

# ETSI TS 129 162 V9.4.0 (2010-04)

---

*Technical Specification*

**Digital cellular telecommunications system (Phase 2+);  
Universal Mobile Telecommunications System (UMTS);  
LTE;  
Interworking between the IM CN subsystem and IP networks  
(3GPP TS 29.162 version 9.4.0 Release 9)**

---



---

**Reference**

RTS/TSGC-0329162v940

---

**Keywords**

GSM, LTE, UMTS

**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**

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

[http://portal.etsi.org/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/ETSI_support.asp)

---

**Copyright Notification**

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2010.  
All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™**, **TIPHON™**, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

**3GPP™** is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**LTE™** is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

---

## 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 Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

# Contents

Intellectual Property Rights .....	2
Foreword.....	2
Foreword.....	5
1 Scope .....	6
2 References .....	6
3 Definitions, symbols and abbreviations .....	7
3.1 Definitions .....	7
3.2 Symbols.....	8
3.3 Abbreviations .....	8
4 General .....	8
4.1 General interworking overview .....	8
4.2 Interworking scenarios .....	9
4.2.1 UE with 3GPP SIP profile capability connecting to an external SIP device.....	9
5 Network characteristics .....	9
5.1 Key characteristics of IP Multimedia Networks.....	9
5.2 Key characteristics of UMTS IM CN Subsystem.....	10
6 Interworking Reference Model for control plane interworking and user plane interworking.....	10
6.1 Interworking Functional Entities .....	11
6.1.1 S-CSCF.....	11
6.1.2 IMS-ALG.....	11
6.1.3 TrGW.....	11
7 Control plane interworking .....	12
7.1 SIP with 3GPP Profile to Standard SIP Interworking .....	12
7.2 Additional interworking of protocol associated with supplementary services .....	12
7.2.1 General.....	12
7.2.2 Terminating Identification Presentation (TIP) and Terminating Presentation Restriction (TIR).....	12
7.2.3 Common Basic Communication .....	12
8 User Plane Interworking.....	12
8.1 Overview .....	12
8.2 VOID .....	12
8.3 VOID.....	13
9 IMS-ALG and TrGW functionality for NAPT and IP Version Interworking.....	13
9.1 Control plane interworking.....	13
9.1.1 Session Set-up.....	13
9.1.1.0 General .....	13
9.1.1.1 Receipt of the first SDP offer .....	13
9.1.1.2 Receipt of the first SDP answer .....	13
9.1.2 Void .....	14
9.1.3 Change of connection information.....	14
9.1.4 Interworking of SIP messages .....	14
9.2 User plane transport.....	14
9.2.1 Payload transport .....	14
9.2.2 IP header interworking.....	15
9.2.2.1 IPv4 to IPv6 .....	15
9.2.2.2 Abnormal cases .....	16
9.2.2.3 IPv6 to IPv4.....	16
9.2.2.4 Abnormal cases .....	18
9.2.3 Fragmentation .....	18
9.2.4 Abnormal cases.....	18
10 IBCF – TrGW Interactions.....	18

10.1	Overview .....	18
10.1.1	General.....	18
10.1.2	Network model .....	18
10.1.3	Example Call Flow .....	19
10.1.3.1	Basic Procedures .....	19
10.1.3.1.1	Call Establishment.....	19
10.1.3.1.2	Call Release .....	21
10.2.0	Introduction.....	22
10.2	Main Functions supported at the Ix Interface .....	22
10.2.1	IP Address and Port Conversion .....	22
10.2.2	Gate Management .....	22
10.2.3	Handling of RTCP Streams .....	22
10.2.4	IP Realm/Domain Indication .....	23
10.2.5	Media Control .....	23
10.2.6	Media Inactivity Detection .....	30
10.2.7	QoS Packet Marking .....	30
10.2.8	Hanging Termination Detection .....	30
10.2.9	Traffic Policing .....	30
10.2.10	IMS end-to-end media plane security .....	30
10.3	VOID .....	31
10.4	Procedures .....	31
10.4.1	Call related Procedures .....	31
10.4.1.1	Reserve TrGW Connection Point.....	31
10.4.1.2	Configure TrGW Connection Point .....	33
10.4.1.3	Reserve and Configure TrGW Connection Point .....	36
10.4.1.4	Release TrGW Termination .....	39
10.4.1.5	IP Bearer Released.....	39
10.4.1.6	Media Inactivity Detection.....	40
10.4.1.7	Termination heartbeat indication .....	40
10.4.2	Non Call related Procedures .....	40
<b>Annex A (informative):</b>	<b>Codecs used for conversational services .....</b>	<b>42</b>
<b>Annex B (informative):</b>	<b>Change history .....</b>	<b>43</b>
History .....		44

---

# Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

---

# 1 Scope

The IM CN subsystem interworks with the external IP networks through the Mb reference point.

This document details the interworking between the IM CN subsystem and external IP networks for IM service support. It addresses the issues of control plane interworking and, user plane interworking for specific interworking use cases. Clause 10 describes the IMS-Ix interface requirements in the form of Use Cases which require H.248 protocol procedures. Subclause 10.4 then details the additional Information Elements required to perform the specific procedures.

The IP version Interworking, between IP version 4 RFC 791 [9] and IP version 6 RFC 2460 [10] detailed in terms of the processes and protocol mappings required in order to support both mobile originated and terminated calls.

---

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 24.229: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".
- [2] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [3] 3GPP TS 23.221: "Architectural requirements".
- [4] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".
- [5] 3GPP TS 23.002: "Network architecture".
- [6] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".
- [7] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [8] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".
- [9] IETF RFC 791: "Internet Protocol".
- [10] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".
- [11] IETF RFC 2766: "Network Address Translation - Protocol Translation (NAT-PT)".
- [12] IETF RFC 2663: "IP Network Address Translator (NAT) Terminology and Considerations".
- [13] 3GPP TR 29.962 version 6.1.0: "Signalling interworking between the 3GPP profile of the Session Initiation Protocol (SIP) and non-3GPP SIP usage".
- [14] ITU-T Recommendation H.263: "Video coding for low bit rate communication".
- [15] ITU-T Recommendation G.723.1: "Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s".

- [16] ITU-T Recommendation G.729: "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)".
- [17] ITU-T Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies".
- [18] IETF RFC 792: "Internet Control Message Protocol".
- [19] IETF RFC 2463: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6".
- [20] IETF RFC 2765: "Stateless IP/ICMP Translation Algorithm (SITT)".
- [21] 3GPP TS 24.608: "Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM)Core Network (CN) subsystem; Protocol specification".
- [22] IETF RFC 3323: "A Privacy Mechanism for the Session Initiation Protocol (SIP)".
- [23] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".
- [24] 3GPP TS 24.628: "Protocols for Advanced Networking (TISPAN); Common Basic Communication procedures; Protocol specification".
- [25] 3GPP TS 29.238: "Interconnection Border Control Functions – Transition Gateway; H.248 Profile; Stage 3"
- [26] ITU-T Recommendation H.248.1 (05): "Gateway Control Protocol: Version 3"
- [27] Void
- [28] 3GPP TS 23.205: "Bearer-independent circuit-switched core network; Stage 2".
- [29] 3GPP TS 29.235: "Interworking between SIP-I based circuit-switched core network and other networks".
- [30] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".
- [31] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers"
- [32] 3GPP TS 33.328: "IMS Media Plane Security"
- [33] IETF RFC 4568 (2006): "Session Description Protocol (SDP) Security Descriptions for Media Streams"
- [34] IETF RFC 3711 (2004): "The Secure Real-time Transport Protocol (SRTP)"
- [35] IETF RFC 5124 (2008): "Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)"

---

## 3 Definitions, symbols and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [7] and the following apply:

**IM CN subsystem:** (IP Multimedia CN subsystem) comprises of all CN elements for the provision of IP multimedia applications over IP multimedia sessions



**IP multimedia session:** set of multimedia senders and receivers and the data streams flowing from senders to receivers. IP multimedia sessions are supported by the IP multimedia CN Subsystem and are enabled by IP connectivity bearers (e.g. GPRS as a bearer). A user may invoke concurrent IP multimedia sessions.

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [7] and the following apply: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [7].

BGCF	Breakout Gateway Control Function
IBCF	Interconnect Border Control Function
I-CSCF	Interrogating CSCF
IMS-ALG	IMS - Application Level Gateway
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
MRFP	Multimedia Resource Function Processor
NAT/NAPT	Network Address Translation / Network Address and Port Translation
NA (P) T-PT	Network Address (and Port) Translation - Protocol Translation
P-CSCF	Proxy CSCF
RTCP	Real Time Control Protocol
SCTP	Stream Control Transmission Protocol
SIP UA	SIP User Agent
SIP	Session Initiation Protocol
THIG	Topology Hiding Internetnetwork Gateway
TrGW	Translation GateWay
WAN	Wide Area Network

---

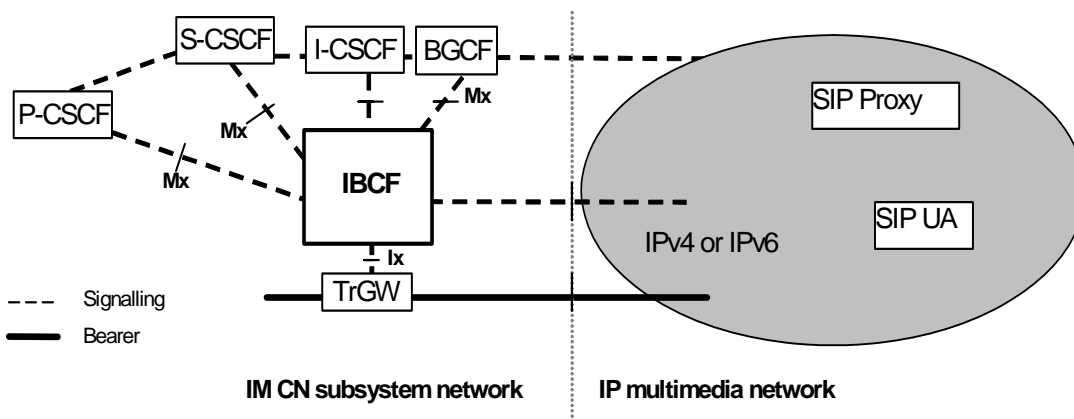
# 4 General

## 4.1 General interworking overview

The IM CN Subsystem interworks with SIP RFC 3261 [2] based IP Multimedia networks. These IP Multimedia networks include:

- SIP User Agents (UAs);
- SIP Servers.

As such, the IM CN Subsystem has to be able to interwork to all of these above functional entities in the IP multimedia network, as there is a possibility that they all may be involved in an IM session. The general interworking model is shown in figure 1. The SIP based Multimedia networks may use IP version 4 RFC 791 [9] or IP version 6 RFC 2460 [10].



**Figure 1: Interworking Model for IM CN Subsystem to IP Multimedia Network**

The UE uses the CSCF in order to communicate with the external IP multimedia network entities.

If no IP version interworking or no NAT/NAPT between different realms is required, the CSCF can communicate with SIP UAs in an external IP multimedia network directly.

If no IP version interworking or no NAT/NAPT between different realms is required, the CSCF can also communicate with SIP proxies in an external IP multimedia network directly, which in turn can then communicate with SIP UAs.

To provide the IP version interworking or NAT/NAPT between different realms the functions of an IMS-ALG and a TrGW may be inserted between the CSCF and external IP Multimedia Network by configuration. The IMS-ALG and the TrGW may be implemented as a part of other physical entities in the IMS.

NOTE: Other methods to provide IP version interworking are for further study.

## 4.2 Interworking scenarios

3GPP specifications design the IM CN subsystem elements and interfaces to exclusively support IPv6. 3GPP TS 23.221 [3] details the interoperability scenarios that an UE may experience when interworking with an external PDN. All of these IP transport layer interworking scenarios can apply to the application layer interworking scenarios detailed in clause 4.2.1.

### 4.2.1 UE with 3GPP SIP profile capability connecting to an external SIP device

The procedures used by an UE with 3GPP SIP profile to connect to an external SIP device, which may lack 3GPP SIP profile capabilities, have been analysed in Release 6 within 3GPP TR 29.962 [13] and are specified in 3 GPP TS 24.229 [1].

## 5 Network characteristics

### 5.1 Key characteristics of IP Multimedia Networks

The Internet is a conglomeration of networks utilising a common set of protocols. IP protocols are defined in the relevant IETF RFCs. The networks topologies may be based on LANs (e.g. Ethernet), Point-to-Point leased lines, PSTN, ISDN, X.25 or WANs using switched technology (e.g. SMDS, ATM).

IP multimedia networks provide the ability for users to invoke IP multimedia applications in order to send and receive (where applicable) voice and data communications. One protocol used to manage IP multimedia sessions is the Session Initiation Protocol (SIP) (RFC 3261 [2]).

## 5.2 Key characteristics of UMTS IM CN Subsystem

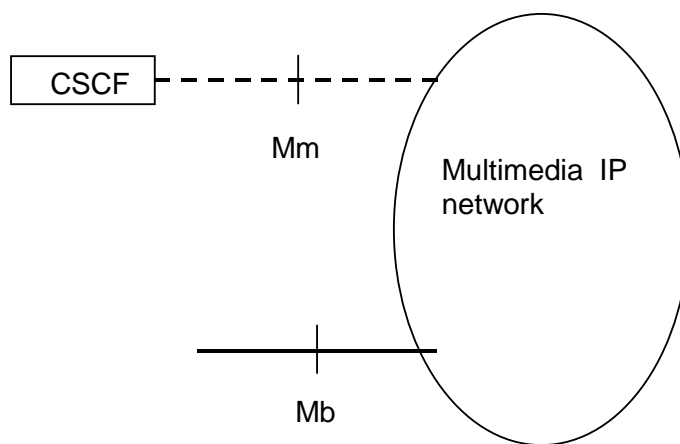
The UMTS IM CN subsystem uses the SIP protocol to manage IP multimedia sessions, and uses IP as the transport mechanism for both SIP session signalling and media transport.

The UMTS IM CN subsystem shall support interworking with existing fixed and mobile voice and IP data networks, including PSTN, ISDN, Mobile and Internet.

---

## 6 Interworking Reference Model for control plane interworking and user plane interworking

Figure 2 details the reference architecture required to support interworking between the IM CN subsystem and IP networks for IM services. Figure 3 details the reference architecture required to support interworking between the IMS and IP SIP networks supporting IP version 4.



NOTE: Multimedia IP networks may be connected via the Mb interface to various network entities, such as an UE (via an GTP Tunnel reaching to the GGSN), an MRFP, or an application server.

**Figure 2: IM CN Subsystem to IP network interworking reference Architecture without IP version interworking**

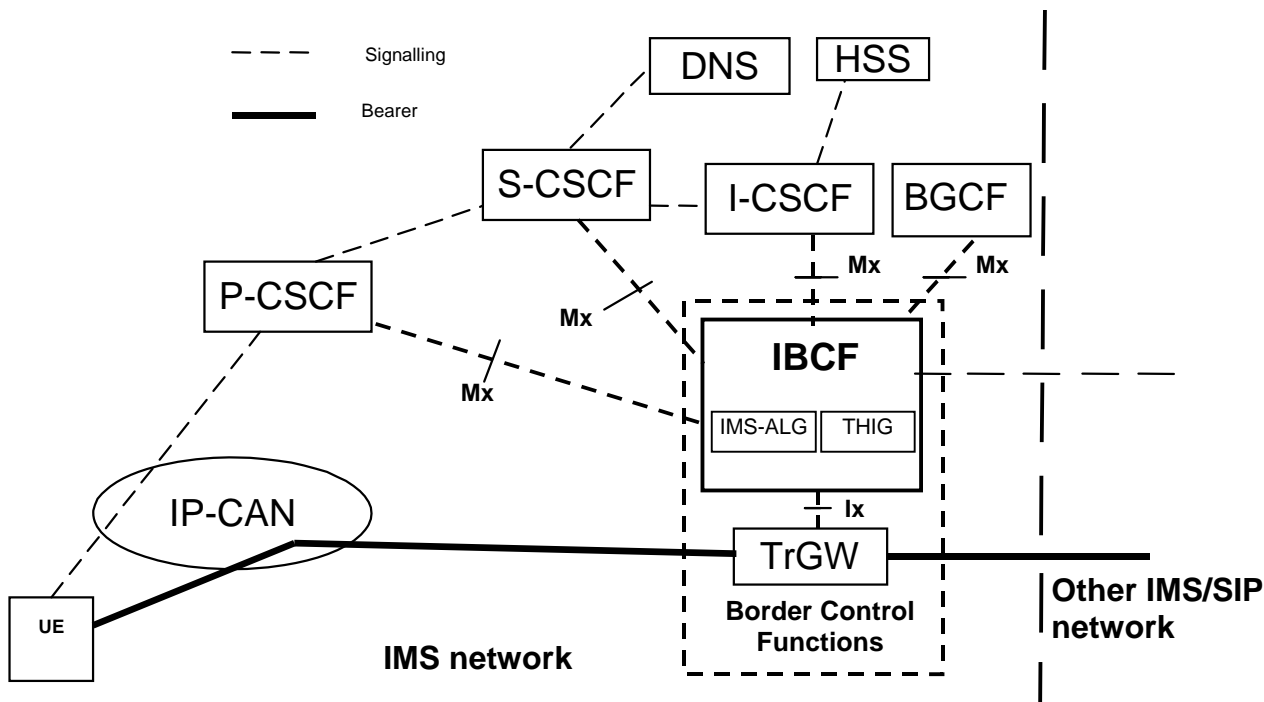


Figure 3: Border Control Functions

**Mm reference point:** The call control protocol applied to the Mm interface between CSCF and external IP networks is SIP, RFC 3261 [2], as detailed in 3GPP TS 24.229 [1]. SIP extension packages mandated by 3GPP are possibly not supported.

**Mb reference point:** This interface is defined in 3GPP TS 23.002 [5] and is IP based. Further information is provided in 3GPP TS 29.061 [4] and 3GPP TS 26.235 [6].

**Mx reference point:** The protocol applied at the Mx reference point is specified in 3GPP TS 24.229 [1].

**Ix reference point:** The protocol applied at the Ix reference point is specified in 3GPP TS 29.238 [25].

## 6.1 Interworking Functional Entities

### 6.1.1 S-CSCF

This entity provides control plane functionality to connect entities following the 3GPP profile of SIP, TS 24.229 [1], and external SIP entities following RFC 3261 [2].

### 6.1.2 IMS-ALG

IMS-ALG functionality resides in IBCF. An IMS-ALG provides the application level translation function for SIP and SDP in order to communicate between IPv6 and IPv4 SIP applications or, based on operator policies between different realms using the same IP version. The IBCF acts as a B2BUA when it performs IMS-ALG functionality.

### 6.1.3 TrGW

The TrGW is a NAT-PT/NAPT-PT, which uses a pool of globally unique IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across the IP version boundaries. NAT-PT binds addresses in IPv6 network with addresses in IPv4 network and vice versa to provide transparent routing between the two IP domain without requiring any changes to end points. NAPT-PT provides additional translation of transport identifier (TCP, SCTP and UDP port numbers). More detailed information on the NAT-PT/NAPT-PT is given in RFC 2766 [11] and RFC 2663 [12].

The TrGW may provide the NAT/NAPT functionality between two disparate address realms.

---

## 7 Control plane interworking

### 7.1 SIP with 3GPP Profile to Standard SIP Interworking

3GPP TS 24.229 [1] defines the procedures, which allow a 3GPP-IMS UE to connect to a standard SIP terminal.

### 7.2 Additional interworking of protocol associated with supplementary services

#### 7.2.1 General

This has no impact beyond that specified in subclause 7.1 provided the necessary SIP extensions are supported on both sides of the interworking point unless otherwise specified by subsequent subclause. Based on operator policy and/or service level agreements the interworking of services may be restricted.

Editor's Note: Impacts when the service is restricted or not supported on one of the interfaces is FFS.

#### 7.2.2 Terminating Identification Presentation (TIP) and Terminating Presentation Restriction (TIR)

See 3GPP TS 24.608 [21] for a description of the service.

If the other IP network is a trusted network and the RFC 3323 [22] and RFC 3325 [23] are supported the following header fields shall be forwarded without changes:

- P-Asserted-Identity header field; and
- Privacy header field.

If the IP network is not trusted the P-Asserted- Identity header field shall be removed from SIP requests and SIP responses.

#### 7.2.3 Common Basic Communication

See 3GPP TS 24.628 [24] for description of service.

Depending on the external IP network and message direction, the IBCF may have a local policy to remove an Error-Info header field, Call-Info header field and/or an Alert-Info header field.

---

## 8 User Plane Interworking

### 8.1 Overview

The present specification addresses user plane interworking between codec types used for either speech or video. Codecs used for conversational services in the PS domain are as defined in 3GPP TS 26.235 [6]. Codecs of particular interest are described in annex A.

### 8.2 VOID

## 8.3 VOID

---

# 9 IMS-ALG and TrGW functionality for NAPT and IP Version Interworking

## 9.1 Control plane interworking

### 9.1.1 Session Set-up

#### 9.1.1.0 General

The procedure described in Clause 9.1.1 applies both for an SDP offer received from the external network and received from the IMS.

If different IP versions are used in the external network and the IMS, the TrGW shall provide IP version interworking of the user plane. Otherwise, it provides NAPT functionality.

#### 9.1.1.1 Receipt of the first SDP offer

At the receipt of the first SDP offer from an offering network A the IMS-ALG shall:

- Request the TrGW to allocate a termination towards an answering network B and provide IP address(es) and port number(s) from its pool for this termination.

When the IMS-ALG has received the requested information from the TrGW, the IMS-ALG shall include the address(es) and port number(s) in a new offer, and sent this offer toward the network B. The IMS-ALG shall create a SIP message in accordance with the rules for the IMS\_ALG described in subclause 9.1.4 with the following clarification:

- The IP address(es) and port number(s) received from the TrGW for the termination towards network B shall replace the IP address(es) and port number(s) in the SDP.

#### 9.1.1.2 Receipt of the first SDP answer

At the receipt of the first SDP answer from network B the IMS-ALG shall:

- Provide to the TrGW the address(es) and port number(s) as received in the c-line(s) and m-line(s) in the SDP answer as destinations for the termination towards answering network B,
- Request the TrGW to allocate a termination towards the offering network A and provide IP address(es) and port number(s) from its pool for this termination, and provide the IP address and port number received in the first SDP offer from network A as destination for this termination, unless this step has already been executed earlier, e.g. at the receipt of the SDP offer, and
- Requests the TrGW to bind the termination towards network A and the the termination towards network B to enable the routing of user plane traffic towards the IPv4 SIP network through the TrGW.

Note: The binding request will be combined with the request to create terminations in the H.248 protocol

When the IMS-ALG has received the requested information, the IMS-ALG shall send an SDP answer to the network A. The IMS-ALG shall create the SIP message in accordance with the rules for the IMS ALG described in subclause 9.1.4 with the following clarification:

- The IP address(es) and port number(s) received from the TrGW for the termination towards network A shall replace the received IP address(es) and port number(s) in the SDP.

## 9.1.2 Void

## 9.1.3 Change of connection information

After the dialog is established it is possible for both ends of the session to change the connection data for the session. When the IMS-ALG/TrGW receives a SDP offer/answer where port number(s) or IP address(es) is included., there are four different possibilities:

- 1) IP address(es) or/and port number(s) have been added. In this case additional binding(s) shall be provided by the IMS-ALG/TrGW as detailed for the first SDP offer in the Clauses above;
- 2) IP address(es) or/and port number(s) have been deleted. In this case binding(s) shall be made free by the IMS-ALG/TrGW;
- 3) IP address(es) and port number(s) have been reassigned of the users. In this case the binding(s) shall reflect the reassignment;
- 4) No change has been made to the IP address(es) and port number(s). In this case no change shall be made to the existing binding(s).

## 9.1.4 Interworking of SIP messages

The IMS-ALG behaves as a SIP B2BUA when interworking SIP messages. The IMS-ALG shall forward all SIP messages transparently with respect to all methods, result codes, headers and attachments except as follows:

- The IMS-ALG modifies SDP according to subclauses 9.1.1, 9.1.2 and 9.1.3;
- When forwarding an incoming SIP request, the IMS-ALG should perform UAC procedures towards the intended target according to IETF RFC 3261 [2], by modifying those headers necessary to ensure that all transactions within the dialog pass through the IMS-ALG;
- When forwarding an incoming SIP response, the IMS-ALG should perform UAS procedures towards the originator of the corresponding request according to IETF RFC 3261 [2], by modifying those headers necessary to ensure that all transactions within the dialog pass through the IMS-ALG and
- The IMS-ALG may perform any appropriate error recovery procedures in the event that an incoming message contains errors inconsistent with the forwarding procedures above.

At the receipt of a BYE request, CANCEL request or non-200 final response, the IMS-ALG shall release the session and request the TrGW to release the bindings established for the session.

# 9.2 User plane transport

## 9.2.1 Payload transport

The TrGW shall use the established bindings described above to transport the messages between the network A and the network B in the following way.

At the receipt of a payload message the TrGW shall:

- Replace the received destination IP address(es) and port number(s) in the payload message with the corresponding IP address(es) and port number(s) that have been signalled by the IBCF.- Replace the received source IP address(es) and port number(s) in the payload message with the corresponding IP address(es) and port number(s) the TrGW allocated at its own terminations.

## 9.2.2 IP header interworking

### 9.2.2.1 IPv4 to IPv6

When the TrGW receives an IPv4 message the following codings shall be set in the IPv6 headers of the message sent to the IPv6 network.

- If the DF bit is set and the packet is not a fragment (i.e., the MF flag is not set and the Fragment Offset is zero) The IPv6 headers shall be set as described in Table 1;
- If the DF bit is not set or the packet is a fragment the IPv6 headers shall be set as described in Table 2.

**Table 1: Derivation of IPv6 Header from IPv4 header (no fragmentation)**

IPv6 field	Value
Version	6
Traffic Class:	The default behaviour is that the value of the IPv6 field Traffic Class field is the value of the IPv4 Type Of Service field (all 8 bits are copied). An implementation of a TrGW should also provide the ability to ignore the value of the IPv4 Type of Service and always set the IPv6 traffic class field to zero.
Flow label	The Ipv6 Flow Label Field is set to 0 (all zero bits)
Payload Length	The IPv6 Payload Length field value is the IPv4 Total length field value minus the size of the IPv4 header and IPv4 options field length, if present.
Next Header	The Ipv6 Next Header value is copied from IPv4 Protocol field
Hop Limit:	The IPv6 Hop Limit value is The value of IPv4 field Time To Live minus 1
Source Address	Shall be handled as the addresses of the payload message as described in subclause 9.2.1.
Destination Address	Shall be handled as the addresses of the payload message as described in subclause 9.2.1.

**Table 2: Derivation of IPv6 Header from IPv4 Header (fragmentation)**

IPv6 field	Value
Version	6
Traffic Class:	The default behaviour is that the value of the IPv6 field Traffic Class field is the value of the IPv4 Type Of Service field (all 8 bits are copied). An implementation of a TrGW should also provide the ability to ignore the value of the IPv4 Type of Service and always set the IPv6 traffic class field to zero.
Flow label	The Ipv6 Flow Label Field is set to 0 (all zero bits)
Payload Length	The IPv6 Payload Length field value is the IPv4 Total length field value plus 8 for the fragment header minus the size of the IPv4 header and IPv4 options field length, if present.



IPv6 field	Value
Version	6
Next Header	The IPv6 Next header field is set to Fragment header (44).
Hop Limit:	The IPv6 Hop Limit value is The value of IPv4 field Time To Live minus 1
Source Address	Shall be handled as the addresses of the payload message as described in subclause 9.2.1.
Destination Address	Shall be handled as the addresses of the payload message as described in subclause 9.2.1.
Fragments headers a) next header b) fragment Offset c) More fragment bit d) Identification	Copied from IPv4 Protocol field Copied from the IPv4 Fragment offset field Copied from the value of the more fragment bit in the IPv4 flags field The low-order 16 bits copied from IPv4 Identification field. The high-order 16 bits set to zero.

### 9.2.2.2 Abnormal cases

If IPv4 options are present in the IPv4 packet, they should be ignored i.e., there is no attempt to translate them. However, if an unexpired source route option is present then the packet shall instead be discarded, and an ICMPv4 "destination unreachable/source route failed" Type 3/Code 5 error message shall be returned to the sender as defined in IETF RFC 792 [16]

When a translator receives the first fragment of a fragmented UDP IPv4 packet and the checksum field is zero the translator should drop the packet and generate a system management event specifying at least the IP addresses and port numbers in the packet. When it receives fragments other than the first it should silently drop the packet since there is no port information to log.

When a translator receives an unfragmented UDP IPv4 packet and the checksum field is zero the translator shall compute the missing UDP checksum as part of translating the packet. Also, the translator should maintain a counter of how many UDP checksums are generated in this manner.

### 9.2.2.3 IPv6 to IPv4

When the TrGW receives an IPv6 message the following codings shall be set in the IPv4 headers of the message sent to the IPv4 network.

- If there is no IPv6 fragment header, the IPv4 header fields shall be set as described in Table 3;
- If there is an IPv6 fragment header, the IPv4 header fields shall be set as described in Table 4;

**Table 3: Derivation of IPv4 Header from IPv6 Header (no fragmentation)**

IPv4 field	Value
Version	4
Internet header length	5 (No IPv4 options)
Type of Service	The default behaviour is that the value of the IPv4 field Type of service field is the value of the IPv6 Traffic class field (all 8 bits are copied). An implementation of a TrGW should also provide the ability to ignore the value of the IPv6 Traffic Class and always set the IPv4 Type of Service field to zero.
	The IPv4 Total Length field value is the IPv6 Payload length value plus

IPv4 field	Value
Version	4
Total length	the size of the IPv4 headers.
Identification	All bits are set to zero
Flags	The more fragment flag is set to zero. The Don't fragment flag is set to one.
Fragment offset	Set to zero
Time to live (TTL)	The value of the field shall be set to the received IPv6 Hop Limit field value minus 1.
Protocol	The IPv4 field Protocol shall be set to the value of IPv6 field The next header value.
Header checksum	Computed once the IPv4 header has been created.
Source Address	Shall be handled as the addresses of the payload message as described in subclause 9.2.1.
Destination Address	Shall be handled as the addresses of the payload message as described in subclause 9.2.1.

**Table 4: Derivation of IPv4 Header from IPv6 Header (fragmentation)**

IPv4 field	Value
Version	4
Internet header length	5 (No IPv4 options)
Type of Service and Precedence:	The default behaviour is that the value of the IPv4 field Type of service field is the value of the IPv6 Traffic class field (all 8 bits are copied). An implementation of a TrGW should also provide the ability to ignore the value of the IPv6 Traffic Class and always set the IPv4 Type of Service field to zero.
Total length	The IPv4 Total Length field value is the IPv6 Payload length value plus the size of the IPv4 headers minus 8 for the Fragment header,
Identification	The IPv4 Identification field is copied from the low-order 16-bits in the IPv6 identification field in the IPv6 Fragment header.
Flags	The IPv4 the More Fragments flag is copied from the IPv6 M flag in the IPv6 Fragment header the IPv4 he Don't Fragments flag is set to zero allowing this packet to be fragmented by IPv4 routers.
Time to live (TTL)	The value of the field shall be set to the received IPv6 Hop Limit field value minus 1.
Protocol	The IPv4 field Protocol shall be set to the value of IPv6 field The next header value.
Header checksum	Computed once the IPv4 header has been created
Source Address	Shall be handled as the addresses of the payload message as described in subclause 9.2.1.
Destination Address	Shall be handled as the addresses of the payload message as described in subclause 9.2.1.

### 9.2.2.4 Abnormal cases

If any of an IPv6 hop-by-hop options header, destination options header, or routing header with the Segments Left field equal to zero are present in the IPv6 packet, they are ignored i.e., there is no attempt to translate them. However, the Total Length field and the Protocol field shall be adjusted to "skip" these extension headers.

If a routing header with a non-zero Segments Left field is present then the packet shall be translated, and an ICMPv6 "parameter problem/ erroneous header field encountered" Type 4/Code 0 error message as defined in IETF RFC 2463 [17], with the Pointer field indicating the first byte of the Segments Left field should be returned to the sender.

### 9.2.3 Fragmentation

If the DF flag is not set and the IPv4 packet will result in an IPv6 packet larger than 1280 bytes the TrGW shall prior to transferring it in the IPv6 network:

- Add the fragment header to the message
- Fragment the IPv4 packets so that their length, excluding the IPv4 header, is at most 1232 bytes (1280 minus 40 for the IPv6 header and 8 for the Fragment header).

### 9.2.4 Abnormal cases

As a part of decrementing the Time To Live /Hop Limit value and the TrGW discovers that the zero value is reached the TrGW shall send an ICMPv4/ICMPv6 message with the error 'time to live exceeded in transit' type 11 code 0 as defined in IETF RFC 792 [16] and 'hop limit exceeded in transit' type 3 code 0 as defined in IETF RFC 2463 [17].

## 10 IBCF – TrGW Interactions

### 10.1 Overview

#### 10.1.1 General

The present specification describes Ix signalling procedures and their interaction with SIP signalling in the control plane, and with user plane procedures. Each scenario or "use case" is described in a separate sub-clause within 10.2. 3GPP TS 29.238 [25] maps these signalling procedures to H.248 messages and defines the required H.248 profile (which provides details of used packages and parameters).

#### 10.1.2 Network model

Figure 10.1.2.1 shows the network model. The broken line represents the call control signalling. The dotted line represents the user plane. The IBCF uses one context with two terminations in the TrGW.

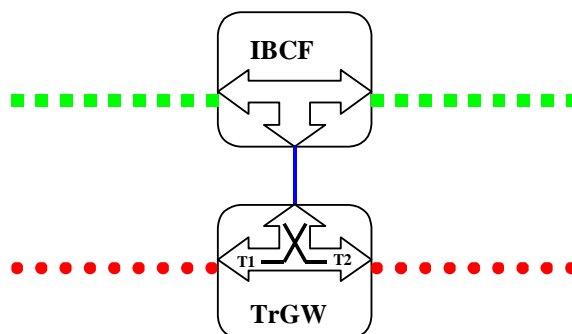


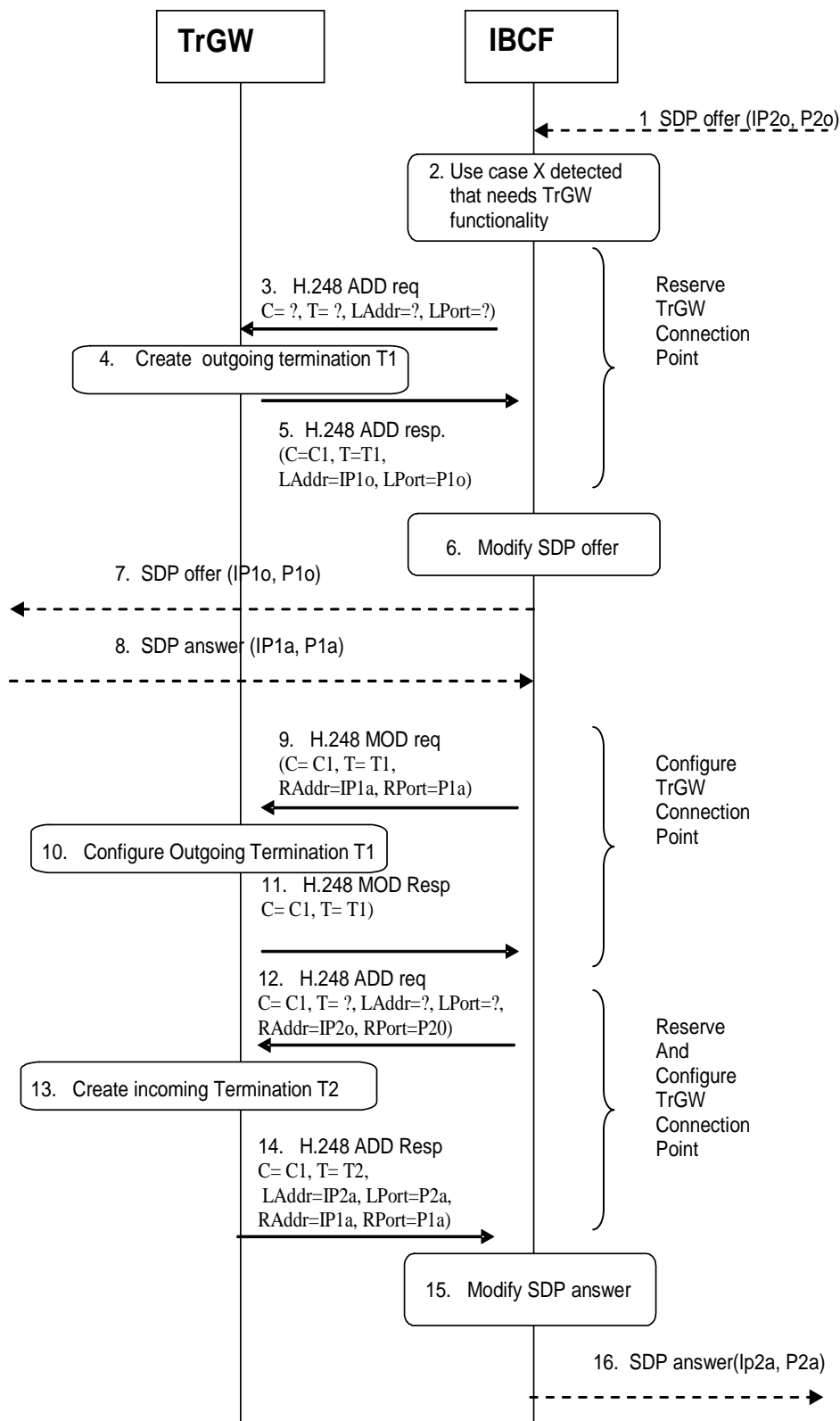
Figure 10.1.2.1: Network model

## Example Call Flow

### 10.1.3.1 Basic Procedures

#### 10.1.3.1.1 Call Establishment

Figure 10.1.3.1.1.1 depicts the signalling flow for a call setup either from or toward an external network.



1. The IBCF receives an SDP offer in SIP signalling.
2. The IBCF detects that one of the CS-TrGW functions is required, e.g. NAPT/NAT.
3. The IBCF sends a H.248 ADD command to create the outgoing termination and to request resources to execute TrGW function.
4. The TrGW creates the outgoing termination.
5. The TrGW replies to IBCF with a H.248 Add reply command and provides the local address and port of the outgoing termination.
6. The IBCF replaces the IP address inside the SDP using the information coming from TrGW.
7. SDP offer is sent to the network at the outgoing side.
8. SDP answer is received by IBCF.

9. The IBCF sends a H.248 MOD command to configure the outgoing termination with address and port information received in the SDP answer.
  10. The TrGW configures the outgoing termination.
  11. The TrGW replies to IBCF with a H.248 MOD reply command.
  12. The IBCF sends a H.248 ADD command to create the incoming termination and to request resources to execute TrGW function.
  13. The TrGW creates the incoming termination.
  14. The TrGW replies to the IBCF with a H.248 Add reply command and provides the local address and port of the incoming termination..
- Note:
- Steps 12 to 14 may also be executed after step 2.
  15. The IBCF replaces the IP address inside the SDP using the information coming from TrGW.
  16. SDP answer is sent to the network at the incoming side.

**Figure 10.1.3.1.1.1: IBCF and TrGW interaction at Call establishment.**

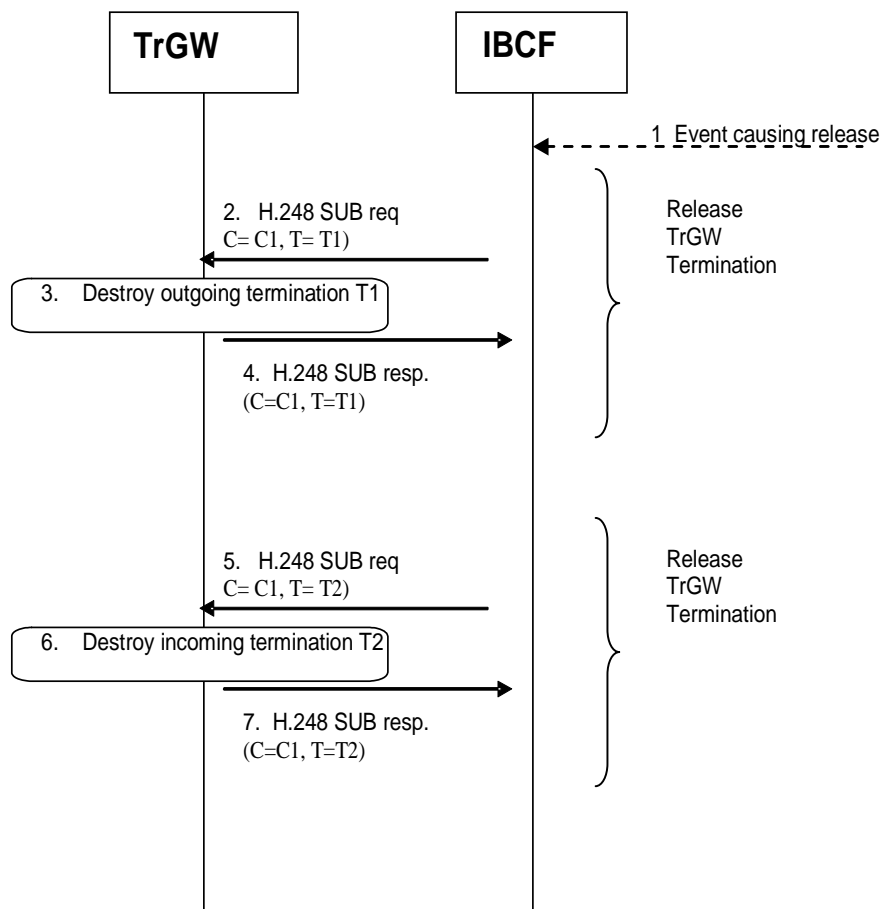
When creating the termination towards the IMS network, the IBCF may also indicate that the IP Interface Type is "MboIP".

*Editor's note: The IP Interface Type for the termination towards the external network is FFS, since the reference point for the user plane interface between the TrGW and the external network can be either Mb or Izi.*

The IP Interface Type allows the TrGW to collect statistics per interface type associated with the RTP bearer termination. The provision of these statistics is outside of the scope of this specification.

10.1.3.1.2 Call Release

Figure 10.1.3.1.2.1 depicts the signalling flow for a call release.



1. The IBCF identifies that the call is to be release. Typically this will be by the receipt of a SIP BYE request.
2. The IBCF sends a H.248 SUB command to release the outgoing termination
3. The TrGW destroys the outgoing termination
4. The TrGW replies to IBCF with a H.248 Sub reply command
5. The IBCF sends a H.248 SUB command to release the incoming termination
6. The TrGW destroys the incoming termination
7. The TrGW replies to IBCF with a H.248 Sub reply command

Note 1: Steps 5 to 7 may also be executed before steps 2 to 4 or in parallel with steps 2 to 4.

Note 2: Rather than releasing the two terminations separately, the IBCF may request the TrGW to release both terminations in a single request.

**Figure 10.1.3.1.2.1: IBCF and TrGW interaction at Call release**

## 10.2.0 Introduction

The following functions shall be supported by the TrGW:

- Gate Management:
  - Opening/closing of gates;
  - Remote source address filtering;
  - Remote source port filtering;
- QoS packet marking (differentiated services);
- NAT and IP Version Interworking;
- Bandwidth policing;
- Hanging termination detection;
- IP Realm Indication.

Additionally, the following functions may be supported by the TrGW:

- Resource allocation per flow;
- Detection and reporting of inactive media flows;
- IP Realm Availability.

## 10.2 Main Functions supported at the Ix Interface

### 10.2.1 IP Address and Port Conversion

The IP Address and port conversion is configured by the standard Ix interactions at call setup depicted in Figure 10.1.3.1.1.1. IP address and port conversion functionality documented in Clause 9.

IP address and port conversion is mandatory every time a TrGW is inserted into the path for any reason to guarantee that all IP packets are routed through this entity.

### 10.2.2 Gate Management

The procedures in subclause A.7.1.2.2.3 of 3GPP TS 29.235 [29] are applicable.

### 10.2.3 Handling of RTCP Streams

The procedures in subclause A.7.1.2.2.x of 3GPP TS 29.235 [29] are applicable.

## 10.2.4 IP Realm/Domain Indication

Whenever requesting a new IP media-path (i.e. creation of IP bearer terminations), the TrGW may indicate the correspondent IP realm/domain to the TrGW. The TrGW shall assign the IP termination in the IP realm indicated. The same IP realm shall be applied to all media streams associated with the termination. The IP realm identifier shall not be changed after the initial assignment.

A default IP realm may be configured such that if the TrGW has not received the IP realm identifier and the TrGW supports multiple IP realms then the default IP realm shall be used.

## 10.2.5 Media Control

The transcoding functionality, where the TrGW processes and possibly converts application / media data (like e.g. RTP payload) is optional for the TrGW and IBCF to support.

The IBCF shall determine the TrGW transcoding capability through provisioning and MGW selection, outside the scope of this specification.

IBCF procedures to offer transcoding in SIP/SDP signalling are described in 3GPP TS 23.228 [8] and in 3GPP TS 24.229 [1]. The IBCF shall only apply those transcoding procedures if an attached TrGW supports transcoding. For media with "RTP/SAVP" (see IETF RFC 3711 [34]) or "RTP/SAVPF" (see IETF RFC 5124 [35]) as transport protocol, the IBCF shall not offer or apply transcoding.

If the IBCF and available TrGW support transcoding, the IBCF may add codecs to a SDP offer within a SIP request,

If the IBCF and available TrGW do not support transcoding, or if the IBCF chooses not to offer transcoding, the IBCF shall pass SDP offers without adding codecs to the SDP offer and the IBCF shall pass SDP answers without modification to the contained codecs.

If the IBCF does not offer or apply transcoding procedures (as described above) but inserts the TrGW for any other reason, the IBCF shall either not signal media related information to the TrGW, or it shall signal the same media related information for all interconnected terminations (i.e. identical media configurations for the two connected H.248 stream endpoints).

If the IBCF does not offer or apply transcoding it but signals media attributes to a TrGW that does not support transcoding without having seized the peer termination (see Figure 10.2.5.3, Step 3) the TrGW shall accept this request even though it cannot reserve any transcoding resources related to this media. When the peer Termination is seized and configured it shall be configured with the same media related sub-fields in the media descriptor as for the first Termination. If the selected codec is not the same as the codec configured at the first termination then this termination shall be modified before the peer termination is seized.

NOTE 1: The signalling of such codec related information by an IBCF to a TrGW not supporting transcoding is an implementation decision.

NOTE 2: A TrGW not supporting transcoding can use such codec related information to learn that RTCP ports need to be reserved, and to derive information about packet size and frequency useful for internal resource reservation.

If the IBCF and available TrGW support transcoding and the IBCF includes in a SDP offer additional codecs, the following procedures apply:

- The IBCF may seize a termination towards the terminating user, using the "Reserve TrGW Connection Point" procedure before sending an SDP offer with added codecs to the terminating user. The IBCF may signal media related information to the TrGW or omit media when adding the IP termination at this stage.

NOTE 3: the signalling of media related information to a MGW requires that it reserve the indicated resources before returning a positive response to the H.248 command, by omitting media related information the TrGW does not need to reserve any associated resources at this stage.

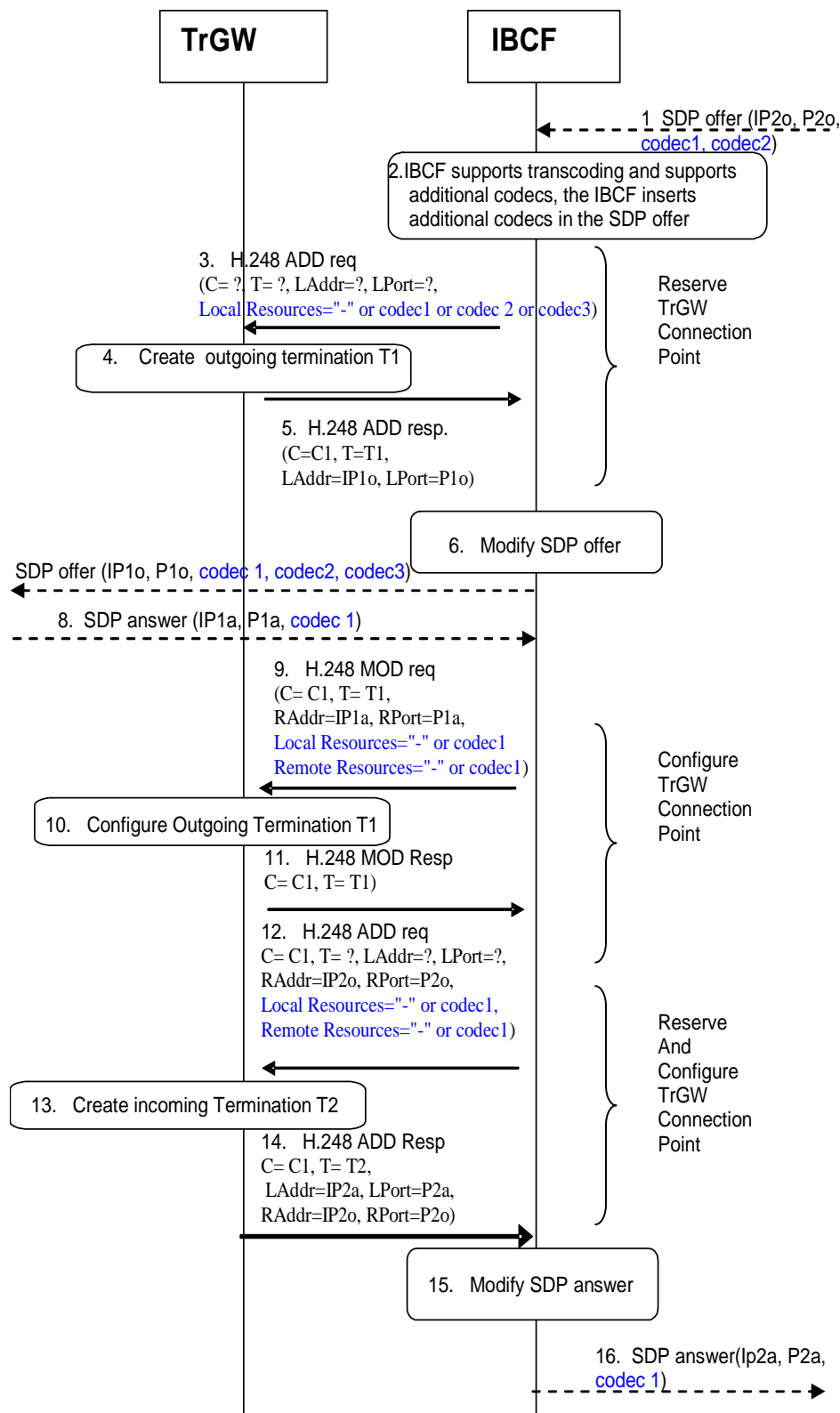
- When the IBCF receives the SDP answer from the terminating user, the IBCF shall check if any of the codecs offered by the originating side are contained in the answer.
- If only the codecs inserted by the IBCF are contained in the answer, the IBCF shall configure the TrGW to transcode. If it previously performed a "Reserve TrGW Connection Point" procedure it shall configure the



TrGW using the "Configure TrGW Connection Point" procedure towards the termination on the terminating user side by supplying the media returned in the answer from the terminating user, otherwise it shall perform a "Reserve and Configure TrGW Connection Point" procedure. Within those procedures, the IBCF shall supply the media returned in the answer from the terminating user. If the IBCF seized the termination only at this point in time, it shall send the IP address and port information received from the TrGW in the acknowledgment to the "Reserve and Configure TrGW Connection Point" procedure towards the terminating user in a new SDP offer. The IBCF shall perform the "Reserve and Configure TrGW Connection Point" procedure towards the termination on the originating user side, supplying the preferred media offered by the originating side.

- If the returned SDP contains media offered by the originating user no transcoding at the TrGW is required. If the IBCF previously performed the "Reserve TrGW Connection Point" procedure the IBCF shall configure the TrGW accordingly by either either supplying the same media related information for all interconnected terminations or by omitting the media related information.

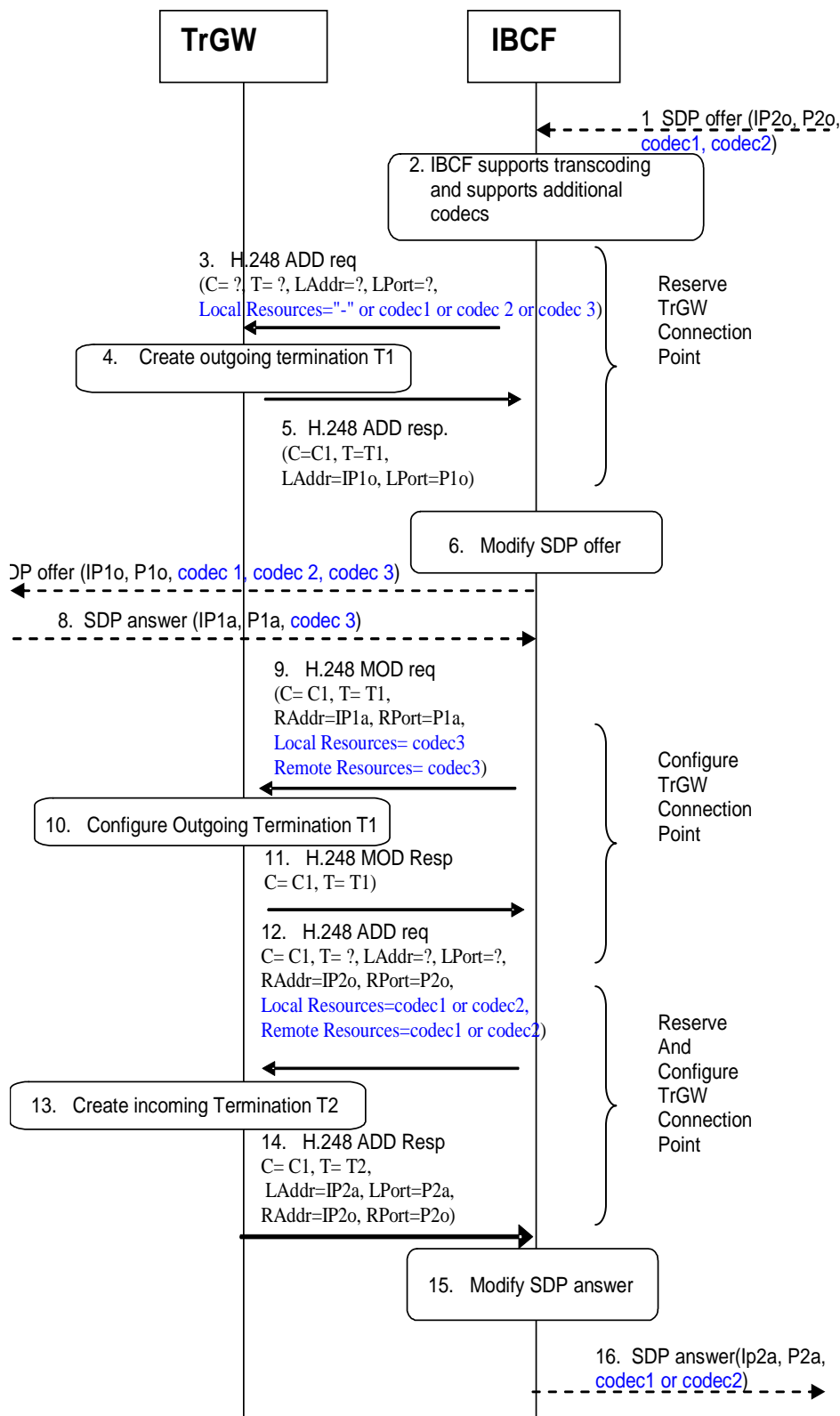
Some basic use cases are depicted in figures 10.2.5.1 and 10.2.5.2, and 10.2.5.3



1. The IBCF receives an SDP offer in SIP signalling.
2. The IBCF adds additional codecs to the subsequent SDP offer, giving priority to those offered by the preceding node/network.
3. In this example the IBCF seizes a TrGW prior to sending the new SDP offer; as this scenario is preparing for a possible transcoding in the TrGW then a TrGW supporting media shall be seized. The IBCF sends a H.248 ADD command to create the outgoing termination and to request IP resources to execute TrGW function. As no media transcoding is yet known to be needed this may be indicated by omitting media related sub-fields in the media descriptor (i.e. signalling "-"). Alternatively the preferred codec (e.g. Codec 1) may be signalled in order to reserve this resource in the event that transcoding was required.
4. The TrGW creates the outgoing termination.

5. The TrGW replies to IBCF with a H.248 Add reply command and provides the local address and port of the outgoing termination.
6. The IBCF replaces the IP address inside the SDP using the information coming from TrGW
7. The IBCF forwards the new offer to the succeeding node. 8. SDP answer is received by IBCF. In this example the codec1 received in the original SDP offer in step1 has been selected by the succeeding network/terminating UE and the IBCF determines that transcoding is not required.
9. The IBCF sends a H.248 MOD command to configure the outgoing termination with address and port information received in the SDP answer. As no media transcoding is needed this may be indicated by omitting media related sub-fields in the media descriptor (i.e. signalling "-"). Alternatively the selected codec (Codec 1) may be signalled
10. The TrGW configures the outgoing termination.
11. The TrGW replies to IBCF with a H.248 MOD reply command.
12. The IBCF sends a H.248 ADD command to create the incoming termination to configure this termination with remote address and port information and to request resources to execute TrGW function. As no media transcoding is needed this may be indicated by omitting media related sub-fields in the media descriptor (i.e. signalling "-"). Alternatively the selected codec received in step 8 (Codec 1) may be signalled
13. The TrGW creates the incoming termination.
14. The TrGW replies to the IBCF with a H.248 Add reply command and provides the local address and port of the incoming termination.
15. The IBCF replaces the IP address inside the SDP using the information coming from TrGW.
16. SDP answer is sent to the network at the incoming side.

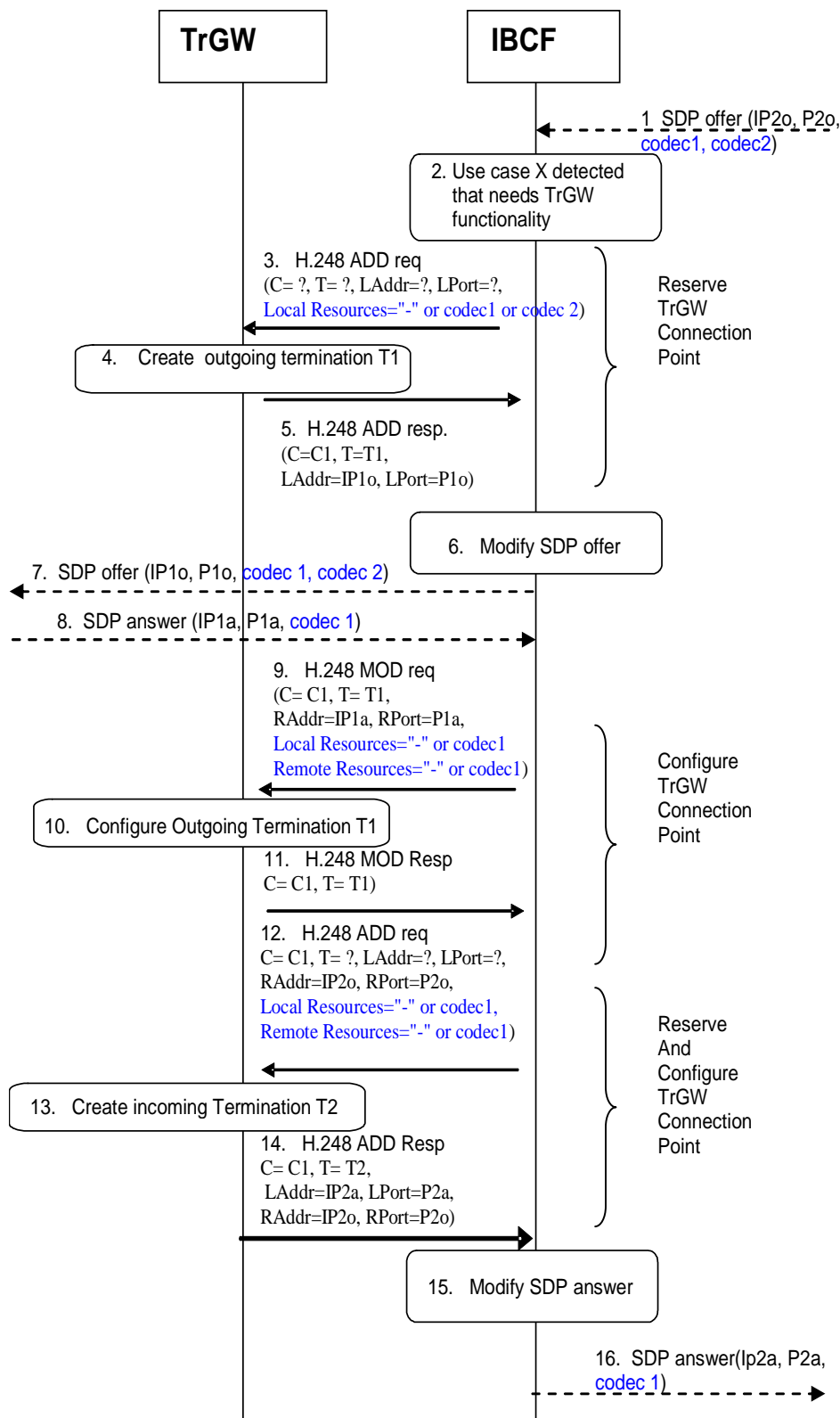
**Figure 10.2.5.1: IBCF and TrGW interaction when the IBCF offers additional codecs but no transcoding is required, and the TrGW is seized in advance.**



1. The IBCF receives an SDP offer in SIP signalling.
2. The IBCF adds additional codecs to the subsequent SDP offer, giving priority to those offered by the preceding node/network.
3. In this example the IBCF seizes a TrGW prior to sending the new SDP offer; as this scenario is preparing for a possible transcoding in the TrGW then a TrGW supporting media shall be seized. The IBCF sends a H.248 ADD command to create the outgoing termination and to request IP resources to execute TrGW function. As no media transcoding is yet known to be needed this may be indicated by omitting media related sub-fields in the media descriptor (i.e. signalling "-"). Alternatively the preferred codec (e.g. Codec 1) may be signalled in order to reserve this resource in the event that transcoding was required.
4. The TrGW creates the outgoing termination.

5. The TrGW replies to IBCF with a H.248 Add reply command and provides the local address and port of the outgoing termination.
6. The IBCF replaces the IP address inside the SDP using the information coming from TrGW.
7. The IBCF forwards the new offer to the succeeding node.
8. The SDP answer is received by IBCF. In this example the codec3 added by the IBCF to the SDP offer has been selected. Transcoding is therefore required.
9. The IBCF sends a H.248 MOD command to configure the outgoing termination with address and port information received in the SDP answer and the selected media attributes (codec 3).
10. The TrGW configures the outgoing termination.
11. The TrGW replies to IBCF with a H.248 MOD reply command.
12. The IBCF sends a H.248 ADD command to create the incoming termination to configure this termination with remote address and port information and to request resources to execute TrGW function. As media transcoding is required it indicates this explicitly with a codec selected by the IBCF for the incoming termination from the offered codec(s) received in step1.
13. The TrGW creates the incoming termination.
14. The TrGW replies to the IBCF with a H.248 Add reply command and provides the local address and port of the incoming termination..
15. The IBCF replaces the IP address inside the SDP using the information coming from TrGW and replaces the codec with the codec it selected for the incoming termination.
16. SDP answer is sent to the network at the incoming side.

**Figure 10.2.5.2: IBCF and TrGW interaction when IBCF offers additional codecs and transcoding is required, and the TrGW is seized in advance.**



1. The IBCF receives an SDP offer in SIP signalling.
2. The IBCF requires a TrGW for another use case but does not offer transcoding.
3. The IBCF sends a H.248 ADD command to create the outgoing termination and to request IP resources to execute TrGW function. As no media transcoding is required this may be indicated by signalling "-". Alternatively the any codec (e.g. Codec 1) can be signalled. If the IBCF selects a TrGW that does not support transcoding, the IBCF may signal media related sub-fields in the media descriptor to the TrGW if the TrGW supports media encoding. The TrGW shall accept the ADD request even though it cannot reserve any transcoding resources for the indicated media.
4. The TrGW creates the outgoing termination.

5. The TrGW replies to IBCF with a H.248 Add reply command and provides the local address and port of the outgoing termination.
6. The IBCF replaces the IP address inside the SDP using the information coming from TrGW .
7. The IBCF forwards the new offer to the succeeding node.
8. The SDP answer is received by IBCF. In this example the codec1 received in the original SDP offer in step1 has been selected.
9. The IBCF sends a H.248 MOD command to configure the outgoing termination with address and port information. As no media transcoding is needed this may be indicated by signalling "-" .Alternatively the selected codec (Codec 1) can be signalled.
10. The TrGW configures the outgoing termination.
11. The TrGW replies to IBCF with a H.248 MOD reply command.
12. The IBCF sends a H.248 ADD command to create the incoming termination to configure this termination with remote address and port information and to request resources to execute TrGW function. As no media transcoding is needed this may be indicated by signalling "-" .Alternatively media related sub-fields in the media descriptor for the codec indicated to the incoming termination may be signalled (e.g. the selected codec received in step 8 (Codec 1).
13. The TrGW creates the incoming termination.
14. The TrGW replies to the IBCF with a H.248 Add reply command and provides the local address and port of the incoming termination.
15. The IBCF replaces the IP address inside the SDP answer using the information coming from TrGW.
16. SDP answer is sent to the network at the incoming side.

**Figure 10.2.5.3: IBCF and TrGW interaction when IBCF does not offer transcoding**

## 10.2.6 Media Inactivity Detection

The procedures in subclause A.7.1.2.2.6 of 3GPP TS 29.235 [29] are applicable.

## 10.2.7 QoS Packet Marking

The procedures in subclause A.7.1.2.2.4 of 3GPP TS 29.235 [29] are applicable.

Those procedures relate to Diffserv code point marking as described in IETF RFC 2474 [31]

## 10.2.8 Hanging Termination Detection

The procedures in subclause A.7.1.2.2.2 of 3GPP TS 29.235 [29] are applicable.

## 10.2.9 Traffic Policing

The procedures in subclause A.7.1.2.2.8 of 3GPP TS 29.235 [29] are applicable.

## 10.2.10 IMS end-to-end media plane security

The IBCF may support the end-to-end IMS media plane security as specified in 3GPP TS 33.328 [32]. If supported, the IBCF shall use the following procedures.

If the IBCF receives SDP containing media lines with "RTP/SAVP" (see IETF RFC 3711 [34]) or "RTP/SAVPF" (see IETF RFC 5124 [35]) as transport protocol, the IBCF shall:

- forward the SDP with unmodified transport protocol for those media lines;
- apply the procedures to not offer or apply transcoding defined in subclause 10.2.5; and
- configure the TrGW to pass media transparently.

NOTE: The transport protocol that the IBCF provides to the TrGW is FFS.

If the IBCF receives SDP containing SDES SDP attribute(s) according to IETF RFC 4568 [33], it shall forward the SDP with unmodified SDES SDP attribute(s), but shall not provide the SDES SDP attribute(s) to the TrGW.

## 10.3 VOID

## 10.4 Procedures

### 10.4.1 Call related Procedures

#### 10.4.1.1 Reserve TrGW Connection Point

This procedure is used to reserve an termination at the TrGW.



Table 10.4.1.1.1: Reserve TrGW Connection Point

Procedure	Initiated	Information element name	Information element required	Information element description
Reserve TrGW Connection Point	IBCF	Context/Context Request	M	This information element indicates the existing context or requests a new context for the bearer termination.
		Termination Request	M	This information element requests a new termination for the bearer to be established.
		IP Interface	O	This information element specifies the type of external interface to be used for the IP termination (e.g. MboIP).
		Local IP Resources	O	This information element indicates the resource(s) (e.g. codec, auxiliary payload types) for which the TrGW shall be prepared to receive user data. May be excluded (i.e. "-" is used in SDP m-line) if no transcoding or other media related functions are required.
		ReserveValue	C	This information element indicates if multiple local resources are to be reserved. This information element shall be included if a speech codec and auxiliary payload types are configured.
		Local Connection Address Request	M	This information element requests an IP address and port number on the TrGW that the remote end can send user plane data to.
		Remote Source Address Filtering	O	This information element indicates that remote source address filtering is required.
		Remote Source Address Mask	C	This information element provides information on the valid remote source addresses. This may be included if remote source address filtering is included. It shall not be included if remote source address filtering is not included.
		Remote Source Port Filtering	O	This information element indicates that remote source port filtering is required.
		Remote Source Port	C	This information element identifies the valid remote source port. This may be included if remote source port filtering is included. It shall not be included if remote source port filtering is not included. (NOTE 1)
		Remote Source Port Range	C	This information element identifies a range of valid remote source ports. This may be included if remote source port filtering is included. It shall not be included if remote source port filtering is not included. (NOTE 1)
		RTCP handling	O	Indicates whether or not the TrGW shall reserve a port for an RTCP flow.
		Notify termination heartbeat	M	This information element requests termination heartbeat indications.
		Notify Released Bearer	O	This information element requests a notification of a released bearer.
DiffServ Code Point	O	This information element indicates a specific DiffServ code point to be used in the IP header in packets sent on the IP termination.		

		DiffServ Tagging Behaviour	O	This information element indicates whether the Diffserv code point in the IP header in packets sent on the IP termination should be copied from the received value or set to a specific value.
		IP Realm Identifier	O	This information element indicates the IP realm of the IP termination.
		Traffic Policing Required	O	This information element indicates that policing of the media flow is required.
		Peak Data Rate	O	This information element may be present if Policing is required and specifies the permissible peak data rate for a media stream. (NOTE 2)
		Sustainable Data Rate	O	This information element may be present if Policing is required and specifies the permissible sustainable data rate for a media stream. (NOTE 2)
		Delay Variation Tolerance	O	This information element may be present if Policing on Peak Data Rate is required and specifies the maximum expected delay variation tolerance for the corresponding media stream.
		Maximum Burst Size	C	This information element shall be present if Policing on Sustainable Data Rate is required and specifies the maximum expected burst size for the corresponding media stream.
		Media Inactivity Detection Required	O	This information element indicates that detection of inactive media flows is required.
		Inactivity Detection Time	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection time.
		Inactivity Detection Direction	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection direction.
Reserve TrGW Connection Point Ack	TrGW	Context	M	This information element indicates the context where the command was executed.
		Termination	M	This information element indicates the termination where the command was executed.
		Local IP Resources	C	This information element indicates the resources that the TrGW has reserved to receive the user plane data from the remote peer.
		Local Connection Address	M	This information element indicates the IP address and port on the TrGW that shall receive user plane data from the remote peer.
NOTE 1: Remote Source Port and Remote Source Port Range are mutually exclusive.				
NOTE 2: At least one of these IEs shall be present when policing is required.				

**Editor's Note:** For the Reserve TrGW Connection Point Ack, it is ffs if Local IP Resources is mandatory or optional to be included if present in the request, currently in other profiles such as Mc this is mandatory to be returned if sent in the request.

#### 10.4.1.2 Configure TrGW Connection Point

This procedure is used to configure or reconfigure an termination at the TrGW.

Table 10.4.1.2.1: Configure TrGW Connection Point Procedure

Procedure	Initiated	Information element name	Information element required	Information element description
Configure TrGW Connection Point	IBCF	Context	M	This information element indicates the existing context.
		Termination	M	This information element indicates the existing bearer termination.
		IP Interface	O	This information element specifies the type of external interface to be used for the IP termination (e.g. MboIP).
		Local IP Resources	O	This information element indicates the resources (e.g. codec, auxiliary payload types) that the TrGW may use on the reception of user plane data. If Local Connection Address is supplied may be excluded (i.e. "-" is used in SDP m-line) if no transcoding or other media related functions are required.
		Remote IP Resources	O	This information element indicates the resources (e.g. codec, auxiliary payload types) that the TrGW may send user plane data to. If Remote Connection Address is supplied may be excluded (i.e. "-" is used in SDP m-line) if no transcoding or other media related functions are required.
		Local Connection Address	O	This information element indicates the IP address and port on the TrGW that the remote peer can send user plane data to.
		Remote Connection Address	O	This information element indicates the IP address and port that the TrGW can send user plane data to.
		Reserve Value	C	This information element indicates if multiple resources are to be reserved. This information element shall be included if a speech codec and auxiliary payload types are configured.
		Remote Source Address Filtering	O	This information element indicates that remote source address filtering is required.
		Remote Source Address Mask	C	This information element provides information on the valid remote source addresses. This may be included if remote source address filtering is included. It shall not be included if remote source address filtering is not included.
		Remote Source Port Filtering	O	This information element indicates that remote source port filtering is required.
		Remote Source Port	C	This information element identifies the valid remote source port. This may be included if remote source port filtering is included. It shall not be included if remote source port filtering is not included. (NOTE 1)
		Remote Source Port Range	C	This information element identifies a range of valid remote source ports. This may be included if remote source port filtering is included. It shall not be included if remote source port filtering is not included. (NOTE 1)
		RTCP handling	O	Indicates whether or not the TrGW shall reserve a port for an RTCP flow
Traffic Policing Required	O	This information element indicates that policing of the media flow is required.		

		Peak Data Rate	O	This information element may be present if Policing is required and specifies the permissible peak data rate for a media stream. (NOTE 2)
		Sustainable Data Rate	O	This information element may be present if Policing is required and specifies the permissible sustainable data rate for a media stream. (NOTE 2)
		Delay Variation Tolerance	O	This information element may be present if Policing on Peak Data Rate is required and specifies the maximum expected delay variation tolerance for the corresponding media stream.
		Maximum Burst Size	C	This information element shall be present if Policing on Sustainable Data Rate is required and specifies the maximum expected burst size for the corresponding media stream.
		DiffServ Code Point	O	This information element indicates a specific DiffServ code point to be used in the IP header in packets sent on the IP termination.
		DiffServ Tagging Behaviour	O	This information element indicates whether the Diffserv code point in the IP header in packets sent on the IP termination should be copied from the received value or set to a specific value.
		Media Inactivity Detection Required	O	This information element indicates that detection of inactive media flows is required.
		Inactivity Detection Time	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection time.
		Inactivity Detection Direction	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection direction.
Configure TrGW Connection Point Ack	TrGW	Context	M	This information element indicates the context where the command was executed.
		Termination	M	This information element indicates the termination where the command was executed.
		Local IP Resources	O	This information element indicates the resources that the TrGW has reserved to receive the user plane data from the far end.
		Remote IP Resources	O	This information element indicates the resource (i.e. codec) that the TrGW shall use to send user data to. May be present only if corresponding IE is present in the request.
		Local Connection Address	O	This information element indicates the IP address and port on the TrGW that the remote end can send user plane data to.
		Remote Connection Address	O	This information element indicates the IP address and port that the TrGW can send user plane data to. May be present only if corresponding IE is present in the request.
NOTE 1: Remote Source Port and Remote Source Port Range are mutually exclusive.				
NOTE 2: At least one of these IEs shall be present when policing is required.				

Editor's Note: For the Configure TrGW Connection Point Ack , it is ffs if Local IP Resources is mandatory or optional to be included if present in the request, currently in other profiles such as Mc this is mandatory to be returned if sent in the request.

### 10.4.1.3 Reserve and Configure TrGW Connection Point

This procedure is used to reserve and configure multimedia-processing resources for a termination at the TrGW.

Table 10.4.1.3.1: Reserve and Configure TrGW Connection Point

Procedure	Initiated	Information element name	Information element required	Information element description
Reserve and Configure TrGW Connection Point	IBCF	Context/Context Request	M	This information element indicates the existing context or requests a new context for the bearer termination.
		Termination/Termination Request	M	This information element indicates the existing bearer termination or requests a new termination for the bearer to be established.
		IP Interface	O	This information element specifies the used interface type for the IP termination (e.g. MboIP).
		Local IP Resources	C	This information element indicates the resource(s) (e.g. codec, auxiliary payload types) for which the TrGW shall be prepared to receive user data. May be excluded (i.e. "-" is used in SDP m-line) if no transcoding or other media related functions are required.
		Remote IP Resources	C	This information element indicates the resources (e.g. codec, auxiliary payload types) that the TrGW shall use to send user data. May be excluded (i.e. "-" is used in SDP m-line) if no transcoding or other media related functions are required.
		Reserve Value	C	This information element indicates if multiple IP resources are to be reserved. This information element shall be included if a speech codec and auxiliary payload types are configured.
		Local Connection Address request	M	This information element requests an IP address and a port number on the TrGW that the remote end can send user plane data to.
		Remote Connection Address	M	This information element indicates the IP address and ports of the remote party that the TrGW can send user plane data to.
		Remote Source Address Filtering	O	This information element indicates that remote source address filtering is required.
		Remote Source Address Mask	C	This information element provides information on the valid remote source addresses. This may be included if remote source address filtering is included. It shall not be included if remote source address filtering is not included.
		Remote Source Port Filtering	O	This information element indicates that remote source port filtering is required.
		Remote Source Port	C	This information element identifies the valid remote source port. This may be included if remote source port filtering is included. It shall not be included if remote source port filtering is not included. (NOTE 1)
		Remote Source Port Range	C	This information element identifies a range of valid remote source ports. This may be included if remote source port filtering is included. It shall not be included if remote source port filtering is not included. (NOTE 1)
		RTCP handling	O	Indicates whether or not the TrGW shall reserve a port for an RTCP flow.
		Notify termination heartbeat	M	This information element requests termination heartbeat indications.
Notify Released Bearer	O	This information element requests a notification of a released bearer.		

		IP Realm Identifier	O	This information element indicates the IP realm of the IP termination.
		Traffic Policing Required	O	This information element indicates that policing of the media flow is required.
		Peak Data Rate	O	This information element may be present if Policing is required and specifies the permissible peak data rate for a media stream. (NOTE 2)
		Sustainable Data Rate	O	This information element may be present if Policing is required and specifies the permissible sustainable data rate for a media stream. (NOTE 2)
		Delay Variation Tolerance	O	This information element may be present if Policing on Peak Data Rate is required and specifies the maximum expected delay variation tolerance for the corresponding media stream.
		Maximum Burst Size	C	This information element shall be present if Policing on Sustainable Data Rate is required and specifies the maximum expected burst size for the corresponding media stream.
		DiffServ Code Point	O	This information element indicates a specific DiffServ code point to be used in the IP header in packets sent on the IP termination.
		DiffServ Tagging Behaviour	O	This information element indicates whether the Diffserv code point in the IP header in packets sent on the IP termination should be copied from the received value or set to a specific value.
		Media Inactivity Detection Required	O	This information element indicates that detection of inactive media flows is required.
		Inactivity Detection Time	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection time.
		Inactivity Detection Direction	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection direction.
Reserve and Configure TrGW Connection Point Ack	TrGW	Context	M	This information element indicates the context where the command was executed.
		Termination	M	This information element indicates the termination where the command was executed.
		Local IP Resources	C	This information element indicates the resources that the TrGW has reserved to receive the user plane data from the remote side.
		Remote IP Resources	O	This information element indicates the resource (i.e. codec) that the TrGW shall use to send user data.
		Local Connection Addresses	M	This information element indicates the IP address and port on the TrGW that shall receive user plane data.
		Remote Connection Address	O	This information element indicates the IP address and port that the TrGW can send user plane data to.
NOTE 1: Remote Source Port and Remote Source Port Range are mutually exclusive.				
NOTE 2: At least one of these IEs shall be present when policing is required.				

Editor's Note: For the Reserve and Configure TrGW Connection Point Ack , It is ffs if Local IP Resources is mandatory or optional to be included if present in the request.

## 10.4.1.4 Release TrGW Termination

This procedure is used to release multimedia-processing resources for a termination at the TrGW.

Table 10.4.1.4.1: Release TrGW Termination

Procedure	Initiated	Information element name	Information element required	Information element description
Release TrGW Termination	IBCF	Context	M	This information element indicates the existing context.
		Termination	M	This information element indicates the existing bearer termination to be released.
Release TrGW Termination Ack	TrGW	Context	M	This information element indicates the context where the command was executed.
		Termination	M	This information element indicates the termination where the command was executed.

Editor's note: Any requirement for statistics in the Release TrGW Termination Ack is ffs and needs to be justified by a use case.

## 10.4.1.5 IP Bearer Released

Table 10.4.1.5.1: IP Bearer Released

Procedure	Initiated	Information element name	Information element required	Information element description
IP Bearer Released	TrGW	Context	M	This information element indicates the context for the bearer termination.
		Termination	M	This information element indicates the bearer termination where the bearer was released.
		Bearer Released	M	This information element notifies a bearer release.
		Release Cause	M	This information element indicates the cause of a bearer release.
IP Bearer Released Ack	IBCF	Context	M	This information element indicates all context are where the command was executed.
		Termination	M	This information element indicates that Bearer termination is where the command was executed.



### 10.4.1.6 Media Inactivity Detection

This command is used to notify the IBCF of media inactivity on the TrGW.

**Table 10.4.1.6.1: Media Inactivity Notification**

Procedure	Initiated	Information element name	Information element required	Information element description
Media Inactivity Notification	TrGW	Context	M	This information element indicates the existing context for the bearer termination.
		Termination	M	This information element indicates that bearer termination is where the media inactivity detection was activated.
		Media Inactivity	M	This information element notifies the IBCF of Media inactivity detection on the bearer termination.
Media Inactivity Notification Ack	IBCF	Context	M	This information element indicates the context where the command was executed.
		Termination	M	This information element indicates the bearer termination where the command was executed.

### 10.4.1.7 Termination heartbeat indication

This command is used by the TrGW to periodically notify the IBCF of a termination heartbeat.

**Table 10.4.1.7.1: Termination heartbeat indication**

Procedure	Initiated	Information element name	Information element required	Information element description
Termination heartbeat indication	TrGW	Context	M	This information element indicates the context for the bearer termination.
		Bearer Termination	M	This information element indicates the bearer termination for which the termination heartbeat is reported.
		Termination heartbeat	M	Hanging Termination event
Termination heartbeat indication Ack	IBCF	Context	M	This information element indicates the context where the command was executed.
		Bearer Termination	M	This information element indicates the bearer termination where the command was executed.

## 10.4.2 Non Call related Procedures

The procedures in Table 10.4.2.1 shall be applied between the IBCF and TrGW.

Table 10.4.2.1: Non-call related procedures

Stage 3 Procedure (for information) defined in 3GPP TS 29.238 [25]	Corresponding Stage 2 Procedure defined in 3GPP TS 23.205 [28]	Remarks
TrGW Out of service	MGW Out of Service	
TrGW Communication Up	MGW Communication Up	
TrGW Restoration	MGW Restoration	
TrGW Register	MGW Register	
TrGW Re-register	MGW Re-register	
CS-IBCF Ordered Re-register	(G)MSC Server Ordered Re-register	
CS-IBCF Restoration	(G)MSC Server Restoration	
CS-IBCF Out of Service	(G)MSC Server Out of Service	
Termination Out-of-Service	Termination Out-of-Service	The 'Termination Out-of-Service procedure' is also used as a call-related H.248 command
Audit Value	Audit Value	
Command Rejected	Command Rejected	The 'Command Rejected' procedure may be used in response both to call-related and non-call-related H.248 Commands.
TrGW Capability Change	Capability Update	
TrGW Resource Congestion Handling – Activate	MGW Resource Congestion Handling – Activate	
TrGW Resource Congestion Handling – Indication	MGW Resource Congestion Handling – Indication	
Inactivity timeout activation	Inactivity timeout activation	
Inactivity timeout indication	Inactivity timeout indication	
Realm Availability Change Activation		See 3GPP TS 29.235 [29] subclause A.7.2
Realm Availability Change Indication		See 3GPP TS 29.235 [29] subclause A.7.2

---

## Annex A (informative): Codecs used for conversational services

Codecs used for Conversational Services For codecs for conversational services in the PS domain are defined according to 3GPP TS 26.235 [6]. These include:

- Narrowband speech: The support of the AMR codec is mandated.
- For wideband speech: The support of the AMR-WB codec is mandated
- For video: The support of the H.263 profile 0 level 10 v1 is mandated, and the support of MPEG4 visual sp @ level 0 and ITU-T Recommendation H.263 [14] profile 3 level 10 are optional.

In non-3GPP SIP networks there are no mandatory codecs. However, the following codecs are of interest:

- Narrowband speech: ITU-T Recommendations G.723.1 [15], G.729 [16] and G.711 [17] are known to be commonly deployed.
- Video codecs: ITU-T Recommendation H.263 [14] and MPEG4 are expected to be used.

## Annex B (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2001-02					Version 0.0.0 Presented to CN3 #16 - Sophia Antipolis - Initial Proposal - TS 29.162 number allocated by MCC		0.0.0
2001-05					Tdocs N3-010226 and N3-010200 agreed at CN3#17 - Rio Grande, Puerto Rico		0.1.0
2001-10					Tdoc N3-010331 agreed at CN3#18 - Dresden, Germany	0.1.0	0.2.0
2001-10					Revised TS based on decision within CN3#19 to reduce the scope of Work Item - as proposed in Tdoc N3-010425. Clean version based on changes agreed in N3-010479 at Cn3#19 - Brighton, UK.	0.2.0	0.3.0
2001-11					Added informative Annex A about interworking between IPv4 and IPv6, as agreed in Cn3#20 Cancun.	0.3.0	0.4.0
2002-01					Included N3-020094, N3-020104, and tidied editors notes.	0.4.0	0.5.0
2002-02					Editorial changes agreed in CN3#21, Sophia Antipolis.	0.5.0	0.6.0
2002-02					DAB, MCC some minor editorials	0.6.0	0.6.1
2002-03					Presented as v1.0.0 to TSG#15 for information	0.6.1	1.0.0
2004-08					Changes e.g. on IPv4-IPv6 interworking agreed in CN3#33, Sophia	1.0.0	1.1.0
2004-09					Editorial corrections made to ensure alignment with 3GPP drafting rules	1.1.0	1.1.1
2004-10					Changes e.g. on IPv4-IPv6 interworking agreed in CN3#33bis, Sophia	1.1.1	1.2.0
2004-11					Included changes agreed at CN3#34	1.2.0	1.3.0
2004-11					Editorial update	1.3.0	2.0.0
2004-12	CN#26				Approved at Release 6	2.0.0	6.0.0
2005-06	CP#28	CP-050037	002	2	ALG transparency	6.0.0	6.1.0
2005-09	CP#29	CP-050377	003		Correction to obsolete reference	6.1.0	6.2.0
2005-12	CP#30				Created by MCC for reference by TISPAN	6.2.0	7.0.0
2006-03	CP#31	CP-060051	005	2	IBCF	7.0.0	7.1.0
2008-05	CP#40	CP-080297	006	1	Additions of subclause for TISPAN TIP/TIR and Common Basic Communication supplementary service interworking	7.1.0	8.0.0
2008-12	CP#42	CP-080753	008	2	Clarification of NAT/NAPT in 29.162	8.0.0	8.1.0
2008-12	CP#42	CP-080767	011	1	[IBCF] 29.162 Ix - Clarification of protocol reference for Ix	8.0.0	8.1.0
2008-12	CP#42	CP-080767	012	6	[IBCF] 29.162 Ix Voice/audio transcoding	8.0.0	8.1.0
2009-03	CP#43	CP-090079	021		Correction to 9.2.2.3	8.1.0	8.2.0
2009-03	CP#43	CP-090093	023	1	Removal of Ix Interface from Release 8	8.1.0	8.2.0
2009-03	CP#43	CP-090098	022	4	Ix procedures	8.2.0	9.0.0
2009-05	CP#44	CP-090352	024	1	Specification re-structuring	9.0.0	9.1.0
2009-05	CP#44	CP-090471	025	3	Use Case for Media Handling	9.0.0	9.1.0
2009-05	CP#44	CP-090352	026	1	Corrections to IM-IBCF / CS-TrGW non-call related procedures	9.0.0	9.1.0
2009-05	CP#44	CP-090352	027		Ix protocol specified in Rel-9	9.0.0	9.1.0
2009-05	CP#44	CP-090352	028	3	IP Address and Port Conversion	9.0.0	9.1.0
2009-05	CP#44	CP-090352	029	1	Source IP Address and Port Filtering	9.0.0	9.1.0
2009-09	CP#45	CP-090582	032	1	Addition of Release TrGW Termination to IMS-IBCF procedures	9.1.0	9.2.0
2009-09	CP#45	CP-090582	033	2	Handling of RTCP Streams	9.1.0	9.2.0
2009-09	CP#45	CP-090582	034	3	Use of Media Information at TrGW not supporting transcoding	9.1.0	9.2.0
2009-09	CP#45	CP-090582	036	1	Notification of released bearer	9.1.0	9.2.0
2009-09	CP#45	CP-090582	037		Remote IP resources in responses optional	9.1.0	9.2.0
2009-12	CP#46	CP-090851	039	4	Media Inactivity Detection	9.2.0	9.3.0
2009-12	CP#46	CP-090851	041	6	Handling of RTCP	9.2.0	9.3.0
2009-12	CP#46	CP-090851	042	2	QoS Packet Marking	9.2.0	9.3.0
2009-12	CP#46	CP-090851	043	2	Termination Heartbeat Procedure	9.2.0	9.3.0
2009-12	CP#46	CP-090851	045	2	Mandatory features in TrGW	9.2.0	9.3.0
2009-12	CP#46	CP-090851	046	2	Specification clean-up	9.2.0	9.3.0
2009-12	CP#46	CP-090851	047	1	Abbreviations Tidy-Up	9.2.0	9.3.0
2009-12	CP#46	CP-090851	048		Non-Call Related Procedure Alignment	9.2.0	9.3.0
2009-12	CP#46	CP-090851	049	1	Use of IP Interface Type	9.2.0	9.3.0
2009-12	CP#46	CP-090851	050	3	Traffic Policing	9.2.0	9.3.0
2010-03	CP#47	CP-100089	052	4	Support of end-to-end IMS media plane security	9.3.0	9.4.0

---

# History

<b>Document history</b>		
V9.3.0	January 2010	Publication
V9.4.0	April 2010	Publication