

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.64

(12/2009)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication
procedures

Gateway control protocol: IP router packages

Recommendation ITU-T H.248.64



ITU-T H-SERIES RECOMMENDATIONS
AUDIOVISUAL AND MULTIMEDIA SYSTEMS

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

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

Recommendation ITU-T H.248.64

Gateway control protocol: IP router packages

Summary

Recommendation ITU-T H.248.64 has in scope ITU-T H.248 media gateways with connection models using only IP-based ITU-T H.248 streams/terminations. The different modes of IP packet forwarding (in the ITU-T H.248 bearer path) are described. This Recommendation further defines an ITU-T H.248 package for discriminating such modes and protocol elements for the so-called IP router forwarding method. Further ITU-T H.248 packages provide capabilities for service enhanced packet forwarding with respect to the support of additional network address translation.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.248.64	2009-12-14	16

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2010

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	Page
1 Scope	1
1.1 Applicability	1
2 References.....	2
3 Terms and Definitions	2
3.1 Terms defined elsewhere	2
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	3
5 Conventions	4
6 Overview – IP packet forwarding in ITU-T H.248 media gateways.....	5
6.1 Unidirectional model	5
6.2 Model for back-to-back IP host (B2BIH) mode.....	5
6.3 Model for native IP router (IPR) mode	7
6.4 MG-embedded router versus router-embedded MG	8
6.5 IPR mode	8
7 Traffic separation for B2BIH and IPR mode processing.....	11
7.1 Discrimination criteria – Disjoint address spaces for local hosts and remote hops and hosts	11
7.2 "Local" delivery and context delivery decisions	12
8 IP-to-IP MG types – Mix of B2BIH and IPR mode processing.....	13
8.1 Hybrid B2BIH-IPR media gateway.....	13
8.2 B2BIH-only media gateway	13
8.3 IPR-only media gateway	14
9 IP Router Package.....	14
9.1 Properties	14
9.2 Events	16
9.3 Signals	19
9.4 Statistics.....	19
9.5 Error codes.....	19
9.6 Procedures	19
10 IP Router NAT Package	21
10.1 Properties	21
10.2 Events	24
10.3 Signals	27
10.4 Statistics.....	27
10.5 Error codes.....	27
10.6 Procedures	27

	Page
Appendix I – Routing tables and relation to route IPR contexts	32
I.1 Routing domains.....	32
I.2 Route advertisement and process of building tables	33
I.3 Interface IPR context and IIPR termination	37
Bibliography.....	38

Recommendation ITU-T H.248.64

Gateway control protocol: IP router packages

1 Scope

An ITU-T H.248 media gateway (MG) may provide ITU-T H.248 IP-to-IP contexts, which implies an *IP forwarding function* (in the ITU-T H.248 bearer path or IP data path). There are many different forwarding functions possible, dependent on the set of packet processing functions executed, and dependent on whether the MG behaves as a *host* or a *hop* system. Two basic forwarding functions may be identified:

- Back-to-back IP host (B2BIH) mode.
- IP router (IPR) mode.

The B2BIH mode is inherently supported by the ITU-T H.248.1 protocol architecture; the IPR mode is addressed within this Recommendation. In the IPR mode, if IP packets are routed between a private network and a public network, network address translation (NAT) functionality is also supported by this Recommendation.

1.1 Applicability

1.1.1 Applicability of the B2BIH mode

This mode is applied in case that an ITU-T H.248 context provides either:

- a single IP host entity (like a physical-to-IP context for residential, access or trunking media gateways); or
- back-to-back host configurations as, e.g., required for *service interworking* [ITU-T Y.1251] above the IP layer (between two IP domains) or L3 address translations, i.e., whenever the IP stack must be entirely terminated.

1.1.2 Applicability of the IPR mode

This mode provides the basic IP router functions and may be also applied with additional routing/forwarding behaviours, e.g.:

- forwarding of session-individual IP bearer traffic;
- forwarding of IP-based signalling traffic;
- forwarding of aggregated IP traffic;
- forwarding with specific NAT behaviour;
- MG-embedded IP edge router (IPER);
- MG-embedded DiffServ IP edge router (DER);
- MG-embedded MPLS label edge router (LER);
- congestion control for IP traffic.

This Recommendation supports IP unicast forwarding. Multicast forwarding (see clause 5.2.1.3 of [IETF RFC 1812]) is basically covered by the design of the ITU-T H.248.64 packages, but details are left for future study.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T H.248.1] Recommendation ITU-T H.248.1 (2005), *Gateway control protocol: Version 3* (including its Amendments 1 and 2).
- [ITU-T H.248.43] Recommendation ITU-T H.248.43 (2008), *Gateway control protocol: Packages for gate management and gate control*.
- [ITU-T Y.1251] Recommendation ITU-T Y.1251 (2002), *General architectural model for interworking*.
- [IETF RFC 1122] IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers*.
- [IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.
- [IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.
- [IETF RFC 3022] IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT)*.
- [IETF RFC 4292] IETF RFC 4292 (2006), *IP Forwarding Table MIB*.
- [IETF RFC 4787] IETF RFC 4787 (2007), *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*.

3 Terms and Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 external (address/network), clause 3.1.3 in [ITU-T H.248.43]: A global or public network is an address realm with unique network addresses assigned by Internet Assigned Numbers Authority (IANA) or an equivalent address registry. This network is also referred to as an external network during NAT discussions.

3.1.2 internal (address/network), clause 3.1.2 in [ITU-T H.248.43]: A private network is an address realm independent of external network addresses. A private network may also be referred to as a local network. Transparent routing between hosts in private realm and external realm is facilitated by a NAT router.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 back-to-back IP host (B2BIH) mode: A context of two or more IP-based terminations, where each termination appears to the rest of the network as an IP host (in contrast to an IP router).

3.2.2 IP forwarding: An IP packet forwarding process following the requirements set given by clause 5.2 of [IETF RFC 1812].

NOTE – IETF RFC 1812-conformant forwarding is also called "classical IP forwarding" function.

3.2.3 interface IP router (IIPR) termination: An IP-based ITU-T H.248 physical (Note 1) termination, belonging to an ITU-T H.248 context of type "IIPR". An IIPR termination is consistent with clause 6.2 of [ITU-T H.248.1], i.e., "sources and/or sinks media". An IIPR termination is tightly coupled to a local layer 2 logical interface in a 1:1 relationship. That layer 2 logical interface (inclusive of the assigned IP interfaces) may thus not be shared (Note 2) by other IIPR or B2B IP terminations (Note 3).

NOTE 1 – The rationale behind this is the persistence of an IP interface associated to an IP router entity. It may be noted that an "ITU-T H.248 physical IP termination" may still represent either a physical or a logical IP interface.

NOTE 2 – The rationale behind this is the underlying lookup process for (IP) packet-to-"IIPR context/termination" assignment. The lookup-key is derived from the forwarding information base (FIB), which relates to the tuple of {NetworkID, Mask} in case of native/classical IP forwarding. The element 'NetworkID' represents L3 destination address (DA) information only (which is tightly coupled to the L2 logical interface, due to local L3-to-L2 address bindings) thus, no L4 (or other PCI) is used for packet classification.

NOTE 3 – Whether the MG resource of a logical layer 2 interface may be shared or not is dependent on the applied lookup-key (e.g., a 1-tuple lookup-key, using the identifier of the logical layer 2 interface as single element, does not allow to share that interface).

3.2.4 IP router (IPR) mode: A dual-homing configuration (for unicast traffic) in next hop mode. The native IPR mode relates to a classical IP forwarding function, i.e., a media-agnostic and transport-protocol-agnostic per-hop behaviour (PHB) of IP packets.

3.2.5 route IP router (RIPR) termination: A virtual ITU-T H.248 ephemeral termination, belonging to an ITU-T H.248 context of type "RIPR". An RIPR termination is based on clause 6.2 of [ITU-T H.248.1], but without the capability to "source and/or sink media". This limits the number of characterizing properties for this termination type. An RIPR termination defines information of a partial or entire forwarding information base (FIB) entry. The addition of further RIPR terminations to the context is for further study.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABNF	Augmented Backus-Naur Form
AS	Autonomous System
B2B	Back-to-Back
B2BIH	Back-to-Back Internet protocol Host (mode), also briefly "B2B"
BGP	Border Gateway Protocol (an IP routing protocol)
DA	Destination Address (IP)
DER	DiffServ IP Edge Router
DiffServ	Differentiated Services (IETF QoS concept)
ER	Edge Router (IP)
FIB	Forwarding Information Base
H	Host (IP)
IIPR	Interface Internet Protocol Router
IP	Internet Protocol
IPER	Internet Protocol Edge Router

IPR	Internet Protocol Router (mode)
LD	Local Descriptor/Local Destination (IP connection endpoint)
LER	(MPLS) Label Edge Router
LS	Local Source (IP connection endpoint)
Lx	(protocol) Layer x (x = 1, 2 or 3)
LxVPN	(protocol) Layer x Virtual Private Network (x = 2 or 3)
MAC	Media Access Control
MD	Media Descriptor
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NIPR	Network address translation Internet Protocol Router
OSPF	Open Shortest Path First (an IP routing protocol)
PCI	Protocol Control Information
PHB	Per-Hop Behaviour
QoS	Quality of Service
R	Router (IP)
RD	Remote Descriptor/Remote Destination (IP connection endpoint)
RIB	Routing Information Base
RIP	Routing Information Protocol (an IP routing protocol)
RIPR	Route Internet Protocol Router
RS	Remote Source (IP connection endpoint)
RTCP	Real-time Transport control protocol
SA	Source Address (IP)
SCTP	Signalling Control Transmission Protocol
SDP	Session Description Protocol
SNMP	Simple Network Management Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
TTL	Time-To-Live (IP)

5 Conventions

This Recommendation refers to the generic and IP connection relevant "connection endpoint naming conventions" according to clause 5.2 of [ITU-T H.248.1].

@ is used to denote an (IP network) address.

6 Overview – IP packet forwarding in ITU-T H.248 media gateways

6.1 Unidirectional model

An ITU-T H.248 MG may provide one or multiple IP interfaces (logical or physical IP interfaces) for bearer traffic. The MG is then a single-homed or multi-homed IP node type. MGs with at least one physical IP interface and at least two logical IP interfaces per MG are considered, i.e., at least a dual-homed IP MG.

Any incoming IP packet is forwarded to an outgoing IP interface. This unidirectional view is the basic model for IP flows. Figure 1 illustrates such a model for an ITU-T H.248 MG. The bearer traffic relates to IP flows going through IP-to-IP contexts. The fact that ITU-T H.248 streams are bidirectional communication paths is not relevant for the model here.

There are k ingress and m egress IP interfaces in the unidirectional model shown in Figure 1. The assumption that each IP route may be used in a bidirectional manner ($k = m$) is typically valid in practice and shall hold thus also for this Recommendation. The process of IP packet forwarding comprises the transfer function to relay a received packet from interface x_i to egress interface y_j . Two basic modes of operation for IP forwarding may be considered (see the following clauses) from an ITU-T H.248 MG point of view.

The differences between both IP forwarding modes are mainly related to the handling of IP header address information and the determination of the egress IP interface.

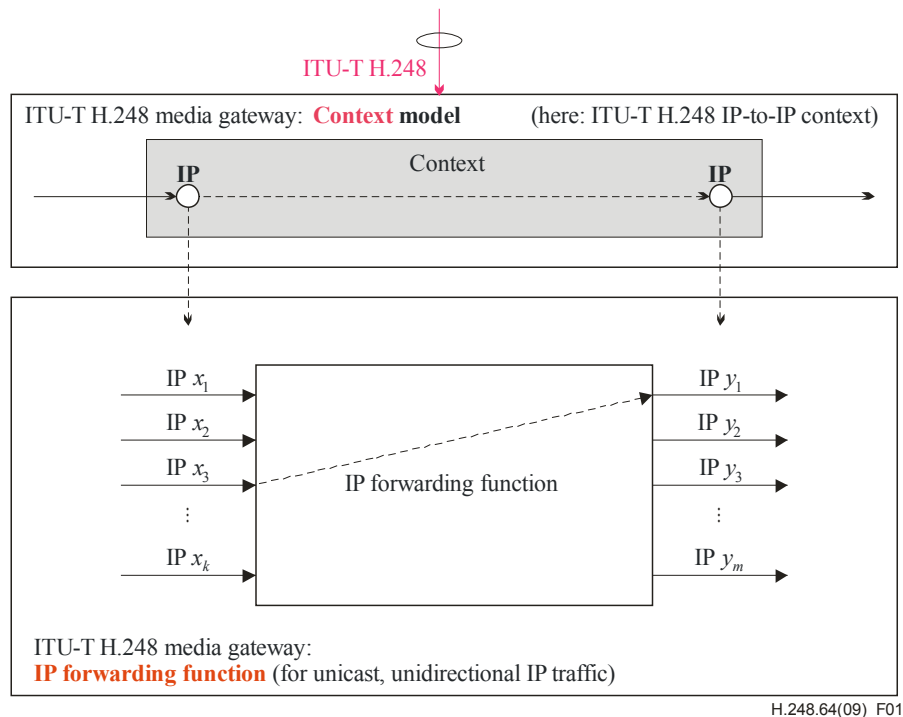


Figure 1 – IP packet forwarding in multi-homed IP ITU-T H.248 media gateways

6.2 Model for back-to-back IP host (B2BIH) mode

Figure 2 illustrates the model for the back-to-back IP host (B2BIH) mode. Any IP packet received at interface x_i has the DA x_i : the interface represents the *destination host* (see [IETF RFC 1812]) for such a packet. Network address DA x_i relates to the ITU-T H.248 *local destination* address LD(A) (of the IP connection *endpoint*, represented by termination Ta). The IP packet is forwarded and sent at interface y_j with SA y_j : the interface represents thus the *source host*. Network address SA y_j relates to the ITU-T H.248 *local source* address LS(A) (of termination Tb). ITU-T H.248 IP

terminations Ta and Tb relate therefore to the *destination host* and *source host* respectively, in the B2BIH *host* model.

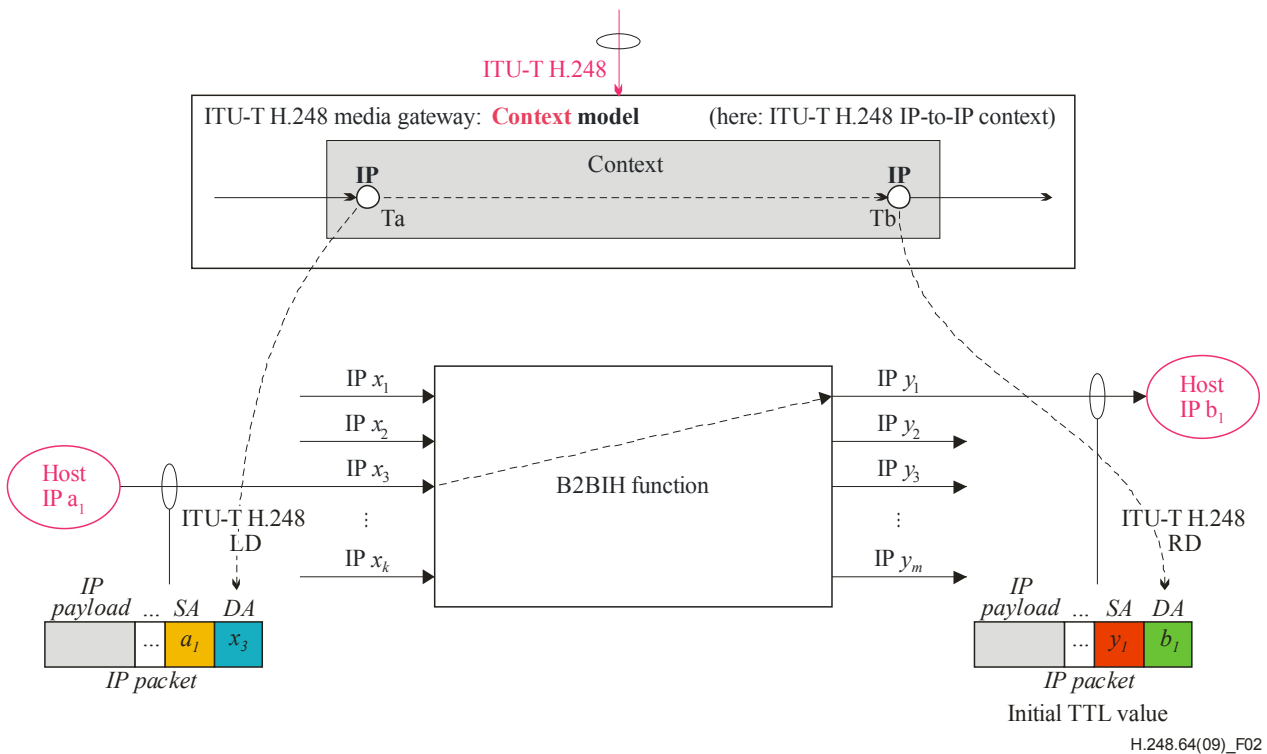


Figure 2 – Model for back-to-back IP host (B2BIH) mode

The major characteristics of the B2BIH mode are:

- 1) IP header processing:
 - a) Address fields: *inherent* network address translation (NAT) function.
 NOTE 1 – If a NAT-less mode is explicitly enforced, see, e.g., [b-ETSI TS 183 018].
 - IP SA field: Ta: *remote source* address RS(A = a_1) → translated to Tb: *local source* address LS(A = y_1).
 - IP DA field: Ta: *local destination* address LD(A = x_3) → translated to Tb: *remote destination* address RD(A = b_1).
 - b) Other header fields: according to regular *host* packet processing (see [IETF RFC 1122]), e.g., initial TTL value setting for outgoing packets.
 NOTE 2 – Native host behaviour may be overruled, e.g., due to security goals in hiding network topology.
- 2) Determination of next hop: given by ITU-T H.248 *context topology*.
 - IP interfaces y_1 and x_3 are associated with the ITU-T H.248 context.
 - In general, *unicast* forwarding is related to a *two* termination context. Such a connection model may be also used for *multicasting*, however multicasting may also be achieved with more than two terminations and corresponding topology settings.
 - FIB: very small table (dependent on number of terminations per context and number of streams per termination); e.g., one row entry in the simplest case.

The B2BIH mode divides an end-to-end (or peer-to-peer) IP connection into two bearer legs.

6.3 Model for native IP router (IPR) mode

The classical IP forwarding function is defined by [IETF RFC 1812], see Figure 3. The major difference to the B2BIH mode is in IP address processing. The MG (or context) acts as *next hop*, which means that neither the SA nor the DA information is modified by the hop.

This means that there is no *direct* relation (as in the B2BIH mode) between network addresses b_1 (DA) and x_3 (interface) from the *hop* perspective.

NOTE 1 – The relation between b_1 and x_3 is a *network* level aspect (due to IP routing). The *previous hop* determined an IP route with *next hop* address x_3 for IP destination address b_1 . This IP route is not dedicated only for destination b_1 in general, it is rather for many different destination addresses or address ranges (subnets), dependent on the network topology (and the current visible routing topology is stored in the local routing information base (RIB)). That means that interface x_3 may theoretically receive IP packets with *any* DA value.

The ITU-T H.248 *local destination* address x_3 (represented by termination Ta) is thus not tightly coupled with *remote destination* address b_1 .

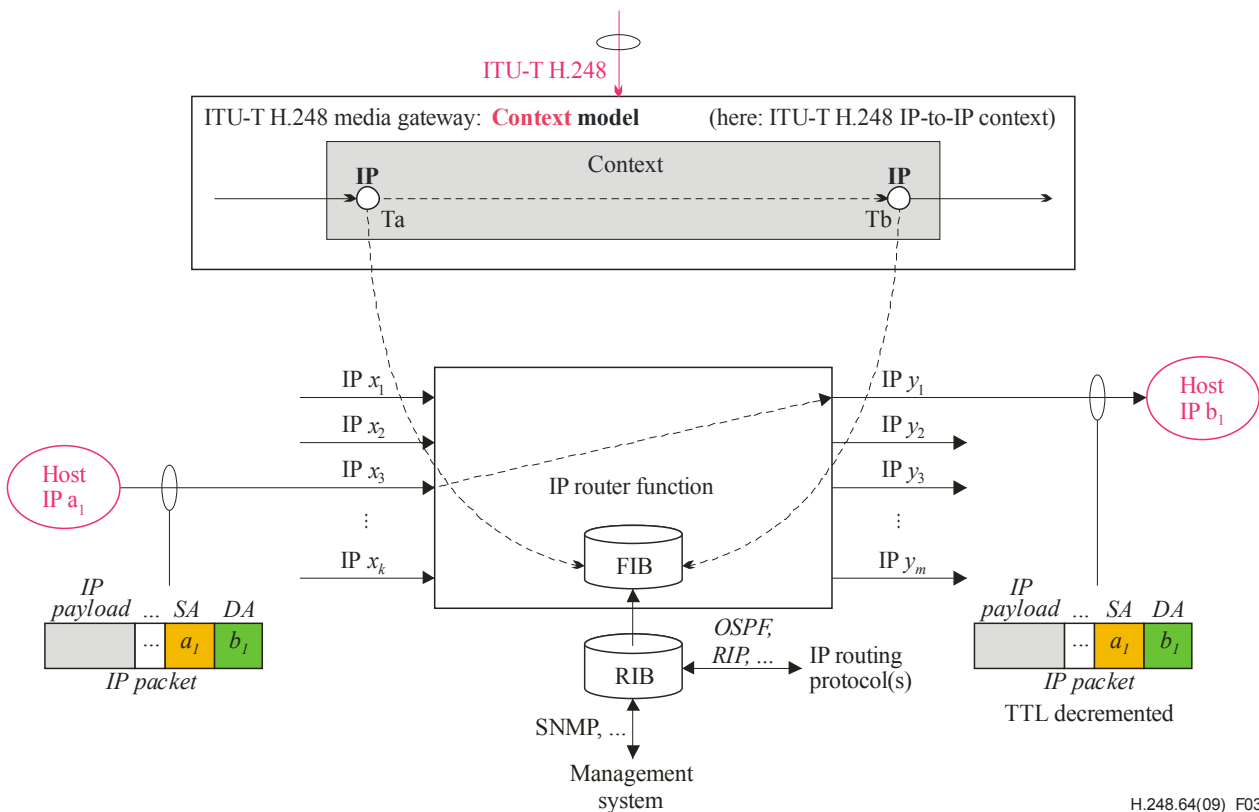


Figure 3 – Model for native IP router (IPR) mode

There is a similar situation for the egress direction and the relation between ITU-T H.248 local source address y_1 (represented by termination Tb) and remote source address a_1 .

The packet forwarding between Ta and Tb (within the context) is controlled via the context-associated FIB. Many FIB structures are possible, e.g., in case of "destination address"-only based routing would lead DA b_1 to a next hop determination behind interface y_1 . The definition of a specific FIB structure is thus out of scope of this Recommendation.

Figure 3 indicates the local FIB, which may provide a self-contained provisioning access interface, or an interface to the MG local RIB, which again may provide an SNMP-based provisioning interface (for static route configuration, see clause 7.4 of [IETF RFC 1812]) and/or routing protocol interfaces.

NOTE 2 – SNMP is mandatory for IP routers (see clause 8.1 of [IETF RFC 1812]).

Major characteristics of the native IPR mode:

- 1) IP header processing:
 - a) Address fields: no NAT per default. This may be achieved, e.g., by "local and remote descriptor"-less ITU-T H.248 IP terminations, or even "media descriptor"-less ITU-T H.248 IP terminations. The descriptors would be then omitted in the ADD.request command for the IP termination (see, e.g., clause 9.6.1.2).
 - b) Other header fields: according to regular next hop packet processing (see [IETF RFC 1812]), e.g., TTL value decrease for outgoing packets.
- 2) Determination of next hop (i.e., interface IP_{yi}): given by a FIB, the FIB may be associated to an ITU-T H.248 context. The FIB table size depends primarily on the set of remote destination addresses b_i (per ingress termination T_a).

This forwarding mode describes very basic per-hop behaviour (PHB). Such a PHB may be augmented by many different IP services. Such services are out of scope of this Recommendation.

6.4 MG-embedded router versus router-embedded MG

The "IP router function" may be realized in a stand-alone manner or be embedded in another system (see clause 2.2.8.1 of [IETF RFC 1812]). Figure 3 illustrates an MG-embedded IP router function. On the other hand, it may be noted that an ITU-T H.248 MG function may also be embedded in a stand-alone IP router as a "router-embedded MG function".

6.5 IPR mode

6.5.1 Basic concepts

The IPR mode context model consists of three concepts:

- 1) **The interface IPR (IIPR) context:** This context describes the connections between the different IP interfaces (and underlying local L2 interfaces) originated/terminated on an MG. This is as per a normal ITU-T H.248 connection model where all terminations connected to a context are "bothway" connected to each other (unless modified by topology). Thus, a packet arriving at an interface/termination has the possibility to leave on any other termination in the context. No routing information is described in the context itself, the routing table is described elsewhere. This context would allow interface-based traffic monitoring, filtering and statistics gathering. This usage of terminations/contexts aligns with clause 6.2 of [ITU-T H.248.1] to describe a multiplexed bearer.
- 2) **The route IPR (RIPR) context:** This context describes a single route entry in the routing table. In this way, when a routing context is created, an entry is added to the table. There are one or more terminations in the route IPR context. When those terminations are subtracted, then the route entry is deleted. It would also allow existing ITU-T H.248 statistics, properties, events to be used to enable route-based traffic management, filtering and statistic gathering. This type of context is labelled a route IPR context and the terminations in it do not contain address information in the local and remote descriptors (basically, it is a "virtual connection").

- 3) **The NAT IPR (NIPR) mapping context:** This context describes a single NAT mapping entry in the NAT mapping table. In this way, when a NAT IPR context is created, an entry is added to the table. There are two terminations in the NAT IPR context. When those terminations are subtracted, then the NAT mapping entry is deleted. It also allows the use of existing ITU-T H.248 statistics, properties and events to enable NAT-based traffic management, filtering and statistic gathering. This type of context is labelled a NAT context. As per the route IPR context, the terminations in the NAT IPR context do not contain address information in the local and remote descriptors.

To tie the concepts together, a correlation identifier is needed in order to tie a particular route IPR context and optionally a NAT IPR context with an interface IPR context. In this way, the MGC can describe distinct routing and NAT tables based on sets of interfaces. An interface IPR context then uses this correlation identifier to build a routing table. The NAT mapping information provides a link to the interface IPR context.

6.5.2 Information for routing and/or address translation

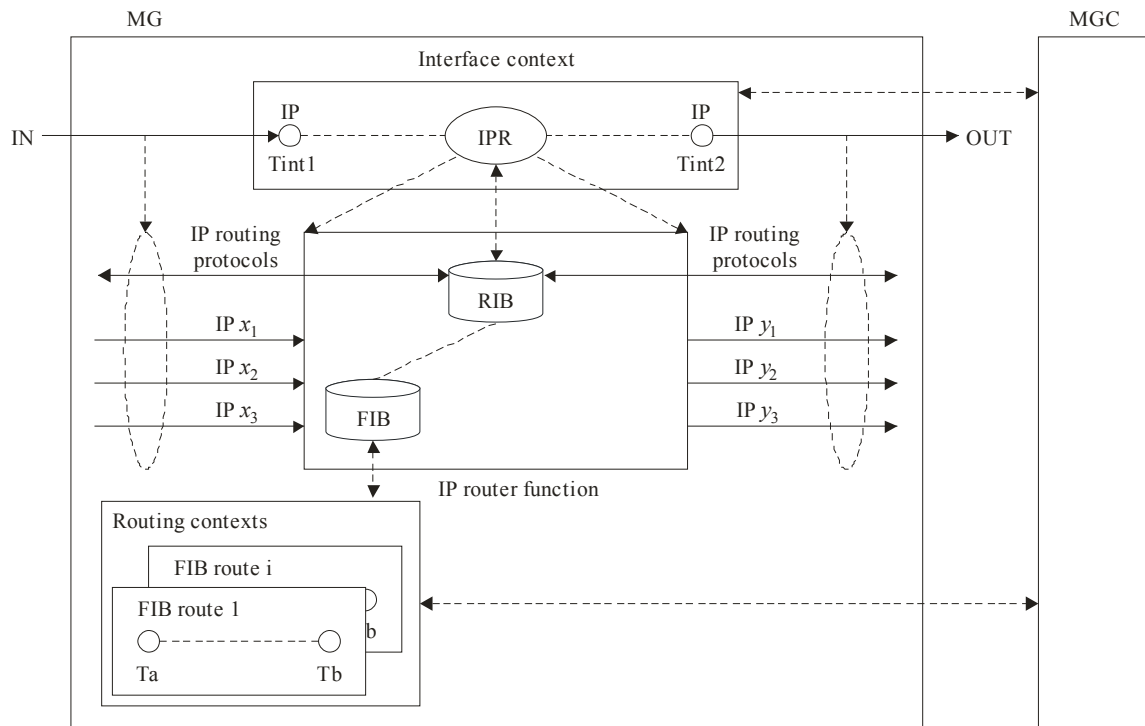
The terminations in the interface context may also terminate/originate dynamic routing protocols such as routing information protocol (RIP), open shortest path first protocol (OSPF) and border gateway protocol (BGP). Any need for modification of routing table data could then be notified to the MGC, which can then modify the routing contexts; this, in turn, would trigger an update to the routing table data.

Likewise, a need for modification of the MG NAT mapping table data could then be notified to the MGC, which can then modify the NAT IPR contexts; this, in turn, would trigger an update to the NAT mapping table data.

As an interface may have a large number of routes/NAT entries associated with it, further event parameters may be utilized to provide a means for controlling the signalling load to the MGC.

6.5.3 Context models for (MG-embedded) IP router function

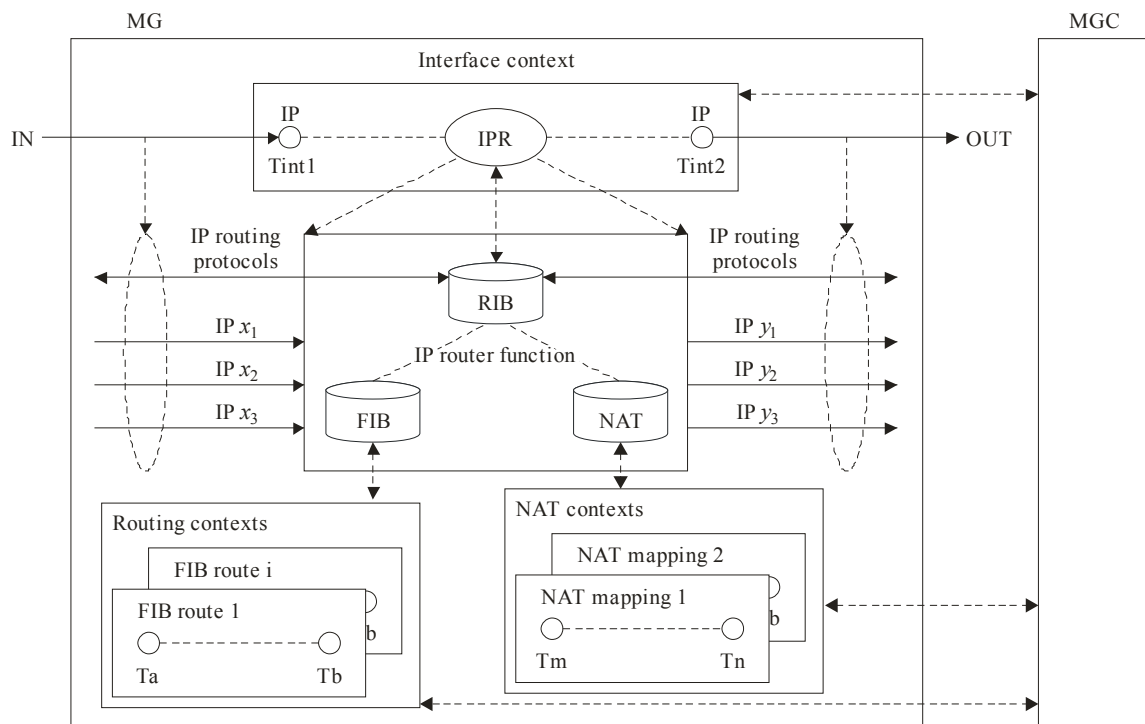
Figures 4 and 5 illustrate the models. Figure 4 illustrates the relationship between the different contexts and functions to provide routing of an IP packet. NAT functionality may also be supported when necessary, see Figure 5.



NOTE – The example RIPR contexts show two RIPR terminations, whereas a single termination is sufficient for IETF RFC 1812 router functions.

H.248.64(09)_F04

Figure 4 – IPR mode context model – RIPR contexts only



NOTE – The example RIPR contexts show two RIPR terminations, whereas a single termination is sufficient for IETF RFC 1812 router functions.

H.248.64(09)_F05

Figure 5 – IPR mode context model – RIPR and NIPR contexts

6.5.4 Creation of IP router function (IIPR Context)

The MGC creates an MG-embedded IP router function by adding k IIPR terminations from the NULL context into a dedicated IIPR context (see also clause 9.6.1.2). Each IIPR termination relates to an MG-local logical layer 2 interface. The ITU-T H.248 termination name shall contain an element for unambiguous indication of the layer 2 interface, which shall be realized by including the field "*InterfaceID*" (see clause 9.1.2) in the TerminationID.

NOTE – The MGC is aware of all IIPR terminations due to their physical type and underlying NULL context.

6.5.5 Processing of IP packets and IP routing protocols

An IP packet received at the MG arrives on an IP interface (logical or physical). The packet handler determines to which type of context (B2B or interface IPR) the packet is delivered; in this case, it is delivered to an IP routing interface context. From the FIB information, the MG will determine the route and interface that the packet will be sent on from the MG. The MG determines the FIB routing table information based on the routing IPR contexts and thus maintains a routing ContextID to route table entry mapping. The MGC manages these routing IPR contexts based on static provisioning data and/or dynamically via IP routing protocol information received on the IP interfaces. So, whilst the MG is responsible for routing protocol signalling and determining what dynamic updates need to be made to the FIB routing table, it indicates the necessary updates to the MGC for it to appropriately configure the routing IPR contexts.

6.5.6 Additional IP address translation

Where an IP packet is routed between private and public networks, or between two private networks, NAT is needed. An MG acts as a NAT router in this case. The MG determines the NAT address mapping based on the NAT IPR contexts and thus maintains a NAT ContextID to NAT mapping entry mapping. The MGC manages these NAT contexts based on static provisioning data and/or dynamically via NAT mapping information caused by packets received on the IP interfaces. So, whilst the MG is responsible for determining what dynamic updates need to be made to the NAT mapping table, it indicates the necessary updates to the MGC for it to appropriately configure the NAT IPR contexts.

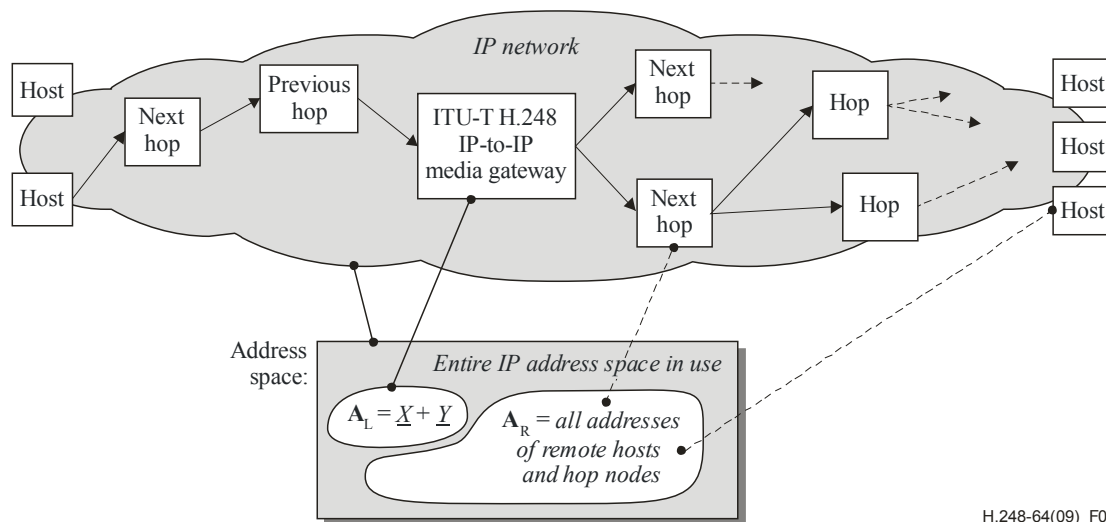
7 Traffic separation for B2BIH and IPR mode processing

Any received IP packet (in the MG bearer path) must be delivered to the associated context. This clause describes the basic principle, for native IETF RFC 1812 routers, where the IP destination address is the only element used of an incoming packet for forwarding and routing decisions.

7.1 Discrimination criteria – Disjoint address spaces for local hosts and remote hops and hosts

7.1.1 Single or non-overlapping realms

The fundamental discrimination criteria is the IP address space because there are *two, disjoint* sets of IP address spaces A_L and A_R (see Figure 6). The MG may be again considered as a *multi-homed IP host* concerning the set of network addresses $\underline{X} = \{x_1, x_2, \dots, x_k\}$ and $\underline{Y} = \{y_1, y_2, \dots, y_m\}$ (see Figure 1) for its (local) IP interfaces. Remote host and hop systems are assigned with disjoint addresses (from an MG perspective, see also clause 7.1.2).



**Figure 6 – Discrimination criteria –
Disjoint address spaces for local hosts and remote hops and hosts**

7.1.2 Overlapping remote realms

Figure 6 omits the possibility of NAT devices, i.e., the separation of the entire address space into multiple, possibly overlapping, address realms. When the MG is connected to multiple realms, then it is possible that these realms lead to an overlapping address values in A_R (see Figure 7). However, the two sets of IP address spaces A_L and A_R would be still disjoint.

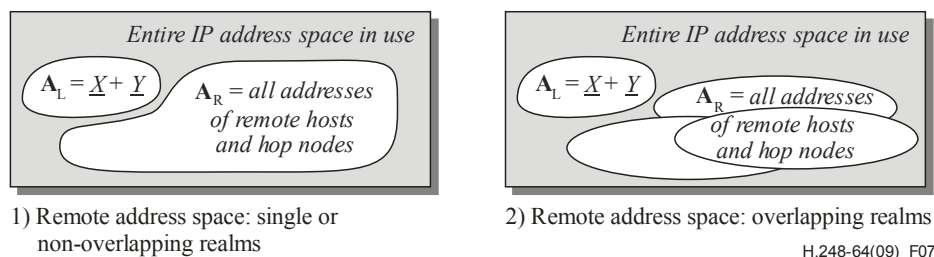


Figure 7 – Discrimination criteria – Overlapping remote realms

7.1.3 Overlapping local and remote address spaces

The MG may be a member itself of one or more realms when connected to multiple realms. This could lead to an overlapping of local and remote address spaces A_L and A_R . An additional discrimination criterion is then required (as usual for overlapping L3VPN or L2VPN address spaces); for example, an L2VPN identifier (e.g., the VLAN tag in the case of Ethernet).

7.2 "Local" delivery and context delivery decisions

Figure 8 illustrates the packet-to-context assignment process. Any received IP packet must firstly be checked against the "IP header validation" rules according to clause 5.2.2 of [IETF RFC 1812]. The next processing step is the "local delivery decision" according to clause 5.2.3 of [IETF RFC 1812]. This decision will lead to a separation into *control path* (i.e., IP packets with destination to the MG itself) and *data path* (or *bearer path*) traffic; and a further *data path* traffic separation into B2BIH and IPR traffic (Figure 8 shows the *bearer path* only).

The "*local*" delivery decision is primarily based on the DA value (see previous subclause) of the received IP packet: any DA matching the *local* space A_L is forwarded to the *context delivery decision* for the B2BIH path, and vice-versa for the IPR path.

Packet forwarding model (Ingress-to-context):

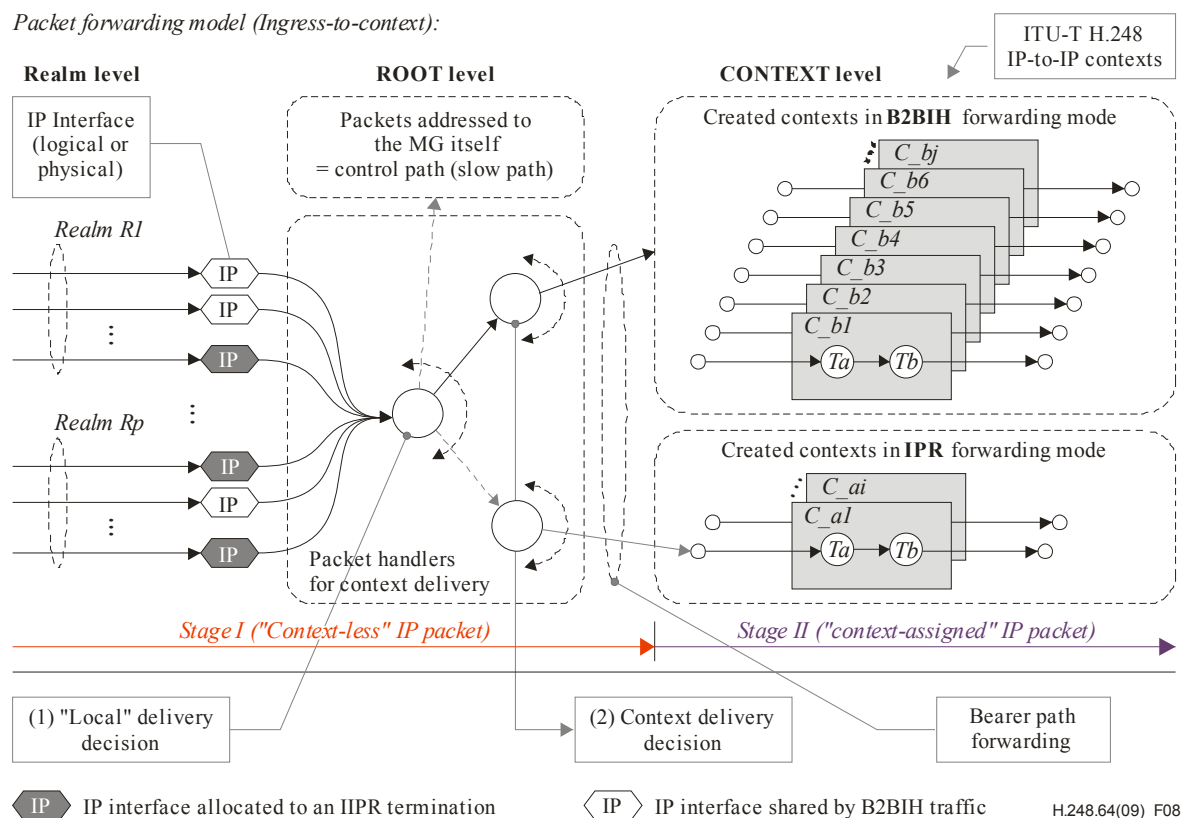


Figure 8 – Packet-to-context assignment – Multi-stage decision process

The subsequent *context delivery decision* functions (for each bearer path) may use other, different and/or additional information elements for packet-to-context assignment.

For instance, the context delivery decision function for B2BIH context types is general based on n -tuple information (also known as *vectors*) for assignment.

For example, a media-agnostic, transport-protocol-aware B2BIH context may carry three IP transport connections as three separate ITU-T H.248 streams. The local IP addresses may be identical, but the transport ports may be different for each stream. A 2-tuple might be then sufficient for packet-to-context assignment.

NOTE – There are furthermore context-to-termination and termination-to-stream assignment functions. However, this is usual ITU-T H.248 processing and thus out of scope of this Recommendation.

8 IP-to-IP MG types – Mix of B2BIH and IPR mode processing

There may be different MG types due to the particular number of created contexts per data path forwarding mode.

8.1 Hybrid B2BIH-IPR media gateway

There are n B2BIH type contexts and m IPR type contexts created (and n and m are greater than zero).

8.2 B2BIH-only media gateway

There are contexts that are only of the B2BIH type. The border MG controlled via the ITU-T H.248 *ETSI_BGF* profile (defined by [b-ETSI TS 183 018] and used over the "*Ia* Interface") is an example of such an MG type.

8.3 IPR-only media gateway

The number of route IPR contexts may vary significantly.

8.3.1 Native IPR forwarding only

Native IPR forwarding denotes again the IETF RFC 1812-conformant, mandatory part of the forwarding data path element. One interface IPR context may be sufficient. Each FIB route entry is saved in a single route IPR context.

8.3.2 Service-enhanced IPR forwarding

Service-enhanced IPR forwarding comprises all functions that may be overlaid on the basic forwarding, e.g., QoS support, traffic control, DiffServ PHBs, policy enforcement (e.g., filtering), traffic metering, etc. There may then be multiple interface IPR contexts, which depend on whether the service was interface- or route-based.

8.3.2.1 IPR forwarding with NAT

NAT functionality defined in [IETF RFC 3022] may also be supported when necessary. The number of NAT IPR contexts will vary with the number of NAT mappings.

8.3.2.2 IPR forwarding with filtering

Policy enforcement via filtering may also be supported when necessary. Such filtering will have an impact on "local" delivery and context delivery decisions (see clause 7.2). Policy enforcement (e.g., filtering) may be achieved on terminations via the use of [ITU-T H.248.43].

NOTE – The definition of complementary filtering capabilities is out of scope of this Recommendation. Other Recommendations of the ITU-T H.248 series may provide additional filtering support.

9 IP Router Package

Package Name: IP Router Package

PackageID: ipr (0x00d4)

Description: This package provides protocol elements for support of a dedicated IP packet forwarding mode in the ITU-T H.248 bearer path (or IP data path).

Version: 1

Extends: None

9.1 Properties

9.1.1 IP forwarding mode

Property Name: IP forwarding mode

PropertyID: ifm (0x0001)

Description: This property indicates the IP forwarding mode for a context. Such a context contains only IP-based terminations. The particular forwarding mode is a context-level property. The particular forwarding mode is a property which is valid for the whole lifetime of the context. The forwarding mode shall not be changed. This property allows the MGC to distinguish three context types: *back-to-back IP host* (B2BIH) mode, interface *IP router* (IIPR) mode and route *IP router* (RIPR) mode.

Type: Enumeration

Possible values: "B2B" (0x0001): Back-to-back IP host mode
 "IIPR" (0x0002): Interface IPR context type of IP router mode
 "RIPR" (0x0003): Route IPR context type of IP router mode

Default: "B2B" (0x0001)

Defined in: ContextAttribute Descriptor

Characteristics: Read/write

9.1.2 Forwarding information base

Property Name: Forwarding information base

PropertyID: fib (0x0002)

Description: This property provides single route entry in the routing table. This property is only relevant for "RIPR" context types.

Type: String

Possible values: A string having the format of *fibentry* defined by the following augmented Backus-Naur Form (ABNF):

```

fibentry = NetworkID "|" Mask "|" Cost "|" [NextHopID]
          "|" InterfaceID
NetworkID = domainAddress
           ; domain Address defined in
           ; clause B.2 / [ITU-T H.248.1]
Mask = "/" UINT16
       ; a bit mask using slash notation may be specified
       ; using the UINT16, for example "[11.9.19.65]/23"
       ; indicates the number of leading one bits that
       ; form the mask to be logical-ANDed with the IP
       ; destination address before being compared to the
       ; value in the FIB NetworkID field
Cost = UINT32
      ; an abstract cost factor of the IP route
      ; UINT32 defined in clause B.2 of [ITU-T H.248.1]
NextHopID = domainAddress
           ; IP address of the next hop (either an IP router
           ; or an IP host)
InterfaceID = UINT32
            ; the local L2 interface used for forwarding

```

NOTE 1 – The FIB element InterfaceID is also part of the name of an IIPR Termination, see clause 6.5.4.

NOTE 2 – The above field elements of a FIB entry, as well as their syntax, are consistent with the IETF MIB for IP forwarding tables [IETF RFC 4292]. This approach allows the support of additional FIB elements in case of provisioned RIPR contexts. This is related to configuration management and thus out of scope of this Recommendation.

Default: Provisioned

Defined in: ContextAttribute Descriptor

Characteristics: Read/write

9.1.3 Interface context identifier

Property Name: Interface context identifier

PropertyID: ici (0x0003)

Description: This property indicates the ContextID of the related interface IPR context. This property is only relevant for "RIPR" context types.

Type: Integer

Possible values: 0x01 to 0xFFFFFFFFD.
Values 0x00, 0xFFFFFFFFE and 0xFFFFFFFFF are reserved.

Default: None

Defined in: ContextAttribute Descriptor

Characteristics: Read/write

9.1.4 Notifications rate

Property Name: Notifications rate

PropertyID: nr (0x0004)

Description: This property indicates the rate at which routing information notifications are sent to the MGC from the MG. The value of this parameter indicates the maximum number of routing information notification messages allowed to be reported to MGC per second. This property is only relevant for interface terminations in the interface IPR context.

Type: Integer

Possible values: 0 and up

Default: 1

Defined in: TerminationState Descriptor

Characteristics: Read/write

9.2 Events

9.2.1 New Route Reporting

Event Name: New Route Reporting

Event ID: nrr (0x0001)

Description: This event indicates a list of new route entries. This event is only relevant for interface terminations in interface IPR context.

9.2.1.1 EventsDescriptor parameters

9.2.1.1.1 Maximum list size

Parameter Name: Maximum list size

ParameterID: mls (0x0001)

Description: This parameter provides the maximum number of new route entries reported by one observed event.

Type: Integer

Optional: Yes

Possible values: 1 to 100

Default: 10

9.2.1.2 ObservedEventsDescriptor parameters

9.2.1.2.1 New route entries

Parameter Name: New route entries

ParameterID: nre (0x0001)

Description: This parameter provides a list of route entries which should be added to the route table.

Type: Sub-List of String

Optional: No

Possible values: A list of elements of type *fibentry* as defined by clause 9.1.2.

Default: None

9.2.2 Delete Route Reporting

Event Name: Delete Route Reporting

Event ID: drr (0x0002)

Description: This event indicates a list of route IPR ContextIDs of "Contexts" which should be deleted. This event is only relevant for interface terminations in interface IPR context.

9.2.2.1 EventsDescriptor parameters

9.2.2.1.1 Maximum list size

Parameter Name: Maximum list size

ParameterID: mls (0x0001)

Description: This parameter provides the maximum number of route IPR ContextIDs reported by one observed event.

Type: Integer

Optional: Yes

Possible values: 1 to 100

Default: 10

9.2.2.2 ObservedEventsDescriptor parameters

9.2.2.2.1 Route IPR Contexts

Parameter Name: Route IPR Contexts

ParameterID: ric (0x0001)

Description: This parameter provides a list of ContextIDs of route IPR contexts.

Type: Sub- List of Integer

Optional: No

Possible values: A list of integers.

The possible values of each element are 0x01 to 0xFFFFFFFFD.

Values 0x00, 0xFFFFFFFFE and 0xFFFFFFFFF are reserved.

Default: None

9.2.3 Modify Route Reporting

Event Name: Modify Route Reporting

Event ID: mrr (0x0003)

Description: This event indicates the modification of a list of route IPR contexts. This event is only relevant for interface terminations in interface IPR context.

9.2.3.1 EventsDescriptor parameters

9.2.3.1.1 Maximum list size

Parameter Name: Maximum list size

ParameterID: mls (0x0001)

Description: This parameter provides the maximum number of ContextIDs and route entries reported by one observed event.

Type: Integer

Optional: Yes

Possible values: 1 to 100

Default: 10

9.2.3.2 ObservedEventsDescriptor parameters

9.2.3.2.1 New route entries

Parameter Name: New route entries

ParameterID: nre (0x0001)

Description: There is a one-to-one relationship between the list positions of the *nre* and *ric* parameters, thus there shall be the same number of list positions. This parameter provides a list of route entries which are associated with a list of route IPR contexts.

Type: Sub-List of String

Optional: No

Possible values: A list of elements of type *fibentry* as defined by clause 9.1.2.

Default: None

9.2.3.2.2 Route IPR Contexts

Parameter Name: Route IPR Contexts

ParameterID: ric (0x0002)

Description: This parameter provides a list of route IPR ContextIDs in which the values of context attribute "fib" should be updated by the values provided in parameter "nre".

Type: Sub-List of Integer

Optional: No

Possible values: A list of integers.

The possible values of each element are 0x01 to 0xFFFFFFFFD.

Values 0x00, 0xFFFFFFFFE and 0xFFFFFFFFF are reserved.

Default: None

9.3 Signals

None.

9.4 Statistics

None.

9.5 Error codes

None.

9.6 Procedures

9.6.1 Successful context creation

9.6.1.1 Context creation of type "B2B"

A context of type "B2BIH" (or briefly "B2B") is created when the *ipr/ifm* property is set to "B2B" or is omitted in the action request.

9.6.1.2 Context creation of type "IIPR"

The MGC places interface terminations into the interface IPR context and designates that the context is of type "IIPR" through the *ipr/ifm* property (see also Table 1). Each interface termination represents a logical or physical L2 interface. MGC may create several interface IPR contexts on one MG. There is no IP forwarding between interfaces/terminations in different interface IPR contexts.

Table 1 – Example command encoding: Basic context creation of type "IIPR"

ITU-T H.248 encoding (shortened command)	Comments
<pre>MEGACO/3 [11.9.19.65]:54321 Transaction = 12345 { Context = \$ { ; Context in IPR mode ; Context properties ContextAttr = { ipr/ifm = "IIPR" ; Interface IPR mode Context indication } Add = ip/<group>/iipr/1 { ; Term. Ta } Add = ip/<group>/iipr/2 { ; Term. Tb } }</pre>	The IP forwarding mode is indicated by the context-level property <i>ipr/ifm</i>. The two ADD.request commands do not provide any <i>media descriptor</i> (MD-less ADDs). The TerminationID name is just an example. The termination name must contain the "<i>InterfaceID</i>" (which is '1' for Ta and '2' for Tb). The used prefix "ip" and field "iipr" may depend on the applied ITU-T H.248 profile. This example TerminationID structure is consistent with [b-ETSI TS 183 018].

9.6.2 Unsuccessful context creation scenarios

Unsuccessful context creation attempts shall be indicated by a correspondent error code by the MG.

9.6.3 Information base related procedures

9.6.3.1 Creation of a FIB for a context of type "RIPR"

The MG determines the FIB routing table information based on the routing IPR contexts and thus maintains a routing ContextID to route table entry mapping. The MG is responsible for routing protocol signalling on the interfaces in interface IPR contexts. As such it determines what dynamic updates need to be made to the FIB routing table and notifies the MGC of the necessary updates.

When the MG detects (see Note) one or more new route entries, the MG reports the information of new route entries to the MGC through the event "*ipr/nrr*". The MGC then creates a new route IPR context for each new route entry. The MGC should set the value of the context attribute "*ipr/ifm*" to "RIPR" (see also Table 2). The ContextID of its related interface IPR context should be set as the value of the context attribute "*ipr/ici*". The new route entry information should be saved in the context attribute "*ipr/fib*". Typically, one termination is added to the route IPR context; however, additional terminations may be used for enhanced services. The use of additional terminations is for further study. The MGC may also set properties for service-enhanced IPR forwarding on these terminations. Parameter "*mls*" of the event "*ipr/nrr*" is used to limit the maximum number of new route entries reported by one observed event.

NOTE – The detection is related to the associated interface, given by the FIB, which includes exactly one InterfaceID. The NOTIFY.req is thus issued on the IIPR termination matching that interface.

When the MG detects (see Note) that one or more route entries have changed, the MG reports those changes to the MGC through the event "*ipr/mrr*". The MGC indicates to the MG to modify the values of context attribute "*ipr/fib*" of the special route IPR contexts to the values of the MG reports. This allows the MGC to enforce any appropriate policy decisions. Parameter "*mls*" of the event "*ipr/mrr*" is used to limit the maximum number of modified route entries reported by one observed event.

When the MG detects (see Note) that one or more route entries are deleted, the MG reports them to the MGC through the event "*ipr/drr*". The MGC then subtracts the termination(s) in the indicated route IPR contexts, and thus deletes the related route information from the FIB. Parameter "*mls*" of the event "*ipr/drr*" is used to limit the maximum number of deleted route entries reported by one observed event.

Property "*nr*" is used to govern the rate at which routing information notifications are sent to the MGC from the MG. See clause 9.3 of [ITU-T H.248.1] for more information about notification rates.

Table 2 – Example command encoding: Creation of a FIB for a context of type "RIPR"

ITU-T H.248 encoding (shortened command)	Comments
<pre>MEGACO/3 [11.9.19.65]:54321 Transaction = 67890 { Context = \$ { ; Context in IPR mode ; Context properties ContextAttr = { ipr/ifm = "RIPR", ; route IPR Context indication ipr/ici = 10000, ;ContextID of the related Interface IPR Context ipr/fib = "xx xx xx xx xx" } Add = ip/iripr/1 { ; Termination Tc } } }</pre>	The IP forwarding mode is indicated by the context-level property <i>ipr/ifm</i>. The ADD.request command do not provide any <i>media descriptor</i> (MD-less ADDs). The TerminationID name is just an example. The used prefix "ip" field "<i>iripr</i>" and field "<i>oripr</i>" may depend on the applied ITU-T H.248 profile.

9.6.4 IP packet forwarding related procedures

An IP packet received at the MG arrives on an IP interface (logical or physical). The packet handler determines to which type of context (B2B or interface IPR) the packet is delivered. If the IP packet is delivered to an interface IPR context, the MG forwards the IP packet according to the route table information derived from the related route IPR context.

9.6.5 Loss of route reporting information

Any loss of route reporting information across the H.248 Control Association may lead to data inconsistency in RIB/FIB tables. The H.248 interface should thus use an assured transport mechanism like the SCTP based transport modes.

10 IP Router NAT Package

Package Name: IP Router NAT Package

PackageID: iprnat (0x0101)

Description: This package provides protocol elements for support of NAT functionality in an IP router mode.

Version: 1

Extends: None

10.1 Properties

10.1.1 IP forwarding mode

Property Name: IP forwarding mode

PropertyID: ifm (0x0001)

Description: This property indicates the IP forwarding mode for a context. Such a context contains only IP-based terminations. The particular forwarding mode is a context-level property. The particular forwarding mode is a property which is valid for the whole lifetime of the context. The forwarding mode shall not be changed. This property allows the MGC to distinguish four context types: *back-to-back IP host* (B2BIH) mode, *interface IP router* (IIPR) mode, *route IP router* (RIPR) mode and *NAT IP router* (NIPR) mode.

Type: Enumeration

Possible values: "B2B" (0x0001): Back-to-back IP host mode
"IIPR" (0x0002): Interface IPR context type of IP router mode
"RIPR" (0x0003): Route IPR context type of IP router mode
"NIPR" (0x0004): NAT IPR context type of IP router mode

Default: "B2B" (0x0001)

Defined in: ContextAttribute Descriptor

Characteristics: Read/write

10.1.2 Notifications Rate

Property Name: Notifications Rate

PropertyID: nr (0x0002)

Description: This property indicates the rate at which routing or NAT mapping information notifications are sent to the MGC from the MG. The value of this parameter indicates the maximum number of NAT mapping information notification messages allowed to be reported to the MGC per second. This property is only relevant for interface terminations in the "interface IPR context".

Type: Integer
Possible values: 0 and up
Default: 1
Defined in: TerminationState Descriptor
Characteristics: Read/write

10.1.3 NAT Type

Property Name: NAT Type
PropertyID: natype (0x0003)
Description: This property indicates the type of NAT as defined in [IETF RFC 2663]. This property is only relevant for interface terminations in the "interface IPR context". This property is set on the external NAT interface.
Type: Enumeration
Possible values: "TrN" (0x0001): Traditional NAT
"BiN" (0x0002): Bi-directional NAT
"TwN" (0x0003): Twice NAT
"MuN" (0x0004): Multihomed NAT
Default: "TrN" (0x0001)
Defined in: TerminationState Descriptor
Characteristics: Read/write

10.1.4 Address and Port Mapping

Property Name: Address and Port Mapping
PropertyID: apmap (0x0004)
Description: This property indicates which address and port mapping behaviour (as defined by clause 4.1 of [IETF RFC 4787]) is used for the NAT mapping. This property is only relevant for interface terminations in the "interface IPR context". This property is set on the external NAT interface.
Type: Enumeration
Possible values: "endind" (0x0001): Endpoint independent mapping
"adep" (0x0002): Address dependent mapping
"apdep" (0x0003): Address and port dependent mapping
Default: "endind" (0x0001)
Defined in: TerminationState Descriptor
Characteristics: Read/write

10.1.5 IP Address Pooling

Property Name: IP Address Pooling
PropertyID: addrpool (0x0005)

Description: In cases where a NAT supports IP address pooling (as defined by clause 4.1 of [IETF RFC 4787]), this property indicates how the address is allocated. This property is only relevant for interface terminations in the "interface IPR context". This property is set on the external NAT interface.

Type: Enumeration

Possible values: "arbit", (0x0000): Arbitrary address allocation
 "pair", (0x0001): Paired address allocation

Default: "arbit", (0x0000)

Defined in: TerminationState Descriptor

Characteristics: Read/write

10.1.6 Port Assignment

Property Name: Port Assignment

PropertyID: portass (0x0006)

Description: This property indicates whether, when assigning the NAT mapping, the MG shall attempt to preserve the port number used internally. This port assignment behaviour is described in clause 4.2.1 of [IETF RFC 4787]. This property is only relevant for interface terminations in the "interface IPR context". This property is set on the external NAT interface.

Type: Enumeration

Possible values: "pres" (0x0001): Attempt to preserve the internal port number
 "nopres" (0x0002): The MG is not required to preserve the internal port numbers, but may still do so

Default: "nopres" (0x0002)

Defined in: TerminationState Descriptor

Characteristics: Read/write

10.1.7 NAT Mapping Information

Property Name: NAT Mapping Information

PropertyID: nmi (0x0007)

Description: This property provides a single NAT mapping entry in the NAT mapping table. This property is only relevant for "NIPR" context types. If the type of the NAT is twice or bidirectional NAT, the property "*nmi*" will describe the mapping in the internal-to-external direction and in the external-to-internal direction. Meanwhile, for the other kinds of NAT (i.e., traditional NAT), the property "*nmi*" describes the address mapping from the internal-to-external direction.

NOTE – When used to describe an interface, "internal" and "external" are general terms indicating the roles of the two interfaces for the purpose of that specific NAT entry. For example, in one mapping, *interface1* might be considered internal and *interface2* might be considered external, and vice-versa in another mapping.

Type: String

Possible values: A string having the format of "NATmapping", given by the following ABNF. See clause 10.6.2 for a detailed explanation of this syntax:

```
NATmapping = InternalPattern "|" ExternalPattern ["|" protocol]
InternalPattern = "I|" Pattern
ExternalPattern = "E|" Pattern
protocol = UINT16 *(COMMA UINT16)
Pattern = "id:" interfaceID "|" ipA:" subnetA ["|ptA:" portRangeA]
        ["|ipB:" subnetB ["|ptB:" portRangeB]]
interfaceID = UINT32
subnetA = subnet
subnetB = subnet
portRangeA = portRange
portRangeB = portRange
subnet = domainAddress ["/" prefix] / "$"
portRange = UINT16 ["-" UNIT16] / "$"
prefix = UINT16
        ; UINT16, COMMA, UINT32 & domainAddress
        ; according to B.2/[ITU-T H.248.1]
```

Default: Provisioned

Defined in: ContextAttribute Descriptor

Characteristics: Read/write

10.1.8 Lifetime of NAT

Property Name: Lifetime of NAT

PropertyID: lt (0x0008)

Description: This property indicates the lifetime of NAT mapping maintained in the NIPR context.

Type: Double

Possible values: 0 ms upwards, -1 indicates that the NAT mapping does not expire.

Default: -1, unless provisioned otherwise

Defined in: TerminationState Descriptor

Characteristics: Read/write

10.2 Events

10.2.1 New NAT Mapping Reporting

Event Name: New NAT Mapping Reporting

Event ID: nnmr (0x0001)

Description: This event indicates a list of new NAT mapping entries. This event is only relevant for interface terminations in an interface IPR context. A NAT mapping entry is relevant for two interfaces, internal side and external side. This event is only reported from the termination of the external side.

10.2.1.1 EventsDescriptor parameters

10.2.1.1.1 Maximum list size

Parameter Name: Maximum list size

ParameterID: mls (0x0001)

Description: This parameter provides the maximum number of new NAT mapping entries reported by one observed event.

Type: Integer

Optional: Yes

Possible values: 1 to 100

Default: 10

10.2.1.2 ObservedEventsDescriptor parameters

10.2.1.2.1 New NAT mapping entries

Parameter Name: New NAT mapping entries

ParameterID: nnme (0x0001)

Description: This parameter provides a list of NAT mapping entries which should be added to NAT mapping table.

Type: Sub-List of String

Optional: No

Possible values: A list of elements, each element having the format of "NATmapping" (clause 10.1.7).

Default: None

10.2.2 Delete NAT Mapping Reporting

Event Name: Delete NAT Mapping Reporting

Event ID: dnmr (0x0002)

Description: This event indicates a list of NAT IPR ContextIDs that should be deleted. This event is only relevant for interface terminations in interface IPR context.

10.2.2.1 EventsDescriptor parameters

10.2.2.1.1 Maximum list size

Parameter Name: Maximum list size

ParameterID: mls (0x0001)

Description: This parameter provides the maximum number of NAT IPR ContextIDs reported by one observed event.

Type: Integer

Optional: Yes

Possible values: 1 to 100

Default: 10

10.2.2.2 ObservedEventsDescriptor parameters

10.2.2.2.1 NAT IPR Contexts

Parameter Name: NAT IPR Contexts

ParameterID: nic (0x0001)

Description: This parameter provides a list of ContextIDs of NAT IPR contexts.

Type: Sub-List of Integer

Optional: No

Possible values: A list of integers.
The possible values of each element are 0x01 to 0xFFFFFFFFD.
Values 0x00, 0xFFFFFFFFE and 0xFFFFFFFFF are reserved.

Default: None

10.2.3 Modify NAT Mapping Reporting

Event Name: Modify NAT Mapping Reporting

Event ID: mnmr (0x0003)

Description: This event indicates the modification of a list of NAT IPR contexts. This event is only relevant for interface terminations in an interface IPR context.

10.2.3.1 EventsDescriptor parameters

10.2.3.1.1 Maximum list size

Parameter Name: Maximum list size

ParameterID: mls (0x0001)

Description: This parameter provides the maximum number of ContextIDs and NAT mapping entries reported by one observed event.

Type: Integer

Optional: Yes

Possible values: 1 to 100

Default: 10

10.2.3.2 ObservedEventsDescriptor parameters

10.2.3.2.1 New NAT mapping entries

Parameter Name: New NAT mapping entries

ParameterID: nnme (0x0001)

Description: There is a one-to-one relationship between the list positions of the *nnme* and *nic* parameters, thus there shall be the same number of list positions. This parameter provides a list of NAT mapping entries which are associated with a list of NAT IPR contexts.

Type: Sub-List of String

Optional: No

Possible values: A list of elements, each element having the format of "NATmapping" (clause 10.1.7).

Default: None

10.2.3.2.2 NAT IPR Contexts

Parameter Name: NAT IPR Contexts

ParameterID: nic (0x0002)

Description: This parameter provides a list of NAT IPR ContextIDs in which the values of context attribute "*nmi*" should be updated by the values provided in parameter "*nnme*".

Type: Sub-List of Integer

Optional: No

Possible values: A list of integers.
The possible values of each element are 0x01 to 0xFFFFFFFFD.
Values 0x00, 0xFFFFFFFFE and 0xFFFFFFFFF are reserved.

Default: None

10.3 Signals

None.

10.4 Statistics

None.

10.5 Error codes

None.

10.6 Procedures

10.6.1 Information base related procedures

10.6.1.1 Creation of a FIB for a context of type "NIPR"

10.6.1.1.1 Information base: FIB creation and preparation for NAT specifications

Property "Notifications Rate" (*iprnat/nr*) is used to govern the rate at which routing or NAT mapping information notifications are sent to the MGC from the MG. See clause 9.3 of [ITU-T H.248.1] for more information about notification rates.

Property "Lifetime of NAT" (*iprnat/lt*) is used to set and audit the lifetime of the NAT mapping. On assignment of the NAT mapping, unless no expiry is indicated, the MG shall count down to zero from the lifetime value. Whenever a packet is handled by the NAT entry, the counter is reset to the original lifetime value. If the lifetime reaches zero, then the NAT mapping is deleted and the "*iprnat/dnmr*" event (see clause 10.6.1.2.5) is triggered.

Properties "NAT Type" (*iprnat/nattype*), "Address and Port Mapping" (*iprnat/apmap*), "IP Address Pooling" (*iprnat/addrpool*) and "Port Assignment" (*iprnat/portass*) are used by the MGC when it requires that the MG assign NAT mappings according to certain behaviours. These parameters are set on the external interface.

NOTE – The MG must be aware of the internal interface or external interface due to the fact that the original NAT mapping is detected by the MG and reported to the MGC. The precondition of this capability is that the MG knows the internal interface and external interface. For example, the route entry configured on the internal interface which connects to the internal network decides which is the external interface for a special route. If one IP packet received from *interface1* in the internal *network1* will be forwarded to the external *network2* via the *interface2* and the source address is mapped, then the *interface2* is the external interface.

The MGC may also set other information elements (properties or SDP lines) that are applicable for NAT mapping. One such example is the use of the RTCP SDP attribute ("a=rtcp") that may have an impact on port contiguity. Another example is the use of filters defined by [ITU-T H.248.43].

If the above properties are set, the MG shall allocate NAT mappings for the interface based on them. If the MGC changes the value of the "*iprnat/nattype*", "*iprnat/apmap*", "*iprnat/addrpool*" or "*iprnat/portass*" properties, the existing NAT mappings are still valid. New NAT mappings will be allocated according to the new setting. In the case that an MGC requires a different NAT behaviour

from the default at the initial creation of the interface, it should consider setting the above properties before setting the "NAT Mapping" event. This is to ensure that NAT mappings are not allocated according to the default. If the MG does not support the NAT behaviour that the MGC sets, the MG should return the error code 449 in the reply message.

10.6.1.1.2 NAT behaviour types

Different types of NAT behave differently, as defined in clause 4 of [IETF RFC 2663]:

- The *basic NAT* will map one private IP address to one external IP address.
- The *Network Address Port Translation NAT* allows the transport identifiers of a number of private hosts to be multiplexed into the transport identifiers of a single external IP address.
- The *Bi-directional NAT* allows the sessions to be initiated from hosts in the public network as well as the private network.
- The *Twice NAT* modifies both the source and destination addresses of the datagram as it crosses address realms.
- The *Multihomed NAT* boxes share the same NAT configuration and can provide fail-safe back-up for each other.

Traditional NATs (i.e., *Basic NAT* and *Network Address Port Translation NAT*) are defined as having certain behaviours. [IETF RFC 4787] discusses these behaviours and outlines requirements for these types of NATs. Therefore, if the MGC sets the "*iprnat/nattype*" property to indicate that a traditional NAT is used, the MG shall follow the requirements from [IETF RFC 4787]. The "*iprnat/apmap*", "*iprnat/addrpool*" or "*iprnat/portass*" properties allow the MGC to set the types of behaviours expected for the particular interface.

Both the *Bi-directional NAT* and the *Twice NAT* bind the private network addresses to globally unique addresses. With a *Bi-directional NAT* or *Twice NAT*, sessions can be initiated from both sides. All requests from the same internal IP address and port are mapped to the same external IP address and port. The "*iprnat/apmap*", "*iprnat/addrpool*" or "*iprnat/portass*" have no relevance when the "*iprnat/nattype*" property is set to "BiN" or "TwN".

10.6.1.2 Creation of a NAT mapping for a context of type "NIPR"

10.6.1.2.1 General

The MG determines the NAT mapping table information based on the NAT IPR contexts and thus maintains a NAT ContextID to NAT mapping table entry mapping. The MG determines what dynamic updates need to be made to the NAT mapping table and notifies the MGC of the necessary updates. The dynamic updating of the NAT mapping table should follow the behaviour rule of the type set in the property *iprnat/nattype* and, if applicable, the "*iprnat/apmap*", "*iprnat/addrpool*" or "*iprnat/portass*" properties.

10.6.1.2.2 MG reporting and MGC updating of new NAT mapping entries

Where an MGC wishes to receive information regarding new NAT mapping entries, it shall set the "*iprnat/nnmr*" event. This event enables a detection logic to analyse incoming IP address information against existing NAT mapping information (defined by the NAT IPR contexts) to determine if a new NAT mapping is required. Therefore, when the MG receives IP packets and dynamically generates one or more new NAT mapping entries, the MG reports the new NAT mapping entries to the MGC through the observed event "*iprnat/nnmr*". Reporting of the "*iprnat/nnmr*" event may also result from a locally assigned NAT mapping (i.e., through a management action).

This event is reported from the termination which represents the interface of the *public* side of the NAT mapping entry. The MGC then creates a new NAT IPR context for each new NAT mapping entry. The MGC should set the value of the context attribute "*iprnat/ifm*" as "NIPR". The new NAT

mapping entry information should be saved in the context attribute "*iprnat/nmi*". One incoming and one outgoing termination are added to this NAT IPR context. The MG determines which interface context is applicable to the NAT mapping entry from the InterfaceIDs in the NAT mapping information. This can be determined as the InterfaceIDs have a one-to-one relationship with a TerminationID and, as a termination may only reside in a single context, this provides a unique mapping. Parameter "*mls*" of the event "*iprnat/nnmr*" is used to limit the maximum number of new NAT entries reported by one observed event.

10.6.1.2.3 MG reporting and MGC updating of changed NAT mapping entries

When the MG detects that one or more NAT mapping entries have changed (e.g., via a permanently enabled detection logic that analyses incoming IP address information), the MG reports those changes to the MGC through the event "*iprnat/mnmr*". This event is reported from the termination which represents the interface of the public side of the NAT mapping entry. Packets still have their network addresses translated according to the original NAT mapping until confirmed by the MGC. The MGC indicates to the MG to modify the values of context attribute "*iprnat/nmi*" of the special NAT IPR contexts based on the values of the MG reports. This allows the MGC to enforce any appropriate policy decisions. Parameter "*mls*" of the event "*iprnat/mnmr*" is used to limit the maximum number of modified NAT mapping entries reported by one observed event.

10.6.1.2.4 MGC controlled new NAT mapping entries without MG reporting

The MGC may create a new NAT IPR context for a new NAT mapping entry without the reporting of IP packets with new IP address information detection from the MG. For example, the MGC may prepare a new NAT mapping for a new call on the MG. The MGC may require the MG to allocate the public mapping address for a particular private IP address and port. The MGC should set the value of the context attribute "*iprnat/ifm*" as "NIPR". The new NAT mapping entry information should be saved in the context attribute "*iprnat/nmi*". Information regarding the mapped-to address may be wildcarded "CHOOSE", in which case the MG will reply with the corresponding mapping. The MG determines the mapped-to address based on *iprnat/nattype* and associated properties (described above). One incoming termination and one outgoing termination are added to this NAT IPR context. The MG allocates a public IP address and port and sends them in the response message to the MGC.

10.6.1.2.5 Deleted NAT entries

When the MG detects that one or more NAT entries are deleted, the MG reports them to the MGC through the event "*iprnat/dnmr*". Packets still have their network addresses translated according to the original NAT mapping until it is removed by the MGC. The MGC then subtracts both terminations in the indicated NAT IPR contexts, and thus deletes the related NAT mapping information from the NAT mapping table. Parameter "*mls*" of the event "*iprnat/dnmr*" is used to limit the maximum number of deleted NAT mapping entries reported by one observed event.

10.6.1.2.6 Lifetime of NAT mapping entries

The MGC may set the lifetime of NAT mapping through the property "*iprnat/lt*".

10.6.2 NAT mapping information structure

This clause explains how the MG uses the contents of the NAT mapping information property for controlling the address translation operations. References to ABNF rules appearing in clause 10.1.7 are given below in **fixed-font**.

10.6.2.1 Internal-to-external direction

A packet will be translated in the internal-to-external direction if it matches the following conditions:

- 1) It is received on the interface matching **interfaceID** of **InternalPattern**.

- 2) Its source IP address belongs to **subnetA** of **InternalPattern**.
- 3) Its destination IP address belongs to **subnetB** of **InternalPattern** (if given).
- 4) Its source and destination ports belong to **portRangeA** and **portRangeB** of **InternalPattern**, respectively (if given).
- 5) Its transport protocol number (as registered by IANA) appears in **protocol** (if given).

Translation will enforce the following changes to the packet:

- 1) Its source address will be changed to an address in **subnetA** of **externalPattern**. The host identifier part of this address shall be identical to that of the original source address.
- 2) Its destination address will be changed to an address in **subnetB** of **externalPattern** (if given). The host identifier part of this address shall be identical to that of the original source address.
- 3) Its source port and destination port will be changed to ports in **portRangeA** and **portRangeB**, respectively, of **externalPattern** (if given). If the port range spans more than one port, the new port will have the same offset within the range as the original port.

Following translation, the packet will be sent through the interface represented by **InterfaceId** of **externalPattern**.

10.6.2.2 External-to-internal direction

Mapping in the external-to-internal direction is simply the reverse of the internal-to-external one. For completeness, it is given below.

A packet will be translated in the external-to-internal direction if it matches the following conditions:

- 1) It is received on the interface matching **interfaceID** of **ExternalPattern**.
- 2) Its destination IP address belongs to **subnetA** of **ExternalPattern**.
- 3) Its source IP address belongs to **subnetB** of **ExternalPattern** (if given).
- 4) Its destination and source ports belong to **portRangeA** and **portRangeB** of **ExternalPattern**, respectively (if given).
- 5) Its transport protocol number (as registered by IANA) appears in **protocol** (if given).

Translation will enforce the following changes to the packet:

- 1) Its destination address will be changed to an address in **subnetA** of **InternalPattern**. The host identifier part of this address shall be identical to that of the original source address.
- 2) Its source address will be changed to an address in **subnetB** of **InternalPattern** (if given). The host identifier part of this address shall be identical to that of the original source address.
- 3) Its destination port and source port will be changed to ports in **portRangeA** and **portRangeB**, respectively, of **InternalPattern** (if given). If the port range spans more than one port, the new port will have the same offset within the range as the original port.

Following translation, the packet will be sent through the interface represented by **InterfaceId** of **InternalPattern**.

10.6.2.3 NAT mapping validity

For a NAT mapping to be valid, it must match the following conditions:

- 1) The same elements appear in **InternalPattern** and **ExternalPattern**, e.g., if **InternalPattern** includes **subnetB**, so shall **ExternalPattern**.
- 2) The size of a subnet or port-range in **InternalPattern** must match the size of the corresponding subnet or port-range in **ExternalPattern**.

The MG shall reject invalid NAT mappings using error code 449 (unsupported or unknown parameter or property value).

10.6.2.4 Example

Table 3 provides an example for the creation of a NAT mapping for a context of type "NIPR".

**Table 3 – Example command encoding –
Creation of a NAT mapping for a context of type "NIPR"**

ITU-T H.248 encoding (shortened command)	Comments
<pre>MEGACO/3 [11.9.19.65]:54321 Transaction = 67891 { Context = \$ { ; Context in NAT IPR mode ; Context properties ContextAttr = { ; ContextAttribute D. ipr/ifm = "NIPR", ;ContextID of the related Interface ;IPR Context ipr/nmi = "I id:1 ipA:[200.200.200.0]/24 ipB:[172.16.1.0]/24 E id: 2 ipA:[138.76.28.0]/24 ipB:[200.200.200.0]/24 " } Add = ip/private/1 { ; incoming Termination Tg } Add = ip/public/1 { Media {TerminationState {iprnat/nattype="TwN"} } ; outgoing Termination Th } } }</pre>	The NAT IPR mode is indicated by the context-level property <i>ipr/ifm</i>. The two ADD.request commands do not provide any <i>media descriptor</i> (MD-less ADDs). The TerminationID name is just an example. The used identity may depend on the applied ITU-T H.248 profile. In this example, Twice NAT is applied (Note).
NOTE – The configuration above sets up Twice NAT behaviour as specified in [IETF RFC 2663]. Datagram flow: Host_A (private) → Host_X (public) a) Within private network DA: 172.16.1.100 SA: 200.200.200.1 b) After Twice NAT translation DA: 200.200.200.100 SA: 138.76.28.1 Datagram flow: Host_X (public) → Host_A (private) a) Within public network DA: 138.76.28.1 SA: 200.200.200.100 b) After Twice NAT translation, in private network SA: 200.200.200.1 DA: 172.16.1.100	

10.6.3 IP packet forwarding with NAT function related procedures

If NAT functionality is needed for this forwarding, the private IP address and layer 4 port in the header of the IP layer and transport protocol layer are replaced by their mapped public IP address and layer 4 port, according to the NAT mapping information that is derived from the related NAT IPR context.

Appendix I

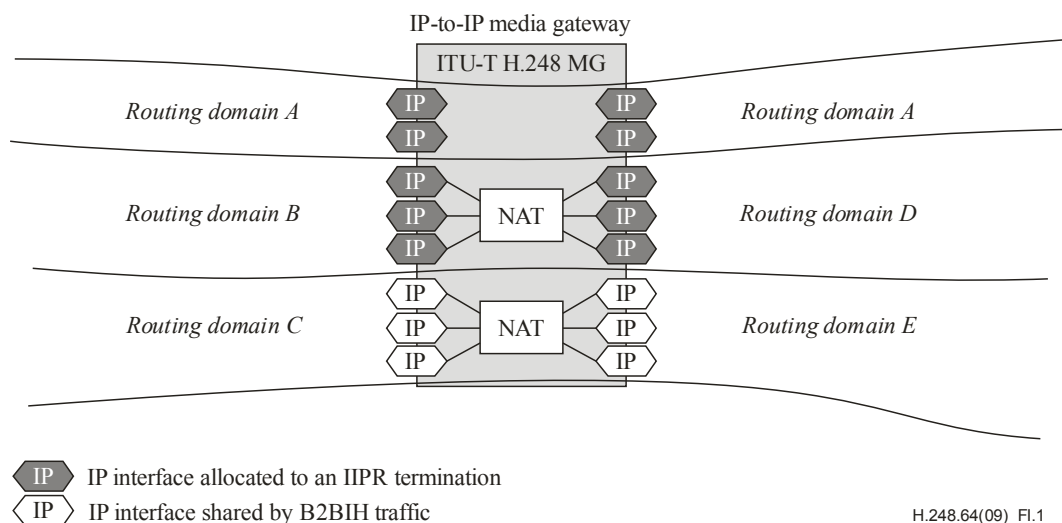
Routing tables and relation to route IPR contexts

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

This appendix provides complementary information with regard to the underlying concepts behind the packages of this Recommendation.

I.1 Routing domains

The local IP interfaces of an ITU-T H.248 MG either belong to ITU-T H.248 IPR terminations of B2B contexts or are related to ITU-T H.248 IIPR terminations of IPR contexts (see also clause 7). Any IP interface itself belongs to an IP address realm, which itself is a member of an IP routing domain or autonomous system (AS), see [b-IETF RFC 1136]. The MG local IP interfaces may be thus partitioned and distributed over multiple routing domains (see Figure I.1).



H.248.64(09)_FI.1

NOTE – Any MG may provide multiple B2B and multiple IIPR contexts in parallel.

Figure I.1 – MG partitioned on multiple routing domains – Example configuration with NAT-less IPR (A-A), NAT-full IPR (B-D) and B2B (C-E) entities

An IIPR termination is tightly coupled to a local L2 interface in a 1:1 relationship (see clause 3.2.3). As an example, in case of Ethernet, the local L2 interface can be either a physical or a logical interface. A physical interface is represented by an Ethernet port (identified by a 48-bit MAC address), whereas a logical interface is represented by an additional 12-bit VLAN identifier. That L2 interface may thus not be shared by other IIPR or B2B IP terminations. Therefore, separation of B2BIH and IIPR traffic can be done based on the physical/logical L2 interface where the IP packet is received (see Figure I.2).

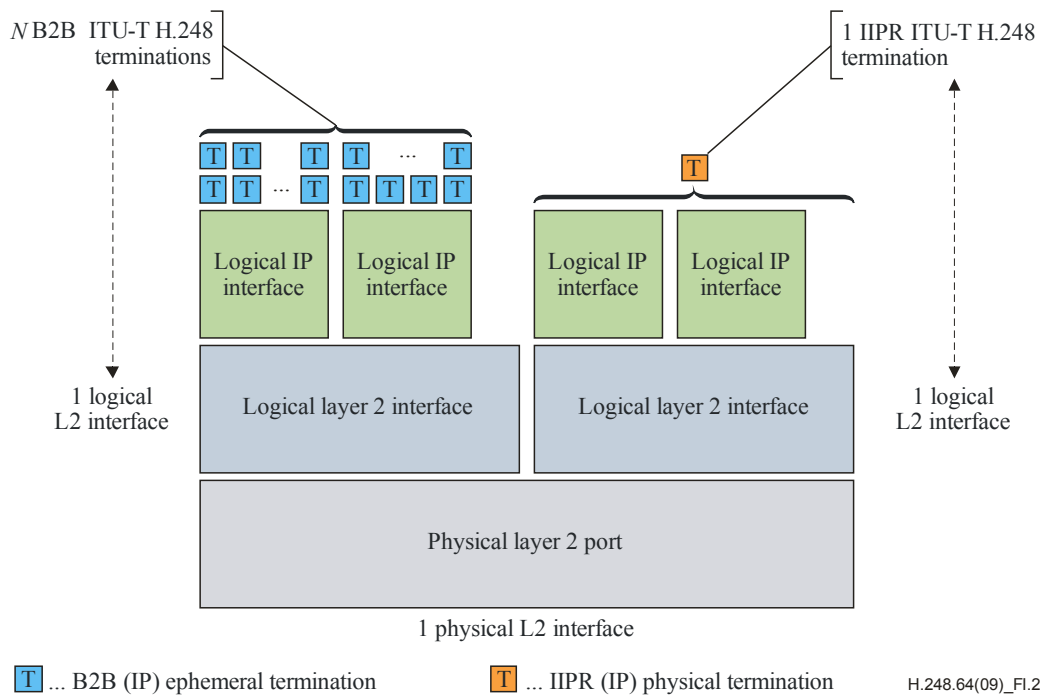


Figure I.2 – Layer 2 interface to ITU-T H.248 termination relationship showing N:1 relation between ITU-T H.248 B2B terminations and logical L2 interface and 1:1 relation between ITU-T H.248 IIPR termination and logical L2 interface

Figure I.2 illustrates the fact that there might be multiple IP interfaces per single ITU-T H.248 IIPR termination (and single logical L2 interface).

A single IIPR context defines an MG-local "router/hop entity". Any router has inherently two or more logical L2 interfaces and L3 (IP) interfaces (see [IETF RFC 1812]). The number of such local IP interfaces is "fixed" (provisioned).

The following clause describes the relationship of IP interfaces and the routing tables (RIB/FIB), i.e., the association to package property *ipr/fib*.

I.2 Route advertisement and process of building tables

I.2.1 Network model

Figure I.3 outlines a single routing domain (e.g., routing domain A from Figure I.1) and a simplified IP network architecture by some host and hop entities. The figure may be useful to illustrate the content and process of building the routing tables in the hop nodes (see Note). This is a unidirectional consideration: IP (uni-, multi- or broadcast) traffic is flowing from source to destination hosts. The route advertisement process is reverse because it happens always in the destination-to-source direction. IP routes (also known as IP paths) are thus unidirectional entities.

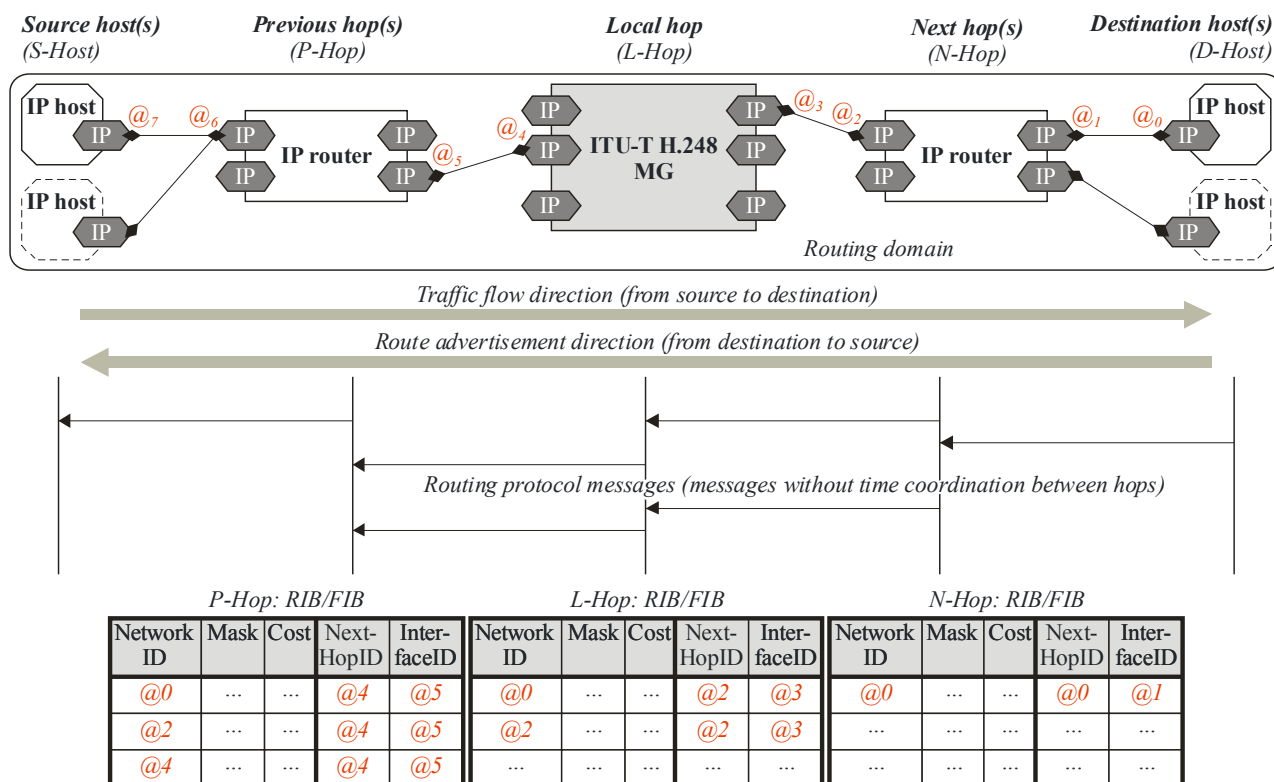
NOTE – There is also a routing table in host nodes, which is not considered in this appendix.

Figure I.3 illustrates the "local hop" perspective provided by the ITU-T H.248 MG.

Any IP node distributes recurrently route advertisement information via IP routing protocol(s) in case of dynamic routing. Figure I.4 depicts a generic routing protocol message, as sent (not received) by the MG as local hop.

The network topology in IP networks (and Figure I.3) may be reduced to "links" (L2 connection on the link layer) and (IP) "routes" (on the IP layer). A link has a local scope and relates to the L2 connection between two peering IP nodes (e.g., the outlined connection between L-Hop and N-Hop

in Figure I.3). Any route spans multiple hops, i.e., a scope beyond the next hop from the MG perspective.



NOTE – Routing tables are simplified. Just one IP route is indicated. Just one direction.

No distinction is indicated between network routes (prefix match) and host routes (exact match).

H.248.64(09)_Fl.3

Figure I.3 – ITU-T H.248 MG in IPR mode – Abstracted route advertisement process in a single IP routing domain

One or multiple route entries <u>Ri</u>	L4 PCI	L3 SA = L3 LD	L3 DA = L3 RD	L2 PCI
---	--------	---------------	---------------	--------

Figure I.4 – Generic routing protocol message for route advertisements (by the MG)

I.2.2 Process of building routing tables

Let us consider the MG in the role as local hop (L-Hop).

MG received advertisements

The MG only receives route advertisements from the next hop, but not from the previous hop (in this model). The N-Hop sends (to the MG) a route advertisement message according to Figure I.4, with the following content:

- L2 PCI:
 - L2 DA = the L3-to-L2 resolved "address = @₃" value.
 - L2 SA = N-Hop local L2 value where @₂ resides.
- L3 PCI:
 - L3 DA = @₃.
 - L3 SA = N-Hop local @₂.

– Carried route entries R_i :

- R_1 = (sub)network in which $@_1$ resides.

NOTE 1 – This is a simplified route entry because network prefixes are not considered.

Semantic of this route entry: "IP(sub)network destination $@_1$ may be reached via a route with NextHopID ' $@_2$ '".

NOTE 2 – Real routing protocols carry route entries either in the L3 payload (like OSPF) or in the L4 payload (e.g., BGP, RIP).

This information is then stored in the L-Hop routing table (see first row in Figure I.3).

The MG receives route advertisement messages from next-hop node(s) and stores the route entries in the local RIB/FIB. There is thus an L2 connection (the "link") in the egress direction, i.e., from the local "router/hop" to the next-hop link endpoints, which is characterized by link endpoint addresses "InterfaceID". The "L3 SA" relates thus to FIB element "NextHopID" entry.

MG-originated advertisements

The ITU-T H.248 gateway correspondingly advertises its IP interfaces and IP routes to all connected previous hop nodes. The scope of interfaces, routes and P-Hops is limited to a particular routing domain. The IP routing protocol(s) may be theoretically located on an MGC or MG level. This Recommendation, however, assumes MG-located IP routing protocols, (see also the "route reporting" capabilities in clause 9.2) (refer to Figure I.5).

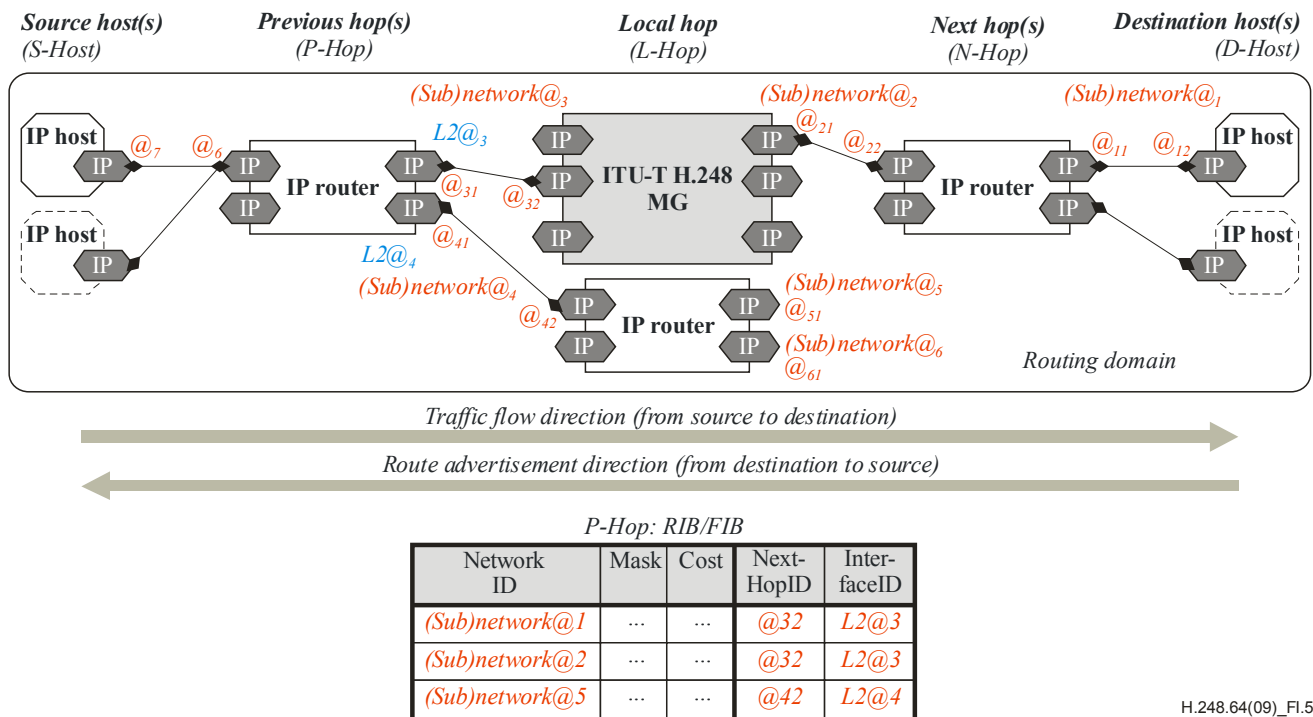
NOTE – The rationale behind this is the fact that the IP routing is related to IP media-/data-paths, which correspond to the ITU-T H.248 bearer paths (of IIPR contexts and terminations).

The advertised MG local addresses ((sub)networks) appear in the P-Hop node(s) FIB entries as "NetworkIDs".

The L3 SA used by the MG advertising a route appears in the P-Hop node(s) FIB entries as "NextHopID".

The L2 interface on which the MG advertisement has been received appears in the P-Hop node(s) FIB entries as "InterfaceID".

The next clause discusses the basic information as maintained by a FIB.



H.248.64(09)_FI.5

Figure I.5 – ITU-T H.248 MG in IPR mode – MG-originated route advertisements (sent to P-Hop)

I.2.3 Topology information in the FIB

Figure I.6 illustrates again a very basic FIB structure (see also the ITU-T H.248 *fib* property in clause 9.1.2). The table itself may be divided into two halves according to two different types of topology information:

- **L2 (egress) link**
 - The two link endpoints are identified by FIB elements NextHopID and InterfaceID.
NOTE – IP routing can be considered protocol-independent of the lower layer L2/L1 protocol stack. The connection endpoint names of the L2 link are therefore either "generic identifiers" or L3 addresses (which may be unambiguously resolved into L2 addresses).
- **L3 (egress) route**
 - The route "originates" at the local IP interface from a (local-) hop perspective.
 - The route goes in the direction of unmasked or masked IP destination address (given by FIB element NetworkID).
 - An unmasked NetworkID relates to a host route entry, and a masked NetworkID relates to a network route entry.
 - Multiple (L3) routes may use the same (L2) link. There could thus be multiple FIB entries with the same value pairs {NextHopID, InterfaceID} (which may be therefore associated to a single IIPR context).

The route entries are consequently only related to the "egress direction" from an L-Hop perspective.

It may be further concluded that the set of advertised routes (by the MG) is bounded by the IIPR context-associated FIB (see also Figure I.3).

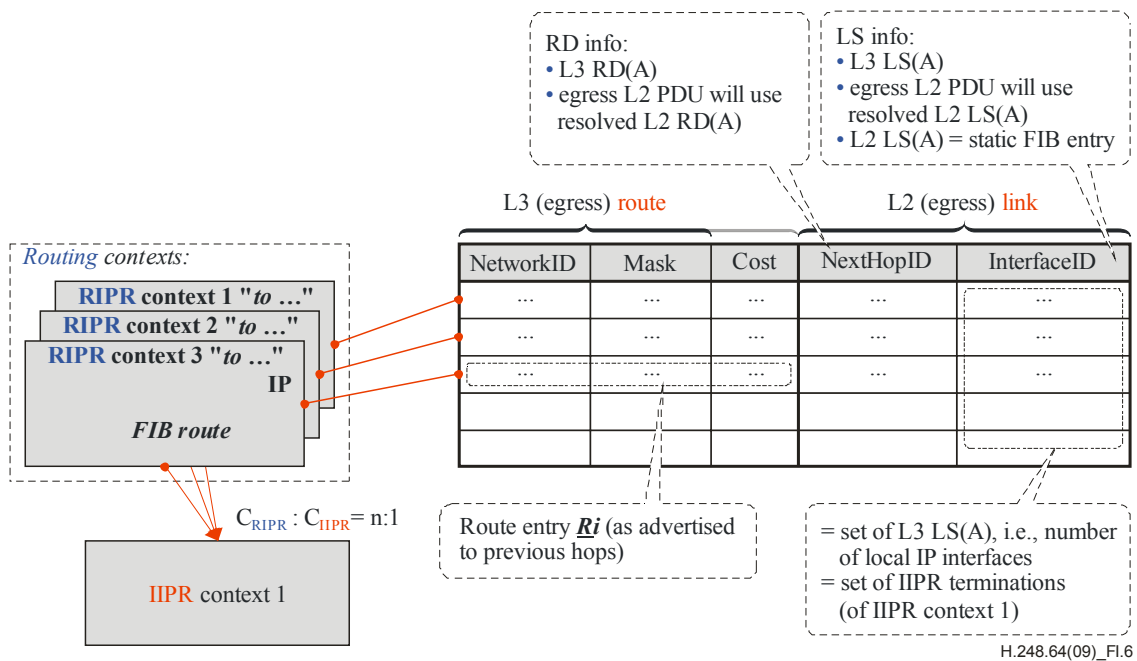


Figure I.6 – FIB representation – Example FIB structure (for properties *ipr/fib*) and association to IPR context types

I.3 Interface IPR context and IIPR termination

The (IP) packet-to-"IIPR context" assignment, as indicated by clause 7.2, is achieved via lookup on the IIPR context-associated "FIB" (which itself is defined by the associated RIPR contexts, see Figure I.6). The *ipr* package version 1 focuses on the very simplest FIB structure (which is given by the [IETF RFC 1812] FIB). The lookup key for FIB queries is thus given by the tuple of {NetworkID, Mask}. It may be underlined that element 'NetworkID' represents L3 DA information only in such a simple FIB (and no L4 (or other protocol control) information is used for the lookup process concerning that particular packet classification step for packet-to-context assignment). Note that the NetworkID may also represent a default route entry (see [b-IETF RFC 4632]).

Consequently, all *IIPR terminations* may receive:

- traffic with (destination) route entries as defined by RIPR contexts (i.e., IP bearer traffic routed to MG); and
- new route entry advertisements (i.e., IP routing protocol traffic, sent from previous hops).

Hence, an IIPR termination represents a bidirectional logical L2 interface with one or multiple assigned *bidirectional IP interface(s)* (see clause 3.2.3). The IIPR context topology between all IIPR terminations is therefore inherently given by the FIB content (which would be a full mesh between all IIPR terminations in case of an IETF RFC 1812 router function). The topology descriptor is not required.

Bibliography

- [b-ETSI TS 183 018] ETSI TS 183 018 (2009), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile Version 3 for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification.*
- [b-IETF RFC 1136] IETF RFC 1136 (1989), *Administrative Domains and Routing Domains: A Model for Routing in the Internet.*
- [b-IETF RFC 4632] IETF RFC 4632 (2006), *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.*

SERIES OF ITU-T RECOMMENDATIONS

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