ETSI TR 183 068 V3.1.1 (2009-08)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Guidelines on using Ia H.248 profile for control of Border Gateway Functions (BGF); Border Gateway Guidelines

Reference

DTR/TISPAN-03202-NGN-R3

Keywords

gateway, H.248, SIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document defines guidelines for usage and implementation of border gateways (BGW), based on H.248 profile definitions for controlling such IP-to-IP gateways like ETSI TISPAN "H.248 Ia profile" specifications [i.1], [i.2] and [i.3].

Figure 1 illustrates the architecture assumed in the present document.

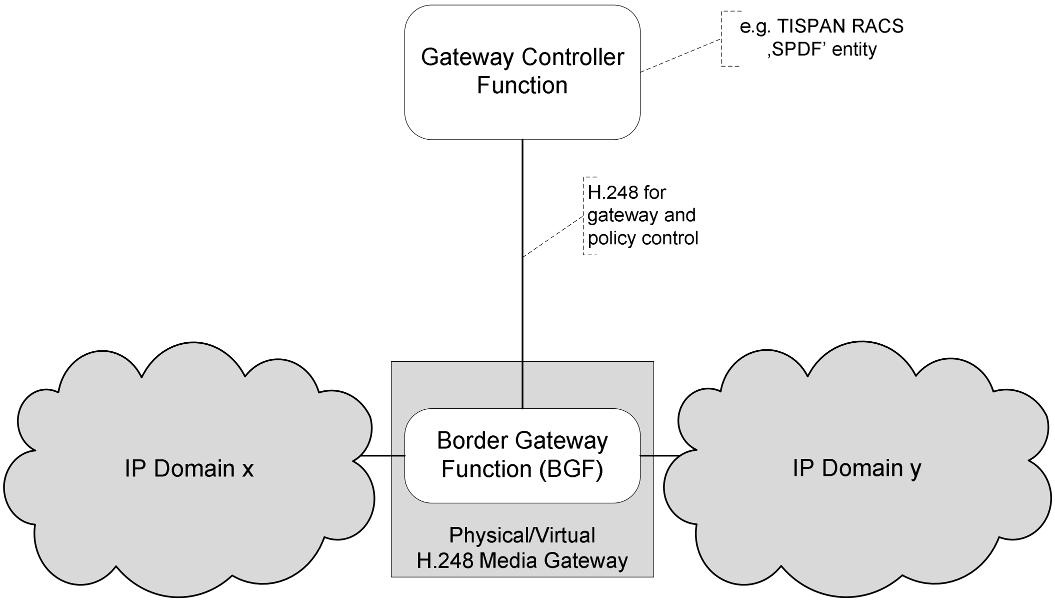

Gateway Controller Function
e.g. TISPAN RACS ‚SPDF' entity
H.248 for gateway and policy control
IP Domain x
Border Gateway Function (BGF)
Physical/Virtual H.248 Media Gateway
IP Domain y

Figure 1: Scope

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI ES 283 018 (Release 1): "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". - also known as "H.248 Ia Profile Version 1".

[i.2] ETSI ES 283 018 (Release 2): "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". - also known as "H.248 Ia Profile Version 2".

[i.3] ETSI TS 183 018 (Release 3): "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". - also known as "H.248 Ia Profile Version 3".

[i.4] ITU-T Recommendation H.248.1 (2005): "Gateway control protocol: Version 3" including its Amendment 1 (05/2008).

[i.5] ETSI TS 183 048: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control System (RACS); Protocol Signalling flows specification; RACS Stage 3".

[i.6] ETSI TS 183 017: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification".

[i.7] ETSI TS 181 018 (Release 2): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN".

[i.8] ETSI TR 182 022 (Release 2): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Architectures for QoS handling".

[i.9] IEEE 802.3: "Ethernet Working Group".

[i.10] ETSI TR 187 008 (Release 1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report".

[i.11] IETF RFC 5117 (2008-01): "RTP Topologies".

[i.12] draft-hunt-avt-rtcptrans-00.txt (2007-11): "RTCP Reporting by Translators".

[i.13] ITU-T Recommendation Y.1251 (08/2002): "General architectural model for interworking".

[i.14] Draft ITU-T Recommendation G.IP2IP: "Functionality and Performance of an IP-to-IP Voice Gateway, optimised for the transport of voice and voiceband data".

[i.15] ITU-T Recommendation Y.1560 (09/2003): "Parameters for TCP connection performance in the presence of middleboxes".

[i.16] IEEE 802.1: "Local Area Networks: Architecture & Overview".

[i.17] IETF RFC 1812: "Requirements for IP Version 4 Routers".

[i.18] IETF RFC 768: "User Datagram Protocol".

[i.19] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

[i.20] IETF RFC 3551: "RTP Profile for Audio and Video Conferences with Minimal Control".

[i.21] IETF RFC 4733: "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals".

[i.22] IETF RFC 3142: "An IPv6-to-IPv4 Transport Relay Translator".

[i.23] IETF RFC 4734: "Definition of Events for Modem, Fax, and Text Telephony Signals".

[i.24] ITU-T Recommendation Draft H.248.64.

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Admission Control
B2BIH	Back-to-Back IP Host (mode)
B2BRE	Back-to-Back RTP Endsystem (mode)
B2BTE	Back-to-Back TCP Endpoint (mode)
BGF	Border Gateway Function
CBR	Constant Bit Rate
IP	Internet Protocol
IPR	IP router (mode)
LCD	Local Control Descriptor
LD	Local Descriptor (H.248)
LS	Local Source
MALG	Media Application lLevel Gateway
MG, MGW	Media GateWay
MGC	Media Gateway Controller
MP	Measurement Point
MSRP	Message Session Relay Protocol
NA(P)T	Network Address (and Port) Translation
NAPT	Network Address and Port Translation
NTE	Network Telephone Events
PCI	Protocol Control Information
PDU	Protocol Data Unit
RD	Remote Descriptor (H.248)
RFC	Request For Comments (IETF)
RP	Reporting Point
RS	Remote Source
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
RTPMTm	RTP Media Translator mode
RTPTTm	RTP Transport Translator mode
SDP	Session Description Protocol
SDU	Service Data Unit
SIP	Session Initiation Protocol
SPDF	Service Policy Decision Function
StAC	Stream Admission Control
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRT	Transport Relay Translator
UDP	User Datagram Protocol
VBR	Variable Bit Rate

4 Structure of this Technical Report

The present document inherits a structure based on annexes from the H.248 Ia profile specifications [i.1], [i.2] and [i.3]. The annex numbering was kept in order to be consistent with the old document versions of these specifications.

Any references from the annexes are related to H.248 Ia profile version 3 specification [i.3].

Annex A: Illustration of Gate/Pinhole Concept

The purpose of this annex is the illustration of the H.248 Stream/Termination model by showing exemplary realizations of gates for uni- versus bidirectional media flows.

A.1 General

Only point-to-point sessions are in scope of this H.248 Profile (see clause 5.4, TS 183 018 [i.3]). Interconnection of individual H.248 Streams is based on the basic principle described in clause 7.1.6/H.248.1 [i.4]. The H.248 Multiplex Descriptor is therefore not necessary (see clause 5.6.2, TS 183 018 [i.3]). The H.248 Topology Descriptor definition includes individual H.248 Streams, but is also not necessary (see clause 5.7.8, TS 183 018 [i.3]).

It has to be noted that all sessions have unicast media flows. Potential multicast applications are transparent for MG point of view.

A.2 Relationships between gates and H.248 Streams

The realization of a gate is illustrated in figure A.1. There is a unidirectional media flow in that example, and there is a single H.248 Stream per Termination. A **H.248 Stream** covers per definition a single **bidirectional** media flow (clause 7.1.6/ITU-T Recommendation H.248.1 [i.4]). In this profile when RTP is used with RTCP, a single H.248 stream represents both RTP media and the corresponding RTCP flow. Media flows are interconnected by using the same **StreamID** (here: StreamID equals to S1 for T1 and T2).

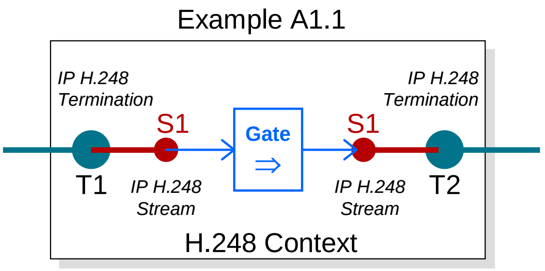


Figure A.1: H.248 Context - Illustration of Gate, Stream and Terminations

The uni- or bidirectional application of an H.248 Streams is controlled via usage of Local Descriptor (LD) and Remote Descriptor (RD). Figure A.2 shows a bidirectional session. There is again a single H.248 Stream per Termination. Gates are direction-dependent, there are consequently two gates in this example.

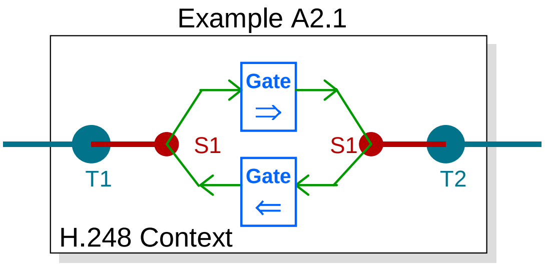


Figure A.2: H.248 Context Bidirectional Session using single H.248 Streams

Annex B: Void

NOTE: This clause is present to be backwards compatible with the H.248 profile specifications in [i.2] and [i.3].

Annex C: Void

NOTE: This clause is present to be backwards compatible with the H.248 profile specifications in [i.2] and [i.3].

Annex D: Illustration of an IP processing model for an H.248 (IP, IP) Context

The purpose of this annex is the illustration of a possible IP flow processing model. Such a model is helpful when considering aspects concerning:

- location of a particular function within the (BGF) processing pipeline; or
- possible interactions between functions (see e.g. clause D.2).

It has to be noted that the model is just an example, not exhaustive concerning all possible functions with regards to supported capabilities by this profile, and not related to any particular implementation.

D.1 Example model

Figure D.1 provides an example pipeline model, which is only indicating a single H.248 Stream of the (IP, IP) Context. A H.248 Stream is fundamentally bidirectional, i.e. relates to two unicast IP flows, one per traffic direction. This example is not considering aspects of RTP/RTCP mapping on a H.248 Stream.

The example model is considering optional and mandatory functions by this profile specification. The example is using modelling components for *filter* (F), *detector* (D), *address* processing (A) and *statistic* (S) entities. There might be further modelling components, e.g. for media-aware specific processing functions. The example model is assuming a pure serial processing pipeline, real implementations could of course benefit from parallelization.

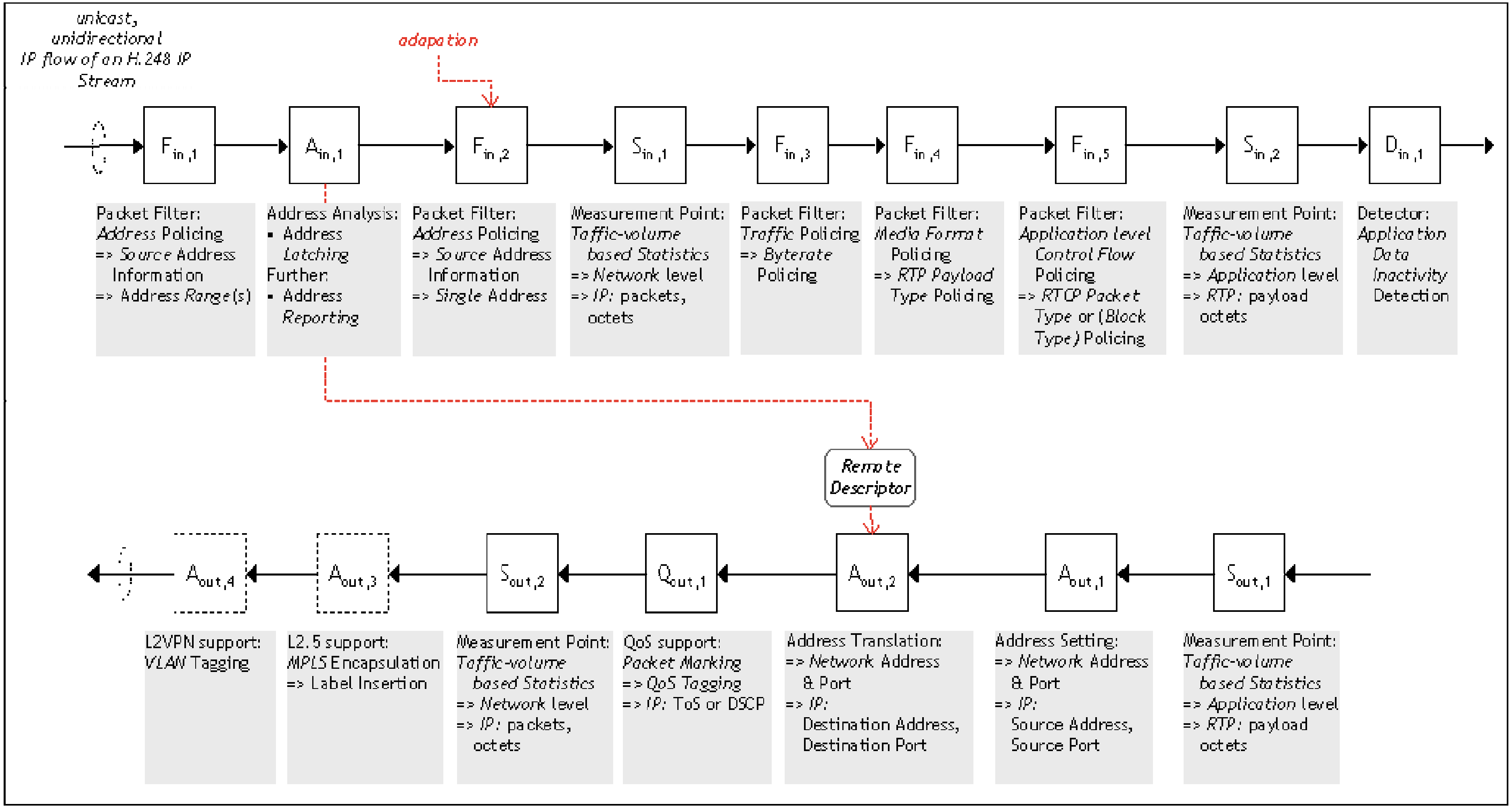

unicast, unidirectional IP flow of an H.248 IP Stream
adapation
F in,1
A in,1
F in,2
S in,1
F in,3
F in,4
F in,5
S in,2
D in,1
Packet Filter: Address Policing => Source Address Information => Address Range(s)
Address Analysis: ▪ Address Latching Further: ▪ Address Reporting
Packet Filter: Address Policing => Source Address Information => Single Address
Measurement Point: Taffic-volume based Statistics => Network level => IP: packets, octets
Packet Filter: Traffic Policing => Byterate Policing
Packet Filter: Media Format Policing => RTP Payload Type Policing
Packet Filter: Application level Control Flow Policing => RTCP Packet Type or (Block Type) Policing
Measurement Point: Taffic-volume based Statistics => Application level => RTP: payload octets
Detector: Application Data Inactivity Detection
Remote Descriptor
A out,4
A out,3
S out,2
Q out,1
A out,2
A out,1
S out,1
L2VPN support: VLAN Tagging
L2.5 support: MPLS Encapsulation => Label Insertion
Measurement Point: Taffic-volume based Statistics => Network level => IP: packets, octets
QoS support: Packet Marking => QoS Tagging => IP: ToS or DSCP
Address Translation: => Network Address & Port => IP: Destination Address, Destination Port
Address Setting: => Network Address & Port => IP: Source Address, Source Port
Measurement Point: Taffic-volume based Statistics => Application level => RTP: payload octets

Figure D.1: H.248 Context - Illustration of IP flow processing - Example Overview

There might be dependencies between different processing stages, which impact the order of pipeline stages.

D.2 Aspects of filter interaction

Possible filter interactions are already indicated in several package specifications of the ITU-T Recommendation H.248.x-series of Recommendations. General solutions/recommendations are not yet provided by the package definitions themselves. This is therefore rather a subject for profile specifications, which using the correspondent packages.

D.2.1 Interaction between address latching and address policing

This profile version indicates two possible cases for filter interaction, either due to:

- enabled *latching* plus *address policing* per H.248 Stream, i.e. application of packages *ipnapt* v1 and *gm* v1; or
- the *correlation* of *SDP information* from the RD and *gm* v1 address policing (see clause 5.18.1.1.1, TS 183 118 [i.3]).

Figure D.2 illustrates the possible interaction: the ingress filter stage $F_{in,1}$ provides explicit source address and port policing and is controlled via *gm* v1 properties (see clause 5.18.1.1.1, TS 183 118 [i.3]). Source address and port policing could be applied for a single individual address/port, a single address/port range, multiple individual addresses/ports, multiple address/port ranges, or combinations thereof. Stage $F_{in,2}$ provides implicit source address/port policing and is controlled via the (re)latching process (and ***not*** controlled via *gm* v1 properties).

The function address latching/re-latching is provided by stage $A_{in,1}$.

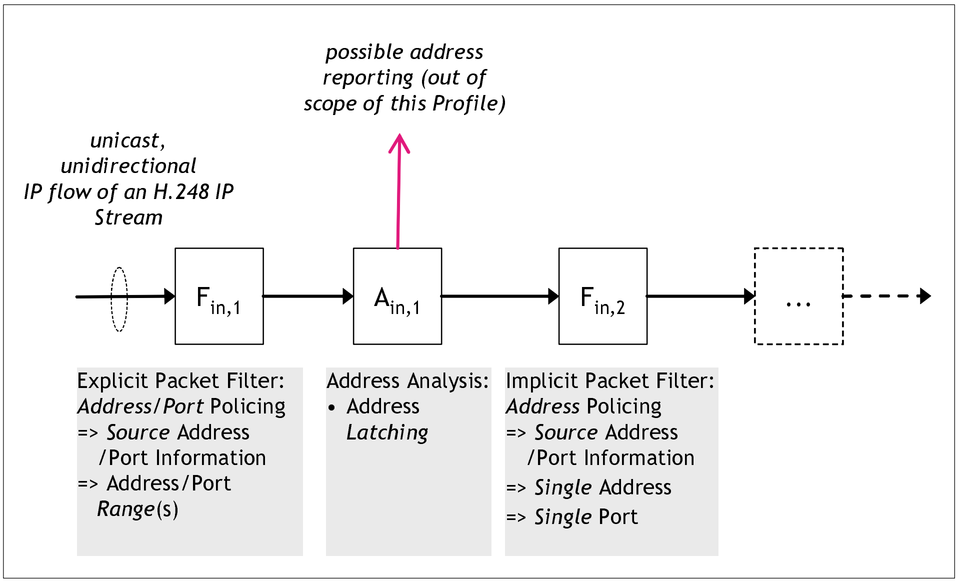

possible address reporting (out of scope of this Profile)
unicast, unidirectional IP flow of an H.248 IP Stream
F in,1
A in,1
F in,2
...
Explicit Packet Filter: Address/Port Policing => Source Address /Port Information => Address/Port Range(s)
Address Analysis: • Address Latching
Implicit Packet Filter: Address Policing => Source Address /Port Information => Single Address => Single Port

Figure D.2: H.248 Context - Illustration of IP flow processing - Interaction between address latching and address policing - Example model 1

Package *gm* v1 controlled filters are independent of the latching process. The latching process could lead to an adaptation of the implicit source address/port filter (according clause 5.18.1.1.1, TS 183 118 [i.3], and as indicated in figures D.2, D.3 or D.4).

The interaction and adaptation could affect different filter stages, dependent on the applied model. Figure D.3 illustrates another example: $F_{in,1}$ filters on some source address and port ranges.

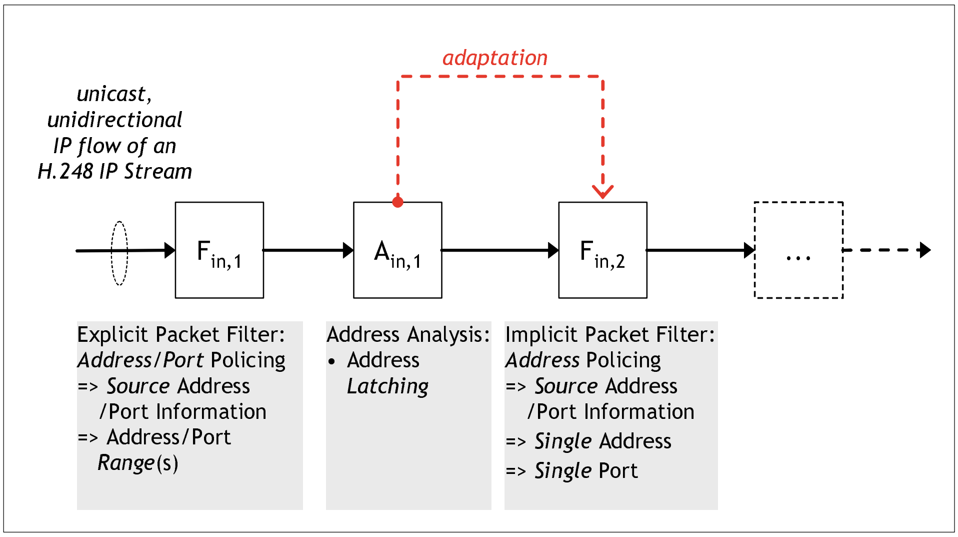

adaptation
unicast, unidirectional IP flow of an H.248 IP Stream
$F_{in,1}$
$A_{in,1}$
$F_{in,2}$
...
Explicit Packet Filter: Address/Port Policing
=> Source Address /Port Information
=> Address/Port Range(s)
Address Analysis:
• Address Latching
Implicit Packet Filter: Address Policing
=> Source Address /Port Information
=> Single Address
=> Single Port

Figure D.3: H.248 Context - Illustration of IP flow processing - Interaction between address latching and address policing - Example model 2

Figure D.4 illustrates another example: stage $F_{in,1}$ filters on a specific source address/port range.

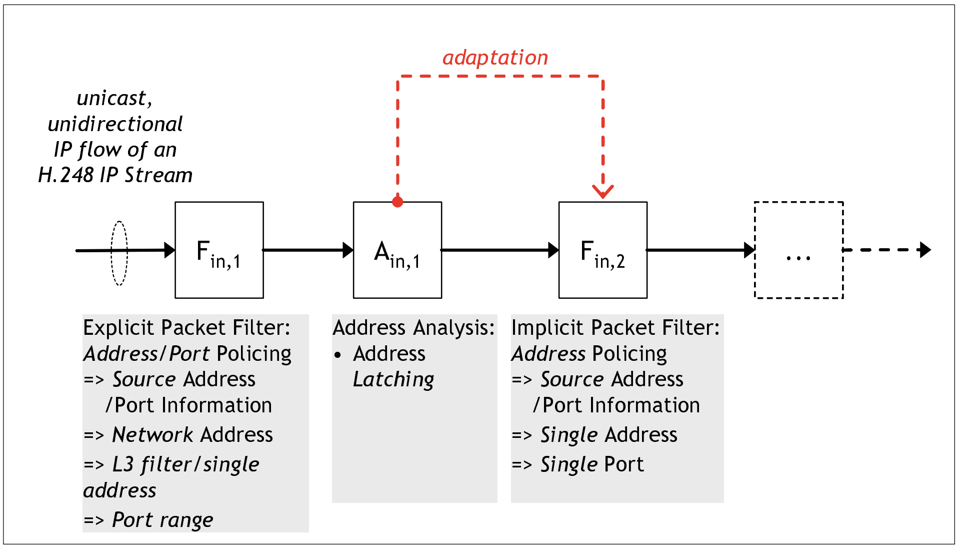

adaptation
unicast, unidirectional IP flow of an H.248 IP Stream
$F_{in,1}$
$A_{in,1}$
$F_{in,2}$
...
Explicit Packet Filter: Address/Port Policing
=> Source Address /Port Information
=> Network Address
=> L3 filter/single address
=> Port range
Address Analysis:
• Address Latching
Implicit Packet Filter: Address Policing
=> Source Address /Port Information
=> Single Address
=> Single Port

Figure D.4: H.248 Context - Illustration of IP flow processing - Interaction between address latching and address policing - Example model 3

Annex E: Guidelines for Ia-to-Gq' mapping

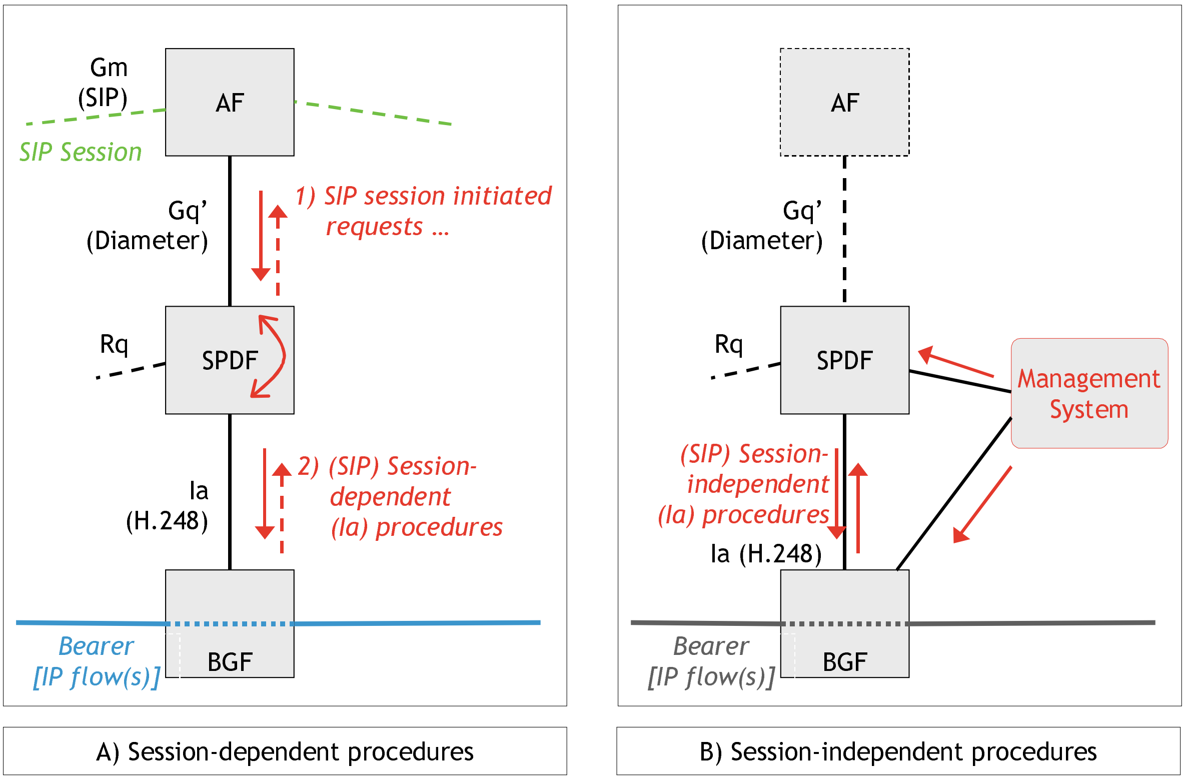
The purpose of this annex is to provide mapping guidelines in the area of:

- session-independent procedures;
- bearer-specific events (e.g. due to failure detection); or
- unsuccessful session completions.

E.1 Guidelines for Ia-to-Gq' mapping with regards to session-independent procedures

E.1.1 Introduction

The procedures of the H.248 Ia profile are divided in *session-dependent* (see clause 5.17.1, TS 183 118 [i.3]) and *session-independent* (see clause 5.17.2, TS 183 118 [i.3]) procedures. Figure E.1 depicts the major difference between both procedure categories when looking at the vertical interfaces Gq' besides Ia.



A) Session-dependent procedures

B) Session-independent procedures

Figure E.1: RACS architecture - Session-dependent vs Session-independent procedures from Ia point of view

E.1.2 Mapping guidelines

E.1.2.1 Session-dependent procedures

Mapping rules for Gq'-to-Ia for *session-dependent* procedures (see (A) in figure E.1) is in scope of TS 183 048 [i.5].

E.1.2.2 Session-independent procedures

The scope of *session-independent* procedures, as defined by this profile, is limited on Ia (see (B) in figure E.1). There are thus neither guidelines required nor provided for mappings from/towards Gq'.

E.2 Guidelines for Ia-to-Gq' mapping with regards to bearer-specific events

E.2.1 Introduction

H.248 provides a much wider set of protocol elements for support of bearer-related events as in comparison to other protocols like Diameter. This means for H.248-to-Diameter mappings, like for Ia-to-Gq' signalling direction, that often typically more than one H.248 procedure could be mapped on the same Diameter procedure.

The Ia-to-Gq' mapping function is therefore not bijective (at least as long as both protocols providing different capability sets). Mapping guidelines might be thus beneficial for implementers.

Figure E.2 illustrates the relevant part of RACS.

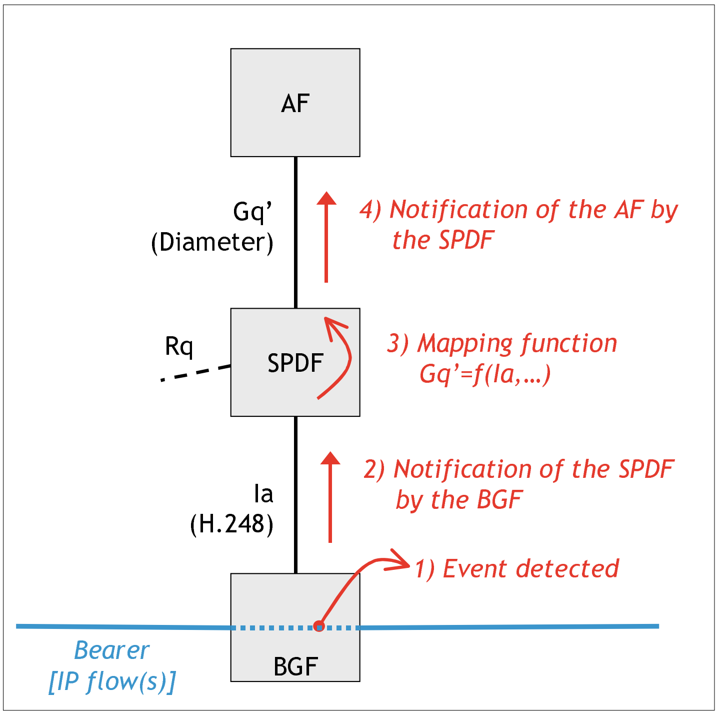

AF
Gq’
(Diameter)
4) Notification of the AF by the SPDF
Rq
SPDF
3) Mapping function Gq’=f(Ia,…)
Ia
(H.248)
2) Notification of the SPDF by the BGF
1) Event detected
Bearer
[IP flow(s)]
BGF

Figure E.2: RACS architecture - Vertical event notifications - Ia-to-Gq' mapping

E.2.2 Mapping guidelines

E.2.2.1 Guidelines for *Specific Action* AVPs

Table E.1: Guidelines for Attribute Value Pairs according clause 7.3.23/TS 183 017

Gq' (Diameter)		**Ia (H.248)**		
Specific action AVP Ref.: TS 183 017 [i.6], clause 7.3.23		Possible H.248 Protocol Elements	Possible H.248 Ia Profile Procedure	Recommended for Ia Version 2
	INDICATION_OF_ LOSS_OF_BEARER (2)	H.248.1 Event: g/cause	User Plane Failure (5.19.12/5.20.18).	Yes
		H.248.1 Event: nt/netfail	ditto	Yes (but optional profile element)
		H.248.1 Event: nt/qualert	ditto	Yes (but optional profile element)
		H.248.40 Event: adid/ipstop	IP Media Stop (clause 5.18.4.1).	(see note 7)
		H.248.36 Event: hangterm/thb (see note 8)	-	-
		H.248 ServiceChange: {Forced/Graceful, 904}	(see note 1)	No
		H.248 ServiceChange: {Forced/Graceful, 905}	(see note 2)	No
		H.248 ServiceChange: {Forced/Graceful, 906}	(see note 3)	No
	INDICATION_OF_ RECOVERY_OF_ BEARER (3)	H.248.13 Event: nt/qac/qualertcease	Not supported by this profile version.	(see note 6)
		H.248 ServiceChange: {Restart, 900}	(see note 4) Not supported by this profile version.	No
	INDICATION_OF_ RELEASE_OF_ BEARER (4)	H.248 Subtract.reply command	Regular H.248 method (see note 5).	Yes

NOTE 1: Indication of "*termination malfunction*" for ephemeral termination.
NOTE 2: Indication of "*termination taken Out-of-Service*" for ephemeral termination.
NOTE 3: Indication of "*loss of lower layer connectivity*" for ephemeral termination.
NOTE 4: Indication of "*service restore*" for ephemeral termination.
NOTE 5: The H.248 Media Gateway is not allowed to autonomously "subtract a H.248 Stream/Termination", which would relate to a "release bearer" event. There is therefore also not any ServiceChange procedure defined.
NOTE 6: This method might be as closest to the AVP (3) semantic, particularly when *nt/qualert* would be used for AVP (2).
NOTE 7: This event could be overlaid with multiple application. Thus, "No" in case that event is already used for other purposes (e.g. like latching deadlock detection), else "Yes".
NOTE 8: Not applicable here.

E.2.2.2 Other AVPs

The AVPs that are discussed in this annex serve as a guideline and are not meant to be an exhaustive list of the AVPs that require mapping to/from Ia (H.248). There may well be further AVPs require mapping guidelines to/from Ia (H.248). Such further mapping is considered to be beyond the scope of this annex.

Annex F: Bandwidth Reservation - Examples for Bandwidth Estimations

The purpose of this annex is to provide some background in estimation methods for bitrate reservations, illustrated by some examples. Figure F.1 summarizes the scope of annex F. Protocol layer specific transformation of bandwidth requests and the aspect of admission control (related to the resource management aspect of resource component "bandwidth") is discussed besides examples for bandwidth calculation and estimation.

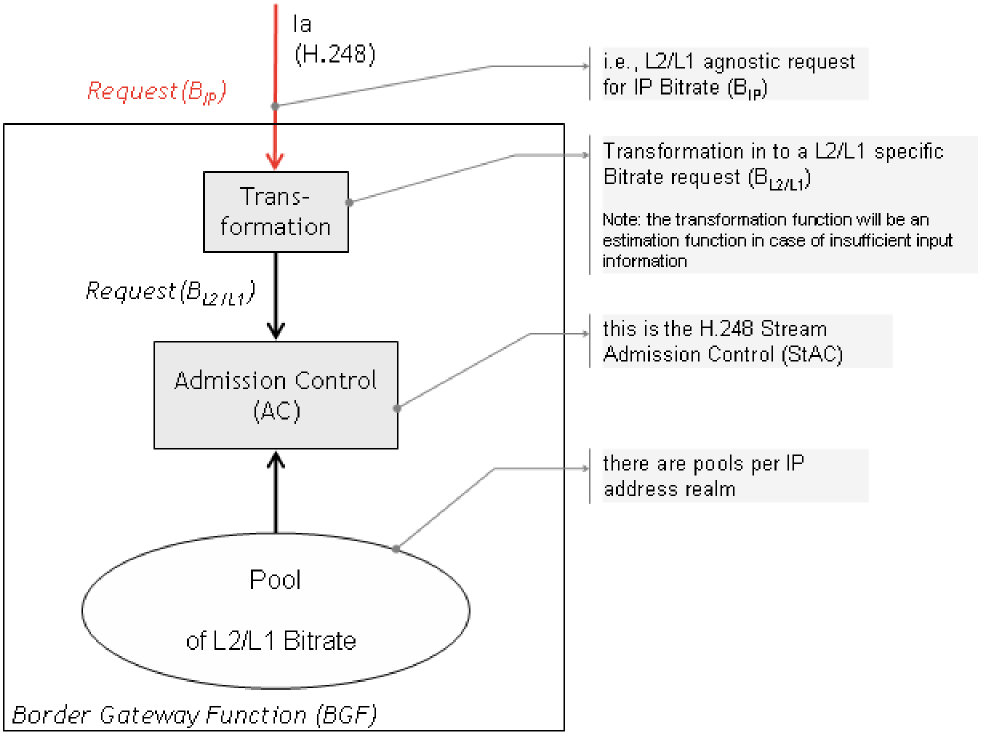

Ia
(H.248)
Request(B_{IP})
Trans-formation
Request($B_{L2/L1}$)
Admission Control (AC)
Pool
of L2/L1 Bitrate
Border Gateway Function (BGF)
i.e., L2/L1 agnostic request for IP Bitrate (B_{IP})
Transformation in to a L2/L1 specific Bitrate request ($B_{L2/L1}$)
Note: the transformation function will be an estimation function in case of insufficient input information
this is the H.248 Stream Admission Control (StAC)
there are pools per IP address realm

Figure F.1: Bandwidth Reservation Request - Processing in the BGF

F.1 Introduction

Resource reservation in RACS is just related to the *single* resource component type "bitrate" *B* (colloquially also termed as "bandwidth"). The *bitrate B* relates to a particular *traffic rate*, i.e. *traffic volume* per *time unit*. The SPDF (or Application Function, or user equipment) provides an *estimate* for *B* for every *new* or *modified* H.248 Stream. It is an estimate (rather than an "exact" stochastically description) due to traffic source abstraction with just a single traffic parameter.

F.1.1 Bitrate B in general

F.1.1.1 Before service admission

As the *stationary* bitrate (i.e. constant time-average) value is *unknown* before the communication phase, the SPDF (or AF, or UE) needs thus an estimation method. There are many possibilities, like e.g. by considering the *distribution functions* of the two metrics *PDU rate* $\mu_{PDU,Lj}$ and *PDU size* $K_{PDU,Lj,i}$. An *estimate* for an average bitrate could be then calculated, e.g. by:

$$\hat{B}_{Lj} = \hat{\mu}_{PDU,Lj} \cdot \hat{K}_{PDU,Lj} \cdot 8 \text{ in } \left[\frac{bit}{s}\right] \qquad \text{(F-1)}$$

NOTE: ^ indicates an estimated value.

a) Estimated expected *PDU rate* $\hat{\mu}_{PDU,Lj}$:

- The PDU rate is often tightly related to the *packetization time* of media encoder units, in case of *media* IP flows. Enabled silence suppression or a muted microphone could reduce temporarily the rate in case of *voice* media.
  The PDU rate estimation could be more challenging for VBR (Variable Bit Rate) sources (e.g. with a high burstiness) than for Constant Bit Rate (CBR) sources.
  The estimated PDU rate is in any case here time-independent.

b) Estimated expected *PDU size* $\hat{K}_{PDU,Lj}$:

- The PDU size is generally varying, i.e. $K_{PDU,Lj,i}$ will not be equal to $K_{PDU,Lj,I-1}$. A mean value is supposed in the estimation here.

F.1.1.1a After service completion

The value of *B would* be *known* after the *completion* of an H.248 Stream (Context): the *average bitrate* relates then to the *time-average* for the entire duration of the stream:

Average bitrate B_{Lx} on protocol layer L_j per H.248 Stream S_v:

$$B_{Lj} = \frac{V_{Lj}}{T_{H,Sv}} \cdot 8 \text{ in } \left[\frac{bit}{s}\right] \qquad \text{(F-2)}$$

The *traffic volume* V_{Lj} (on protocol layer *Lj*) is basically given by the sum of *all octets* of all transferred protocol data units (PDUs). The lifetime (or holding time) of the H.248 Stream S_v is given by T_H in equation (F-2).

F.1.1.2 Transport efficiency

Every P*rotocol Data Unit* (PDU) is composed of the *Service Data Unit* (SDU) and *Protocol Control Information* (PCI). The same traffic volume (service data) could be carried with different PDU "rate × size" products (e.g. μ low and *K* high, or μ high and *K* low). Every PDU "rate × size" product has a different transport efficiency concerning the ratio of service data to control information, or "net bitrate" (for the service data) versus "gross bitrate". This aspect may need consideration when managing the transport capacity of a BGF interface. Another aspect is discussed in clause F.1.2.

F.1.2 Some important RACS principles

F.1.2.1 Independence of layer 2 and layer 1

A RACS is based on an IP infrastructure. The underlying protocol layers below IP are *not* considered for "resource admission and control". This IP-centric view allows the consideration of *many different transport technologies* for IP in RACS. This is a *L2-independent resource management model* from network perspective. Such a model does offload the SPDF from lower layer information.

F.1.2.2 Awareness of IP version

The SPDF is basically aware of the underlying IP version of an H.248 Stream. This is important due to the different amount of PCI behind the figures for B_{IPv4} and B_{IPv6}.

F.1.3 VPN Identifiers

Support of VPNs could lead to increased PCI figures. For instance, Ethernet-based L2VPNs do consume two octets additional PCI per L2 frame (for the IEEE 802.1 [i.16] *Tag Control Information* field, which includes the VLAN identifier).

F.1.4 SDP "b=" line semantic in H.248 Ia profile versions

There are unfortunately different semantics due to historical reasons:

- H.248 Ia Profile Version 1: … defines the **layer 2 bandwidth** B_{L2} for the specific H.248 Stream.
- H.248 Ia Profile Version 2 and 3: … defines the **IP layer bandwidth** B_{IP} for the specific H.248 Stream.

F.1.5 Conclusion: ideal resource management model for resource "bitrate"

The SPDF has view on IP realms. The BGF provides a certain "L1 bitrate capacity" per each realm. An ideal model for managing the bitrates for H.248 Streams would be related to a "constant" IP bitrate capacity (per realm). However, the available IP bitrate capacity is *varying* in reality as outlined in previous clauses.

EXAMPLE: BGF supports a (gross) capacity of 10 Gbit/s L2 bitrate for realm R_i. What is the available IP bitrate in case of Ethernet as L2 technology? The answer on this question is in general unknown and may be only given for some special conditions ("it is known that all sessions in this realm will use the same PDU rate with value …").

However, the variety concerning available IP bitrate capacity is in practice unproblematic: the BGF will anyway do a Stream Admission Control (StAC, see 5.17.1.5.1.2. TS 183 018 [i.3]). The received estimate $\hat{B}_{IP}$ from the SPDF has to be *transformed* (see note) into e.g. a $\hat{B}_{L2}$ and checked against the available realm L2 bitrate capacity.

NOTE: It may be reminded that such a transformation (by the BGF) is not accurately possible in all cases. E.g. in case of media agnostic mode the BGF does not know the estimate for $\hat{\mu}_{PDU,IP}$, and could not derive correspondent information from the H.248 Media Descriptor. That is, the BGF has to take appropriate assumptions.

F.2 Traffic aspects

F.2.1 Quality of bitrate reservation

The *bitrate reservation* process is based on an *estimate* for the expected bitrate of a traffic flow, and that estimate is used for the BGF-level *Admission Control* (AC) functions, see figure F.1. The *quality* of that *bitrate reservation* process is dependent on, e.g.:

- the difference between the *estimated* and *real* "bitrate *value*" (e.g. estimated value $\hat{B}_{IP}$ according clause F.1.1.1 versus real value B_{IP} according clause F.1.1.2);
- the particular interpretation of the "bitrate *value*" as *traffic parameter* of the underlying distribution function (e.g. peak-rate, average-rate, equivalent-rate, sustainable-rate, etc.);
- *service*-specific bitrate control scenarios (see e.g. clause 4.1.2.2 in [i.7]); or
- the applied *admission control* algorithm scheme (see clause A.1 in [i.8]).

F.3 Examples

F.3.1 Examples for media-aware streams

F.3.1.1 Example for G.711

This example assumes a media-aware stream which consists of G.711, "a=ptime" equal to 20 ms and that VAD/CNG is not applied.

The MGC/SPDF will perform a bandwidth estimation for the signalled "b="-line L3 bitrate (RTP and RTCP) as follows:

Table F.1: L3 bandwidth estimate:

PDU Size (K) Parameters	**Value**
RTP payload (*ptime*=20 ms):	$K_{RTP-Payload} = K_{SDU,G.711,20\ ms} = 160$ byte
RTP header:	$K_{PCI,RTP} = 12$ byte
UDP header:	$K_{PCI,UDP} = 8$ byte
IP header:	$K_{PCI,IP} = 20$ byte
IP packet:	$K_{PDU,IP} = 200$ byte
Bitrate (B) Parameters	**Value**
IP bitrate (exclusive RTCP):	
RTCP overhead (5 %):	
IP bitrate:	

BGF transformation to L2 bitrate equivalent:

By means of provisioning the BGF knows the packetization time for each particular codec and could take the same assumption regarding RTCP traffic overhead (=> 5 %). Based on this knowledge the BGF could accurately transform the received L3 bandwidth into a L2 equivalent taking into account the characteristic of its local L2 interfaces.

- Case 1: Ethernet V2 header:
  - 30 byte (Preamble/8, DA/6, SA/6, 802.1pQ/4, Type/2, FCS/4).

- The BGF can calculate the IP PDU and add the L2 headers including the L2 Inter Packet Gap (for a 1 Gbit/s interface an IPG of 12 bytes is assumed). Thus the resulting L2 PDU has (200 + 30 + 12 =) 242 bytes:

Table F.2: L2 bandwidth estimate for Ethernet V2 header:

Bitrate (B) Parameters	Value
Layer 2 bitrate (exclusive RTCP):	
RTCP overhead (5 %):	
Layer 2 bitrate:	

In this case the resulting G.711 transformation **Factor** would be: 101,64/84 = 1,21.

- Case 2: Ethernet IEEE 802.3 [i.9] header (including VLAN tag):
    - 38 byte (Preamble/8, DA/6, SA/6, 802.1pQ/4, Length/2 LLC/SNAP/8, FCS/4).
    - The BGF can calculate the IP PDU and add the L2 headers including the L2 Inter Packet Gap (for a 1 Gbit/s interface an IPG of 12 bytes is assumed). Thus the resulting L2 PDU has (200 + 38 + 12 =) 250 bytes:

Table F.3: L2 bandwidth estimate for Ethernet IEEE 802.3 header:

Bitrate (B) Parameters	Value
Layer 2 bitrate (exclusive RTCP):	
RTCP overhead (5 %):	
Layer 2 bitrate:	

In this case the resulting G.711 transformation **Factor** would be: 105/84 = 1,25.

F.3.2 Examples for media-agnostic streams

As pointed out in clause F.1.5 the BGF has to make assumptions in case of media agnostic streams.

Example: In this example the following assumptions are taken regarding codec, packetization time and RTCP overhead applicable to all streams.

Codec:	G.711;
packetization time:	10 ms;
RTCP overhead:	5 %.

Knowing its L2 interfaces the MG can derive a generic transformation factor, which is applied to all streams and the particular received b-line values.

The factor is to be calculated taking into account the known characteristic of the particular L2 interface (V2 or IEEE 802.3 [i.9]; VLAN present or not).

For instance: G.711 with 10 ms, 5 % RTCP on a V2 formatted, untagged L2 interface.

Table F.4: L3 bandwidth estimate

PDU Size (K) Parameters	Value
RTP payload (*ptime*=10 ms):	$K_{RTP-Payload} = K_{SDU,G.711,10ms} = 80$ byte
RTP header:	$K_{PCI,RTP} = 12$ byte
UDP header:	$K_{PCI,UDP} = 8$ byte
IP header:	$K_{PCI,IP} = 20$ byte
IP packet:	$K_{PDU,IP} = 120$ byte
Bitrate (B) Parameters	**Value**
IP bitrate (exclusive RTCP):	$B_{IP,RTP\ only} = 96{,}00$ kbit/s
RTCP overhead (5 %):	$B_{IP,RTCP\ only} = 5\%\ B_{IP,RTP\ only} = 4{,}80$ kbit/s
IP bitrate:	$B_{IP} = 100{,}80$ kbit/s

L2 bandwidth estimate:

Table F.5: L2 bandwidth estimate:

PDU Size (K) Parameters	Value
IP packet:	$K_{PDU,IP} = 120$ byte
Layer 2 header:	$K_{PCI,L2} = 30$ byte
Inter-Packet Gap:	$K_{IPG} = 12$ byte
Layer 2 packet:	$K_{PDU,L2} = 162$ byte
Bitrate (B) Parameters	**Value**
Layer 2 bitrate (exclusive RTCP):	$B_{L2,RTP\ only} = 129{,}60$ kbit/s
RTCP overhead (5 %):	$B_{L2,RTCP\ only} = 5\ \%B_{L2,RTP\ only} = 6{,}48$ kbit/s
Layer 2 bitrate:	$B_{L2} = 136{,}08$ kbit/s

Resulting transformation Factor = 136,08/100,8 = 1,35.

Annex G: Illustration of BGF modes of operation

The mode of operation of the BGF relates to the IP-to-IP interworking mode (see clause 3.1 of [i.3]) as configured (via H.248 signalling) for a particular H.248 (IP, IP) Context. Supported modes of operation depending primarily on the supported SDP information elements (by the profile; see clauses 5.15 and 5.16 in [i.3]). The number of BGF modes did consequently evolve over the various versions of the Ia profile specification due to correspondent SDP extensions in each profile version. Terminology was needed (and thus introduced by Ia version 2 in clause 3.1 of [i.2]) in order to distinguish the several modes.

The purpose of this annex is to explain the underlying principle in more detail concerning that terminology.

G.1 Major SDP Information Elements for Media/Bearer/Resource Control in the BGF

There are separate SDP specifications for *ingress* traffic (provided by the H.248 LD) and *egress* traffic (provided by the H.248 RD). The (SDP) *media description* within that SDP block provides the BGF mode determining information (see figure G.1).

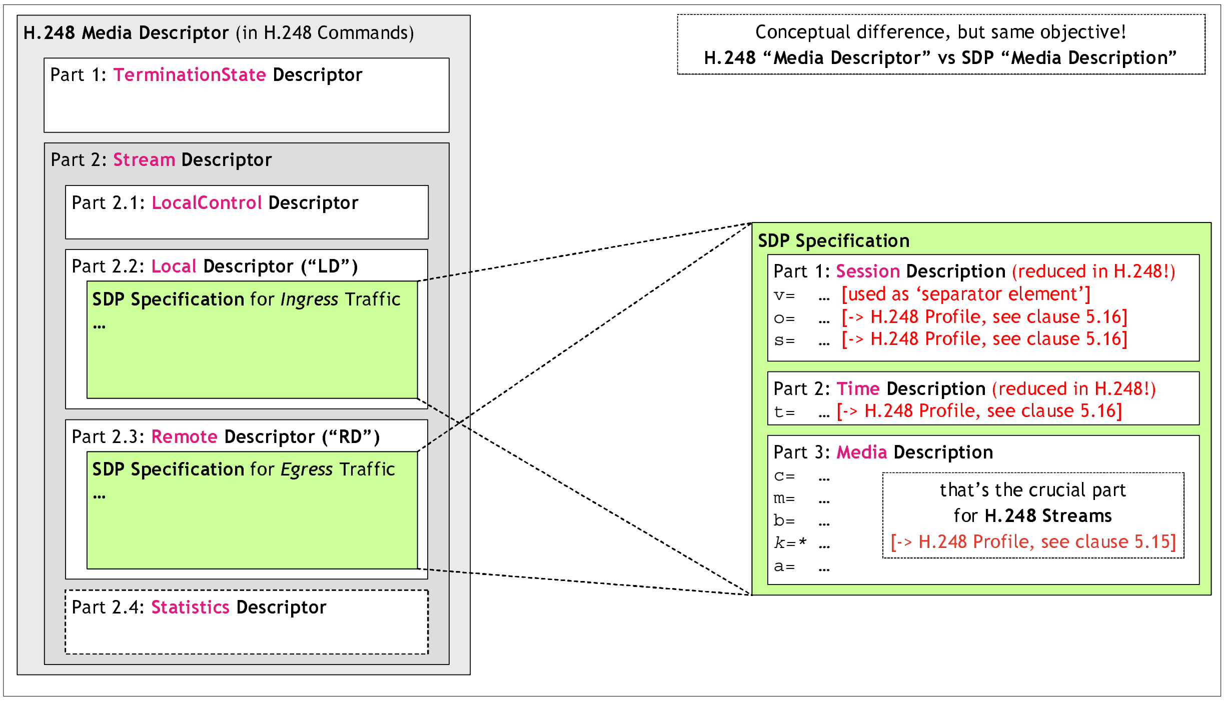

H.248 Media Descriptor (in H.248 Commands)
Part 1: TerminationState Descriptor
Part 2: Stream Descriptor
Part 2.1: LocalControl Descriptor
Part 2.2: Local Descriptor ("LD")
SDP Specification for Ingress Traffic
…
Part 2.3: Remote Descriptor ("RD")
SDP Specification for Egress Traffic
…
Part 2.4: Statistics Descriptor
Conceptual difference, but same objective!
H.248 "Media Descriptor" vs SDP "Media Description"
SDP Specification
Part 1: Session Description (reduced in H.248!)
v= … [used as 'separator element']
o= … [-> H.248 Profile, see clause 5.16]
s= … [-> H.248 Profile, see clause 5.16]
Part 2: Time Description (reduced in H.248!)
t= … [-> H.248 Profile, see clause 5.16]
Part 3: Media Description
c= …
m= …
b= …
k=* …
a= …
that's the crucial part
for H.248 Streams
[-> H.248 Profile, see clause 5.15]

Figure G.1: BGF modes - Overview Structure of H.248 Media Descriptor (H.248 "Media Descriptor" vs SDP "Media Description")

NOTE: H.248.1 may provide in future that general information on H.248 "Media Descriptor" vs SDP "Media Description". The information of this clause may be then replaced by a reference to H.248.1.

G.1.1 Example

Figure G.2 provides an example of an (SDP) media description for a BGF H.248 *IP Stream* with PCM wideband media over an IPv6 bearer:

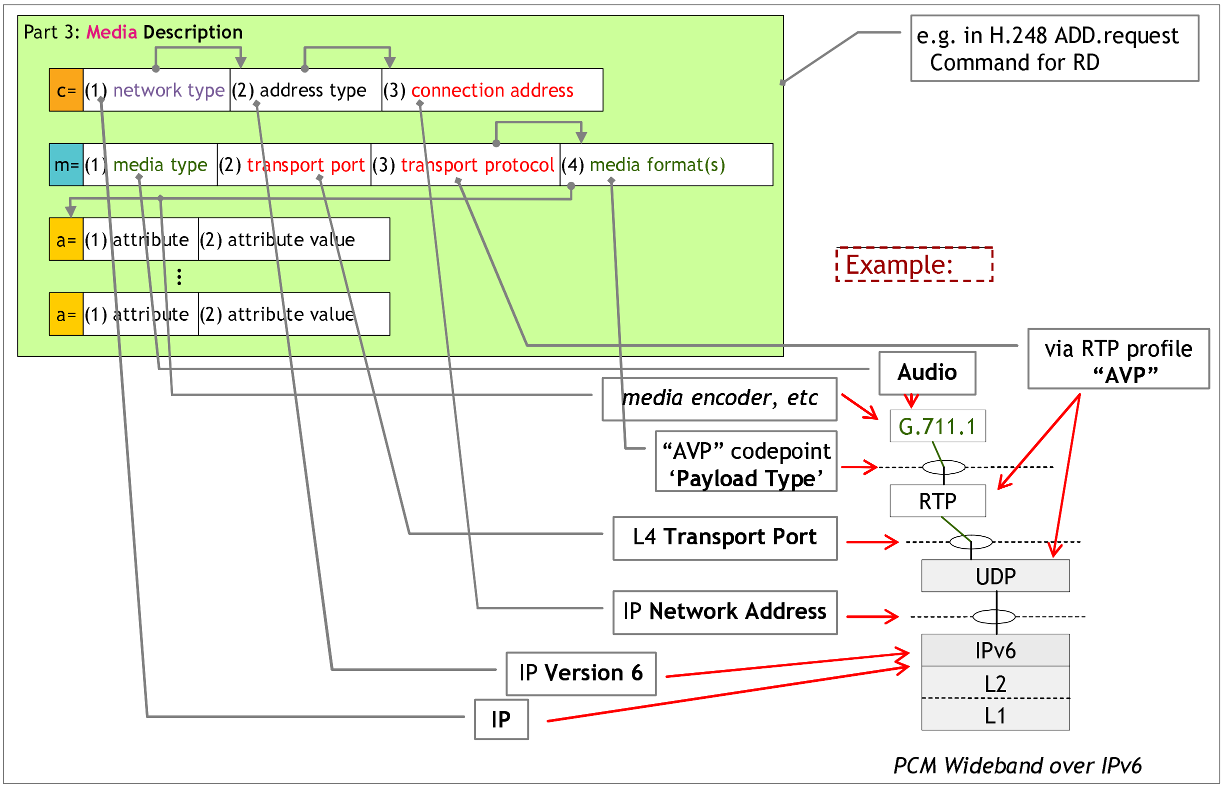


Figure G.2: BGF mode determined by SDP "Media Description" - Example of G.711.1-over-IPv6

The (SDP) *media description* contains primarily single "c=" and "m=" lines, and multiple, optional "a=" lines. The example in figure G.2 may lead to a "*media-aware*" mode in the BGF.

G.2 BGF modes driven by particular SDP lines

The SDP "c=" and "m=" lines determining the BGF mode of operation. There are many combinations possible because H.248 and this profile permits the *full* specification, *over* specification, *wildcarding* (*under* specification) and "cancelling" (by using a "-" character) of some field elements in these lines.

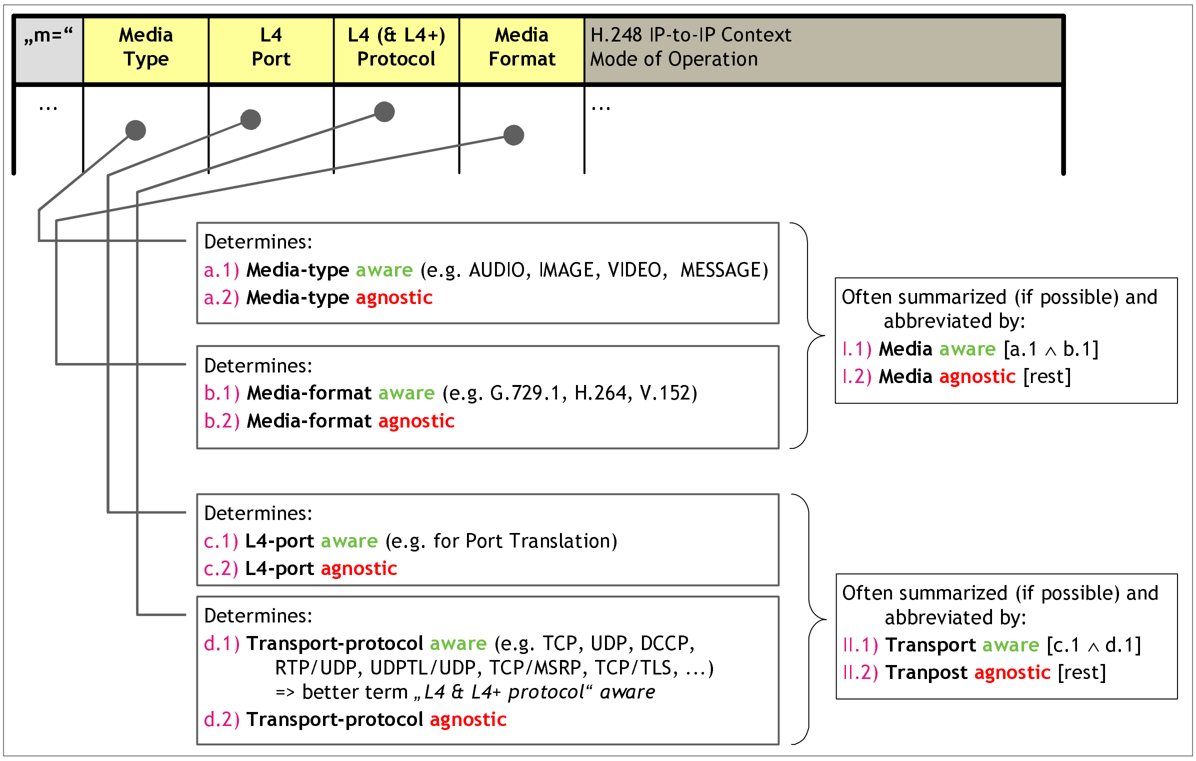
G.2.1 SDP "c=" line

Supported SDP protocol values are defined by table 85 in clause 5.15 of [i.3]. The "c=" line determines essentially the BGF mode with regards to:

- back-to-back IP host (B2BIH) mode, which implies *network address translation* (NAT);
- B2BIH with additional *protocol translation* for V4-to-V6 interworking (i.e. NAT-PT B2BIH); or
- IP router (IPR) mode, i.e. a *NAT-less* IP forwarding function.

G.2.2 SDP "m=" line

The "m=" consists of *four* field elements. Supported SDP protocol values are defined by table 85 in clause 5.15of [i.3]. The "m=" line determines essentially the BGF modes according the mode definitions of clause 3.1 of [i.3]. Figure G.3 provides a summary and some more detailed terminology.



Determines:
a.1) Media-type aware (e.g. AUDIO, IMAGE, VIDEO, MESSAGE)
a.2) Media-type agnostic

Determines:
b.1) Media-format aware (e.g. G.729.1, H.264, V.152)
b.2) Media-format agnostic

Often summarized (if possible) and abbreviated by:
I.1) Media aware [a.1 ∧ b.1]
I.2) Media agnostic [rest]

Determines:
c.1) L4-port aware (e.g. for Port Translation)
c.2) L4-port agnostic

Determines:
d.1) Transport-protocol aware (e.g. TCP, UDP, DCCP, RTP/UDP, UDPTL/UDP, TCP/MSRP, TCP/TLS, ...)
=> better term „*L4 & L4+ protocol*" *aware*
d.2) Transport-protocol agnostic

Often summarized (if possible) and abbreviated by:
II.1) Transport aware [c.1 ∧ d.1]
II.2) Tranpost agnostic [rest]

Figure G.3: BGF modes - H.248 Local and Remote Descriptor: SDP "m="-line specification combinations

This profile version is supporting some out of theoretically 16 BGF modes (due to "m=" line specifications).

G.3 BGF modes driven by configuration management

G.3.1 Media-related modes

The *media aware* mode implies awareness of the *media type* **and** the *media format* (see clause G.2.2). The *media agnostic* mode is given by *media-type agnostic* mode, or *media-format agnostic* mode or both.

G.3.2 Transport-related modes

The *transport aware* mode implies awareness of the *L4 port* **and** the *transport protocol* (see clause G.2.2). The *transport agnostic* mode is given by *L4-port agnostic* mode, or *transport-protocol agnostic* mode or both.

A transport aware MG could or could not support transport protocol agnostic behaviour. It is up to implementation and/or configuration to support transport protocol aware and agnostic behaviours. The MGC could know about the type of support provided by MG (transport protocol aware, transport protocol agnostic or both) through mechanisms which are outside the scope of the present document.

Annex H:
Illustration of NAPT modes of operation

The BGF could provide an embedded NAPT function, which is controlled according clauses 5.17.1.1 and 5.17.1.2 of [i.3]. There are several NA(P)T types known in networks and deployed. H.248 itself and in addition some capabilities of the *gate management* package version 1 provide an extensive tool for controlling various The purpose of this annex is to assist implementers in NA(P)T understanding by illustrating some example use cases. The annex is organized as follows:

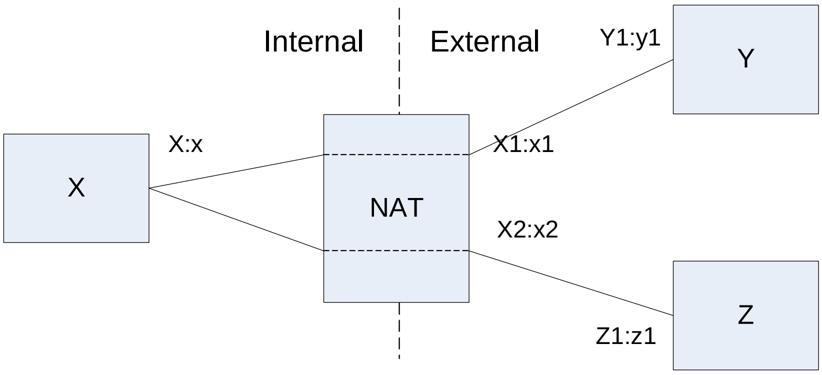
- overview of remote and local NA(P)T types (clause H.1);
- BGF "NA(P)T-full" modes (clause H.2); and
- BGF "NA(P)T-less" modes (clause H.3).

H.1 NAPT types

There might be *remote* NA(P)T devices (from BGF perspective) besides a *local*, BGF provided NA(P)T function, in the end-to-end IP media path.

H.1.1 Remote NA(P)T devices

Behaviour of NAT devices and NA(P)T types with regards to address mapping are defined in clause 4.3.1 in TR 187 008 [i.10]. The address mapping behaviour is described in table H.1 with respect to the configuration given in figure H.1.



X = Host X
X.x = Internal Address:Port tuple of host X
Xn:xn = External Address:port tuple presented by NAT for host X
Y, Z = Hosts that host X is communicating with
Yn:yn = Address:port tuple visible to the NAT for host Y
Zn:zn = Address:port tuple visible to the NAT for host Z

Figure H.1 (Copy of figure 2 from [i.10]): Types of NATs (Address Mapping) - The "NAT function" is provided by the BGF in the present document

In figure H.1, address X:x inside the NAT is translated to address X1:x1 when communicating with host Y outside the NAT. The same address X:x translates to X2:x2 when communicating with Y2:y2.

Table H.1 (Copy of Tab. 1 from [i.10]): Types of NATs (Address Mapping)

Type of NAT	Mapping Description
Endpoint Independent Mapping	X1:x1 always equals X2:x2
Address Dependent mapping	X1:x1 equals X2:x2 only if Y1 equals Z1
Address and Port Dependent Mapping	X1:x1 equals X2:x2 only if Y1:y1 equals Z1:z1
NOTE: For small NATs (e.g. residential NATs), a single public IP address is normally assigned as the external IP address (i.e. X1 = X2). However, larger NATs will assign the external IP address from a pool of available IP addresses.	

H.1.2 MG-local NA(P)T function

It may be concluded that a BGF (MG) provided NA(P)T function may provide all above three NAT types. This is dependent on SPDF (MGC) control and transparent for the BGF (MG) due to the H.248 Context concept ("MGC-strict control of NA(P)T function").

H.2 NAPT-full modes

This annex is just considering the example of NAPT, i.e. *both* network *address* and transport *port* are translated, and not the sub-scenarios of NAT or port translation only.

NAPT could be applied for *both traffic directions* (called "*bidirectional*" NAPT in the present document) or only for *one direction* (called "*unidirectional*" NAPT). The BGF is further supporting the two categories concerning the Local Source transport address: *with* or *without explicit* Local Source network address and/or transport port settings.

NOTE 1: It may be noted that "bidirectional NA(P)T" (aka "two-way NA(P)T") in RFC 2663 has a different meaning: session may be initiated from *both* sides of the NA(P)T device.

The *remote* IP nodes could furthermore use *asymmetrical* or *symmetrical* network addresses. The symmetry condition holds e.g. in case of single-homed IP hosts or remote NAT devices, and remote multi-homed IP hosts *could* lead to asymmetry.

NOTE 2: There is not any requirement for *symmetrical local* network addresses in H.248. The MG could thus assign different values for LS(A) and LD(A). The MGC could enforce symmetry by explicitly setting LS(A) with the same value as the MG-assigned value for LD(A).

The shown examples are related to clause 5.17.1.2 of [i.3], see also figure 3 in [i.3] with regards to the IP-to-IP Context model and transport address value examples for the H.248 LDs and RDs.

H.2.1 General case: non-symmetrical remote network addresses

Conventions: All following figures are using a colour code. Any changing colour in IP packet flow direction is indicating a translation function of the correspondent PCI (i.e. network address, and transport port). The white colour means that this information is not influenced by H.248 descriptors. The associated IP endpoints of the two traffic directions have the same colour in case of address symmetry, or a different colour in case of asymmetry.

H.2.1.1 "Double" NAPT mode *without* explicit Local Source settings

Figure H.2 illustrates such a scenario, the LCD is *not* providing explicit Local Source (LS) settings. This is a very usual BGF scenario, and actually reflecting the standard case for all other profiles not using these *gm* package properties.

NOTE: Properties *gm/esas*, *gm/lsa*, *gm/esps* and *gm/lsp*; see also clause 5.14.2.5.

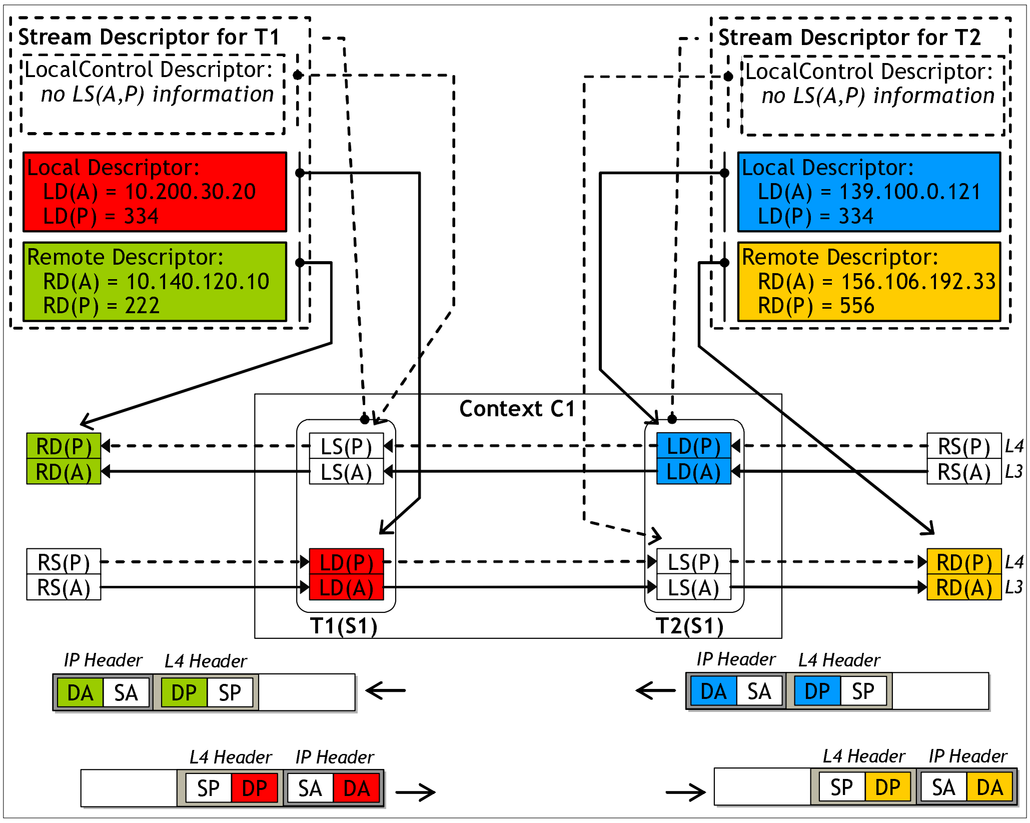


Figure H.2: NAPT modes by BGF - "Double" NAPT mode *without* Local Source settings - Non-symmetrical Remote Network Addresses

The *Local Source* transport addresses, - LS(A) and LS(P) -, are solely allocated by the BGF (MG) because the SPDF (MGC) is *not* using the correspondent *gm* package properties for explicit LS settings. There is thus implicitly a "source-double" NAPT (due to H.248 B2BIH Context type), besides the "destination-double" NAPT due to *gm* package capabilities.

The *Remote Source* transport addresses, - RS(A) and RS(P) -, are *unknown* to the BGF (MG) due to the *asymmetry* assumption here (RS(A) ≠ RD(A); RS(P) ≠ RD(P)). They remain unknown as long as *latching* is not enforced.

NOTE 1: "latching" will lead to "*symmetrical remote* network addresses", see clause H.2.2.1).

NOTE 2: It may be noted that policing of *remote source* transport addresses could lead to additional information with regards to RS values.

H.2.1.2 "Double" NAPT mode *with* explicit Local Source settings

Figure H.3 illustrates such a scenario.

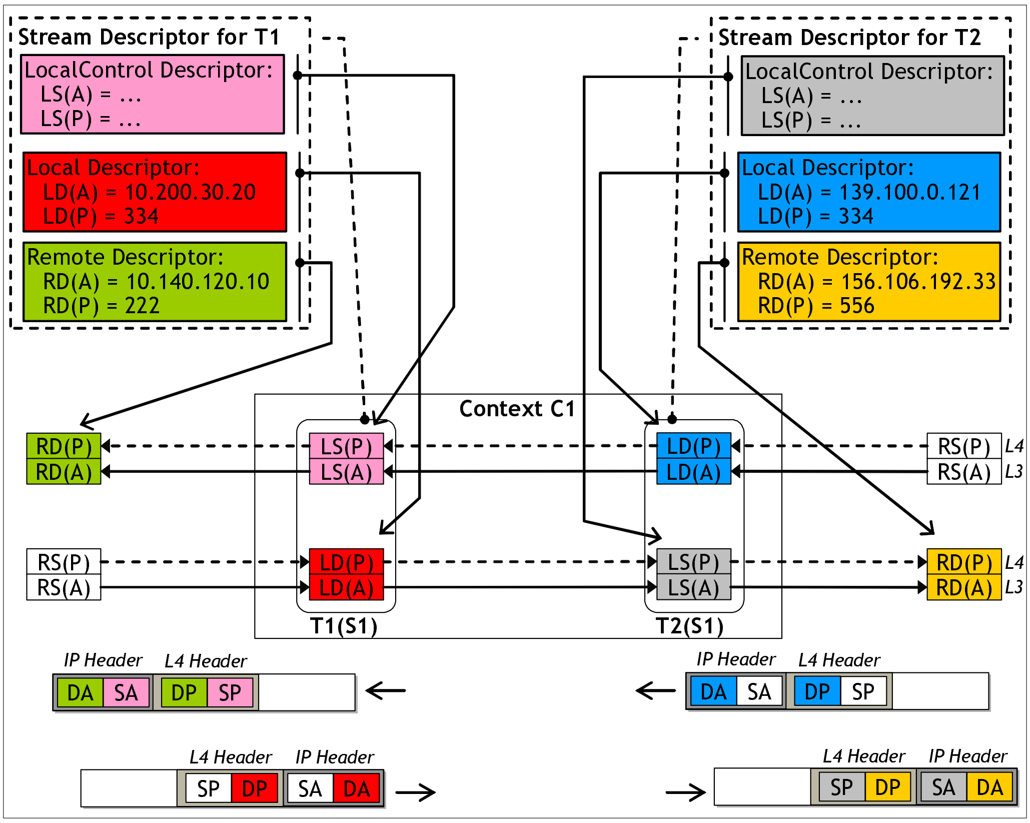


Figure H.3: NAPT modes by BGF - "Double" NAPT mode with explicit setting of Local Source Transport Address LS(A,P) in both directions - Non-symmetrical Remote Network Addresses

The *Local Source* transport addresses, - LS(A) and LS(P) for both directions -, are here *explicitly allocated* by the SPDF (MGC), using the correspondent *gm* package properties for explicit LS settings.

The *Remote Source* transport addresses, - RS(A) and RS(P) -, are still *unknown* to the BGF (MG) due to the *asymmetry* assumption here (RS(A) ≠ RD(A); RS(P) ≠ RD(P)). They remain unknown as long as *latching* is not enforced (note: "latching" will lead to "*symmetrical remote* network addresses", see clause H.2.2.1). The *Remote Source* transport addresses are over-written by the BGF (MG) by the explicitly controlled *Local Source* transport addresses. It may be noted that the ***actual*** *Local Source* transport addresses *used by the BGF* (MG) could be *different* with the ***inserted*** *Local Source* transport address values in the *outgoing IP packets*.

H.2.2 Special case: symmetrical remote network addresses

It may be noted that symmetrical *remote* network addresses does not imply any symmetry condition for BGF (MG) *local* network addresses.

H.2.2.1 "Double" NAPT mode *without* explicit Local Source settings

Figure H.4 illustrates such a scenario, the LCD is *not* providing explicit Local Source (LS) settings.

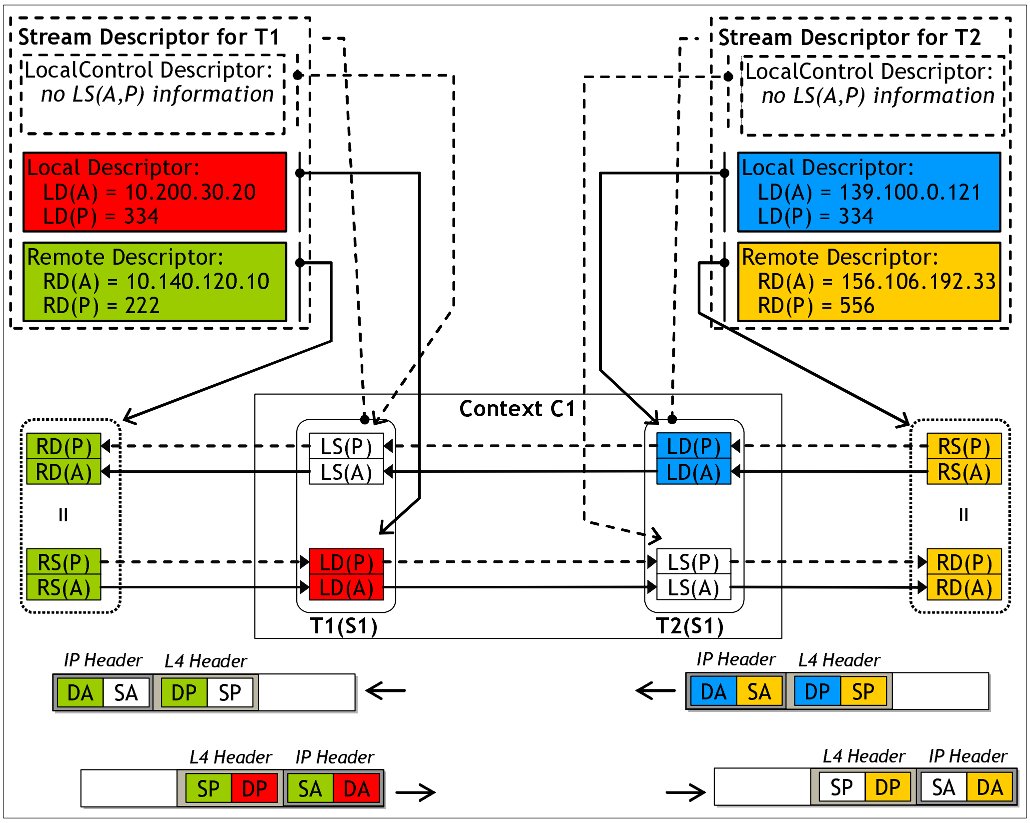

Stream Descriptor for T1
LocalControl Descriptor: no LS(A,P) information
Local Descriptor: LD(A) = 10.200.30.20 LD(P) = 334
Remote Descriptor: RD(A) = 10.140.120.10 RD(P) = 222
Stream Descriptor for T2
LocalControl Descriptor: no LS(A,P) information
Local Descriptor: LD(A) = 139.100.0.121 LD(P) = 334
Remote Descriptor: RD(A) = 156.106.192.33 RD(P) = 556
Context C1
RD(P)
RD(A)
II
RS(P)
RS(A)
LS(P)
LS(A)
LD(P)
LD(A)
T1(S1)
LD(P)
LD(A)
LS(P)
LS(A)
T2(S1)
RS(P)
RS(A)
II
RD(P)
RD(A)
IP Header
L4 Header
DA SA DP SP
L4 Header
IP Header
SP DP SA DA

Figure H.4: NAPT modes by BGF - "Double" NAPT mode *without* Local Source settings - Condition of symmetrical Remote Network Addresses

The *Local Source* transport addresses, - LS(A) and LS(P) -, are again solely allocated by the BGF (MG) because the SPDF (MGC) is *not* using the correspondent *gm* package properties for explicit LS settings.

The *Remote Source* transport addresses, - RS(A) and RS(P) -, are supposed to be equal to the *Remote Destination* transport addresses, - RD(A) and RD(P) -, by the BGF (MG) due to *symmetry* assumption here (RS(A) = RD(A); RS(P) = RD(P)). The symmetry condition is always given in case of NAT Traversal support by the BGF (MG) via latching, see also [Assumption 2 "*Symmetry assumption for remote address A2*"] in clause 1.1 of H.248.37.

This scenario is supported by profile [i.3], see table 1 on *Remote Source* transport address allocation in clause 5.17.1.1 of [i.3].

H.2.2.2 "Double" NAPT mode *with* explicit Local Source settings

Figure H.5 exemplifies such a scenario, which represents a combination of clauses H.2.2.1 and H.2.1.2.

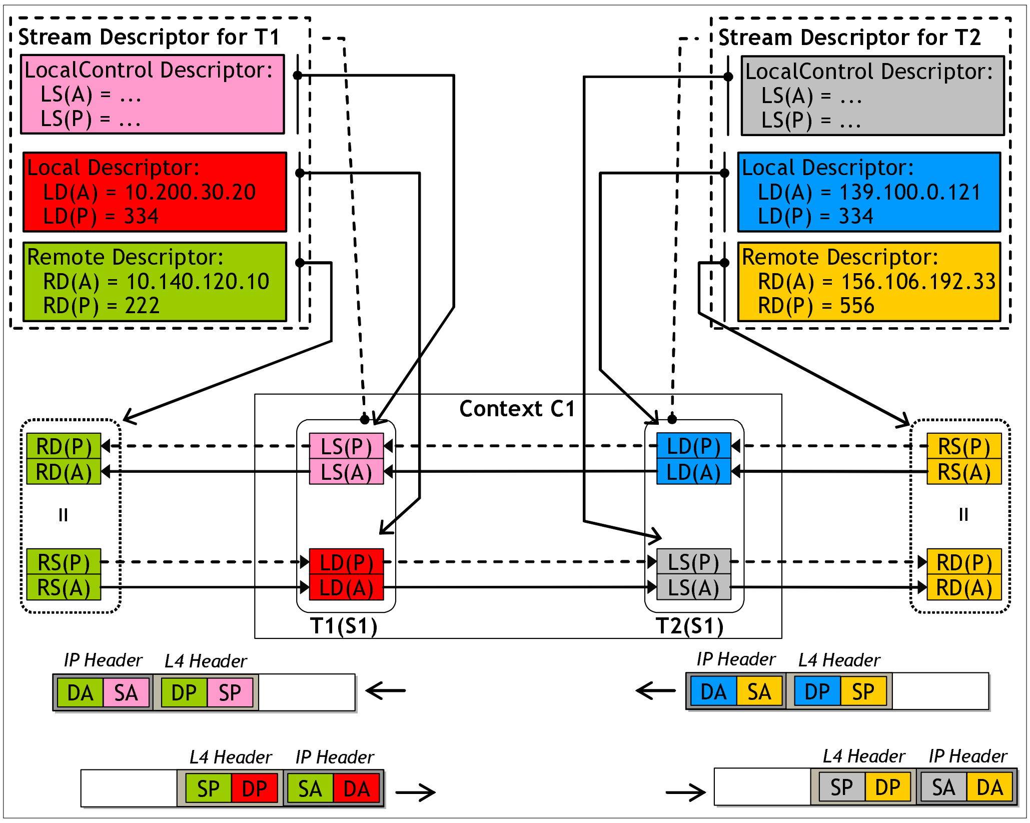


Figure H.5: NAPT modes by BGF - "Double" NAPT mode with explicit setting of Local Source Transport Address LS(A,P) in both directions - Condition of symmetrical Remote Network Addresses

The *Local Source* transport address, - LS(A) and LS(P) -, and the correspondent *Local Destination* transport address, - LD(A) and LD(P) -, could be different, i.e. asymmetrical.

H.3 NAPT-less

NOTE: This clause is considering the case of *both* network address and transport port *translation-less behaviour*.

H.3.1 Definition

The NAPT-less handling implies that neither the *destination* nor *source* network address and transport port values of an *incoming* IP packet will be changed by the BGF (MG). These IP and L4 header fields, i.e. the *4-tuple* of {DA, SA, DP, SP}, *remains unchanged* in the *outgoing* IP packet. The BGF (MG) behave in the NAPT-less mode then as usual "next hop" node (as opposed to the Back-to-Back IP Host (B2BIH) mode), according the native IP forwarding function as defined by RFC 1812 [i.17].

H.3.2 BGF (MG) behaviour for NAPT-less

This clause recalls again the basic requirements for a BGF (MG) in NAPT-less mode.

H.3.2.1 Handling of *source* transport address values {SA, SP}

The SA and SP values of an outgoing IP packet will be identical to the 2-tuple of the received IP packet. This implies that the SPDF (MGC) will *not* use the correspondent *gm* package properties for explicit LS settings. The BGF (MG) will also not insert the *local source* transport address values in the outgoing IP packet.

H.3.2.2 Handling of *destination* transport address values {DA, DP}

The DA and DP values of an outgoing IP packet will be identical to the 2-tuple of the received IP packet. The BGF (MG) will thus not overwrite the *local destination* transport address values, as received by the incoming IP packet, in the outgoing IP packet.

H.3.3 Control methods of NAPT-less mode

There are several options in how a SPDF (MGC) could indicate the NAPT-less mode to the BGF (MG).

H.3.3.1 Method 1: mirrored H.248 LD and RD between the two H.248 IP terminations (stream endpoints)

The SPDF (MGC) signals the *same transport address* in the LD of termination T1 (T2) as used for the RD of termination T2 (T1). This implies a couple of conditions:

- usage of H.248 *full specification method* for these resources, i.e. *wildcarding* in the LD is *not* allowed;
- availability of RD information *when* LD is signalled; and
- BGF (MG) compares correspondent RD and LD values in order to conclude NAPT-less mode.

This *implicit* method is supported by profile [i.3], see clause 5.17.1.2 of [i.3].

H.3.3.2 Method 2: omitted address information in H.248 LD and RD

The *network address* value could be carried by the SDP "c=" line, the *transport port* value in the "m=" line. Both values could be basically omitted by using a "-" character. This *explicit* method is *not supported* by present Ia profile versions (because this H.248 profiles are not allowing the "-" for the correspondent field elements in these SDP lines; see clause 5.15 of [i.3]).

H.3.3.3 Method 3: explicit indication via H.248 Context Attribute

The NAPT-less mode relates to the "IP router mode" (IPR) of an H.248 IP-to-IP Context which could be explicitly indicated by using property *ipr/ifm* according Draft H.248.64. This *explicit* method is *not supported* by present Ia profile versions (because this H.248 package is not supported by this profile).

H.3.4 NAPT-less examples

H.3.4.1 "Double" NAPT-less mode, controlled via method 1

Figure H.6 illustrates such a scenario of mirrored H.248 LD and RD transport address values.

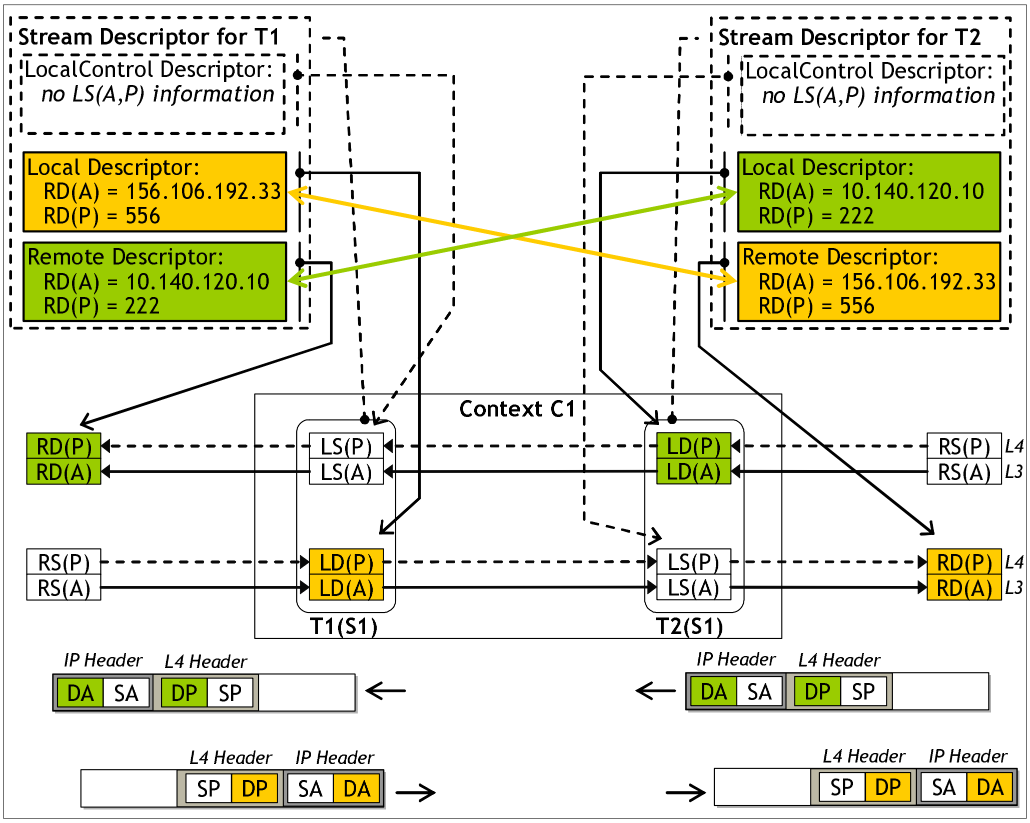


Figure H.6: NAPT modes by BGF - "Double" NAPT-less mode, controlled via method 1 - Non-symmetrical Remote Network Addresses

H.4 Mixed NA(P)T-full/NA(P)T-less modes

This examples provides further examples with scope on mixed NA(P)T modes. Purpose of this clause is the indication of further feasible modes, but also to point out the limitations of this profile version.

H.4.1 Example of combination of Double-NAPT and NAPT-less

Figure H.7 illustrates a hybrid scenario with following NA(P)T behaviour:

Direction	Source information	Destination information
X-to-Y	NAPT-less	NAPT-less
Y-to-X	NAPT-full	NAPT-less

There is not any NAPT for destination information, in both traffic directions.

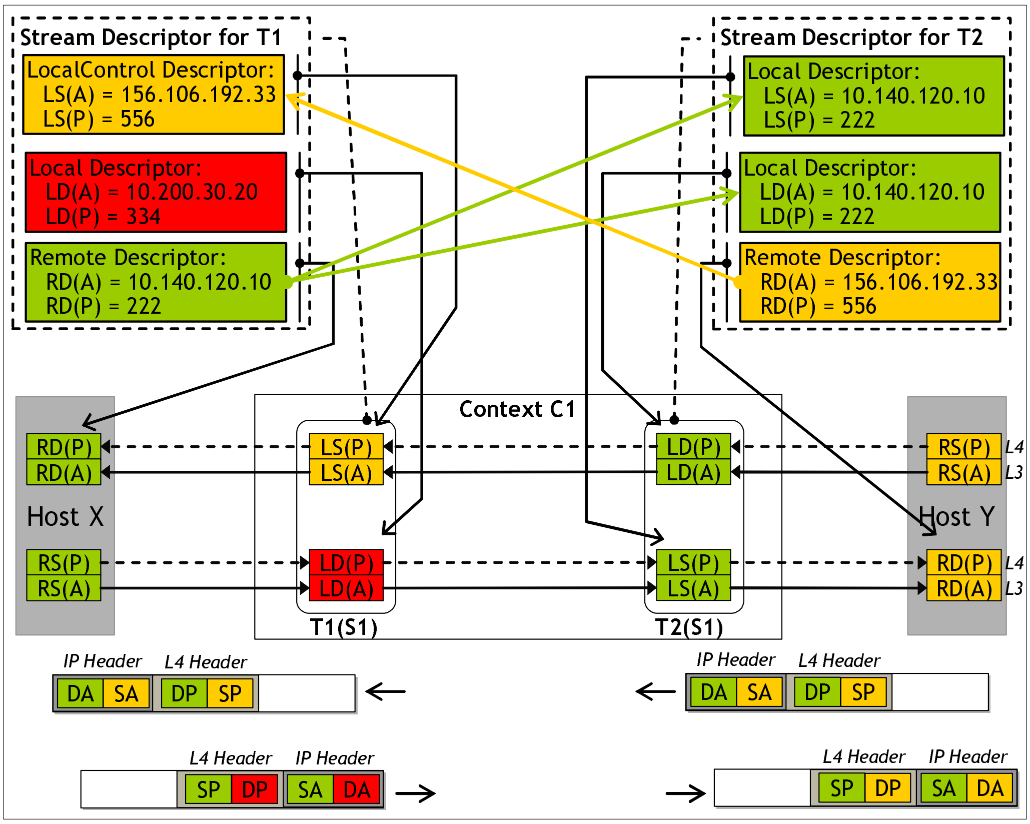


Figure H.7: NAPT modes by BGF - Example of combination of Double-NAPT and NAPT-less

Control aspects of the NAPT-less paths:

- the "destination *NAPT-less*" behaviour (X-to-Y direction) could be controlled via mirrored LD/RD values ("method 1");
- the "source *NAPT-less*" behaviour (Y-to-X direction) could be controlled via explicit Local Source settings, using an LS(A,P) value according the RD(A,P) of host Y; and
- a "destination *NAPT-less*" behaviour (Y-to-X direction) via mirrored LD/RD values ("method 1").

The feasibility of this scenario is due to following condition:

- assumption of single-homed IP peer nodes, i.e. condition of "RS(A,P) = RD(A,P)" for both hosts X and Y.

H.4.2 Profile limitations

The hybrid NA(P)T modes could be not controlled in case of dual-/multi-homed IP peer nodes, i.e. source and/or destination host entities with different IP interfaces per traffic direction, i.e. "RS(A,P) ≠ RD(A,P)".

Annex I:
Illustration of "Protocol Layer Lx"-based Packet Processing BGF modes

The mode of operation of the BGF relates to the IP-to-IP interworking mode (see clause 3.1/ [i.3]) as configured (via H.248 signalling) for a particular H.248 (IP, IP) Context (see annex G). The BGF mode is tightly coupled to the set of enforced policy rules. A particular policy rule is typically related to a specific protocol layer. Table I.1 provides some examples for protocol layer dependent policy rules.

Purpose of this annex is to illustrate:

- the basic H.248 control framework for policy control;
- example BGF modes of operation in more detail;
- example H.248 encoding for some selected BGF modes; and
- the identification of supported and not (yet) supported BGF modes.

Table I.1: Protocol layer dependent Policy Rules (Examples)

Handling options of IP media flows [= Set of Policy Rules (Conditions and Actions) for Policy Enforcement]	**Protocol Layer**	**Applicability to profile version 3 [i.3]**
L2-VPN indication and marking	L2	Yes
MPLS LSP indication and marking	L2+	Yes
NAT	L3	Yes: B2BIH mode No: IPR mode
NAPT	L4	Yes: B2BIH mode No: IPR mode
IP Protocol (Version) Translation	L3	Yes
Traffic (byterate) Policing of ingress traffic	L3	Yes
Traffic (byterate) Shaping of egress traffic	L3	No
QoS (ToS, DSCP, TC) Pre-marking	L3	Yes
Policing of Remote Source Transport Addresses	L3/L4	Yes
Policing of (Local) Destination Transport Addresses (in IPR mode)	L3/L4	Yes
Policing of (IP Transport) Protocol Type	L3	Yes
Policing of (IP Application) Protocol Type	L4+	Yes
(IP Application) Data Inactivity Detection	L4	Yes
RTCP packet policing	L4+	Yes (partially)
RTCP report generation	L4+ … L7	Yes (partially)
Media format conversion (e.g. audio transcoding)	L7	Yes

Policy enforcement (session-dependent or session-independent) could be complemented by measurements of QoS, GoS, capacity, load or performance related metrics, and the generation and reporting of correspondent statistics. Such a measurement is either explicitly subject of a particular policy rule (as a policy action), or generally associated to a traffic flow. Table I.2 provides some examples (see also annex J).

Table I.2: Protocol layer dependent measurements, statistics generation and reporting (Examples)

Metric	Protocol Layer	Applicability to this profile
Stream holding time	-	Yes (via *nt/dur*)
L2 traffic volume	L2	No
IP traffic volume	L3	Yes (*ipocs* package)
L4 traffic volume	L4	Yes (via nt and *rtp* packages)
L7 traffic volume	L7	Partially yes, just for RTP-based applications (*rtpad* package)
Discarded IP packets due to IP byterate policing	L3	Yes
Discarded IP packets due to IP packet size policing	L3	No
Discarded IP packets due to network address filtering	L3	Yes
Discarded IP packets due to transport address filtering	L4	Yes
RTP packet delay variation, delay, etc.	L4+	Yes
RTCP XR/HR based RTP metrics	L3 … L7	No

I.1 BGF modes - Technological Framework

The Ia *Border Gateway Function* (BGF) is provided by an H.248 *Media Gateway* (MG) entity. The H.248 *bearer-path* is therefore synonym to the IP *media-path* (also known as IP *data-path*): the BGF could be enforced for various modes of operations ("BGF modes"), dependent on the overall set of enforced policy rules per H.248 Stream/Termination/Context.

A particular BGF mode could be limited to a specific protocol layer, but covers typically multiple layers (e.g. L4/L3 in case of NAPT). Common to all BGF modes is the processing of L3 (IP) layer. There are BGF modes up to the application layer (viz. L7-to-L3) in case of "media awareness". But there are also BGF modes down to L2.5 or L2, e.g. in case of usage of H.248 packages *mpls* or *vlan*.

The BGF could consequently behave as, e.g.:

- L2 (VPN) switch function;
- MPLS LSP switch or edge router function;
- native or service-enhanced IP router function;
- L4 transport connection switch function;
- back-to-back IP host function;
- media format conversion function (e.g. "transcoder", "transrater", "transpacker"); or
- Media Application lLevel Gateway (MALG) function.

complemented by:

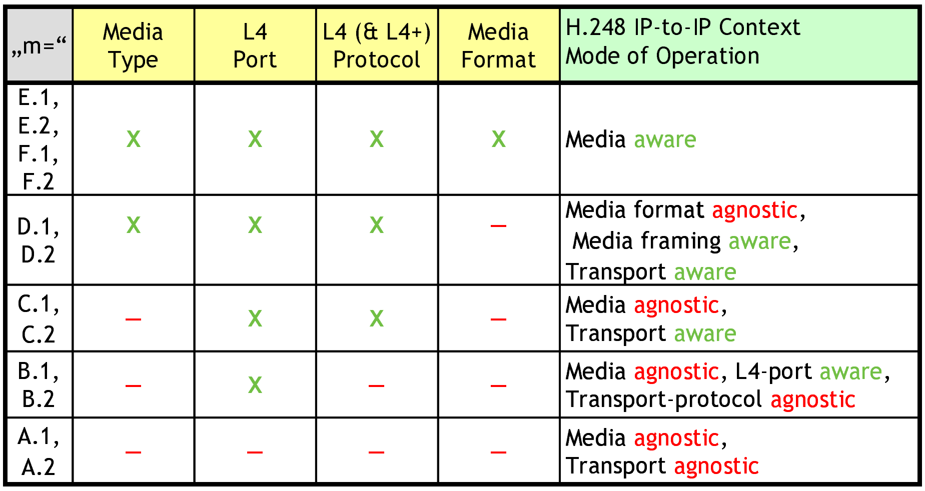
- security-specific policy rules (e.g. due to session-dependent or/and session-independent policing on various protocol layers).

It is self-evident that the aimed BGF mode requires an unambiguous policy control "command" ("which relates to the pushed (or pulled) policy rules").

Purpose of this annex is to summarize the major BGF modes, complemented by example H.248 Stream Descriptor settings.

I.2 BGF modes - Control Framework

The "m=" line is the prime BGF mode determining SDP line. Clause G.2.2 outlines 16 possible BGF mode combinations due to SDP "m=" line signalling. The basic control framework (from policy decision point) could be derived by considering the simplified model of just 4-out-of-16 "m=" line modes, see figure I.1.



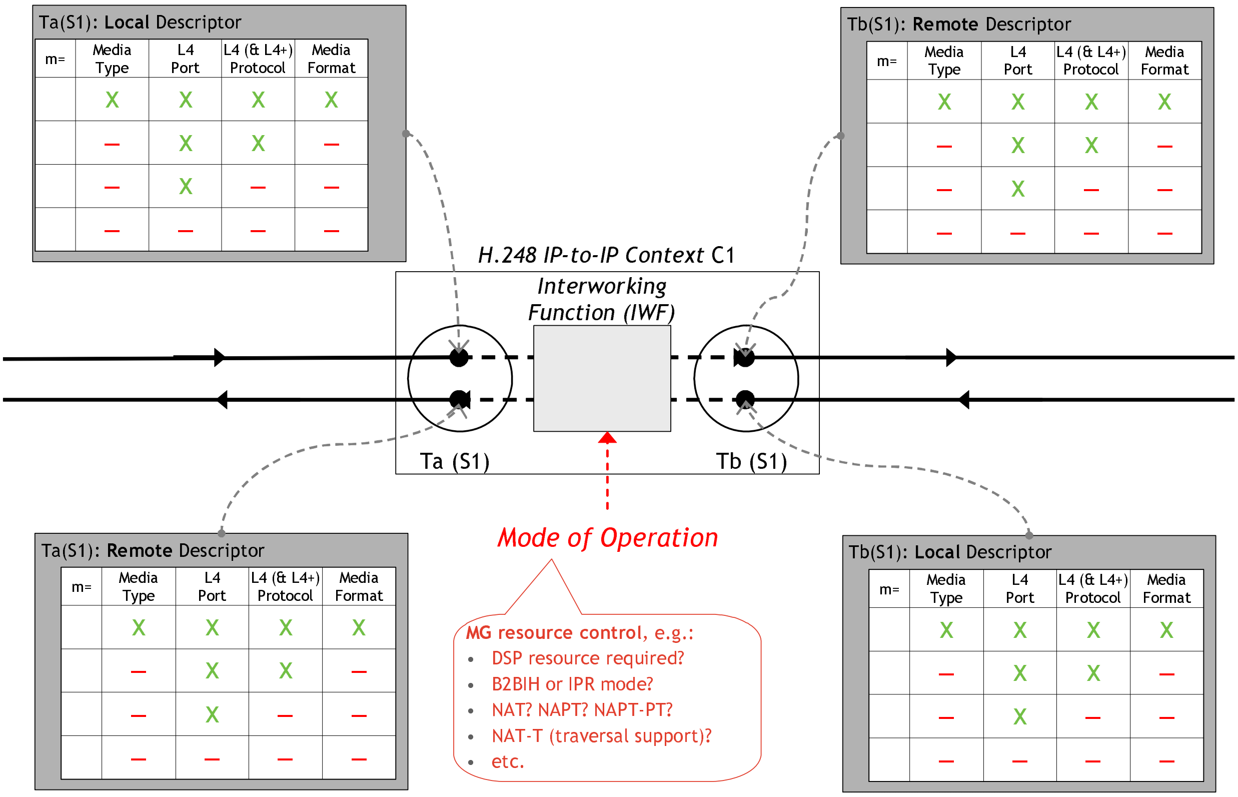
„m=“	Media Type	L4 Port	L4 (& L4+) Protocol	Media Format	H.248 IP-to-IP Context Mode of Operation
E.1, E.2, F.1, F.2	X	X	X	X	Media aware
D.1, D.2	X	X	X	–	Media format agnostic, Media framing aware, Transport aware
C.1, C.2	–	X	X	–	Media agnostic, Transport aware
B.1, B.2	–	X	–	–	Media agnostic, L4-port aware, Transport-protocol agnostic
A.1, A.2	–	–	–	–	Media agnostic, Transport agnostic

NOTE: Column "m=" refers to example BGF modes in subsequent clauses.

Figure I.1: BGF modes - Control framework - Major SDP "m="-line specification combinations

NOTE: In case of BGF modes A and B, the BGF, in case of NA(P)T, cannot re-calculate the *L4 PCI checksum*, as the actual transport protocol (DCCP, UDP, UDP-Lite, TCP, SCTP, …) in use is unknown to the BGF. Thus it is assumed that the SPDF only asks for these modes, if either NA(P)T less operation modes are intended or, in case of NA(P)T, L4 checksum updates are not expected (some L4 protocols define the checksum as an optional element). In other words, the BGF cannot be made responsible for incorrect L4 checksum values, if the SPDF asks for NA(P)T.

There are further four "IP traffic" endpoints in an H.248 IP-to-IP Contexts with a single H.248 Stream, see figure I.2. The mode of each traffic endpoint is primarily under control of the LD for ingress and the RD for egress direction. All four descriptors do finally determine the enforced mode of operation(s) of the "IWF" (the understanding of "*interworking*" and "*interworking function*" is according ITU-T Recommendation Y.1251 [i.13]).



Ta(S1): **Local** Descriptor

m=	Media Type	L4 Port	L4 (& L4+) Protocol	Media Format
	X	X	X	X
	–	X	X	–
	–	X	–	–
	–	–	–	–

Tb(S1): **Remote** Descriptor

m=	Media Type	L4 Port	L4 (& L4+) Protocol	Media Format
	X	X	X	X
	–	X	X	–
	–	X	–	–
	–	–	–	–

Ta(S1): **Remote** Descriptor

m=	Media Type	L4 Port	L4 (& L4+) Protocol	Media Format
	X	X	X	X
	–	X	X	–
	–	X	–	–
	–	–	–	–

Tb(S1): **Local** Descriptor

m=	Media Type	L4 Port	L4 (& L4+) Protocol	Media Format
	X	X	X	X
	–	X	X	–
	–	X	–	–
	–	–	–	–

MG resource control, e.g.:

- DSP resource required?
- B2BIH or IPR mode?
- NAT? NAPT? NAPT-PT?
- NAT-T (traversal support)?
- etc.

Figure I.2: BGF modes - Control Framework - H.248 Local and Remote Descriptor: SDP "m="-line and H.248 IP-to-IP Context

The BGF mode is theoretically *independent* for each *traffic direction*, see figure I.3 and figure I.4. Fortunately the symmetry assumption holds in the very majority of real world use cases, i.e. the signalled mode of the LD is identical to the RD per Stream endpoint.

An example asymmetric use case according figure I.3 is a single NA(P)T case, whereas:

- the NA(P)T-less direction can be media agnostic and transport agnostic; and
- the NA(P)T-full direction has to be transport protocol aware due to required L4 checksum updates.

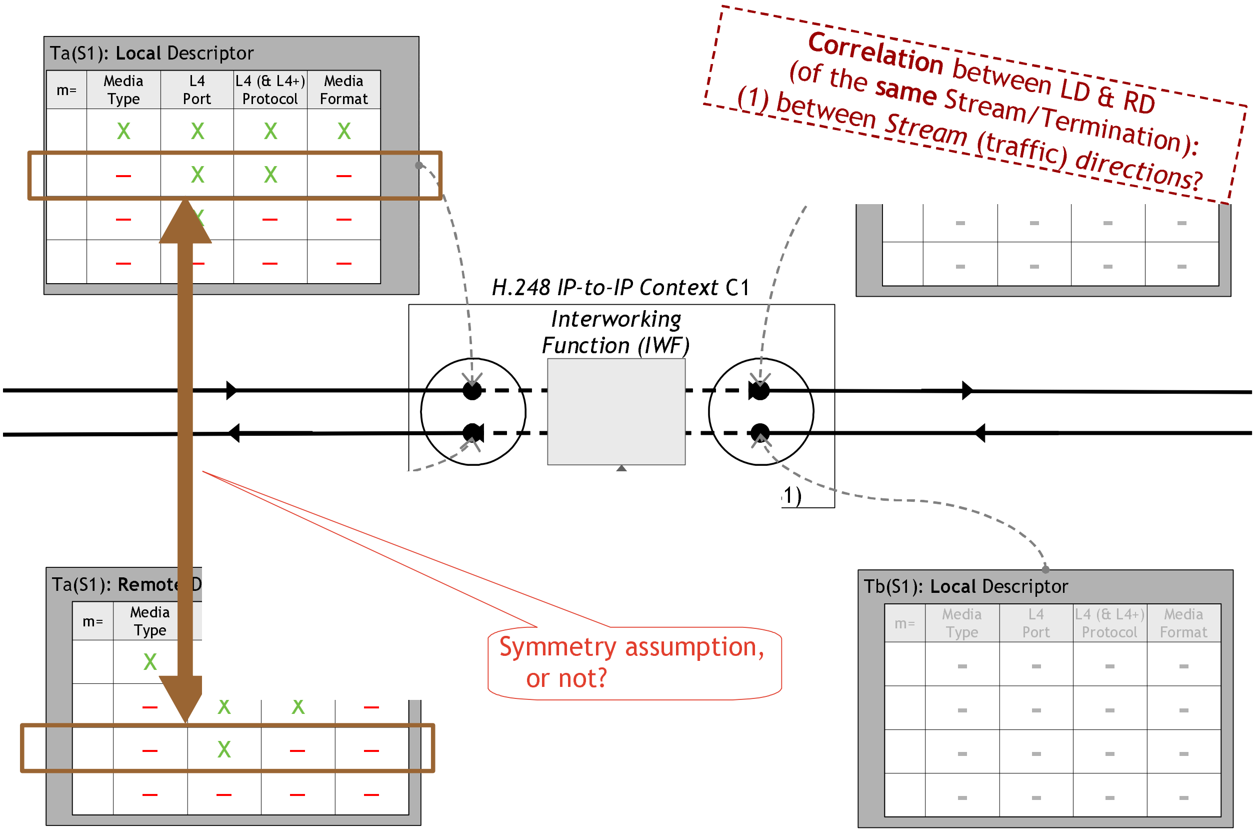

Correlation between LD & RD
(of the same Stream/Termination):
(1) between Stream (traffic) directions?
Ta(S1): Local Descriptor
m=
Media Type
L4 Port
L4 (& L4+) Protocol
Media Format
X
–
H.248 IP-to-IP Context C1
Interworking Function (IWF)
1)
Ta(S1): Remote D
Symmetry assumption, or not?
Tb(S1): Local Descriptor

Figure I.3: BGF modes - Control Framework - Correlation between LD and RD (of the same Stream/Termination): (1) between Stream (traffic) directions

To figure I.3: the selected mode for Ta(S1) *ingress* side (by $LD_{Ta(S1)}$) is different to the selected mode for Ta(S1) *egress* side (by $RD_{Ta(S1)}$). Such an asymmetry might be due to specific NAT behaviour, different media formats per direction, etc.

Figure I.4 depicts the 2nd dimension of the control framework: the correlation between the signalled modes of the two terminations in the context. The symmetry assumption is applicable as there are no reasonable asymmetry use cases. If the BGF receives asymmetric descriptors ($LD_{Ta(S1)} \leftrightarrow RD_{Tb(S1)}$), the BGF could use the joined information of both descriptors from the two Stream endpoints to derive the mode of operation for the particular direction.

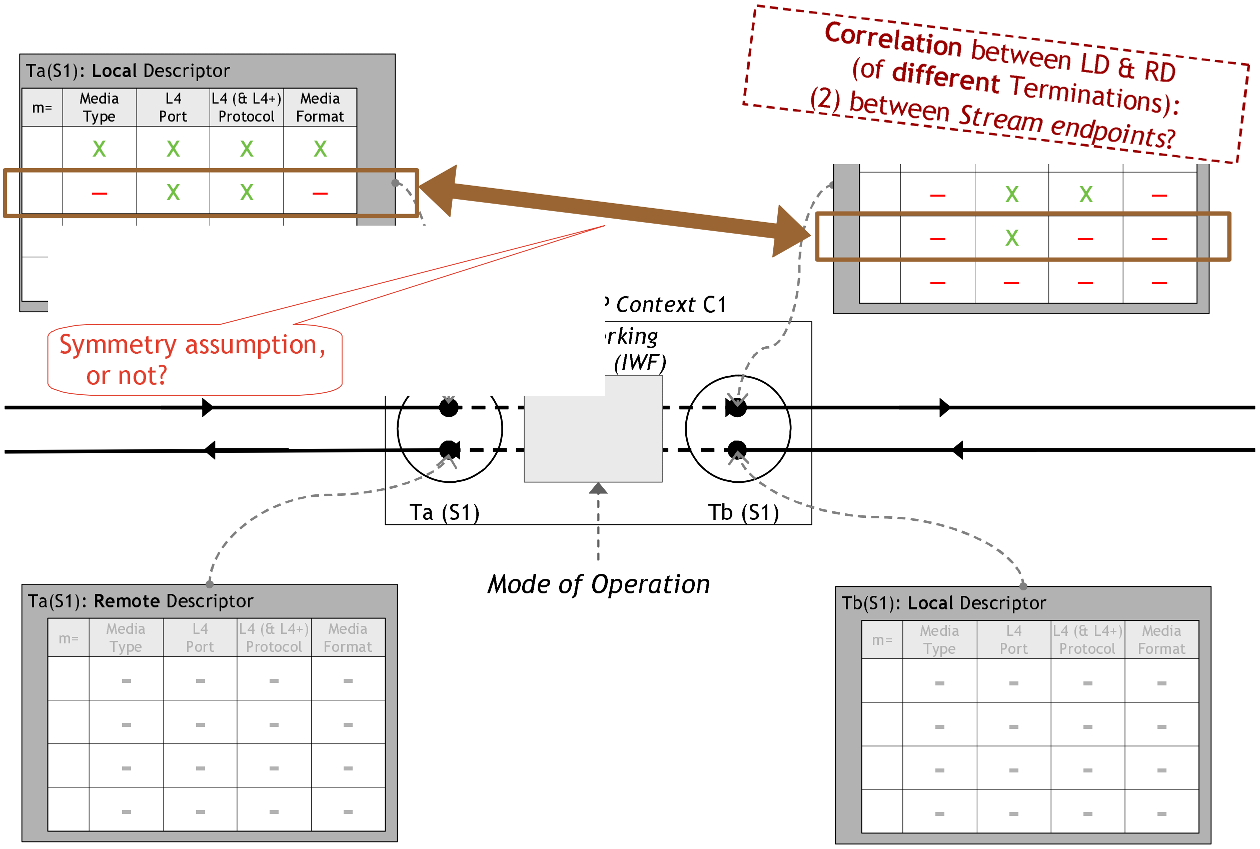


Figure I.4: BGF modes - Control Framework - Correlation between LD and RD (of the same Stream/Termination): (2) between Stream endpoint?

To figure I.4: there would be asymmetry in case of different selected modes between $LD_{Ta(S1)}$) and $RD_{Tb(S1)}$. A real word use case is difficult to imagine, such kind of BGF control could thus lead to an error scenario (e.g. a media-agnostic, transport agnostic Stream connected to a media-aware Stream could lead to an error code reply by the BGF).

The following clauses provide some example modes, inclusive exemplary H.248 signalling.

I.3 Example BGF modes - RTP-based Applications

I.3.1 Example application

This clause considers generic applications, using a RTP session for media transport in the bearer plane. The H.248 Stream do thus carry an RTP *media flow* and RTCP *control flow*. The introduced BGF modes by annex G could be further discriminated with regards to the enforcement of address information translation or not.

I.3.2 Transport-agnostic modes

Figure I.5 illustrates transport-agnostic modes, i.e. the BGF is *not aware* of the used *transport protocols* by the IP flow(s). Each IP packet could be forwarded with or without network address translation (NAT-full (A.1) versus NAT-less (A.2)).

EXAMPLES:

- mode A.1: native NAT function, V4-to-V6 translator;

NOTE: This mode can only be supported in case of UDP and UDP-Lite transport, if the SPDF can ensure that the involved host systems abstain from using a UDP checksum (UDP RFC 768 [i.18]: "An all zero transmitted checksum value means that the transmitter generated no checksum".

- mode A.2: native IP forwarding (see also Draft H.248.64 [i.24]).

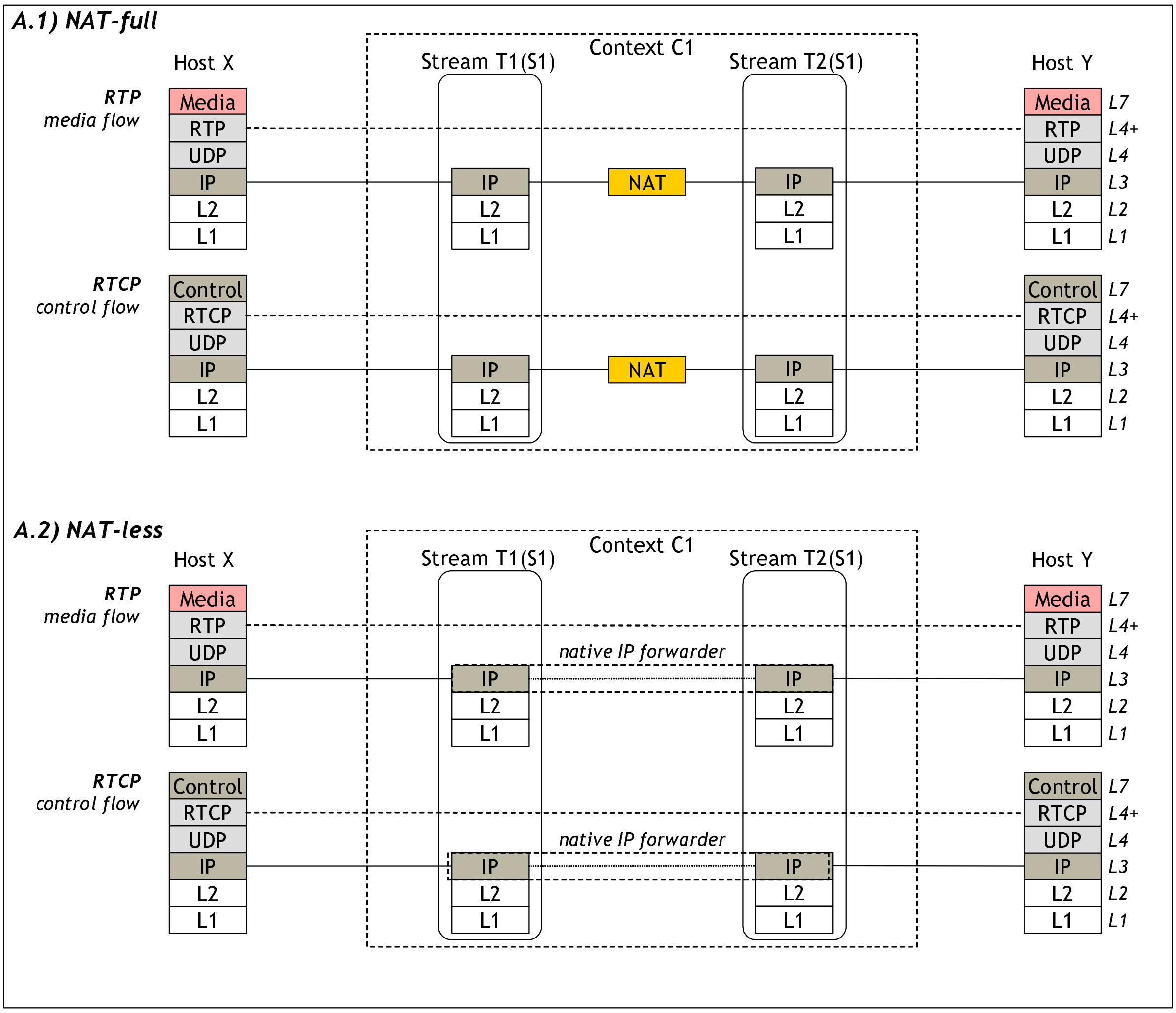


Figure I.5: "Protocol Layer *Lx*"-based Packet Processing BGF modes - Transport-agnostic modes

Tables I.3 and I.4 provide example Stream Descriptor encodings for enforcing the particular modes.

Table I.3: Example H.248 Stream Descriptor for enforcing (A.1) NAT-full transport-agnostic mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
    ipdc/realm = "1"
    },
    Local {
     v=0
     c=IN IP4 $
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     b=…
    }
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
    ipdc/realm = "2"
    },
    Local {
     v=0
     c=IN IP4 $
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     b=…
    }
 }}}
	There is a single H.248 Stream established. NAT implies the indication of the network addresses, which is subject of the SDP "c=" line.
	The network address is underspecified in the LD, because allocated by the BGF itself, and full specified in the RD.
	The IP domain, for each IP connection endpoint, is indicated by the LCD level property *ipdc/realm*. This example uses an abstract format ("1", "2") as binding element between the name-based domain and the numerical IP address realm.
	It may be noted that neither the LD nor RD contains any transport and media related information; there is thus not any "m=" line nor "a=" lines. The "b=" line could be used for IP layer bitrate information.

Table I.4: Example H.248 Stream Descriptor for enforcing (A.2) NAT-less transport-agnostic mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "1"},
    Local {
     v=0
     c=IN IP4 20.20.20.20
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     b=…
    }
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "2"},
    Local {
     v=0
     c=IN IP4 10.10.10.10
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     b=…
    }
 }}}
	NAT-less mode is enforced by identical IP1-LD/IP2-RD and IP1-RD/IP2-LD transport addresses (see clause 5.17.1.2.4.1/ [i.3]).

I.3.3 L4-port aware and transport-protocol agnostic modes

Figure I.6 illustrates L4-port aware and transport-protocol agnostic modes, i.e. the BGF knows the allocated port number, but is not aware of the used transport protocols by the IP flow(s). Each IP packet could be forwarded with or without network address and port translation (NAPT-full (B.1) versus NAPT-less (B.2)).

EXAMPLES:

- mode B.1: "L4-independent, native NAPT";

NOTE: This mode can only be supported in case of UDP and UDP-Lite transport, if the SPDF can ensure that the involved host systems abstain from using a UDP checksum (UDP RFC 768 [i.18]: "An all zero transmitted checksum value means that the transmitter generated no checksum").

- mode B.2: "L4-independent, L4 switching".

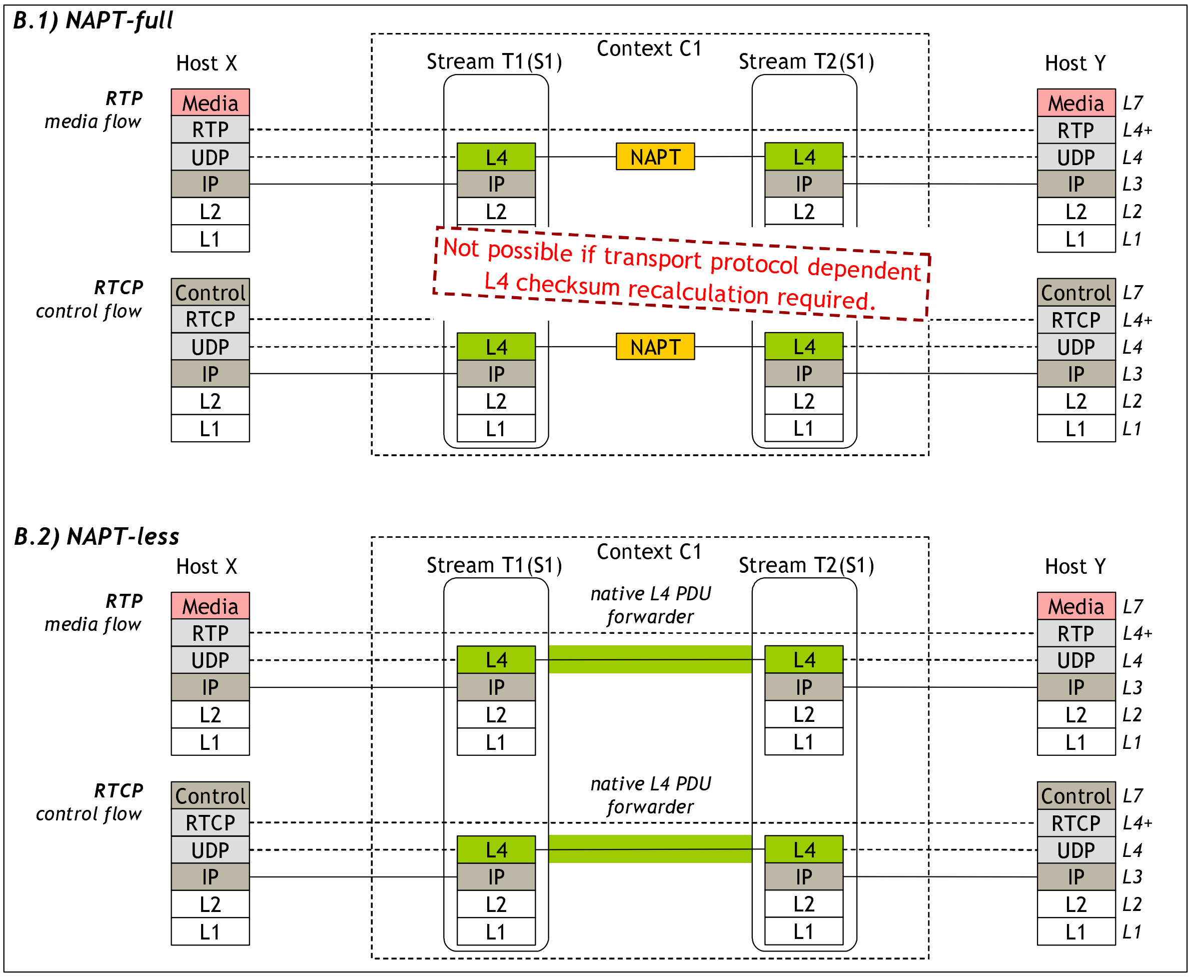


Figure I.6: "Protocol Layer *Lx*"-based Packet Processing BGF modes -
L4-port aware and transport-protocol agnostic modes

Tables I.5 and I.6 provide example Stream Descriptor encodings for enforcing the particular modes.

Table I.5: Example H.248 Stream Descriptor for enforcing (B.1) NAPT-full, L4 aware transport-agnostic mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
Add = ip/321/$/$ {
Media {
Stream = 1 {
LocalControl {
ipdc/realm = "1"},
Local {
v=0
c=IN IP4 $
m=- $ - -
b=…
}
Remote {
v=0
c=IN IP4 10.10.10.10
m=- 40000 - -
b=…
}
Add = ip/321/$/$ {
Media {
Stream = 1 {
LocalControl {
ipdc/realm = "2"},
Local {
v=0
c=IN IP4 $
m=- $ - -
b=…
}
Remote {
v=0
c=IN IP4 20.20.20.20
m=- 50000 - -
b=…
}
}}}
	The LD and RD does now contain also the "m=" line, because the transport port value is one of the four "m=" line fields.
	The other "m=" line fields are "dashed" by the "-" value. The BGF is thus not aware of the media type, media format and used transport.
	It may be noted that this "m=" line specification reflects the Ia profile version 1 BGF mode.

Table I.6: Example H.248 Stream Descriptor for enforcing (B.2) NAPT-less, L4 aware transport-agnostic mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
Add = ip/321/$/$ {
Media {
Stream = 1 {
LocalControl {
ipdc/realm = "1"},
Local {
v=0
c=IN IP4 20.20.20.20
m=- 50000 - -
b=…
}
Remote {
v=0
c=IN IP4 10.10.10.10
m=- 40000 - -
b=…
}
Add = ip/321/$/$ {
Media {
Stream = 1 {
LocalControl {
ipdc/realm = "2"},
Local {
v=0
c=IN IP4 10.10.10.10
m=- 40000 - -
b=…
}
Remote {
v=0
c=IN IP4 20.20.20.20
m=- 50000 - -
b=…
}
}}}
	NAPT-less mode is enforced by identical IP1-LD/IP2-RD and IP1-RD/IP2-LD transport addresses.

I.3.4 Transport aware (= L4-port aware and transport-protocol aware) modes

Figure I.7 illustrates transport aware (= L4-port aware and transport-protocol aware) modes. Each IP packet could be forwarded with or without network address and port translation (NAPT-full (C.1) versus NAPT-less (C.2)).

EXAMPLES:

- mode C.1: "L4-dependent, native NAPT";
- mode C.2: "L4-dependent, L4 switching".

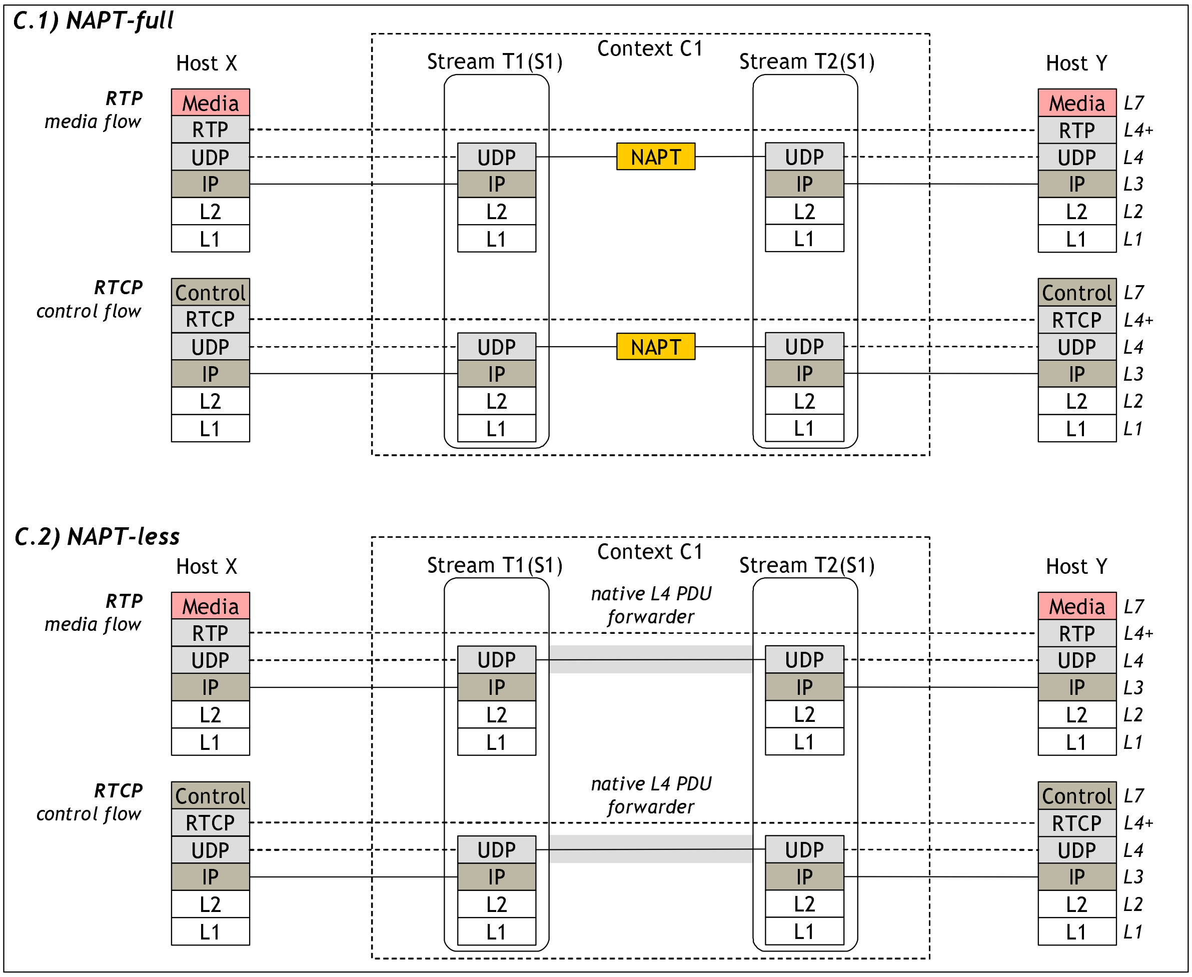


Figure I.7: "Protocol Layer *Lx*"-based Packet Processing BGF modes - Transport aware (= L4-port aware and Transport-protocol aware) modes

Tables I.7 and I.8 provide example Stream Descriptor encodings for enforcing the particular modes.

Table I.7: Example H.248 Stream Descriptor for enforcing (C.1) NAPT-full, L4 aware transport-aware mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "1"},
    Local {
     v=0
     c=IN IP4 $
     m=- $ udp -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=- 40000 udp -
     b=…
    }
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "2"},
    Local {
     v=0
     c=IN IP4 $
     m=- $ udp -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=- 50000 udp -
     b=…
    }
 }}}
	The used transport (protocol) is now indicated in the "m=" line, which is still media type agnostic and media format agnostic.

Table I.8: Example H.248 Stream Descriptor for enforcing (C.2) NAPT-less, L4 aware transport-aware mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "1"},
    Local {
     v=0
     c=IN IP4 20.20.20.20
     m=- 50000 udp -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=- 40000 udp -
     b=…
    }
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "2"},
    Local {
     v=0
     c=IN IP4 10.10.10.10
     m=- 40000 udp -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=- 50000 udp -
     b=…
    }
 }}}
	NAPT less mode is enforced by identical IP1-LD/IP2-RD and IP1-RD/IP2-LD transport addresses.

I.3.5 Media framing aware (= media-type aware, media-format agnostic, L4-port aware and transport-protocol aware) modes

Figure I.8 illustrates *media framing* aware (= media-type aware, media-format agnostic, L4-port aware and transport-protocol aware) modes, i.e. the BGF is not aware of the used media format. But the BGF knows the media framing protocol, which is in this example the application level framing protocol RTP, or more precisely: profile RTP/AVP. Each H.248 Stream endpoint (i.e. T1(S1) and T2(S1)) represents a single *RTP endsystem*. The H.248 Context is consequently representing a *back-to-back RTP endsystem* (B2BRE) model. A single "end-to-end" RTP session is partitioned in two RTP session legs in case of the B2BRE mode. Any RTP session (leg) is constituted (and could be thus identified) by the tuple of {SSRC, CNAME}. The "CNAME" is the SDES element carried by the RTP media flow associated RTCP control flow. However, as the BGF acts media formats agnostic a couple of RTP header elements (RFC 3550 [i.19]) needs to be carried over from the received RTP packet to the transmitted RTP packet, like:

- Padding bit.
- Extension bit.
- Timestamp.
- CSRC count and CSRC values.
- Marker bit.
- Payload type.

RTCP is terminated, i.e. each session leg has an independent RTCP session.

EXAMPLES:

- mode D.1: H.248.xnq-based QoS reporting;

NOTE: H.248.xnq is not defined for RTP Translator modes.

- mode D.2: native IP forwarding (see also Draft H.248.64).

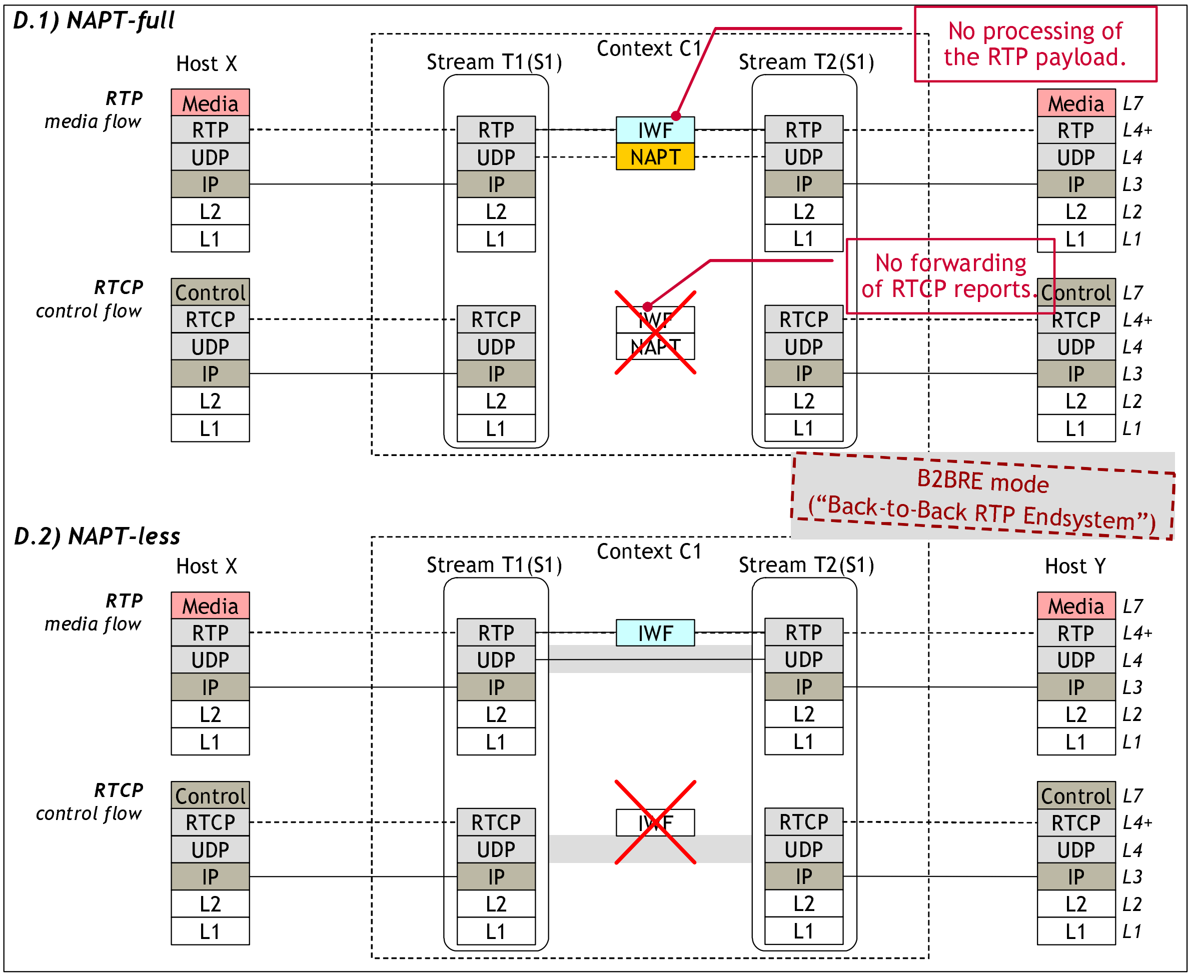


Figure I.8: "Protocol Layer *Lx*"-based Packet Processing BGF modes - Media framing aware (= Media-type aware, Media-format agnostic, L4-port aware and Transport-protocol aware) modes

Tables I.9 and I.10 provide example Stream Descriptor encodings for enforcing the particular modes.

Table I.9: Example H.248 Stream Descriptor for enforcing (D.1) NAPT-full, Media framing aware, media format agnostic mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
Add = ip/321/$/$ {
Media {
Stream = 1 {
LocalControl {
ipdc/realm = "1"},
Local {
v=0
c=IN IP4 $
m=- $ RTP/AVP -
b=…
}
Remote {
v=0
c=IN IP4 10.10.10.10
m=- 40000 RTP/AVP -
b=…
}
Add = ip/321/$/$ {
Media {
Stream = 1 {
LocalControl {
ipdc/realm = "2"},
Local {
v=0
c=IN IP4 $
m=- $ RTP/AVP -
b=…
}
Remote {
v=0
c=IN IP4 20.20.20.20
m=- 50000 RTP/AVP -
b=…
}
}}}
	If at all, then the used media framing protocol will be indicated in the "m=" line by field "transport protocol", which relates here to "RTP-over-UDP" in case of RFC 3551 [i.20] profile "RTP/AVP".
	Conclusion:
	• Transport protocol: UDP
	• Application level framing protocol: RTP
	The Add commands are still media type agnostic and media format agnostic (e.g. the BGF is not aware whether the RTP service data unit carries e.g. audio (e.g. G.72X), video (e.g. H.26X), realtime text (e.g. T.140), realtime facsimile (e.g. T.38 over RTP) or multimedia (e.g. MPEG)).

Table I.10: Example H.248 Stream Descriptor for enforcing (D.2) NAPT-less, Media framing aware, media format agnostic mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "1"},
    Local {
     v=0
     c=IN IP4 20.20.20.20
     m=- 50000 RTP/AVP -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=- 40000 RTP/AVP -
     b=…
    }
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "2"},
    Local {
     v=0
     c=IN IP4 10.10.10.10
     m=- 40000 RTP/AVP -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=- 50000 RTP/AVP -
     b=…
    }
 }}}
	NAPT-less mode is enforced by identical IP1-LD/IP2-RD and IP1-RD/IP2-LD transport addresses.

I.3.5.1 Open items

This particular BGF mode may lead to different variants concerning RTCP processing (e.g. inspection of report content, protocol termination, forwarding/filtering of particular report types). This mode is also related to ongoing work in IETF and ITU-T, and thus for further studies.

I.3.6 Media aware "RTP Transport Translator" (= media-type aware, media-format aware) modes

Figure I.9 illustrates media aware "RTP *Transport Translator*" (= media-type aware, media-format aware) modes. The BGF acts as a B2BRE with two session legs and the corresponding RTCP sessions. More information on this modes is provided by [i.11] and [i.12].

EXAMPLES:

- mode E.1/E.2:
  - "Media Transpacking" (e.g. packetization time conversion according Draft ITU-T G.IP2IP [i.14]).
  - "Dejittering" (Draft ITU-T G.IP2IP [i.14]: e.g. jitter adjustment/limitation or jitter elimination (or complete dejittering between two interconnected IP domains with substantially different IPDV conditions).

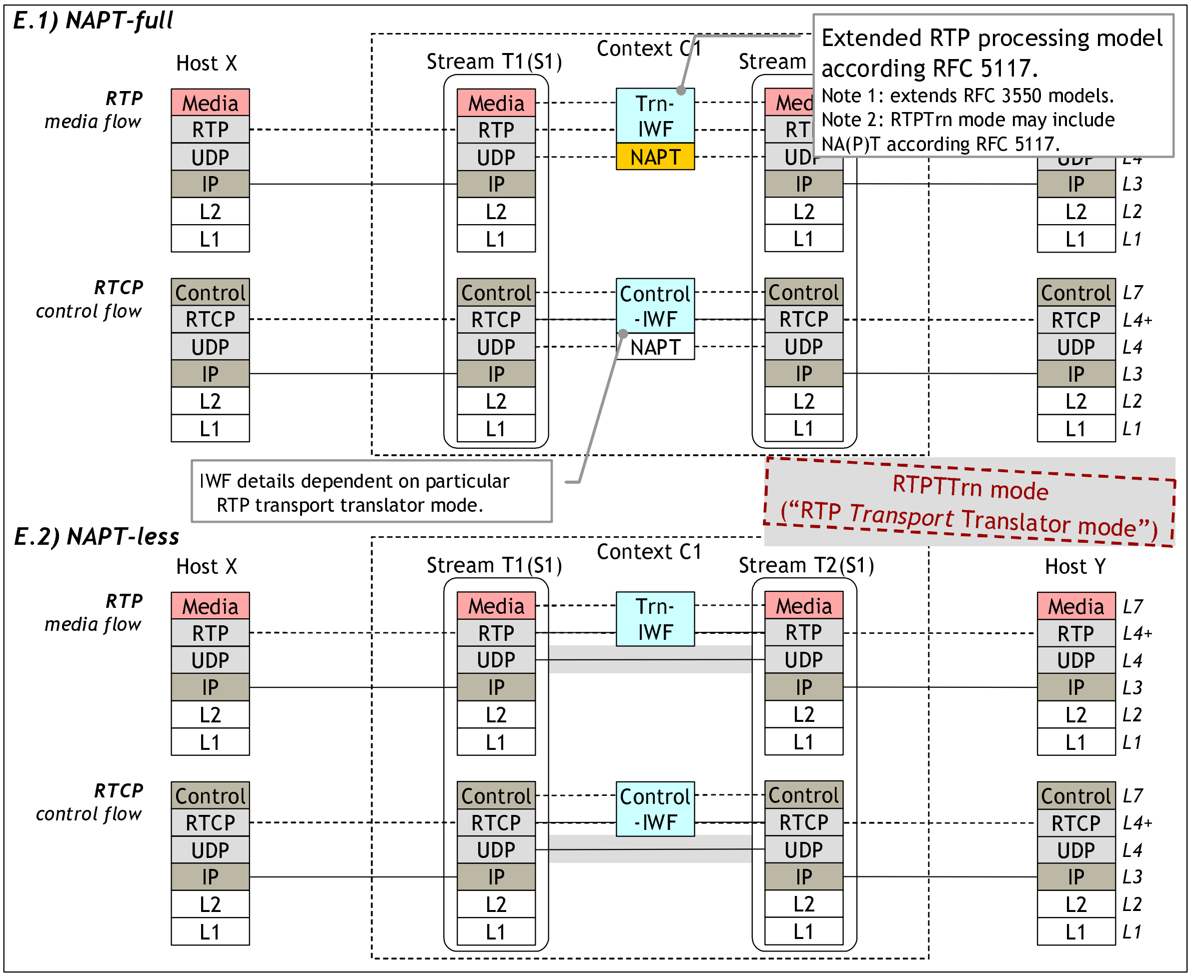

E.1) NAPT-full
Host X
Context C1
Stream T1(S1)
Stream
Extended RTP processing model according RFC 5117.
Note 1: extends RFC 3550 models.
Note 2: RTPTrn mode may include NA(P)T according RFC 5117.
RTP media flow
RTCP control flow
Media
RTP
UDP
IP
L2
L1
Control
RTCP
Trn-IWF
NAPT
Control-IWF
L7
L4+
L4
L3
L2
L1
IWF details dependent on particular RTP transport translator mode.
RTPTTrn mode
("RTP Transport Translator mode")
E.2) NAPT-less
Stream T2(S1)
Host Y

Figure I.9: "Protocol Layer *Lx*"-based Packet Processing BGF modes - Media aware "RTP Transport Translator" (= Media-type aware, Media-format aware) modes

Tables I.11 and I.12 provide example Stream Descriptor encodings for enforcing that particular modes.

Table I.11: Example H.248 Stream Descriptor for enforcing (E.1) NAPT-full, Media aware mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "1"},
    Local {
     v=0
     c=IN IP4 $
     m=audio $ RTP/AVP 8
     a=ptime:20
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=audio 40000 RTP/AVP 8
     a=ptime:20
     b=…
    }
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "2"},
    Local {
     v=0
     c=IN IP4 $
     m=audio $ RTP/AVP 8
     a=ptime:30
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=audio 50000 RTP/AVP 8
     a=ptime:30
     b=…
    }
 }}}
	The "m=" lines are now fully explicit concerning media type, framing and format.
	Example:
	Different packetization times for the same codec type ("media format") result in media transpacking. Transpacking implies RTP SDU processing, but also the modification of RTP PCI (e.g. timestamp value).

Table I.12: Example H.248 Stream Descriptor for enforcing (E.2) NAPT-less, Media-aware mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "1"},
    Local {
     v=0
     c=IN IP4 20.20.20.20
     m=audio 50000 RTP/AVP 8
     a=ptime:20
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=audio 40000 RTP/AVP 8
     a=ptime:20
     b=…
    }
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "2"},
    Local {
     v=0
     c=IN IP4 10.10.10.10
     m=audio 40000 RTP/AVP 8
     a=ptime:30
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=audio 50000 RTP/AVP 8
     a=ptime:30
     b=…
    }
 }}}
	NAPT less mode is enforced by identical IP1-LD/IP2-RD and IP1-RD/IP2-LD transport addresses.
	Different *ptimes* for the same codec result in media transpacking.

I.3.7 Media aware "RTP Media Translator" (= media-type aware, media-format aware) modes

Figure I.10 illustrates media aware "RTP *Media Translator*" (= media-type aware, media-format aware) modes.

EXAMPLES:

- mode F.1/F.2:
  - "Media (format) transcoding"
    (e.g. voice transcoding, audio transcoding, video transcoding, image transcoding).
  - "(PSTN) bearer service adaptation" like e.g. peering V.152 VBDoIP domains with T.38 FoIP domains.
  - Inband signalling for Network Telephone Events (NTE): adaptation between RTP pass-through mode ("NTE-over-voice codec-over-RTP") and RTP packet relay mode ("NTE via RFC 4733 [i.21] and RFC 4734 [i.23] RTP packets").

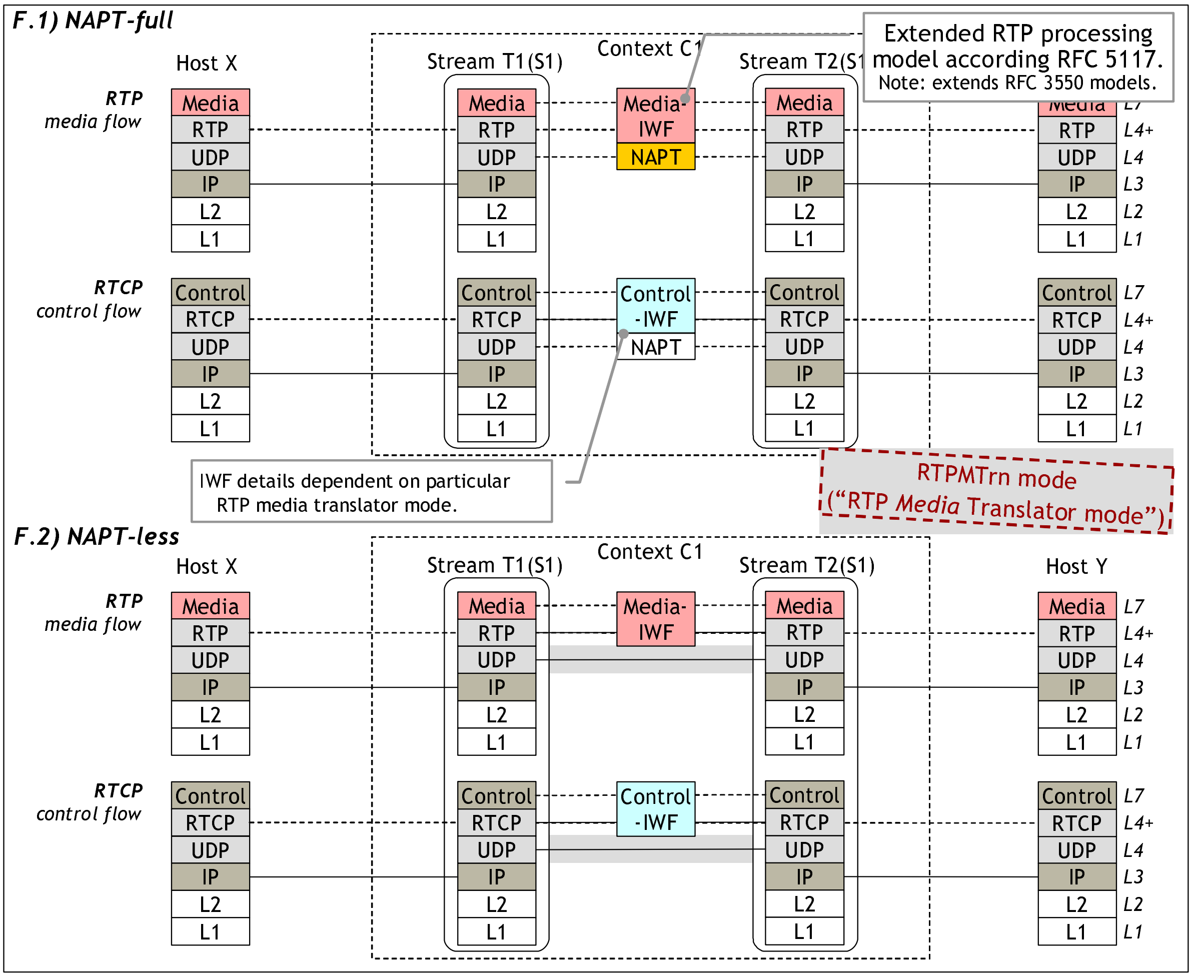

F.1) NAPT-full
Host X
Context C1
Stream T1(S1)
Stream T2(S1)
Extended RTP processing model according RFC 5117.
Note: extends RFC 3550 models.
RTP media flow
RTCP control flow
Media
RTP
UDP
IP
L2
L1
Control
RTCP
Media-IWF
NAPT
Control-IWF
L7
L4+
L4
L3
IWF details dependent on particular RTP media translator mode.
RTPMTrn mode ("RTP Media Translator mode")
F.2) NAPT-less
Host Y

Figure I.10: "Protocol Layer *Lx*"-based Packet Processing BGF modes - Media aware "RTP Media Translator" (= Media-type aware, Media-format aware) modes

Tables I.13 and I.14 provide example Stream Descriptor encodings for enforcing that particular modes.

Table I.13: Example H.248 Stream Descriptor for enforcing (F.1) NAPT-full, Media aware mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
Add = ip/321/$/$ {
Media {
Stream = 1 {
LocalControl {
ipdc/realm = "1"},
Local {
v=0
c=IN IP4 $
m=audio $ RTP/AVP 8
a=ptime:20
b=…
}
Remote {
v=0
c=IN IP4 10.10.10.10
m=audio 40000 RTP/AVP 8
a=ptime:20
b=…
}
Add = ip/321/$/$ {
Media {
Stream = 1 {
LocalControl {
ipdc/realm = "2"},
Local {
v=0
c=IN IP4 $
m=audio $ RTP/AVP 4
a=ptime:30
b=…
}
Remote {
v=0
c=IN IP4 20.20.20.20
m=audio 50000 RTP/AVP 4
a=ptime:30
b=…
}
}}}
	There are different media formats requested for each IP Stream endpoint, resulting here in voice transcoding between G.711 A-law and G.723.1. The G.723.1 codec type does support two sub-modes, which are not indicated here in the SDP blocks. It may be then supposed that the BGF is selecting (per default) the high-rate speech (6.3 kbit/s) mode in egress direction (due to QoS reasons).

Table I.14: Example H.248 Stream Descriptor for enforcing (F.2) NAPT-less, Media-aware mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "1"},
    Local {
     v=0
     c=IN IP4 20.20.20.20
     m=audio 50000 RTP/AVP 8
     a=ptime:20
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=audio 40000 RTP/AVP 8
     a=ptime:20
     b=…
    }
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     ipdc/realm = "2"},
    Local {
     v=0
     c=IN IP4 10.10.10.10
     m=audio 40000 RTP/AVP 4
     a=ptime:30
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=audio 50000 RTP/AVP 4
     a=ptime:30
     b=…
    }
 }}}
	NAPT less mode is enforced by identical IP1-LD/IP2-RD and IP1-RD/IP2-LD transport addresses.

I.4 Example BGF modes - TCP-based Applications

I.4.1 Example application

This clause considers generic applications, using a TCP transport connection for data transport in the bearer plane. The H.248 Stream relates therefore to an TCP *data flow*. The introduced BGF modes by annex G is further refined, using the following terminology:

- **Transport (TCP)** ***relay*** **(translator) mode:** transparent forwarding of TCP packets in terms of stateless behaviour concerning the TCP connection state machine.

NOTE 1: The term T*ransport Relay Translator* (TRT) mode is based on RFC 3142 [i.22], which scopes the IP version translation for transport protocol aware IP nodes.

- **Transport (TCP)** ***proxy*** **(translator) mode** (also known as Back-to-Back TCP Endpoint (B2BTE) mode)**:** statefull forwarding of TCP packets in terms of full protocol termination. The end-to-end TCP connection is partitioned in two TCP connection legs by the BGF. Each H.248 Stream endpoint provides a stateful TCP connection state machine.

NOTE 2: The term *proxy* mode is similar as used for HTTP proxy, FTP proxy, SIP proxy, etc.

I.4.1.1 Mode discrimination

There is not yet any defined protocol element (like e.g. a SDP information element or a H.248 property) for the explicit discrimination between the TCP relay and proxy mode. The examples here are using thus an interim solution by re-using the "media type" codepoint for discrimination. See e.g.:

- Table I.13: TCP relay mode, media type = "-".
- Table I.15 :TCP proxy mode, media type = "application".

The examples are just illustrative and will be updated as soon as the solution is syntactically and semantically clarified.

I.4.2 TCP relay modes

TCP relay mode is only applicable for fully media agnostic applications.

I.4.2.1 Unencrypted transport layer

Figure I.11 illustrates TCP relay modes, i.e. the BGF is aware that the IP flow is comprised by TCP packets. The BGF will be "TCP aware" for unambiguous recalculation of L4 header checksum.

EXAMPLES:

- mode G.1: NAPT function, for e.g.:
  - instant messaging in session mode: (MSRP) messages transport over TCP ("MSRPoTCP");
  - media streaming (IPTV, VoD) control via RTSP ("RTSPoTCP"); or
  - hypertext downloading (WWW) via HTTP ("HTTPoTCP").
- mode G.2: same, but NAPT-less.

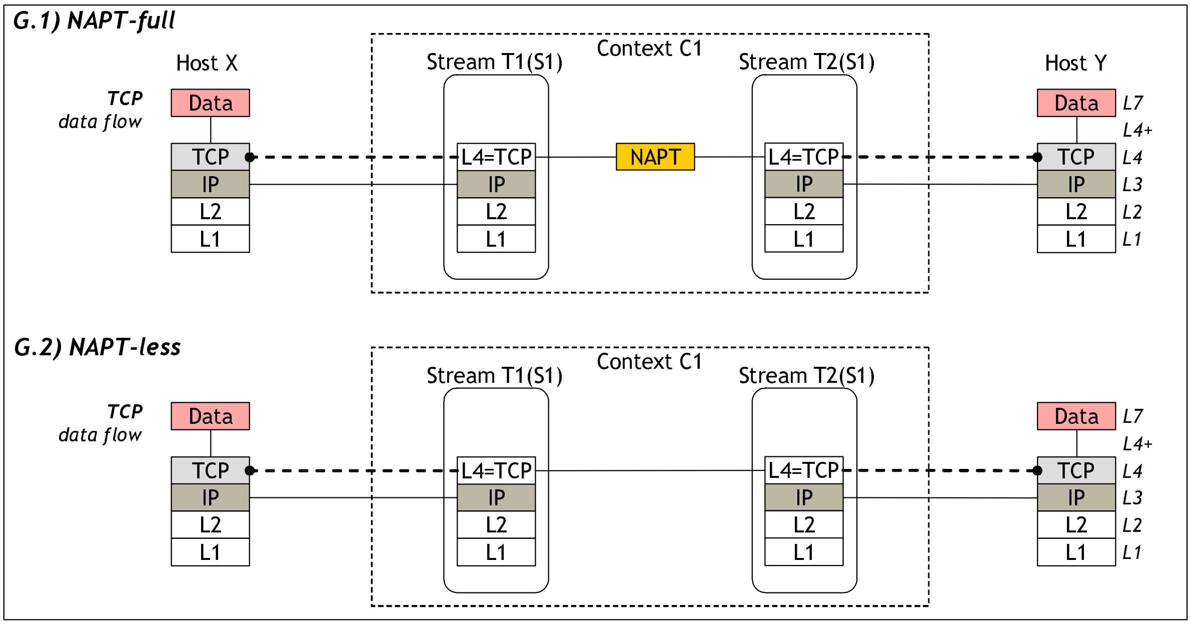


Figure I.11: "Protocol Layer *Lx*"-based Packet Processing BGF modes - TCP relay modes

Tables I.15 and I.16 provide example Stream Descriptor encodings for enforcing that particular modes.

Table I.15: Example H.248 Stream Descriptor for enforcing (G.1) NAT-full TCP relay mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     …},
    Local {
     v=0
     c=IN IP4 $
     m=- $ TCP/MSRP -
     a=…
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=- 40000 TCP/MSRP -
     a=…
     b=…
    }
 }}
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     …},
    Local {
     v=0
     c=IN IP4 $
     m=- $ TCP/MSRP -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=- 50000 TCP/MSRP -
     b=…
    }
 }}}
	Media type and media format is not specified. The media (data) framing is indicated by "MSRP", but transparent for BGF (because not processing any kind of MSRP related protocol element or data).

Table I.16: Example H.248 Stream Descriptor for enforcing (G.2) NAT-less TCP relay mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     …},
    Local {
     v=0
     c=IN IP4 20.20.20.20
     m=- 50000 tcp -
     a=…
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=- 40000 tcp -
     a=…
     b=…
    }
 }}
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     …},
    Local {
     v=0
     c=IN IP4 10.10.10.10
     m=- 40000 tcp -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=- 50000 tcp -
     b=…
    }
 }}}
	Media type and media format is not specified. The applied data framing or application protocol is also not specified.

I.4.2.2 Encrypted transport layer using TLS

Figure I.12 illustrates TCP relay modes with TLS encrypted traffic. TLS is transparent for the BGF, because above the TCP layer. TLS en-/decryption is subject of the two (BGF remote) TCP endpoints.

EXAMPLES: See clause I.3.2.1.

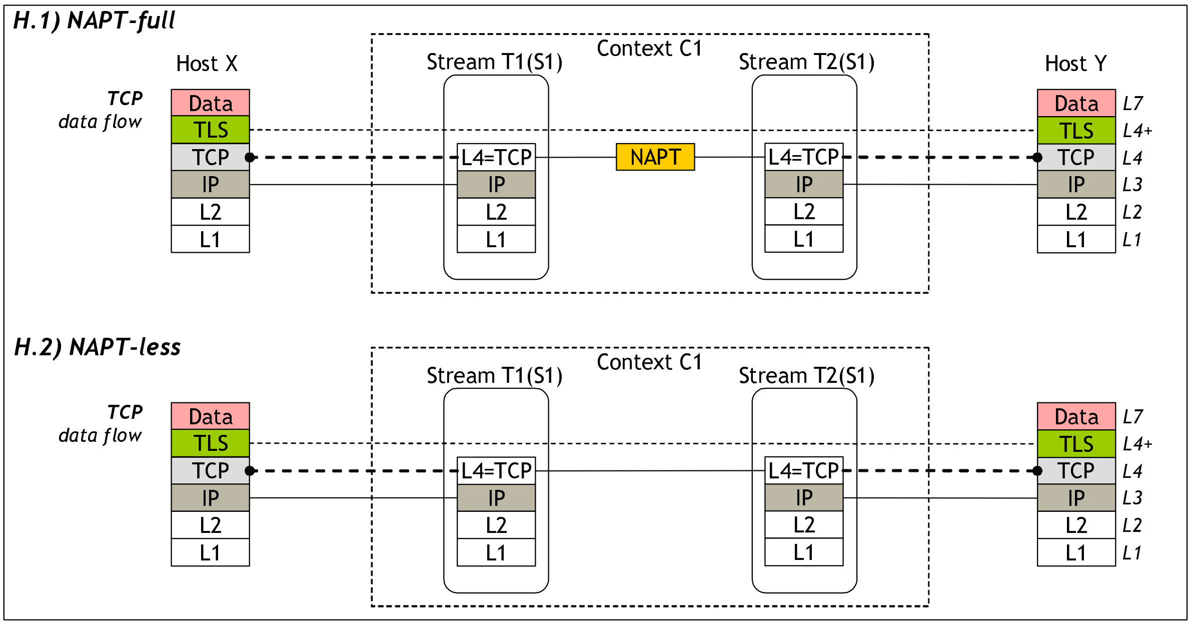


Figure I.12: "Protocol Layer *Lx*"-based Packet Processing BGF modes - TCP relay modes - Transparent TLS forwarding

Usage of TLS is transparent, thus there is no difference on the H.248 interface and the Stream Descriptor encoding examples of tables I.13 and I.14 apply here as well.

I.4.3 TCP proxy modes

TCP proxy mode is applied in case of media (type) awareness. Figure I.13 illustrates TCP proxy modes, i.e. the BGF is terminating the TCP connection from host X and from host Y. The end-to-end TCP path is thus comprised by two interconnected TCP connections.

EXAMPLES:

- mode G.1: NAPT function, for e.g.:
  - TLS/TCP to non-TLS/TCP interworking;
  - BGF with embedded MSRP relay; or
  - ITU-T Recommendation Y.1560 "TCP" middlebox [i.15].
- mode G.2: same, but NAPT-less.

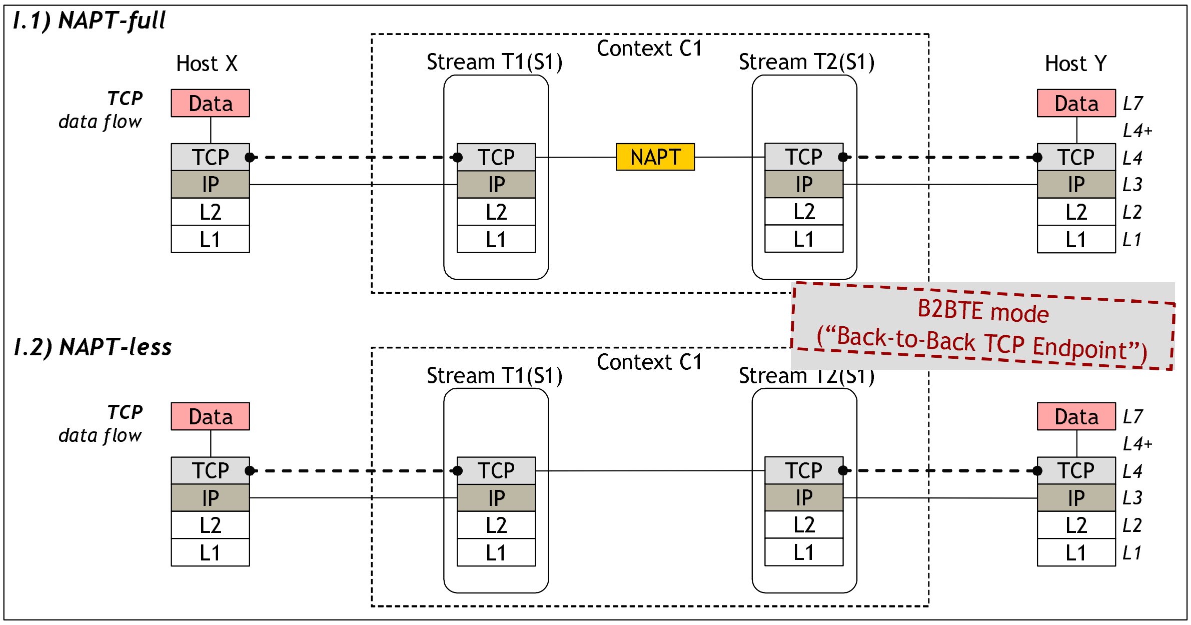


Figure I.13: "Protocol Layer *Lx*"-based Packet Processing BGF modes - TCP proxy modes

Tables I.17 and I.18 provide example Stream Descriptor encodings for enforcing that particular modes.

Table I.17: Example H.248 Stream Descriptor for enforcing (I.1) NAPT-full TCP proxy mode

H.248 encoding (shortened command)	Comments

MEGACO/3 [11.9.19.65]
…
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     … },
    Local {
     v=0
     c=IN IP4 $
     m=application $ TCP/MSRP -
     a=…
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=application 40000 TCP/MSRP -
     a=…
     b=…
    }
 }}
 Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     … },
    Local {
     v=0
     c=IN IP4 $
     m=application $ TCP/MSRP -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=application 50000 TCP/MSRP -
     b=…
    }
 }}}
	Media type is specified in order to discriminate proxy from relay mode.
	The media type value "application" is used in this example.
	The media format is unspecified and also not required: just TCP is terminated, but not the application protocol itself.

Table I.18: Example H.248 Stream Descriptor for enforcing (I.2) NAPT-less TCP proxy mode

<table>
<tr><th>H.248 encoding (shortened command)</th><th>Comments</th></tr>
<tr><td><pre>
MEGACO/3 [11.9.19.65]
…
Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     … },
    Local {
     v=0
     c=IN IP4 20.20.20.20
     m=application 50000 tcp -
     a=…
     b=…
    }
    Remote {
     v=0
     c=IN IP4 10.10.10.10
     m=application 40000 tcp -
     a=…
     b=…
    }
 }}
Add = ip/321/$/$ {
  Media {
   Stream = 1 {
    LocalControl {
     … },
    Local {
     v=0
     c=IN IP4 10.10.10.10
     m=application 40000 tcp -
     b=…
    }
    Remote {
     v=0
     c=IN IP4 20.20.20.20
     m=application 50000 tcp -
     b=…
    }
 }}}
</pre></td><td>Media type is specified</td></tr>
</table>

I.5 Summary

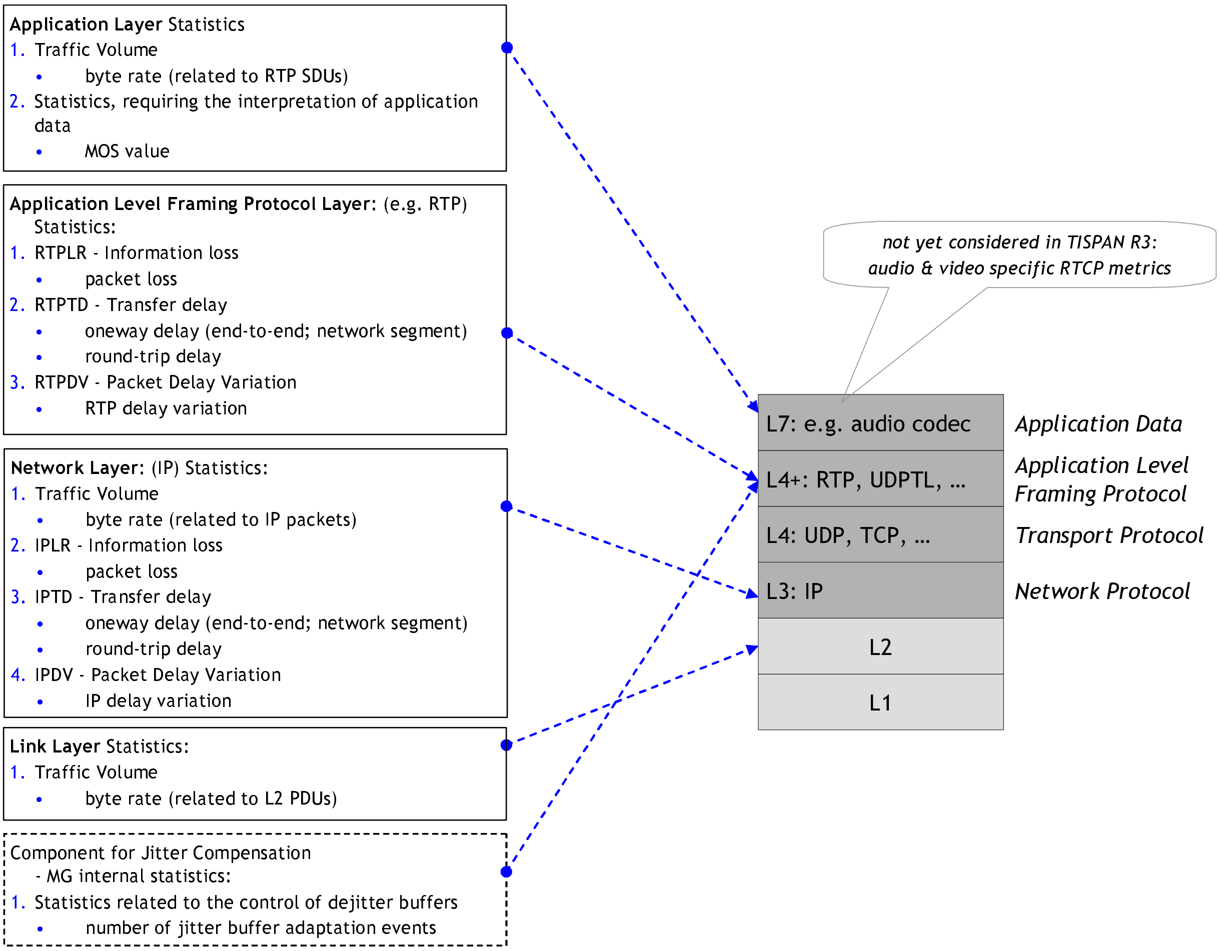
This annex provides around 20 examples for BGF modes. The number may be further multiplied when considering additional security functions and statistics support. The exemplary H.248 signalling underlines the basic possibility of unambiguous enforcement of particular modes by proper usage of SDP specifications in the LD and RD. However, any slight deviation may lead to a discrepancy between the requested mode by the SPDF and finally enforce mode in the BGF.

Annex J: Illustration of BGF Reporting of Protocol Layer Lx based Performance Measurements

The BGF supports measurement points (MP) for the measurement of service, load, capacity and performance related metrics. There are metrics with particular scope on SIP session-dependent and session-independent measurements. The session-dependent measurements are reported at the Ia interface as H.248 statistics. The Ia interface is thus a reporting point (RP) in the RACS control plane.

The BGF supports *local* measurement points, but also the reporting of *remote* measurement data in case of RTP bearers. Remote measurement data is carried via RTCP packets by specific report types.

Table I.1 provides some examples for protocol layer dependent measurements, statistics generation and reporting. Figure J.1 illustrates the relation between performance metrics and protocol layering.



Application Layer Statistics
1. Traffic Volume
   - byte rate (related to RTP SDUs)
2. Statistics, requiring the interpretation of application data
   - MOS value

Application Level Framing Protocol Layer: (e.g. RTP) Statistics:
1. RTPLR - Information loss
   - packet loss
2. RTPTD - Transfer delay
   - oneway delay (end-to-end; network segment)
   - round-trip delay
3. RTPDV - Packet Delay Variation
   - RTP delay variation

Network Layer: (IP) Statistics:
1. Traffic Volume
   - byte rate (related to IP packets)
2. IPLR - Information loss
   - packet loss
3. IPTD - Transfer delay
   - oneway delay (end-to-end; network segment)
   - round-trip delay
4. IPDV - Packet Delay Variation
   - IP delay variation

Link Layer Statistics:
1. Traffic Volume
   - byte rate (related to L2 PDUs)

Component for Jitter Compensation - MG internal statistics:
1. Statistics related to the control of dejitter buffers
   - number of jitter buffer adaptation events

Figure J.1: Categories of Statistics - Some example metrics (not exhaustive list; list is also not correlated to a specific Ia profile version)

NOTE: Even if statistics are shown on e.g. IP level, they could require higher level awareness inside the BGF.

The aspect of protocol layer Lx-based performance measurements is relevant in respect of BGF modes of operation (see annex I). E.g. the SPDF request of a transport-protocol agnostic mode, together with a request of application related performance metrics, is inconsistent.

NOTE: The BGF reaction on such a control activity is not yet defined in existing profile versions [i.1], [i.2] and [i.3].

Or vice versa: the demand of specific protocol layer Lx-related performance measurements could impact the enforced BGF mode.

History

Document history		
V3.1.1	August 2009	Publication