International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3303.2

(08/2007)

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): H.248 alternative

ITU-T Recommendation Q.3303.2

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 NGN networks	Q.3900–Q.3999

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

ITU-T Recommendation 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): H.248 alternative

Summary

ITU-T Recommendation Q.3303.2 specifies the resource control protocol No. 3 (rcp3) 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 NAPT Control and NAT Traversal at PE-PEs as needed. It satisfies the requirements for information flows across the Rw reference point as specified in clause 8.2 of ITU-T Recommendation Y.2111. It is also used to control the PE-PE in transport devices, including QoS resource control (e.g., packet marking, filtering and policing) and gate control.

Source

ITU-T Recommendation Q.3303.2 was approved on 6 August 2007 by ITU-T Study Group 11 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

CONTENTS

ITU-T Recommendation 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): H.248 alternative

1 Scope

This Recommendation provides the stage 3 technical specifications for the 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] ITU-T Recommendation H.248.1 (2005), *Gateway control protocol: Version 3*, plus Amendment 1.

[ITU-T H.248.4] ITU-T Recommendation H.248.4 (2000), *Gateway control protocol: Transport over Stream Control Transmission Protocol (SCTP)*, plus Corrigendum 1 (2004).

[ITU-T H.248.11] ITU-T Recommendation H.248.11 (2002), *Gateway control protocol: Media gateway overload control package*.

[ITU-T H.248.14] ITU-T Recommendation H.248.14 (2002), *Gateway control protocol: Inactivity timer package*.

[ITU-T H.248.37] ITU-T Recommendation H.248.37 (2005), *Gateway control protocol: IP NAPT traversal package*.

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

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

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[ITU-T Y.2111] ITU-T Recommendation Y.2111 (2006), *Resource and admission control functions in Next Generation Networks.*

[ETSI TS 102 333] ETSI TS 102 333 V1.2.0 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Gate control protocol*.

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

[IETF RFC 4234] IETF RFC 4234 (2005), *Augmented BNF for Syntax Specifications: ABNF*.

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

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 are in conformance to the same set of policy decisions.

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

3.2.4 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].

3.2.5 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].

3.2.6 IP-to-IP interworking modes: The available 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 the 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 conclude for 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>) are unambiguously defining the entire protocol stack of the H.248 IP termination, i.e., the PE-PE (MG) knows 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).
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 H.248. The PE-PE (MG) is still transport protocol-agnostic from a H.248 point of view.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
DiffServ	Differentiated Services
HW	Hardware
ID	Identifier
IP	Internet Protocol
IPSec	IP security
LCD	LocalControl Descriptor
LD	Local Descriptor
LSP	Label Switched Path
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
MPLS	Multiple Protocol Label Switching
NA	Not Applicable
NAPT	Network Address and Port Translation
NAT	Network Address Translation
PD-PE	Policy Decision Physical Entity
PDU	Protocol Data Unit
PE-PE	Policy Enforcement Physical Entity
QoS	Quality of Service
RD	Remote Descriptor
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SRTP	Secure RTP
TLS	Transport Level Security
UDP	User Datagram Protocol
VLAN	Virtual LAN
VPN	Virtual Private Network

5 Conventions

Figures and tables are numbered relative to the clause number.

6 Rw interface Protocol specification (H.248 profile description)

The protocol specification relates to the definition of an H.248 profile applicable for use at an H.248-based Rw interface. The profile concept is inherently part of H.248 (see clause 13 of [ITU-T H.248.1]). This profile is based on [b-ETSI ES 283 018] 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 H.248 Profile.

NOTE 1 – This function relates to the service policy decision function (SPDF) in [b-ETSI ES 283 018].

The PE-PE has the "H.248 MG" role in the scope of this H.248 Profile.

NOTE 2 – This function relates to the border gateway function (BGF) in [b-ETSI ES 283 018].

6.1 Profile identification

Table 6.1 – Profile identification

Profile name:	**ITU_PE-PE**
Version:	1

This ITU-T H.248 Profile is based on Profile "ETSI_BGF/1" as defined in [b-ETSI ES 283 018].

6.2 Gateway control protocol version

[ITU-T H.248.1] Version 3 should apply for the Rw interface.

H.248.1 version 2 may be chosen as the minimum protocol version if capabilities specific to version 3 are not to be used. In that case, the ServiceChange based procedures for registration and re-registration will stop at the version 2 level.

NOTE 1 – Version 3 specific capabilities, which could be of particular interest in applications using this profile, include:

– statistics about the stream level;

– message segmentation package (in the case of H.248-over-UDP/IP; see clause 6.11); and

– IEPS context property.

NOTE 2 – Warning: H.248 messages may exceed the maximum UDP payload size in the case of H.248.1 v2 with UDP-based transport (see also clause 6.11). Such cases will produce the error code "#533 Response exceeds maximum transport PDU size".

6.3 Connection model

Table 6.3 – 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 6.4 – 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 H.248 and shall be based on four fields:

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

The individual fields are described and defined in following table.

Table 6.5.1.1.1 – 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 (0-65535)	No	Yes
Interface	Logical or physical interface to a network to/from which the termination will be sending/receiving media. 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.	String of max 51 alphanumeric characters	No	Yes
Id	Termination specific identifier NOTE – The combination of Interface and Id is unique.	Non-zero 32-bit integer	Yes	Yes

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.

H.248 wildcarding may be applied on IP Termination Identifiers. Wildcarding is limited according to the two columns on the right-hand side.

There are two potential relationships between <group> and <interface> within the TerminationID structure:

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 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 allocate an adequate number of terminations within a <group>. Therefore Audits could be paced for example: `ip/1/*, ip/2/*, .., ip/n/*`.

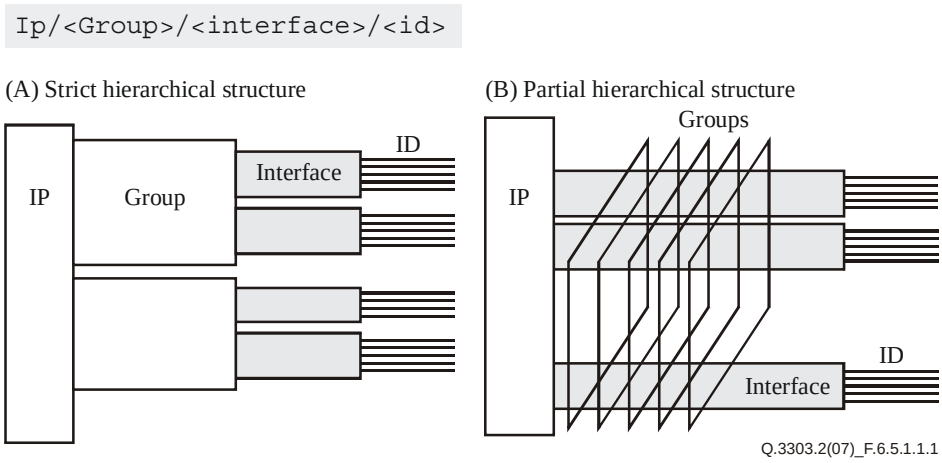

Figure 6.5.1.1.1 – Group/interface relationships for the structure of TerminationIDs

6.5.1.1.2 Syntactical specification

6.5.1.1.2.1 ABNF grammar for H.248 text encoding mode

ABNF [IETF RFC 4234] 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 6.5.2 – Multiplexed terminations

MultiplexTerminations Supported?	No

6.6 Descriptors

6.6.1 TerminationState descriptor

Table 6.6.1/1 – ServiceState property

ServiceState property used:	No

NOTE 1 – All 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 6.6.1/2 – EventBufferControl property

EventBufferControl property used:	No

6.6.2 Stream descriptor

Table 6.6.2/1 – Stream descriptor

Maximum number of streams per termination type	IP	5 (Note)
NOTE – Five H.248 streams are sufficient to handle various combinations of flows associated with media including possible separation of RTP from RTCP and possible control streams.		

Table 6.6.2/2 – Stream configuration

Stream configuration:	ALL configurations are allowed

6.6.2.1 LocalControl Descriptor (LCD)

Table 6.6.2.1/1 – LocalControl Descriptor

		Termination type	**Stream type**
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 6.6.2.1/2 – Termination type

Termination type	**Stream type**	**Allowed StreamMode values**
IP	ALL	SendOnly, RecvOnly, SendRecv, Inactive

6.6.3 Events descriptor

Table 6.6.3/1 – Events descriptor

Events settable on termination types and stream types:	Yes		
	Event ID	**Termination type**	**Stream type**
	See 6.13.2.1 g/cause	ALL except ROOT	ANY
	See 6.13.2.3 nt/netfail nt/qualert	ALL except ROOT	ANY
	See 6.13.2.13 rtp/pltrans	ALL except ROOT	ANY
	See 6.13.2.11 it/ito	only ROOT	not applicable
	See 6.13.2.14 ocp/mg_overload	only ROOT	not applicable

Table 6.6.3/2 – EventBuffer control

EventBuffer control used:	No

Table 6.6.3/3 – KeepActive

KeepActive used on events:	No

Table 6.6.3/4 – Embedded events and signals

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

Table 6.6.3/5 – Regulated embedded events

Regulated embedded events are triggered on:	None

Table 6.6.3/6 – ResetEventsDescriptor

ResetEventsDescriptor used with events:	None

Table 6.6.3/7 – NotifyImmediate, NotifyRegulated and NeverNotify

NotifyImmediate:	ALL Events
NotifyRegulated:	None
NeverNotify:	None

6.6.4 EventBuffer descriptor

Table 6.6.4 – EventBuffer descriptor

EventBuffer descriptor used:	No

6.6.5 Signals descriptor

Table 6.6.5/1 – Signals descriptor

Signals settable dependant on termination or streams types:	Yes		
	Signal ID	**Termination type**	**Stream type/ID**
	ipnapt/*	ALL except ROOT	ANY

Table 6.6.5/2 – Signals lists

Signals lists supported:	No

Table 6.6.5/3 – Signals type and duration

Signal type and duration supported:	No

Table 6.6.5/4 – Signals direction

Signal direction supported:	No

Table 6.6.5/5 – NotifyCompletion and RequestID

NotifyCompletion supported:	No
RequestID Parameter Supported:	No

Table 6.6.5/6 – Simultaneously played signals

Signals played simultaneously:	No

Table 6.6.5/7 – KeepActive

KeepActive used on signals:	No

6.6.6 DigitMap descriptor

Table 6.6.6 – DigitMap descriptor

DigitMaps supported:	No

6.6.7 Statistics descriptor

Table 6.6.7/1 – Statistics descriptor

Statistics supported on:	Stream

Table 6.6.7/2 – Statistics Reported On Subtract

Statistics reported on Subtract:	Yes	
	Statistic IDs reported:	ALL (see clause 6.13 for details)

6.6.8 ObservedEvents descriptor

Table 6.6.8 – ObservedEvents descriptor

Event detection time supported:	No

6.6.9 Topology descriptor

Table 6.6.9 – Topology descriptor

Allowed triples:	NA (Note)
NOTE – Optional in the case of more than two terminations (see also clause 6.3).	

6.6.10 Error Descriptor

Table 6.6.10/1 – Error codes sent by MGC

Supported H.248.8 error codes:	ALL
Supported error codes defined in packages:	All error codes defined in supported packages need to be supported.

Table 6.6.10/2 – Error codes sent by MG

Supported H.248.8 error codes:	ALL with the 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

NOTE – Below are three informative tables which provide a summary overview of clauses 6.6 and 6.7 concerning descriptors and commands respectively. Whenever there are discrepancies between these tables and the corresponding specifications in clauses 6.6 and 6.7, the specifications in clauses 6.6 and 6.7 take precedence over those described in these tables.

Table 6.7/1 shows in which direction commands are sent, which terminations they can be associated with, and which wildcard options are supported for the specific command.

Table 6.7/1 – 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	Yes

Tables 6.7/2 and 6.7/3 show for which termination types a specific descriptor can be applied, and with which commands and replies the descriptor can be used.

Table 6.7/2 – Descriptors and requests

Descriptor type	Termination type		Request					
	Root	IP	Add	Audit Value	Modify	Notify	Service change	Subtract
Audit		Yes		Yes	Yes			Yes
Error								
Events	Yes	Yes	Yes	Yes	Yes			Yes
Local		Yes	Yes		Yes			
LocalControl		Yes	Yes		Yes			
Media	Yes	Yes	Yes	Yes	Yes			Yes
ObservedEvents		Yes				Yes		
Packages	Yes			Yes				
Remote		Yes	Yes		Yes			
ServiceChange	Yes	Yes					Yes	
Signals		Yes	Yes		Yes			
Statistics		Yes	Yes	Yes	Yes			Yes
Stream		Yes	Yes		Yes			Yes
TerminationState	Yes	Yes	Yes	Yes	Yes			

Table 6.7/3 – Descriptors and replies

Descriptor type	Termination type		Reply					
	Root	IP	Add	Audit Value	Modify	Notify	Service Change	Subtract
Audit		Yes		Yes	Yes			Yes
Error	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Events				Yes				Yes
Local		Yes	Yes		Yes			
LocalControl			Yes		Yes			
Media	Yes	Yes	Yes	Yes	Yes			Yes
ObservedEvents								
Packages				Yes				
Remote		Yes	Yes		Yes			
ServiceChange	Yes	Yes					Yes	
Signals								
Statistics		Yes	Yes	Yes	Yes			Yes
Stream		Yes	Yes		Yes			Yes
TerminationState	Yes	Yes	Yes	Yes	Yes			

6.7.1 Add

Table 6.7.1/1 – Descriptors used by Add Request

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

Table 6.7.1/2 – Descriptors used by Add Reply

Descriptors used by Add reply:	Media (TerminationState, (Stream(Local, Remote)))

6.7.2 Modify

Table 6.7.2/1– Descriptors used by Modify Request

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

Table 6.7.2/2 – Descriptors used by Modify Reply

Descriptors used by Modify reply:	Media (Stream(Local, Remote)), Statistics

6.7.3 Subtract

Table 6.7.3/1 – Descriptors used by Subtract Request

Descriptors used by Subtract request:	Audit (Media (Stream (Statistics)))

Table 6.7.3/2 – Descriptors used by Subtract Reply

Descriptors used by Subtract reply:	Statistics

6.7.4 Move

Table 6.7.4 – Descriptors used by Move command

Move command used:	No

6.7.5 AuditValue

Table 6.7.5 – Descriptors used by AuditValue command

Audited Properties:	None
Audited Statistics:	ALL
Audited Signals:	None
Audited Events:	ALL
Packages Audit possible:	Yes

6.7.6 AuditCapabilities

Table 6.7.6 – Descriptors used by AuditCapabilities command

AuditCapabilities command used:	No (Note)
NOTE – There is no use case for AuditCapability command in Rw H.248 profile version 1.	

6.7.7 Notify

Table 6.7.7 – Descriptors used by Notify command

Descriptors used by Notify Request:	ObservedEvents
Descriptors used by Notify Reply:	Error

6.7.8 ServiceChange

Table 6.7.8/1 – ServiceChangeMethods and ServiceChangeReasons sent by MGC

Service Change Methods Supported:	ServiceChange Reasons supported:
Handoff	909

Table 6.7.8/2 – ServiceChangeMethods and ServiceChangeReasons sent by MG

Service Change Methods Supported:	ServiceChange Reasons supported:
Restart	901, 902
Forced	904, 905, 906, 908, 915
Disconnected	900
Graceful	905
Failover	908, 909, 919, 920
Handoff	903

Table 6.7.8/3 – ServiceChangeAddress

ServiceChangeAddress used:	Yes

Table 6.7.8/4 – ServiceChangeDelay

ServiceChangeDelay used:	Yes

Table 6.7.8/5 – ServiceChange Incomplete Flag

ServiceChange Incomplete Flag used:	No

Table 6.7.8/6 – ServiceChangeVersion

Version used in ServiceChangeVersion:	3 or 2 (Note)
NOTE – Version 2 is also supported, see clause 6.2.	

Table 6.7.8/7 – ServiceChangeProfile

ServiceChangeProfile parameter mandatory:	Yes, with ProfileID according to clause 6.1.

Table 6.7.8/8 – Profile negotiation

Profile negotiation as per H.248.18:	No

6.7.9 Manipulating and auditing context attributes

Table 6.7.9 – Context attributes manipulation and auditing

Context attributes manipulated:	Emergency, Priority
Context attributes audited:	None

6.8 Generic command syntax and encoding

Table 6.8 – Command encoding

Supported encodings:	Text

6.9 Transactions

Table 6.9/1 – Maximum number of Transaction Requests/Replies/TransResponseAcks/Segment

Maximum number of Transaction Requests/Replies/TransResponseAcks/Segment Replies per message:	1

Table 6.9/2 – Maximum number of Commands per Transaction Request

Maximum number of commands per Transaction request:	Not specified

Table 6.9/3 – Maximum number of Commands per Transaction Reply

Maximum number of commands per Transaction reply:	Not specified

Table 6.9/4 – Optional Commands

Commands able to be marked "Optional":	AuditValue

Table 6.9/5 – Wildcarded commands

Commands able to be marked "Wildcarded":	Subtract

Table 6.9/6 – Transaction timer

Transaction timer:	Value
normalMGExecutionTime	Provisioned
normalMGCExecutionTime	Provisioned
MGOriginatedPendingLimit	Provisioned
MGCOriginatedPendingLimit	Provisioned
MGProvisionalResponseTimerValue	Provisioned
MGCProvisionalResponseTimerValue	Provisioned

6.10 Messages

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

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

6.11 Transport

Table 6.11/1 – Transport

Supported transports:	Either SCTP or UDP must be supported

Table 6.11/2 – Segmentation

Segmentation Supported:	**SCTP:** Inherent in transport **UDP:** The UDP itself is a non-segmenting transport protocol. Segmentation support is not required if H.248 message sizes can be bounded below the maximum allowed UDP payload size. If this is not the case, then support for Segmentation Package is required (see clause 6.13.2.12).

Table 6.11/3 – Control association

Control association monitoring supported:	Monitoring mechanism is dependent on used H.248 transport (see above Table 6.11/1): **SCTP:** Inherent capability of SCTP. **UDP:** H.248.14 (MG-driven monitoring). Empty AuditValue on ROOT (MGC-driven monitoring).

6.12 Security

Table 6.12 – Security

Supported Security:	None

6.13 Packages

6.13.1 Overview

Table 6.13.1/1 – Mandatory packages

Mandatory packages:		
Package name	**Package ID**	**Version**
Generic	g	2
Base root	root	2
Network	nt	1
Differentiated services	ds	1
Gate management	gm	1
Traffic management	tman	1
IP NAPT traversal	ipnapt	1

Table 6.13.1/2 – Optional packages

Optional packages:			
Package name	**Package ID**	**Version**	**Support dependent on:**
MPLS	mpls	1	Support for MPLS label stacks, i.e., label switched paths (LSP) terminated by the MG and related to the H.248 termination.
VLAN	vlan	1	Support for VLAN tags and/or Ethernet priorities. Applicable only in the case of Ethernet-based IP interfaces, together with the usage of network-based Layer 2 VPNs.
MGC information	mgcinfo	1	Support for MGC related recovery.
Inactivity timer	it	1	Applicable only for UDP transport (because UDP does not support any inherent keep alive mechanism).
Segmentation	seg	1	Applicable for UDP transport where the H.248 message size could not be bounded below the maximum allowed. Or if the message size exceeds the UDP payload size.
RTP	rtp	1	H.248 IP terminations with RTP as application layer framing protocol, with or without RTCP. Support of usage metering and QoS reporting.
Media gateway overload control	ocp	1	Support for MG overload control.
IP domain connection	ipdc	1	MGC to address specific IP realm (Note).
NOTE – See also clause 6.16.1.7 and the relation with the profile specific termination name structure.			

6.13.2 Package usage information

6.13.2.1 Generic (g)

Table 6.13.2.1 – 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:**

Table 6.13.2.1 – Generic package

Events	**Mandatory/ Optional**	**Used in command:**		
Cause (g/cause)	M	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 6.13.2.2 – Base root package

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**
ALL	O	MODIFY	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				

6.13.2.3 Network (nt)

Table 6.13.2.3 – Network package

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**
Maximum jitter buffer (nt/jit)	O	ADD, MODIFY	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:**		
Network failure (nt/netfail)	O	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	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)	M	SUBTRACT	ALL
Octets sent (nt/os)	M	SUBTRACT	ALL
Octets received (nt/or)	M	SUBTRACT	ALL
Error codes	**Mandatory/Optional**		
None			

NOTE – This event may be semantically overloaded if there are multiple failure causes (see clause E.11.5.1.2 of [ITU-T H.248.1]). An unambiguous distinction between the MGC and MG sides implies mutually agreed cause code points. This is a provisioning activity.

6.13.2.4 Differentiated services (ds)

Table 6.13.2.4 – Differentiated services package

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**
ALL	M	ADD, MODIFY	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				

6.13.2.5 Gate management (gm)

Table 6.13.2.5 – Gate management package

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**
ALL	M	ADD, MODIFY	ALL	Not Applicable
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Duration provisioned value:**

Table 6.13.2.5 – 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	Subtract	ALL	
Error codes	**Mandatory/Optional**			
None				

6.13.2.6 Traffic management (tman)

Table 6.13.2.6 – Traffic management package

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**
ALL	M	ADD, MODIFY	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				

6.13.2.7 IP NAPT traversal (ipnapt)

Table 6.13.2.7 – 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				
Error codes	**Mandatory/Optional**			
None				

6.13.2.8 MPLS (mpls)

Table 6.13.2.8 – MPLS package

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**
ALL	O	ADD, MODIFY	ALL	Not Applicable
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Duration provisioned value:**

Table 6.13.2.8 – MPLS 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				

6.13.2.9 VLAN (vlan)

Table 6.13.2.9 – VLAN package

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**
ALL	M	ADD, MODIFY	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				

6.13.2.10 MGC information (mgcinfo)

Table 6.13.2.10 – MGC information package

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**
ALL	M	ADD, MODIFY	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 6.13.2.11 – 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 6.13.2.11 – 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 (Note)
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	None			
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	
None				
Error codes	**Mandatory/Optional**			
None				

NOTE – This profile supports provisioning of that value, but it has to be considered that the Inactivity Timer package Version 1 (it/1; [ITU-T H.248.14]) does not define any default value for the event parameter mit. Consequently,

a) in the case of a provisioned value the MGC could either omit this parameter, or overwrite the value by signalling that parameter value; or

b) in the case of no provisioning, the MGC must provide always the parameter value.

6.13.2.12 Segmentation (seg)

Table 6.13.2.12 – Segmentation package

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**
MGSegmentation TimerValue	M	MODIFY, AUDITVALUE	ALL	YES
MGCSegmentation TimerValue	M	MODIFY, AUDITVALUE	ALL	YES
MGMaxPDUSize	M	MODIFY, AUDITVALUE	ALL	YES
MGCMaxPDUSize	M	MODIFY, AUDITVALUE	ALL	YES
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**
None				
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Duration provisioned value:**

Table 6.13.2.12 – Segmentation 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**			
459	M			

6.13.2.13 RTP package (rtp)

Table 6.13.2.13 – 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:**
Events	**Mandatory/ Optional**	**Used in command:**		
Payload Transition (rtp/pltrans) (Note 3)	O	NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	None			
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	rtppayload (rtppltype)	O	ALL	Not Applicable

Table 6.13.2.13 – RTP package

Statistics	Mandatory/ Optional	Used in command:	Supported values:
Packets Sent (rtp/ps)	M	ADD, SUBTRACT, AUDITVALUE	ALL
Packets Received (rtp/pr)	M	ADD, SUBTRACT, AUDITVALUE	ALL
Packet Loss (rtp/pl)	M	ADD, SUBTRACT, AUDITVALUE	ALL
Jitter (rtp/jit)	O	ADD, SUBTRACT, AUDITVALUE	ALL
Delay (rtp/delay)	O	ADD, SUBTRACT, AUDITVALUE	ALL
Octets sent, (rtp/os) (Note 1)	O	ADD, AUDITVALUE, SUBTRACT	ALL
Octets received, (rtp/or) (Note 2)	O	ADD, AUDITVALUE, SUBTRACT	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]).

NOTE 3 – This profile version does not define any procedure for this event.

6.13.2.14 Media gateway overload control (ocp)

Table 6.13.2.14 – 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:**
	–	–	–	–

Table 6.13.2.14 – Overload control package

Events	**Mandatory/ Optional**	**Used in command:**		
MG_Overload (ocp/mg_overload)	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	–			

6.13.2.15 IP domain connection (ipdc)

Table 6.13.2.15 – 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	–			

6.14 Mandatory 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 6.14 – 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 ("$").
Media "m=" line	Mandatory	There are four fields (or SDP values) <media>, <port>, <proto> and <fmt> in the "m=" line (see [IETF RFC 4566]; Note 3). 1) "–" may be used for the *media* value. Other values shall be ignored, unless media specific information is required. 2) The *port* value may be underspecified with CHOOSE wildcard ("$"). 3) "–" may be used for the *proto* value, unless transport protocol specific behaviour is required by the MG. (Notes 1 and 2) 4) "–" may be used for the *format list* value. Other values shall be ignored (Note 2).
Bandwidth "b=" line	Mandatory NOTE – MUST be used together with a "m=" line.	The *modifier* value must always be "AS". The *bandwidth-value* value defines the required protocol layer 2 (e.g., Ethernet) bandwidth for the specific H.248 Stream. For RTP flows, where 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 RTP and RTCP together.

Table 6.14 – Supported SDP information elements

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 – IETF RFC 2327 defines the m-line as "m=<media> <port> <transport> <fmt list>"

For the <media>, <proto> and <fmt list> fields, the Ia profile version 1 H.248 profile [b-ETSI ES 283 018] specifies "–" may be used and values other than "–" shall be ignored. Although, according to IETF RFC 2327, "–" is not allowed for media type, transport and media format fields (see section 9 of IETF RFC 2327 "SDP grammar"), it is considered to be an admitted SDP extension in the scope of the Ia version 1 H.248 profile.

In this context, "Ignore" means: If the MG receives within the LocalDescriptor or RemoteDescriptor any values other than "–", these values shall be removed and replaced by "–" within the H.248 reply.

For Ia profile version 2 H.248 profile, [IETF RFC 4566] shall be used as a basis. [IETF RFC 4566] enables "–" as a valid character. As long as the Ia profile stays "media agnostic", then the behaviour of ignoring the <media> and <fmt list> elements shall remain. However, this may be used in the future to distinguish between media agnostic and media aware applications.

NOTE 3 – [IETF RFC 4566] obsoleted IETF RFC 2327, but the ABNF grammar did slightly change for the "m=" line:
a) IETF RFC 2327: m=<media> <port> <transport> <fmt list>
b) [IETF RFC 4566]: m=<media> <port> <proto> <fmt> ....
There is a syntactical change for the last two fields, but the semantical meaning is unchanged.

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 6.15 – 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.

Table 6.15 – Optional SDP information elements

SDP information element	Mandatory/Optional	Description
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 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.

6.16 Procedures

6.16.1 General 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.

6.16.1.1 Gate control

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.

By default, terminations representing gates for RTP traffic will typically require two UDP streams per media (one for RTP packets, one for RTCP packets). Hence, monomedia sessions require two bidirectional media streams, while a multimedia session with voice and video traffic would require four media streams, sourced and/or sinked by the same termination.

However, RTP traffic may also be controlled through a single 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.

The H.248 base protocol enables the MGC to choose the IP address and port on which a termination will receive media flows. In addition, the Gate Management package enables the MGC 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 H.248 descriptors in this Profile and the addresses used in packets sent and received by the gate is indicated in Table 6.16.1.1.

Table 6.16.1.1 – Relation between packet direction, IP address/port and H.248 descriptor/information

Packet direction	IP address/port	H.248 descriptor or information
Received by termination	Source	LocalControl Descriptor/gate management/remote source address mask + remote source port range or, if not present: Source address not explicitly enforced/signalled via "gm" package
Received by termination	Destination	Local Descriptor
Sent by termination	Source	LocalControl Descriptor/gate management/local source address + local source port or, if not present: Source address not explicitly enforced/signalled via "gm" package
Sent by termination	Destination	Remote Descriptor

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 H.248 streams in the termination.

In the context of conversational services, an active session requires that both the upstream and downstream gate be opened in bidirectional mode.

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 MG. If the gate management package is used, it shall override the configured value in the MG.

NOTE – It should be noticed that the IP source address and port may not always be available to the MGC. When 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, source port filtering should not be activated.

The gate concept, together with 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)

The procedures of this clause support the following NAPT-PT functionalities:

- 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 H.248 base protocol enables the MGC to either choose the addresses and ports associated with a termination or to request the MG 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 MGC 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 MG within the indicated IP address realm from MGC side (see also below).

If the PE-PE has router functionality, or direct L2 connectivity with the user terminals, the addressee 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 MGC (instead of being selected by the MG). The MGC shall copy the remote descriptor of the public network into the local descriptor towards the private network.

The MGC has the ability to choose the address space in which the MG allocates an IP address. This is achieved by setting the "interface" field of the IP termination identifier 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 IP termination field "interface" requires a mutual agreement between MGC and MG. This is realized via provisioning, thus beyond the scope of this Profile.

Figure 6.16.1.2 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).

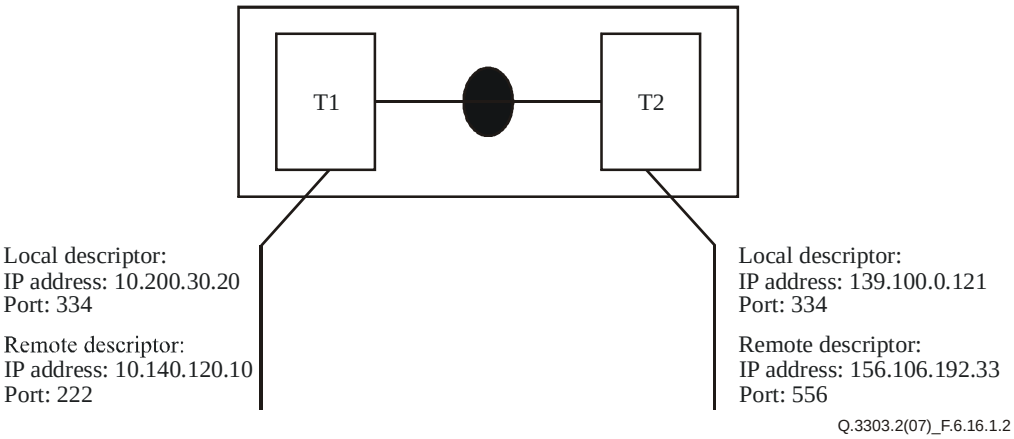

Figure 6.16.1.2 – Network address and port translation (NAPT)

For "single" network address and port translation applications, the T1 local descriptor address and port in Figure 6.16.1.2 has to be changed to 156.106.192.33: 556 (equal to the T2 remote descriptor address and port).

NAPT control on source addresses and ports 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.

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

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 BGW perspective. The remote IP address information cannot be retrieved from the remote descriptor. The "Hosted NAT Traversal" function is controlled by the MGC using the IP NAPT traversal package (ipnapt). Using the napt package, the MG is requested to perform media latching, i.e., listen for incoming media and latch to the remote address information of that media.

6.16.1.4 QoS marking

The Differentiated services package enables the MGC to control the setting of the DSCP value for all packets leaving the MG.

6.16.1.5 Bandwidth control

Resources are reserved independently on upstream and downstream gates. 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 and are ignored (Note) by the MG.

NOTE – The term "ignored" is not defined in ITU-T, the expected behaviour shall be therefore more detailed: The MGC should not use these H.248 protocol elements. When using these protocol elements, then the MG should assume the default values ('False') for ReserveValue and ReserveGroup. Furthermore, the MG shall not reply with any error code concerning these H.248 properties.

The ReserveValue and ReserveGroup properties may be also used in this profile (see clause 6.6.2.1).

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 sending packets is expressed using the "b=" line of SDP description contained in the local descriptors or using the properties of the traffic management package. The traffic management package (tman version 1) should be used in case of variable bit rate traffic.

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 with the "b=" line value of the local descriptor.

If no bandwidth information is provided, the MG will not perform traffic policing, and may not allocate enough bandwidth for all types of traffic.

6.16.1.5.1 Additional information on RTP/RTCP

RTP and its associated RTCP flow could be mapped on either:

a) a common H.248 stream; or

b) individual H.248 streams (one for RTP and one for RTCP).

The *tman* package properties are used for the configuration of the traffic policer. This traffic policer is acting on H.248 stream level due to the usage of these properties on stream level. There will be consequently either:

a) a single traffic policer enable in case of a single H.248 stream for RTP and RTCP together; or

b) two individual traffic policers used in case of dedicated stream mapping for RTP and RTCP.

Use of case a) is more simple and often already sufficient, e.g., when the amount of RTCP traffic is rather small or follows the "smaller than 5% rule" from [b-IETF RFC 3550], or when it is difficult to estimate sufficient precise RTCP traffic parameters for an explicit traffic policing. A single policer with a rather coarse configuration is then often a good compromise with regard to usage parameter control and/or the blocking of invalid RTP/RTCP traffic.

Use of case b) is more general and may be justified for, e.g.:

- RTCP flows with more than 5% of the RTP bit rate; or
- the availability of an explicit RTCP "traffic descriptor" (e.g., due to signalled information from an RTP end system); or
- significant differences of the packet sizes between RTP and RTCP;

NOTE 1 – The allowed maximum packet size could be also policed, see ITU-T Rec. H.248.53; or

- RTP sessions with "heavy" RTCP traffic due to QoS measurements and RTCP reports transports in case of RTCP XR or HR; or
- others.

NOTE 2 – An individual traffic policer for RTCP could be also used to "gate" RTCP traffic, i.e., open/close an explicit pinhole for RTCP. For example, forwarding of RTCP traffic could be suppressed by policing the ingress RTCP traffic against a bit rate of 0 bit/s, which would lead to the discard of every incoming RTCP packet.

It has to be noted that such a "misuse" of an RTCP packet policer is not generally applicable, e.g., the application should take into account whether the H.248 termination belongs to an RTP endsystem or an RTP translator, or whether the RTP application may continue correctly without any RTCP reports, etc.

6.16.1.6 Usage metering and statistics reporting

Usage metering is supported by the statistics defined in the network package. Such statistics are notified to MGC when a termination is subtracted from a context (e.g., at the end of a session). They provide information about the duration of the time a termination has been in a context, the number of octets sent and received. 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 H.248 termination (see clause E.11.5.1.5 of [ITU-T H.248.1]).

RTP statistics are in scope of this version 1 of the Profile.

The number of discarded packets due to source filtering may be reported on basis of the gm/dp statistic.

6.16.1.6.1 More details on statistics

6.16.1.6.1.1 Statistics dependent on IP-to-IP interworking mode

The available statistics for the IP streams and terminations of a dedicated context are dependent on the IP-to-IP interworking mode (see clause 3.2).

6.16.1.6.1.2 Traffic volume related statistics

6.16.1.6.1.2.1 General case

The general case relates to media-agnostic IP-to-IP interworking.

NOTE – This relates to [b-ETSI ES 283 018], the H.248 Ia profile version 1.

Traffic volume related statistics are accessible by the *nt* package.

6.16.1.6.1.2.2 RTP case

"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 and RTP header information.

6.16.1.6.1.2.2.1 RTP application data related statistics

H.248 statistics for [b-IETF RFC 3550] related octets sent/received metrics are not supported by this profile version.

6.16.1.7 IP domain/realm indication and management

6.16.1.7.1 Introduction

An IP address realm (briefly realm) is a network domain in which the network addresses are uniquely assigned to entities (see subclause 2.1 of [b-IETF RFC 2663] and clause 3.1 of [ITU-T H.248.41]). The PE-PE provides an address translation function (see clause 6.16.1.2), which implies a change between two IP address realms. This means that the two IP terminations of an H.248 context in the PE-PE would then belong to different realms. The PD-PE requires a mechanism (Note) to indicate towards the PE-PE to which realm a new added IP termination belongs.

NOTE 1 – The reason behind is the possibility of the PD-PE to use a CHOOSE wildcard for connection address in the SDP "c=" line, see clause 6.14.

The realm is distinct from a physical or logical interface on a MG (e.g., as specified by the "Interface" field of the TerminationID name) which may represent a resource on the MG.

However, in some MG provisioning scenarios there may be a mapping between the realm and the interface. The mapping between the "interface" field and the IP realm may be done through provisioned mapping tables or in case the IP realm may be encoded in the interface field.

NOTE 2 – Whether the use of H.248.41 package is mandatory or optional is for further study.

6.16.1.7.2 Methods

The IP realm identifier is sent to the PE-PE by means of the H.248.41 package (see package details in clause 6.13.2.15).

Where the PD-PE requires a termination ID to be associated with a logical or physical interface, the "group" and "interface" field may be used.

6.16.1.7.3 Unsuccessful scenarios

If the value of the IP realm identifier sent by the PD-PE within the H.248.41 package property cannot be recognized by the PE-PE, the PE-PE will fail to create the IP based H.248 termination

and replies with an error descriptor using the error code 449 (Unsupported or Unknown Parameter or Property Value).

6.16.2 Call independent procedures

6.16.2.1 PE-PE (MG) overload control

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

6.16.2.2 Failure handling procedures: interface failure

Background:

> As an example clause 9.1.2.2.1 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 the **failure of the reference point path**, 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 Annex F.4.1.3 of [ITU-T H.248.1]).

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

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, and/or to send modified, reordered information. There might be a risk that an attacker can impersonate a MGC and/or a MG illicitly acquire and tamper the information. Even though the information is encrypted, reply attack might be possible. For these security threats, operators need to be 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 MGCs can access and exchange information with each other, and particular attention on the credence and information integrity is necessary.

In the case where 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 H.248 messages, it is recommended to consider using IPSec or the interim 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 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 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 this Recommendation, although the categorization described in the next clause could apply to session-independent as well as session-dependent policing.

Rw H.248 profile version 1 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 and/or 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 1 – The differentiation between "media flow" and "media type" policing is debatable. The motivation here was driven by H.248, which provides dedicated capabilities for each policing type.

All supported policing functions at Rw interface by Rw 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), see also Appendix II.

The following policing areas are FFS, but mentioned for completeness:

5) Authorization policing

NOTE 2 – This is rather a PD-PE policing function, but could be relevant for pull mode.

6) Transport security policing

Policy conditions are based on transport related encryption information elements (e.g., 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 inband signalling.

I.2 Support by Rw H.248 profile version 1

Table I.1 provides a summary with scope on Rw H.248 profile version 1.

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

Policy category	Examples	Support by Rw H.248 profile version 1
Address policing	*Source* filtering	Yes, with gm/1 package.
	Destination filtering	No.
Traffic policing	Traffic *descriptor* based policing (Note 1)	Yes, with tman/1 package (Note 2).
	Traffic *contract* based policing (Note 1)	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 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 H.248 profile version 1, 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 of 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 H.248 packages (inclusive their statistics) are used for specific stages of the "processing pipeline". Statistics may be used at H.248 stream- or termination-level.

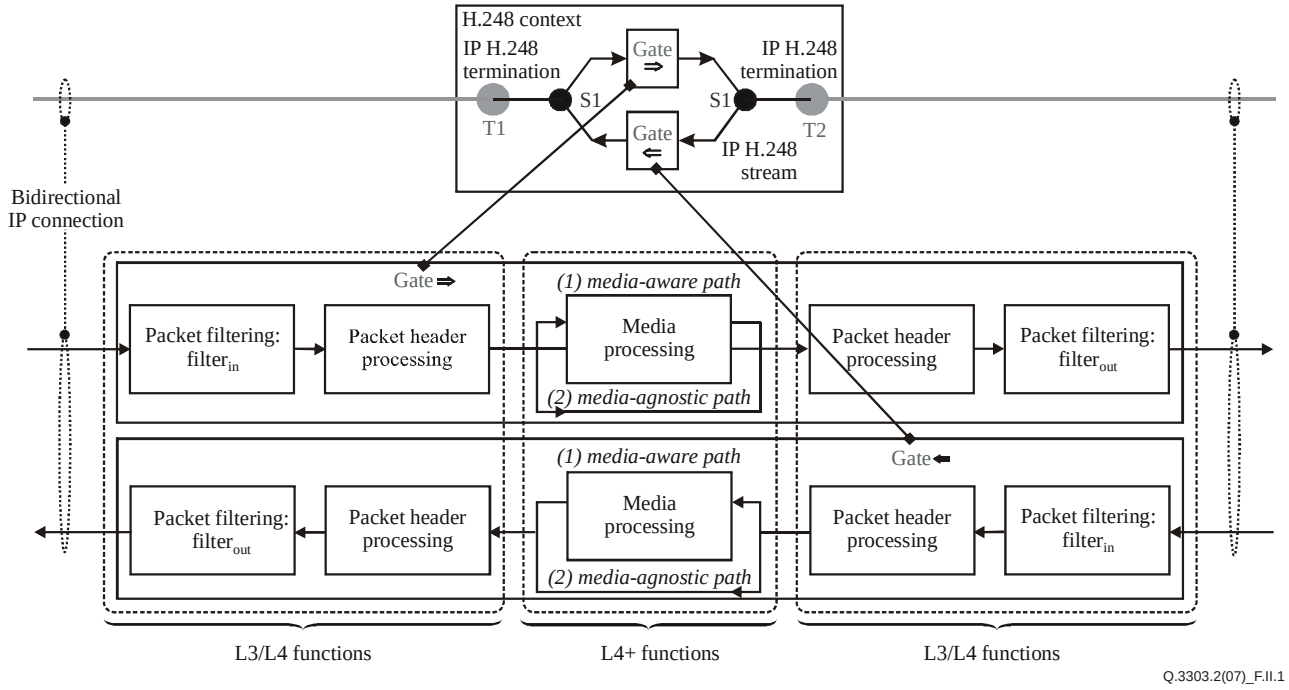

Figure II.1 – PE-PE – General IP-to-IP interworking model (Example with a single H.248 stream per termination)

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

II.2 Overview of H.248 statistics

Statistics are required to be supported at the Rw reference point. They could be categorized into 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 SNMP MIBs).

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

Statistics category	Examples	Support by Rw H.248 profile version 1
1) Usage metering	Metering of application data, e.g., for: • 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: • IETF 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 H.248.30 and 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 (see Appendix I).	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 on the IP-to-IP interworking model. The majority of statistics is in the ingress path.

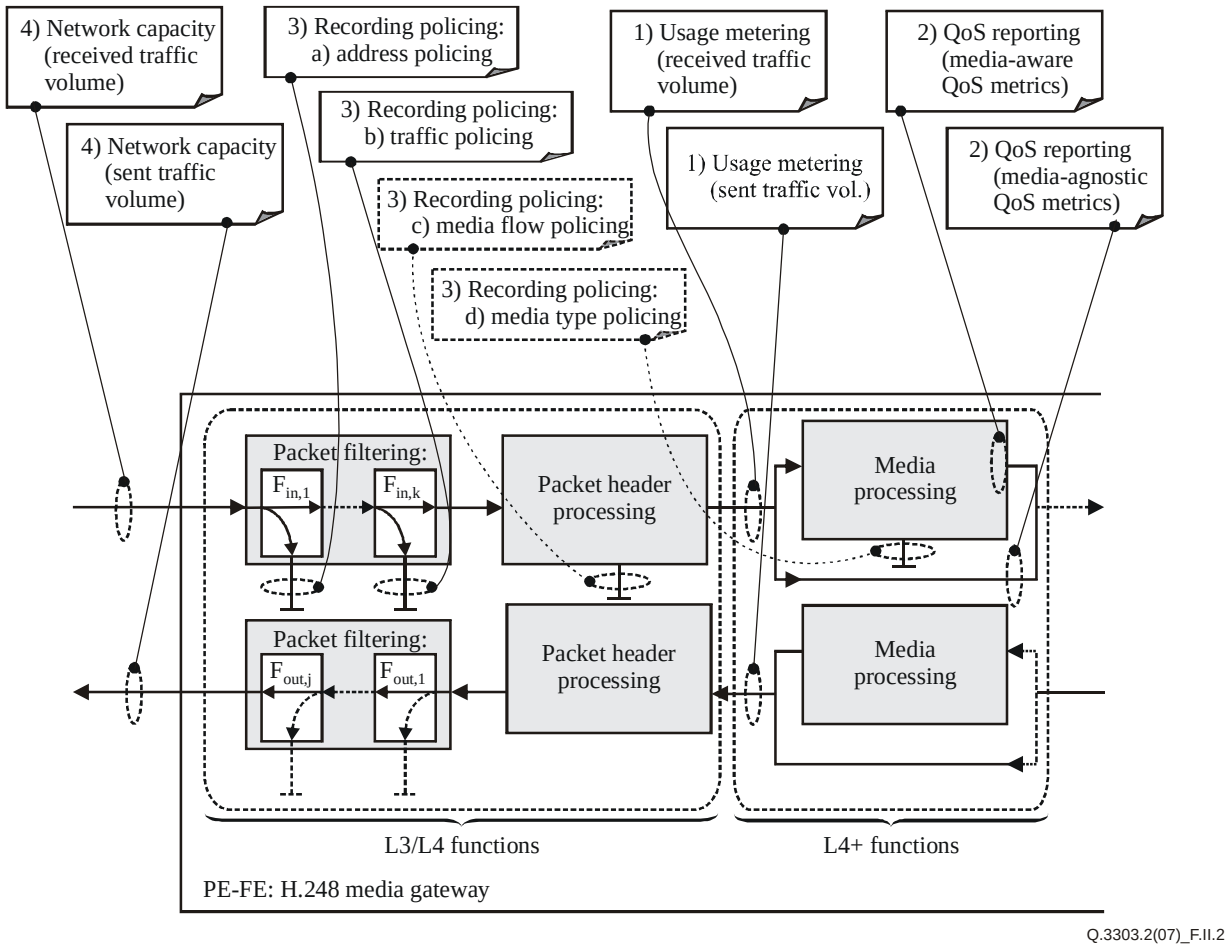

Figure II.2 – Schematic mapping of H.248 statistics on the IP-to-IP interworking model

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

Appendix III

Differences between ETSI ES 283 018 V1.1.4 and ITU-T Rec. Q.3303.2

(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 ITU-T Rec. Q.3303.2.

Table III.1 – Differences between [b-ETSI ES 283 018] and ITU-T Rec. Q.3303.2

Topic	[b-ETSI ES 283 018]	ITU-T Rec. Q.3303.2
Required H.248 Gateway Control Protocol Version	H.248 Version 3	H.248 Version 3 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 H.248 streams are sufficient to handle various combinations of flows associated with media including possible separation of RTP from RTCP 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 – Differences between [b-ETSI ES 283 018] and ITU-T Rec. Q.3303.2

Topic	[b-ETSI ES 283 018]	ITU-T Rec. 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: NA (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, 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 – Differences between [b-ETSI ES 283 018] and ITU-T Rec. Q.3303.2

Topic	[b-ETSI ES 283 018]	ITU-T Rec. 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 H.248 Termination (see clause E.11.5.1.5 of [ITU-T H.248.1]). RTP statistics are in scope of this version 1 of the Profile. More details on Statistics are described in clause 6.16.1.6.1

Table III.1 – Differences between [b-ETSI ES 283 018] and ITU-T Rec. Q.3303.2

Topic	[b-ETSI ES 283 018]	ITU-T Rec. Q.3303.2
IP domain/realm indication	Supported, but ETSI ES 283 018 does not provide any explicit description for that function.	Described in clause 6.16.1.7
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 H.248 profile specifications, i.e., ETSI TR 183 025 complements each profile specification. The set of profile-applicable call-independent procedures is primarily given by the supported H.248 Command API capabilities for AuditValue (see clause 5.8.5), AuditCapabilities (see clause 5.8.6) and ServiceChange (see clause 5.8.8), 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

Table III.1 – Differences between [b-ETSI ES 283 018] and ITU-T Rec. Q.3303.2

Topic	[b-ETSI ES 283 018]	ITU-T Rec. Q.3303.2
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-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 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 3611] IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR)*.

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	Telephone transmission quality, telephone installations, local line networks
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, 2008