International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3303.2

(03/2014)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Resource control protocols

Resource control protocol No. 3 – Protocol at the interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE) (Rw interface): ITU-T H.248 alternative version 2

Recommendation ITU-T Q.3303.2

International Telecommunication Union

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	**Q.3300–Q.3369**
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3649
NGN applications	Q.3700–Q.3849
Testing for next generation networks	Q.3900–Q.3999

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

Recommendation ITU-T Q.3303.2

Resource control protocol No. 3 – Protocol at the interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE) (Rw interface): ITU-T H.248 alternative version 2

Summary

Recommendation ITU-T Q.3303.2 specifies the resource control protocol No. 3 (rcp3) ITU-T H.248 profile used at the Rw interface, i.e., between the policy decision physical entity (PD-PE) and the policy enforcement physical entity (PE-PE) in the resource and admission control functional block.

This protocol profile allows the final admission policy decisions to be installed (either push or pull mode) to a PE-PE from a PD-PE, supports resource control for both fixed and mobile networks and supports the network address and port translation (NAPT) control and network address translation (NAT) traversal at the PE-PEs as needed. It satisfies the requirements for information flows across the Rw reference point as specified in clause 8.2 of Recommendation ITU-T Y.2111. It is also used to control the PE-PE in transport devices, including quality of service (QoS) resource control (e.g., packet marking, filtering and policing) and gate control.

This version of the Recommendation improves the published version 1 in 2007 and adds additional features to satisfy the full requirements as defined in Recommendation ITU-T Y.2111, based on the developments and progresses of both ITU-T Y.2111 and ITU-T H.248 protocols. New functional packages as well as their procedures are introduced in this version such as "hanging termination detection", "statistics conditional reporting", "IP realm availability" and "Pull mode". Meanwhile, a number of changes are made to refine the profile definitions and the details.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3303.2	2007-08-06	11	11.1002/1000/9120
2.0	ITU-T Q.3303.2 v2	2014-03-29	11	11.1002/1000/12165

* 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 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 Q.3303.2

Resource control protocol No. 3 – Protocol at the interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE) (Rw interface): ITU-T H.248 alternative version 2

1 Scope

This Recommendation provides the stage 3 technical specifications for the ITU-T H.248 profile of the Rw interface. The functional requirements and the stage 2 specifications of the Rw interface are contained in [ITU-T Y.2111]. The Rw interface is the interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE).

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.248.4] Recommendation ITU-T H.248.4 (2009), *Gateway control protocol: Transport over Stream Control Transmission Protocol (SCTP).*

[ITU-T H.248.8] Recommendation ITU-T H.248.8 (2013), *Gateway control protocol: Error code and service change reason description*.

[ITU-T H.248.11] Recommendation ITU-T H.248.11 (2013), *Gateway control protocol: Media gateway overload control package*.

[ITU-T H.248.14] Recommendation ITU-T H.248.14 (2009), *Gateway control protocol: Inactivity timer package*.

[ITU-T H.248.36] Recommendation ITU-T H.248.36 (2013), *Gateway control protocol: Hanging Termination Detection package.*

[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.248.41] Recommendation ITU-T H.248.41 (2013), *Gateway control protocol: IP domain connection 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.248.45] Recommendation ITU-T H.248.45 (2006), *Gateway control protocol: MGC information package*.

[ITU-T H.248.47] Recommendation ITU-T H.248.47 (2008), *Gateway control protocol: Statistic conditional reporting package.*

[ITU-T H.248.48] Recommendation ITU-T H.248.48 (2008), *Gateway control protocol: Statistic conditional reporting package.*

[ITU-T H.248.49] Recommendation ITU-T H.248.49 (2007), *Gateway control protocol: Session description protocol RFC and capabilities packages.*

[ITU-T H.248.52] Recommendation ITU-T H.248.52 (2008) Amendment 1 (2009), *Gateway control protocol: QoS Support packages*.

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

[ITU-T H.248.54] Recommendation ITU-T H.248.54 (2007), *Gateway control protocol: MPLS support package.*

[ITU-T H.248.55] Recommendation ITU-T H.248.55 (2008), *Gateway control protocol: Generic pull mode package*.

[ITU-T H.248.56] Recommendation ITU-T H.248.56 (2007), *Gateway control protocol: Packages for virtual private network support.*

[ITU-T H.248.57] Recommendation ITU-T H.248.57 (2013), *Gateway control protocol: RTP control protocol package.*

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

[ITU-T H.248.65] Recommendation ITU-T H.248.65 (2009) *Gateway control protocol: Support of the resource reservation protocol*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks1*.

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

[IETF RFC 1123] IETF RFC 1123 (1989), *Requirements for Internet Hosts -- Application and Support*.

[IETF RFC 3264] IETF RFC 3264 (2002), *An Offer/Answer Model with Session Description Protocol (SDP)*.

[IETF RFC 4566] IETF RFC 4566 (2006), SDP: *Session Description Protocol*.

[IETF RFC 5234] IETF RFC 5234 (2008), *Augmented BNF for Syntax Specifications: ABNF*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 gate: A construct used to enable or disable the forwarding of IP packets based on the policy decision. A gate is identified by the classifier (e.g., IPv4 5-tuple) and direction of a media flow or a group of media flows that in conformance to the same set of policy decisions.

NOTE – The ITU-T H.248 gate (and pinhole) concept is depicted in Annex A of [b-ETSI ES 283 018].

3.2.2 gate control: The operation of opening or closing a gate. When a gate is open, the packets in the media flows are allowed to pass through; when a gate is closed, the packets in the media flows are not allowed to pass through.

3.2.3 IP-to-IP interworking modes: The available session description protocol (SDP) information elements and values in the signalled SDP "media description" (mainly "m=" and "a=" lines) by the policy decision entity (MGC), may be used to categorize following interworking modes from policy enforcement entity (MG) perspective:

(1) "**Media-agnostic**": the "m=" line values of *media type* (<media>) and *media format* (<fmt>) are not allowing to terminate the PE-PE (MG) on the transported "media" information.

(2) "**Media-aware**": the "m=" line values of *media type* (<media>), *transport protocol* (<proto>) and *media format* (<fmt>) unambiguously define the entire protocol stack of the ITU-T H.248 IP termination, i.e., the PE-PE (MG) is cognizant of transported "media" information and the underlying transport protocol type.

(3) "**Transport protocol-agnostic**" (or briefly "**transport-agnostic**"): the PE-PE (MG) may not conclude from signalled SDP information elements on the transported IP payload information (Note 1).

(4) "**Transport protocol-aware**" (or briefly "**transport-aware**"): the value of the IP *protocol* field is indicated by the signalled SDP information elements, e.g., by the "m=" line value of the *transport protocol* (<proto>) field.

NOTE – The PE-PE (MG) could principally derive the used transport protocol by analysing the protocol field (http://www.iana.org/assignments/protocol-numbers) in the IP header, but such a function is beyond ITU-T H.248. The PE-PE (MG) is still transport protocol-agnostic from ITU-T H.248 point of view.

3.2.4 media flow: A unidirectional media stream, which is specified by two endpoint identifiers and bandwidth, as well as class of service if needed.

3.2.5 pinhole: Configuration of two associated ITU-T H.248 IP terminations within the same ITU-T H.248 context, which allows and prohibits unidirectional forwarding of IP packets under specified conditions.

NOTE 1 – A pinhole may also be referred to as a "gate".

NOTE 2 – E.g., address tuple.

NOTE 3 – See [ITU-T H.248.37].

3.2.6 policy decision physical entity (PD-PE): The PD-PE is an implemented instance of the policy decision functional entity (PD-FE) as identified in [ITU-T Y.2111].

3.2.7 policy enforcement physical entity (PE-PE): The PE-PE is an implemented instance of the policy enforcement functional entity (PE-FE) as identified in [ITU-T Y.2111].

3.2.8 transcoding: Translation from one type of encoded media format to another media format (examples: G.711 A-law to μ-law or vice versa; ITU-T G.711 to ITU-T G.726-40K; ITU-T G.729 to adaptive multi-rate (AMR) with 4.75 rate; ITU-T G.711 to a broadband codec that operates at 256 kbps, etc.).

NOTE – The definition of 'transcoding' is based on the definition in clause 3 of [b-ITU-T V.152].

Transcoding belongs to the category of "media aware" IP-to-IP interworking (see above).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABNF Augmented Backus-Naur Form

AC Admission Control

AH	Authentication Header
AMR	Adaptive Multi-Rate
API	Application Programming Interface
AVP	Attribute-Value Pair
B2BIH	Back-to-Back IP Host
B2BRE	Back-to-Back RTP Endsystem
BGF	Gateway Function
BGW	Border Gateway
CBR	Constant Bit Rate
CNAME	Canonical Name
CoAC	Context Admission Control
CPE	Customer Premises Equipment
DiffServ	Differentiated Services
ESP	Encapsulation Security Payload
GoS	Grade of Service
HW	Hardware
ID	Identifier
IBCF	Interconnection Border Control Function
ICMP	Internet control message protocol
IEPS	International Emergency Preference Scheme
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPR	IP Router
IPsec	IP security
LAN	Local Area Network
LCD	LocalControl Descriptor
LD	Local Descriptor
LSP	Label Switched Path
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
MID	Message Identifier (ITU-T H.248)
MPLS	Multi-Protocol Label Switching
NAPT	Network Address and Port Translation
NAPT-PT	NAPT and Protocol Translation
NAT	Network Address Translation
PCI	Protocol Control Information

PD-PE	Policy Decision Physical Entity
PDU	Protocol Data Unit
PE-PE	Policy Enforcement Physical Entity
PHB	Per-Hop Behaviour
QoS	Quality of Service
RD	Remote Descriptor
RP	Reporting Point
RSVP	Resource Reservation Protocol
RTCP	RTP Control Protocol
RTCP XR	RTP Control Protocol extended Report
RTP	Real-time Transport Protocol
SCF	Service Control Functions
SCTP	Stream Control Transmission Protocol
SDES	Source Description
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SPDF	Service Policy Decision Function
SRTP	Secure RTP
StAC	Stream Admission Control
SSRC	Synchronization Source
THF	Topology Hiding Function
THIG	Topology Hiding Gateway
TLS	Transport Level Security
TTL	Time-To-Live
UDP	User Datagram Protocol
UE	User Equipment
VBR	Variable Bit Rate
VLAN	Virtual LAN
VPN	Virtual Private Network
XR	Extended Report

5 Conventions

None.

6 Rw interface protocol specification (ITU-T H.248 profile description)

The protocol specification relates to the definition of an ITU-T H.248 profile applicable for use at an ITU-T H.248-based Rw interface. The profile concept is inherently part of ITU-T H.248 (see clause 13 of [ITU-T H.248.1]). This profile is based on [b-ETSI TS 183 018] and follows the same structure (which is in line with the profile definition template according to Appendix III of [ITU-T H.248.1]).

The PD-PE has the "H.248 MGC" role in the scope of this ITU-T H.248 profile.

NOTE 1 – The function of PD-PE corresponds to the service policy decision function (SPDF) in [b-ETSI TS 183 018].

The PE-PE has the "H.248 MG" role in the scope of this ITU-T H.248 profile.

NOTE 2 – The function of PE-PD corresponds to the border gateway function (BGF) in [b-ETSI TS 183 018].

6.1 Profile identification

Table 6-1 – Profile identification

Profile name:	**ITU_PE-PE**
Version:	2

This ITU-T H.248 Profile for Rw interface is based on Profile "ETSI_BGF/3" as defined in [b-ETSI TS 183 018].

6.2 Gateway control protocol version

Recommendation ITU-T H.248.1 Version 3 should be applied to the Rw interface.

NOTE – Version 3 of the ITU-T H.248 protocol is needed, due to the possible usage of stream statistics and large size user datagram protocol (UDP) payload.

6.3 Connection model

Table 6-2 – Connection model

Maximum number of contexts	Provisioned
Maximum number of terminations per context	At least 2
Allowed terminations type combinations	(IP, IP)

6.4 Context attributes

Table 6-3 – Context attributes

Context attribute	Supported	Values supported
Topology	No	NA
Priority indicator	Yes	0-15
Emergency indicator	Yes	ON/OFF
IEPS indicator	No	NA
ContextAttribute descriptor	No	NA
ContextIdList parameter	No	NA
AND/OR context attribute	No	NA

6.5 Terminations

6.5.1 Termination names

6.5.1.1 IP termination

6.5.1.1.1 Overview and prose specification

The TerminationID structure shall follow the guidelines of ITU-T H.248 and shall be based on four fields:

- "ip/<group>/<interface>/<id>".

The individual fields are described and defined in Table 6-4.

Table 6-4 – IP termination fields

Name	Description	Values	CHOOSE wildcard	ALL wildcard
Ip	'ip' is a fixed prefix identifying the termination	'ip'	No	No
Group	Group of Interface and Id	Integer (0-65 535)	No	Yes
Interface	Logical or physical interface to a network to/from which the termination will be sending/receiving media (Notes 1 and 2).	String of maximum 51 alphanumeric characters	Yes (Note 5)	Yes
Id	Termination specific identifier (Note 3)	Non-zero 32-bit integer	Yes (Note 4)	Yes
NOTE 1 – A specific <Interface> may be used together with different groups. NOTE 2 – The generic field <Interface> may relate specifically to an "IP interface", "protocol layer 2 interface" or others. NOTE 3 – The combination of Interface and Id is unique. NOTE 4 – In version 1 of this profile, there was a tacit assumption that the media gateway controller (MGC) used a CHOOSE wildcard in an ADD request command. In this version, the MGC shall always use CHOOSE in an ADD request command. If not, the media gateway (MG) shall reply with an error descriptor using error code #501 "Not Implemented". See also clause 6.5.1.1.1.3. NOTE 5 – The MGC shall always use CHOOSE in an ADD request command. If not, the MG shall reply with an error descriptor using error code #501 "Not Implemented".				

NOTE – A specific address space may be associated with each interface or group of interfaces. In such cases, by specifying a partially wildcarded TerminationID in an ADD command, the PD-PE has the ability to choose the address space in which the PE-PE will allocate an IP address for the termination (e.g., ip/<group>/<interface>/$). The association of a TerminationID with a dedicated address space is related to "IP domain indication", which is also provided by the ipdc/realm property, see clause 6.16.1.7.

ITU-T H.248 wildcarding may be applied on IP termination identifiers. Wildcarding is limited according to the two columns on the right hand side.

6.5.1.1.1.1 Combined usage of fields group and interface

There are two potential relationships between <group> and <interface> within the TerminationID structure (see Figure 6-1):

a) *strictly hierarchical*: a single "interface" is completely associated to a dedicated "group"

e.g., may be driven for instance by hardware architecture or addressing schemes with the goal of minimizing ServiceChange command load by using wildcards such as `ip/<group>/*` for potential hardware (HW) failures that may lead to issuing a single ServiceChange command rather than multiple ServiceChange commands.

b) *partially hierarchical*: an "interface" is distributed over multiple "groups"

e.g., A logical partition concept may be driven for instance for selective auditing with the goal of minimizing the AuditReply to be of a manageable size by having the MGC to allocate an adequate number of terminations within a <group>. Therefore, audits could be paced for example: `ip/1/*`, `ip/2/*`, .., `ip/n/*`.

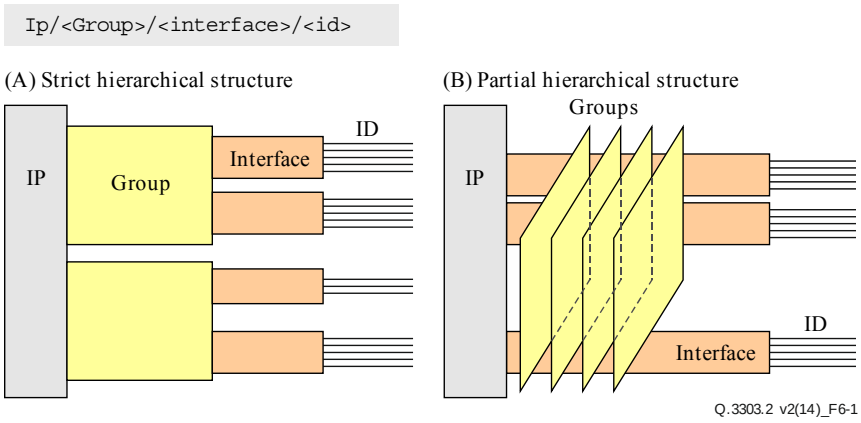


Figure 6-1 – Group/Interface relationships for the structure of terminationIDs

The following examples in Tables 6-5 and 6-6 depict the advantages that each group/interface relationship may facilitate.

Table 6-5 – Examples of group/interface relationship in ServiceChange

Semantic of termination name	**ServiceChange command (e.g., due to a HW failure)**	

Strictly hierarchical	Upon a HW failure the command issued is (by MG):
	`ServiceChange=ip/1/*{Services{`
	`Method=Restart,Reason="906"`
	`Version=3,Profile = ITU_PE-PE`
	`_2}}},`
	a single wildcarded command is possible (facilitated by a strict hierarchical relationship).	

Partially hierarchical	Upon a HW failure the command issued is (by MG):
	`ServiceChange=ip/*/1/*{Services{`
	`Method=Forced,Reason="906"`
	`}}},`
	`ServiceChange=ip/*/2/*{Services{`
	`Method=Forced,Reason="906"`
	`}}},`
	…
	`ServiceChange=ip/*/x/*{Services{`
	`Method=Forced,Reason="906"`
	`}}}`
	… a single wildcarded command is not always possible when not using a strict hierarchical relationship	

Table 6-6 – Examples of termination ID usage in AuditValue

Usage of termination ID structure	AuditValue command (e.g., Requesting a list of context IDs present in the MG where n and N are number of contexts in the AuditValue replies and n<<N)
Neither group nor interface levels specified in request	The command (from MGC): Context=*{AuditValue=Root{Audit{}}} Returns: Context=1{AuditValue=ip/1/11/101{},AuditValue=ip/1/12/102{}}, Context=2{AuditValue=ip/1/21/201{},AuditValue=ip/1/22/202{}}, Context=3{AuditValue=ip/1/31/301{},AuditValue=ip/1/32/302{}}, … Context=N{AuditValue=ip/256/11/504{},AuditValue=ip/256/12/534{}} … this could potentially return very large AuditValue Replies.
Group level specified in request	The command (by MGC): Context=*{AuditValue=ip/1/*{Audit{}}} Returns: Context=1{AuditValue=ip/1/11/101{},AuditValue=ip/1/12/102{}}, … Context=n{AuditValue=ip/1/51/121{},AuditValue=ip/1/52/122{}} … and this command would be repeated for each group. (facilitated by loose hierarchical relationship).

6.5.1.1.1.2 Optimization of call-independent procedures

The CHOOSE wildcard for "Interface" is introduced by this version of the profile.

The MGC may optimize (Note 1) call-independent procedures, e.g., based on the AuditValue command, by fully controlling the value allocation for the field Group.

NOTE 1 – "Optimization" could e.g., mean a load shaping function concerning ITU-T H.248 processing load.

The MG may optimize (Note 2) call-independent procedures, e.g., based on the ServiceChange command, via full control over the value allocation for field Interface.

NOTE 2 – "Optimization" may allow single wildcarded commands, see discussion in Tables 6-5 and 6-6.

6.5.1.1.1.3 Field "Id": Usage of wildcard CHOOSE or not

The CHOOSE wildcard for "Id" must be applied in the ADD.request command. It is the MGs responsibility for managing the value range of this logical resource.

6.5.1.1.2 Syntactical specification

6.5.1.1.2.1 ABNF grammar for ITU-T H.248 text encoding mode

Augmented Backus-Naur form (ABNF) [IETF RFC 5234] is used for the syntax specification. The ABNF for TerminationID and relation to pathNAME is defined in Annex B.2 of [ITU-T H.248.1].

ABNF coding:

```
pathNAME            = EphToken SLASH EPHsystem
EphToken            = "ip"                          ; prefix
EPHsystem           = WildcardALL
                        / WildcardALL SLASH Interface
                        / Group SLASH WildcardALL
                        / Group SLASH Interface SLASH  (Identifier/
                        WildcardALL/WildcardCHOOSE)
Group               = %d0-65535          ; data type: INT16
Interface           = 1*51ALPHANUM
Identifier          = %d1-4294967295   ; data type: INT32
ALPHANUM            = ALPHA/DIGIT
WildcardCHOOSE      = "$"
WildcardALL         = "*"
```

6.5.2 Multiplexed terminations

Table 6-7 – Multiplexed terminations

MultiplexTerminations supported?	No

6.6 Descriptors

6.6.1 TerminationState Descriptor

Table 6-8 – ServiceState property

ServiceState property used:	No

NOTE 1 – All ITU-T H.248 Terminations have a ServiceState property according to [ITU-T H.248.1], but explicit usage of the TerminationState Descriptor ServiceState property is not required by this profile. ServiceState changes can still occur, however, and be indicated in ServiceChange commands.

NOTE 2 – The value of the ServiceState property may be implicitly changed by ServiceChange procedures, or the value may be read by audit procedures, i.e., "Yes" for ServiceStates "InService" and "OutOfService" due to AuditValue and ServiceChange commands or "No" for ServiceState "Test".

Table 6-9 – EventBufferControl property

EventBufferControl property used:	No

6.6.2 Stream Descriptor

Table 6-10 – Stream Descriptor

Maximum number of streams per termination type	IP	5

Table 6-11 – Stream configuration

Stream configuration	All configurations are allowed.

6.6.2.1 LocalControl Descriptor (LCD)

Table 6-12 – LocalControl Descriptor

If not generic list appropriate termination and stream types		Termination type	Stream type
ReserveGroup used	No	–	–
ReserveValue used	No	–	–

Table 6-13 – Termination type

Termination type	Stream type	Allowed StreamMode values
IP	RTP/AVP	SendOnly, RecvOnly, SendRecv, Inactive
	TCP	SendRecv, Inactive
	UDPTL	SendRecv, Inactive
	UDP	SendOnly, RecvOnly, SendRecvInactive
NOTE – Other stream types are for further study.		

6.6.3 Events Descriptor

Table 6-14 – Events Descriptor

Events that can be set based on termination types and stream types	Yes		
If Yes	**Event ID**	**Termination type**	**Stream type**
	See clause 6.13.2.1 • g/cause	All except ROOT	Any
	See clause 6.13.2.3 • nt/netfail • nt/qualert	All except ROOT	Any
	See clause 6.13.2.11 • it/ito	Only ROOT	Not applicable
	See clause 6.13.2.16 • adid/ipstop	All except ROOT	Any
	See clause 6.13.2.14 • ocp/mg_overload	Only ROOT	Not applicable
	See clause 6.13.2.17 • hangterm/thb	All except ROOT	Not applicable
	See clause 6.13.2.18 • scr/cr	All except ROOT	Not applicable
	See clause 6.13.2.1 • ipra/arc	Only ROOT	Not applicable

Table 6-15 – EventBuffer control

EventBuffer control used	No

Table 6-16 – KeepActive

KeepActive used on events	No

Table 6-17 – Embedded events and signals

Embedded events in an Events Descriptor	No
Embedded signals in an Events Descriptor	No

Table 6-18 – Regulated embedded events

Regulated embedded events are triggered on	None

Table 6-19 – ResetEventsDescriptor

ResetEventsDescriptor used with events	None

Table 6-20 – NotifyImmediate, NotifyRegulated and NeverNotify

NotifyImmediate	All events
NotifyRegulated	None
NeverNotify	None

6.6.4 EventBuffer Descriptor

Table 6-21 – EventBuffer Descriptor

EventBuffer Descriptor used	No

6.6.5 Signals Descriptor

Table 6-22 – Signals Descriptor

Signals that can be set and are dependent on termination or streams types	Yes		
If yes	**Signal ID**	**Termination type**	**Stream type/ID**
	ipnapt/*	All except ROOT	Any

Table 6-23 – Signals lists

Signals lists supported	No

Table 6-24 – Signals type and duration

Signal type and duration supported	No

Table 6-25 – Signals direction

Signal direction supported	No

Table 6-26 – NotifyCompletion and RequestID

NotifyCompletion supported	No
RequestID parameter supported	No

Table 6-27 – Simultaneously played signals

Signals played simultaneously	No

Table 6-28 – KeepActive

KeepActive used on signals	No

6.6.6 DigitMap Descriptor

Table 6-29 – DigitMap Descriptor

DigitMaps supported	No

6.6.7 Statistics Descriptor

Table 6-30 – Statistics Descriptor

Statistics supported on	Stream

Table 6-31 – Statistics reported on subtract

Statistics reported on subtract	Yes	
If yes	**Statistic IDs reported**	All (see clause 6.13 for details)

6.6.8 ObservedEvents Descriptor

Table 6-32 – ObservedEvents Descriptor

Event detection time supported	No

6.6.9 Topology Descriptor

Table 6-33 – Topology Descriptor

Allowed triples	Not applicable.

6.6.10 Error Descriptor

Table 6-34 – Error codes sent by MGC

Supported ITU-T H.248.8 error codes	All
Supported error codes defined in packages	All error codes defined in supported packages need to be supported.

Table 6-35 – Error codes sent by MG

Supported ITU-T H.248.8 error codes	All with exception of • #514 "Media gateway cannot send the specified announcement" • #518 "Event buffer full" • #519 "Out of space to store digit map" • #520 "Digit map undefined in the MG" • #522 "Functionality requested in topology triple not supported"
Supported error codes defined in packages	All error codes defined in supported packages need to be supported.

6.7 Command API

Introductory note:

Tables 6-36 to 6-38 provide a summary overview of clauses 6.6 and 6.7 concerning descriptors and commands respectively. Where there are discrepancies between these tables and the corresponding text in clauses 6.6 and 6.7, the text takes precedence over those described in these tables.

Table 6-36 shows in which direction commands are sent, with which terminations they can be associated with and which wildcard options are supported for the specific command.

Table 6-36 – Commands and terminations

Command	**Sent by**	**Used on termination type**		**Wildcard support**	
		IP	**ROOT**	**W–**	**O–**
Add	PD–PE	Yes	No	No	No
AuditCapabilities	–	–	–	–	–
AuditValue	PD–PE	Yes	Yes	No	Yes
Modify	PD–PE	Yes	Yes	No	No
Move	–	–	–	–	–
Notify	PE–PE	Yes	Yes	No	No
ServiceChange	PE–PE	Yes	Yes	No	No
Subtract	PD–PE	Yes	No	Yes	No
NOTE 1 – O– indicates an optional command NOTE 2 – W– indicates a wildcarded response to a command					

Table 6-36 shows for which termination types a specific descriptor can be applied and Tables 6-37 and 6-38 show with which commands and replies the descriptor can be used, respectively.

Table 6-37 – Descriptors and requests

Descriptor type (Note 1)	Termination type							
	Root	**IP**						
Audit	Yes	Yes						
Error								
Events	Yes	Yes						
Local		Yes						
LocalControl		Yes						
Media	Yes (Note 2)	Yes						
ObservedEvents	Yes	Yes						
Packages	Yes							
ServiceChange	Yes	Yes					Yes	
Signals		Yes						
Statistics		Yes						
Stream		Yes						
TerminationState	Yes (Note 2)							

NOTE 1 – Only ITU-T H.248 descriptors supported within this ITU-T H.248 profile specification are shown.
NOTE 2 – E.g., Base Root package properties.

Table 6-38 – Descriptors and replies

Descriptor type (Note 1)	Termination type							
	Root	**IP**	**Add**					
Audit								
Error	Yes	Yes						
Events	Yes	Yes						
Local								
LocalControl (Note 2)		Yes						
Media	Yes	Yes						
ObservedEvents								
Packages	Yes							
Remote								
ServiceChange	Yes	Yes						
Signals (Note 3)								

Table 6-38 – Descriptors and replies

Descriptor type (Note 1)	Termination type							
	Root	**IP**	**Add**					
Statistics		Yes						
Stream		Yes						
TerminationState	Yes							
NOTE 1 – Only ITU-T H.248 descriptors supported within this ITU-T H.248 profile specification are shown. NOTE 2 – According to clause 6.7.5, **auditing** of mgcinfo/db ITU-T H.248 property in LocalControl is required. NOTE 3 – According to clause 6.7.5, **auditing** of ITU-T H.248 signals descriptors is not required.								

It is seen that an Error Descriptor may be returned in any command reply and thus the Error Descriptor is not included in any subsequent command reply table.

6.7.1 Add

Table 6-39 – Descriptors used by Add request

Descriptors used by Add request	Media (Stream(LocalControl, Statistics, Local, Remote)), Event, Signals
NOTE – Statistics are enabled by default. The MGC may explicitly request or suppress statistics generation for individual streams or terminations by inclusion of the Statistics Descriptor in the Add request command (see clause 7.1.15 of [ITU-T H.248.1]).	

Table 6-40 – Descriptors used by Add reply

Descriptors used by Add reply	Media (Stream(Local))

6.7.2 Modify

Table 6-41 – Descriptors used by Modify request

Descriptors used by Modify request	Media (TerminationState, Stream(LocalControl, statistics, Local, Remote)), Audit(Media(Stream(Statistics))), Signals, Event

Table 6-42 – Descriptors used by Modify reply

Descriptors used by Modify reply	Media(Stream(Local Statistics))

6.7.3 Subtract

Table 6-43 – Descriptors used by Subtract request

Descriptors used by Subtract request	Audit () OR NONE
NOTE – This profile version supports reporting of statistics on all streams or none of the streams. Reporting and disabling of statistics from a subset of the streams in case of multiple streams is not supported by this profile version. Termination level statistics are not supported.	

Table 6-44 – Descriptors used by Subtract reply

Descriptors used by Subtract reply	Media(Stream(Statistics)) or None

6.7.4 Move

Table 6-45 – Descriptors used by Move command

Move command used	No

6.7.5 AuditValue

Table 6-46 –AuditValue

Audited properties	Media(Termination state) (Note 1) Media(Stream(local control)) (Note 2)
Audited statistics	All
Audited signals	None
Audited events:	None
Packages audit possible	Yes
NOTE 1 – These are the root/*, seg/* and ipra/* properties. NOTE 2 – This is the mgcinfo/db property.	

6.7.6 AuditCapabilities

Table 6-47 – Descriptors used by AuditCapabilities command

AuditCapabilities command used	No

6.7.7 Notify

Table 6-48 – Descriptors used by Notify request

Descriptors used by Notify request	ObservedEvents

Table 6-49 – Descriptors used by Notify reply

Descriptors used by Notify reply	None

6.7.8 ServiceChange

Table 6-50 – ServiceChangeMethods and ServiceChangeReasons sent by MGC

Service change methods supported	ServiceChange reasons supported
Restart	900, 901
Handoff	903

Table 6-51 – ServiceChangeMethods and ServiceChangeReasons sent by MG

Service change methods supported	ServiceChange reasons supported
Restart	900, 901, 902
Forced	904, 905, 906, 915
Disconnected	900
Graceful	905, 908
Failover	909
Handoff	903

Table 6-52 – ServiceChangeAddress

ServiceChangeAddress used	No

Table 6-53 – ServiceChangeDelay

ServiceChangeDelay used	Yes	
If yes	Valid time period	Provisioned

Table 6-54 – ServiceChange incomplete flag

ServiceChange incomplete flag used	No

Table 6-55 – ServiceChangeVersion

Version used in ServiceChangeVersion	3

Table 6-56 – Profile negotiation

Profile negotiation as per ITU-T H.248.18	No

Table 6-57 – ServiceChangeMGCid

ServiceChangeMGCid used	Yes

6.7.9 Manipulating and auditing context attributes

Table 6-58 – Context attributes manipulation and auditing

Context attributes manipulated	Emergency, Priority
Context attributes audited	None

6.8 Generic command syntax and encoding

Table 6-59 – Command encoding

Supported encodings	Text (Notes 1 and 2)
NOTE 1 – The receiver shall be capable of receiving both short token notation and long token notation on an ITU-T H.248 control association. NOTE 2 – The transmitter may select between long and short token forms per ITU-T H.248 control association.	

6.9 Transactions

Table 6-60 – Maximum number of Transaction Requests/Replies/TransResponseAcks/Segment

Maximum number of Transactions Requests/Replies/TransResponseAcks/Segment Replies per message	1

Table 6-61 – Maximum number of commands per Transaction request

Maximum number of commands per Transaction request	2

Table 6-62 – Maximum number of commands per Transaction reply

Maximum number of commands per Transaction reply	2

Table 6-63 – Optional commands

Commands able to be marked "Optional"	AuditValue

Table 6-64 – Wildcarded commands

Commands able to be marked "Wildcarded"	Subtract

Table 6-65 – Transaction timer

Transaction timer	Value
normalMGExecutionTime	Provisioned, changeable with Base Root package (see clause 6.13.2)
normalMGCExecutionTime	Provisioned, changeable with Base Root package (see clause 6.13.2)
MGOriginatedPendingLimit	Provisioned, changeable with Base Root package (see clause 6.13.2)
MGCOriginatedPendingLimit	Provisioned, changeable with Base Root package (see clause 6.13.2)
MGProvisionalResponseTimerValue	Provisioned, changeable with Base Root package (see clause 6.13.2)
MGCProvisionalResponseTimerValue	Provisioned, changeable with Base Root package (see clause 6.13.2)

6.10 Messages

It is recommended that MGC and MG names are formatted as fully qualified domain names. For example the domain name of the MGC may be formatted as `mgc1.whatever.net` and the name of the MG may be formatted as `mg1.whatever.net`.

The fully qualified domain name will be used by the MGC and MG as part of the "Message Identifier" in the ITU-T H.248 messages, which identifies the originator of the message.

6.11 Transport

Table 6-66 – Transport

Supported transports	SCTP (Recommended) UDP (Optional)

Table 6-67 – Segmentation

Segmentation supported	**SCTP:** Inherent in transport **UDP:** Optional (dependent on support of Segmentation package, see clause 6.13.2.12)

Table 6-68 – Control association

Control association monitoring supported:	Monitoring mechanism is dependent on used ITU-T H.248 transport (see Table 6-66): **SCTP:** Inherent capability of SCTP. **UDP:** ITU-T H.248.14 (MG-driven monitoring). Empty AuditValue on ROOT (MGC-driven monitoring).

6.12 Security

Table 6-69 – Security

Supported security	None

6.13 Packages

This clause includes details of the mandatory and optional ITU-T H.248 packages that are included in this profile. A MG supporting this profile must support all the mandatory packages and may support zero, some or all of the optional packages. The MGC may use the ITU-T H.248 packages audit mechanism to determine which of the optional packages are supported by the MG. The meaning of mandatory and optional packages and their properties, signals, events, and statistics is provided in Appendix III of [ITU-T H.248.1].

6.13.1 Overview

Table 6-70 – Mandatory packages

Mandatory packages		
Package name	**Package ID**	**Version**
Generic (clause E.1 of [ITU-T H.248.1])	g	2
Base Root (clause E.2 of [ITU-T H.248.1])	root	2
Network (clause E.11 of [ITU-T H.248.1])	nt	1
Differentiated services [ITU-T H.248.52]	ds	2
Gate management (Appendix I of [ITU-T H.248.43])	gm	1
Traffic management [ITU-T H.248.53]	tman	1
IP NAPT traversal [ITU-T H.248.37]	ipnapt	1
IP domain connection [ITU-T H.248.41]	ipdc	1
Generic pull mode package [ITU-T H.248.55]	plm	1

Table 6-71 – Optional packages

Optional packages			
Package name	**Package ID**	**Version**	**Support dependent on**
MPLS [ITU-T H.248.54]	mpls	1	Support for MPLS label stacks, i.e., label switched paths (LSPs) terminated by the MG and related to the ITU-T H.248 termination.
VLAN [ITU-T H.248.56]	vlan	1	Support for virtual LAN (VLAN) tags and/or Ethernet priorities.
MGC information [ITU-T H.248.45]	mgcinfo	1	Support for MGC related recovery.
Inactivity timer [ITU-T H.248.14]	it	1	Applicable only for UDP transport (because UDP does not support any inherent keep alive mechanism).
Segmentation (clause E.14 of [ITU-T H.248.1])	seg	1	Applicable for UDP transport where sufficiently large messages are required to be supported.
RTP (clause E.12 of [ITU-T H.248.1])	rtp	1	Support of usage metering and statistics reporting. Particular package capabilities are only applicable for "media-aware" bearer connections.
Media gateway overload control [ITU-T H.248.11]	ocp	1	Support of message throttling, based on rate limitation, from MGC towards MG
Application data inactivity detection [ITU-T H.248.40]	adid	1	MGC requires to be explicitly informed of a cessation of an application data flow.

Table 6-71 – Optional packages

Optional packages			
Package name	**Package ID**	**Version**	**Support dependent on**
Hanging termination detection [ITU-T H.248.36]	hangterm	1	Support of hanging termination detection
Statistics conditional reporting [ITU-T H.248.47]	scr	2	Support of real time reporting of specific statistics based on a particular condition. This package may be supported as an operator option.
Gate management [ITU-T H.248.43]	gm	2	Support of filtering based on source port range
IP realm availability [ITU-T H.248.41]	ipra	1	Complements the IP domain connection package. Support of a mechanism allowing the MGC to discover the IP realms that are available at the MG at a certain time and on a mechanism allowing the MG to inform the MGC about change of availability of realms.
RTP application data package [ITU-T H.248.58]	rtpad	1	Support of usage metering and statistics reporting. Scope on traffic-volume based measurement of real-time transport protocol (RTP) application data (i.e., the media stream).
IP domain connectionLatch statistics [ITU-T H.248.37]	ipdclstat	1	MGC to address specific IP realm NOTE – Complements the IP NAPT traversal package to enable the recording of discarded packets due to implicit filtering by the latching function.
Traffic policing statistics [ITU-T H.248.53]	tmanr	2	Complements the traffic management package, allowing the recording of the number of packets and octets that did not conform to the traffic parameters, and the number of packets that were dropped due to such violations.
RSVP extension package [ITU-T H.248.65]	rsvp	1	Support of resource reservation protocol (RSVP) based on Pull mode resource control.

6.13.2 Package usage information

6.13.2.1 Generic (g)

Table 6-72 – Generic package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None				
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
Events	**Mandatory/ Optional**	**Used in command**		
Cause (g/cause)	M	ADD, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	None.			
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	General cause (Generalcause)	M	All	Not applicable
	Failure cause (Failurecause)	M	All	Not applicable
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				
Error codes	**Mandatory/Optional**			
None				

6.13.2.2 Base root (root)

Table 6-73 – Base root package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
MaxNrOfContexts (root/maxNumber OfContexts)	O	AUDITVALUE	All	Yes
MaxTerminationsPerContext (root/maxTermination PerContext)	O	AUDITVALUE	All	Yes

Table 6-73 – Base root package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
normalMGExecutionTime (root/normalMG ExecutionTime)	O	MODIFY, AUDITVALUE	All	Yes
normalMGCExecutionTime (root/normalMGC ExecutionTime)	O	MODIFY, AUDITVALUE	All	Yes
MGProvisional ResponseTimer Value (root/MGProvisionalResponse TimerValue)	O	MODIFY, AUDITVALUE	All	Yes
MGCProvisional ResponseTimer Value (root/MGCProvisional ResponseTimerValue)	O	MODIFY, AUDITVALUE	All	Yes
MGCOriginatedPendingLimit (root/MGCOriginated PendingLimit)	O	MODIFY, AUDITVALUE	All	Yes
MGOriginatedPendingLimit (root/MGOriginated PendingLimit)	O	MODIFY, AUDITVALUE	All	Yes
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ optional**	**Supported values**	**Duration provisioned value**
Events	**Mandatory/ Optional**	**Used in command**		
None				
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported Values**	
None				
Error codes	**Mandatory/Optional**			
None				

6.13.2.3 Network (nt)

Table 6-74 – Network package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
Maximum jitter buffer (nt/jit)	O	ADD, MODIFY	All	Yes
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
Events	**Mandatory/ Optional**	**Used in command**		
Network failure (nt/netfail)	O	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	None	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Cause (cs)	O	For further study (Note)	For further study (Note)
Quality alert (nt/qualert)	O	ADD, MODIFY, NOTIFY		
	Event Parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Threshold (th)	O	All	Not applicable
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned Value:**
	Threshold (th)	O	All	Not applicable

Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**
Duration (nt/dur)	O	ADD, SUBTRACT, MODIFY, AUDITVALUE	All
Octets sent (nt/os)	M	ADD, SUBTRACT	All
	O	MODIFY, AUDITVALUE	All
Octets received (nt/or)	M	ADD, SUBTRACT	All
	O	MODIFY, AUDITVALUE	All
Error codes	**Mandatory/Optional**		
None			

Table 6-74 – Network package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
NOTE – This event may be overloaded in order to address multiple failure causes (see clause E.11.5.1.2 of [ITU-T H.248.1]). An unambiguous distinction on MGC and MG sides implies mutually agreed cause code points. This is a provisioning activity.				

6.13.2.4 Differentiated services (ds)

Table 6-75 – Differentiated services package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
Differentiated services code point (ds/dscp)	M	ADD, MODIFY	All	Yes
Tagging behaviour (ds/tb)	O	ADD, MODIFY	All	Yes
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
Events	**Mandatory/ Optional**	**Used in command**		
None				
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				
Error codes	**Mandatory/Optional**			
None				

6.13.2.5 Gate management (gm)

Table 6-76 – Gate management package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
Remote source address filtering (gm/saf)	M	ADD, MODIFY	All	Not applicable (Note 1)
Remote source address mask (gm/sam)	O	ADD, MODIFY	All	Not applicable
Remote source port filtering (gm/spf)	M	ADD, MODIFY	All	Note 1
Remote source port (gm/spr)	O	ADD, MODIFY	All	Not applicable
Remote source port range (gm/sprr) (Note 3)	O	ADD, MODIFY	All	Not applicable
Explicit source address setting (gm/esas)	O	ADD, MODIFY	All	(Note 1)
Local source address (gm/lsa)	O	ADD, MODIFY	All	Not applicable
Explicit source port setting (gm/esps)	O	ADD, MODIFY	All	(Note 1)
Local source port (gm/lsp)	O	ADD, MODIFY	All	Not applicable
RTP specific behaviour (gm/rsb) (Note 4)	M	ADD, MODIFY	All	OFF (Note 2)
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	–	–	–

Table 6-76 – Gate management package

Events	**Mandatory/ Optional**	**Used in command**		
None	**–**	**–**		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	–	**–**	–	**–**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	–	–	–	–

Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**
Discarded packets gm/dp	O	ADD, MODIFY, SUBTRACT, AUDITVALUE	All
Error codes	Mandatory/Optional		
None			

NOTE 1 – Default value is 'OFF' in gm/1 (see clause B.2 of [ITU-T H.248.43]).

NOTE 2 – Default value must be provisioned in gm/1 (see clause B.2 of [ITU-T H.248.43]). The provisioned value in this profile shall be OFF.

NOTE3 – This property is defined in gm/2 while all other properties exist in gm/1.

NOTE 4 – The *gm/rsb* property is identical to the *rtcph/rsb* property (see Figure II.1 in [ITU-T H.248.43]) and defined by [ITU-T H.248.57]. The *rtcph* package defines *rsb* property semantics for the session description protocol (SDP) attribute according to [b-IETF RFC 3605] (see in particular clause 6.6.1.4.1 of [ITU-T H.248.57]). There are following package usage details for this profile specification: the SDP attribute "`a=rtcp:`" may be used in the ITU-T H.248 RD and shall **not** be used in the ITU-T H.248 **LD**.

6.13.2.6 Traffic management (tman)

Table 6-77 – Traffic management package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
Tman/pol	M	ADD, MODIFY	All	Yes
tman/pdr	M	ADD	All	Not applicable
tman/dvt	M	ADD	All	Yes
tman/sdr	M	ADD	All	Not applicable
tman/mbs	M	ADD	All	
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**

Table 6-77 – Traffic management package

Events	**Mandatory/ Optional**	**Used in command**		
None				
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				
Error codes	**Mandatory/Optional**			
None				

6.13.2.7 IP NAPT traversal (ipnapt)

Table 6-78 – IP NAPT traversal package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None				
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
Latching (ipnapt/latch)	M	ADD, MODIFY		Not applicable
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	NAPT traversal processing (napt)	M	All	Not applicable
Events	**Mandatory/ Optional**	**Used in command**		
None				
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				

Table 6-78 – IP NAPT traversal package

Error codes	Mandatory/Optional
None	

6.13.2.8 MPLS (mpls)

Table 6-79 – MPLS package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
Mpls/stack	M	ADD, MODIFY	All	Not applicable (Note)
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
Events	**Mandatory/ Optional**	**Used in command**		
None				
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				
Error codes	**Mandatory/Optional**			
None				
NOTE – "Not applicable" means that in case the *mpls/stack* property is absent, the MG shall not apply any MPLS label to the given termination/stream.				

6.13.2.9 VLAN (vlan)

Table 6-80 – VLAN package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported Values**	**Provisioned Value**
VLAN tags (vlan/tags)	O	ADD, MODIFY	All (Note)	Yes
Ethernet priority (vlan/pri)	O	ADD, MODIFY	All	Yes
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
Events	**Mandatory/ Optional**	**Used in command**		
None				
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				
Error codes	**Mandatory/Optional**			
None				
NOTE – "All" means value range "0 to 4 095" of property VLAN tags used for VLAN tagging; value "4 096" of property VLAN tags defines the semantic for "no VLAN tagging".				

6.13.2.10 MGC information (mgcinfo)

Table 6-81 – MGC information package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
All	M	ADD, MODIFY, AUDITVALUE	All	Not applicable
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
Events	**Mandatory/ Optional**	**Used in command**		
None				
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				
Error codes	**Mandatory/Optional**			
None				

6.13.2.11 Inactivity timer (it)

Table 6-82 – Inactivity timer package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None				
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**

Table 6-82 – Inactivity timer package

Events	**Mandatory/ Optional**	**Used in command**		
Inactivity timeout (ito)	M	MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Maximum inactivity time (mit)	O	All	Yes
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	None			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				
Error codes	**Mandatory/Optional**			
None				

6.13.2.12 Segmentation (seg)

Table 6-83 – Segmentation package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
MGSegmentation TimerValue (seg/ MGSegmentation TimerValue)	M	MODIFY, AUDITVALUE	All	Yes
MGCSegmentation TimerValue (seg/ MGCSegmentation TimerValue)	M	MODIFY, AUDITVALUE	All	Yes
MGMaxPDUSize (seg/ MGMaxPDUSize)	M	MODIFY, AUDITVALUE	All	Yes
MGCMaxPDUSize (seg/ MGCMaxPDUSize)	M	MODIFY, AUDITVALUE	All	Yes

Table 6-83 – Segmentation package

Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
Events	**Mandatory/ Optional**	**Used in command**		
None				
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				
Error codes	**Mandatory/Optional**			
459	M			

6.13.2.13 RTP package (rtp)

Table 6-84 – RTP package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None				
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**

Table 6-84 – RTP package

Events	**Mandatory/ Optional**	**Used in command**	
None			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**
Packets sent (rtp/ps)	M	ADD, SUBTRACT, AUDITVALUE	All
	O	MODIFY	
Packets received (rtp/pr)	M	ADD, SUBTRACT AUDITVALUE	All
	O	MODIFY	
Packet loss (rtp/pl)	M	ADD, SUBTRACT AUDITVALUE	All
	O	MODIFY	
Jitter (rtp/jit)	O	ADD, SUBTRACT AUDITVALUE, MODIFY	All
Delay (rtp/delay)	O	ADD, SUBTRACT AUDITVALUE, MODIFY	All
Octets sent, (rtp/os) (Note 1)	O	ADD, AUDITVALUE, SUBTRACT, MODIFY	All
Octets received, (rtp/or) (Note 2)	O	ADD, AUDITVALUE, SUBTRACT, MODIFY	All
Error codes	**Mandatory/Optional**		
None			

NOTE 1 – Inherited statistic from nt package. Value of rtp/os must be identical to nt/os (see clause E.12.5.2 of [ITU-T H.248.1]).

NOTE 2 – Inherited statistic from nt package. Value of rtp/or must be identical to nt/or (see clause E.12.5.2 of [ITU-T H.248.1]).

6.13.2.14 Media gateway overload control (ocp) package

Table 6-85 – Media gateway overload control package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None.	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	–	–	–
Events	**Mandatory/ Optional**	**Used in command**		
MG_Overload (ocp/mg_overload) (Note)	M	MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	None	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	None	–	–	–
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None.	–	–	–	
Error codes	**Mandatory/Optional**			
None.	–			

NOTE –When the MG is overloaded, overload events may be sent **either** only following the **first ADD.request** which creates a new Context, **or** following **all ADD.request** commands (see [ITU-T H.248.11]).

These two options result in different normalisations of the overload event rate as an indicator of the level of MG overload (see clause 6.16.2.3).

6.13.2.15 IP domain connection (ipdc)

Table 6-86 – IP domain connection package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
IP realm identifier (ipdc/realm)	M	ADD, MODIFY	All	Yes
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None	**–**	**–**		**–**
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	–	–	–
Events	**Mandatory/ Optional**	**Used in command**		
None	**–**	**–**		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	–	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	–	–	–	–
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None	–	–	–	
Error codes	**Mandatory/Optional**			
No	–			
NOTE – [ITU-T H.248.41] does specify a length limit for the ipdc/realm string, i.e., "Length limitation: Where the IP realm identifier property uses a domain name format, it shall handle names of up to 63 characters and should handle domain names of up to 255 characters in accordance with section 2.1 of [IETF RFC 1123]". In case the MGC uses an ipdc/realm property exceeding the above defined length limitation, the MG shall reply with an error descriptor using error code #4449: "Unsupported or Unknown Parameter or Property Value ".				

6.13.2.16 Application data inactivity detection (adid)

Table 6-87 – Application data inactivity detection package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None				
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
Events	**Mandatory/ Optional**	**Used in command**		
IP flow stop detection (adid/ipstop)	M	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Detection time (dt)	O	All	Yes
	Direction (dir)	O	All	Yes
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	None			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None				
Error codes	**Mandatory/Optional**			
None				

6.13.2.17 Hanging termination detection (Hangterm)

Table 6-88 – Hanging termination detection package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None	**–**	**–**		**–**
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	**–**	–	**–**
Events	**Mandatory/ Optional**	**Used in command**		
Termination	M	ADD, MODIFY, NOTIFY		

Table 6-88 – Hanging termination detection package

heartbeat (hangterm/-thb)	**Event parameters**	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Timerx (timerx)	**O**	0,1 up	**Yes**
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	–	–	–	–

Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**
None	–	–	–

Error codes	**Mandatory/Optional**
No	–

6.13.2.18 Statistic conditional reporting (scr)

Table 6-89 – Statistic conditional reporting package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	–	–	–
Events	**Mandatory/ Optional**	**Used in command**		
Conditional reporting, scr/cr	M	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Statistic identifier, si	M	All	Yes
	Duration, dur	O	All	Yes
	Period, per	O	All	Yes
	Maximum, max	O	All	Yes
	Minimum, min	O	All	Yes
	Normal, nor	O	All	Yes
	Request timestamp (rt)	O	All	Yes
	Value type (typ)	O	All	Yes
	Deviation (dev)	O	All	Yes

Table 6-89 – Statistic conditional reporting package

	Compliance (com)	O	All	Yes
	Direction (dir)	O	All	Yes
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Statistic identifier, si	M	All	–
	Value, val	M	All	–
Statistics	**Mandatory/ Optional**	**Used in command**		**Supported values**
None	–	–		–
Error codes	**Mandatory/Optional**			
None	–			

6.13.2.19 IP realm availability (ipra)

Table 6-90 – IP realm availability package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
Available realms, (ipra/ar)	M	AUDITVALUE	All	Not applicable
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	–	–	–
Events	**Mandatory/ Optional**	**Used in command**		
Available realms changed, (ipra/arc)	M	MODIFY, NOTIFY		
	Event parameters	**Mandatory/Optional**	**Supported Values**	**Provisioned value**
	–	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Newly available realms (nar)	O (Note)	All	Not applicable
	Newly unavailable realms (nur)	O (Note)	All	Not applicable

Table 6-90 – IP realm availability package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
None	–	–	–	
Error codes	**Mandatory/Optional**			
None	–			
NOTE – Although the ObservedEvent parameters ipr/nar and ipra/nur are optional as such, at least one parameter must be included in an ipra/arc ObservedEvent.				

6.13.2.20 RTP application data (rtpad)

Table 6-91 – RTP application data package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
None	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	–	–	–
Events	**Mandatory/ Optional**	**Used in command**		
None				
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
RTP payload octets sent, (rtpad/ payloados)	M	ADD, AUDITVALUE, SUBTRACT	All	
	O	MODIFY		
RTP payload octets received, (rtpad/ payloador)	M	ADD, AUDITVALUE, SUBTRACT	All	
	O	MODIFY		
Error codes	**Mandatory/Optional**			
None	–			

6.13.2.21 Latch statistics (lstat)

Table 6-92 – Latch statistics package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	–	–	–
Events	**Mandatory/ Optional**	**Used in command**		
None				
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
Discarded packets, (lstat/dp)	M	ADD, AUDITVALUE, SUBTRACT	All	
	O	MODIFY		
Error codes	**Mandatory/Optional**			
None	–			

6.13.2.22 Traffic policing statistics (tmanr)

Table 6-93 – Traffic policing statistics package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	–	–	–
Events	**Mandatory/ Optional**	**Used in command**		
None				
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**	
Discarded packets,	M	ADD, AUDITVALUE, SUBTRACT	All	

Table 6-93 – Traffic policing statistics package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
(tmanr/dp)	O	MODIFY		
Peak-rate violating packets, (tmanr/pvp)	O	ADD, AUDITVALUE, SUBTRACT		All
	O	MODIFY		
Peak-rate violating octets, (tmanr/pvo)	O	ADD, AUDITVALUE, SUBTRACT		All
	O	MODIFY		
Sustained-rate violating packets, (tmanr/svp)	O	ADD, AUDITVALUE, SUBTRACT		All
	O	MODIFY		
Sustained-rate violating octets, (tmanr/svo)	O	ADD, AUDITVALUE, SUBTRACT		All
	O	MODIFY		
Error codes	**Mandatory/Optional**			
None	–			
NOTE – The statistic tmanr/dp is mandatory because independent of the applied policing mechanism. The other four statistics are optional because dependent on peak- or sustained-rate policing.				

6.13.2.23 Generic pull mode package (plm)

Table 6-94 – Generic pull mode package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
Path coupled request domains under MGC ownership (plm/rdmo)	M	MODIFY, AUDITVALUE	All	Provisioned
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
None.	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	–	–	–	–
Events	**Mandatory/ Optional**	**Used in command**		
Decision request for QoS resource reservation (plm/rdrr)	M	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**

Table 6-94 – Generic pull mode package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
	Bearer request address value (brav)	O	–	–
	Bearer request port value (brpv)	O	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Authorization token (authtok)	M	–	–
Decision request for QoS resource modification (plm/rdrm)	M	ADD, MODIFY, NOTIFY	–	–
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	None.	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Authorization token (authtok)	M	–	–
Events	**Mandatory/ Optional**	**Used in command**		
Decision request for QoS resource release (plm/rdrl)	M	ADD, MODIFY, NOTIFY	–	–
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	None.	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Authorization token (authtok)	M	–	–

Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**
None.	–	–	–

Error codes	**Mandatory/Optional**
None.	–

6.13.2.24 RSVP extension package (rsvp)

Table 6-95 –RSVP extension package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
None	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**
Send path (rsvp/path)	M	ADD, MODIFY		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	Session ID (session)	M	–	–
	Sender TSpec (stspec)	O	–	–
	Ad spec (adspec)	O	–	–
	Policy data (policy)	O	–	–
	Data TTL (dttl)	O	–	–
	Time value (time)	O	–	–
Send Resv (rsvp/resv)	M	MODIFY		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	Session ID (session)	M	–	–
	Style (style)	M	FF, SE, WF (Note)	Provisioned
	Flow spec (flowspec)	O	–	–
	Filter spec (filterspec)	O	–	–
	Policy data (policy)	O	–	–
	Confirm flag (confirm)	O	ON, OFF	Provisioned
	Time value (time)	O	–	–
RSVP release (rsvp/release)	M	MODIFY		–
	Signal parameters	**Mandatory/ Optional**	**Supported values**	**Duration provisioned value**
	Session ID (session)	M	–	–

Table 6-95 –RSVP extension package

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**
	Message Type (mtype)	O	PathTear, ResvTear	–
Events	**Mandatory/ Optional**	**Used in command**		
Path received (rsvp/pathr)	M	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported value:**	**Provisioned value**
	None.	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**Provisioned value**
	Session ID (session)	M	–	–
	Sender TSpec (stspec)	O	–	–
	Ad Spec (adspec)	O	–	–
	Policy data (policy)	O	–	–
Resv received (rsvp/resvr)	M	ADD,MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Event parameters**
	None.	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**ObservedEvent parameters**
	Session ID (session)	M	–	–
	Style (style)	M	FF, SE, WF (Note)	Provisioned
	Flow Spec (flowspec)	O	–	–
	Filter Spec (filterspec)	O	–	–
	Policy data (policy)	O	–	–
Path error (rsvp/patherr)	M	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Event parameters**
	None.	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**ObservedEvent parameters**
	Session ID (session)	M	–	–
	Error spec (errspec)	M	–	–
	Policy data (policy)	O	–	–

Table 6-95 –RSVP extension package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
Resv Error (rsvp/resverr)	M	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Event parameters**
	None.	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**ObservedEvent parameters**
	Session ID (session)	M	–	–
	Error specification (errspec)	M	–	–
	Flow spec (flowspec)	O	–	–
	Filter spec (filterspec)	O	–	–
	Policy data (policy)	O	–	–
Resv Confirm (rsvp/resvconf)	M	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Event parameters**
	None.	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**ObservedEvent parameters**
	Session ID (session)	M	–	–
	Style (style)	M	FF, SE, WF (Note)	Provisioned
	Flow spec (flowspec)	O	–	–
	Filter spec (filterspec)	O	–	–
	Policy data (policy)	O	–	–
RSVP teardown (rsvp/teardown)	M	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Event parameters**
	None.	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**ObservedEvent parameters**
	Session ID (session)	M	–	–

Table 6-95 –RSVP extension package

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value
State expiration (rsvp/se)	M	ADD, MODIFY, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values**	**Event parameters**
	State expiration interval (sei)	O	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values**	**ObservedEvent parameters**
	Session ID (session)	M	–	–
Error codes	**Mandatory/Optional**			
None	–			
NOTE – FF = Fixed-Filter, SE=Shared-Explicit and WF=Wildcard-Filter				

6.14 Mandatory support of SDP and Annex C information elements

Elements listed as mandatory shall be supported by MGC and MG but does not have to be present in all commands containing SDP. Details of which elements are included in each command are provided in clause 6.17.

NOTE – "Annex C" relates to [ITU-T H.248.1] Annex C, "Tags for media stream properties". Annex C information elements are not required in ITU-T H.248 text encoding mode.

Table 6-96 – Supported SDP information elements

SDP information element		Mandatory	Description
Protocol version "v=" line		Mandatory	The value must always be equal to zero: v=0
Connection "c=" line		Mandatory	The *network type* must always be "IN". The *address type* value must be "IP4" or "IP6". The *connection address* value may be underspecified with CHOOSE wildcard ("$").
Media "m=" line		Mandatory	There are four fields (or SDP values) <media>, <port>, <proto> and <fmt> in the "m=" line (see [IETF RFC 4566]; (Note 3)). The "m=" line may be omitted from SDP (Note 6)
	Media type <media>	Mandatory if "m=" line included	"-" may be used for the *media* value. Other values shall be ignored, unless media specific information is required. The *media* value shall be specified in case of media-aware interworking. (Note 2)

Table 6-96 – Supported SDP information elements

SDP information element		Mandatory	Description	
	Transport port <port>	Mandatory if "m=" line included	The *port* value may be underspecified with CHOOSE wildcard ("$").	
	Transport protocol <proto>	Mandatory if "m=" line included	udp	Allow only L4 protocol = UDP.
			tcp	Allow only L4 protocol = TCP.
			RTP/AVP	Allow only L4 protocol = UDP. (Note 1)
			udptl	Allow only L4 protocol = UDP.
			–	No transport protocol specific behaviour is required by the MG.
	Media format <fmt>	Mandatory if "m=" line included	"-" may be used for the *format list* value, e.g., in case of media-agnostic interworking. Other values may be used for media-aware interworking (e.g., transcoding; see clause 6.16.1.13). (Note 2)	
Bandwidth "b=" line		Mandatory NOTE – MUST not be used without a "m=" line.	The *modifier* value must always be "AS". This implies that the *bandwidth-value* represents the ""maximum bandwidth" (see section 5.8 of [IETF RFC 4566]). The *bandwidth-value* relates therefore to the *peak bit-rate* (Note 7). The *bandwidth-value* defines the IP layer bandwidth for the specific ITU-T H.248 Stream. (Notes 4 and 5). For RTP flows, where RTP control protocol (RTCP) resources are reserved together with the RTP resources using the "RTP Specific Behaviour" property of the Gate Management package (gm) property, the *bandwidth* value will include the bandwidth used by the RTP and the RTCP together.	

NOTE 1 – Even if the transport value is RTP, the "RTP Specific Behaviour" property of the Gate Management package (gm) shall be used to indicate whether RTCP resource reservation is also requested.

NOTE 2 – For Ia profile version 2 ITU-T H.248 profile [IETF RFC 4566] shall be used as basis. [IETF RFC 4566] enables "-" as a valid character (Ia profile version 1 uses [b-IETF RFC2327], which does not allow the "-" in place of media type, transport and media format fields. However, in the scope of Ia profile version 1, this was considered as an admitted SDP extension).

NOTE 3 – RFC 4566 obsoleted RFC 2327, but the augmented Backus-Naur form (ABNF) grammar did slightly change for the "m=" line:

a) RFC 2327: `m=<media> <port> <transport> <fmt list>`

b) RFC 4566: `m=<media> <port> <proto> <fmt> ...`.There is a syntactical change for the last two fields, but the semantical meaning is unchanged.

See also [ITU-T H.248.49], Appendix I "Comparison of SDP variants between RFC 4566 and RFC 2327"

Table 6-96 – Supported SDP information elements

SDP information element	Mandatory	Description
and in particular: Table I.7 of [ITU-T H.248.49] "RFC 4566 versus RFC 2327 – SDP specification – "m=" line". NOTE 4 – This semantic is consistent for RTP traffic (see section 6.2 of [IETF RFC 3550]) and non-RTP traffic (see section 5.8 of [IETF RFC 4566]). NOTE 5 – It has to be noted that Ia profile version 1 has a different semantic (see Table 81 in [ETSI ES 283 018]) defined, which incorporates also layer 2 bit-rate. A transformation between both "b=" line usages (in case of IP-over-L2) is not straightforward because the transformation parameters are based on L2-PCI and the IP packet rate. The L2-PCI is typically constant for a dedicated L2 technology (like IP-over-IEEE 802.3), but the packet rate is application-specific. E.g., the IP packet rate is usually unknown at Ia for media-agnostic IP-to-IP interworking. NOTE 6 – The "m=" and "b=" lines may be omitted in certain procedures, which are further described in clause 6.16.1.11. NOTE 7 – The unit for the *bandwidth-value* (peak bit rate) is "kbit/s". The unit for the *peak data rate* (tman/pdr) is "byte/s". The "b=" line is not providing any information about the traffic characteristic, i.e., whether the traffic flow has a constant bit rate (CBR) or variable bit rate (VBR). The *bandwidth-value* is thus independent of the traffic characteristic and relates to the peak bit rate for CBR and VBR traffic (see also clause 6.16.1.5).		

6.15 Optional support of SDP and Annex C information elements

NOTE – "Annex C" relates to [ITU-T H.248.1] Annex C, "Tags for media stream properties". Annex C information elements are not required in H.248 text encoding mode.

Table 6-97 summarizes the "optional" SDP information elements, based on their specific usage according to clause 7.1.8 of [ITU-T H.248.1]. Their usage may depend on the direction from MGC towards MG or vice versa.

Table 6-97 – Optional SDP information elements

SDP information element	Mandatory/optional	Description
Origin "o=" line	Optional for MGC, Mandatory for MG	The origin line consists of six fields (<username>, <session id>, <version>, <network type>, <address type>, and <address>). The MGC is not required to supply this line, but shall accept it (see clause 7.1.8 of [ITU-T H.248.1]). The MG shall populate this line as follows, e.g.,: `o=- 0 0 IN IP4 11.9.19.65` or use the value received from the MGC.
Session name "s=" line	Optional for MGC, Mandatory for MG	The session name "s=" line contains a single field (<session name>). The MGC is not required to supply this line, but shall accept it (see clause 7.1.8 of [ITU-T H.248.1]). The MG shall populate this line as

Table 6-97 – Optional SDP information elements

SDP information element	Mandatory/optional	Description
		follows, e.g.,: `s=-` or use the value received from the MGC
Times, repeat times and time zones "t=" line	Optional for MGC, Mandatory for MG	The time "t=" line consists of two fields (<start time> and <stop time>). The MGC is not required to supply this line but shall accept it (see clause 7.1.8 of [ITU-T H.248.1]). The MG shall populate this line as follows, e.g.,: `t=0 0` or use the value received from the MGC.
Attribute "a=" line	Optional for MGC, Recommended for MG	1) Application "RTCP port control": The attribute "a=" line may either contain (a=rtcp: <port>) or (a=rtcp: <port> <network type> <address type> <connection address>) when the "a=" line is used for RTCP port transmission. The MGC shall supply the "a=" line in the Remote Descriptor (RD) when non-default RTCP port values are used by the peer media entity. The "a=" line is ignored by the MG if received from the MGC with a request for latching (ipnapt/latching) or if property gm/rsb=OFF (see clause 6.16.1.7).
	Optional for MGC, Optional for MG	2) Application "Media-aware interworking (transcoding)": The "a=" line provides the complementary information for the "m=" line (see Table 6-15) with regards to a specified media type/format. For a dynamic RTP payload type, for each media information on the codec type shall be provided in a separate SDP "a=rtpmap" line and possibly additional SDP "a=fmtp"-line(s).

6.16 Overview of procedures

Details of session dependent procedures are provided in clauses 6.17. Details of session independent procedures are provided in clauses 6.18 and 6.19.

6.16.1 Overview of session dependent procedures

The various policing functions of the PE-PE are summarized in Appendix I. The specific types of *address* policing and *traffic* policing are in scope of clauses 6.16.1.1 and 6.16.1.5 respectively.

The general procedures are related to session-dependent (also known as ITU-T H.248 call-dependent) procedures. There are procedures in following categories:

- Address allocation and translation is in scope of clauses 6.16.1.2. The adaptation of addresses (latching) is the subject of clause 6.16.1.2.
- Session-dependent policing is applicable to this profile. The specific types of address policing and traffic policing are in scope of clauses 6.16.1.1 and 6.16.1.5 respectively. Media type policing is discussed in clause 6.16.1.8.
- QoS support mechanisms are discussed in clause 6.16.1.4.
- Measurement and reporting of statistics are discussed in clause 6.16.1.6.
- RTCP handling (e.g., IP port allocation rules for RTCP) is discussed in clause 6.16.1.7.
- Detection of inactive bearer connections is in scope of clauses 6.16.1.9.
- IP realm/domain indication is discussed in clause 6.16.1.10.
- Two-stage MG resource reservation is discussed in clause 6.16.1.11.
- Detection of hanging ITU-T H.248 terminations is discussed in clause 6.16.1.12.
- Real time statistics reporting 6.16.1.13.
- Transcoding is discussed in clause 6.16.1.14.
- Virtual private network (VPN) identification is discussed in clause 6.16.1.15.
- Topology hiding is discussed in clause 6.16.1.16.

6.16.1.1 Gate control

6.16.1.1.1 Streams, terminations and gates

The realization of a gate requires two ephemeral terminations. An ephemeral termination sources and/or sinks one or more media streams. Gates are direction and stream dependent.

In this Profile, RTP traffic shall also be controlled through a single ITU-T H.248 stream, representing both the RTP and RTCP flows, if the RTP Specific Behaviour property of the Gate Management package is set to ON. In such a case, when the MG is requested to allocate a port for an RTP flow, a consecutive port for the associated RTCP flow is automatically allocated (see also clause 6.16.7).

In this case, mono-media sessions require one bidirectional ITU-T H.248 stream on a termination, while a multi-media sessions (e.g., audio and video) would require multiple ITU-T H.248 streams on a termination (one stream per media type).

6.16.1.1.2 Assignment of L3 address and L4 port values

The ITU-T H.248 base protocol enables the PD-PE to choose the IP address and port on which a termination will receive media flows. In addition, the Gate Management package enables the PD-PE to explicitly provide the following information:

- expected IP source address and port of received packets;
- IP source address and port of sent packets.

The relationship between ITU-T H.248 descriptors in this Profile and the addresses used in packets sent and received by the gate is indicated in Table 6-98. Figure 6-2 illustrates the used naming conventions for the IP transport connection endpoints in the PE-PE and remote IP node.

Table 6-98 – Relation between packet direction, IP address/port and ITU-T H.248 descriptor/information

Packet direction	IP Address/L4 Port	Source of information for transport address values
Received by termination	Source: • RS (A) • RS (P)	The source of information for the expected remote source transport address RS (A, P) value is dependent on the usage of remote source filtering and hosted NAP(T) traversal as per Table 6-99.
	Destination : • LS (A) • LS (P)	Local destination transport address LD (A, P): Local Descriptor
Sent by termination	Source : • LS (A) • LS (P)	Local source transport address LS (A, P): 1. Availability of LS information due to explicit setting of local source transport address: LocalControl Descriptor/gate management/local source address + local source port or, if not present: 2. Availability of LS information in ITU-T H.248 Local Descriptor SDP: Source address not explicitly enforced/signalled via "gm" package. The source address is determined from the local SDP (which implies a symmetrical local network address, i.e., LD (A) = LS (A)).
	Destination : • RD (A) • RD (P)	The source of information for the remote destination transport address RD (A, P) value is dependent on the usage of hosted NAP(T) traversal as per Table 6-100.

Table 6-99 – Expected remote source transport address

Expected remote source transport address RS (A, P):		Hosted NA(P)T traversal	
		No	**Yes**
Filtering on remote source address(es)	**No**	As no source filtering activated no specific RS (A, P) is expected. The PE-PE may determine actual RS (A) and RS (P) values by monitoring incoming IP packets.	The expected remote source transport address is determined by the NAPT traversal process as described in [ITU-T H.248.37]. Even if no filtering is ordered, the NAPT traversal process implies source filtering on the transport address after latching has occurred.
	Yes	Alt 1. LocalControl Descriptor/gate management/remote source address mask AND/OR remote source port or remote source port range is used to determine the expected. RS(A) and RS(P) values, which allows for the peer IP node to use asymmetric network address (RS(A) ≠ RD(A)). Alt 2. Combination of gate management and Remote Descriptor, which assumes symmetrical remote network address (RS(A) = RD(A)).	First stage (before latching): Same as in cell to the left. Second stage (after latching): Same as in above cell.

Table 6-100 – Source of information for the remote destination transport address

Remote destination transport address RD (A, P):	Hosted NA(P)T traversal	
	No	**Yes**
Source of information	The remote destination transport address is determined by the Remote Descriptor.	The remote destination transport address is determined by the NAPT traversal process as described in [ITU-T H.248.37]. This implies a symmetrical remote network address, i.e., RD(A) = RS(A).

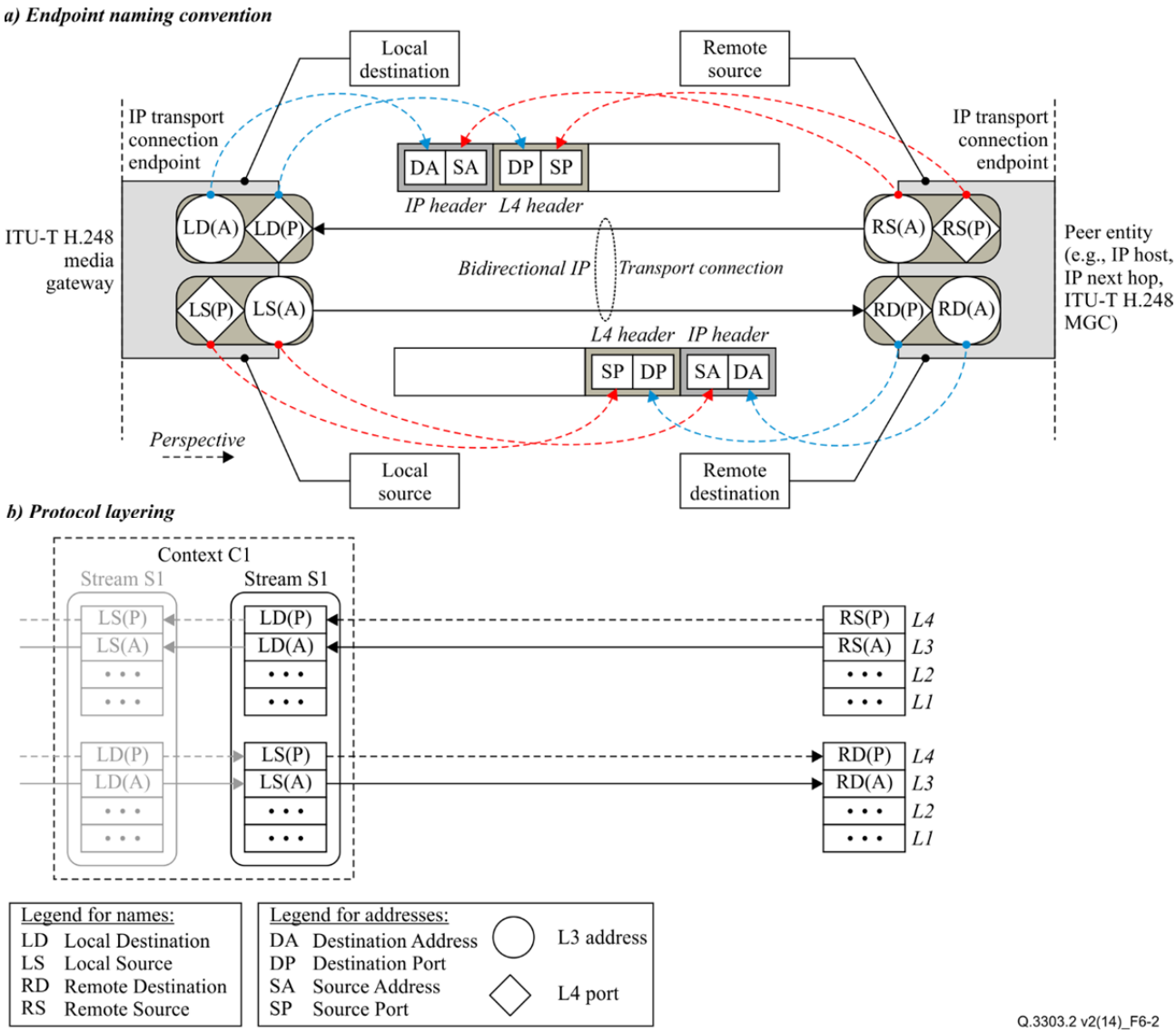


Figure 6-2 – Naming conventions for IP *transport connection* endpoints (from PE-PE perspective; in line with ITU-T H.248.1 conventions)

NOTE – ITU-T H.248.1 may in the future provide a general overview of IP transport connection endpoints similar to Figure 6-2. Figure 6-2 will be then replaced by a reference to [ITU-T H.248.1].

6.16.1.1.3 Opening and closing gates

Opening and closing gates is achieved by setting the Stream mode parameter of the associated termination(s) to the appropriate values. Subtracting a termination from a context also closes the gate for all ITU-T H.248 streams in the termination.

In the context of conversational services, an active session requires that the gates in both directions be opened (terminations in bi-directional mode).

6.16.1.1.4 Filtering due to conditions on L3 address and/or L4 port values

Filtering on the IP source address and/or port might be implemented using the Gate Management package, or using the SDP information in the Remote Descriptor. In case the filtering is done based on the Remote Descriptor, the activation/deactivation of the filtering is configured in the PE-PE. If the Gate Management package is used, it shall override the configured value in the PE-PE.

NOTE – It should be noticed that the IP source address and port may not always be available to the PD-PE. When session initiation protocol (SIP) signalling is used, the session description does not contain this information (i.e., according to [IETF RFC 3264], the IP address and port present in an SDP offer indicate

nothing about the source IP address and source port of RTP and RTCP packets that will be sent by the offerer). Any other protocol that uses SDP as a session description mechanism (e.g., RTSP) has the same constraints.

In such configurations, the Gate Management package may be used as follows:

- in an IPv6 environment, the Source Address Mask property contains the 64 bits prefix of the IP address that is set in the termination's Remote Descriptor;
- in an IPv4 environment, the Source Address Mask property contains the IP address that is set in the termination's Remote Descriptor, except that a number of trailing digits may be wildcarded;
- in both cases above, Source Port filtering should not be activated.

The gate concept, together with ITU-T H.248 Stream/Termination handling, is further illustrated in Annex A of [b-ETSI ES 283 018].

6.16.1.2 Allocation and translation of IP addresses, ports and versions (NAPT-PT)

6.16.1.2.1 Allocation methods

The procedures of this clause support the following NAPT and protocol translation (NAPT-PT) functionality:

- NAPT-PT functionality with "double" addresses and ports translation (both source and destination addresses and ports are translated), or;
- optional NAPT-PT functionality with "single" address and port translation (either source or destination address and port translation) – applicable if the PE-PE has router functionality, or direct L2 connectivity with user terminals.

The ITU-T H.248 base protocol enables the PD-PE to either choose the addresses and ports associated with a termination or to request the PE-PE to allocate these IP addresses and ports. NAPT control on destination addresses and ports is achieved by setting the Local and Remote Descriptors according to the following principles:

- The IP and port address in the Remote Descriptors are set by the PD-PE according to the information received in call/session signalling (e.g., SDP in SIP INVITE and 200 OK).
- The address and port in the Local Descriptor are selected by the PE-PE within the indicated IP address realm from PD-PE side (see also below).

If the PE-PE has router functionality, or direct L2 connectivity with the user terminals, the address and port of the Local Descriptor towards the private network may optionally be set according to the following principles:

- The IP and port address in the Local Descriptor towards the private network is provided by the PD-PE (instead of being selected by the PE-PE). The PD-PE shall copy the Remote Descriptor of the public network into the Local Descriptor towards the private network.

The PD-PE has the ability to choose the address space in which the PE-PE allocates an IP address. This is achieved by setting the IP realm identifier in the Domain Connection package to the appropriate value (see clause 6.5.1.1). The association of dedicated "IP address spaces" (also known as "IP address realms" or briefly "IP realms", see [b-IETF RFC 2663]) with the IP realm identifier requires a mutual agreement between PD-PE and PE-PE. This is realized via provisioning, thus beyond the scope of this Profile. However the PD-PE can discover which realms are supported by the PE-PE through the use of the IP realm availability package (see clause 6.16.1.10.5).

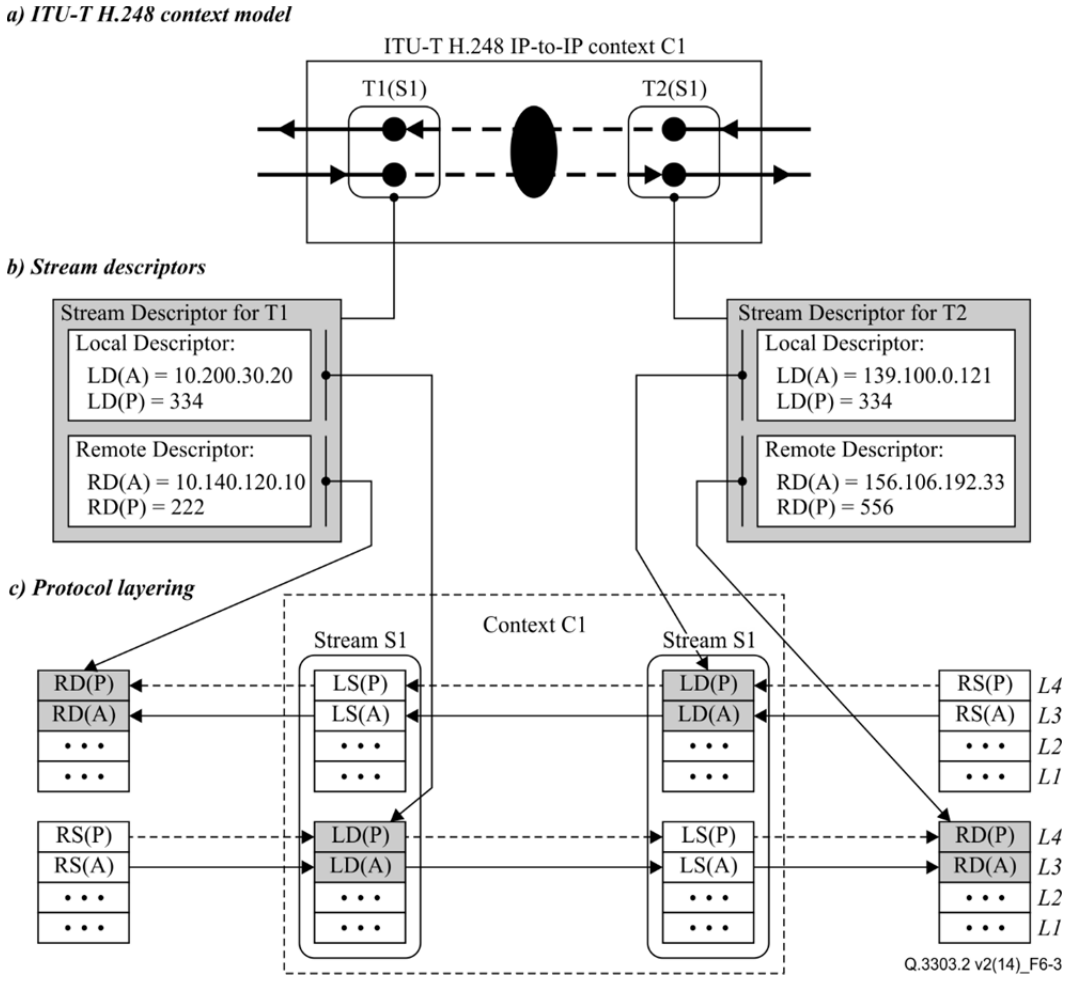
6.16.1.2.2 "Double" NA(P)T

The term "double" NA(P)T relates to the translation of source *and* destination address information:

- "double" NAT = translation of 2-tuple (DA, SA) is *not* supported by this profile (because it would require the L4-port agnostic mode);
- "double" NAPT = translation of 4-tuple (DA, SA, DP, SP), i.e., L4-port aware mode.

Example: (here "double" NAPT):

Figure 6-3 provides an example of "double" network address and port translation, where a session is to be established between IPv4 addresses 10.140.120.10 (private address) and 156.106.192.33 (public address).



NOTE – There is only one ITU-T H.248 Stream (S1) per Termination in this example

Figure 6-3 – Network address and port translation (NAPT) – Example for bidirectional ("double") translation

6.16.1.2.3 "Single" NA(P)T

The term "single" NA(P)T relates to the translation of either source-only or destination-only address information:

- "single" NAT = translation of 1-tuple (SA) or (DA) is not supported by this profile (because it would require the L4-port agnostic mode);
- "single" NAPT = translation of 2-tuple (SA, SP) or (DA, DP), i.e., L4-port aware mode.

Example (here "single" NAPT on (DA, DP)-tuple elements):

For "single" network address and port translation applications, the T1 Local Descriptor address and port in Figure 6-3 has to be changed to 156.106.192.33: 556 (equal to the T2 Remote Descriptor address and port).

T1-to-T2 IP flow direction:

- The (DA, DP)-tuple values will be then *not* changed (called "destination NAPT-less"), whereas the (SA, SP)-tuple values are translated ("source NAPT-full" mode).
  = single NAPT

T2-to-T1 IP flow direction:

- The (DA, DP)-tuple values *and* the (SA, SP)-tuple values are both translated ("source and destination NAPT-full" mode).
  = double NAPT

6.16.1.2.4 NA(P)T-less case

See also Annex H.3 of [b-ETSI TR 183 068]

6.16.1.2.4.1 NA(P)T-less B2BIH mode

For NA(P)T-less applications, the T1 Local Descriptor address and port in Figure 3 has to be changed to 156.106.192.33: 556 (equal to the T2 Remote Descriptor address and port) and the T2 Local Descriptor address and port in Figure 6-3 has to be changed to 10.140.120.10: 222 (equal to the T1 Remote Descriptor address and port).

Further aspects from ITU-T H.248 control perspective:

- there is either a "source and destination NAT-less" mode (briefly NAT-less),
- or a "source and destination NAPT-less" mode (briefly NAPT-less);
- all other combinations may be mapped on NA(P)T-full scenarios (e.g., L3 NAT-less but L4 port translation).
- The NAT-less back-to-back IP host (B2BIH) and NAPT-less B2BIH mode using both the same ITU-T H.248 control method, i.e., the RD(A,P) address value from the ITU-T H.248 RD is copied by the PD-PE in the LD(A,P) value of the ITU-T H.248 LD of the other ITU-T H.248 IP Termination. This can only be done once the RD of both terminations are known to the PD-PE and the profile thus allows for a LD to be absent in the ADD request command.

6.16.1.2.4.2 NA(P)T-less IP router (IPR) mode

See Annex H of [b-ETSI TR 183 068], not supported by this profile.

6.16.1.2.5 NA(P)T and explicit local source transport address settings

NAPT control on source addresses and ports (i.e., source NAPT) is achieved by setting the local source address and local source port properties defined in the Gate Management package to a value that differs from the actual source address of the packets received from the remote entity.

The *gm* package capabilities may be also used for source NAT control only, i.e., without explicit L4 port settings.

The explicit local source setting capabilities will lead to an overall:

- "single NA(P)T" mode in case of a destination NA(P)T-less mode; or
- "double NA(P)T" mode in case of a destination NA(P)T-full mode.

6.16.1.2.6 Protocol translation (between V4 and V6)

Protocol translation (NAPT-PT) can be controlled by the PD-PE by adding to the same ITU-T H.248 context, two terminations whose media descriptors have different address-type values in the "c=" line.

NOTE – It is recommended that the PD-PE takes precaution if setting up streams with both fully specified and under specified address and/or port towards the same realm in a PE-PE, as this could otherwise lead to

conflicting address or port assignments. The exact mechanism for how clashes are avoided is beyond the scope of this profile.

6.16.1.3 Support of hosted NAT traversal

"Hosted NAT Traversal" relates to "assisting remote NAT/NAPT traversal" for the remote (peer) IP connection endpoints from PE-PE/PD-PE point of view. This relates to an interim NA(P)T device from border gateway (BGW) perspective. The remote IP address information cannot be retrieved from the Remote Descriptor. The "Hosted NAT Traversal" function is controlled by the PD-PE using the IP NAPT Traversal package (ipnapt). Using the napt package, the PE-PE is requested to perform media latching, i.e., listen for incoming media and latch to the remote address information of that media.

When Hosted NAT Traversal is applied to a stream associated with multiple flows (for example RTP and RTCP), the PE-PE shall perform individual latching and/or re-latching on the various flows. This means that an RTP and an RTCP flow of a single stream can be latched to different remote addresses and/or ports.

6.16.1.4 QoS marking

The Differentiated Services package enables the PD-PE to control the setting of the DSCP value for all packets leaving the PE-PE.

6.16.1.4.1 Copying DSCP/ToS values from the ingress to egress

The copy mechanism is specified in Amendment 1 to ITU-T H.248.52

6.16.1.4.2 Auditing the "Per-Hop Behaviour"

The per-hop behaviour (PHB) concerning "MGC-signalled QoS marking" versus "copying of QoS values" may be explicitly controlled (and audited) using *Differentiated Services package version 2*, see Amendment 1 to H.248.52.

The *Differentiated Services package version 1* does not allow to audit the behaviour, see the note at the end of clause 7.6.1.3 in Amendment 1 to [ITU-T H.248.52].

6.16.1.5 Bandwidth control-reservation, allocation and policing

The PD-PE should support different *resource control modes* in order to handle different types of user equipment (UE), customer premises equipment (CPE) and/or transport QoS capabilities (see clause 6 of [ITU-T Y.2111]).

There are two basic *resource control modes* (see clause 6.1.1 of [ITU-T Y.2111]):

1) Push mode: The PD-PE makes the authorization and resource control decision based on policy rules and autonomously instructs the PE-PE to enforce the policy decision.
2) Pull mode: The PD-PE makes the authorization decision based on policy rules and, *upon the request* of the PE-PE, re-authorizes the resource request and responds with the final policy decision for enforcement.

The support of the "push mode" is typically inherent for ITU-T H.248 controlled resource (e.g., QoS) control mechanisms. The "pull mode" requires the support of the "pull mode package" [ITU-T H.248.55] in order for the PD-PE to determine the correct policy request (see clause 6.16.1.17 for further information). The remainder of this clause deals with how the PD-PE requests policy enforcement.

Resources are reserved independently per gate. For each gate, reservation of local resources for handling incoming and outgoing traffic is achieved by setting the appropriate properties in the Local and Remote Descriptors. Only one session description shall be included in each Stream Descriptor. Hence, the ReserveValue and ReserveGroup properties should not be used.

The function of bandwidth control (which relates to bit- and byte rate control in this profile) is structured in following clauses:

- admission control (AC; clause 6.16.1.5.1);
- traffic descriptor (clause 6.16.1.5.2);
- bandwidth reservation and allocation (clause 6.16.1.5.3); and
- traffic policing (clause 6.16.1.5.4).

6.16.1.5.1 Admission control

Admission control (AC) is defined in [ITU-T Y.2111] for the PE-PE (MG role) level. There is no concept of a call in ITU-T H.248 MGs due to the separation of call and bearers in the ITU-T H.248 model, which means that AC translates in a context admission control (CoAC; see also [b-ITU-T H-Sup.6]) and stream admission control (StAC) on PE-PE side.

The StAC and CoAC are triggered with the first incoming ADD.request command. At that point a decision is taken on whether the new context can be established or not.

The StAC is triggered whenever a modification of an existing ITU-T H.248 context, e.g., in terms of traffic descriptor, is requested. At that point a decision is taken on whether the context modification can be accepted or not.

6.16.1.5.1.1 Admission control in this profile

The PE-PE AC is based on the requested ITU-T H.248 stream level usage parameters and already established Contexts. The stream level usage parameters are given by the ITU-T H.248 Media Descriptor in the ADD.request (and MODIFY.request) commands. The "usage parameters" as input for the AC of this profile are mainly related to "bandwidth" information (see next clause on "traffic descriptor").

Specific AC algorithms could principally follow a deterministically or a statistically based multiplexing model. Concrete algorithms are implementation specific, thus out of scope of this profile.

The *result* of an admission control (here CoAC or StAC) is either an *accept* or a *reject* decision.

NOTE – Step 2 in Figure 4 of [b-ETSI TS 183 018] shows an accept decision, which is implicitly given by the command reply on the ADD.request for the IP termination. A reject decision would be indicated by an appropriate ITU-T H.248.8 error code in the reply.

6.16.1.5.2 Traffic descriptor

A *traffic descriptor* is the set of traffic parameters that is used to capture the traffic characteristics of an IP flow (see clause 3.2.10 of [b-ITU-T Y.1221]). The traffic parameters for an ITU-T H.248 Stream of an ITU-T H.248 IP Termination are direction-independent and given by either:

1) an explicit specification via:

   the "b=" line in the SDP description of the Local Descriptor and Remote Descriptor; or

   the properties of the Traffic Management package, or

2) an implicit specification via:

   the "m=" line in the SDP description of the Local Descriptor and Remote Descriptor (e.g., traffic usage estimate based on SDP media type and further mode of operation information).

NOTE – There is no concept of a *traffic contract* explicitly used in the scope of this Profile version, because specific QoS classes (see [b-ITU-T Y.1541]) are not signalled per termination. Nevertheless, the "QoS marking" information (see clause 6.16.1.4) could be used for QoS class indications, but such concepts are orthogonal to profile specifications, therefore out of scope of this Recommendation.

6.16.1.5.3 Bandwidth reservation and allocation

6.16.1.5.3.1 SDP "b=" line for constant bit-rate traffic

The amount of required bandwidth for sending packets is expressed using the "b=" line of the SDP description contained in the Remote Descriptors.

The amount of required bandwidth for receiving packets is expressed using the "b=" line of SDP description contained in the Local Descriptors or using one of the properties (tman/pdr or tman/sdr) of the traffic management package.

6.16.1.5.3.2 Properties of the Traffic Management package for variable bit-rate traffic

The Traffic Management package (tman version 1) should be used in case of variable bit rate traffic. There are then two semantics for some *tman* properties. *All* properties may be applied for bandwidth *policing*. The two properties *tman/pdr* and *tman/sdr* would be used additionally for bandwidth *reservation* (see note).

NOTE – The property *tman/pol* indicates whether just reservation is applied ('OFF'), or whether both semantics are in use ('ON'). The semantic for 'OFF' is going beyond the property definition in *tman* version 1 package. These *tman* properties may be considered as elements of a *traffic descriptor*, i.e., information elements used for admission control (besides policing).

6.16.1.5.3.3 Resource reservation protocol

When the PD-PE and PE-PE are operating in a pull mode the RSVP protocol for bandwidth reservation may be supported through the use of the RVSP Extension package (rsvp version 1).

6.16.1.5.3.4 Examples for bandwidth reservation

See Annex F of [b-ETSI TR 183 068].

6.16.1.5.4 Bandwidth policing

Policing of incoming traffic can be enabled using the Traffic Management package. Policing on incoming traffic can be set independently for each gate.

The properties of the Traffic Management package shall be set to values that are compatible (see note) with the "b=" line value of the Local Descriptor.

NOTE – The term "compatible" means that the b-line and the traffic management represent identical bandwidth value with respect to the protocol layer they are defined upon:

– Constant bit rate: "b=" line = *tman/pdr* = *tman/sdr*;

– Variable bit rate: "b=" line = *tman/pdr*.

6.16.1.5.4.1 Statistics for bandwidth policing

Policing of incoming traffic is related to policy rules based on the following:

- policy *conditions* on:
  - "IP byte-rate" parameter(s) (peak-rate and/or sustainable-rate); and/or
  - "IP packet size" parameter(s) (see [ITU-T H.248.53]; signalling method not supported by this profile); and
- policy *actions*:
  - *accept* conforming IP packet; or
  - *silently discard* non-conforming IP packet (in case that profile is not supporting the *tmanr* package); or
  - *discard* non-conforming IP packet *and record* event by *tmanr* statistics (see clause 6.16.1.6.3.3).

The policy actions are executed per IP packet.

6.16.1.5.5 Non-specification of tman properties

If no properties of the Traffic Management package are provided, the PE-PE will not perform traffic policing. If only the tman/pol property set to ON is present, traffic policing shall not be done based on the b-line value, i.e., the policing function cannot be activated at this stage.

Summary on bandwidth control actions:

Table 6-101 – Bandwidth control actions in relationship to *tman* version 1 properties

ITU-T H.248 property usage					Semantic
tman/pol	**tman/pdr**	**tman/dvt**	**tman/sdr**	**tman/mbs**	**Bandwidth control actions**
ON	Not sent	Not sent (use default)	Not sent	Not sent (use default)	No traffic management.
OFF or not sent (default=OFF)	Not sent	Sent or not sent (use default)	Not sent	Sent or not sent (use default)	No traffic management.
OFF or not sent (default=OFF)	Sent	Sent or not sent (use default)	Not sent	Sent or not sent (use default)	No traffic management The property tman/pdr may be used for bandwidth reservation and allocation in the receiving direction in accordance to clause 6.16.1.5.3.
OFF or not sent (default=OFF)	Not sent	Sent or not sent (use default)	Sent	Sent or not sent (use default)	No traffic management The property tman/sdr may be used for bandwidth reservation and allocation in the receiving direction in accordance to clause 6.16.1.5.3.
OFF or not sent (default=OFF)	Sent	Sent or not sent (use default)	Sent	Sent or not sent (use default)	No traffic management The property tman/pdr or tman/sdr may be used for bandwidth reservation and allocation in the receiving direction in accordance to clause 6.16.1.5.3.
ON or not sent (default=ON)	Sent	Sent or not sent (use default)	Not sent	Sent or not sent (use default)	Single stage policer (pdr, dvt) The property tman/pdr may be used for bandwidth reservation and allocation in the receiving direction in accordance to clause 6.16.1.5.3.
ON or not sent (default=ON)	Not sent	Sent or not sent (use default)	Sent	Sent or not sent (use default)	Single stage policer (sdr, mbs) The property tman/sdr may be used for bandwidth reservation and allocation in the receiving direction in accordance to clause 6.16.1.5.3.
ON or not sent (default=ON)	Sent	Sent or not sent (use default)	Sent	Sent or not sent (use default)	Dual stage policer ((pdr, dvt); (sdr, mbs)) The property tman/pdr or

Table 6-101 – Bandwidth control actions in relationship to *tman* version 1 properties

ITU-T H.248 property usage					Semantic
tman/pol	**tman/pdr**	**tman/dvt**	**tman/sdr**	**tman/mbs**	**Bandwidth control actions**
					tman/sdr may be used for bandwidth reservation and allocation in the receiving direction in accordance to clause 6.16.1.5.3.

6.16.1.6 Usage metering and statistics reporting

Usage metering is supported by the statistics defined in the network and other packages. Such statistics may be notified to the PD-PE when a stream is removed (and stats explicitly requested by the PD-PE) or a termination is subtracted from a context (e.g., at the end of a session). They provide information about:

1) resource usage, e.g.,:
   - the duration of the time a termination has been in a context;
   - the traffic volume, e.g., number of octets sent and received.
2) grade of service (GoS)/quality of service (QoS), e.g.,:
   - the packet delay variation or packet transfer delay.

The "number of octets" for the case of *nt* package based measurement is calculated as defined in clause E.11.4 of [ITU-T H.248.1] .

The number of discarded packets due to ITU-T H.248.43-based, explicit source filtering may be reported on basis of the gm/dp statistic.

The number of discarded packets due to ITU-T H.248.37-based, implicit source filtering may be reported on basis of the *lstat/dp* statistic.

The number of discarded packets and octets due to ITU-T H.248.53-based, explicit traffic filtering may be reported on basis by the *tmanr* statistics.

6.16.1.6.1 Statistics for media/transport-agnostic IP packets

The available statistics for the IP streams and terminations of a dedicated context are dependent of the IP-to-IP interworking mode (see clause 3.2.6).

6.16.1.6.2 Traffic volume related Statistics

Figure 6-4 provides an overview of different traffic volume related statistics, which might be useful for the various IP-to-IP interworking modes (e.g., media-agnostic, media-aware, transport-protocol agnostic).

6.16.1.6.2.1 General case

The general case relates to media-agnostic IP-to-IP interworking (NOTE – this relates to [b-ETSI ES 283 018], the ITU-T H.248 Ia profile version 1). Traffic volume related statistics are only accessible by the *nt* package.

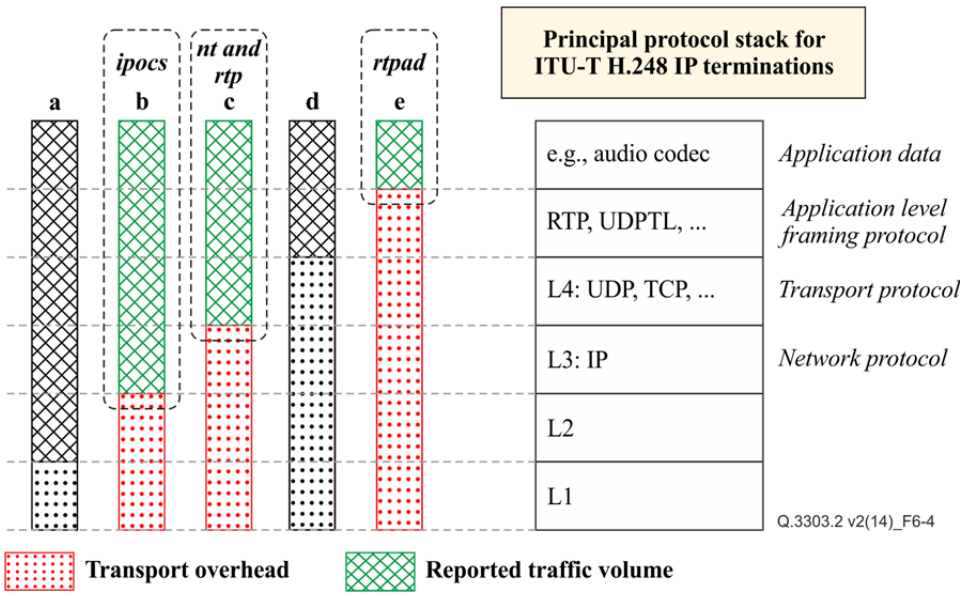


Figure 6-4 – Overview of supported statistics – Traffic volume related statistics on different protocol layers

6.16.1.6.2.2 RTP case (general)

"Media-aware" IP terminations with RTP as application level framing protocol may use traffic volume based statistics via the RTP package:

- packet granularity:

  RTP packets sent and/or received (NOTE – packet level statistics could already provide useful volume measurements in case of RTP packets with constant length).

- octet granularity:

  RTP octets send/received statistics are coupled with nt package statistics, i.e., these statistics also include RTP padding, RTP header information and UDP transport overheads. Such overhead is excluded in the RTP application data specific statistics (see clause 6.16.1.6.2.3).

6.16.1.6.1.2.3 RTP case: Application data

The RTP Application data package provides support for explicit octet count statistics concerning media traffic, i.e., the RTP payload volume.

The IP layer octets count statistics package provides traffic volume statistics on IP layer for IP version 4 or 6. The ITU-T H.248 *ipocs* package (see clause 6.16.1.6.2.1) is *not* supported by this profile version.

6.16.1.6.3 Statistics for packet filtering

6.16.1.6.3.1 Address policing: explicit remote source transport address filtering

Filter conditions based on source transport address information for remote IP endpoints may be enabled with gate management properties (see also clause 6.16.1.1). The number of discarded packets due to remote source filtering may be reported on the basis of the *gm/dp* statistic.

6.16.1.6.3.2 Address policing: implicit remote transport address filtering due to latching

The *lstat/dp* statistic is used for recording the number of discard packets due to implicit filtering of the latching function. See also clauses 1.3 and 6.6.7.2 of [ITU-T H.248.37].

6.16.1.6.3.3 Traffic policing: byte-rate policing

See clause 7.4 of [ITU-T H.248.53].

6.16.1.6.3.4 Traffic policing: packet-size policing

Not supported by this profile specification.

6.16.1.7 RTCP handling

Handling of RTCP is already partially addressed by clause 6.16.1.1. This clause defines further procedures for RTCP.

6.16.1.7.1 RTCP transport address allocation

6.16.1.7.1.1 Local RTCP IP transport address allocation

In line with the recommendations of [b-IETF RFC 3605], non-contiguous RTCP port numbers (identified via the "a=rtcp" media attribute) shall not be used by the PE-PE in its Local Descriptor (LD).

Local ports for RTCP are implicitly allocated by the PE-PE whenever instructed to do so by the PD-PE via the gm/rsb=ON property. The PE-PE must follow the port allocation rules as defined in section 11 of [b-IETF RFC 3550], which results in the allocation of a contiguous port pair for RTP and RTCP within a single stream. .

If the gm/rsb property is set to OFF, then no RTCP port is allocated in conjunction with an RTP stream. This behaviour is irrespective of the presence of the "a=rtcp" attribute in the related RD.

6.16.1.7.1.2 Remote RTCP transport address representation/usage, implicit allocation of IP transport address for RTCP

RTCP ports are allocated either implicitly or explicitly when support of RTCP is required. RTCP support and RTCP transport address and allocation is controlled as by the gm/rsb property and the "a=rtcp" media attribute line in the Remote Descriptor. If RTCP is sent within the same stream as RTP then RTCP port allocation is handled as follows:

- gm/rsb=OFF or gm/rsb omitted.

  RTCP support is not required. No pinhole is opened for received RTCP packets. No RTCP packets are sent and any received RTCP packets are silently discarded. This is irrespective of whether the "a=rtcp" attribute is present in the Remote Descriptor.

- gm/rsb=ON & "a=rtcp" media attribute line not present.

  RTCP support is required. A pinhole is opened for received RTCP packets. The PE-PE must follow the port allocation rules as defined in section 11 of [b-IETF RFC 3550], which results in the allocation of a contiguous port pair for RTP and RTCP within a single stream in the Local Descriptor (see clause 6.16.1.7.1.1). RTCP packets are sent to the same address and contiguous port number to the RTP port as specified in the Remote Descriptor.

- gm/rsb=ON & "a=rtcp" media attribute line present.

  RTCP support is required. A pinhole is opened for received RTCP packets. The RTCP port and optionally address are explicitly identified by the included "a=rtcp" media attribute line. The MG must follow the port allocation rules as defined in section 11 of [b-IETF RFC 3550], which results in the allocation of a contiguous port pair for RTP and RTCP within a single stream in the Local Descriptor (see clause 6.16.1.7.1.1). If the "a=rtcpmap" media attribute line in the Remote Descriptor contains an address it is used as destination when sending RTCP packets. The destination port for RTCP packets is always explicitly identified via the "a=rtcp" media attribute line in the Remote Descriptor.

6.16.1.7.1.3 Unsuccessful transport address allocation

In line with clause 6.16.1.7.1.1, neither a fully specified RTCP port nor RTCP address are ever used by the PD-PE in the Local Descriptor. Therefore, unsuccessful port/address allocation can only occur due to there being insufficient resources on the PE-PE to allocate the (contiguous) RTCP port. Unsuccessful scenarios result in the PE-PE responding with ITU-T H.248 error code #510 ("Insufficient Resources").

6.16.1.7.2 RTP/RTCP to ITU-T H.248 stream mapping

In line with clause 6.16.1.7.1.1, a single common ITU-T H.248 stream is always used for RTP and its associated RTCP flow.

6.16.1.8 RTCP forwarding

Every RTP session may be accompanied by RTCP control flows. Blocking (by the PE-PE) of such RTCP packets may violate the end-to-end RTP/RTCP protocol and/or the served applications. However, security threats or specific RTCP reports types may request for dedicated RTCP packet policing rules.

6.16.1.8.1 Conditions for RTCP packet policing

Conditions for RTCP packet policing are typically based on following n-tuple elements:

- IP *port* for RTCP flow,
- RTCP *packet type* codepoint,
- RTCP synchronization source *(SSRC)* codepoint,
- RTCP source description information element (e.g., canonical name (*CNAME)* codepoint), and/or
- RTCP *block type* codepoint in the case of RTCP extension reports (XR, HR).

6.16.1.8.2 Forwarding of regular RTCP traffic

"Regular" RTCP packets shall be understood in the scope of this Recommendation as packet units with a packet type value equal to a value from the range of {192, 193, 200 to 206}. Thus, regular traffic excludes extended report (XR) and HR RTCP packets. Regular RTCP packets must be basically forwarded towards the RTP endpoint.

Regular RTCP packets are unambiguously identified by the 3-tuple of {packet type, SSRC, CNAME}.

Thus, RTCP packets with e.g., an incorrect {SSRC, CNAME} combination may be blocked.

6.16.1.8.3 Handling of RTCP XR/HR traffic

Extended reports (XRs) and XR-based high resolution reports, – i.e., RTCP reports with a packet type value equal to 207 –, carry measurement data from measurement points (PE-PE) to reporting points (RPs). Such measurement reports do not have necessarily an end-to-end significance; their scope may be e.g., limited to a single IP domain or "RTP network segment". The MG may have to apply dedicated forwarding policy rules for such RTCP packets. Concrete policy rules are for further studies.

6.16.1.9 Media inactivity

Application data inactivity detection (also known as media inactivity detection) may have multiple, different use cases as cited in [12] e.g.,:

- detection of interrupted IP routes,
- detection of released RTP endpoints,
- detection of hanging SIP/RTP sessions (see note), or

- detection of deadlocks in IP latching scenarios.

NOTE – The notation of "SIP/RTP session" relates to a SIP-controlled RTP session, which implies a RTP session on PE-PE level and a SIP session on PD-PE level. There might be a hanging RTP session (leg) or a SIP session (leg). The application of [ITU-T H.248.40] is able to address both failure scenarios.

In all use cases, the *adid v1* package (with possible different *timing* and/or *direction* configurations of the detection logic) is used to report the detected inactivity.

The *adid/ipstop* event is enabled on a per ITU-T H.248 IP termination basis, i.e., not on ITU-T H.248 stream level. The PE-PE monitors all IP transport ports associated with the termination.

6.16.1.10 IP domain/realm indication

6.16.1.10.1 Codepoint and format/encoding

The IP realm identifier (i.e., ITU-T H.248 property *ipdc/realm*) may be sent to the PE-PE in order to indicate the IP domain/realm of the ITU-T H.248 IP termination. The IP realm identifier is a flexible string and may convey a numerical IP address, domain name or mutually understood name (e.g., "in" and "out", "1" and "2", etc.) (see Note). The ephemeral termination string layout ("ip/<group>/<interface>/<id>") is still used in this version of the profile but the "interface" field is always set to CHOOSE by the PD-PE in an Add request command and is assigned by the PE-PE. The PE-PE may use the "interface" field to denote a physical or logical interface on the PE-PE.

NOTE –The usage of the IP realm identifier in this version of the profile is generalized and goes somewhat beyond the original definition (by [ITU-T H.248.41]) of the identifier. This is due to the following reasons:

a) syntax: backward compatibility with Ia profile version 1 (format/encoding syntax by field "Interface" in TerminationID); and

b) semantic: generic "domain identifier" for "domain concepts" beyond IP address spaces. Such "domain concepts" could be related to specific technologies, specific protocol layers, virtual private network types, etc.

6.16.1.10.2 Unsuccessful indication

If the value of the IP realm identifier sent by the PD-PE within the [ITU-T H.248.41] package property cannot be recognized by the PE-PE, the PE-PE will fail to create the IP based ITU-T H.248 termination and replies with an error descriptor using the error code 449 (Unsupported or unknown parameter or property value).

6.16.1.10.3 Fix assignment per termination lifetime

The PD-PE may or may not choose to assign IP realm identifier when communicating with the PE-PE e.g., not sent if IP Realm configured on the PE-PE. If the PD-PE assigns IP Realm, then this must be communicated at termination seizure (Add). The value of IP Realm shall be applied to all streams associated with the termination. The IP Realm identifier indicates the IP domain/realm of the ITU-T H.248 termination and cannot therefore be changed after the initial assignment at Add.

The IP Realm identifier cannot be subsequently changed in a Modify command once assigned to a termination. Only an identical/unchanged setting of IP realm identifier may be sent in a Modify command. If the PD-PE attempts to change the IP realm on an existing termination via a Modify command, the PE-PE will reply with an error descriptor using the error code 501 (Not implemented).

6.16.1.10.4 Number of IP realms/domains

The PE-PE supports typically multiple logical IP interfaces, which may belong to different IP address realms. Following principal use cases may be distinguished:

1) Single realm:

All IP interfaces of the PE-PE, and therefore all created ITU-T H.248 IP terminations, belong to the same IP address space.

2) Multiple realms (N private realms and M public realms with $N + M \geq 2$):

- The two ITU-T H.248 IP terminations of an ITU-T H.248 context may belong to the same IP address space or different realms.
- The PE-PE may be principally connected to many IP address realms. For instance, N private domains or one public and M private domains. Furthermore, there could be overlapping address spaces between multiple private domains (see note). The ITU-T H.248.41 package property is used to indicate each realm.

In general, if [ITU-T H.248.41] property is omitted, according to the ITU-T H.248.41 procedures the configured default IP realm is applied by the PE-PE.

NOTE – Overlapping IP address spaces could be discriminated by separation e.g., via physical (IP) interfaces, via a L3VPN technology (e.g., IP security (IPsec) in tunnel mode), or via a L2VPN technology (e.g., VLANs).

All above use cases are related to specific PE-PE deployment scenarios due to the static nature of a connection of a particular IP domain with the PE-PE.

6.16.1.10.5 IP realm availability

The PE-PE may support IP realm availability (*ipra*) package to facilitate the detection of available IP realms by the PD-PE.

The PD-PE can audit the "Available realms" (*ipra/ar*) property with the AuditValue command to get the information regarding the available realms. If the "Available realms changed" (*ipra/arc*) event is set, whenever the available realms change the information regarding the change is reported by the PE-PE.

6.16.1.11 One-stage and two-stage PE-PE resource reservation

The SDP offer/answer model allows offers and answers to be generated with or without "m=" and "b=" lines.

The normal case is when both information contained in SDP "c=" and "m=" lines is available to the PD-PE and at the time it requests the PE-PE to create a termination, it is referred to as one-stage reservation. This means both "c=" and "m=" line information can be passed to the PE-PE in a single step.

If information contained in SDP "c=" line, but "m=" and "b=" lines are not available to the PD-PE at the time it requests the PE-PE to create a termination, the PD-PE refrains from sending "m=" and "b=" lines to the PE-PE. In order for media plane communication to take place through the PE-PE, the PD-PE must, at a later stage, come back with at least "m=" lines to the PE-PE. This would typical happen at a subsequent offer/answer exchange on the SIP plane. Such a reservation procedure is referred to as two-stage reservation.

These actions at the Rw interface can be described with the following two-stage PE-PE resource reservation procedure:

1. PD-PE requests the PE-PE to reserve an IP address (via the LD) in accordance with the specified IP realm and may also optionally reserve an IP port. In the former case, the SDP in Local and/or Remote Descriptors does not contain "m=" nor "b=" lines. In the latter case, the SDP in Local and/or Remote Descriptors does contain an underspecified "m=" line. The PD-PE does not request the PE-PE to open any pinhole at this stage.
2. PD-PE requests the PE-PE, in addition to the previously assigned IP address, to also allocate port(s) (if not done at stage 1) and optionally bandwidth or to optionally further specify the previously allocated port together with an optional bandwidth. The SDP in

Local and/or Remote Descriptors does contain "m=" and optionally "b=" lines. The PD-PE may request the PE-PE to open pinholes at this stage.

The command level details of one-stage and two-stage reservation procedures are specified in clause 6.17, where one-stage is considered the default scenario and thus only the specifics of two-stage reservation are called out.

Both stages in two-stage reservation are part of the overall session establishment phase.

6.16.1.12 Hanging termination detection

For the correct operation of a PE-PE, synchronization of termination information between the PD-PE and PE-PE is essential for the traffic, maintenance and charging purposes. In some cases, the PD-PE may have lost a record of a termination but the termination is not subtracted on PE-PE. The *hangterm/thb* event defined in [ITU-T H.248.36] may be used to solve this problem. After a period of message inactivity the PE-PE may issue a periodic Notify command on the concerned termination and the PD-PE may use this to check if it has a record of the termination or not. The time period for this Notify may be parameter driven. Optionally the hangterm/thb event may result in an audit of *PD-PEinfo/db* property in order to determine the PD-PE information string.

6.16.1.13 Real time statistics reporting

6.16.1.13.1 Overview of conditional reporting

A PD-PE normally obtains bearer related statistics through periodic auditing of the ITU-T H.248 Statistics Descriptor or at the time of deletion of a stream or subtraction of a termination. However, in both cases, there is an interval of delay between when a reporting condition occurs on a PE-PE (e.g., a statistic threshold being passed) and when the PD-PE learns of the statistic. In many cases, such a delay is of no consequence. However, in some cases, the PD-PE may require to be immediately informed of a given statistical threshold condition occurring. In this case, the PD-PE must use the [ITU-T H.248.47] Statistic Conditional Reporting package. This package may be applied to multiple statistics. The PD-PE should set the reporting thresholds and ranges as appropriate and must specify at least one "condition" for conditional reporting (i.e., the PD-PE must signal at least one condition per requested packageID/statisticID item).

The exact statistics and reporting conditions are determined by the operator’s configuration based on the application/service required.

6.16.1.13.2 Basic conditional reporting

Basic conditional reporting uses the protocol elements of the *Statistic Conditional Reporting* package version 1 (i.e., in the 2007 edition of ITU-T H.248.47 which is has now been superseded by the 2008 edition). This allows the definition of many, but limited reporting conditions.

6.16.1.13.3 Extended conditional reporting

Extended conditional reporting uses the protocol elements of the *Statistic Conditional Reporting* package version 2 [ITU-T H.248.47]. This package allows in addition:

- to control whether a timestamp is reported with the detection of the (conditional reporting) events; and
- extends the reporting conditions with value-based metric conditions.

6.16.1.14 Transcoding

Definition see clause 3.2.8.

6.16.1.14.1 Media types and formats (codecs)

[b-ETSI TS 181 005] defines the codec services for TISPAN NGNs. It provides codec recommendations for *narrowband audio*, *wideband audio* and *video* media.

6.16.1.14.2 Decision for transcoding

The decision for transcoding may be principally reached at the beginning or later during the lifetime of a call/session. The corresponding triggers (for transcoding decisions) from PE-PE side would be either related to ADD or MODIFY request commands.

6.16.1.14.2.1 Decision at stream/termination creation

The first ADD.request (of a new Context) for a new stream/termination provides either a full specification (by the PD-PE) of the media type and format, or an under-specification, which is then completed by the PE-PE.

The subsequent request for the peer stream/termination (within this Context) is then leading to a possible transcoding decision. The PE-PE is comparing the SDP information elements for media description of the two ITU-T H.248 Stream Descriptors:

- In case of identical media type and formats then there will be no transcoding. The PE-PE may even handle this stream in media-agnostic mode.
- In case of different media type or/and formats then the PE-PE may decide for transcoding support, or reject the request with an appropriate ITU-T H.248.8 error code (e.g., due to temporarily lacking resources for transcoding).

6.16.1.14.2.2 Decision at stream/termination modification

MODIFY.request commands for existing streams/terminations may lead to a decision for transcoding.

6.16.1.15 VPN identification

6.16.1.15.1 VLAN marking

The PE-PE VLAN tagging behaviour is summarized in the following table:

Table 6-102 – VLAN marking using *vlan* version 1 package

ITU-T H.248 property usage		**Semantic**
vlan/pri	**vlan/tags**	**Action**
Sent	Value smaller than "4 096" sent	Apply VLAN tagging accordingly
Sent	Not sent (use provisioned default value)	Apply VLAN tagging accordingly
Not sent (use provisioned default value)	Value smaller than "4 096" sent	Apply VLAN tagging accordingly
Not sent	Not sent	Do not apply VLAN tagging
Sent or not sent	Value "4 096" sent	Do not apply VLAN tagging

6.16.1.16 Topology hiding function

Topology hiding may basically be related to the:

a) hiding of "*remote* topology information", i.e., the PE-PE provides *local* support for topology hiding to network elements "*behind*" the PE-PE;

b) hiding of "*local* topology information", i.e., the PE-PE provides *local* support for topology hiding of the PE-PE *itself* in one-way direction for the egress media-path.

Topology hiding functions (THFs) are required on PD-PE (MGC) level for the IP signalling-path and on PE-PE (MG) level for the IP media-path, see [ETSI TS 187 003]

NOTE 1 – THF relates basically to the hiding of (network element) local address information ("network topology hiding"). Address information is primarily related to the L3 addresses, which are used in the IP layer and by IP application protocols (like SIP).

NOTE 2 – PE-PE related THF scenarios are e.g., outlined by clause A.2 of [b-ETSI TS 187 003] . For instance, the so-called topology hiding gateway (THIG) function relates to a THF on interconnection border control function (IBCF) (MGC) level for the IP signalling-path and on I-PE-PE (MG) level for the IP media-path in the IP multimedia subsystem (IMS) interconnect scenario (Figure A.6 of [b-ETSI TS 187 003]).

6.16.1.16.1 THF for the IP signalling path

The assumption by this ITU-T H.248 profile specification (and decomposed gateway architecture) is a media-path decoupled signalling path. Any THF for the IP signalling-path is thus out of scope of this Recommendation.

6.16.1.16.2 THF for the IP media /bearer path

This clause introduces topology hiding functions (THF) for the IP media/bearer path on different protocol layers.

6.16.1.16.2.1 THF on IP network protocol layer (L3)

THF on IP network protocol layer (L3) includes IP address information and other IP protocol control information (PCI) elements and Internet control message protocol (ICMP).

6.16.1.16.2.1.1 THF on IP address information elements

THF in the IP media-path may be basically achieved by NAT within the end-to-end IP connection. *Remote* NAT devices may support the hiding of PE-PE local IP addresses, i.e., LS (A) and LD (A) information (see also Figure 6-2).

PE-PE-local THF support:

- hiding of "*remote* topology information" via PE-PE-local NA(P)T (see clause 6.16.1.2) may used for hiding of remote IP address information (i.e., RS(A) or/and RD(A) information).
- hiding of "*local* topology information" via explicit source address setting capability (via *gm* package properties, see e.g., clause 6.17) with regards to the LS (A) value.

NOTE – Properties *gm/esas* and *gm/lsa* for LS (A) control, and *gm/esps* and *gm/lsp* for LS (P) control.

6.16.1.16.2.1.2 THF on other IP PCI elements and ICMP

THF on L3 is furthermore supported by:

- IP time-to-live (TTL) value reset in B2BIH mode

  NOTE – Not in IPR mode.
- ICMP: there is an ICMP traffic flow for each IP interface, however, the ICMP flow does *not* appear as a flow component within ITU-T H.248 IP streams (because ICMP is an IP layer service, out of control of ITU-T H.248).

6.16.1.16.2.2 THF above the IP layer

IP address information may be carried by media-path protocols above the IP layer.

RTP packets may be forwarded transparently (e.g., in transport-protocol agnostic mode) or terminated like in media-aware PE-PE mode. Termination implies a *Back-to-Back RTP Endsystem* (B2BRE mode) because each ITU-T H.248 IP termination provides an IP host and RTP endsystem function. Thus, RTCP packets are sourced/sinked by the PE-PE in that mode. The source description (SDES) RTCP packet is mandatory, as well as the SDES item 'CNAME' (*Canonical End-Point Identifier*).

[b-IETF RFC 3550] recommends that:

"The CNAME item SHOULD have the format "user@host", or "host" if a user name is not available as on single-user systems. For both formats, "host" is either the **fully qualified domain name** of the host from which the real-time data originates … **or** the standard ASCII representation of the host's **numeric address** on the interface used for the RTP communication."

Such a CNAME format would advertise topology information via RTCP. THF for RTP/RTCP could be achieved e.g., either via secure RTP (SRTP) [b-IETF RFC 3711] or by just encrypting the SDES CNAME item (see section 9.1 of [b-IETF RFC 3550]).

6.16.1.17 Pull Mode QoS resource control

If a PE-PE supports pull mode operation, the PD-PE may utilise this functionality through the use of the "Pull mode package" [ITU-T H.248.55].

In order that the PE-PE may detect and forward resource requests to the PD-FE, the QoS resource reservation event shall be set. When the *plm/rdrr* event is set on the ROOT termination of the PE-PE, the *brav* and *brpv* parameters should be also included in order to specify the signalling address that the resource reservation signalling will be received.

In the case where a PE-PE and PD-PE may serve multiple domains where requests may be received from, in order to indicate the appropriate domain, the PD-PE shall also send the 'Path coupled requests domains under MGC ownership' parameter (i.e., ITU-T H.248 property *plm/rdmo*) within the event. The pull mode QoS resource control is invoked when the PE-PE receives a QoS request over dedicated path-coupled QoS signalling from the CPE to create a media stream. The PE-PE resolves the source identifier of the message and matches it with the *plm/rdmo* information to select the correct PE-PE for the service. The PE-PE then notifies the request via the QoS resource reservation event (i.e., ITU-T H.248 Event *plm/rdrr*) to the PD-PE in order to request the resource decision for the service. On receipt of the authorization token carried in the event, the PD-PE shall send a resource action request to the service control function (SCF) to retrieve the service information associated with the flow. The PD-PE makes the resource decision based on the service information and resource availability and then responds the PE-PE to enforce the policy decision (see clause 6.16.1.5).

In order to support a CPE-requested QoS resource modification procedure the QoS resource modification event (i.e., ITU-T H.248 Event *plm/rdrm*) is set by the PD-PE. As in the request case above upon reception of a QoS resource modification from the CPE, the PE-PE resolves the source and if it matches sends the notification to the PD-PE via the *plm/rdrm* event.

In order to support a CPE-requested QoS resource release procedure QoS resource release event (i.e., ITU-T H.248 Event *plm/rdrl*) is set by the PD-PE. As in the request case above upon reception of a QoS resource release from the CPE, the PE-PE resolves the source and if it matches the PE-PE sends the notification to the PD-PE via the *plm/rdrl* event.

6.16.1.18 RSVP handling

When the CPE uses RSVP to initiate the QoS resource reservation for the service flow, the PE-PE and the PD-PE are required to support the RSVP extension package for RSVP message handling. The PE-PE acts in different roles as sender and receiver for the corresponding two unidirectional data flows in the same session.

The procedures specified in clause 6.6.2 of [ITU-T H.248.65] are applied when the PE-PE and the PD-PE are involved in the pull mode QoS resource control scenario using RSVP protocol.

6.16.2 Overview of call independent procedures

"Call independent" procedures are also known as "session independent" or "non-call related" procedures.

6.16.2.1 Introduction – Relation to ETSI TR 183 025

Session-independent procedures for [b-ETSI ES 283 018] are defined in [b-ETSI TR 183 025], which is an overall description for all ETSI defined ITU-T H.248 profile specifications, i.e., [b-ETSI TR 183 025] complements each profile specification.

The set of profile-applicable call-independent procedures is primarily given by the supported ITU-T H.248 command API capabilities for AuditValue (see clause 6.7.5), AuditCapabilities (see clause 6.7.6) and ServiceChange (see clause 6.7.8), and supported packages (e.g., for overload control), by each profile.

6.16.2.2 Session-independent procedures

Session-independent procedures are described in clauses 6.18 and 6.19.

6.16.2.3 PE-PE (MG) overload control

[ITU-T H.248.11] may be used for controlling MG overload, by throttling and limiting the rate of ITU-T H.248 messages from MGC to MG.

See clause 5.19.14 of [b-ETSI TS 183 018] for the procedure and for the command level details.

6.16.2.4 Failure handling procedures: interface failure

Background:

As an example clause 10.1.1.2.1 of [ITU-T Y.2111]: "*During the running of a media flow, if the PE-FE cannot provide the reserved QoS resource any longer for the media flow due to its* ***interface failure****, the PE-FE shall send a Resource Notification to the PD-FE on its own initiative.*"

Interface failures (e.g., failures of logical or physical IP interfaces, or physical Ethernet interfaces) could be generally addressed by ServiceChange procedures, for instance, ServiceChange with Method 'Forced', Reason '904', '905', or '907' (dependent on failure type) and on ephemeral terminations (see clause F.4.1.3 of [ITU-T H.248.1]). Clause 5.19 for MG failure, MG Termination failure and user plan failure of [ETSI TS 183 018] shall be applied.

NOTE – Specific failure types could be addressed by dedicated ITU-T H.248 protocol elements, like for instance clause E.11.2 of [ITU-T H.248.1], [b-ITU-T H.248.13], [ITU-T H.248.36] or [ITU-T H.248.40]. This is for further study.

6.17 Session dependent procedures (command level details)

Clause 5.18 of [ETSI TS 183 018] shall be applied.

6.18 Non-session related use cases

Clause 5.19 of [ETSI TS 183 018] shall be applied.

6.19 Session independent procedures (command level details)

Clause 5.20 of [ETSI TS 183 018] shall be applied.

7 Security considerations

There might be several possible security threats at the Rw interface, such as denial of service, message disclosure by unauthorized snooping, unauthorized message creation and modification.

In general, an attacker can surreptitiously intercept information, attempt to create unauthorized information, send modified or reordered information or all of the above. There might be a risk that an attacker can impersonate a MGC or a MG illicitly acquire (or both) and tamper the information. Even though the information is encrypted, reply attack might be possible. For these security threats, operators need to aware that sufficient authentication and encryption mechanisms are needed

between MGC and MG as described in [ITU-T H.248.1]. To minimize the risk, the MG is needed to be properly configured so that only authorized MGC can access and exchange information each other, and particular attention on the credence and information integrity is necessary.

In the case where ITU-T H.248 messages are open to an insecure domain, there is a risk that an attacker can impersonate, illicitly acquire and tamper information and execute replay attacks. To ensure the security of ITU-T H.248 messages, it is recommended to consider using IPSec or the interim authentication header (AH) scheme described in clause 10 of [ITU-T H.248.1].

If IPSec is used, IPSec authentication header (AH) provides data origin authentication, connectionless integrity and optional anti-replay protection of messages passed between the PD-PE and the PE-PE. Optionally, the IPSec encapsulation security payload (ESP) can be used to provide confidentiality of messages.

If IPSec is not provided in transport, the interim AH scheme can be used to provide similar functions as those of IPSec AH. The interim AH scheme extends the ITU-T H.248.1 protocol header by adding an AH header. Note that the interim AH scheme cannot provide protection against eavesdropping and reply attacks.

This version of the Rw ITU-T H.248 profile does not specify any security support, see clause 6.12.

Appendix I

Overview of specific policing functions in the policy enforcement physical entity

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

PE-PE is responsible for both session-dependent and session-independent policing. Session-independent policing through the Rw interface is out of scope of this Recommendation, although the categorization described in clause I.1 could apply to session-independent as well as session-dependent policing.

Rw ITU-T H.248 profile version 2 only supports session-dependent policing.

I.1 Categorization attempt

The PE-PE provides specific policy types, which could be categorized into following policing areas:

1. Address policing

Policy conditions are based on L3/L4 protocol control information (PCI) elements.

2. Traffic policing

Policy conditions are based on 'traffic descriptors', e.g., like sizes of protocol data units or/and correspondent data rates.

3. Media flow policing

Policy conditions are based on application level framing protocol (e.g., RTP) control information elements, e.g., RTP sequence numbers, timestamps, SSRCs, CNAME in case of RTP. The "general condition" is a "syntactically and semantically" correct PCI block.

4. Media type policing

Policy conditions are based on protocol control information elements for the indication of specific "media types" (e.g., RTP payload type codepoint, RTCP packet type codepoint, etc.) and/or "media areas" (e.g., RTP/AVP).

NOTE – The differentiation between "media flow" and "media type" policing is debatable. The motivation here was driven by ITU-T H.248, which provides dedicated capabilities for each policing type.

All supported policing functions at Rw interface by Rw ITU-T H.248 profile version 1 are related to "packet filters", i.e., policing is acting at packet level and not on octet or even bit level. This might be a relevant aspect when considering statistics for the recording of "negative" policing actions (e.g., packet discard action).

The following policing areas are for further study but mentioned for completeness:

5. Authorization policing

See [ITU-T H.248.65] regarding the use of authorisation and RSVP when used in a pull mode.

6. Transport security policing

Policy conditions are based on transport related encryption information elements (e.g., transport level security (TLS), IPSec).

7. Media security policing

Policy conditions are based on application data related encryption information elements (e.g., SRTP).

8. Others

There might be further policing types, e.g., due to the monitoring/processing of in-band signalling.

I.2 Support by Rw ITU-T H.248 profile version 2

Table I.1 provides a summary with scope on Rw ITU-T H.248 profile version 2.

Table I.1 – Overview of policer types in the policy enforcement physical entity

Policy category	Examples	Support by Rw ITU-T H.248 profile version 2
Address policing	• *Source* filtering • *Destination* filtering	Yes, with gm/1 package. No.
Traffic policing	• Traffic *descriptor* based policing (Note 1) • Traffic *contract* based policing (Note 1)	Yes, with tman/1 package (Note 2). No.
Media flow policing	• Validity checks of RTP packed headers	Yes, e.g., in case of RTP-transported media inherently due to RTP protocol termination (in case of an "RTP endsystem" as ITU-T H.248 IP termination).
Media type policing	• Check of valid media formats	No.
NOTE 1 – The concept of traffic "descriptor" and "contract" is defined in ITU-T Recommendations with particular scope on technology-dependent traffic policing (e.g., Y.1221 for IP, I.371 for ATM or I.378 for AAL2). NOTE 2 – Traffic descriptor elements related to packet size (e.g., average packet size, maximum packet size) may be not signalled with Rw ITU-T H.248 profile version 2, but could be partially supported on provisioning basis.		

Appendix II

Overview of statistics in the policy enforcement physical entity

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

II.1 Introduction

Figure II.1 recalls again the gate concept (see Annex A of [b-ETSI ES 283 018]) and the relation to a general IP-to-IP interworking model. The general model is based on a bidirectional IP connection, comprised by two unidirectional IP flows. The PE-PE/MG provides generally a pipeline with four or five stages per direction in the user plane. Every pipeline stage could be optional in real instances and Rw deployments. Dedicated ITU-T H.248 packages (inclusive of their statistics) are used for specific stages of the "processing pipeline". Statistics may be used at ITU-T H.248 stream- or termination-level.

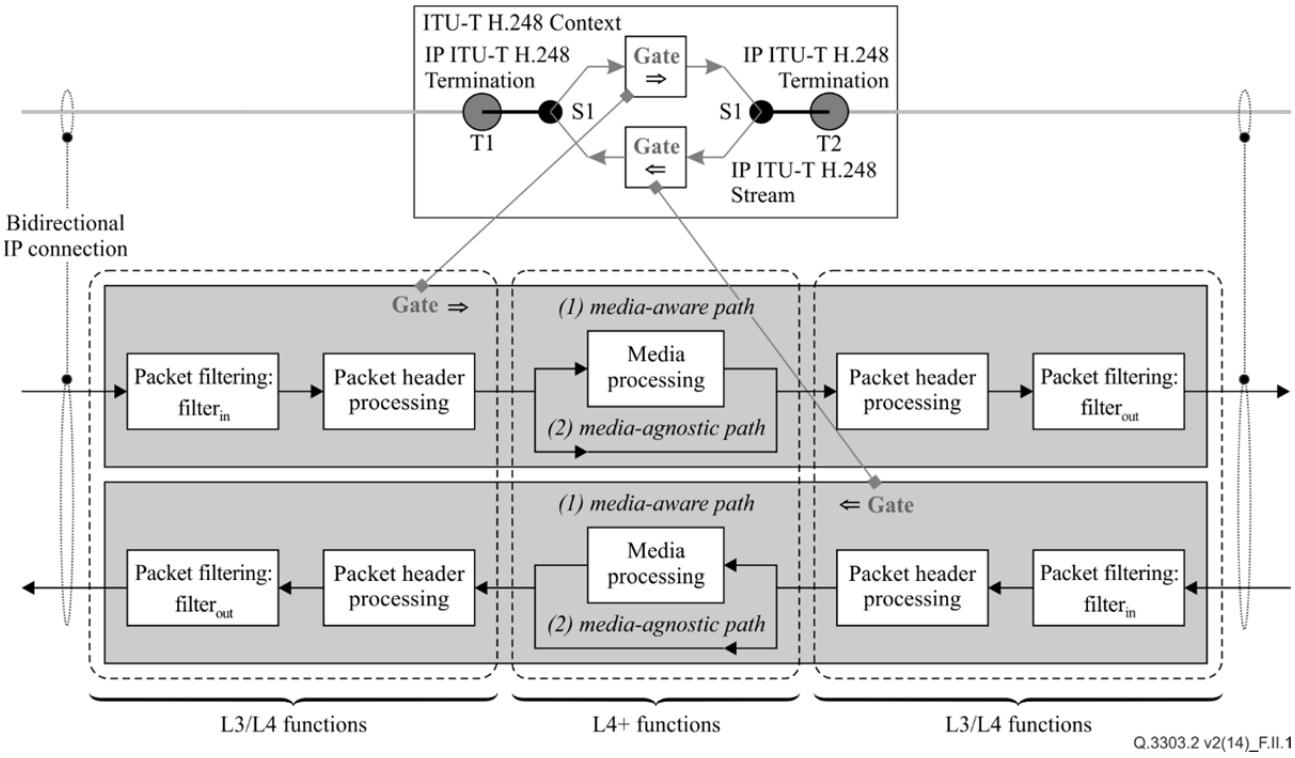


Figure II.1 – PE-PE – general IP-to-IP interworking model (Example with a single ITU-T H.248 stream per termination)

Clause II.2 is summarizing PE-PE relevant statistics. Clause II.3 provides a statistics mapping on the PE-PE model.

II.2 Overview of ITU-T H.248 statistics

Statistics are required to be supported at the Rw reference point. They could be categorized into the following main areas:

1. Usage metering (relates typically to the traffic volume on application level)
2. Reporting of QoS related metrics
3. Recording of "negative" policing actions (see Table II.1)
4. Validation of network capacity allocations (relates typically to the traffic volume on the lowest layer of transport capacity reservation, e.g., could be Layer 2, 3 or other; dependent on the specific LD/RD information)

It has to be recalled again that the above list items are only the call or session dependent statistics, intended to be signalled between PE-PE and PD-PE. There are, in addition, typically further statistics supported by PE-PEs like the ones related to performance management with a served user located in the management plane (e.g., counters defined by simple network management protocol (SNMP) management information bases (MIBs)).

Table II.1 – Overview of statistics in the policy enforcement physical entity

Statistics category	Examples	Support by Rw ITU-T H.248 Profile version 2
1. Usage metering	Metering of application data e.g., for • service level agreement (SLA) verification or • charging.	Usage metering implies a "media-aware" mode of interworking in order to obtain direct statistics (see clause in 6.16.1.6 on RTP application data related statistics). Indirect measurements are supported in V1, e.g., by *nt/os*, *nt/or*, *rtp/ps* or *rtp/pr* statistics.
2. Reporting of QoS related metrics	Media-agnostic QoS metrics like • packet loss rate, • packet delay variation or • round trip delays.	Supported in V1.
	Media-aware QoS metrics like • RFC 3611 VoIP metrics.	Out of scope of V1. Such statistics would relate to dedicated metrics as defined for RTCP XR and/or HR. See also [b-ITU-T H.248.30] and [ITU-T H.248.48].
3. Recording of "negative" policing actions	The element of policy enforcement is a "packet", which is either accepted and forwarded (a) unmodified or (b) modified (e.g., tagged), or (c) rejected and discarded. The number of discarded packets may be recorded in statistics. The specific statistic may depend on the specific policing type.	V1 supports statistics for "address policing" (see statistic *gm/dp*) and partially for "media flow policing" (as part of *rtp/pl*). Statistics related to "traffic policing" or "media type policing" could be subject of a later profile version. Statistics in egress direction are not supported (NOTE – could be a subject of next gm package version).
4. Validation of network capacity allocations	Transport capacity could be e.g., requested explicitly via SDP "b=" lines or implicitly via SDP "m="/"a=" field elements (e.g., codec type and codec mode of operation; disabled silence suppression). The finally used network capacity could be recorded in statistics. NOTE – "Traffic policing" parameters are also related to network capacity parameters. These statistics could be then complementary information, indicating the difference between reserved and used capacity.	V1 provides some initial support by the nt traffic volume statistics (NOTE – recorded volume does correspond to IP packet payloads only in case of IP terminations). Statistics related to the IP packet level for IP terminations, or other statistics for other transport technologies could be subject of a later profile version.

II.3 Mapping statistics on the IP-to-IP interworking model

Figure II.2 shows how the various statistics types could be mapped into the IP-to-IP interworking model. The majority of statistics is in the ingress path.

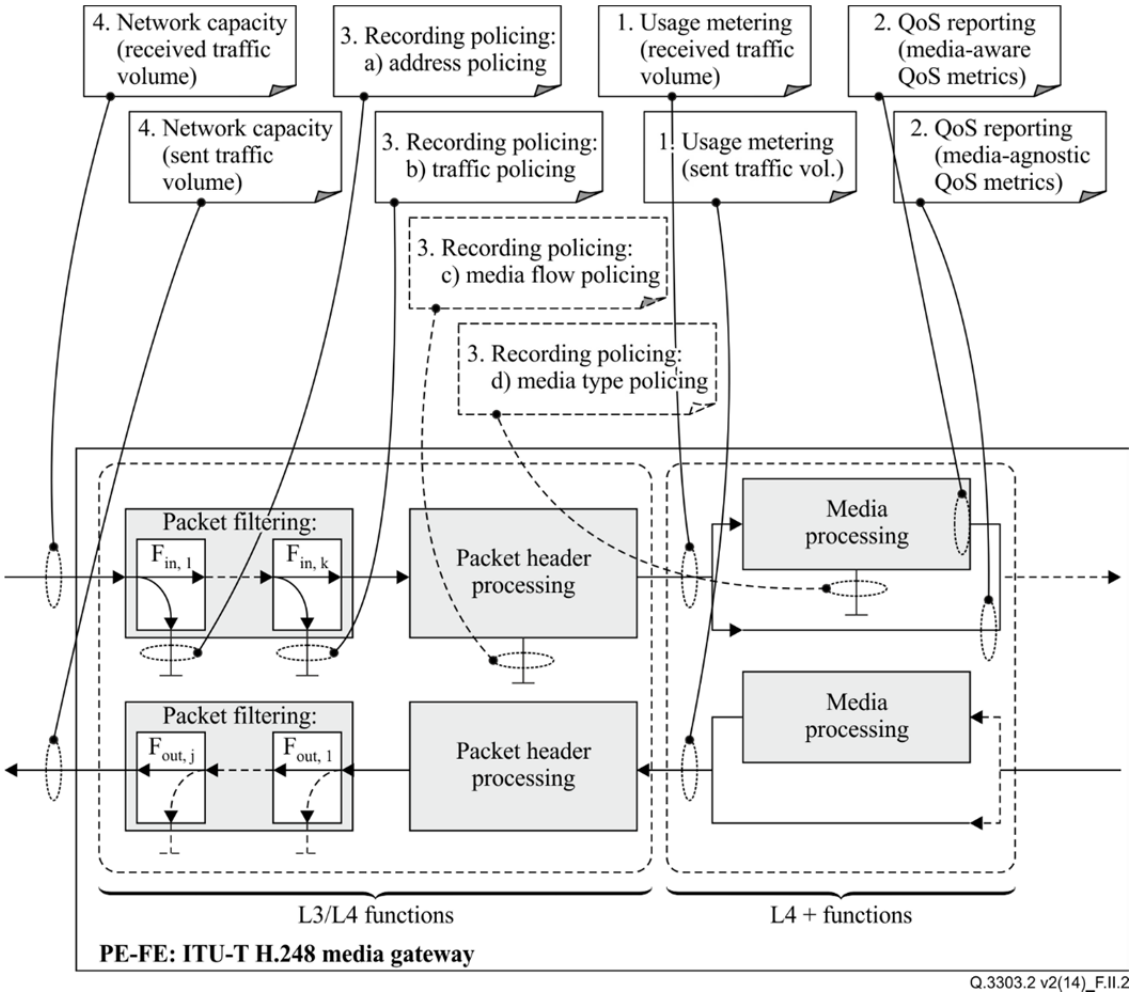


Figure II.2 – Schematic mapping of ITU-T H.248 statistics on the IP-to-IP interworking model

NOTE – The policing related statistics are distributed over the (ingress and egress) IP forwarding paths, dependent on the policer type.

Appendix III

Differences between [ETSI ES 283 018] and this Recommendation

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

Table III.1 provides an overview of the differences between [b-ETSI ES 283 018] and this Recommendation.

Table III.1 – Difference between [b-ETSI ES 283 018] and this Recommendation

Topic	[b-ETSI ES 283 018]	Recommendation ITU-T Q.3303.2
Required ITU-T H.248 gateway control protocol version	ITU-T H.248 Version 3	ITU-T H.248 Version 3 ITU-T H.248.1 Version 2 may be chosen as the minimum protocol version if no capabilities specific to Version 3 are used.
Connection model	Maximum number of terminations per context: up to 2	Maximum number of terminations per context: at least 2
Termination ID structure	ip/<group>/<interface>/<id> Group Values : 0-255	ip/<group>/<interface>/<id> Group Values : 0-65535
TerminationState Descriptor	ServiceState property used: No	ServiceState property used: No NOTE – The value of the ServiceState property may be implicitly changed by ServiceChange procedures, or the value may be read by audit procedures, i.e., "Yes" for ServiceStates "InService" and "OutOfService" due to AuditValue and ServiceChange commands or "No" for ServiceState "Test".
Stream Descriptor	Termination type: IP Maximum number: 5	Termination type: IP Maximum number: 5 (Note) NOTE – Five ITU-T H.248 streams are sufficient to handle various combinations of flows associated with media including possible separation of RTP from RCTP and possible control streams.
LocalControl Descriptor	ReserveGroup used: No ReserveValue used: No	ReserveGroup used: Yes ReserveValue used: Yes NOTE – This profile is "media aware", i.e., ReserveGroup and/or ReserveValue may be principally applied for ALL termination and stream types.

Table III.1 – Difference between [b-ETSI ES 283 018] and this Recommendation

Topic	[b-ETSI ES 283 018]	Recommendation ITU-T Q.3303.2
Events Descriptor	–	Event ID: rtp/pltrans Termination type: All except ROOT Stream type: Any Event ID: it/ito Termination type: Only ROOT Stream type: not applicable Event ID: ocp/mg_overload Termination type: Only ROOT Stream Type: not applicable
Topology Descriptor	Allowed triples: NA	Allowed triples: Not applicable (Note) NOTE – Optional in the case of more than two terminations (see also clause 6.3).
Command API	Notify command used on termination type ROOT: No	Notify command used on termination type ROOT: Yes
	Subtract command wildcard support O-: No	Subtract command wildcard support O-: Yes
Add	Descriptors used by Add request: Media (Stream(LocalControl, Local, Remote)), Event, Signals	Descriptors used by Add request: Media(TerminationState, (Stream(LocalControl, Local, Remote))), Statistics (Note), Event, Signals
	Descriptors used by Add reply: Media (Stream(Local))	Descriptors used by Add reply: Media (TerminationState, (Stream(Local, Remote)))
Modify	Descriptors used by Modify request: Media (Stream (LocalControl, Local, Remote)), Audit(Media (Stream (Statistics)), Statistics, Signals, Event	Descriptors used by Modify request: Media (TerminationState, (Stream (LocalControl, Local, Remote))), Audit(Media (Stream (Statistics))), Statistics, Signals, Event
	Descriptors used by Modify reply: Media(Stream(Local)), Statistics	Descriptors used by Modify reply: Media(Stream(Local, Remote)), Statistics

Table III.1 – Difference between [b-ETSI ES 283 018] and this Recommendation

Topic	[b-ETSI ES 283 018]	Recommendation ITU-T Q.3303.2
ServiceChange	MGC: –	MGC: Handoff (909)
	MG: Forced(904, 905, 906, 915) Graceful, Failover, Handoff: None	MG: Forced (904, 905, 906, 908, 915) Graceful (905) Failover (908 909, 919, 920) Handoff (903)
	ServiceChangeAddress used: No	ServiceChangeAddress used: Yes
	ServiceChangeDelay used: No	ServiceChangeDelay used: Yes
	ServiceChangeVersion: 3	ServiceChangeVersion: 3 or 2 (Note) NOTE – Version 2 is also supported, see clause 6.2.
	ServiceChangeProfile ServiceChangeProfile parameter mandatory: None	ServiceChangeProfile ServiceChangeProfile parameter mandatory: Yes, with ProfileID according to clause 6.1.
Transport	Supported transports: SCTP (Recommended) UDP (Optional)	Supported transports: Either SCTP or UDP must be supported
Transactions	Maximum number of commands per transaction request: 2	Maximum number of commands per transaction request: Not specified
	Maximum number of commands per transaction reply: 2	Maximum number of commands per transaction reply: Not specified
	Commands able to be marked "Optional": AuditValue	Commands able to be marked "Optional": AuditValue, AuditCapabilities, Subtract
SDP Usage ("o=", "s=", "t=" lines)	–	Optional support
Usage metering and statistics reporting	RTP statistics is out of scope of this version 1 of the Profile.	The "number of octets" excludes all transport overhead (see clause E.11.4 of [ITU-T H.248.1]), i.e., IP header is excluded in case of an IP-based ITU-T H.248 Termination (see clause E.11.5.1.5 of [ITU-T H.248.1]). RTP statistics are in scope of version 1 of the Profile. More detail on statistics described in clause 6.16.1.6.1
IP domain/realm indication	Supported, but [ETSI ES 283 018] does not provide any explicit description for that function.	Described in clause 6.16.1.10

Table III.1 – Difference between [b-ETSI ES 283 018] and this Recommendation

Topic	[b-ETSI ES 283 018]	Recommendation ITU-T Q.3303.2
Call independent procedures	Call-independent procedures for [ETSI ES 283 018] are defined in a separate document [ETSI TR 183 025], which is an overall description for all ETSI defined ITU-T H.248 profile specifications, i.e., [b-ETSI TR 183 025] complements each profile specification. The set of profile-applicable call-independent procedures is primarily given by the supported ITU-T H.248 command API capabilities for AuditValue (see clause 6.7.5), AuditCapabilities (see clause 6.7.6) and ServiceChange (see clause 6.7.8), and supported packages (e.g., for overload control), by each profile.	As [ETSI ES 283 018]. Further details are described in clause 6.16.2
Overview of specific policing functions in the policy enforcement physical entity	–	Described in Appendix I
Overview of statistics in the policy enforcement physical entity	–	Described in Appendix II
Packages		
Network (nt/1)	Supported ObservedEvent Parameters: None Statistics: Duration: Optional	Supported ObservedEvent Parameters: Cause (Optional) Statics: Duration: Mandatory
VLAN (vlan/1)	Optional Properties: All: Optional	Optional Properties: All: Mandatory
Segmentation (seg/1)	Optional Properties: MGSegmentationTimerValue, MGCSegmentationTimerValue, MGMaxPDUSize, MGCMaxPDUSize Used in command: NOTIFY	Optional Properties: MGSegmentationTimerValue, MGCSegmentationTimerValue, MGMaxPDUSize, MGCMaxPDUSize Used in command: MODIFY, AUDITVALUE
RTP (rtp/1)	Not supported	Optional
Media gateway overload control (ocp/1)	Not supported	Optional
IP domain connection (ipdc/1)	Not supported	Optional

Bibliography

[b-ITU-T H.248.13] Recommendation ITU-T H.248.13 (2002), *Gateway control protocol: Quality Alert Ceasing package.*

[b-ITU-T H.248.30] Recommendation ITU-T H.248.30 (2007), *Gateway control protocol: RTCP extended performance metrics packages.*

[b-ITU-T H-Sup.6] ITU-T H-series Recommendations – Supplement 6 (2006), *Control load quantum for decomposed gateways.*

[b-ITU-T V.152] Recommendation ITU-T V.152 (2010), *Procedures for supporting voice-band data over IP networks*.

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

[b-ITU-T Y.1541] Recommendation ITU-T Y.1541 (2011), *Network performance objectives for IP-based services*.

[b-ETSI TR 183 025] ETSI TR 183 025 V2.2.0 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); H.248 Non-Call Related Procedures and Management System Interaction.*

[b-ETSI TR 183 068] ETSI TR 183 068 V3.1.1 (2009), *Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); Guidelines on using Ia H.248 profile for control of Border Gateway Functions (BGF); Border Gateway Guidelines.*

[b-ETSI TS 181 005] ETSI TS 181 005 V3.3.1 (2009), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements.*

[b-ETSI TS 183 018] ETSI TS 183 018 V3.5.1 (2009),*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile Version 3 for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification*.

[b-ETSI TS 187 003] ETSI TS 187 003 V3.4.1 (2011), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);NGN Security; Security Architecture.*

[b-ETSI ES 283 018] ETSI ES 283 018 V1.1.4 (2007), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification*.

[b-IETF RFC 2327] IETF RFC 2327 (1998), *SDP: Session Description Protocol.*

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.

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

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

[b-IETF RFC 3611] IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR)*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

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