ETSI TS 129 162 V15.0.0 (2018-11)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Interworking between the IM CN subsystem and IP networks (3GPP TS 29.162 version 15.0.0 Release 15)

Reference

RTS/TSGC-0329162vf00

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or
print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any
existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the
print of the Portable Document Format (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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

ETSI

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd 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 (IETF RFC 791 [9]) and IP version 6 (IETF RFC 2460 [10]) detailed in terms of the processes and protocol mappings required in order to support both IMS 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]   Void.

[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]   Void.

[15]   Void.

[16]   Void.

[17]   Void.

[18]   IETF RFC 792: "Internet Control Message Protocol".

[19]   IETF RFC 2463: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6".

[20]   Void.

[21]   Void.

[22]   Void.

[23]   Void.

[24]   Void.

[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]   Void.

[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: "Session Description Protocol (SDP) Security Descriptions for Media Streams".

[34]   IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)".

[35]   IETF RFC 5124: "Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)".

[36]   3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[37]   IETF RFC 3168: "The Addition of Explicit Congestion Notification (ECN) to IP".

[38]   IETF RFC 6679: "Explicit Congestion Notification (ECN) for RTP over UDP".

[39]   3GPP TS 29.079: "Optimal Media Routeing within the IP Multimedia Subsystem; Stage 3".

[40]   3GPP TS 29.165: "Inter-IMS Network to Network Interface (NNI)".

[41]   3GPP TS 23.237: "IP Multimedia subsystem (IMS) Service Continuity; Stage 2".

[42]   3GPP TS 24.237: "IP Multimedia subsystem (IMS) Service Continuity; Stage 3".

[43]   3GPP TS 23.334: "IP Multimedia Subsystem (IMS) Application Level Gateway (IMS-ALG) – IMS Access Gateway (IMS-AGW) interface: Procedures descriptions".

[44]   3GPP TS 22.153: "Multimedia Priority Service".

[45]   IETF RFC 5285: "A General Mechanism for RTP Header Extensions".

[46]   IETF RFC 6236: "Negotiation of Generic Image Attributes in the Session Description Protocol (SDP)".

[47]   IETF RFC 4975: "The Message Session Relay Protocol (MSRP)".

[48]   IETF RFC 6714: "Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)".

[49]   IETF RFC 4583: "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams".

[50]   IETF RFC 5245: "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

[51]   IETF RFC 6947: "The Session Description Protocol (SDP) Alternate Connectivity (ALTC) Attribute".

[52]   3GPP TS 26.441: "Codec for Enhanced Voice Services (EVS); General Overview".

[53]   3GPP TS 26.445: "Codec for Enhanced Voice Services (EVS); Detailed Algorithmic Description".

[54]   IETF RFC 4573: "MIME Type Registration for RTP Payload Format for H.224".

[55]   ITU-T Recommendation H.224 (01/2005): "A real time control protocol for simplex applications using the H.221 LSD/HSD/MLP channels".

[56]   ITU-T Recommendation H.281 (11/1994): "A far end camera control protocol for videoconferences using H.224".

[57]   IETF RFC 5939: "Session Description Protocol (SDP) Capability Negotiation".

[58]   IETF RFC 5009: "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".

[59]   IETF RFC 7728: "RTP Stream Pause and Resume".

[60]   IETF RFC 4585: "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)".

[61]   IETF RFC 5104: "Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)".

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:

End-to-end security: media protection between two IMS UEs without being terminated by any intermediary node.

ICE lite: The lite implementation of the Interactive Connectivity Establishment (ICE) specified in IETF RFC 5245 [50].

Full ICE: The full implementation of the Interactive Connectivity Establishment (ICE) specified in IETF RFC 5245 [50].

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.

MSC Server enhanced for ICS: An MSC Server that supports the network based ICS functionality.

MSC Server enhanced for SRVCC: An MSC Server that supports the network based SRVCC functionality.

3.2 Symbols

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

Mm	Reference Point between a CSCF/BGCF/IMS-ALG and an IP multimedia network.
Mx	Reference Point between a CSCF/BGCF/MSC Server enhanced for ICS/MSC Server enhanced for SRVCC and IBCF.
Mb	Reference Point defined in 3GPP TS 23.002 [5] and is IP based.
Ix	Reference Point between IBCF and TrGW or CS-IBCF and CS-TrGW.

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].

ALTC	ALTernative Connection
APP	APPlication-defined RTCP packet
ATCF	Access Transfer Control Function
ATGW	Access Transfer Gateway
B2BUA	Back-to-Back User Agent
BFCP	Binary Floor Control Protocol
CCM	Codec Control Messages
BGCF	Breakout Gateway Control Function
CS-TrGW	CS (domain) TrGW
CVO	Coordination of Video Orientation
DRVCC	Dual Radio Voice Call Continuity
ECN	Explicit Congestion Notification
ECN-CE	ECN Congestion Experienced
EVS	Enhanced Voice Services
FECC	Far End Camera Control
FIR	Full Intra Request
IBCF	Interconnect Border Control Function
ICE	Interactive Connectivity Establishment
ICS	IMS Centralized Services
I-CSCF	Interrogating CSCF
IMS-ALG	IMS - Application Level Gateway
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
MboIP	Mb over IP
MPS	Multimedia Priority Service
MRFP	Multimedia Resource Function Processor
MSRP	Message Session Relay Protocol
NAT/NAPT	Network Address Translation / Network Address and Port Translation
NA (P) T-PT	Network Address (and Port) Translation - Protocol Translation
OMR	Optimal Media Routeing
P-CSCF	Proxy CSCF
ROI	Region of Interest
RTCP	Real Time Control Protocol
SCTP	Stream Control Transmission Protocol
SDPCapNeg	SDP Capability Negotiation
SIP UA	SIP User Agent
STUN	Session Traversal Utilities for NAT
UAC	User Agent Client
UAS	User Agent Server
URN	Uniform Resource Name
THIG	Topology Hiding Internetwork Gateway
TLS	Transport Layer Security
TMMBN	Temporary Maximum Media Stream Bit Rate Notification
TMMBR	Temporary Maximum Media Stream Bit Rate Request
TRF	Transit and Roaming Function
TrGW	Translation GateWay
WAN	Wide Area Network

4 General

4.1 General interworking overview

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

- SIP User Agents (SIP UAs); and

- 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 (IETF RFC 791 [9]) or IP version 6 (IETF RFC 2460 [10]).
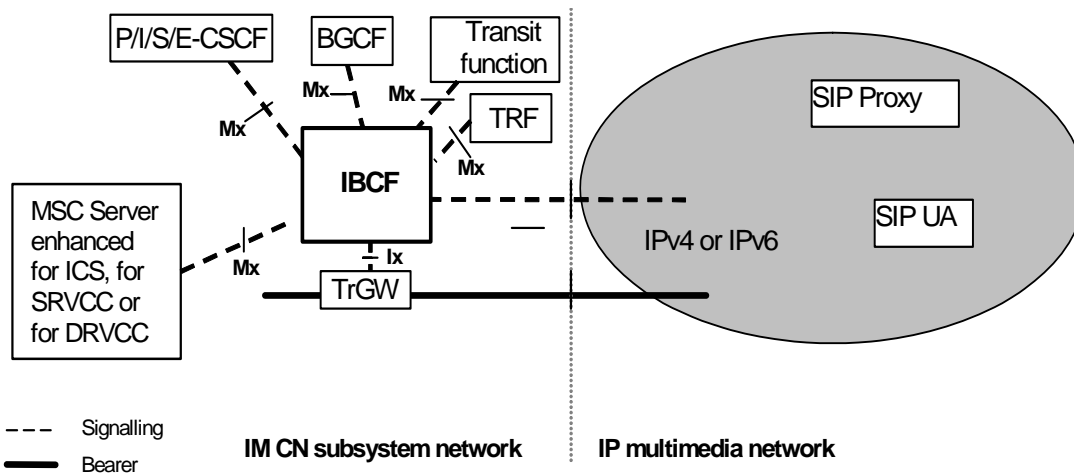
Figure 1: Interworking Model for IM CN Subsystem to IP Multimedia Network

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

The CS UE uses a MSC Server to communicate with external IP multimedia network entities.

If no IP version interworking or no NAT/NAPT between different realms is required, the CSCF and the MSC Server 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 and the MSC Server 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 or the MSC Server and the 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 outside the scope of this release.

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 subclause 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 3GPP 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) (IETF 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

6.0 Reference Model

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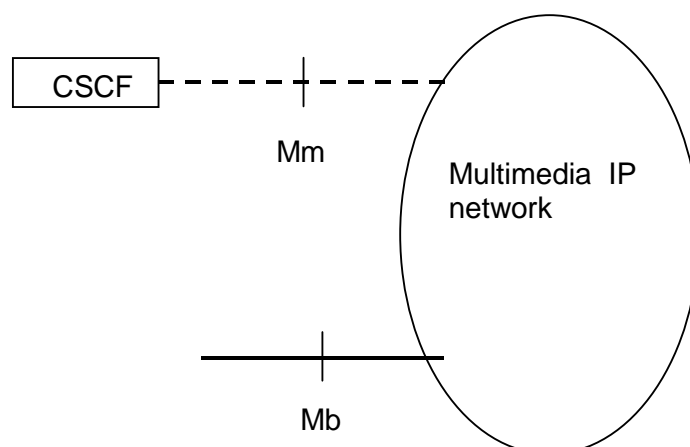
NOTE: Multimedia IP networks may be connected via the Mb interface to various network entities, such as an UE (via an GTP Tunnel reaching to the GGSN), an MRFP, or an application server.

Figure 2: IM CN Subsystem to IP network interworking reference Architecture without IP version interworking
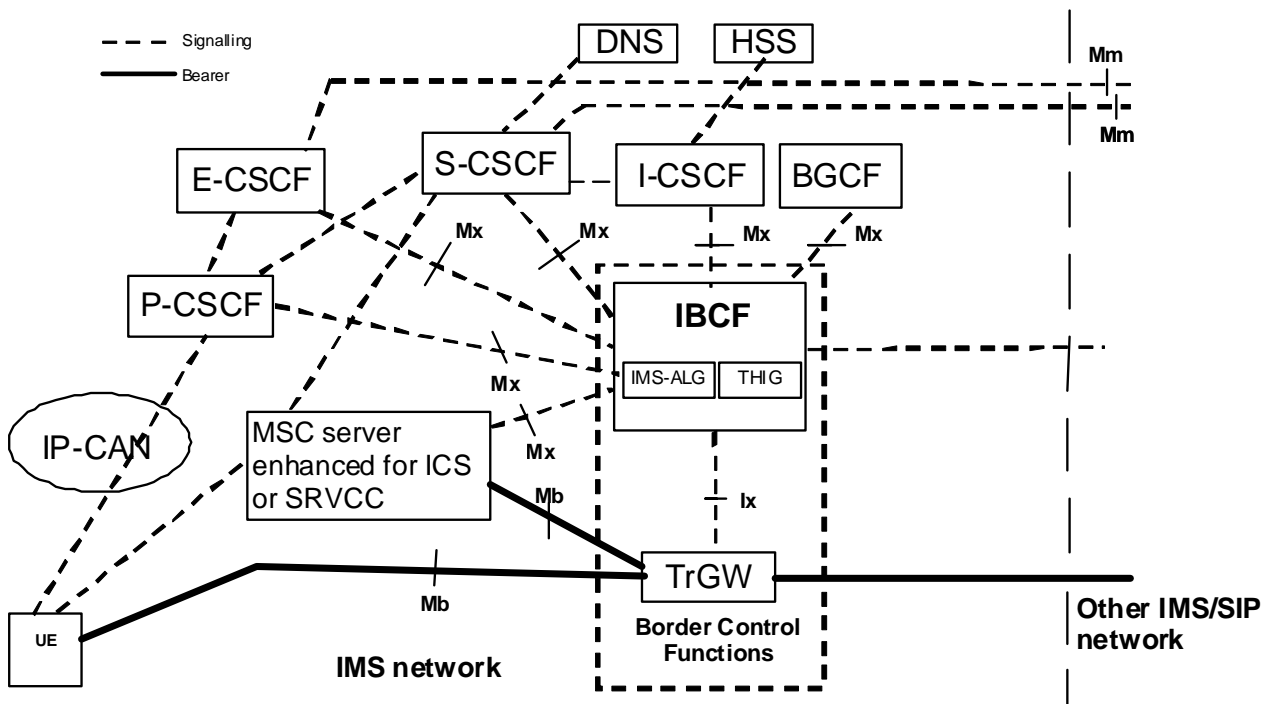
Figure 3: Border Control Functions

Mm reference point: The call control protocol applied to the Mm interface between CSCF and external IP networks is SIP, IETF 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 26.114 [36].

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 IBCF

This entity provides control plane functionality to connect entities following the 3GPP profile of SIP, 3GPP TS 24.229 [1], and external SIP entities following IETF 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 SIP B2BUA when IBCF 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 IETF RFC 2766 [11] and IETF RFC 2663 [12].

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

6.1.4   Acces Transfer Control Function

The ATCF may reside within the IBCF to support "SRVCC enhanced with ATCF" procedures as described in 3GPP TS 23.237 [41] and 3GPP TS 24.237 [42] . In this case, the Ix reference point is used for IMS sessions that the ATCF decides to anchor at the ATGW to provide the following functions:

- reservation and configuration of ATGW resources for media anchoring during PS session origination or termination;

- reconfiguration of ATGW resources during access transfer to the CS domain;

- release of ATGW resources upon completion of the access transfer or release of the session;

- media transcoding if the media that was used prior to the access transfer is not supported by the MSC server;

- IP version interworking if different IP versions are used between the access and the remote legs; and

- indication of IP realm during allocation of transport addresses/resources (the PS and CS accesses may be reachable via different IP realms).

6.1.5   Acces Transfer GateWay

The ATGW may reside within the TrGW to support "SRVCC enhanced with ATCF" procedures as described in 3GPP TS 23.237 [41] and 3GPP TS 24.237 [42]. If the IBCF supports the ATCF functionality (see subclause 6.1.4), the IBCF shall select a TRGW which supports the ATGW functionality.

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 protocols associated with services

There is no impact beyond that specified in subclause 7.1 provided the necessary SIP extensions are supported on both sides of the interworking point.

Based on operator policy and/or service level agreements the interworking of services may be restricted.

Additional information related to interworking with services is provided in 3GPP TS 29.165 [40].

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 26.114 [36].

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 subclause 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, the TrGW 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 subclauses 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; and

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 subclause 9.1.1, subclause 9.1.3, subclause 9.1.5 and clause 10.

NOTE: SDP not described in subclause 9.1.1, subclause 9.1.3 or clause 10 can be handled according to 3GPP TS 24.229 [1] clause A.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.

-    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.

-    The IBCF can perform screening of SIP request and SIP responses based on local policy as described in subclause 5.10.6 of 3GPP TS 24.229 [1].

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

9.1.5   Modification of SDP bandwidth information for IP version interworking

When the IMS ALG performs IP version interworking and passes an SDP offer or answer, it should adjust any SDP b=AS bandwidth modifiers contained in the SDP.

NOTE 1: 3GPP TS 26.114 [36] annex K and annex Q contain information about bandwidths for speech media transported over IPv4 and IPv6. 3GPP TS 26.114 [36] subclause 12.7.5 contains information how to convert b=AS for video media.

NOTE 2: If the b=AS bandwidth modifiers are not adjusted, this can negatively impact the end-to-end media negotiation (e.g. the selection of a speech codec mode) and lead to an inaccurate resource reservation.

The IMS-ALG may support the enhanced bandwidth negotiation mechanism defined in 3GPP TS 26.114 [36]. The enhanced bandwidth negotiation mechanism is based on the "a=bw-info" SDP attribute (defined in clause 19 of 3GPP TS 26.114 [36]) to negotiate the additional bandwidth properties end-to-end.

If the IMS-ALG receives an SDP body containing the "a=bw-info" SDP attribute(s) and if:

- the IMS-AGW interconnects call legs in IP domains where different IP versions (IPv4 or IPv6) are used; and

- the received "a=bw-info" SDP attribute lines related to the same payload type and the same direction do not contain bandwidth properties for both IPv4 and IPv6;

the IMS-ALG shall, before forwarding the SDP body:

- re-calculate the received bandwidth properties (the maximum supported bandwidth, the maximum desired bandwidth, the minimum desired bandwidth and the minimum supported bandwidth for sending and/or receiving direction);

- include in the modified "a=bw-info" SDP attribute lines the IP version used for the re-calculation of the bandwidth properties;

NOTE 3: If no IP version is included for any of the "a=bw-info" SDP attribute lines related to a certain payload type and direction then IPv6 is assumed for all bandwidth properties related to the same direction and payload type, on all of the related "a=bw-info" SDP attribute lines, see clause 19 of 3GPP TS 26.114 [36].

- include the maximum packet rate assumed when re-calculating the maximum supported bandwidth, the maximum desired bandwidth and the minimum desired bandwidth properties; and

- include the minimum packet rate assumed when re-calculating the minimum supported bandwidth.

Otherwise, if the received SDP body contains bandwidth properties for both IPv4 and IPv6 and if the IMS-ALG does not support or does not apply the transcoding procedure defined in subclause 10.2.5, the IMS-ALG shall forward the SDP body with unmodified "a=bw-info" SDP attribute lines.

9.2 User plane transport

9.2.1 Payload transport

The TrGW shall use the established bindings described in subclause 9.1 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; and

- replace the received source IPaddress(es) and port number(s) in the payload message with the corresponding IPaddress(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
HopLimit:	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.
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 value of this field should be mapped from the triple of the source address, destination address and IPv4 identification field of the incoming packet/fragments to a unique value for the source and destination address of the outgoing IPv6 packet/fragments.

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 [18].

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 the translator 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.
Total length	The IPv4 Total Length field value is the IPv6 Payload length value plus 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 value of this field should be mapped from the triple of the source address, destination address and IPv6 fragmentation header field "identification" of the incoming packet/fragments to a unique value for the source and destination address of the outgoing IPv4 packet/fragments.
Flags	The IPv4 More Fragments flag is copied from the IPv6 M flag in the IPv6 Fragment header the IPv4. The 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 [19], 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; and

- 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 [18] and "hop limit exceeded in transit" type 3 code 0 as defined in IETF RFC 2463 [19].

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 subclause within subclause 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.
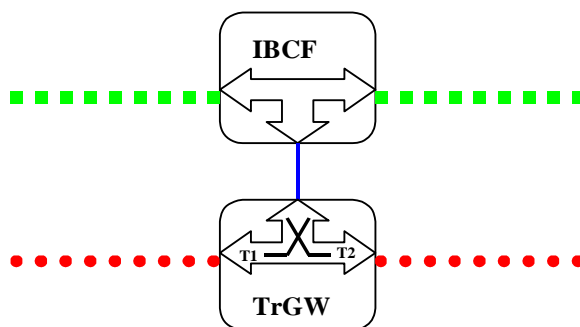
Figure 10.1.2.1: Network model

10.1.3 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.

```
        ┌──────────────┐                    ┌──────────────┐
        │     TrGW     │                    │     IBCF     │
        └──────────────┘                    └──────────────┘
                                                   │
                                            1  SDP offer (IP2o, P2o)
                                            ◄ ─ ─ ─ ─ ─ ─ ─ ─ ─
                                       ┌───────────────────┐
                                       │ 2. Use case X detected │
                                       │    that needs TrGW     │
                                       │    functionality       │
                                       └───────────────────┘
```

3. H.248 ADD req
C= ?, T= ?, LAddr=?, LPort=?)

Reserve TrGW Connection Point (, Change Through-Connection)

4. Create outgoing termination T1

5. H.248 ADD resp.
(C=C1, T=T1, LAddr=IP1o, LPort=P1o)

6. Modify SDP offer

7. SDP offer (IP1o, P1o)

8. SDP answer (IP1a, P1a)

9. H.248 MOD req
(C= C1, T= T1, RAddr=IP1a, RPort=P1a)

Configure TrGW Connection Point (, Change Through-Connection)

10. Configure Outgoing Termination T1

11. H.248 MOD Resp
C= C1, T= T1)

12. H.248 ADD req
C= C1, T= ?, LAddr=?, LPort=?, RAddr=IP2o, RPort=P20)

Reserve And Configure TrGW Connection Point (, Change Through-Connection)

13. Create incoming Termination T2

14. H.248 ADD Resp
C= C1, T= T2,
 LAddr=IP2a, LPort=P2a,
 RAddr=IP1a, RPort=P1a)

15. Modify SDP answer

16. SDP answer(Ip2a, P2a)

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 1: 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 or towards external networks, the IBCF may also indicate that the IP Interface Type is "MboIP".

NOTE : Other values may be indicated by a CS-IBCF, as detailed in 3GPP TS 29.235 [29].

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.
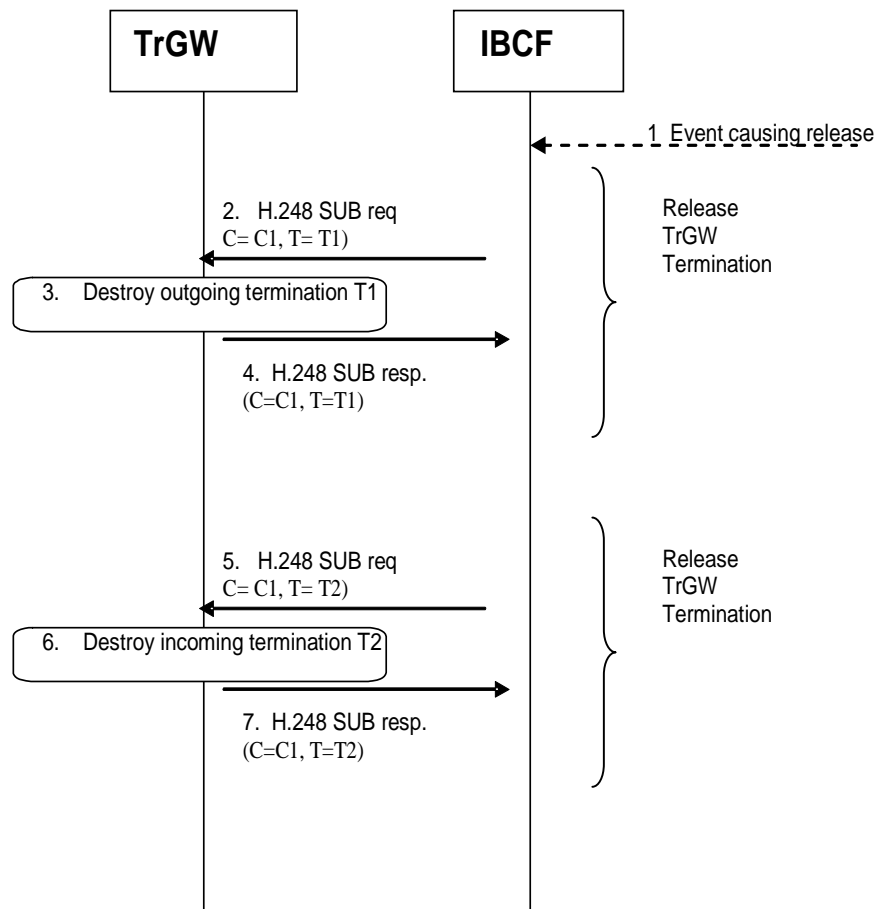
1.   The IBCF identifies that the call is to be release. Typically this will be by the receipt of a SIP BYE request.
2.   The IBCF sends a H.248 SUB command to release the outgoing termination.
3.   The TrGW destroys the outgoing termination.
4.   The TrGW replies to IBCF with a H.248 SUB reply command.
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 Main Functions supported at the Ix Interface

10.2.0 Introduction

The following functions shall be supported by the TrGW:

-   Gate Management including:

    -   Opening/closing of gates;

    -   Remote source address filtering; and

    -   Remote source port filtering;

- QoS packet marking (differentiated services);

- NAPT and IP Version Interworking;

- Bandwidth policing;

- Hanging termination detection;

- IP Realm Indication;

- Media Control; and

- Through-Connection.

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

- Resource allocation per flow;

- Media Inactivity Detection;

- IP Realm Availability;

- Optimal Media Routeing;

- Explicit Congestion Notification support;

- Emergency Call;

- IMS end-to-end media plane security;

- Access Transfer procedures with media anchored in ATGW;

- Multimedia Priority Service;

- RTP Header extension to signal Coordination of Video Orientation;

    - Generic image attribute;

- Interactive Connectivity Establishment;

- Video Region of Interest (ROI) ;

- RTP-level pause and resume functionality ; and

- "RTCP Codec Control Commands and Indications"

10.2.1   NAPT and IP version interworking

NAPT and IP version interworking is documented in clause 9.

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 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   RTCP Handling

The procedures in subclause A.7.1.2.2.7 of 3GPP TS 29.235 [29] are applicable.

10.2.4   IP Realm 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

10.2.5.1   General

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 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, 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 request 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 offer using the information coming from TrGW
7. The IBCF forwards the new SDP 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 by the succeeding network/terminating UE and the IBCF determines that transcoding is not required.
9. The IBCF sends a H.248 MOD request 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 request 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. The 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 request 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 offer using the information coming from TrGW.
7. The IBCF forwards the new SDP offer to the succeeding node.
8. The SDP answer is received by IBCF. In this example the codec 3 added by the IBCF to the SDP offer has been selected. Transcoding is therefore required.
9. The IBCF sends a H.248 MOD request command to configure the outgoing termination with address and port information received in the SDP answer and the selected media attibutes (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 request 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. The 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.
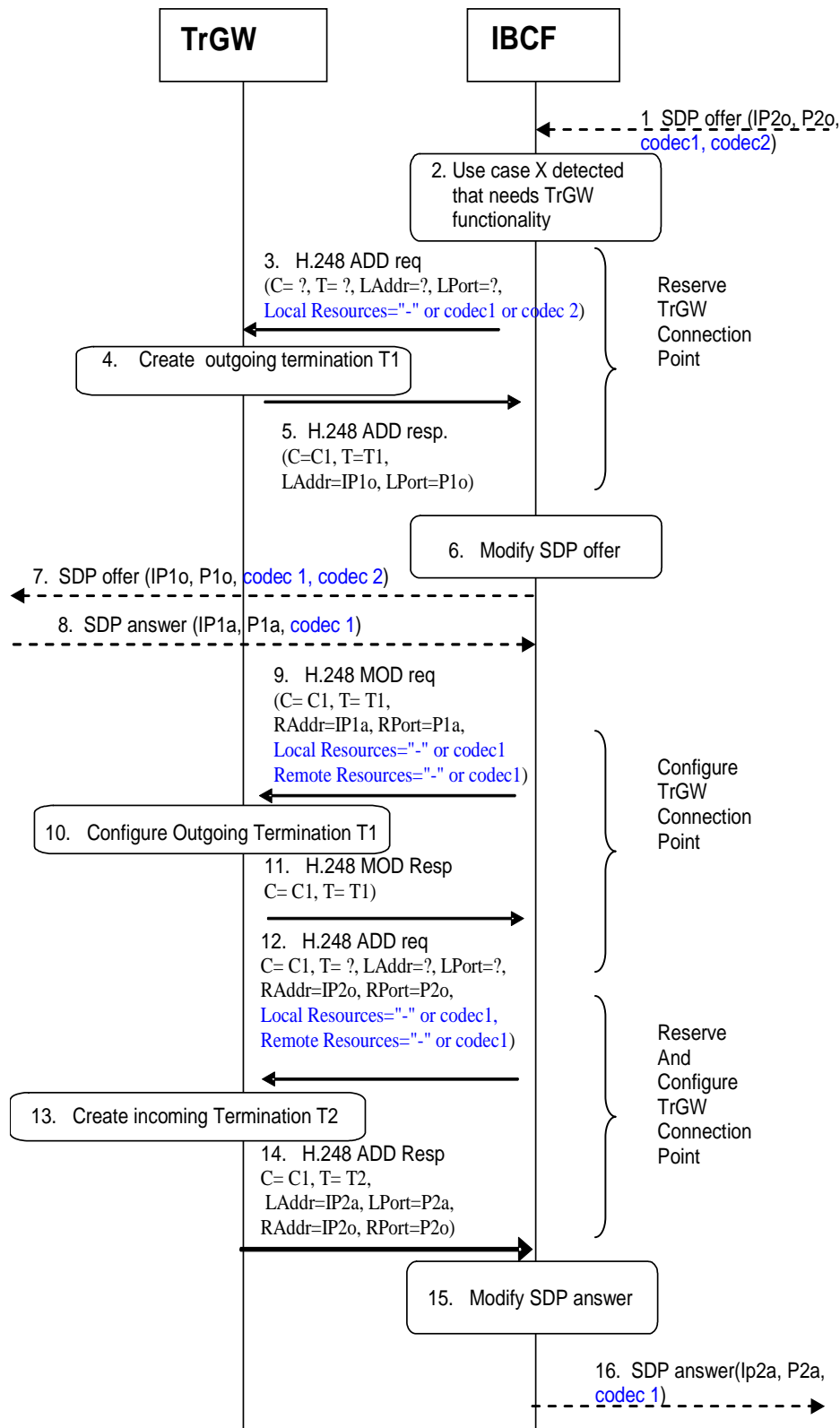
1. The IBCF receives an SDP offer in SIP signalling.
2. The IBCF requires a TrGW for another use case but does not offer transcoding.
3. The IBCF sends a H.248 ADD request command to create the outgoing termination and to request IP resources to execute TrGW function. As no media transcoding is required this may be indicated by signalling "-". Alternatively 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 codec 1 received in the original SDP offer in step 1 has been selected.

9.   The IBCF sends a H.248 MOD request 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.   The 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

10.2.5.2   Handling of common codec parameters

The requirements as described in subclause 5.13.2 of 3GPP TS 23.334 [43] for the IMS-ALG and the IMS-AGW, apply to the IBCF and the TrGW.

10.2.5.3   EVS speech codec parameters handling

The Enhanced Voice Services (EVS) speech codec is defined in 3GPP TS 26.441 [52]. Its RTP payload type is defined in 3GPP TS 26.445 [53], and procedures for its usage as IMS Multimedia Telephony speech codec are defined in 3GPP TS 26.114 [36].

The IBCF and the TrGW may support transcoding to and from the EVS speech codec. If they do so, the requirements as described in subclause 5.13.3 of 3GPP TS 23.334 [43] for the IMS-ALG and the IMS-AGW, apply to the IBCF and the TrGW.

10.2.5.4   Rate adaptation for media endpoints

If the IBCF and the TrGW support rate adaptation for media endpoints using the enhanced bandwidth negotiation mechanism defined in 3GPP TS 26.114 [36] the requirements and procedures in the present subclause apply.

If the IBCF receives an SDP offer and if the IBCF and the TrGW apply the transcoding procedure, defined in subclause 10.2.5.1, then the following additional actions may be performed:

- if the received SDP offer (figure 10.2.5.2, step 1) contained the SDP "a=bw-info" attribute(s), defined in clause 19 of 3GPP TS 26.114 [36] for payload type(s) that the IBCF retains in the forwarded SDP offer, the IBCF:

    a) if the IP version interworking is required and the received "a=bw-info" SDP attribute lines do not contain bandwidth properties for both IPv4 and IPv6, should adjust the bandwidth properties in accordance with subclause 9.1.5; or

    b) otherwise (if the IP version interworking is not required or the received "a=bw-info" SDP attribute lines contain bandwidth properties for both IPv4 and IPv6), should forward the SDP offer with unmodified related SDP "a=bw-info" attribute(s); and

  NOTE 1: The IBCF can modify the related SDP "a=bw-info" attribute(s) according to operator policies as specified in 3GPP TS 26.114 [36].

- for the each added codec in the SDP offer (figure 10.2.5.2, step 6) the IBCF shall include appropriate bandwidth information in new or existing "a=bw-info" attribute lines(s).

If the IBCF then receives an SDP answer (figure 10.2.5.2, step 8) and if only the codecs inserted by the IBCF with the corresponding SDP "a=bw-info" attribute(s) are contained in the SDP answer the IBCF:

- when requesting the TrGW to configure resources towards the succeeding node (figure 10.2.5.2, step 9), shall include for the selected codec the "Additional Bandwidth Properties" information element containing "a=bw-info" SDP attribute(s) providing information for the selected codec in the remote descriptor about bandwidths that will be used for the selected codec in the sending direction towards the succeeding node;

NOTE 2:   The included information corresponds to "a=bw-info" SDP attribute(s) from the received SDP answer for the "recv" or "sendrecv" direction.

- shall select a codec from the ones in the previously received SDP offer from the preceding node;

- if the received SDP offer contained the SDP "a=bw-info" attribute(s) for the selected codec:

    a) shall construct appropriate SDP "a=bw-info" attribute(s) for the selected codec according to the rules in 3GPP TS 26.114 [36]; and

NOTE 3:   The offer/answer negotiation is performed for each "a=bw-info" SDP attribute line, payload type, direction and bandwidth property individually.

    b) shall include the "Additional Bandwidth Properties" information element containing "a=bw-info" SDP attribute(s) in the remote descriptor describing bandwidths that will be used for the selected codec in the sending direction towards the preceding node when requesting the TrGW to reserve resources towards the preceding node (figure 10.2.5.2, step 12); and

NOTE 4:   The included information corresponds to "a=bw-info" SDP attribute(s) in the sent SDP answer for the "send" or "sendrecv" direction.

- include the selected codec with the corresponding SDP "a=bw-info" attribute(s) in the modified SDP answer (figure 10.2.5.2, step 15) that will be sent towards the preceding node.

If the received SDP answer contains codecs received in the SDP offer no transcoding at the TrGW is required and the IBCF shall:

- not include the "Additional Bandwidth Properties" information element containing the "a=bw-info" SDP attribute(s) when requesting the TrGW to configure resources towards the succeeding node (figure 10.2.5.2, step 9);

- not include the "Additional Bandwidth Properties" information element containing the "a=bw-info" SDP attribute(s) when requesting the TrGW to configure resources towards the preceding node (figure 10.2.5.2, step 12); and

- if the received SDP answer (figure 10.2.5.2, step 8) contained the SDP "a=bw-info" attribute(s), the IBCF shall check:

    a) if the IP version interworking is required and the received "a=bw-info" SDP attribute lines do not contain bandwidth properties for both IPv4 and IPv6, the IBCF may adjust the bandwidth properties in accordance with subclause 9.1.5;

    b) otherwise (if the IP version interworking is not required or the received "a=bw-info" SDP attribute lines contain bandwidth properties for both IPv4 and IPv6), the IBCF shall forward the SDP answer with unmodified SDP "a=bw-info" attribute(s).

The TrGW may use the "Additional Bandwidth Properties" information element indicating media bandwidth range for rate adaption (i.e. to select an appropriate encoding and redundancy) when transcoding media streams.

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 (differentiated services)

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   Bandwidth Policing

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

NOTE 1:   In order to support services that generate media with variable bitrate (e.g. video), the policing function needs to provide sufficient buffer space. The derivation of the correspondent token bucket size can be based on the estimated traffic volume over the expected maximum burst length (supposed time interval of the burst). For example, for MTSI media, 3GPP TS 26.114 [36] subclause 7.5.5 recommends a default period of 2 seconds for the derivation of average bitrates and provides further considerations regarding suitable time periods for speech and video.

NOTE 2:   The IBCF can derive the sustainable data rate from bandwidth parameters if it receives them within an SDP media description. The IBCF can:
- use the "b=AS" bandwidth modifier if received within an SDP body; or
- if the IBCF supports the enhanced bandwidth negotiation mechanism, use the "maximum supported bandwidth for the receiving direction" property value from the "a=bw-info" SDP attribute received within an SDP answer.
If the value of the "maximum supported bandwidth for the receiving direction" for the selected RTP payload type differs from the value of the "b=AS" bandwidth modifier, then the IBCF can use "maximum supported bandwidth for the receiving direction" property value from the "a=bw-info" SDP attribute to determine the sustainable data rate for the selected RTP payload.

10.2.10 IMS end-to-end media plane security

10.2.10.1   End-to-end security for RTP based media

An IBCF and a TrGW may support the end-to-end IMS media plane security for RTP based media 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

- provide "RTP/SAVP" or "RTP/SAVPF", as received in the SDP, to the TrGW as transport protocol for all related terminations, and not provide media related information to these terminations, to configure the TrGW to pass media and possibly associated RTCP control flows and not to reserve any resources.

NOTE: RTP/SAVP or SAVPF are provided to the TrGW even though it does not reserve any resources for this as such, but this is needed in order to allocate dual ports to support RTCP flows. These are also controlled as described in subclause 10.2.3. For "RTP/SAVP" or "RTP/SAVPF", RTCP will be encrypted and can not be interpreted by the TrGW. Media information is also meaningless as encryption will modify the properties of the media streams.

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

10.2.10.2   End-to-end security for TCP based media using TLS

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

NOTE: End-to-end IMS media plane security for TCP based media using TLS does not impact the TrGW.

End-to-end protection of MSRP (used in IMS session-based messaging) and BFCP (used in IMS conferencing) media is based on TLS, according to the TLS profile specified in Annex M of 3GPP TS 33.328 [32].

If the IBCF receives SDP containing media lines with "TCP/TLS/MSRP" (see IETF RFC 4975 [47] and IETF RFC 6714 [48]) and/or "TCP/TLS/BFCP" (see IETF RFC 4583 [49]) as transport protocol, the IBCF shall:

- forward the SDP with unmodified transport protocol for those media lines and unmodified TLS related SDP attribute(s); and

- indicate "TCP" to the TrGW as transport protocol for all related terminations, and provide no media related information to these terminations, to configure the TrGW to pass media transparently.

10.2.11 Through-Connection

10.2.11.1 General

The procedures in subclause A.7.1.2.2.9 of 3GPP TS 29.235 [29] are applicable.

In addition, prior to the completion of the SIP session set-up, i.e. until a 2xx response to the initial INVITE request is received, the IBCF may enable or disable media stream(s), thus allowing or forbidding early media in forward and/or backward direction.

If there is:

1) no SIP early dialog and the IBCF receives an 18x provisional response including an SDP answer; or

2) only one SIP early dialog, and the IBCF receives a SIP message with an SDP answer on that SIP early dialog,

then;

1) the IBCF shall save the received SDP answer; and

2) based on the operator policy, the IBCF may:

   - set the value of the Through-Connection information element based on the value of the direction attribute in the received SDP answer; or

   - set the value of the Through-Connection information element considering the em-param(s) of the P-Early-Media header field (defined in IETF RFC 5009 [58]) according to subclause 10.2.11.2; or

   - set the value of the Through-Connection information element based on the value of the direction attribute in the received SDP answer downgraded according to the configuration provisioned in the IBCF.

Upon reception of the 2xx response to the initial INVITE request, the IBCF shall enable the media stream by setting the value of the Through-Connection information element based on the value of the direction attribute in the last received SDP answer on the established SIP dialog, if the IBCF has not already set the value of the Through-Connection information element based on the same value of the direction attribute in the last received SDP answer on the corresponding SIP early dialog.

NOTE: The setting of StreamMode property by through-connection control does not impact a "control flow" component (i.e. an RTCP control component) as described in ITU-T Recommendation H.248.1 [26].

After the session establishment (i.e. after the 2xx response to the INVITE request is received and media session is established), if the IBCF receives an SDP answer indicating a different media stream direction than the current setting of the StreamMode property of the termination(s), the IBCF shall set the value of the Through-Connection information element based on the received SDP answer.

10.2.11.2 Through-connect control procedures considering the P-Early-Media header field

If the IBCF uses the em-param(s) of the P-Early-Media header field for the through-connect control of early media, the IBCF shall perform the procedures described in this subclause.

When a SIP 18x provisional response to an initial INVITE request with the P-Early-Media header field is received from the functional entity within the trust domain, then:

- the IBCF may decide not to perform the through-connect control of early media if the P-Early-Media header field includes the "gated" parameter and the IBCF shall not block early media in both directions on both terminations; and

- if the P-Early-Media header field includes the "gated" parameter and the IBCF decides to perform the through-connection control, or if the P-Early-Media header field does not include the "gated" parameter then the IBCF shall perform the procedures in the subsequent bullet 1), or the procedures in the subsequent bullet 2), or both of those procedures. If the IBCF does not perform the procedures in the bullets 1) or 2), the IBCF shall not block early media in both directions on the termination for which the IBCF does not perform the procedures in the bullet 1) or 2).

   1) For the termination which resides on the side receiving the 18x provisional provisional response;

      a) if the received em-param(s) in the P-Early-Media header field is set to "sendrecv", the IBCF shall set the Through-Connection information element to "sendrecv";

      b) if the received em-param(s) in the P-Early-Media header field is set to "recvonly", the IBCF shall set the Through-Connection information element to "sendonly";

      c) if the received em-param(s) in the P-Early-Media header field is set to "sendonly", the IBCF shall set the Through-Connection information element to "recvonly"; and

      d) if the received em-param(s) in the P-Early-Media header field is set to "inactive", the IBCF shall set the Through-Connection information element to "inactive".

   2) For the termination which resides on the side forwarding the 18x provisional response;

      a) if the received em-param(s) in the P-Early-Media header field is set to "sendrecv", the IBCF shall set the Through-Connection information element to "sendrecv";

      b) if the received em-param(s) in the P-Early-Media header field is set to "sendonly", the IBCF shall set the Through-Connection information element to "sendonly";

      c) if the received em-param(s) in the P-Early-Media header field is set to "recvonly", the IBCF shall set the Through-Connection information element to "recvonly"; and

      d) if the received em-param(s) in the P-Early-Media header field is set to "inactive", the IBCF shall set the Through-Connection information element to "inactive".

NOTE 1: According to IETF RFC 5009 [58], the non-direction parameter "gated" can be included after the direction parameter (e.g. "sendrecv") in the parameter list. The proxy performing gating of early media can add the parameter before forwarding the response.

NOTE 2: It is regarded as an error case if the direction authorized by the P-Early-Media header field is not enabled in the received SDP direction attribute. As indicated in IETF RFC 5009 [58] the applicable preconditions need to be met in order to allow early media in a particular direction, but the related handlig is left to the implementation.

When an 18x provisional response to an initial INVITE request without the P-Early-Media header field is received from the functional entity within the trust domain and no previous 18x provisional response to the initial INVITE request with the P-Early-Media header field has been received, then the IBCF may:

1) set the Through-Connection information element to "inactive"; or

2) set the Through-Connection information element to the value of the direction attribute in the last received SDP answer (received in the 18x provisional response or in a previous SIP message); or

3) set the value of the Through-Connection information element based on the value of the direction attribute in the received SDP answer (received in the 18x provisional response or in a previous SIP message) downgraded according to the configuration provisioned in the IBCF.

When an 18x provisional response to an initial INVITE request with the P-Early-Media header field is received from the functional entity other than the functional entity within the trust domain, then the IBCF shall not use the received em-param(s) in the P-Early-Media header field and the IBCF shall:

1) set the Through-Connection information element to "inactive"; or

2) set the Through-Connection information element based on the value of the direction attribute in the last received SDP answer(received in the 18x provisional response or in a previous SIP message); or

3) set the value of the Through-Connection information element based on the value of the direction attribute in the received SDP answer (received in the 18x provisional response or in a previous SIP message) downgraded according to the configuration provisioned in the IBCF.

NOTE 3: The IBCF will remove or modify the P-Early-Media header field in the above case.

10.2.12 Emergency Call

The procedures in subclause A.7.1.2.2.10 of 3GPP TS 29.235 [29] are applicable.

10.2.13 Explicit Congestion Notification support

10.2.13.1 General

An IBCF and TrGW may support Multimedia Telephony using Explicit Congestion Notification (ECN) according to IETF RFC 3168 [37], and may act as an ECN endpoint to enable ECN with a local ECN-capable terminal within a local network that properly handles ECN-marked packets.

10.2.13.2 Incoming SDP offer with ECN

If the IBCF receives an SDP offer containing the "a=ecn-capable-rtp" attribute (see IETF RFC 6679 [38]), then if all of the following statements are true:

a) the IBCF supports ECN according to 3GPP TS 26.114 [36];

b) the TrGW supports ECN according to 3GPP TS 26.114 [36];

c) the IBCF knows (via configuration) that the succeeding network supports ECN according to 3GPP TS 26.114 [36]; and

d) the IBCF does not insert any transcoding;

then the IBCF shall:

- if the "ecn-capable-rtp" attribute includes both the "ice" initiation method and other initiation methods, remove the "ice" initiation method from the "ecn-capable-rtp" attribute and forward the attribute with this modification in the outgoing SDP offer;

- if the "ecn-capable-rtp" attribute only includes the "ice" initiation method, remove the "ecn-capable-rtp" attribute, any "rtcp-fb" attribute with the "nack" feedback parameter and the "ecn" feedback parameter value, and any "ecn-sum" parameter within a "rtcp-xr" attribute from the outgoing SDP offer;

- if the "ecn-capable-rtp" attribute did not includes the "ice" initialisation method, forward the unmodified "ecn-capable-rtp" attribute within the outgoing SDP offer; and

- if the IBCF includes the "ecn-capable-rtp" attribute within the outgoing SDP offer, forward the SDP offer containing ECN parameters to the succeeding network.

Otherwise the IBCF shall remove the "ecn-capable-rtp" attribute, any "rtcp-fb" attribute with the "nack" feedback parameter and the "ecn" feedback parameter value, and any "ecn-sum" parameter within an "rtcp-xr" attribute from the outgoing SDP offer.

If the IBCF forwarded the SDP offer containing the "a=ecn-capable-rtp" attribute and receives an SDP answer also containing the "a=ecn-capable-rtp" attribute (the reception of the attribute indicates a successful ECN negotiation) then the IBCF shall forward the SDP answer to its preceding node and shall indicate to the TrGW that it shall transfer ECN bits in IP header transparently.

If the IBCF forwarded the SDP offer containing the "a=ecn-capable-rtp" attribute and receives an SDP answer without the "a=ecn-capable-rtp" attribute and the TrGW supports at least some of the initialisation methods within the "a=ecn-capable-rtp" attribute in the previously received SDP offer,

NOTE 1: Only the "leap" initialisation method is supported over the Ix interface in this release.

the IBCF shall:

- act as an end point for ECN;

- select an initialisation method supported by the TrGW;

- determine if application specific feedback or ECN feedback messages shall be used, taking into account whether the TrGW supports ECN feedback messages, and the negotiation procedures in 3GPP TS 26.114 [36];

- determine if ECN XR summary reports can be used, taking into account whether they are supported at the TrGW, and the negotiation procedures in 3GPP TS 26.114 [36];

- send the SDP answer according to 3GPP TS 26.114 [36] and the capabilities of the TrGW, containing the ECN attribute "a=ecn-capable-rtp"; and

- indicate to the TrGW that it shall apply the ECN procedures (according to 3GPP TS 26.114 [36]) and act as an ECT endpoint.

If the IBCF receives an SDP offer containing the "a=ecn-capable-rtp" attribute and bullets a) and b) above are satisfied but if bullet c) or d) or both are not met then the IBCF shall remove ECN related attributes before forwarding the SDP offer. If the TrGW supports at least some of the initialisation methods offered within the "a=ecn-capable-rtp" attribute,

NOTE 2: Only the "leap" initialisation method is supported over the Ix interface in this release.

the IBCF shall:

- act as an end point for ECN;

- select an initialisation method supported by the TrGW;

- determine if application specific feedback or ECN feedback messages shall be used, taking into account whether the TrGW supports ECN feedback messages, and the negotiation procedures in 3GPP TS 26.114 [36];

- determine if ECN XR summary reports can be used, taking into account whether they are supported at the TrGW and the negotiation procedures in 3GPP TS 26.114 [36];

- send an SDP answer according to 3GPP TS 26.114 [36] and the capabilities of the TrGW, containing the "a=ecn-capable-rtp" attribute; and

- indicate to the TrGW that it shall apply the ECN procedures (according to 3GPP TS 26.114 [36]) and act as an ECT endpoint.

The TrGW should not send RTCP XR ECN summary reports.

10.2.13.3 Incoming SDP offer without ECN

If the IBCF receives an SDP offer without the "a=ecn-capable-rtp" attribute then if all of the following statements are true:

a) the IBCF supports ECN according to 3GPP TS 26.114 [36];

b) the TrGW supports ECN according to 3GPP TS 26.114 [36]; and

c) the IBCF knows (via configuration) that the succeeding network supports ECN according to 3GPP TS 26.114 [36];

the IBCF may include the "a=ecn-capable-rtp" attribute in the SDP offer it forwards towards the succeeding node, indicating the related capabilities of the TrGW.

NOTE: ECN XR summary reports and RTCP AVPF ECN feedback message are not supported in this release towards IMS terminations.

If the IBCF inserted ECN attributes in the SDP offer and receives an SDP answer containing the "a=ecn-capable-rtp" attribute the IBCF shall act as an endpoint and shall return the SDP answer to the preceding node removing the "a=ecn-capable-rtp" attribute, any "rtcp-fb" attribute with the "nack" feedback parameter and the "ecn" feedback parameter value, and any "ecn-sum" parameter within a "rtcp-xr" attribute, and shall indicate to the TrGW that it shall apply the

ECN procedures according to 3GPP TS 26.114 [36] and act as an ECT endpoint. The TrGW should not send RTCP XR ECN summary reports.

If the IBCF inserted the "a=ecn-capable-rtp" attribute in the SDP offer and receives an SDP answer without the "a=ecn-capable-rtp" attribute the IBCF shall continue the call without any ECN active.

10.2.13.3a Detection of ECN failures by TrGW

If the TrGW acts as ECN endpoint and detects an ECN-related error case, for example non-ECT in the received packets when ECT(0) was expected or detecting a very high packet loss rate when ECN is used, the TrGW shall notify the IBCF. The IBCF should then initiate a session re-negotiation to disable ECN.

10.2.13.4 Interworking with non-3GPP ECN IP terminal

10.2.13.4.1 Support for additional ECN parameters

An IBCF and TrGW may support additional ECN parameter settings than defined in subclause 10.2.13.2. The following sub-clauses describe the optional behaviour if the IBCF and TrGW support these additional values.

10.2.13.4.2 Incoming SDP offer from external IP network with ECN

If the IBCF receives an incoming SDP offer from the external IP network containing values in the incoming SDP offer not supported by MTSI then it shall configure the SDP offer as defined in subclause 10.2.13.2 when forwarding the SDP offer to the IMS.

When receiving the SDP answer from the IMS the IBCF may configure the SDP answer to the external IP network with alternative settings depending on what is received from the IMS and what was offered by the external IP network. The permitted alternatives are listed in table 10.2.13.4.1; the supported alternatives are implementation options which need to be derived through configuration or package auditing.

10.2.13.4.3 Incoming SDP offer from the IMS with ECN

If the IBCF receives an incoming SDP offer from the IMS and it supports additional ECN parameter settings than those defined in subclause 10.2.13.2 the IBCF may add these to the SDP offer forwarded to the external IP network.

When receiving an SDP answer from the external IP network the IBCF shall respond to the IMS in accordance with subclause 10.2.13.2. If the IBCF modifies any ECN-related parameters in the forwarded SDP answer compared to the received SDP answer, the IBCF shall configure its TrGWas an ECN endpoint. The permitted alternatives are listed in table 10.2.13.4.1; the supported alternatives are implementation options which need to be derived through configuration or package auditing.

Table 10.2.13.4.1: Possible configurations when interworking with non-3GPP ECN IP terminal

ECN SDP Attribute and required TrGW Action		
IMS side	**External IP Network**	**TrGW Action**
Initiation		
"leap"	"rtp" NOTE 3	Act as an Endpoint and trigger explicit initiation using RTP and RTCP as described in IETF RFC 6679 [38] toward the external IP network. When initial ECT marked packets are received from the external IP network these are forwarded to the IMS (all packets shall be marked) and early feedback and XR Summary reports are sent back to the external IP network. If ECT marked packets are received from the IMS before any initiation is completed with the external IP network then ECT marking should be removed and only a fraction of the packets should be marked until feedfback is received from the external IP network.
	"ice"	This initiation method is not supported in the present release.
Mode		
"setread"	"readonly"	Act as ECN transparent unless required to act as an Endpoint for other reasons but mark packets toward the IMS with ECT(0). If ECN-CE is received from the IMS then this shall be handled by the IMS termination as currently specified for the non-interworking case and not forwarded to the external IP network.
	"setonly"	Act as ECN transparent (unless required to act as ECN Endpoint for other reasons) - ECN-CE marked packets will not be received from external IP network, ECN-CE marked packets from the IMS will be passed to the external IP network.
ECT		
"ect(0)"	"ect(1)"	Act as ECN transparent unless required to act as an Endpoint for other reasons but mark packets toward the IMS with ECT(0) and mark packets toward external network with ECT(1).
	"random"	Act as ECN transparent unless required to act as an Endpoint for other reasons but mark packets toward IMS with ECT(0). Packets received from the IMS are left as ECT(0).
RTCP feedback		
no "rtcp-fb:* nack ecn" (received driven congestion control)	"rtcp-fb:* nack ecn " (sender driven congestion control)	For AMR, the handling of an AVPF feedback message received from the external IP the handling is not defined. For video related AVFP feedback messages received from the external IP network the TrGW shall generate the appropriate TMBR request towards the IMS. If a TMBR request is received from the IMS the TrGW shall generate an appropriate AVPF feedback message to the external IP network.
"rtcp-fb:* nack ecn" (sender driven congestion control)	rtcp-fb:* nack ecn" (sender driven congestion control)	An AVPF feedback message received from the external IP network shall be forwarded via the IMS termination.
RTCP XR ECN summary report		
-	"rtcp-xr:ecn-sum"	RTCP XR is not bi-directions and each end-point indicates wheteever XR feedback it supports. Hence, if the SDP offer does not contain rtcp-xr with "ecn-sum" then it can still be added in the SDP answer. The TrGW shall include XR ECN Summary reports towards the external IP network and receive reports from the external IP network. (NOTE 4)
NOTE1: The settings for IMS side may be supported on the External IP Network side in which case no interworking is specified.		
NOTE 2: Each parameter is described separately as each parameter may or may not need to be interworked. Unless stated otherwise the assumption is that each parameter can be treated independently.		
NOTE 3: RTCP feedback messages need to be supported and negotiated for the "rtp" initialisation method.		
NOTE 4: The contents of the XR reports will be limited to data received from the external IP network.		

10.2.13.5 Message sequence chart

10.2.13.5.1 ECN support requested (ECN endpoint)

Figure 10.2.13.5.1.1 shows the message sequence chart example for requesting ECN.
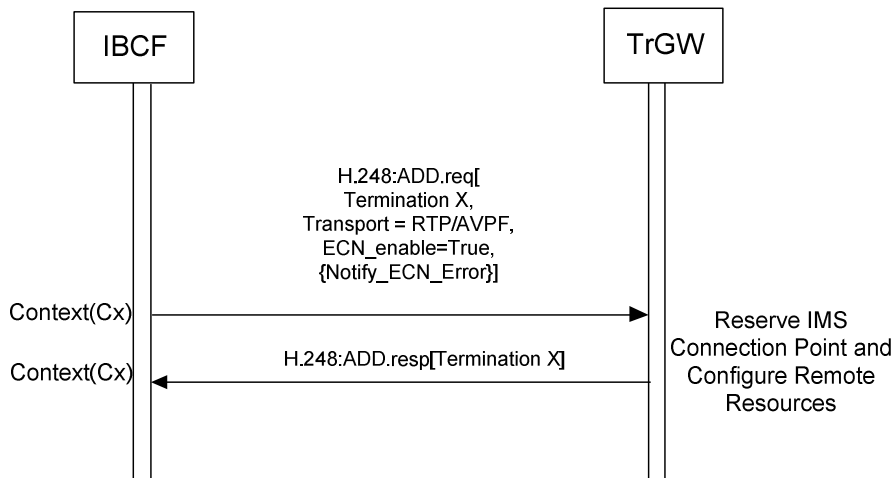
Figure 10.2.13.5.1.1: Procedure to Request ECN

Upon receipt of a request to apply ECN the TrGW shall set the ECN field of the IP header in accordance with 3GPP TS 26.114 [36] when sending any data packets.

Upon receipt of any IP headers indicating ECN Congestion Experienced (ECN-CE) the TrGW shall trigger rate adaptation in accordance with 3GPP TS 26.114 [36].

NOTE: ECN requires the IBCF to configure the TrGW with all media attributes to allow rate adaptation even if no transcoding is required/supported in the TrGW.

10.2.13.5.2 ECN Active Indicated (ECN transparent)

Figure 10.2.13.5.2.1 shows the message sequence chart example for indicating ECN transparent.
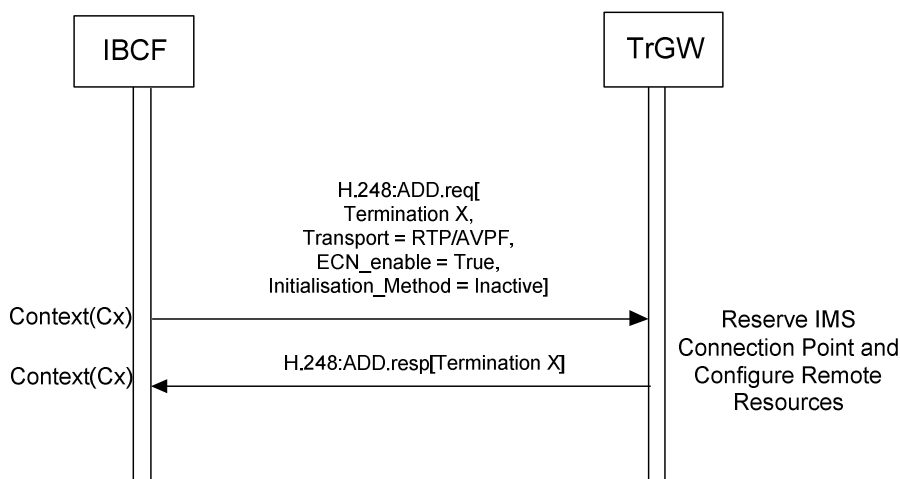
Figure 10.2.13.5.2.1: Procedure to indicate ECN transparent negotiated

Upon receipt of the indication that ECN transparent has been negotiated the TrGW shall forward IP packets with ECN bits set unmodified.

10.2.13.5.3 ECN Failure Indication (ECN endpoint)

Figure 10.2.13.5.3.1 shows the message sequence chart example for an ECN Failure Event.
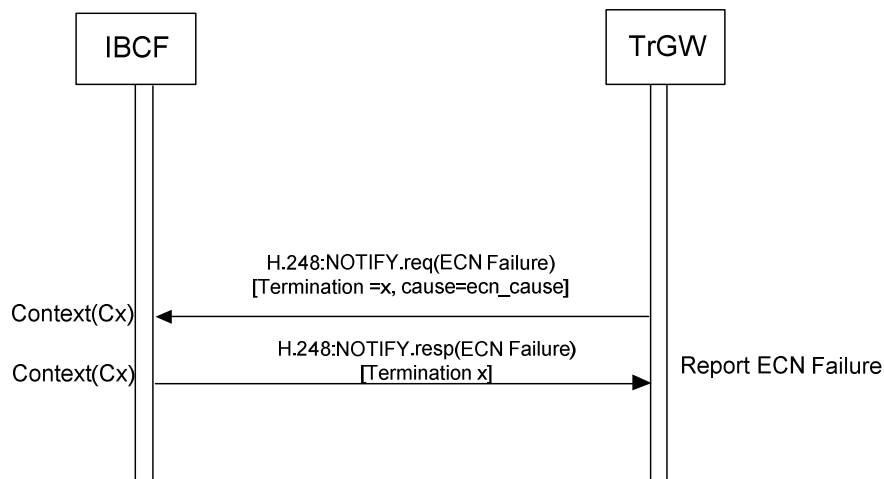
Figure 10.2.13.5.3.1: Procedure to Report ECN Failure

When the IBCF receives a Notification indicating that a failure has occurred, the MGCF may trigger a new SDP offer to disable ECN.

10.2.14 Optimal Media Routeing

An IBCF may support optimal media routeing (OMR) procedures, as defined in 3GPP TS 29.079 [39].

3GPP TS 29.079 [39] specifies that "secondary media resources" may be allocated in addition to "primary media resources". If cotrolled by an IBCF, such primary or secondary media resources are TrGWs controlled over the Ix interface with procedures specified in the present specification.

If the IBCF applies OMR procedures, the following modifications to the procedures within the present specification are applicable:

- Under conditions specified in 3GPP TS 29.079 [39], the IBCF uses information from OMR related SDP attributes as remote connection and port information that is provided towards the TrGW within the call establishment procedures in subclause 10.1.3.1.1.

- Under conditions specified in 3GPP TS 29.079 [39], the IBCF encapsulates local addess and port information, as received from the TrGW within the call establishment procedures in subclause 10.1.3.1.1, in OMR related SDP attributes.

- Under conditions specified in 3GPP TS 29.079 [39], the IBCF uses information from OMR related SDP attributes as codec information that is provided towards the TrGW within the media control procedures in clause 10.2.5.

- 3GPP TS 29.079 [39] specifies OMR-specific events that trigger the call release procedures in subclause 10.1.3.1.2.

10.2.15 IP Realm Availability

The procedures in subclause A.7.1.2.2.5 of 3GPP TS 29.235 [29] are applicable.

10.2.16 Access Transfer procedures with media anchored in ATGW

The procedures in the present clause are optional to be supported for both IBCF and TrGW when supporting the ATCF and ATGW functionality (see subclause 6.1.4).

The procedures in subclause 6.2.14 of 3GPP TS 23.334 [43] are applicable, except that where the Iq interface is mentioned in those procedures, the Ix interface is applicable.

10.2.17 Multimedia Priority Service (MPS) Support

10.2.17.1 General

The Multimedia Priority Service (MPS) is specified in 3GPP TS 22.153 [44]. The IBCF/TrGW may support the priority treatment of a call/session identified as an MPS call/session. If MPS is supported then upon receipt of the MPS priority information in the call control signalling:

- The IBCF shall recognise the call/session as having priority.

- The IBCF shall send the Priority information for a context to the TrGW to enable the priority treatment described below related to the TrGW.

- The IBCF shall apply priority handling to H.248 transactions related to priority calls/sessions when network resources are congested, e.g., preferential treatment in any queues or buffers.

- The IBCF may send the updated priority information and, if DiffServ is used, provision a suitable DSCP marking for the updated MPS priority level to the TrGW if it needs to change the priority information previously communicated to the TrGW for an MPS call/session.

- If the H.248 control association utilises a transport with the possibility for prioritisation, the IBCF may apply priority using the appropriate prioritisation procedures.

- If the MPS Priority service requires a specific MPS DSCP setting, the IBCF shall configure the TrGW to apply a specific MPS DSCP marking to the user data transport packets to indicate that the packets are of a higher priority than those for normal calls.

- If the TrGW receives an indication to apply a specific MPS DSCP marking to the user data transport packets, it shall apply this DSCP marking to the IP headers.

NOTE 1: Support of Diffserv procedures by the TrGW assumes an operator uses Diffserv for prioritising user plane traffic related to an MPS call/session.

- When the IBCF marks a Context with Priority information, the TrGW may use the Priority information for selecting resources for the media and signaling transport with priority. The following actions may be taken by the TrGW if it has reached a congested state:

  i) seize priority reserved resources; or

  ii) if resources are completely congested, indicate that in a Command Response error code.

NOTE 2: The Priority information can be used to derive Layer 2 QoS marking and trigger priority identification and priority treatment for other QoS technologies than Diffserv.

This clause describes the Ix signalling procedures and their interactions with SIP signalling in the control plane and with user plane procedures to support the requirements for MPS. These Ix signalling procedures may or may not apply depending on the network configuration (e.g. whether the TrGW is shared by multiple IBCFs or whether the IBCF controls multiple TrGWs for a given route – Media Gateway Group).

The IBCF can receive a SIP INVITE with MPS priority information (see 3GPP TS 23.228 [8], subclause 5.21).

10.2.17.2 TrGW Resource Congestion in ADD response, request is queued

If the IBCF requests a resource via the Reserve and Configure TrGW Connection Point procedure or Reserve TrGW Connection Point procedure and receives an error indicating that the requested resource could not be seized (e.g. H.248 error code #510 "insufficient resources") and the IBCF does not have an alternative TrGW through which it can route the call/session, the IBCF queues the priority call/session and gives it priority over any further Reserve and Configure TrGW Connection Point or Reserve TrGW Connection Point procedures for lower priority calls/sessions towards this TrGW until the requested resource for this queued call/session is successfully seized. The example sequence is shown in Figure 10.2.17.2.1.
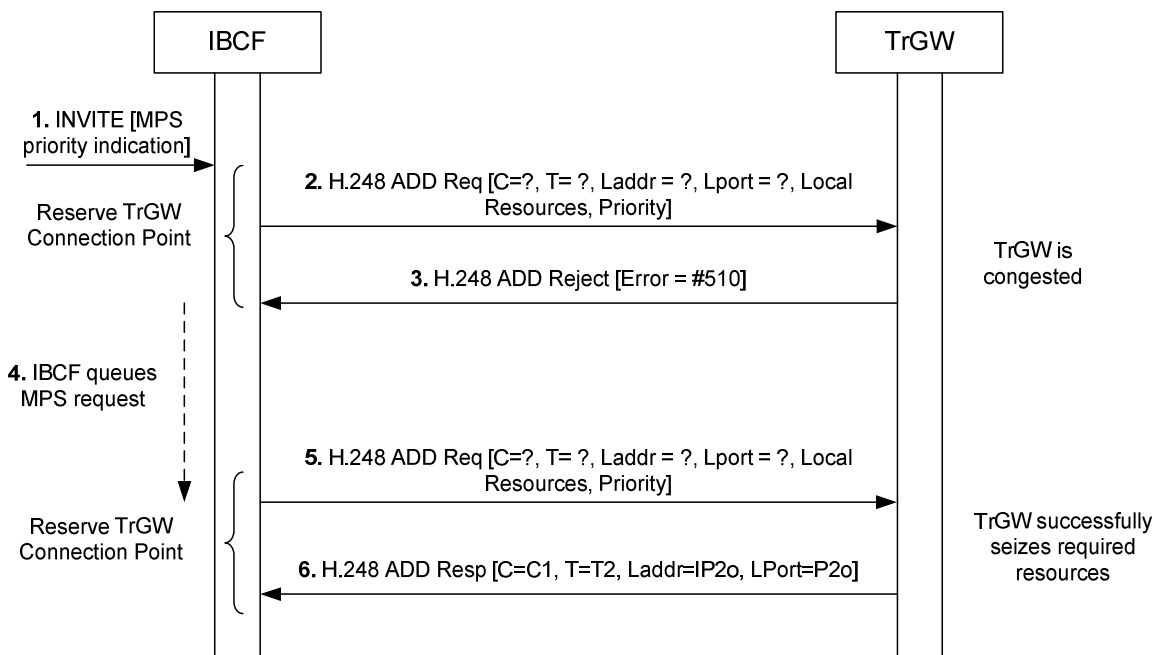
Figure 10.2.17.2.1: Request to Reserve MPS priority call resources when TrGW is congested

10.2.17.3 TrGW Resource Congestion in ADD response, IBCF seizes new TrGW

If the IBCF requests a resource via the Reserve and Configure TrGW Connection Point procedure or Reserve TrGW Connection Point procedure and receives an error indicating that the requested resources could not be seized due to congestion (e.g. H.248 error code #510 "insufficient resources") and Media Gateway Groups are implemented the IBCF seizes a new TrGW from the same Media Gateway Group before resorting to any queuing of the priority call/session (as described in subclause 10.2.17.2) to enable the MPS call/session to proceed as early as possible.

10.2.17.4 TrGW Priority Resource Allocation

If the TrGW supports the Priority information (e.g. determined through provisioning or package profile), the IBCF requests a resource via the Reserve and Configure TrGW Connection Point procedure or Reserve TrGW Connection Point procedure and includes the Priority information. The TrGW may then provide priority allocation of resources once a congestion threshold is reached. The example sequence is shown in figure 10.2.17.4.1. If the TrGW is completely congested it shall indicate this to the IBCF as described in subclause 10.2.17.2.
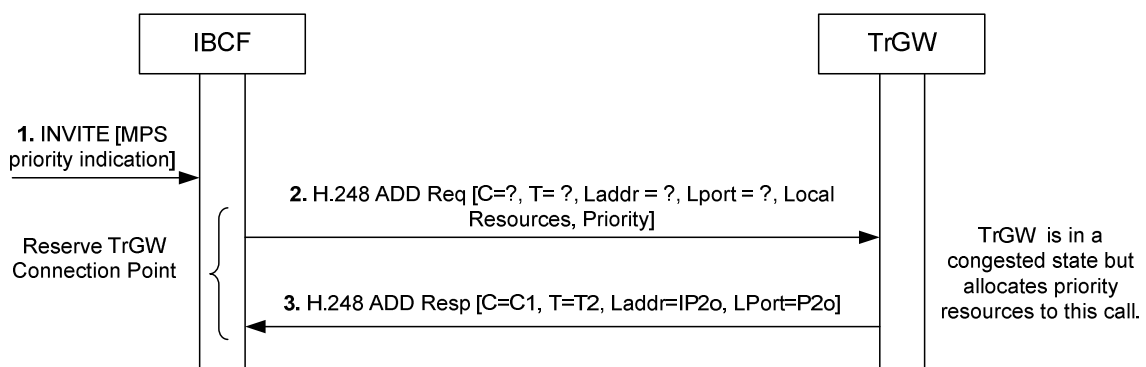
Figure 10.2.17.4.1: Request to reserve MPS priority call resources when TrGW is congested, priority resources are allocated

The TrGW may also provide priority allocation for resources requested via a subsequent Configure TrGW Connection Point procedure not including Priority information if the related context has been marked with priority information during the Reserve TrGW Connection Point or Reserve and Configure TrGW Connection Point procedure.

10.2.17.5   TrGW Priority User Data marking

The IBCF may request the streams associated to an MPS call/session to be marked with certain priority code point as described in subclause 10.2.7. The TrGW shall then mark each IP packet header accordingly. The example sequence is shown in figure 10.2.17.5.1.
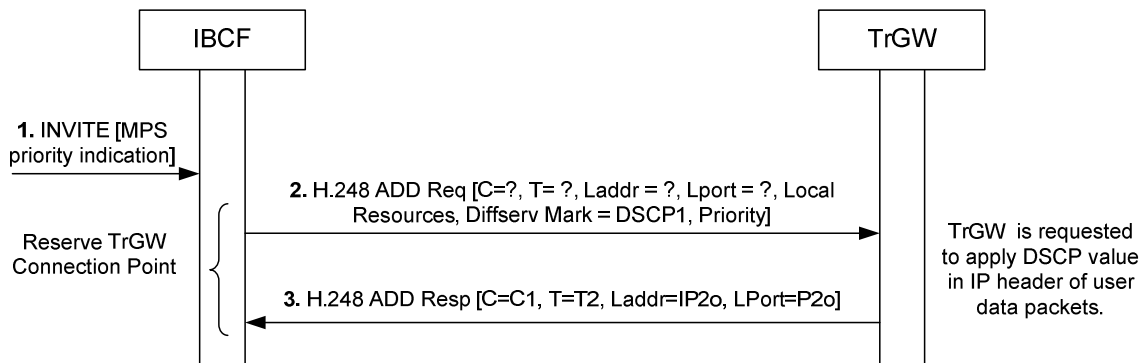
Figure 10.2.17.5.1: Request to reserve IMS resources and apply DSCP marking for MPS

10.2.17.6   TrGW Priority Modification

If the IBCF seized an IP termination for a priority call/session with a default priority and subsequently needs to modify the priority information previously communicated to the TrGW (e.g. subject to subsequent authorisation by an authorisation point, see 3GPP TS 24.229 [1] subclause 4.11), the IBCF may modify the existing IP termination for the MPS call/session with the actual priority and, if DiffServ is used, provision a suitable DSCP marking for the updated MPS priority level to the TrGW via the Configure TrGW Connection Point Procedure.

> NOTE: The specific Ix related call sequence which details the handling to support the requirements defined in 3GPP TS 24.229 [1] subclause 4.11 and 3GPP TS 23.228 [8], subclause 5.21 is not specified and therefore implementations might exist which fulfil these requirements but do not require modification of the priority information across the Ix interface.

10.2.18   Coordination of Video Orientation

10.2.18.1   General

The IBCF and the TrGW may support the Coordination of Video Orientation (CVO) as defined in 3GPP TS 26.114 [36].

If the IBCF receives an SDP body containing the RTP header extension attribute(s) "a=extmap", as defined in IETF RFC 5285 [45], and if "a=extmap" attribute indicates a CVO URN(s) (i.e. the CVO URN for a 2 bit granularity of rotation and/or the CVO URN for a higher granularity of rotation) as defined in 3GPP TS 26.114 [36], then:

a) if the IBCF and the TrGW support the CVO feature:

-   the IBCF shall include an "extended RTP header for CVO" information element when seizing resources in the TrGW to indicate to the TrGW that it shall allow the RTP header extension for CVO to pass; and

-   the IBCF shall forward within SIP signalling the SDP body received from the preceding node to the succeeding node with unmodified "a=extmap" attribute(s); or

b) if the TrGW does not support the CVO feature the IBCF shall forward within SIP signalling, the SDP body received from the preceding node to the succeeding node without any "a=extmap" attributes.

If the TrGW supports the CVO feature and has been instructed as described above to pass on the extended RTP header for CVO for both incoming and outgoing terminations then:

-   if the TrGW does not apply video transcoding, it shall pass any received RTP CVO header extension to succeeding RTP streams; or

- if the TrGW applies video transcoding, it shall keep the video orientation unchanged during the transcoding and copy the received RTP CVO header extension to the succeeding outgoing RTP stream(s) after transcoding the associated group of packets.

NOTE 1: IETF RFC 5285 [45] provides a framework for header extensions and can also be used for non-CVO related purposes. It is an implementation decision of the TrGW if it only passes CVO related RTP header extensions, or if it passes any RTP header extension when being instructed with the "extended RTP header for CVO" information element.

NOTE 2: The behaviour of the TrGW when being instructed with the "extended RTP header for CVO" information element only at one termination is an implementation decision.

10.2.18.2 Message sequence chart

Figure 10.2.18.2.1 shows the message sequence chart example for indicating extended RTP header for Coordination of Video Orientation.
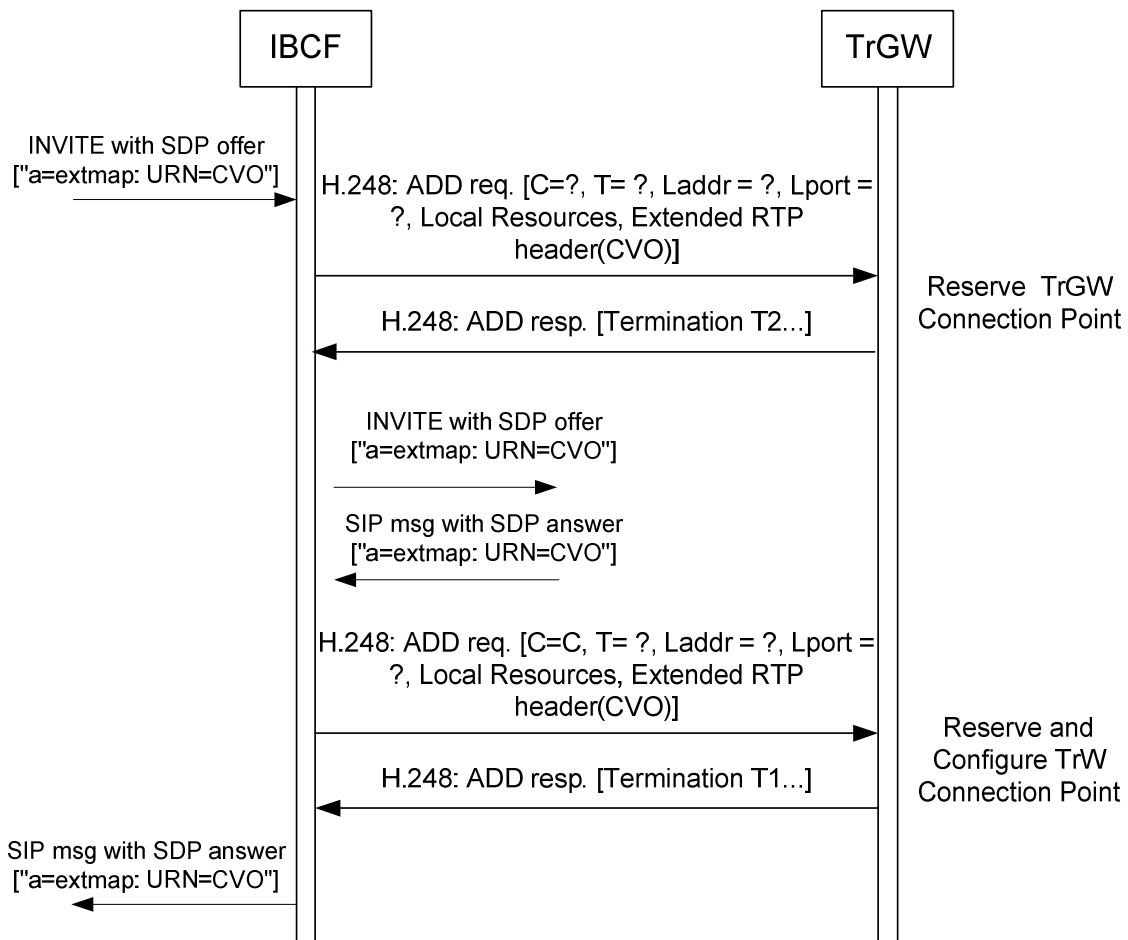
Figure 10.2.18.2.1: Procedure to indicate RTP extension header for CVO

The IBCF shall send the "extended RTP header for CVO" information element only with supported CVO URN(s) to the TrGW. If the TrGW does not support the CVO feature, the IBCF shall not send the "extended RTP header for CVO" information element to the TrGW.

NOTE: If the IBCF receives an SDP answer which includes the "a=extmap" attribute with a CVO URN with a granularity that the TrGW has not included in its response, or if the SDP answer does not include any "a=extmap" CVO related attribute, it is not necessary to modify the TrGW for this reason alone. Doing that would only add unnecessary signalling without requiring any action or changes in the TrGW. However if the IBCF needs to modify the media attributes for other purposes, in particular due to transcoding then the TrGW is updated in accordance with the received SDP answer, that is, either with the "extended RTP header for CVO" information element containing the received CVO URN if the CVO related "a=extmap" attribute has been included in the received SDP answer or without the "extended RTP header for CVO" information element if the CVO related "a=extmap" attribute has not been included in the received SDP answer (thus removing the requirement for sending the received RTP header extension with CVO bits for the transcoded stream.

10.2.19 Generic image attributes

10.2.19.1 General

The IBCF and TrGW may support a media-level SDP image attribute "a=imageattr" defined in IETF RFC 6236 [46] to negotiate the image size for sending and receiving video as required by 3GPP TS 26.114 [36].

NOTE 1: The image attribute may be used within the SDP capability negotiation framework and its use is then specified using the "a=acap" parameter.

If the IBCF:

- supports the negotiation of the image size;

- receives an SDP body containing the image attribute(s) "imageattr" defined in IETF RFC 6236 [46]; and

- does not offer or does not apply transcoding procedures defined in subclause 10.2.5;

the IBCF shall forward the SDP body with unmodified image attribute(s).

If the IBCF applies transcoding procedures defined in subclause 10.2.5 then the following additional actions may be performed if the negotiation of the image size is supported by the IBCF and the TrGW.

a) Upon receipt of an SDP offer containing the image attribute(s) from the preceding node (figure 10.2.5.2, step 1) and if the received image sizes are supported by the TrGW:

1) if the IBCF seizes an outgoing IP termination with the media related information before sending the SDP offer the IBCF may send the generic image attribute parameter to the TrGW (figure 10.2.5.2, step 3).

2) the IBCF shall include the SDP image attribute(s) "a=imageattr" indicating the supported image sizes in the modified SDP offer (figure 10.2.5.2, step 6).

b) Upon receipt of an SDP answer from the succeeding node (figure 10.2.5.2, step 8) and if the returned SDP answer:

1) does not contain the image attribute(s) and contains media offered by the preceding node (i.e. no transcoding at the TrGW is required) then the IBCF shall send to the preceding node the SDP answer without image attribute;

2) does not contain the image attribute(s) and if the IBCF is an endpoint for the video stream (transcoding) then the IBCF:

- may send the generic image attribute parameter to the TrGW when seizing or modifying resources (figure 10.2.5.2, step 12); and

- shall include the SDP image attribute(s) "a=imageattr" indicating the supported image sizes in the modified SDP answer (figure 10.2.5.2, step 15);

3) contains the image attribute(s) and the media offered by the preceding node (i.e. no transcoding at the TrGW is required) then the IBCF shall send to the preceding node the SDP answer containing the received image attribute(s); or

4) contains the image attribute(s) and if the IBCF is an endpoint for the video stream (transcoding) and if the received image sizes are supported by the TrGW then the IBCF:

- may send the generic image attribute parameters for the send and receive directions to the TrGW when seizing or modifying resources (figure 10.2.5.2, step 9 and step 12); and

- shall include the SDP image attribute(s) "a=imageattr" indicating the supported image sizes in the modified SDP answer (figure 10.2.5.2, step 15)

NOTE 2: The IBCF not supporting the negotiation of generic image attributes will ignore the SDP image attribute received in the SDP offer and will return the SDP answer without any associated SDP image attribute.

When sending the SDP body with image attribute(s) on the Mx interface the IBCF shall include in the "a=imageattr":

- "recv" keyword and corresponding image sizes which the TrGW supports in the receiving direction; and

- "send" keyword and corresponding image sizes which the TrGW supports in the sending direction.

If the TrGW is configured with different image sizes on the receive direction of one termination and the send direction of another interconnected termination, then it shall adjust the frame sizes accordingly when forwarding video media streams and use the image size as described in 3GPP TS 26.114 [36] when sending media.

NOTE 3: The relation between the negotiated image sizes and CVO are specified in 3GPP TS 26.114 [36].

NOTE 4: The generic image attribute includes information related to the send and receive capabilities of a single termination, and the adjustment of image sizes is typically based on the setting of two connected terminations in a single context.

10.2.19.2   Indication of generic image attributes

The IBCF may include the generic image attributes to the TrGW. The example sequence is shown in figure 10.2.19.2.1.

The list of image sizes per payload type supported by the TrGW shall be preconfigured in the IBCF. If the image sizes received within an SDP body on the Mx interface are not all supported by the TrGW then the IBCF shall only send the list of corresponding TrGW supported image sizes to the TrGW. If no image size is supported by the TrGW, the IBCF shall not send the generic image attribute parameter to the TrGW.
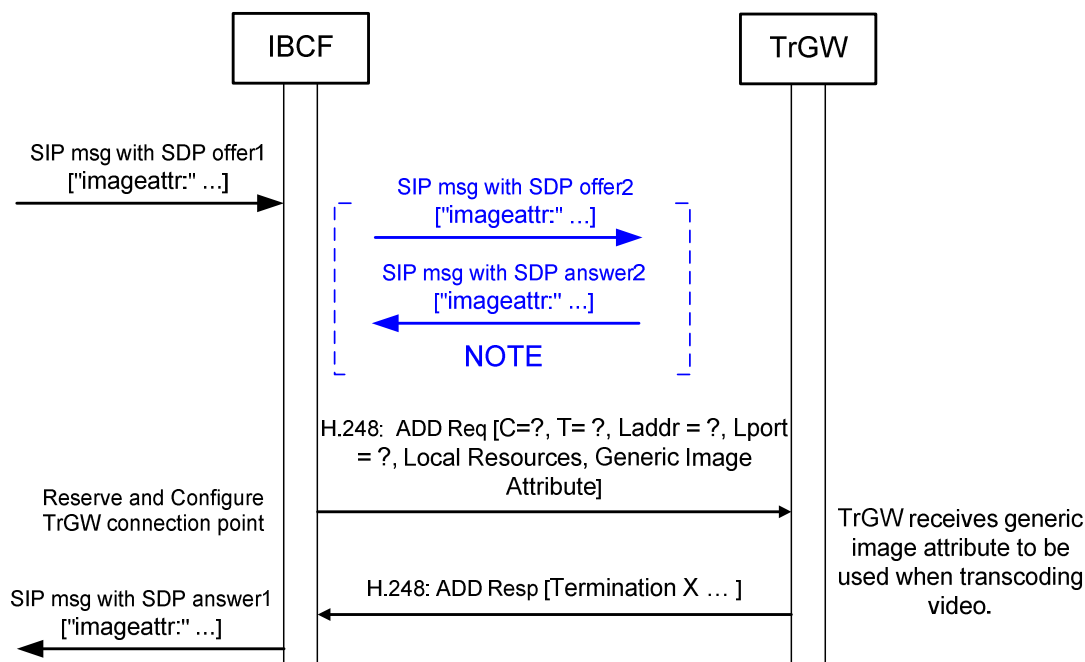
NOTE: shown sequence applies to the creation of the incoming termination T2 from the figure 10.2.5.2 and when both, the IBCF and the TrGW support the generic image attribute. The outgoing termination T1 may be created in advance (i.e. before sending SDP offer2) as shown in the figure 10.2.5.2 or upon receipt of the SDP answer2. Even if the IBCF reserves the resources in advance the media information may be omitted at this stage (as described in subclause 10.2.5) and thus the generic image attribute will not be sent to the TrGW if the media information is omitted.

Figure 10.2.19.2.1: Request to reserve TrGW connection point with generic image attribute

10.2.20 Interactive Connectivity Establishment (ICE)

The IBCF and the TrGW may support ICE functionality as specified in IETF RFC 5245 [50] and 3GPP TS 24.229 [1] to support a UE residing behind a remote NAT.

Support of full ICE functionality is optional, but if ICE is supported, the IBCF and the TrGW shall at least support ICE lite as specified in IETF RFC 5245 [50].

The requirements for the IMS-ALG and the IMS-AGW as specified in subclause 5.17 of 3GPP TS 23.334 [43], apply to the IBCF and the TrGW when the ICE procedures are supported.

10.2.21 MSRP handling

The IBCF and TrGW may support the handling of the Message Session Relay Protocol (MSRP), IETF RFC 4975 [47]. If they support MSRP handling, they shall apply the procedures as specified in the subclause 5.19 and subclause 6.2.19 of 3GPP TS 23.334 [43].

10.2.22 Alternative connection (ALTC) addresses management

An IBCF may support the ALTC functionality as specified in IETF RFC 6947 [51] and 3GPP TS 24.229 [1] to advertise alternative IP addresses (IPv4 and IPv6 address types) to the terminating side.

The requirements for the IMS-ALG as specified in subclause 5.21 of 3GPP TS 23.334 [43], apply to the IBCF when the procedures related to ALTC are supported.

The ALTC procedures as described specified in subclause 6.2.20 of 3GPP TS 23.334 [43] are then applicable, except that where the Iq interface is mentioned in those procedures, the Ix interface is applicable.

10.2.23 Video Region-of-Interest (ROI)

10.2.23.1 General

The IBCF and the TrGW may support the video Region-of-Interest (ROI) as defined in 3GPP TS 26.114 [36]. Three modes are specified for supporting ROI, including "Far End Camera Control (FECC)", "Arbitrary ROI" and "Pre-defined ROI". The IBCF and the TrGW may independently support any of these modes.

10.2.23.2 "Far End Camera Control" mode

10.2.23.2.1 General

The procedures in subclause 5.22.2 of 3GPP TS 23.334 [43] are applicable.

10.2.23.2.2 Message sequence chart

Figure 10.2.23.2.2.1 shows the message sequence chart example for indicating Video Region-of-Interest (ROI) using FECC.
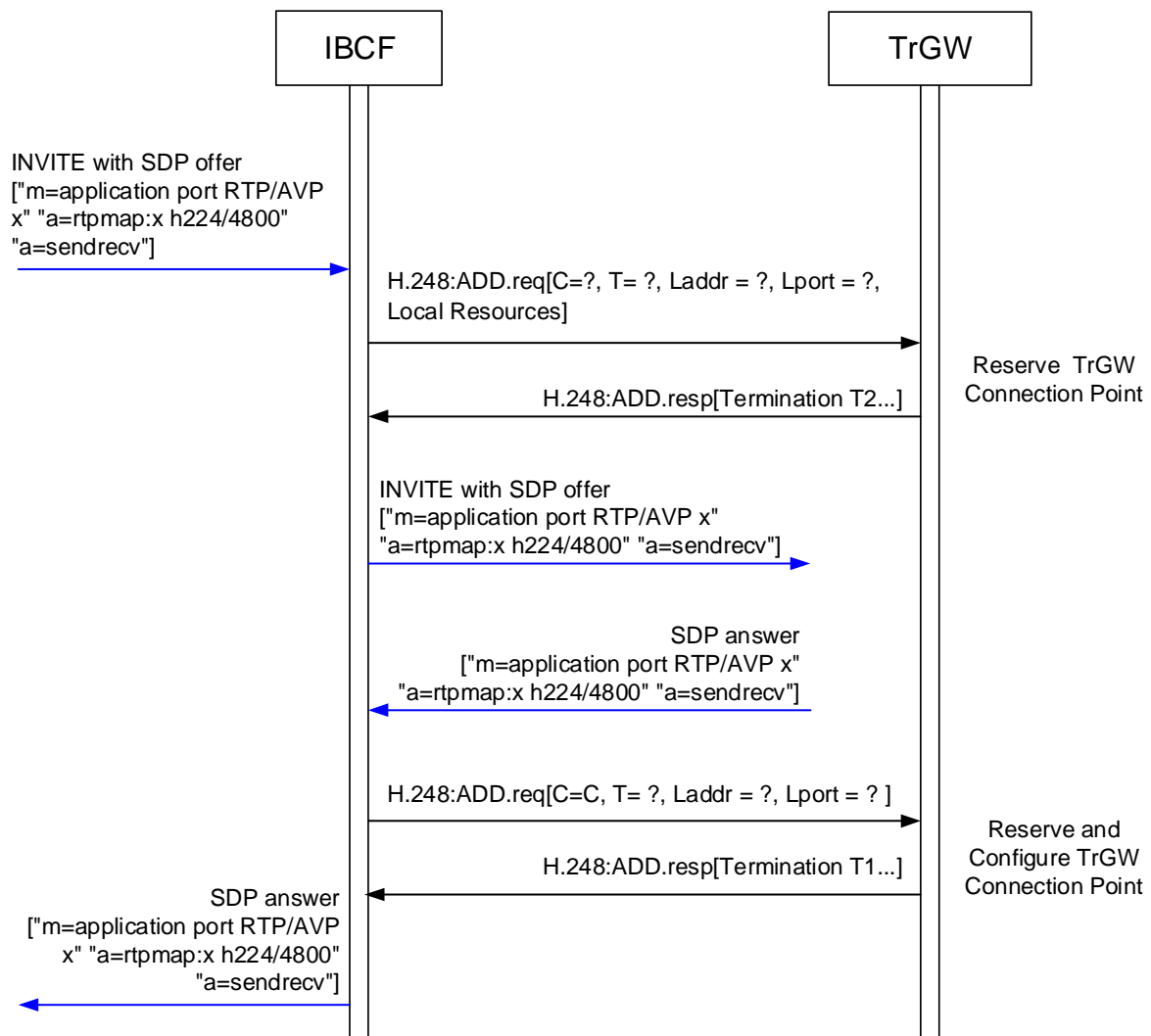
Figure 10.2.23.2.2.1: Procedure to indicate Video ROI using FECC

10.2.23.3 "Predefined ROI" mode

10.2.23.3.1 General

The procedures in subclause 5.22.3 of 3GPP TS 23.334 [43] are applicable.

10.2.23.3.2 Message sequence chart

Figure 10.2.23.3.2.1 shows the message sequence chart example for indicating Predefined ROI mode.
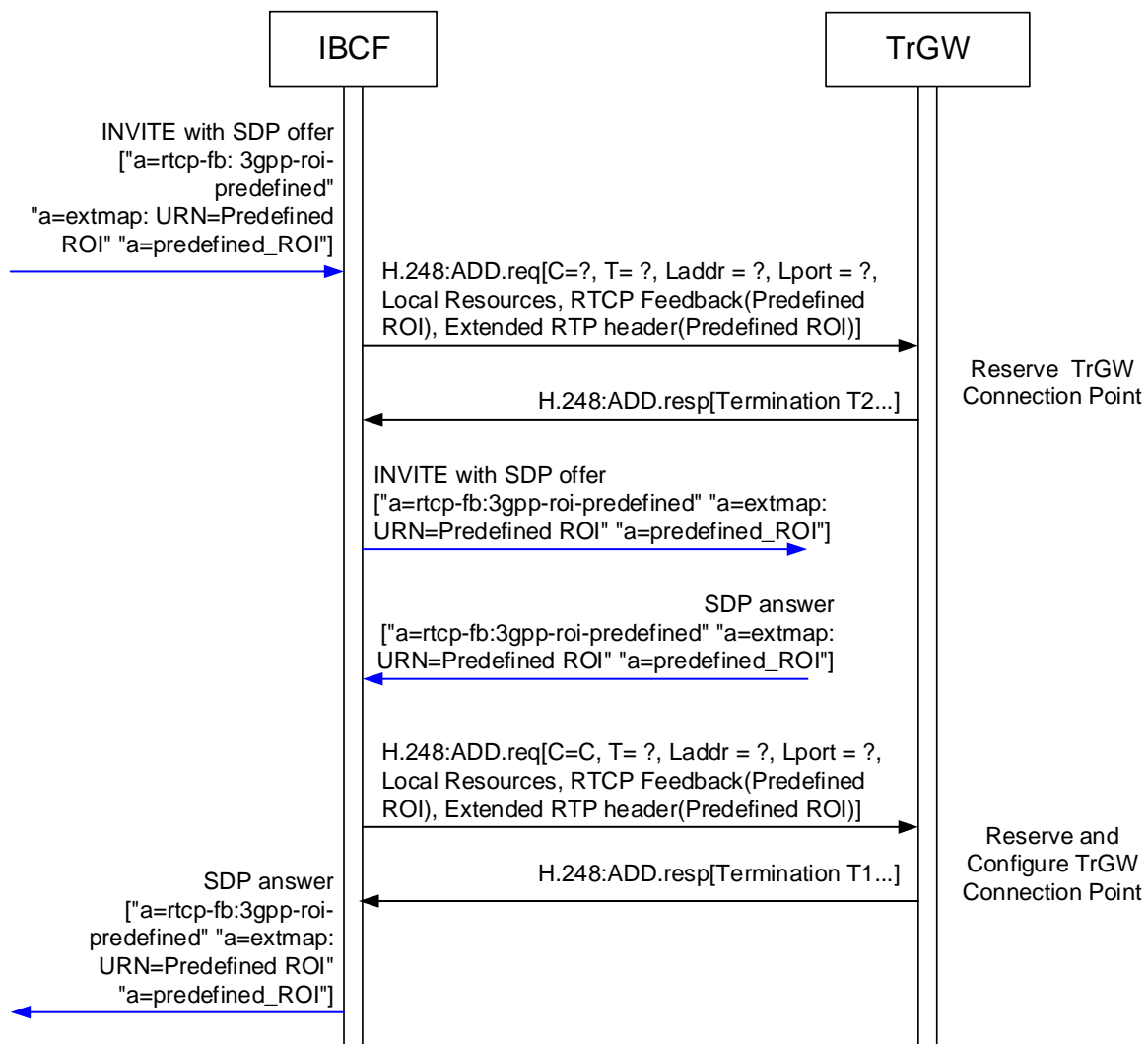
Figure 10.2.23.3.2.1: Procedure to indicate Predefined ROI mode

According to this procedure, the IBCF shall send to the TrGW the information element on the RTCP feedback message capability for "Predefined ROI" type expressed by the parameter "3gpp-roi-predefined" as described in 3GPP TS 26.114 [36], and the RTP Header Extension capability for carriage of predefined ROI information as defined in IETF RFC 5285 [45] and 3GPP TS 26.114 [36]. In addition, the IBCF shall send to the TrGW the media-level SDP predefined ROI attribute "a=predefined_ROI" defined in 3GPP TS 26.114 [36].

10.2.23.4 "Arbitrary ROI" mode

10.2.23.4.1 General

The procedures in subclause 5.22.4 of 3GPP TS 23.334 [43] are applicable.

10.2.23.4.2 Message sequence chart

Figure 10.2.23.4.2.1 shows the message sequence chart example for indicating Arbitrary ROI mode.
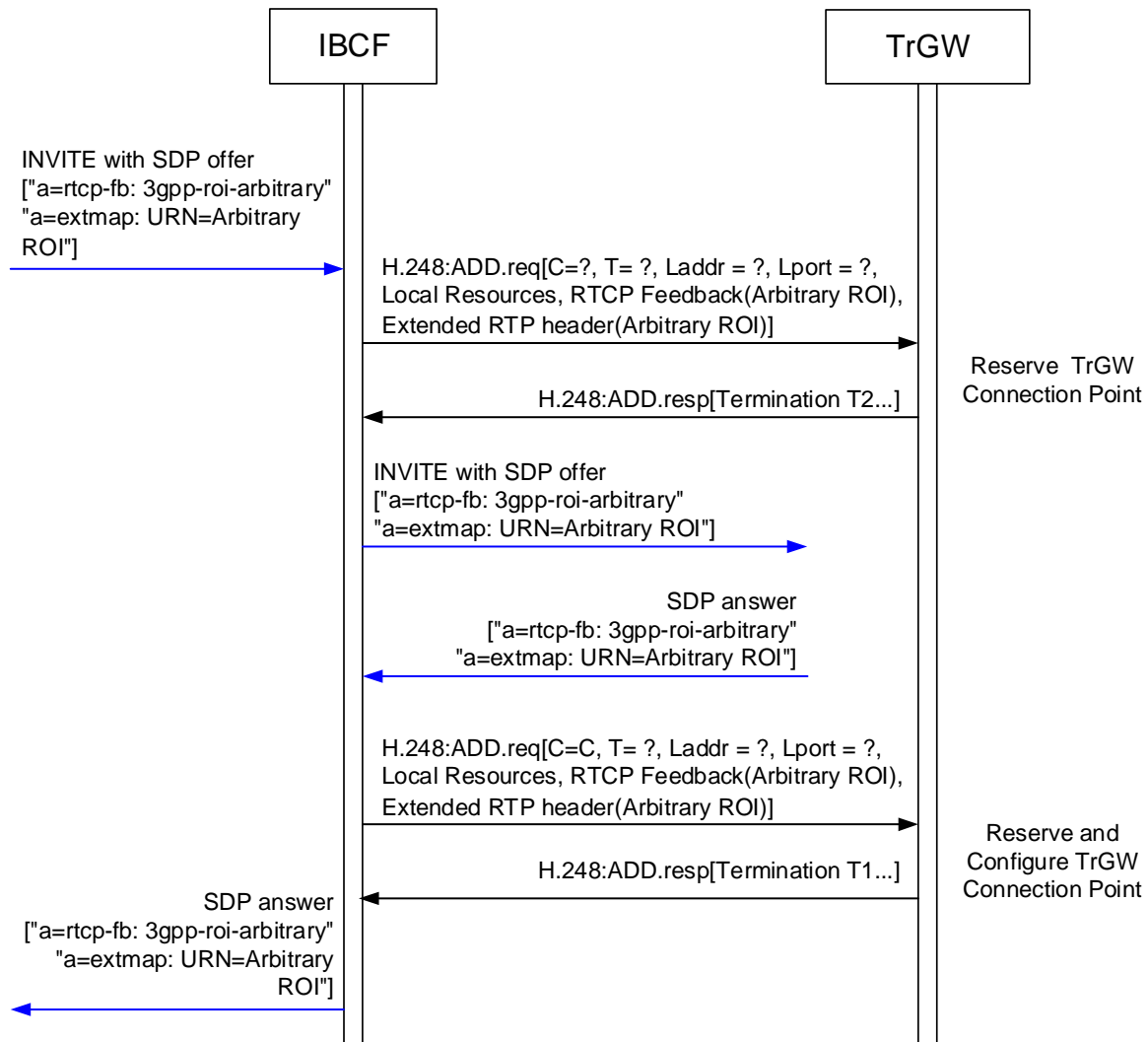
Figure 10.2.23.4.2.1: Procedure to indicate Arbitrary ROI mode

According to this procedure, the IBCF shall send to the TrGW the information element on the RTCP feedback message capability for "Arbitrary ROI" type expressed by the parameter "3gpp-roi-arbitrary" as described in 3GPP TS 26.114 [36], and the RTP Header Extension capability for carriage of arbitrary ROI information as defined in IETF RFC 5285 [45] and 3GPP TS 26.114 [36].

10.2.24 SDP Capability Negotiation (SDPCapNeg)

10.2.24.1 General

The SDP Capability Negotiation (SDPCapNeg) as specified in IETF RFC 5939 [57] is adopted as an optional functionality to negotiate capabilities and the associated configurations according to 3GPP TS 24.229 [1].

Upon receipt of an incoming SDP offer containing the attributes of SDP capability negotiation, e.g. offer AVPF and AVP together for the RTP profile negotiation using the "a=tcap", "a=pcfg" and "a=acfg" attributes, the IBCF shall:

- request the TrGW to reserve resources only for the default configuration without SDPCapNeg, and make the decision on support of the alternative configurations based on the IBCF/TrGW capability as provisioned before forwarding the SDP offer, i.e. handling SDPCapNeg at the controller level; or

- request the TrGW to reserve resources for all of these configurations by signalling SDPCapNeg to the TrGW, and update the SDP offer based on the response from the TrGW before forwarding.

NOTE: The additional benefit of signalling SDPCapNeg between the IBCF and the TrGW is to check the resource availability for the corresponding configurations and to avoid the further session failure in case of inadequate resources for the configuration changes in the final confirmation. However, due to the extra resources reserved only during the call establishment phase, there is increased risk of call establishment failures.

In case the IBCF decides to request the TrGW to reserve resources for all of those configurations, the IBCF shall:

- use legacy SDP attributes as specified in IETF RFC 4566 [53] to do the mapping of actual and potential configurations with the H.248 ReserveGroup concept; or

- use SDP extensions for SDP capability negotiation as specified in IETF RFC 5939 [57], if supported by the TrGW.

Before using SDP extensions for SDP capability negotiation as specified in IETF RFC 5939 [57] towards the TrGW, the IBCF shall perform the necessary checks (i.e. through auditing or via prior provisioning) to ensure that the TrGW supports the syntax and capabilities requested. For an auditing the procedure in subclause 6.1.8.1 is used with the "SDPCapNeg Supported Capabilities" as the object.

When receiving a request from the IBCF with information element "SDPCapNeg configuration" indicating the potential use of multiple configurations, the TrGW shall reserve resources for all of those configurations that it supports and shall send indicate the configurations for which it reserved resources in an "SDPCapNeg configuration" information element in the response. The IBCF shall update the SDP offer with SDPCapNeg configurations in the response from the TrGW and shall forward the SDP offer to the next hop.

The IBCF may also provide SDP configurations to the TrGW with no dependency on the incoming SDP offer, e.g. the IBCF may wildcard the supported configurations in order to construct or update an SDP offer with the addition of alternative configurations via SDPCapNeg attributes.

On receipt of an SDP answer with SDPCapNeg, the IBCF shall request the TrGW to configure the resources for the selected configuration. If the TrGW previously reserved any temporary resources for configurations that were not selected, the IBCF shall also request the TrGW to release those resources.

10.2.24.2   Message sequence chart

10.2.24.2.1   Audit SDPCapNeg Supported Capabilities

The IBCF may request the TrGW to report the current values assigned to distinct objects, here as the "SDPCapNeg Supported Capabilities" in the TrGW. This procedure may be used when the IBCF is unsure of the applicability for SDPCapNeg of the TrGW.

Figure 10.2.24.2.1.1 shows the message sequence chart example for the auditing.
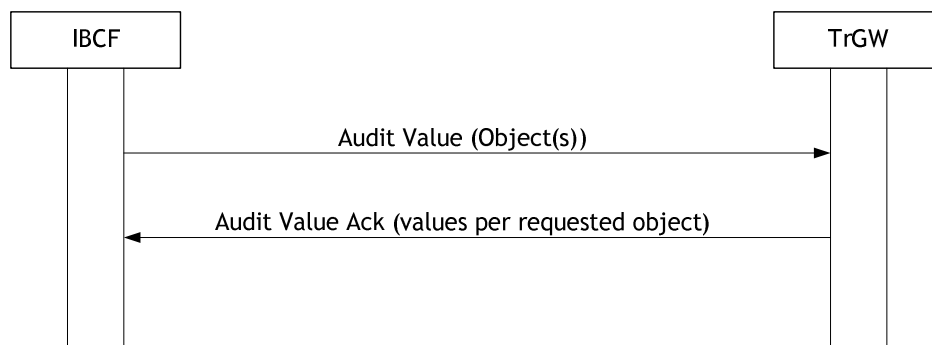
Figure 10.2.24.2.1.1: Audit Value of the TrGW

10.2.25   WebRTC Media Plane Optimization

10.2.25.1   General

The IBCF and the TrGW may support the WebRTC media plane optimization as defined in 3GPP TS 23.228 [8], annex U.2.4, and 3GPP TS 24.229 [1], subclause 6.7.1.5.

The purpose of WebRTC media plane optimization procedures is to convey media between WebRTC clients without bearer level protocol conversion. When both ends are WebRTC IMS clients (WIC), the TrGW remain allocated but media plane interworking is disabled.

The SDP attributes associated with WebRTC media plane optimization procedures "tra-contact", "tra-m-line", "tra-att", "tra-SCTP-association", "tra-media-line-number" and "tra-bw" are defined in 3GPP TS 24.229 [1], subclause 7.5.4.

10.2.25.2   SDP offer handling

If the IBCF receives an SDP offer that contains any "tra-contact" SDP attribute, and the IBCF decides to include a TrGW in the media path, the IBCF shall:

1) reserve resources at the TrGW that are suitable for the media described in the SDP offer outside the "tra-m-line", "tra-att" and "tra-bw" SDP attributes.

2) include the address information as received from the TrGW in that contact line and also encapsulate the address information into each received "tra-contact" attribute, replacing previous information; and

3) transparently pass (in the forwarded SDP offer) all received "tra-m-line", "tra-att", "tra-SCTP-association", "tra-media-line-number" and "tra-bw" SDP attributes.

10.2.25.3   SDP answer handling

If the IBCF receives an SDP answer and the SDP answer includes "tra-m-line" media level SDP attributes, the IBCF shall:

1) configure the TrGW to transparently pass the media described in the received "tra-m-line", "tra-att", "tra-SCTP-association", and "tra-bw" SDP attributes; and

2) transparently pass all received "tra-m-line", "tra-att", "tra-SCTP-association" and "tra-bw" SDP attributes.

NOTE: If interconnected H.248 Stream endpoints or terminations at the TrGW are configured with transport "UDP", they will pass the payload within UDP without modifications, known as UDP transparent forwarding. For WebRTC media plane optimization, the UDP payload will be either DTLS encapsulating SCTP and data channel(s), DTLS-SRTP encapsulating key management information, or SRTP encapsulating audio or video media.

10.2.26   RTP-level pause and resume

The IBCF and the TrGW may support the "RTP-level pause and resume" signalling as defined in 3GPP TS 26.114 [36] and IETF RFC 7728 [59].

If the IBCF and the TrGW support the "RTP-level pause and resume" signalling, they shall apply the requirements and procedures specified in 3GPP TS 23.334 [43] subclause 524 and subclause 6.223.

10.2.27   RTCP Codec Control Commands and Indications

The IBCF and the TrGW may support signalling of "RTCP Codec Control Commands and Indications", as defined in 3GPP TS 26.114 [36] and IETF RFC 5104 [60].

NOTE 1:   3GPP TS 26.114 [36] specifies support of the following RTCP feedback codec control messages (CCM): "Full Intra Request (FIR)", "Temporary Maximum Media Stream Bit Rate Request (TMMBR)" and "Temporary Maximum Media Stream Bit Rate Notification (TMMBN)".

The RTCP feedback FIR message can be used both by point-to-point video calls, and by conference participants supporting Multi-stream Multiparty Conferencing Media Handling feature, as specified in 3GPP TS 26.114 [36] annex S, to request the media sender to send a decoder refresh point.

The RTCP TMMBR and TMMBN feedback messages can also be used in reaction to the Explicit Congestion Notification, as specified in subclause 10.2.13.

Usage of the RTCP feedback "CCM" messages is negotiated via SDP offer/answer exchange through an extension (defined in IETF RFC 5104 [60]) of the RTCP feedback capability attribute "a=rtcp-fb" (defined in IETF RFC 4585 [61]).

NOTE 2: The SDP offer/answer negotiation is performed with a separate "a=rtcp-fb" attribute line for each CCM message type.

If the IBCF and the TrGW support the "RTCP Codec Control Commands and Indications" signalling, they shall apply the requirements and procedures specified in 3GPP TS 23.334 [43] subclause 5.25 and subclause 6.2.24.

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

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.
		Emergency Call Indicator	O	This information element identifies the call as emergency call that requires a preferential handling.
		Priority information	O	This information element requests the TrGW to apply priority treatment for the terminations and bearer connections in the specified context.
		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 theIP 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.
		ECN Enable	O	This information element requests the TrGW to apply ECN procedures
		ECN Initiation Method	C	This information element specifies the ECN Initiation method and requests the TrGW to perform IP header settings as an ECN endpoint, or indicates that ECN bits shall be passed transparently. It may be included only if ECN is enabled.
		Congestion Response Method	C	This information element specifies the ECN Congestion Response Method; receiver driven or sender driven. The default is "received driven congestion control". It may be included only if ECN is enabled and the TrGW acts as ECN endpoint. (NOTE 3)
		ECN ECT Marking	C	This information element specifies the ECN ECT Marking. It may be included only if ECN is enabled and the TrGW acts as ECN endpoint. (NOTE 3)
		ECN Mode	C	This information element specifies the ECN Mode. It may be included only if ECN is enabled and the TrGW acts as ECN endpoint. (NOTE 3)
		RTCP Feedback	C	This information element specifies the RTCP Feedback support. (NOTE 3)

		XR Summary Report	C	This information element specifies the support of XR Summary Reporting.
		Notify ECN Failure Event	C	This information element requests a notification if a ECN failure occurs. It may only be supplied if ECN is enabled and the TrGW acts as ECN endpoint.
		Extended RTP Header for CVO	O	This information element requests the TrGW to pass on the CVO extended RTP header as defined by IETF RFC 5285 [45].
		Generic Image Attributes	O	This information element indicates image attributes (e.g. image size) as defined by IETF RFC 6236 [46].
		ICE password request	O	This information element is present if IBCF requests an ICE password.
		ICE Ufrag request	O	This information element is present if IBCF requests an ICE ufrag.
		ICE host candidate request	O	This information element is present if IBCF requests an ICE host candidate.
		STUN server request	O	This information element is present if IBCF requests the TrGW to answer STUN connectivity checks for ICE.
		Application-aware MSRP interworking request	O	This information element is present if IBCF requests the TrGW to perform application-aware MSRP Interworking.
		Extended RTP Header for Sent ROI	O	This information element requests the TrGW to pass on the ROI extended RTP header for carriage of predefined and/or arbitrary ROI information as defined by IETF RFC 5285 [45] and 3GPP TS 26.114 [36].
		Predefined ROI	O	This information element requests the TrGW to support the RTCP feedback message capability for "Predefined ROI" type expressed by the parameter "3gpp-roi-predefined", as described in 3GPP TS 26.114 [36].
		Arbitrary ROI	O	This information element requests the TrGW to support the RTCP feedback message capability for "Arbitrary ROI" type expressed by the parameter "3gpp-roi-arbitrary", as described in 3GPP TS 26.114 [36].
		SDPCapNeg configuration	O	This information element provides SDPCapNeg configuration(s) using as "a=acap", "a=tcap", "a=pcfg" and "a=acfg" SDP attributes.
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. This information element shall be present if it was contained in the request. If the information element was not contained in the request, it may be present in the reply.
		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.

		ICE password	C	This information element shall be present only if it was contained in the request. It indicates the ICE password assigned by the TrGW.
		ICE Ufrag	C	This information element shall be present only if it was contained in the request. It indicates the ICE Ufrag assigned by the TrGW.
		ICE host candidate	C	This information element shall be present only if it was contained in the request. It indicates the ICE host candidate assigned by the TrGW.
		ICE lite indication	C	This information element shall be present only if an ICE host candidate request was contained in the request, and the IBCF supports ICE lite, but not full ICE. It indicates that the TrGW only supports ICE lite.
		SDPCapNeg configuration	C	This information element shall be present only if it was contained in the request. It provides SDPCapNeg configuration(s) using as "a=acap", "a=tcap", "a=pcfg" and "a=acfg" SDP attributes.
NOTE 1: Remote Source Port and Remote Source Port Range are mutually exclusive.				
NOTE 2: At least one of these information elementsshall be present when policing is required.				
NOTE 3: This parameter does not need to be signalled if support is for 3GPP defined ECN only.				

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.
		Priority information	O	This information element shall be present if the priority information needs to be modified, it may be present otherwise.
		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

ETSI

		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 theIP 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.
		ECN Enable	O	This information element requests the TrGW to apply ECN procedures.
		ECN Initiation Method	C	This information element specifies the ECN Initiation method and requests the TrGW to perform IP header settings as an ECN endpoint, or indicates that ECN bits shall be passed transparently. It may be included only if ECN is enabled.
		Congestion Response Method	C	This information element specifies the ECN Congestion Response Method; receiver driven or sender driven. The default is "received driven congestion control". It may be included only if ECN is enabled and the TrGW acts as ECN endpoint. (NOTE 3)
		ECN ECT Marking	C	This information element specifies the ECN ECT Marking. It may be included only if ECN is enabled and the TrGW acts as ECN endpoint. (NOTE 3)
		ECN Mode	C	This information element specifies the ECN Mode. It may be included only if ECN is enabled and the TrGW acts as ECN endpoint. (NOTE 3)
		RTCP Feedback	C	This information element specifies the RTCP Feedback support. (NOTE 3)
		XR Summary Report	C	This information element specifies the support of XR Summary Reporting.

		Notify ECN Failure Event	C	This information element requests a notification if a ECN failure occurs. It mayonly be supplied if ECN is enabled and the TrGW acts as ECN endpoint.
		Extended RTP Header for CVO	O	This information element requests the TrGW to pass on the CVO extended RTP header as defined by IETF RFC 5285 [45].
		Generic Image Attributes	O	This information element indicates image attributes (e.g. image size) as defined by IETF RFC 6236 [46].
		ICE Connectivity Check	C	This information element requests the TrGW to perform ICE connectivity check as defined by IETF RFC 5245 [50]. It is only applicable for full ICE.
		Notify ICE Connectivity Check Result	C	This information element requests a notification of ICE connectivity check result. It is only applicable for full ICE.
		Notify New Peer Reflexive Candidate	C	This information element requests a notification of new peer reflexive candidate was discovered during a connectivity check. It is only applicable for full ICE.
		Additional ICE Connectivity Check	C	This information element requests the TrGW to perform additional ICE connectivity check as defined by IETF RFC 5245 [50]. It is only applicable for full ICE.
		ICE received candidate	O	This information element is present if IBCF indicates a received candidate for ICE.
		ICE received password	O	This information element is present if IBCF indicates a received password for ICE.
		ICE received Ufrag	O	This information element is present if IBCF indicates a received Ufrag for ICE.
		MSRP Path	O	This information element is present for application-aware MSRP Interworking. It provides the path information that the TrGW shall insert in the MSRP layer "To-Path" Information element.
		Allowed RTCP APP message types	O	This information element is present if the IBCF allows the TrGW to send RTCP APP packets of the indicated types. The TrGW shall not send other RTCP APP packets. If the parameter is not supplied, the TrGW shall not send any RTCP APP packets.
		Extended RTP Header for Sent ROI	O	This information element requests the TrGW to pass on the ROI extended RTP header for carriage of predefined and/or arbitrary ROI information as defined by IETF RFC 5285 [45] and 3GPP TS 26.114 [36].
		Predefined ROI	O	This information requests the TrGW to support the RTCP feedback message capability for "Predefined ROI" type expressed by the parameter "3gpp-roi-predefined", as described in 3GPP TS 26.114 [36].
		Arbitrary ROI	O	This information element requests the TrGW to support the RTCP feedback message capability for "Arbitrary ROI" type expressed by the parameter "3gpp-roi-arbitrary", as described in 3GPP TS 26.114 [36].

		SDPCapNeg configuration	O	This information element provides SDPCapNeg configuration(s) using as "a=acap", "a=tcap", "a=pcfg" and "a=acfg" SDP attributes.
		Additional Bandwidth Properties	O	This information element indicates additional bandwidth properties using "a=bw-info" SDP attribute(s) as defined by 3GPP TS 26.114 [36].
		CCM BASE	O	This information element indicates that the TrGW shall be prepared to receive and is allowed to send, respectively, the RTCP feedback "CCM FIR" and/or "CCM TMMBR" messages (defined in IETF RFC 5104 [60]).
		CCM pause-resume	O	This information element indicates to the TrGW that RTCP feedback "CCM PAUSE-RESUME" messages shall be passed transparently.
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 information elementis 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 information element 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 information elementsshall be present when policing is required.				
NOTE 3: This parameter does not need to be signalled if support is for 3GPP defined ECN only.				

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

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.
		Emergency Call Indicator	O	This information element identifies the call as emergency call that requires a preferential handling.
		Priority information	O	This information element requests the TrGW to apply priority treatment for the terminations and bearer connections in the specified context.
		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	This information element 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 theIP 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.
		ECN Enable	O	This information element requests the TrGW to apply ECN procedures.
		ECN Initiation Method	C	This information element specifies the ECN Initiation method and requests the TrGW to perform IP header settings as an ECN endpoint, or indicates that ECN bits shall be passed transparently. It may be included only if ECN is enabled.
		Congestion Response Method	C	This information element specifies the ECN Congestion Response Method; receiver driven or sender driven. The default is "received driven congestion control". It may be included only if ECN is enabled and the TrGW acts as ECN endpoint. (NOTE 3)
		ECN ECT Marking	C	This information element specifies the ECN ECT Marking. It may be included only if ECN is enabled and the TrGW acts as ECN endpoint. (NOTE 3)

		ECN Mode	C	This information element specifies the ECN Mode. It may be included only if ECN is enabled and the TrGW acts as ECN endpoint. (NOTE 3)
		RTCP Feedback	C	This information element specifies the RTCP Feedback support. (NOTE 3)
		XR Summary Report	C	This information element specifies the support of XR Summary Reporting.
		Notify ECN FailureEvent	C	This information element requests a notification if a ECN failure occurs due to ECN. It mayonly be supplied if ECN is enabled and the TrGW acts as ECN endpoint.
		Extended RTP Header for CVO	O	This information element requests the TrGW to pass on the CVO extended RTP header as defined by IETF RFC 5285 [45].
		Generic Image Attributes	O	This information element indicates image attributes (e.g. image size) as defined by IETF RFC 6236 [46].
		STUN server request	O	This information element is present if IBCF requests the TrGW to answer STUN connectivity checks for ICE.
		ICE Connectivity Check	C	This information element requests the TrGW to perform ICE connectivity check as defined by IETF RFC 5245 [50]. It is only applicable for full ICE.
		Notify ICE Connectivity Check Result	C	This information element requests a notification of ICE connectivity check result. It is only applicable for full ICE.
		Notify New Peer Reflexive Candidate	C	This information element requests a notification of new peer reflexive candidate was discovered during a connectivity check. It is only applicable for full ICE.
		ICE password request	O	This information element is present if IBCF requests an ICE password.
		ICE Ufrag request	O	This information element is present if IBCF requests an ICE ufrag.
		ICE host candidate request	O	This information element is present if IBCF requests an ICE host candidate.
		ICE received candidate	O	This information element is present if IBCF indicates a received candidate for ICE.
		ICE received password	O	This information element is present if IBCF indicates a received password for ICE.
		ICE received Ufrag	O	This information element is present if IBCF indicates a received Ufrag for ICE.
		MSRP Path	O	This information element is present for application-aware MSRP Interworking. It provides the path information that the TrGW shall insert in the MSRP layer "To-Path" Information element.
		Application-aware MSRP interworking request	O	This information element is present if IBCF requests the TrGW to perform application-aware MSRP Interworking.
		Allowed RTCP APP message types	O	This information element is present if the IBCF allows the TrGW to send RTCP APP packets of the indicated types. The TrGW shall not send other RTCP APP packets. If the parameter is not supplied, the TrGW shall not send any RTCP APP packets.
		Extended RTP Header for Sent ROI	O	This information element requests the TrGW to pass on the ROI extended RTP header for carriage of predefined and/or arbitrary ROI information as defined by IETF RFC 5285 [45] and 3GPP TS 26.114 [36].

		Predefined ROI	O	This information element requests the TrGW to support the RTCP feedback message capability for "Predefined ROI" type expressed by the parameter "3gpp-roi-predefined", as described in 3GPP TS 26.114 [36].
		Arbitrary ROI	O	This information element requests the TrGW to support the RTCP feedback message capability for "Arbitrary ROI" type expressed by the parameter "3gpp-roi-arbitrary", as described in 3GPP TS 26.114 [36].
		SDPCapNeg configuration	O	This information element provides SDPCapNeg configuration(s) using as "a=acap", "a=tcap", "a=pcfg" and "a=acfg" SDP attributes.
		Additional Bandwidth Properties	O	This information element indicates additional bandwidth properties using "a=bw-info" SDP attribute(s) as defined by 3GPP TS 26.114 [36].
		CCM BASE	O	This information element indicates that the TrGW shall be prepared to receive and is allowed to send, respectively, the RTCP feedback "CCM FIR" and/or "CCM TMMBR" messages (defined in IETF RFC 5104 [60]).
		CCM pause-resume	O	This information element indicates to the TrGW that RTCP feedback "CCM PAUSE-RESUME" messages shall be passed transparently.
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. This information element shall be present if it was contained in the request. If the information element was not contained in the request, it may be present in the reply.
		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.
		ICE password	C	This information element shall be present only if it was contained in the request. It indicates the ICE password assigned by the TrGW.
		ICE Ufrag	C	This information element shall be present only if it was contained in the request. It indicates the ICE Ufrag assigned by the TrGW.
		ICE host candidate	C	This information element shall be present only if it was contained in the request. It indicates the ICE host candidate assigned by the TrGW.
		ICE lite indication	C	This information element shall be present only if an ICE host candidate request was contained in the request, and the TrGW supports ICE lite, but not full ICE. It indicates that the TrGW only supports ICE lite.

		SDPCapNeg configuration	C	This information element shall be present only if it was contained in the request. It provides SDPCapNeg configuration(s) using as "a=acap", "a=tcap", "a=pcfg" and "a=acfg" SDP attributes.
NOTE 1: Remote Source Port and Remote Source Port Range are mutually exclusive.				
NOTE 2: At least one of these information elements shall be present when policing is required.				
NOTE 3: This parameter does not need to be signalled if support is for 3GPP defined ECN only.				

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.

NOTE: No requirement for statistics in the Release TrGW Termination Ack has been 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.

10.4.1.8 Change Through-Connection

This procedure is used to change the Through-connection in the bearer termination.

Table 10.4.1.8.1: Change Through-Connection

Procedure	Initiated	Information element name	Information element required	Information element description
Change Through-Connection	IBCF	Context/Context Request	M	This information element indicates the existing context or requests a new context for the bearer termination.
		Bearer Termination/Bearer Termination Request	M	This information element indicates the existing bearer termination or requests a new Bearer termination where the through connection is changed.
		Through-Connection	M	This information element indicates the through-connection of the bearer termination.
Change Through-Connection Ack	TrGW	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.

NOTE: This procedure may be combined with Reserve and Configure TrGW Connection Point, Reserve TrGW Connection Point or Configure TrGW Connection Point procedure. This list of procedures is not exhaustive.

10.4.1.9 ECN Failure Indication

This procedure is used to report ECN related failures (see clause 10.2.13.3a).

Table 10.4.1.9.1: Procedures toward the IM Subsystem: ECN Failure Indication

Procedure	Initiated	Information element name	Information element required	Information element description
ECN Error 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 ECN failure is reported.
		ECN Error Indication	M	This information element indicates an ECN failure event.
ECN Error 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.

10.4.1.10   Change Flow Direction

This procedure may be used to change the flow direction between bearer terminations within a context for access transfer procedures (see subclause 10.2.15).

Table 10.4.1.10.1: Procedures toward the IM Subsystem: Change Flow Direction

Procedure	Initiated	Information element name	Information element required	Information element description
Change Flow Direction	IBCF(ATCF)	Context/Context Request	M	This information element indicates the existing context or a new context where the flow direction is changed.
		Bearer Termination 1/ Bearer Termination 1 Request	M	This information element indicates the existing bearer termination or a new bearer termination from where the new flow direction is applied.
		Bearer Termination 2/ Bearer Termination 2 Request	M	This information element indicates the existing bearer termination or a new bearer termination where to the new flow direction is applied.
		Flow Direction	M	This information element indicates the flow direction from the bearer termination 1 to bearer termination 2 within the context.
Change Flow Direction Ack	TrGW(ATGW)	Context	M	This information element indicates the context where the command was executed.

10.4.1.11   ICE Connectivity Check Result Notification

This procedure is used to report ICE connectivity check result for Full ICE.

Table 10.4.1.11.1: Procedures toward the IM Subsystem: ICE Connectivity Check Result Notification

Procedure	Initiated	Information element name	Information element required	Information element description
ICE Connectivity Check Result Notification	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 ICE Connectivity Check Result is reported.
		ICE Connectivity Check Result Indication	M	This information element indicates an ICE Connectivity Check Result event.
ICE Connectivity Check Result Notification 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.

10.4.1.12 ICE New Peer Reflexive Candidate Notification

This procedure is used to report ICE New Peer Reflexive Candidate for Full ICE.

Table 10.4.1.12.1: Procedures toward the IM Subsystem: ICE New Peer Reflexive Candidate Notification

Procedure	Initiated	Information element name	Information element required	Information element description
ICE New Peer Reflexive Candidate Notification	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 ICE New Peer Reflexive Candidate is reported.
		ICE New Peer Reflexive Candidate Indication	M	This information element indicates an ICE New Peer Reflexive Candidate event.
ICE New Peer Reflexive Candidate Notification 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	The "Audit Value" procedure may be used to determine the support of SDPCapNeg in response to non-call-related H.248 commands.
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):
Void.

Annex B (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
06-2015	CT-68	CP-150351	0139	-		Bearer Termination in Acknowledgements	12.6.0	12.7.0
09-2015	CT-69	CP-150483	0141	2	B	Support for Video Enhancements by Region-of-Interest Information Signalling	12.7.0	13.0.0
12-2015	CT-70	CP-150667	0142	11	B	Support of SDP capability negotiation	13.0.0	13.1.0
12-2015	CT-70	CP-150665	0144	4	B	Support for Video Enhancements by Region-of-Interest Information Signalling	13.0.0	13.1.0

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New**
03-2016	CT#71	CP-160105	0149	-	F	Bandwidth adjustment for EVS codec	13.2.0
03-2016	CT#71	CP-160102	0150	2	B	Support of enhanced bandwidth negotiation mechanism for MTSI sessions	13.2.0
03-2016	CT#71	CP-160105	0151	-	F	Removal of references to TS 26.235	13.2.0
03-2016	CT#71	CP-160097	0152	4	B	WebRTC media plane optimization procedure	13.2.0
06-2016	CT#72	CP-160269	0153	-	F	Clarifications related to the enhanced bandwidth negotiation mechanism	13.3.0
09-2016	CT#73	CP-160451	0154	3	B	Clarification of the gate control procedure between SIP and H.248 for early media over Ix interface	14.0.0
12-2016	CT#74	CP-160625	0155	1	B	Support of RTP-level pause and resume functionality	14.1.0
03-2017	CT#75	CP-170082	0156	-	F	Correcting references for "RTP-level pause and resume" signalling	14.2.0
03-2017	CT#75	CP-170082	0157	1	B	RTCP Codec Control Commands and Indications	14.2.0
09-2018	CT#81					Automatic upgrade to Rel-15	15.0.0

History

Document history		
V15.0.0	November 2018	Publication