)

III.1 Overview of principal signalling methods

The following principle signalling methods for policy rules may be identified:

1 Explicit rule signalling

1.1 Explicit rule in native ITU-T H.248 syntax

1.2 Explicit rule encapsulated in container over ITU-T H.248

2 Signalling of pointer to rule and rule MG-locally provisioned

3 Signalling of pointer to rule and rule MG-remotely provisioned

Figure III.1 outlines three examples for policy rules signalled between a policy decision point (here MGC) and policy enforcement point (here MG).

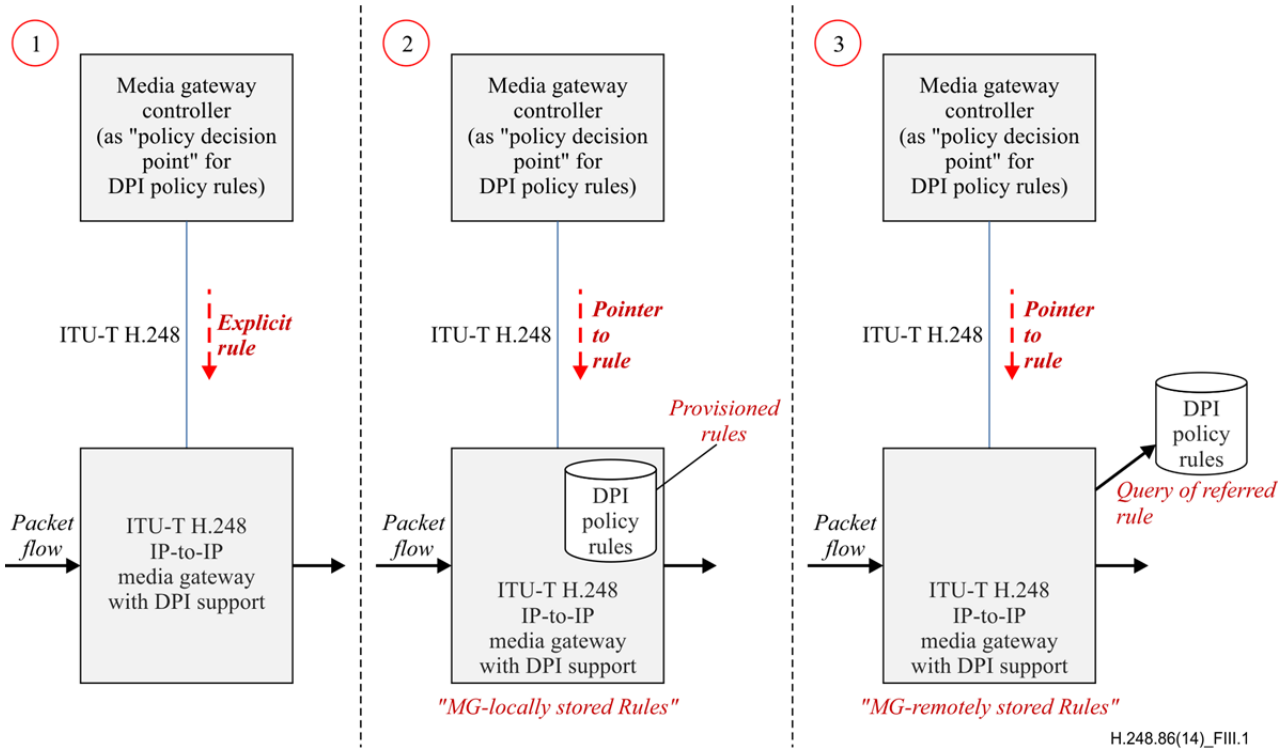


Figure III.1 – Principle signalling methods for policy rules

The high-level principle behind each method is as follows.

Option (1):

– the complete rule is carried by a single ITU-T H.248 command.

Option (2):

– the ITU-T H.248 command carries a 'pointer' (which relates to an "identifier for a rule"; also known as the "reference" principle in [ITU-T H.248.69]),

– the rule would be already available in a MG local data base,

– the identifier correlates rule and correspondent ITU-T H.248 context/termination/stream.

Option (3):

– as in (2), the ITU-T H.248 command carries a 'pointer' (which relates to an "identifier for a rule"),

– the rule would be already available in a MG remote data base,

– the MG issues a query to that data base for requesting the rule,

– the interface between MG and remote data base is "non-H.248" based (and is out of scope of ITU-T H.248.x-series of Recommendations),

– the downloaded rule is assigned to ITU-T H.248 context/termination/stream.

Method (1) may be further categorized see Figure III.2:

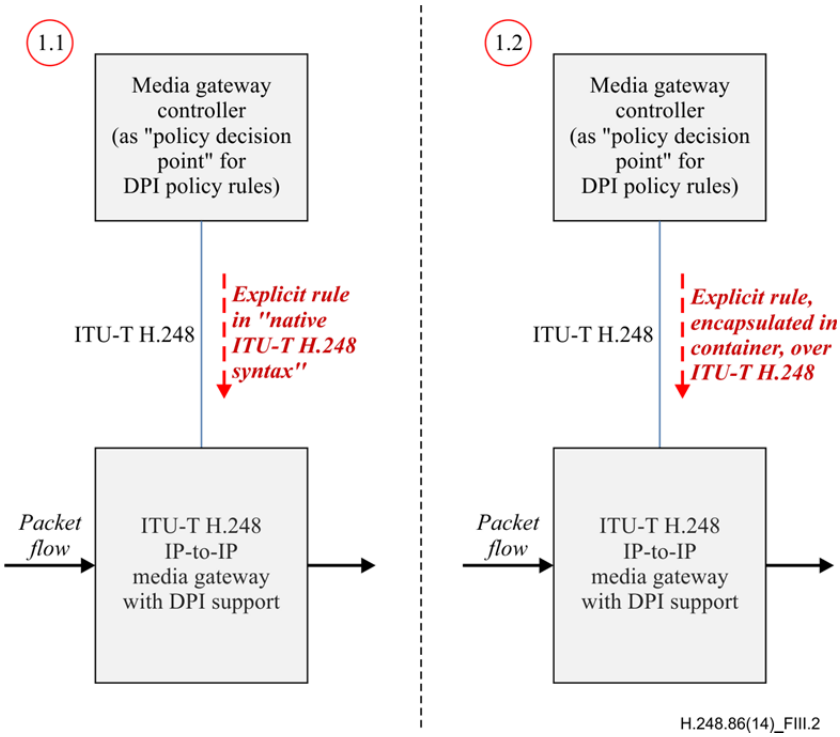


Figure III.2 – Two sub-options for the first method

Sub-option (1.1):

– the rule is encoded in native ITU-T H.248 syntax, i.e., based on (existing or new) ITU-T H.248 properties, events, signals, and/or statistics, including error codes.

Sub-option (1.2):

– the rule itself is specified in a non-H.248 language (also known as *policy specification language (PSL)*, see Appendix IV),

– ITU-T H.248 provides support of a "container" for carrying the rule,

NOTE – A "container" relates to a data object in general. The container principle is already used by some ITU-T H.248 packages. See e.g., the *data block* property in [b-ITU-T H.248.45].

The several options are not mutually exclusive. Multiple options could be principally applied in parallel, which implies a carefully evaluation of possible interaction issues.

III.2 H.248 support

Table III.1 summarizes present ITU-T H.248 capabilities for support of the outlined methods.

Table III.1 – Signalling methods versus ITU-T H.248 support

Method	Present ITU-T H.248 support	Comment/reference
1.1	Not supported. [Primarily due to the existence of sufficient PSLs with DPI policy rule specification support, see Appendix IV.]	Main advantage would be a tight coupling and alignment with existing ITU-T H.248 protocol elements (see e.g., clause 6.2).
1.2	Supported by *inspection rule base* package, *container for rule* property.	See clauses 7.1.2 and 7.6.1.2
2	Supported by *inspection rule base* package, *pointer to rule conditions* property.	See clauses 7.1.1 and 7.6.1.3
3	Support, as method 2.	See clauses 7.1.1 and 7.6.1.4

Appendix IV

Discussion on policy specification languages

(This appendix does not form an integral part of this Recommendation.)

IV.1 Introduction

This appendix provides complementary information on *policy specification languages* (PSLs), also known as *policy expression languages* (PELs) or *filter specification languages* (FSLs). The definition of a PSL is out of scope of this Recommendation. However, the question of PSLs is related here to multiple network interfaces, like a *control plane* policy control interface between a remote policy decision function and the DPI node function and a *management plane* policy management interface between network (policy) management functions and the DPI node function. There are thus inherent protocol requirements across multiple, different network interfaces concerning the "transport[3] of policy rule sets" down to the DPI-FE (see also Figure IV.1).

NOTE – This appendix only illustrates how PSL 'SNORT' might be used in combination with this Recommendation, but does not specify concrete usage.

IV.2 PSL for policy control and policy management interfaces

Figure IV.1 provides a summary of a typical network scenario. The policy operations by the control plane and network plane address the same objects of the policy enforcement path in the user plane. Thus, an aligned PSL usage across all relevant interfaces would be crucial for efficient DPI node functions.

[3] E.g., via high-level push mode or pull mode operations between policy decision entities and the policy enforcement processing path.

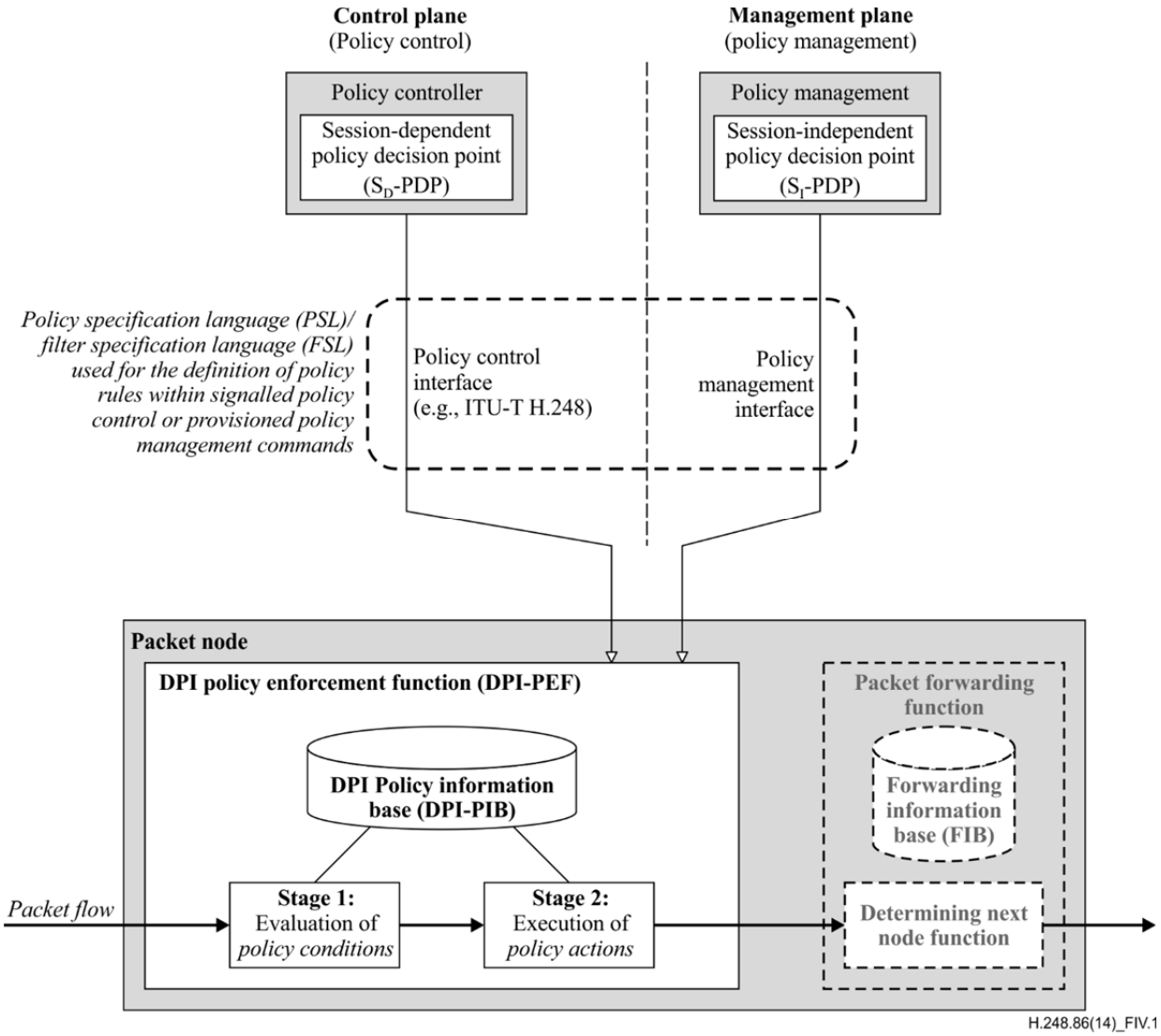


Figure IV.1 – Policy specification language (PSL) – PSL for policy control and policy management interfaces

IV.3 Survey of possible PSLs (non-exhaustive list)

(DPI) policy rules are enforced on *Protocol Data Units* (PDU) in general, briefly called packets in this appendix. The *objects* of DPI are therefore parts of or entire PDUs. A PSL must consequently provide a means of specification for the definition of such objects ("*data structure*") and methods executed on these objects (i.e., "*operations*", related to policy conditions and policy actions). Table IV.1 provides a list of example standardized protocols (Note), which may be candidates for DPI-capable PSLs. The example PSLs provide initial support for the specification of such *data objects* or/and considered *operations*.

NOTE – There may also be proprietary protocols, particularly for management interfaces (like command line interfaces (CLI) or man-machine interfaces (MMI)).

Table IV.1 – Example list of policy specification languages (PSLs) (also known as policy expression languages (PELs) or filter specification languages (FSLs))

No	Policy specification language	Reference
1	SNORT	[b-SNORT]
2	SAML – Security Assertion Markup Language (SAML 2.0)	[b-ITU-T X.1141]
3	XACML – eXtensible Access Control Markup Language (XACML 2.0)	[b-ITU-T X.1142]
4	Open Service Access (OSA) Application Programming Interface (API); Part 13: Policy management Service Capability Feature (SCF)	[b-3GPP 29.198-13]
5	SIEVE – An Email Filtering Language	[b-IETF RFC 5228]
6	BPEL – Business Process Expression Language	[b-OASIS BPEL]
7	BPML – Business Process Modeling Language	[b-OMG BPML]
8	XCAP – XML Configuration Access Protocol	[b-IETF RFC 4825]
9	PEEM Policy Expression Language (by Open Mobile Alliance)	[b-OMA PEEM]
10	PacketTypes	[b-PacketTypes]
11	APF – A Packet Filter	[b-APF]
12	RTAG – Real-Time Asynchronous Grammars	[b-RTAG]
13	TAP/APC – Timed Abstract Protocol & Austin Protocol Compiler	[b-TAP]
14	GAPAL – Generic Application-Level Protocol Analyzer and its Language	[b-GAPAL]
15	Perl (Compatible) Regular Expressions	
16	POSIX Regular Expressions	
17	others	

IV.4 PSLs on different network levels

It may be worth to consider PSLs on different network levels. There may be very high-level PSLs with focus on behavioural policy definitions, using natural languages. On the other side could be low-level PSLs, close to the program code ("e.g., configurations of policy rules at API level") of packet-path processing components for policy enforcement (e.g., ASIC, FPGA, network processor, general purpose CPU), using a formal specification approach, which is also a prerequisite for the detection of possible rule interaction problems.

Figure IV.2 illustrates some examples for policy rule specifications.

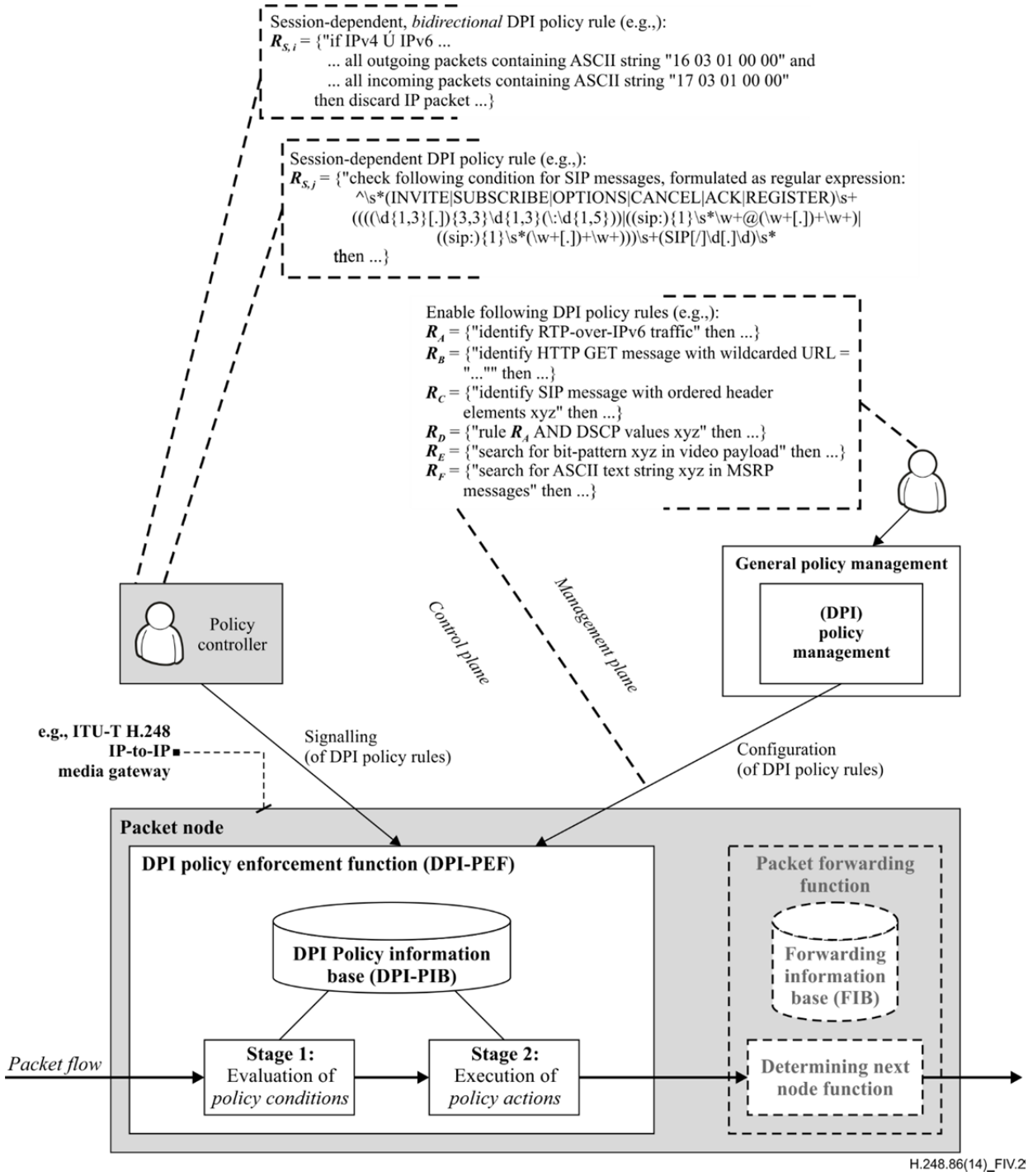


Figure IV.2 – Policy specification languages – Example (DPI) policy rules (on different network levels)

IV.5 Recommendations for selected PSLs

Figure IV.3 outlines a possible PSL architecture concept, which would satisfy the requirements of:

(R1) *single*, aligned PSL for policy control and policy management;

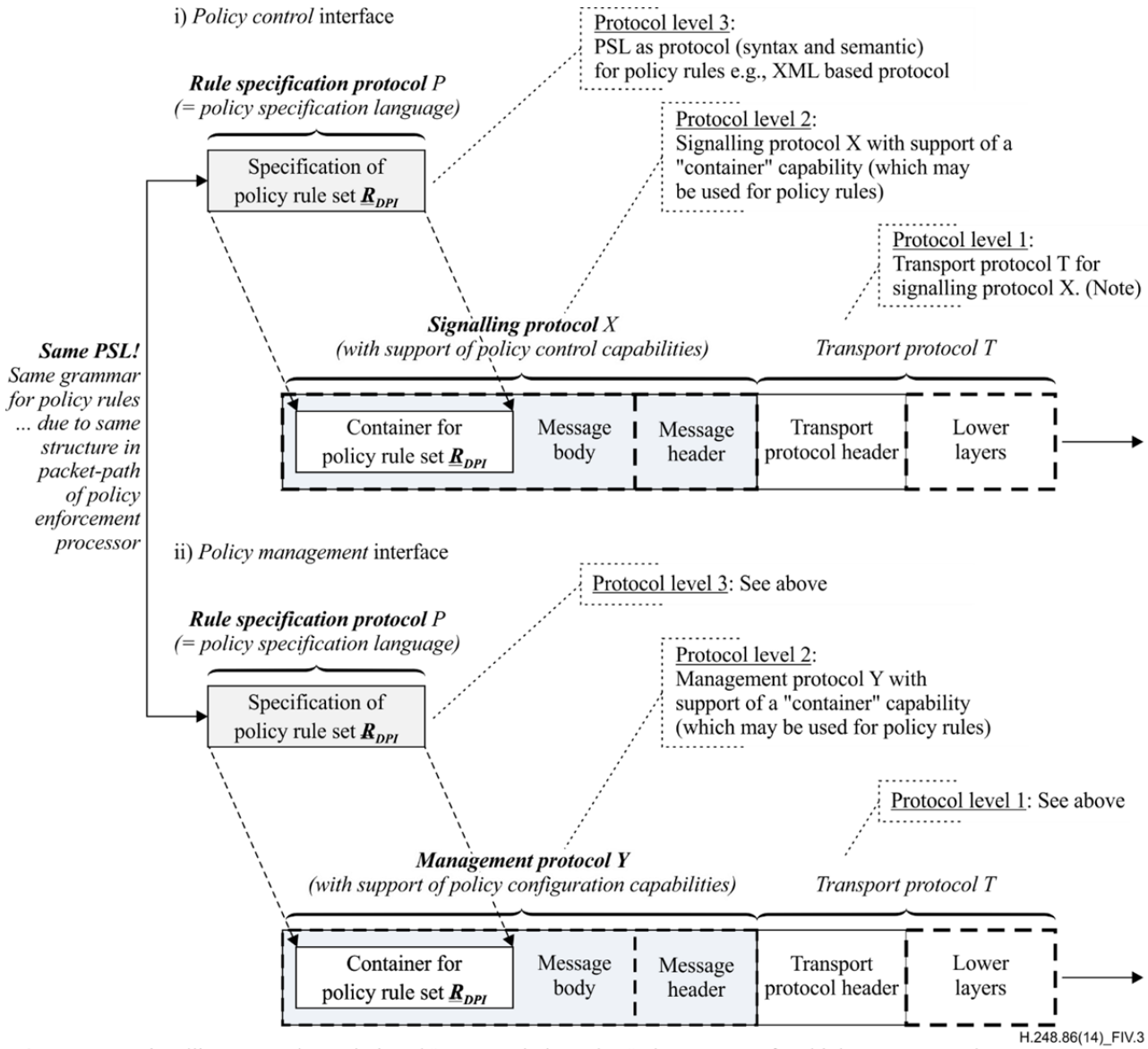
(R2) PSL *decoupled* from a control plane *signalling protocol*, thus PSL-independent of a dedicated signalling protocol;

NOTE – The concept is already well established in many protocols, the principle is equal to the "MIME concept for electronic mail", i.e., a *multipurpose extension* capability by the "carrier protocol". A "multipurpose extension" mechanism would also allow different PSL types.

(R3) PSL *decoupled* from a management plane *protocol*, thus PSL-independent of a dedicated *management protocol*;

(R4) the specification of a Policy Rule set $\underline{\underline{R}}_{DPI}$ (but also $\underline{\underline{R}}_{non\text{-}DPI}$) would be embedded in a container of the underlying signalling or management protocol;

(R5) alignment of object models and information bases (e.g., between PIBs on PEF-level and policy decision/management entities).



NOTE – Many signalling protocols are designed "transport-independent", thus support of multiple transport modes.

Figure IV.3 – Policy specification languages – Possible PSL architecture concept

Figure IV.3 shows an abstract rule specification protocol *P* (as PSL), which is preferably used by network entities in the control and management plane. Any aligned PSL leads to aligned PIBs. Any Policy Rule set $\underline{\underline{R}}_{DPI}$ is carried by signalling (*X*) or management (*Y*) protocols.

IV.6 Discussion of policy specification language candidates

Appendix III highlights possible mechanisms for signalling the policy rules to the MG. The principal options are again:

1. Explicit rule signalling

   1.1 Explicit rule in native ITU-T H.248 syntax

1.2 Explicit rule encapsulated in container over ITU-T H.248

2. Signalling of pointer to rule and rule MG-locally provisioned

3. Signalling of pointer to rule and rule MG-remotely provisioned

From an analysis of the DPI scenarios (Appendix II) it can be determined that the breadth and complexity of the scenarios do not lend themselves to option 1.1. Using multiple properties and multiple Contexts/Termination would be problematic and overly complex.

This leaves options 1.2, 2 and 3 as a possible means to signal policy rules for the illustrated scenarios. In terms of signalling, option 2 and 3 are essentially the same as they are simple pointers to an existing rule set. These three options are all supported by the *instruction rule base* package (clause 7).

In order to make this choice one must consider how the rule set is specified (i.e., what is the policy specification language (PSL)?) and what framework it is specified in. In order to determine an appropriate PSL the candidate PSLs must be compared to the scenario list to see if the functionality can be supported.

Preferentially, a single PSL should be used by ITU-T H.248 applications using this Recommendation. This would increase interoperability between implementations. It is expected that ITU-T H.248 profile specifications will define allowed PSLs for the particular network operation.

An example of an open source system is SNORT [b-SNORT], see clause IV.7.

IV.7 Example PSL "SNORT" – Analysis and comments

SNORT is considered to be a good candidate for the PSL in ITU-T H.248-based DPI applications. SNORT has many benefits:

1. SNORT is open source and is already used in many products.

2. There is a large base of existing rules that may be applied to address known vulnerabilities.

3. There is a large address space for proprietary/custom rules (approximately one million IDs).

4. There is an extensive community updating and developing new rules.

The SNORT PSL can be found in Section 3 of the SNORT Manual [b-SNORT].

IV.7.1 Signalling

SNORT is a text based PSL and thus lends itself to being potentially carried in ITU-T H.248 commands as a string (i.e., using property *irb*/*cfr*; see clause 7.1.2). It also defines a Snort Rule ID (*sid*) that allows a unique identification of each rule, which lends itself to being used as a pointer in an ITU-T H.248 command (e.g., information used in property *irb*/*ptr* (see clause 7.1.1) or reported via event *iro*/*src*; see clause 8.2.1). Thus SNORT would not prevent the signalling options 1.2, 2 and 3 (indicated above) from being supported.

IV.7.2 Structure

Figure III.1 outlines a generic high-level format of a policy rule, identifier/name part, condition part and action part.

The SNORT PSL provides several elements that enable clear identification and version handling. The Snort Rule identifier (sid) as mentioned above allows a unique identification of SNORT rules. For version handling the Revision (rev) element can be used. The Reference (reference) element can provide further information regarding the definition of a set of rules. The Priority element (priority) may be assigned to the rule in order to prioritise one rule over another.

SNORT rules consist of a rule header and rule options. As indicated in [b-SNORT]:

"Snort rules are divided into two logical sections, the rule header and the rule options. The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information. The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken."

So, whilst the rule structure itself does not follow Figure III.1 strictly, it does allow conditions and actions to be specified.

IV.7.3 Rule conditions: Comment to address information

SNORT currently supports the TCP, UDP, ICMP and IP protocols. The IP address, port and source and destination (direction indicator) information is carried in the SNORT rule header. ITU-T H.248 supports the sending of this information via Termination/Stream configuration and the Local and Remote Descriptors. This implies certain alignment of such address information between enforced SNORT rules and ITU-T H.248 non-root terminations.

IV.7.4 Rule actions: general SNORT concept

SNORT defines a rich set of actions (see 3.2.1 of [b-SNORT]), including:

– alert – generate an alert using the selected alert method, and then log the packet
– log – log the packet
– pass – ignore the packet
– activate – alert and then turn on another dynamic rule
– dynamic – remain idle until activated by an activate rule , then act as a log rule
– drop – block and log the packet
– reject – block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
– sdrop – block the packet but do not log it.

SNORT allows the logging and alerting of events. The served user instance for such information might be basically a policy server/controller/manager in the network control or/and management plane (see also clause 6.3). These SNORT events would be part of performance management and alarm/security management in case of management plane usage. In case of control plane, then there are relations to ITU-T H.248 statistics and ITU-T H.248 event reporting (see clause 8). Any detailed mapping between SNORT and ITU-T H.248 is out of scope of this Recommendation (e.g., part of an ITU-T H.248 profile specification; see also clause V.2).

IV.7.5 Rule conditions: principal inspection process

SNORT defines many detection rule options. These are effectively classified into three groups:

1. Content detection rule option
2. Non-payload detection rule option
3. Post-detection rule options

The elements contained in these groups allow complex filtering behaviour to be specified.

Appendix II outlines a number of DPI scenarios. Table IV.2 summarizes a brief discussion of SNORT support.

Table IV.2 – Examples (from appendix) versus principal SNORT support

No.	Example name	SNORT
VI	Media type/media format policing	The "content" element with associated content modifier allow would allow a rule to be specified to look at the bits associated with the payload type field and to see whether they matched an allowed value/s.
VII	Detect application X of an "application-agnostic" bearer	The example indicates several different methods for determining applications. In the generic example it can be seen that SNORT allows simple bit pattern searching. SNORT also allows complex regular expression matching utilising the "*pcre*" element (section 3.5.23 in [b-SNORT]). Heuristic analysis is supported via multiple rules and dynamic rule specification. NOTE – There is an active community defining rules for well-known and emerging attack signatures.
VIII	Detect application X = 'BitTorrent'	SNORT has several elements that deal with searching and matching in HTTP bodies. I.e., "http_method" (section 3.5.13 of [b-SNORT]) and "http_client_body" (section 3.5.8 of [b-SNORT]).
IX	Detect application X = 'Skype'	SNORT allows a stateful based rule definition approach. It is possible that one rule triggers another. It is also possible to extract information via one rule and save it for use in another rule (i.e., through the use of the "byte_extract" (section 3.5.29 of [b-SNORT])).
X	Detect application X = 'Open Game Protocol'	SNORT may achieve this through simple pattern matching.
XI	Detect application X = 'audio channel in a multi-channel media application'	Whilst SNORT may allow the detection of the condition it is currently unclear whether it can support the removal of an audio frame within an SDU. SNORT does have the "replace" element that can be utilised for simple replacement of data (where length can be maintained). However removal of payload data has implications for checksums etc. Further investigation is needed.
XII	Detect & measure application X = 'greek Jabber traffic'	SNORT may achieve this through simple pattern matching.
XIII	TCP attack detection	SNORT allows the detection of TCP attacks. It has several elements dedicated to TCP checks, i.e., the elements "flags", "flow", "flowbits", "seq", "ack" and "window" from section 3.6 of [b-SNORT]).
XIV	Remove invalid MIME attachments from Instant Messaging	As per example XI. SNORT support for selective removal of payload information is for further study.
XV	RTCP Block Type Filtering	As per example XI. SNORT support for selective removal of payload information is for further study.
XVI	Application-specific traffic handling	As discussed in section IV.7.4 above SNORT has several defined actions but also allows user defined actions.
XVII	Abnormal packet size detection	The SNORT element "dsize" (section 3.6.7 of [b-SNORT]) allows the testing of packet payload size.
XVIII	Delete old packets of application X	The SNORT element "ttl" (section 3.6.2 of [b-SNORT]) allows the testing of the time to live for a packet.

Appendix V

Emulation of DPI policy rule control interfaces

(This appendix does not form an integral part of this Recommendation.)

V.1 Purpose

Appendix IV provides an overview of known policy specification languages (PSLs). The behaviour of some of such PSLs could be principally emulated by ITU-T H.248 based policy control interfaces. Such an emulation of DPI policy rule control interfaces would be based on ITU-T H.248 capabilities as defined by this Recommendation and other ITU-T H.248.x-series of Recommendation, depending on the aimed set of DPI policy rules.

The purpose of this appendix is to provide principal indications and high-level information on how such a DPI policy rule emulation could work. The concrete specification of such ITU-T H.248 interface behaviour is out of scope of this appendix, rather considered to be subject of ITU-T H.248 profile definitions.

Two examples are discussed.

V.2 Guidelines for ITU-T H.248 profile specifications using native SNORT interfaces as an example

V.2.1 Motivation

Benefit from the huge base of existing SNORT based DPI policy rules.

V.2.2 Scope

[b-SNORT] defines the syntax for SNORT DPI policy rules, following a common structure of rule header and rule options, which again comprises the rule conditions and rule actions.

V.2.3 Possible emulation by ITU-T H.248

Table V.1 provides an example approach for emulating the behaviour by ITU-T H.248:

Table V.1 – Emulation approach of SNORT policy rules by ITU-T H.248

SNORT	Generic information element	Possible ITU-T H.248 solution
SNORT rule	Entire DPI policy rule object	Either reference- or container-based emulation, i.e., using property "Pointer to rule conditions" (*irb*/*ptr*), see clause 6.1.1, or property "Container for rule" (*irb*/*cfr*), see clause 6.1.2).

V.3 Guidelines for ITU-T H.248 profile specifications using 3GPP Diameter interfaces as an example

V.3.1 Motivation

There are e.g., the following reasons:

– There are multiple protocol options (ITU-T H.248, COPS and Diameter) for support of the ITU-T *Rw* policy control interface [b-ITU-T Y.2111]. Prerequisite (for protocol selection) is the functional parity between the different protocol alternatives. I.e., using ITU-T H.248 implies the same service as supported by Diameter.

– The policy decision entity in the ITU-T RACF architecture needs to map policy control information from the northbound *Rs* to the southbound *Rw* interface (see Figure 9 of [b-ITU-T Y.2111]). Diameter may be used for *Rs*, whereas an ITU-T H.248 based *Rw* interface is very common at policy enforcement level. Hence, ITU-T H.248 emulates in some way Diameter in such a mapping scenario.

V.3.2 Scope

[b-ETSI TS 129 212] defines a Diameter object with support of DPI policy rule signalling, called *Application Detection and Control* (ADC) rule. It contains primarily a set of possible rule actions, without any support of explicit rule conditions, which are referred by a pointer mechanism (see clause 4.3b of [b-ETSI TS 129 212]).

V.3.3 Possible emulation by ITU-T H.248

Table V.2 provides an example approach for emulating the behaviour by ITU-T H.248.

Table V.2 – Emulation approach of Diameter ADC policy rule by ITU-T H.248

ADC-Rule-Definition AVP	Generic information element	Possible ITU-T H.248 solution
ADC-Rule-Name	Name of DPI policy rule	No support required (Note 1).
TDF-Application-Identifier	Pointer to actual rule conditions	Property "Pointer to rule conditions" (*irb*/*ptr*), see clause 7.1.1.
Flow-Status	Policy rule action related to gate control (Note 2)	Either implicit in the policy rule specification itself, or/and (complemented) by ITU-T H.248 gate control means (e.g., [ITU-T H.248.43]).
QoS-Information	Policy rule action related to traffic policing (Note 3)	Either implicit in the policy rule specification itself, or/and (complemented) by ITU-T H.248 traffic policing tools (e.g., [ITU-T H.248.53]).
Monitoring-Key	Identifier for policy rule actions, related to usage parameter control across an aggregated traffic structure	Such an aggregated traffic structure could be emulated by e.g., a multiple-stream-to-termination mapping in ITU-T H.248.
Redirect-Information	Policy rule action related to traffic redirection	Either implicit in the policy rule specification itself, or/and by ITU-T H.248 support for explicit IP destination/source (transport) address setting capabilities (e.g., [ITU-T H.248.43]).
NOTE 1 – Only name of the specific "application detection service". NOTE 2 – Relation to *StreamMode* and [ITU-T H.248.43] properties to be clarified. NOTE 3 – Relation to [ITU-T H.248.53] properties to be clarified.		

Bibliography

[b-ITU-T H.248.39] Recommendation ITU-T H.248.39 (2006), *Gateway control protocol: H.248 SDP parameter identification and wildcarding*.

[b-ITU-T H.248.45] Recommendation ITU-T H.248.45 (2006), *Gateway control protocol: MGC information package*.

[b-ITU-T H.248.52] Recommendation ITU-T H.248.52 (2008), *Gateway control protocol: QoS support packages*.

[b-ITU-T H.248.87] Recommendation ITU-T H.248.87 (2014), *Guidelines on the use of ITU-T H.248 capabilities for performance monitoring in RTP networks in ITU-T H.248 Profiles*.

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

[b-ITU-T X.1142] Recommendation ITU-T X.1142 (2006), *eXtensible Access Control Markup Language (XACML 2.0).*

[b-ITU-T X.Sup18] Supplement 18 to ITU-T X.series (2013), *ITU-T X.1205 – Supplement on guidelines for abnormal traffic detection and control on IP-based telecommunication networks*.

[b-ITU-T Y.2111] Recommendation ITU-T Y.2111 (2011), *Resource and admission control functions in next generation networks.*

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.Sup 23] Supplement 23 to ITU-T Y-series Recommendations (2013), *Supplement on DPI terminology*.

[b-ETSI TS 129 212] ETSI TS 129 212 (2013), *Universal Mobile Telecommunications System (UMTS); LTE; Policy and Charging Control (PCC); Reference points (3GPP TS 29.212 version 10.10.0 Release 10)*.

[b-IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[b-IETF RFC 3551] IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal Control*.

[b-IETF RFC 4825] IETF RFC 4825 (2007), *The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)*.

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

[b-3GPP 29.198-13] 3GPP Open Service Access (OSA) *Application Programming Interface (API*), *Part 13: Policy management Service Capability Feature (SCF)*.

[b-APF] H.D. Lambright & S.K. Debray. APF: *A modular language for fast packet classification*. Dept of Computer Science, University of Arizona, Tucson, August 30, 1996.
<http://www.cs.arizona.edu/~debray/Publications/filter.html>

[b-GAPAL] N. Borisov, D.J. Brumley, and H.J. Wang, *Generic Application-Level Protocol Analyzer and its Language*. Proceedings of the Network and Distributed System Security Symposium, NDSS 2007, San Diego, USA, 2007.

[b-OASIS BPEL] OASIS Standard BPEL (2007), *Web Services Business Process Execution Language Version 2.0*. http://www.oasis-open.org/specs/index.php #wsbpelv2.0

[b-OMG BPML] Object Management Group (OMG) BPML (2002), *Business Process Modeling Language Version 1.0*. http://www.bpmi.org/bpml-spec.htm

[b-OMA PEEM] Open Mobile Alliance OMA-TS-PEEM_PEL-V1 (2007), *PEEM Policy Expression Language Technical Specification", Draft Version 1.0*.

[b-PacketTypes] P.J. McCann, S. Chandra, *PacketTypes: Abstract Specification of Network Protocol Messages*. In SIGCOMM '00: Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pages 321-333, New York, NY, USA, 2000. ACM Press.

[b-RTAG] D.P. Anderson & L.H. Landweber, *A grammar-based methodology for protocol specification and implementation.* In SIGCOMM '85: Proceedings of the ninth symposium on Data communications, pages 63−70, New York, NY, USA, 1985. ACM Press.

[b-SNORT] *SNORT Manual.* http://www.snort.org/assets/166/snort_manual.pdf

[b-TAP] T. McGuire, *The Austin Protocol Compiler*. http://apcompiler.sourceforge.net/

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2014