International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.61

(03/2009)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Gateway control protocol: Packages for network level H.248 statistics

Recommendation ITU-T H.248.61

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
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

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

Recommendation ITU-T H.248.61

Gateway control protocol: Packages for network level H.248 statistics

Summary

Recommendation ITU-T H.248.61 defines H.248 Packages for network level statistics for the Internet Protocol. The IP layer octets count statistics Package is used to support explicit octet count statistics on the Internet Protocol layer. The IP layer packets count statistics Package is used to support explicit packet count statistics on the Internet Protocol layer. The IP traffic flow of an IP-based H.248 Stream or Termination may be either IPv4 or IPv6.

Source

Recommendation ITU-T H.248.61 was approved on 16 March 2009 by ITU-T Study Group 16 (2009-2012) under Recommendation ITU-T A.8 procedures.

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/.

CONTENTS

Recommendation ITU-T H.248.61

Gateway control protocol: Packages for network level H.248 statistics

1 Scope

1.1 Introduction to areas with usage of H.248 statistics

H.248 statistics are defined and used for different purposes. There are four major categories identified, see clause 1.1 of [ITU-T H.248.58].

1.2 Scope of H.248 statistics defined by this Recommendation

The scope of this Recommendation is related to H.248 statistics defined, in particular, for measurements on the network protocol layer. A potential application is the validation of network capacity allocations.

Figure 1 illustrates the different scope of several packages with octets count statistics on different protocol layers. The IP layer octets count statistics package provides statistics on Internet Protocol (IP) layer.

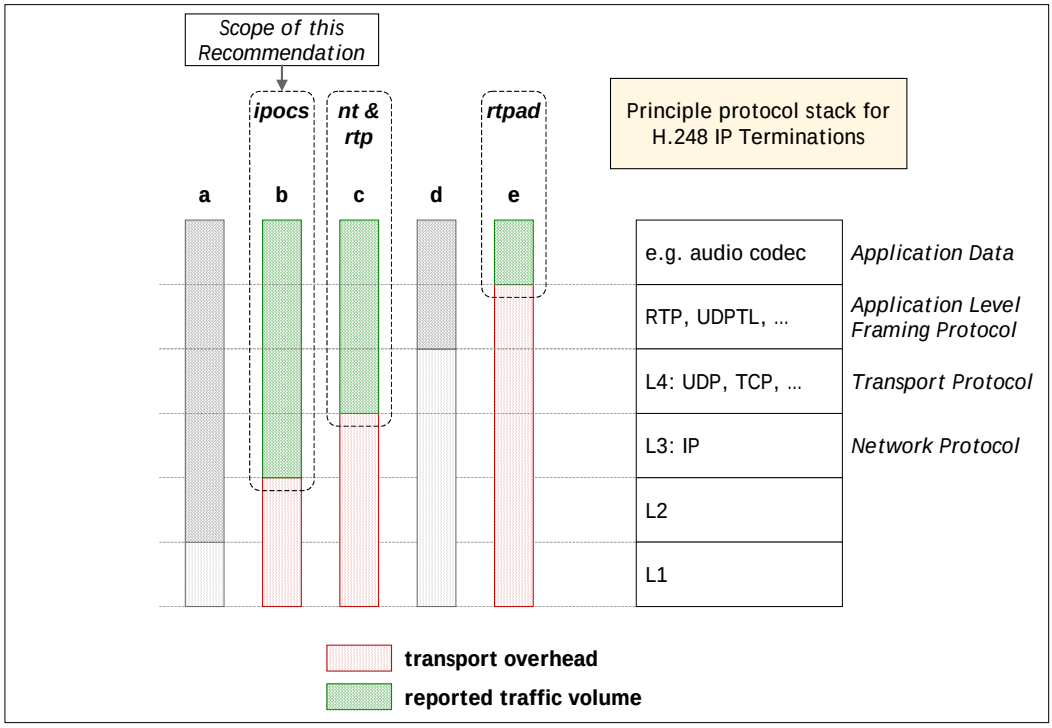

Figure 1 – Semantics of the ipocs package versus rtpad package and nt and rtp packages

The ipocs package provides complementary statistics with regard to other packages for octets count measurement of different protocol layers.

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 (2005), *Gateway control protocol: Version 3*, including its Amendment 1 (2008).

[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.248.53] Recommendation ITU-T H.248.53 (2008), *Gateway control protocol: Traffic management packages*.

[ITU-T H.248.58] Recommendation ITU-T H.248.58 (2008), *Gateway control protocol: Packages for application level H.248 statistics*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 flow (see clause 3.3 of [b-ITU-T Y.2121]): A unidirectional sequence of packets with the property that, along any given network link, a flow identifier has the same value for every packet.

3.1.2 flow identifier (see clause 3.6 of [b-ITU-T Y.2121]): A vector (or n-tuple) comprising the values of a number of elements taken from the IP, TCP/UDP header fields, encapsulation header, and label fields attached to a packet. The flow identifier for a flow within a single IP network is unique.

3.1.3 measurement point (see clause 3.9 of [b-ITU-T M.2301]): The physical or logical point at which measurements can be made and to which the data obtained is related.

3.1.4 IP bearer (see clause 3.1 of [b-ITU-T Q.1970]): A bidirectional user plane association between two BIWFs for carrying media stream information across IP networks. An IP bearer is an instance of a backbone network connection (BNC) type defined in clause 3 of [b-ITU-T Q.1902.1].

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 lookup-key: Flow identifier elements that can be used for packet classification with regard to H.248 Context delivery.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

'QoS' Codepoint for 'QoS' (e.g., DSCP, IPv4 ToS, IPv6 TC)

B2BIH Back-to-Back IP Host (mode)

BIWF Bearer Interworking Function

BNC	Backbone Network Connection
CDIB	Context Delivery Information Base
DA	(L2 or L3) Destination Address
DP	(L2 or L3) Destination Port
FlowID	Flow Identifier (in general) or IPv6 Flow Label (in case of L3-FlowID)
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPR	IP Router (mode)
L2VPN	Layer 2 Virtual Private Network
LCD	(H.248) LocalControl Descriptor
LD	(H.248) Local Descriptor
LSP	(MPLS) Label Switched Path
Lx	Protocol Layer x
MD	(H.248) Media Descriptor
MG	Media Gateway
MGC	Media Gateway Controller
MP	Measurement Point
MPLS	MultiProtocol Label Switching
NAT	Network Address Translation
nt	Network Package (clause E.11 of [ITU-T H.248.1])
OSPF	Open Shortest Path First (routing protocol)
PDU	Protocol Data Unit
PROT	(Upper Layer) Protocol
PT	(RTP) Payload Type; (RTCP) Packet Type
RD	(H.248) Remote Descriptor; Remote Destination (IP connection endpoint)
RS	Remote Source (IP connection endpoint)
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
rtp	RTP Package (clause E.12 of [ITU-T H.248.1])
rtpad	RTP Application Data Package [ITU-T H.248.58]
SA	(L2 or L3) Source Address
SD	(H.248) Stream Descriptor
SDP	Session Description Protocol

SP	(L2 or L3) Source Port
SSRC	(RTP) Synchronization Source
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UDPTL	(Facsimile) UDP Transport Layer Protocol
VERS	(L3, IP) Version
VPNID	Virtual Private Network Identifier

5 Conventions

None.

6 IP Layer Octets Count Statistics Package

Package Name: IP Layer Octets Count Statistics Package

Package ID: ipocs (0x00d0)

Description: This package is used to support explicit octet count statistics on the Internet Protocol layer.

Version: 1

Extends: None.

6.1 Properties

None.

6.2 Events

None.

6.3 Signals

None.

6.4 Statistics

6.4.1 IP Octets Sent

Statistic Name: IP Octets Sent

Statistic ID: ipos (0x0001)

Description: Provides the number of octets sent from the termination or stream since the termination or stream has existed and the statistic has been set. The octets represent the egress *IP protocol data units* (PDU) of all *IP flows* of an H.248 Stream.

At the termination level, it is equal to the sum of the egress IP flows over all streams.

Type: Double

Possible values: Any 64-bit integer 0 and up

Level: Either

6.4.2 IP Octets Received

Statistic Name: IP Octets Received

Statistic ID: ipor (0x0002)

Type: Double

Description: Provides the number of octets received on the termination or stream since the termination or stream has existed and the statistic has been set. The octets represent the ingress *IP protocol data units* (PDU) of all *IP flows* of an H.248 Stream.

At the termination level, it is equal to the sum of the ingress IP flows over all streams.

Possible values: Any 64-bit integer 0 and up

Level: Either

6.5 Error codes

None.

6.6 Procedures

6.6.1 Semantic in detail

6.6.1.1 Ingress IP traffic – Statistic "IP Octets Received"

Every incoming IP packet *successfully delivered* to its H.248 Context and H.248 IP stream/termination is counted. The measurement represents the volume of all *IP flows* of an H.248 Stream. The IP flow identifier is given by the H.248 Stream Descriptor (see also Appendix I).

6.6.1.2 Egress IP traffic – Statistic "IP Octets Sent"

The measurement represents the volume of all *IP flows* of an H.248 Stream. The IP flow identifier is given by the H.248 Stream Descriptor (see also Appendix I).

6.6.2 IP versions

The statistics may be applied for any IP version.

6.6.3 Measurements when policing is enabled (possible policing-measuring interactions)

6.6.3.1 IP address policing [ITU-T H.248.43]

The semantic is clarified in clause 6 of [ITU-T H.248.43]: the location of the measurement point (MP) defined by this Recommendation for IP *ingress* Statistics is *before* any H.248.43 defined *Context* level filters. The traffic is thus measured before entering the Stream-assigned filter unit(s).

6.6.3.2 IP byterate policing [ITU-T H.248.53]

This relates to *tman*-based IP byterate policing versus *ipocs*-based IP byte metering. The location of H.248.61 defined measurement point (MP) for IP *ingress* Statistics is *before* the H.248.53 defined policing point, see also Figure I.5. The traffic is thus measured before entering the traffic policer.

7 IP Layer Packets Count Statistics Package

Package Name: IP Layer Packets Count Statistics Package

Package ID: ippcs (0x00e8)

Description: This Package is used to support explicit packet count statistics on the Internet Protocol layer.

NOTE – There is no assumption about the IP version. The IP version may also change during the lifetime of the Stream/Termination.

Version: 1

Extends: None

7.1 Properties

None.

7.2 Events

None.

7.3 Signals

None.

7.4 Statistics

7.4.1 IP Packets Sent

Statistic Name: IP Packets Sent

Statistic ID: ipps (0x0001)

Description: Provides the number of packets sent from the termination or stream since the statistic has been set. The packets represent the egress *IP protocol data units* (PDU) of all *IP flows* of an H.248 Stream.

At the termination level, it is equal to the sum of the egress IP flows over all streams.

Type: Double

Possible values: Any 64-bit integer 0 and up

Level: Either

7.4.2 IP Packets Received

Statistic Name: IP Packets Received

Statistic ID: ippr (0x0002)

Type: Double

Description: Provides the number of packets received on the termination or stream since the statistic has been set. The packets represent the ingress *IP protocol data units* (PDU) of all *IP flows* of an H.248 Stream.

At the termination level, it is equal to the sum of the ingress IP flows over all streams.

Possible values: Any 64-bit integer 0 and up

Level: Either

7.5 Error codes

None.

7.6 Procedures

7.6.1 Semantic in detail

According to clause 6.6.1 (and Appendix I), any IP packet is counted on *Context* level when correctly delivered and associated to the "IP flow".

7.6.2 IP versions

Both versions are supported. There is no explicit protocol element defined by the *ippcs* Package for discrimination of the IP version. It is assumed that the MGC has this information for the particular H.248 IP Stream/Termination (e.g., due to the SDP "c=" line information of the LD and RD).

7.6.3 Measurements when policing is enabled (possible policing-measuring interactions)

As per clause 6.6.3.

Appendix I

Relation between "IP flow" and "IP layer H.248 Statistic"

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

This Recommendation defines H.248 statistics on network protocol layer, i.e., the Internet Protocol (IP) layer. The relation (and thus the semantic of the statistic) between an IP flow and the IP layer H.248 statistic is not evident *per se*, due to the wide range of description possibilities of an H.248 IP stream (e.g., NAT-less[1], media-agnostic, media-aware, transport-protocol agnostic, L2VPN related, etc.).

I.1 Model (for packet-to-Context delivery)

Figure I.1 provides a H.248 Media Gateway level model concerning the handling of IP packets entering and subsequently leaving the MG. This is related to the particular H.248 IP-to-IP connection model applied. However, the statistics defined by this Recommendation are also applicable for IP-to-X Context types ("X" is used in this appendix as a placeholder for all non-IP bearer technologies).

There is a measurement point (MP) in the bearer-path for any bearer-level H.248 statistic. Every MP (of an H.248 statistic) is associated to an H.248 Stream (endpoint)[2], Termination and Context. H.248 statistics are thus Context/Stream/Termination-level statistics (which relates to the Context-level in Figure I.1). It should be noted that Root-level statistics are out of scope of this Recommendation.

Any measurement event (for ingress traffic) implies the correct delivery of an incoming IP packet to the corresponding H.248 Stream (and the thus correct Termination and Context)[3]. Figure I.1 shows that an ingress IP packet is firstly in a "Context-less" stage, and then, after successful delivery, in a "Context/Termination/Stream-assigned" stage.

The (H.248) Context delivery decision relates in general to an (IP) packet classification function. The classification function discriminates IP packets belonging to the same IP flow (see clause 3.1.1). The identifier (see clause 3.1.2) of such a packet flow (within an H.248 MG entity) is given by the corresponding H.248 Stream Descriptor (of the associated H.248 IP Stream) specification. There is a N:1 relationship between an IP flow and an H.248 Stream, for instance in case of RTP/RTCP flows carried within a single H.248 Stream.

It may be noted that:

1) The syntax of the IP flow identifier may vary because it is Stream-dependent, and there are many options concerning specifications of H.248 IP Stream Descriptors for IP Streams (see also clause I.2.2); and

2) There may be multiple IP flow identifier structures in place within a single H.248 MG (due to different modes of operation concerning IP-to-IP interworking).

A flow identifier (FlowID) is fundamentally the lookup-key for packet classification with regard to Context delivery.

---

[1] An H.248 IP-to-IP Context in "NAT-less" mode means that there is no translation of IP source and destination addresses.

[2] An H.248 Stream within an H.248 IP-IP context.

[3] That is the reason for calling this "packet-to-Stream" assignment a "packet-to-Context delivery" model.

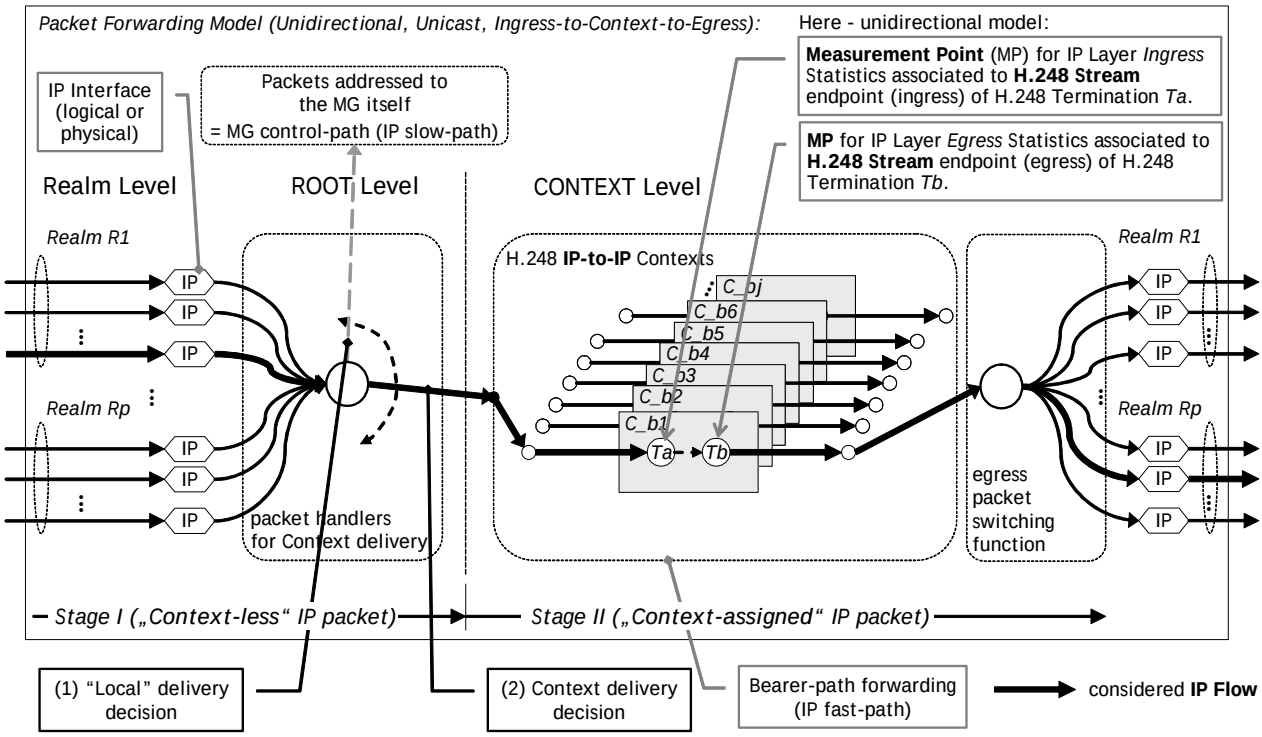

Figure I.1 – MG model showing an IP-to-IP bearer-path – Classification of incoming IP packets and delivery to the "identified" H.248 Context and H.248 IP Stream endpoint

I.2 Correlation between H.248 Stream Identifier and IP Flow Identifier

The statistics of the ipocs package are related to IP flows (see clause 6.4). The particular statistics semantic is thus defined by the correlation between the H.248 Stream Identifier (for Stream-level statistics) or H.248 Termination Identifier (for Termination-level statistics) and the IP Flow Identifier(s), unambiguously identifying all IP packets of that Stream or Termination.

I.2.1 Possible packet header fields as representation of IP flow identifiers

The (IP) flow identifier represents in general a n-tuple (which is then used as lookup-key for Context delivery). Figure I.2 shows some of the header fields (and their widths) that might be used for classifying a packet (according to the H.248 Stream description). Although not shown in the figure, higher layer (e.g., application-level framing) header fields (e.g., RTP PT or SSRC), or other layer header fields (e.g., MPLS LSP identifier), may be also used for classification.

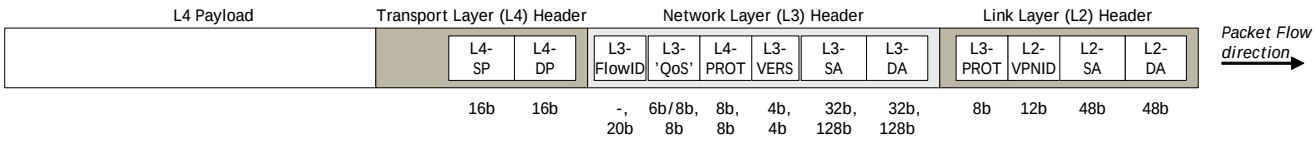

Figure I.2 – Possible header fields as lookup-key input (with Ethernet as example L2 protocol)

The (IP) flow identifier relates to meta-data in the MG because there is not any explicit identifier information element at the H.248 interface (with exceptions of the 1-tuple keys in Table II.1).

I.2.2 Possible H.248 (Stream Descriptor) defined lookup-key structures

The lookup-key structure is also dependent on whether SDP wildcarding is used (clause II.2) or not (clause II.1).

NOTE – Also see clause 7.1.8 of [ITU-T H.248.1] for details on local and remote descriptors, and [b-ITU-T H.248.39] for H.248 SDP parameter identification and wildcarding.

I.2.2.1 Lookup-keys based on fully specified SDP

There may be many different lookup-key structures, given the network environment of an H.248 IP-to-IP MG and the variety of services and applications provided. Table II.1 provides a non-exhaustive list of some example lookup-key types. The lookup-key format is primarily defined by:

- H.248 **SDP** information elements (mainly "c=" and "m=" line fields, but in specific cases also "a=" line (e.g., [b-IETF RFC 3605])), and/or
- H.248 **Properties** (defined by H.248 packages with protocol elements for "identification" of bearer traffic).

The lookup-keys could be categorized into key types with SDP-only, with Property-only or with both information elements. Table II.1 uses a protocol layer oriented structure (lower to upper layers).

I.2.2.2 Lookup-keys based on wildcarded SDP

Wildcarding of SDP of information elements of the "c=" and/or "m=" lines will lead to further lookup-key structures. The examples in Table II.2 are inline with possible wildcarding options according to [b-ITU-T H.248.39]. The relevant clauses are 6.13 of [b-ITU-T H.248.39] for the connection information ("c=" line, Note) and 6.11 for the media description ("m=" line) of [b-ITU-T H.248.39].

NOTE – The wildcarding options may be limited in the scope of this Recommendation as follows:

a) the network type must always be "IN";

b) the address type value may be "IP4" or "IP6" or both (in case of "ALL" wildcarding).

Table II.2 provides some examples, divided in L3 (I) and L4-L7 (II) related wildcarding options.

I.2.2.3 Lookup-keys based on remote peer information

Remote source (RS) and/or remote destination (RD) information may be also used for lookup-keys, see e.g.,:

- [b-ITU-T Y.1221] describes the combination of parameters "source IP address", "destination IP address", "source and destination port numbers", "protocol", and "experimental/Diffserv value" as a basis for a flow identifier; or
- [b-ITU-T Y.2121] generalized flow identifier concept.

I.2.2.3.1 H.248 statistics in IP egress direction

The H.248 egress statistics of this Recommendation cover all IP flows of an H.248 Stream, thus, any (successfully) sent IP packet shall be counted. There is no packet classification (and thus no lookup process) at the egress side (see also clause I.3). H.248 egress statistics are therefore independent of remote IP connection endpoint information.

I.2.2.3.2 H.248 statistics in IP ingress direction

There may be useful lookup-key structures with additional "remote source" information elements. Currently, no protocol semantics are defined that would allow the derivation of lookup-key information from H.248 protocol elements, such as:

- H.248 remote descriptor (RD) elements
- H.248 properties for remote filter definitions (e.g., from [ITU-T H.248.43]).

NOTE – The H.248.61 defined measurement point is located before any possible (Context level) filter stage (also see Figure I.5). This allows already the derivation of some other statistics. For example, the number of IP packets received after filtering would be equal to the difference of all received packets (statistic ippcs/ippr) minus discarded packets (statistics dp of H.248 packages with policing functionality).

I.2.2.4 Lookup-keys for tunnelled IP traffic

The lookup-key may further change when tunnelling techniques are used in IP domain/realms. For example, the encapsulating protocol header with IPv4 address may be used as the identifier for flow aggregates in case of:

- IP-in-IP encapsulation [b-IETF RFC 2003]
- Generic routing encapsulation (GRE) [b-IETF RFC 2784])

Due to the deployment of IPv6, other possible lookup-key structures for tunnelling of IPv4 or IPv6 packets include IPv6-over-IPv4 [b-IETF RFC 3056] and IPv4-over-IPv6.

They are also dependent on whether the MG is the tunnel endpoint or not.

I.2.3 Common header fields used for Context delivery and H.248.43 packet filter rules

The IP layer H.248 statistics (as defined by this Recommendation) may be affected by H.248.43 packet filter rules. The purpose of this clause is to clarify possible interactions.

I.2.3.1 Introduction

There are some header fields that may be subject of Context delivery, but also used in filter conditions like H.248.43 supported filter rules. Figure I.3 provides an overview of both packet handling applications, from the ingress side perspective (thus, H.248.43 outgoing filtering is omitted).

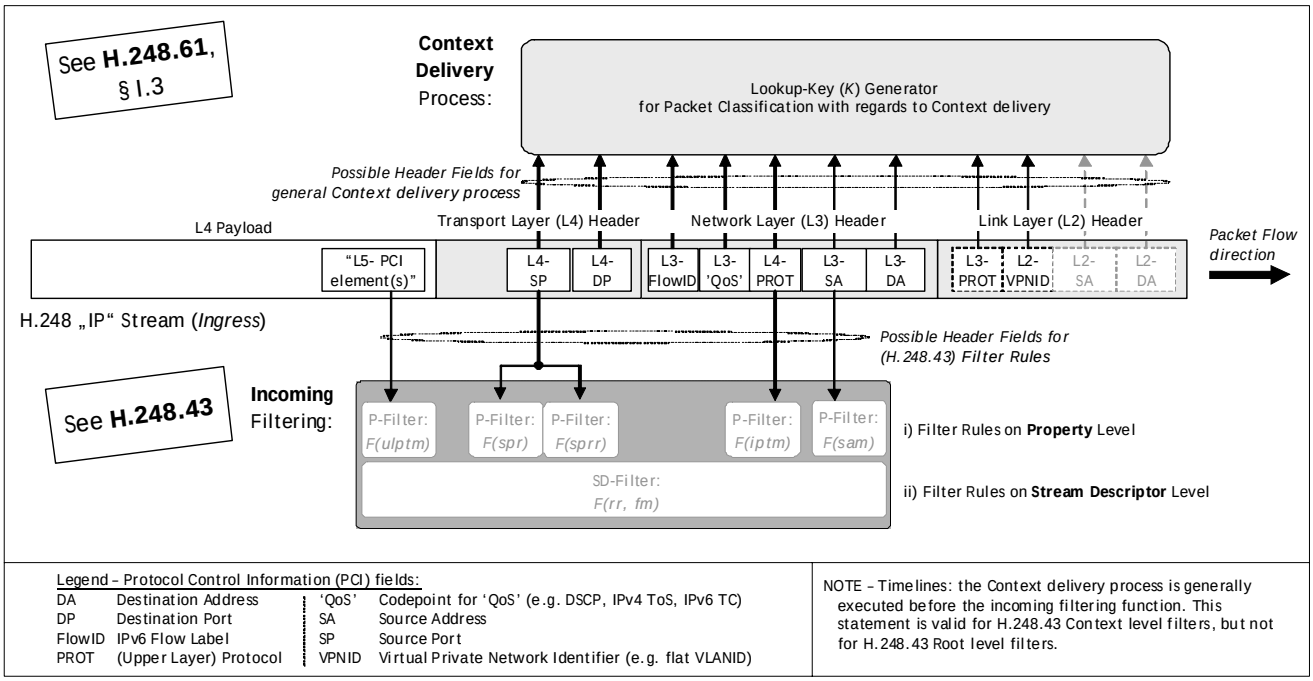

Figure I.3 – Context delivery (lookup-keys) and H.248.43 packet filter rules

There are only three common header fields (common to IP flow identification and H.248.43 related filters) on the ingress side: L3-SA, L4-PROT and L4-SP. Consequently, there is no interaction between Context delivery and H.248.43 incoming filtering in case of lookup-key tuples without any of these PCI elements.

[ITU-T H.248.43] allows the definition of filters on Context level and Root level for session-dependent and session-independent policing, respectively. It may be further noted that H.248.43 Context level filter rules are executed after the (successful) Context delivery process. H.248.43 Root level filters would be in contrary already executed in the Context-less stage (e.g., before or as part of the Context delivery process).

I.2.3.2 Possible interactions

There may be theoretical interactions between IP layer H.248 statistics and H.248.43 packet filter rules in case of L3-SA, L4-PROT or L4-SP usage by both packet handling applications (IP flow identification and H.248.43 filters). However, any such interactions are resolved by the strict ordering between Context delivery and H.248.43 filtering. Specifically:

- The packet is first delivered to a Context based solely on the Context delivery process, regardless of any H.248.43 filters applied to the Context. It is then counted by IP layer statistics.
- Subsequently, the packet is filtered based on the Context's H.248.43 filters. Whether the packet is dropped by the filter depends on the relation between the set of tuples matching the Context's delivery rule and the set of tuples rejected by the filter. All, some or none of the packets will be dropped depending on whether the first set is contained in, intersects with or is disjoint from the second.

I.3 The general Context delivery process for incoming IP packets

NOTE – Packet classification and Context delivery is only relevant for ingress flows.

The general Context delivery process for incoming IP packets is summarized in Figure I.4. This lookup table (also known as context delivery information base, CDIB) is located in the Context-less IP processing stage (see again Figure I.1) of the H.248 MG. The CDIB size is related to the maximum MG capacity with regard to H.248 IP Streams, Terminations and Contexts. The number of valid CDIB entries is dynamic and given by the number of created H.248 IP Stream endpoints.

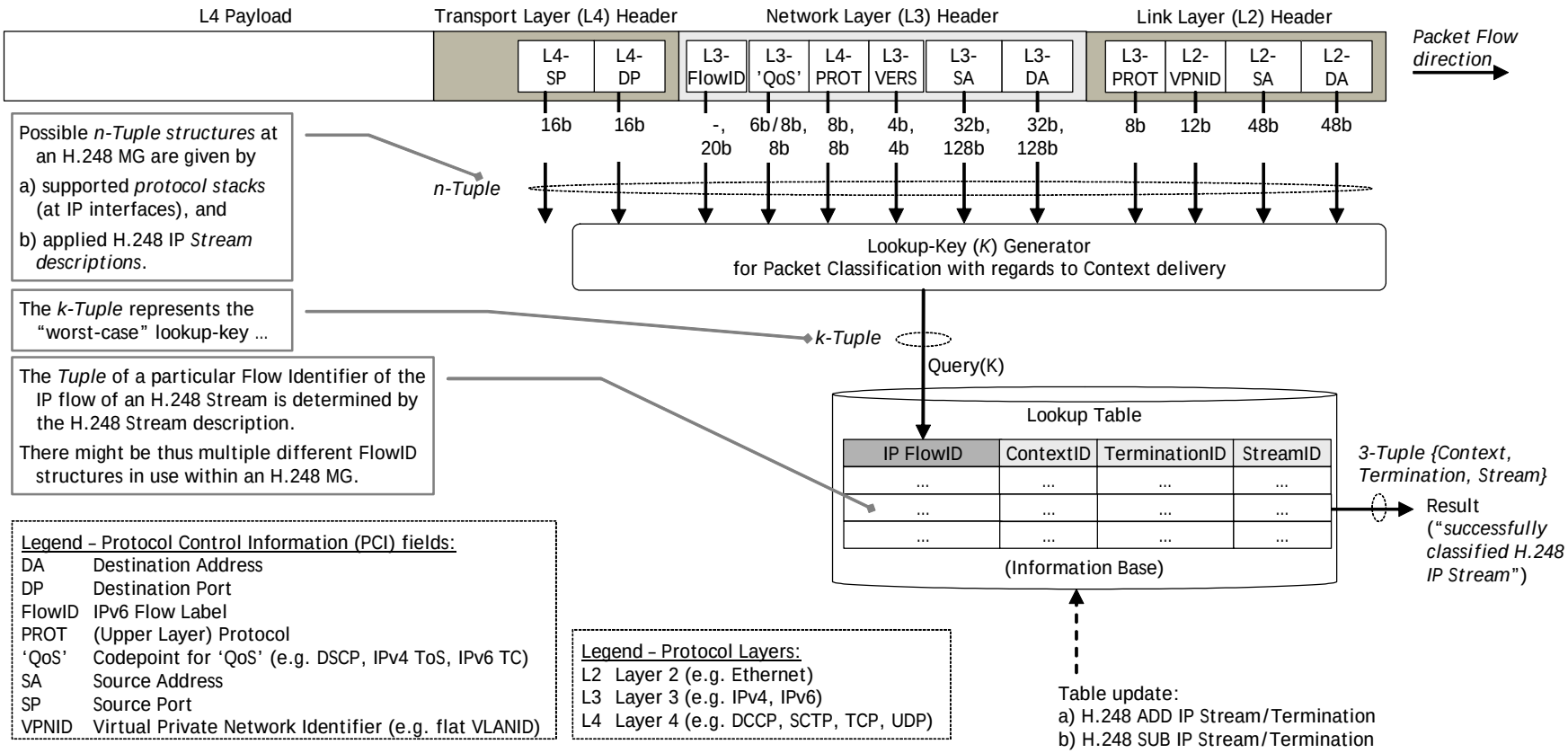

Figure I.4 – General Context delivery process for incoming IP packets

I.4 Context level IP packet processing: relation of H.248.61 and other H.248.x-series technologies concerning IP-related functions

Clause I.2.3 already discusses the relationship between this Recommendation and [ITU-T H.248.43]. Figure I.5 outlines other possible Context level IP packet processing functions and their processing order within the IP bearer-path (which relates here to the so-called IP fast-path in IP hop/host systems).

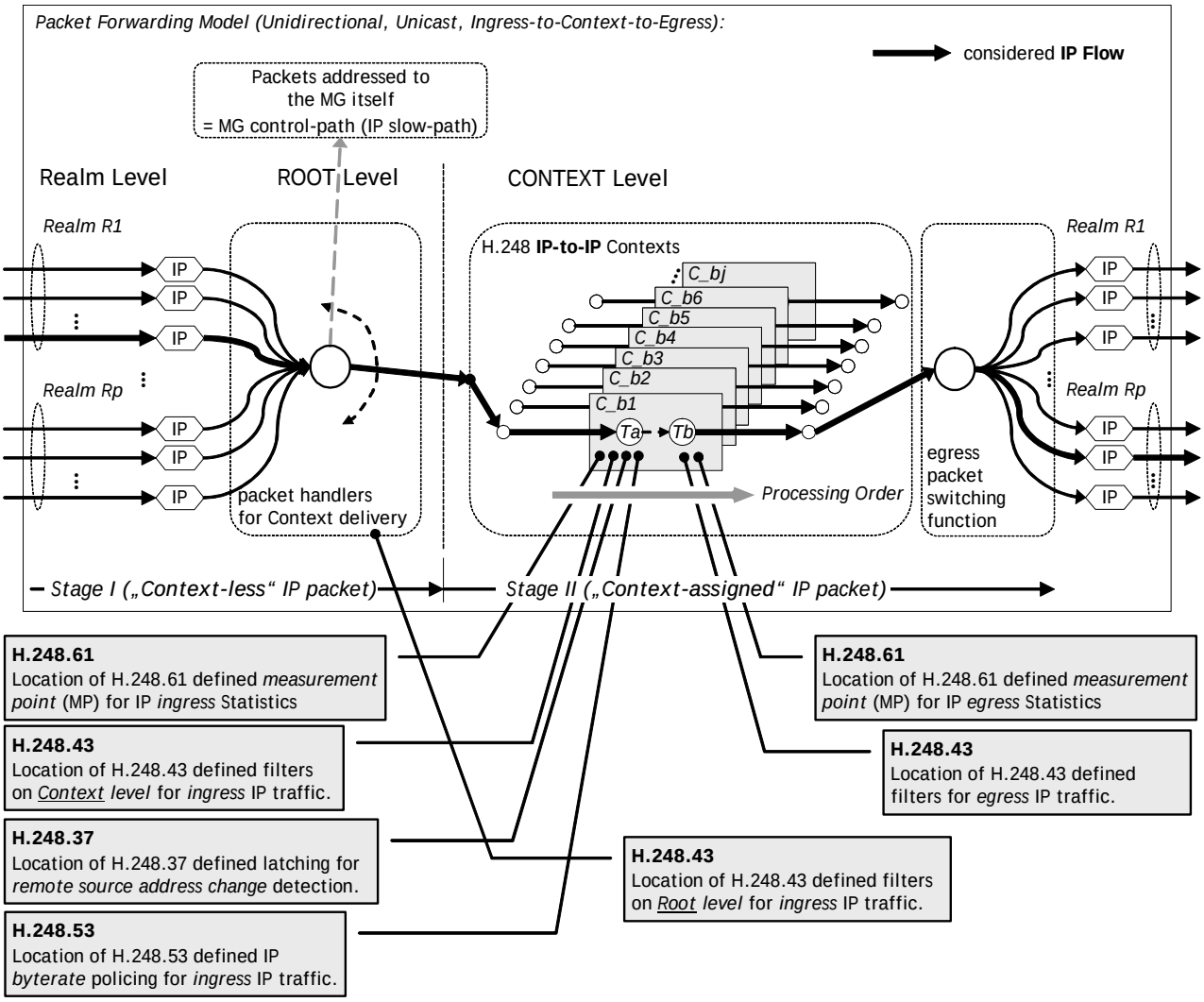

Figure I.5 – Context-level IP packet processing – Relation of H.248.61 and other H.248.x-series technologies concerning IP-related functions

I.4.1 Common header fields, used for Context delivery (lookup-keys) and H.248.37 address latching

Latching or re-latching (according to [b-ITU-T H.248.37]) may also affect the Context delivery process, and thus the measurement of IP layer H.248 Statistics. [b-ITU-T H.248.37] is only for ingress traffic, and there are two relevant header fields, L3-SA and L4-SP. Possible interactions (between Context delivery and latching) are again of pure theoretical nature due to the justification given in clause I.2.3.2. Any processing according to the procedures of [b-ITU-T H.248.37] is performed after the packet is delivered to the correct Context, i.e., after the ingress H.248.61 statistics were updated.

I.5 Special IP bearer traffic

The IP flow(s) of the H.248 bearer path correlate usually to a single "upper layer" protocol, which is identified by the 8-bit protocol number in the IP header (see field 'L4-PROT' in Figure I.2).

Example: The IP packets of the RTP media flow and RTCP control flow of a single H.248 IP stream using both L4-PROT equal to 17 for UDP as upper layer protocol.

However, the H.248 IP bearer-path may carry additional IP traffic, e.g., the IP applications without any transport protocol as the ICMP (1), IGMP (2) or OSPF (89).

NOTE 1 – Such IP packets, like for Ping (ICMP echo request), multicast group control (IGMP) or IP routing (OSPF), would be either locally delivered (see IP slow-path (1) in Figure I.1), or forwarded to the next hop/host.

Such IP packets will be counted by H.248 statistics (as defined by this Recommendation) in case they match the lookup-key condition of an H.248 Stream identifier (see clause I.2).

NOTE 2 – Table II.1 provides a number of lookup-key examples without L4-PROT consideration.

I.5.1 ICMP

ICMP is exceptional because it must be processed by every IP host and hop entity. The handling of ICMP packets is for further study; it is assumed that ICMP packets are not counted and dedicated statistics (e.g., for ICMP query and error messages) could be introduced in the future.

Appendix II

Lookup-key structures

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

This appendix provides examples for possible H.248 (Stream Descriptor) defined lookup-key structures (see also clause I.2).

II.1 Lookup-keys based on fully specified SDP

This lookup-key format is introduced in clause I.2.2.1. Table II.1 provides a non-exhaustive list of some example lookup-key types.

Table II.1 – Non-exhaustive list of lookup-key structures (i.e., k-tuple formats for IP Flow identification, as given by the signalled H.248 stream descriptor for an H.248 IP Stream/Termination – Ingress IP traffic only)

No.	Elements of k-tuple: Header (PCI) fields	Tuple size	Example network application	Comments to H.248 stream descriptor (SDP & properties)	Key type
1	{L2-VPNID}	1	Interconnection of two L2VPN domains	Just LCD (i.e., SD without LD and RD)	b
2	{L2-VPNID, L2-VPNID}	2	Ditto for, e.g., stacked VLANs	Just LCD (e.g., with *vlan/tags = [VIDx, VIDy]*)	b
3	{L2-VPNID, L2-PRIO}	2	Ditto, but particular H.248 Context for L2 priority	Just LCD (e.g., with *vlan/tags = VIDx*, *vlan/pri = PRIOz*)	b
4	{L2.5-LABEL}	1	Interconnection of two MPLS LSPs (Note 4)	Just LCD (i.e., SD without LD and RD; e.g., with *mpls/stack = LABELx*)	b
5	{L2.5-LABEL, …, L2.5-LABEL}	*n*	Ditto, but stacked MPLS (with stack depth n) (Note 4)	-"- (with *mpls/stack = [LABELx, …]*)	b
6	{L3-DA}	1	Native, RFC 1812 IP forwarding (IPR mode)		a, c
7	{L4-DP}	1	B2BIH mode, small MG sizes ("single L4 port space in use")		a
8	{L4-PROT}	1			a
9	{L3-DA, L4-DP}	2	B2BIH mode, e.g., MG as *multihomed* IP host		a
10	{L3-DA, L4-PROT, L4-DP}	3	Ditto		a
11	{L4-PROT, L4-DP}	2			a

Table II.1 – Non-exhaustive list of lookup-key structures (i.e., k-tuple formats for IP Flow identification, as given by the signalled H.248 stream descriptor for an H.248 IP Stream/Termination – Ingress IP traffic only)

No.	Elements of k-tuple: Header (PCI) fields	Tuple size	Example network application	Comments to H.248 stream descriptor (SDP & properties)	Key type
12	{L3-DA, L3-SA} (Note 6) (Note 1) or only {L3-DA}	2 1	IP (*network*) *connection* interworking: a) NAT-less IPR mode b) NAT-less B2BIH mode c) NAT-full B2BIH mode	LD (RD, Note 1) contains only SDP "c=" line, but *no* "m=" line a) *ipr/ifm = "IPR"* b) *ipr/ifm = "B2B"* c) *ipr/ifm = "B2B"*	a, c
13	{L3-DA, L3-SA, L4-DP, L4-SP} (Note 1)	4	IP *transport connection* interworking (application-agnostic)		a
14	{L3-DA, L3-SA, L4-PROT, L4-DP, L4-SP} (Note 1)	5	IP *transport connection* interworking (application-aware)		a
15	{L2-VPNID, L4-DP}	2	Interconnection of L3VPN domains, with an MG "front-end" entity for L3VPN-to-L2VPN translation		c
16	{L3-VPNID, L3-DA, L4-DP}	3	Same as No. 8, but with underlying L3VPN technology (Note 7)		c
17	{L2-VPNID, L2-VPNID, L3-DA, L3-SA, L4-PROT, L4-DP, L4-SP} (Note 1)	7	Application-aware IP transport connection via a stacked VLAN endpoint	According to combination of No. 2 and 12	c
18	{L3-DA, L3-'QoS', L4-DP}	3	QoS-aware IP classification, e.g., a) DS PHB support b) "Traffic Class"ification for IPv6	Plus, e.g., H.248.52 protocol elements (Note 2)	c
19	{L3-FlowID}	1	Classification based on IPv6 Flow Label only (Note 5)	Signalling of IPv6 Flow Label values is so far out of scope of H.248 or any bearer path-coupled or decoupled QoS signalling protocol (Note 3).	–
20	{L3-DA, L3-SA}, {L3-DA, L3-SA, L4-DP, L4-SP}	2, 4	H.248 IP bearer according to IPBCP ([b-ITU-T Q.1970], [b-ITU-T Q.1990])	Local and remote address information is implicitly coupled due to the IPBCP bidirectional bearer definition (see [b-ITU-T Q.2631.1] or [b-ITU-T Q-Sup.43]).	a

Table II.1 – Non-exhaustive list of lookup-key structures (i.e., k-tuple formats for IP Flow identification, as given by the signalled H.248 stream descriptor for an H.248 IP Stream/Termination – Ingress IP traffic only)

No.	Elements of k-tuple: Header (PCI) fields	Tuple size	Example network application	Comments to H.248 stream descriptor (SDP & properties)	Key type
21	more…	–	–	–	–

Abbreviations for H.248 Descriptors: MD = Media Descriptor, SD = Stream Descriptor, LCD = LocalControl Descriptor, LD = Local Descriptor, RD = Remote Descriptor

NOTE 1 – Such a lookup-key requires information about *remote source* address, either via: a) SDP information from the RD, or b) correspondent properties.

NOTE 2 – Such a lookup-key requires enforcement of a QoS-aware IP classification function on the ingress traffic side, before or after entering the H.248 Context. This is for further study.

NOTE 3 – The FlowID value may be self-learnt by the MG by derivation of that information from the first packet. Subsequent arriving packets may be then delivered to the Context by using the 1-tuple of {L3-FlowID}. This may drastically simplify the Context delivery process, under the conditions that the Flow Label values are: a) unique across all flows in a particular MG, and b) not changing during the lifetime of the flow.

NOTE 4 – There is a symmetry assumption in this MPLS example by identical label values for both traffic directions.

NOTE 5 – This is possible for some IPv6 scenarios, but does not represent the general use case for IPv6.

NOTE 6 – An IP connection endpoint is usually defined by the 2-tuple of {L3-DA, L3-SA}.

NOTE 7 – e.g., IPsec as L3VPN technology, the L3-VPNID element would then relate to the IPsec SPI (security parameter index for IPsec security association (SA)).

II.2 Lookup-keys based on wildcarded SDP

This lookup-key format is introduced in clause I.2.2.2. Table II.2 provides a non-exhaustive list of some example lookup-key types.

Table II.2 – Further lookup-key structures due to possible SDP wildcarding (i.e., k-tuple formats for IP Flow identification, as given by the signalled H.248 stream descriptor for an H.248 IP Stream/Termination – Ingress IP traffic only)

No.	Elements of k-tuple: Header (PCI) fields	Tuple size	Example network application	Comments to H.248 stream descriptor (SDP & properties)	Key type
(I) "Connection"-wildcarding of SDP of information elements ("c=" line, see clause 6.13 of [b-ITU-T H.248.39]). The "m=" line elements are "not significant" (Note 1).					

I.1	{L3-VERS}	1	The entire ingress IP traffic of *all* IPv4 (or IPv6) interfaces of the MG is received and mapped on a single H.248 Stream. Such an IP traffic aggregate may be then subject of, e.g., Stream-dependent policing functions.	SDP wildcarding in LD:
				`c=IN <addrtype> *`
				`m=- - - -`
				Further: LCD without RD, thus unidirectional Stream. Context supposed to be in IPR mode.	

Table II.2 – Further lookup-key structures due to possible SDP wildcarding (i.e., k-tuple formats for IP Flow identification, as given by the signalled H.248 stream descriptor for an H.248 IP Stream/Termination – Ingress IP traffic only)

No.	Elements of k-tuple: Header (PCI) fields	Tuple size	Example network application	Comments to H.248 stream descriptor (SDP & properties)	Key type

I.2	{}	0	As above, but now also IP version independent "traffic aggregate".	SDP wildcarding in LD:
				`c=IN * *`
				`m=- - - -`
				Further: LCD without RD, thus unidirectional Stream. Context supposed to be in IPR mode.	

(II) "Media"-wildcarding of SDP of information elements ("m=" line, see clause 6.11 of [b-ITU-T H.248.39]). The "c=" line elements are *not wildcarded* in these examples.					

II.1	{L3-VERS, L3-DA, L4-DP, L4+-M-TYPE}	4	Not applicable.
			Wildcarding of *all media types* is *not* possible without indication of *media format*.
				SDP wildcarding in LD:
				`c=IN <addrtype> <connection-address>`
				`m=* - - -`	

II.2	{L3-VERS, L3-DA, L4-DP, L4-PROT, L4+-M-TYPE}	5	The entire ingress IP traffic of a specific IPv4 (or IPv6) transport endpoint, independent of the media-format, is received and mapped on a single H.248 Stream. The Stream is media-format agnostic and transport aware.
			Example: The IP flow aggregate might be the sum of all RTCP packet types and all media-type specific RTP payload types in case of RTP-over-IP.
				SDP wildcarding in LD:
				`c=IN <addrtype> <connection-address>`
				`m=<media> <port> <proto> *`	

II.3	{L3-VERS, L3-DA, L4-PROT, L4+-M-TYPE, L4+-M-FORMAT}	5	The entire ingress IP traffic for all transport endpoints of a specific IPv4 (or IPv6), for a specific media-format, is received and mapped on a single H.248 Stream.
			Example: The IP flow aggregate might be the sum of all X-over-RTP packets.
				SDP wildcarding in LD:
				`c=IN <addrtype> <connection-address>`
				`m=<media> * <proto> <fmt>`	

Table II.2 – Further lookup-key structures due to possible SDP wildcarding (i.e., k-tuple formats for IP Flow identification, as given by the signalled H.248 stream descriptor for an H.248 IP Stream/Termination – Ingress IP traffic only)

No.	Elements of k-tuple: Header (PCI) fields	Tuple size	Example network application	Comments to H.248 stream descriptor (SDP & properties)	Key type

II.4	{L3-VERS, L3-DA}	2	The entire ingress IP traffic of a specific IPv4 (or IPv6) interface and the entire L4 port range of the MG is received and mapped on a single H.248 Stream. The Stream is media-agnostic and transport-protocol agnostic.	SDP wildcarding in LD:
				`c=IN <addrtype> <connection-address>`
				`m=- * - -`	

II.5	{L3-VERS, L3-DA, L4-PROT}	3	The entire ingress IP traffic of a specific IPv4 (or IPv6) interface and the entire port range of a specific transport protocol (e.g., TCP) is received and mapped on a single H.248 Stream. The Stream is media-agnostic and transport-protocol aware.	SDP wildcarding in LD:
				`c=IN <addrtype> <connection-address>`
				`m=- * <proto> -`	

II.6	{L3-VERS, L3-DA, L4-DP, L4-PROT, L4+-M-TYPE, L4+-M-FORMAT}	6	Wildcarding *all* on the the "*number of port*" qualifier: e.g., *all* RTP/RTCP *flow pairs* of a single H.248 Stream (Note 2).	SDP wildcarding in LD:
				`c=IN <addrtype> <connection-address>`
				`m=<media> <port>/* <proto> <fmt>`	

NOTE 1 – [b-ITU-T H.248.39] denotes the potential wildcards by using "$" for *Choose*, "*" for *All* and "–" for "*Not Significant*". It may be noted that wildcards "*" and "–" are synonyms concerning their H.248 behaviour.

NOTE 2 – See also clause 6.6.1.6 of [b-ITU-T H.248.57].

Bibliography

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

[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.248.57] Recommendation ITU-T H.248.57 (2008), *Gateway control protocol: RTP control protocol package*.

[b-ITU-T M.2301] Recommendation ITU-T M.2301 (2002), *Performance objectives and procedures for provisioning and maintenance of IP-based networks*.

[b-ITU-T Q.1902.1] Recommendation ITU-T Q.1902.1 (2001), *Bearer independent call control protocol (Capability Set 2): Functional description*.

[b-ITU-T Q.1970] Recommendation ITU-T Q.1970 (2006), *BICC IP bearer control protocol*.

[b-ITU-T Q.1990] Recommendation ITU-T Q.1990 (2001), *BICC bearer control tunnelling protocol*.

[b-ITU-T Q.2631.1] Recommendation ITU-T Q.2631.1 (2003), *IP connection control signalling protocol – Capability Set 1*.

[b-ITU-T Q-Sup.43] ITU-T Q-series Recommendations – Supplement 43 (2003), Technical Report TRQ.2415: *Transport control signalling requirements – Signalling requirements for IP connection control in radio access networks Capability Set 1*.

[b-ITU-T Y.1221] Recommendation ITU-T Y.1221 (2002), *Traffic control and congestion control in IP-based networks*.

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

[b-IETF RFC 2003] IETF RFC 2003 (1996), *IP Encapsulation within IP*.

[b-IETF RFC 2784] IETF RFC 2784 (2000), *Generic Routing Encapsulation (GRE)*.

[b-IETF RFC 3056] IETF RFC 3056 (2001), *Connection of IPv6 Domains via IPv4 Clouds*.

[b-IETF RFC 3605] IETF RFC 3605 (2003), *Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)*.

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, 2010