ETSI TS 123 334 V12.5.0 (2014-10)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
IP Multimedia Subsystem (IMS)
Application Level Gateway (IMS-ALG)
- IMS Access Gateway (IMS-AGW)
interface: Procedures descriptions
(3GPP TS 23.334 version 12.5.0 Release 12)

Reference

RTS/TSGC-0423334vc50

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

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

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Intellectual Property Rights

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

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**", "**may not**", "**need**", "**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

Annex G of 3GPP TS 23.228 [2] gives out an IMS Application Level Gateway (IMS-ALG) and IMS Access Media Gateway (IMS-AGW) based reference model to support NAPT-PT, gate control and traffic policing between IP-CAN and IMS domain.

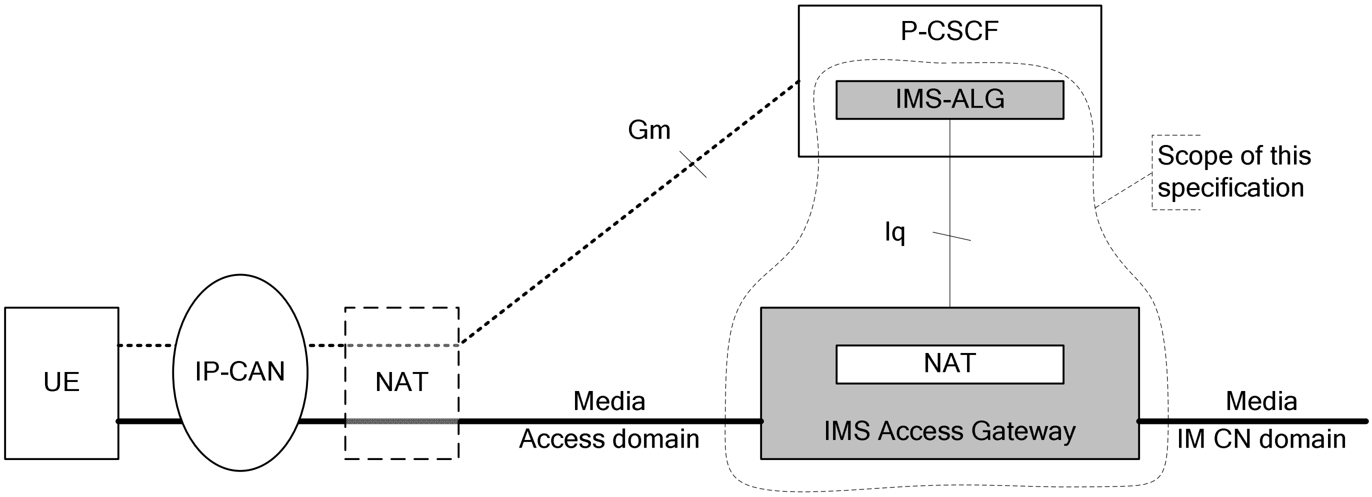


Figure 1.1: Scope of the specification

Figure 1.1 illustrates the reference model for Iq:

- the dashed line represents the IP signalling-path with SIP (at Gm) as call/session control protocol between the UE and the P-CSCF (IMS-ALG);
- the bold, horizontal line represents the IP media-path (also known as (IP) bearer-path or (IP) data-path; the notion 'media' is used as generic term for "IP application data"); and
- the vertical line represents the Iq control-path with H.248 as gateway/policy control protocol between the IMS-ALG and the IMS-AGW (H.248 messages are transported over IP).

The Iq reference point is between the P-CSCF (IMS-ALG) and the IMS-AGW. It conveys the necessary information that is needed to allocate, modify and release (IP) transport addresses.

The present document defines the stage 2 description for the Iq reference point. The stage 2 shall cover the information flow between the P-CSCF (IMS-ALG) and IMS-AGW. The protocol used over the Iq interface is the gateway control protocol according ITU-T Recommendation H.248 (which is specified for Iq by an H.248 profile according 3GPP TS 29.334 [3]).

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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS), stage 2".

[3] 3GPP TS 29.334: "IMS Application Level Gateway (IMS-ALG) – IMS Access Gateway (IMS-AGW) Iq interface, stage 3".

[4] IETF RFC 2663: "IP Network Address Translator (NAT) Terminology and Considerations".

[5] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[6] IETF RFC 3556: "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[7] IETF RFC 3605: "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)".

[8] 3GPP TS 23.205: "Bearer independent circuit-switched core network; Stage 2".

[9] ITU-T Recommendation H.248.1 (05/2002): "Gateway Control Protocol: Version 2" including the Corrigendum1 for Version 2 (03/04).

[10] IETF RFC 2216: "Network Element Service Template".

[11] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP".

[12] 3GPP TS 33.328: "IMS Media Plane Security".

[13] IETF RFC 4568: "Session Description Protocol (SDP) Security Descriptions for Media Streams".

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

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

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

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

[18] 3GPP TS 23.237: "IP Multimedia subsystem (IMS) Service Continuity; Stage 2".

[19] 3GPP TS 24.237: "IP Multimedia subsystem (IMS) Service Continuity; Stage 3".

[20] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[21] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[22] 3GPP TS 22.153: "Multimedia Priority Service".

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

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

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

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

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

[28] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[29] IETF RFC 793: "Transmission Control Protocol – DARPA Internet Program – Protocol Specification".

[30] IETF RFC 4145: "TCP-Based Media Transport in the Session Description Protocol (SDP)".

[31] IETF RFC 4582: "The Binary Floor Control Protocol (BFCP)".

[32] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[33] IETF draft-ietf-mmusic-udptl-dtls-10: "UDP Transport Layer (UDPTL) over Datagram Transport Layer Security (DTLS)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[34] IETF draft-schwarz-mmusic-sdp-for-gw-02: "SDP codepoints for gateway control".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[35] GSM Association RCC.07: "Rich Communication Suite 5.1 Advanced Communications Services and Client Specification, Version 2.0, 03 May 2013".

[36] GSM Association RCC.07: "Rich Communication Suite 5.1 Advanced Communications Services and Client Specification, Version 3.0, 25 September 2013".

[37] IETF RFC 4572: "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)".

[38] ITU-T Recommendation H.248.84 (07/2012): "Gateway control protocol: NAT-traversal for peer-to-peer services".

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

[40] IETF RFC 5389: "Session Traversal Utilities for NAT (STUN)".

[41] IETF RFC 5766: "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)".

[42] IETF RFC 5763: "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)".

[43] IETF RFC 5764: "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)".

[44] 3GPP TS 24.371: "Web Real-Time Communications (WebRTC) client access to the IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[45] IETF RFC 6135: "An Alternative Connection Model for the Message Session Relay Protocol (MSRP)".

[46] OMA-TS-CPM_Conversation_Function-V2_0-20130926-D: "CPM Conversation Functions".

Editor´s Notes: Spec is not yet public. Reference to be updated once OMA makes new version public.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

End-to-access edge security: media protection extending between an IMS UE and the first IMS core network node in the media path without being terminated by any intermediary node.

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

Full ICE: The full implementation of the Interactive Connectivity Establishment (ICE) specified in IETF RFC 5245 [39].

ICE lite: The lite implementation of the Interactive Connectivity Establishment (ICE) specified in IETF RFC 5245 [39].

Local (near-end) NAPT control: the operation of providing network address mapping information and NAPT policy rules to a near-end NAT in the media flow.

NAT-PT/NAPT-PT: see definition in 3GPP TS 23.228 [2].

NAPT control and NAT traversal: controls network address translation for both near-end NA(P)T and far-end NA(P)T

Network Address Translation (NA(P)T): see definition in 3GPP TS 23.228 [2].

Remote (far-end) NAT traversal: the operation of adapting the IP addresses so that the packets in the media flow can pass through a far-end (remote) NAT.

TLS-client: the entity that initiates a TLS session establishment to a server (see IETF RFC 5246 [28]).

TLS-server: the entity that responds to requests for TLS session establishment from clients (see IETF RFC 5246 [28]).

TLS endpoint: either a TLS-client or a TLS-server.

Convention:

Wherever the **term NAT** is used in this specification, it may be replaced by **NA(P)T or NA(P)T-PT.**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.237 [18] apply:

Access Leg
Access Transfer Control Function (ATCF)
Access Transfer Gateway (ATGW)
Remote Leg
Target Access Leg
Source Access Leg

3.2 Symbols

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

Iq	Interface between the IMS Application Level Gateway and the IMS Access Media Gateway

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

ATCF	Access Transfer Control Function
ATGW	Access Transfer Gateway
BFCP	Binary Floor Control Protocol
CVO	Coordination of Video Orientation
DTLS	Datagram Transport Layer Security
e2ae security	End-to-access-edge security
e2e security	End-to-end security
ECN	Explicit Congestion Notification
ECN-CE	ECN Congestion Experienced
eIMS-AGW	IMS Access Gateway enhanced for WebRTC
eP-CSCF	P-CSCF enhanced for WebRTC
ICE	Interactive Connectivity Establishment
IMS-AGW	IMS Access Media Gateway
IMS-ALG	IMS Application Level Gateway
IM CN	IMS Core Network
MSRP	Message Session Relay Protocol

NA(P)T	Network Address and optional Port Translation
NAPT	Network Address Port Translation
NAT	Network Address Translation
NA(P)T-PT	NAT Address (and optional Port-) Translation and Protocol Translation
P-CSCF	Proxy-CSCF
SRTP	Secure Real-time Transport Protocol
SRVCC	Single Radio Voice Call Continuity
STUN	Session Traversal Utilities for NAT
TLS	Transport Layer Security
TURN	Traversal Using Relay NAT
UDPTL	User Datagram Protocol Transport Layer
URN	Uniform Resource Name
WebRTC	Web Real Time Communication
WIC	WebRTC IMS Client
WWSF	WebRTC Web Server Function

4 Architecture

4.1 Reference architecture

The reference architecture for the IMS-ALG and the IMS-AGW when NAT is invoked between the UE and the IMS domain is shown in figure 4.1.1 below.

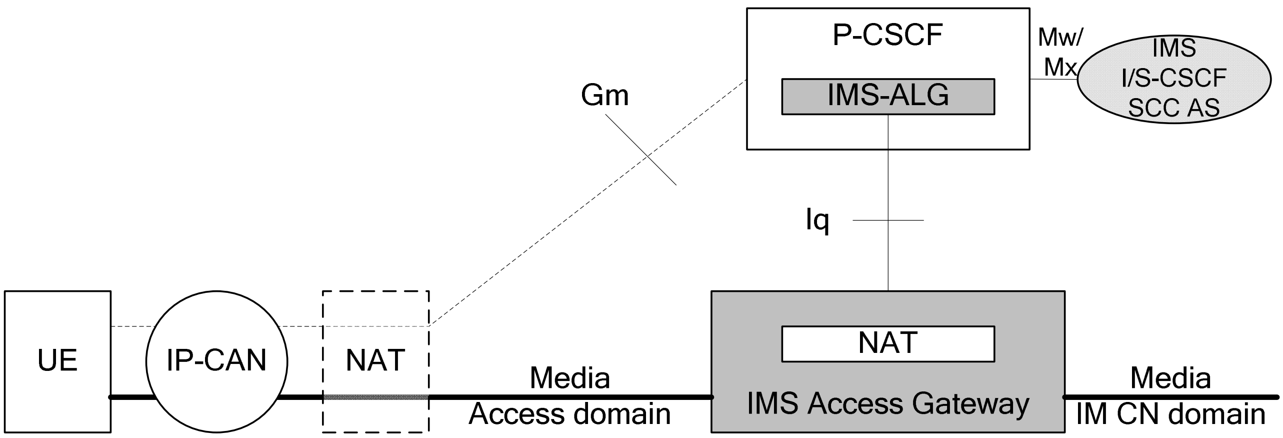


Figure 4.1.1: Reference Architecture with NAT invoked between the UE and the IMS domain

See 3GPP TS 23.228 [2] Annexes G.1 and G.2 for a comprehensive description of the reference models.

The reference architecture for the IMS-ALG and the IMS-AGW supporting the ATCF/ATGW function is shown in figure 4.1.2 below.

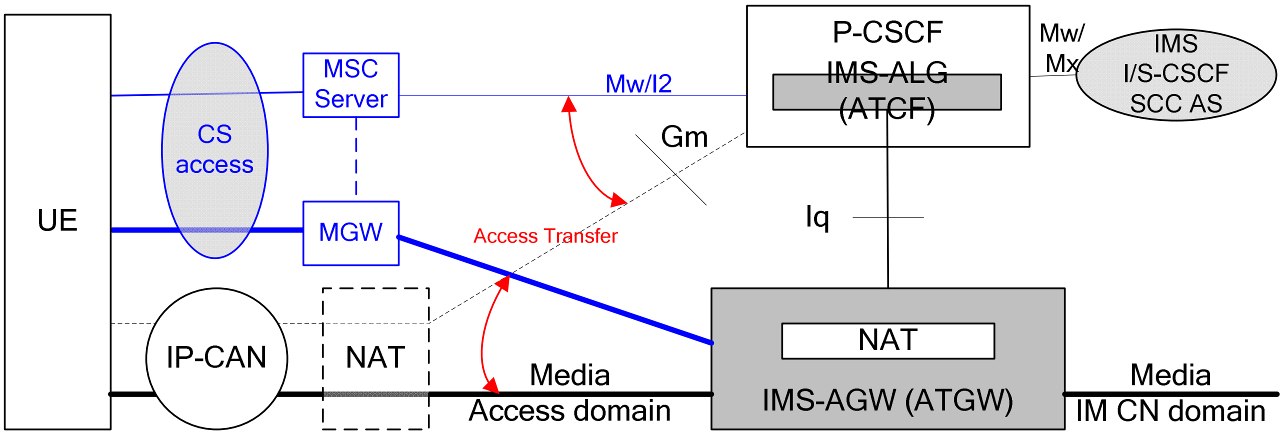
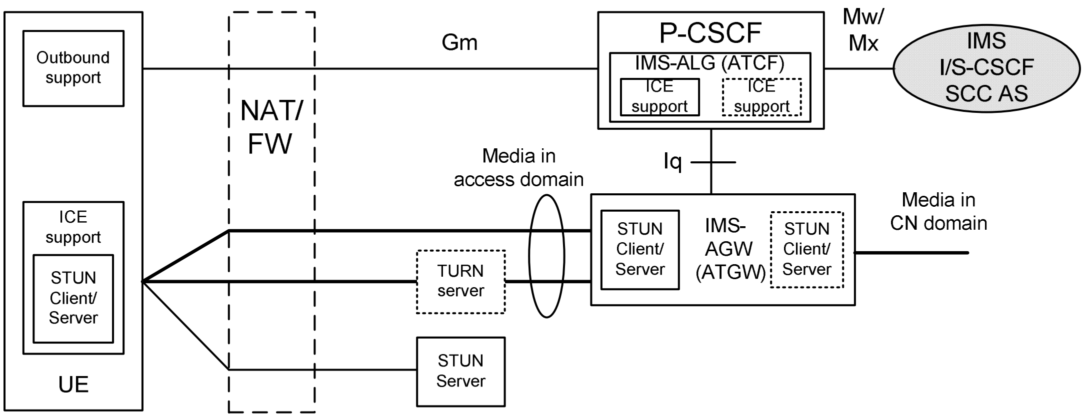


Figure 4.1.2: Reference Architecture for IMS-ALG/IMS-AGW with ATCF/ATGW function

See 3GPP TS 23.237 [18] subclause 5.2 for a comprehensive description of the reference model.

The reference architecture for the IMS-ALG and IMS-AGW supporting Interactive Connectivity Establishment (ICE) is shown in figure 4.1.3, for the case when both the signalling and media traverses NAT devices. There might be an ICE process towards access network domain and/or an ICE process towards core network domain. Both ICE processes are independent of each other. The network entities that support Session Traversal Utilities for NAT (STUN) and Traversal Using Relays NAT (TURN) are described in IETF RFC 5389 [40] and IETF RFC 5766 [41] respectively.



NOTE 1: If the IMS-AGW only supports ICE lite, it will only contain a STUN server.

NOTE 2: The IMS-AGW and IMS-ALG may support ICE only towards the served UE, and will then only contain a STUN client/server and ICE support on related terminations.

NOTE 3: The TURN server is a deployment option but not required for all ICE deployments.

NOTE 4: The separate STUN server is used by the served UE while it gathers ICE candidates. The STUN server in the IMS-AGW is used to answer ICE connectivity checks.

Figure 4.1.3: Reference architecture for ICE

The reference architecture for the P-CSCF enhanced for WebRTC (eP-CSCF) and the IMS-AGW enhanced for WebRTC (eIMS-AGW) to support WebRTC client access to IMS is shown in figure 4.1.4 as below, see Annex U in 3GPP TS 23.228 [2] for a comprehensive description of the reference model.

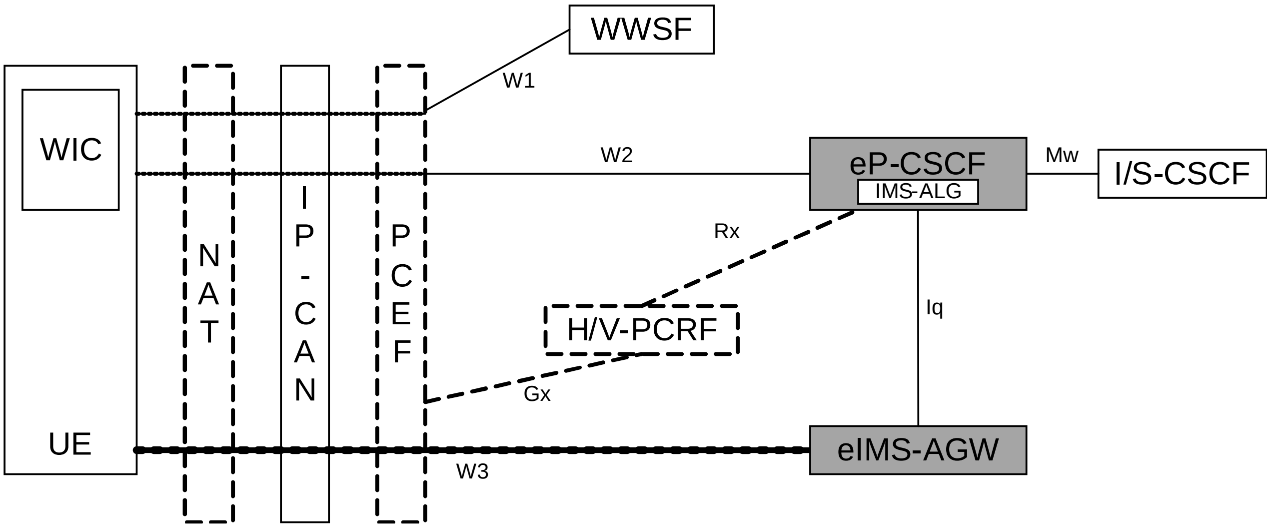


Figure 4.1.4: Reference Architecture for eP-CSCF/eIMS-AGW supporting WebRTC access to IMS

4.2 NAT Function

An operator may need NAT function between UE and IMS domain. Such function can be provided by the IMS-AGW and can be called local (near-end) NAT or IM CN hosted NAT (see subclause 5.2). There can also be an independent NAT device between UE and IMS domain (see subclause 5.4), referred as remote (far end) NAT. Thus the IMS-AGW shall support remote NA(P)T traversal.

Figure 4.1.1 illustrates the particular IP media-path scenario with both a remote NAT and local NAT function. Each NAT function is partitioning an IP domain into two address domains, or partitioning the used IP address space (realm) into two realms.

The reference architecture of Figure 4.1.1 may be mapped on various network scenarios, like e.g. to three IPv4 realms, indicated by a) IP-CAN (connectivity access network), b) (Media) Access Domain and c) (Media) IM CN domain. If there would not be any remote NAT device between the UE and IMS-AGW, then there would be just two IP domains (a and c).

The two types of NATs are also typically different from control perspective: local (near-end) NAT can be controlled by the operators directly, and remote (far-end) NAT that cannot be controlled by the operators directly.

The support of local NAT is thus implicitly leading to the requirement for IP realm indication at Iq (see subclause 5.3).

The edge node of the IP-CAN may be a remote (far-end) NAT device (see Figure 4.1.1). This NAT device provides NAT or NAPT or NA(P)T-PT for IP traffic in the media-path and signalling path (e.g. IP network addresses and possibly L4 transport port values may be translated of SIP Gm messages).

The remote NAT device cannot be directly controlled by the operators of the (Media) Access and IP CN domain. The IMS-ALG is consequently lacking the direct information with regards to the applied NAT bindings by the remote NAT device.

4.3 ATCF/ATGW Function

The ATCF/ATGW functions may be supported by the IMS-ALG/IMS-AGW when SRVCC enhanced with ATCF is used. In this case, the Iq reference point is used for IMS sessions that the IMS-ALG (ATCF) decides to anchor at the IMS-AGW (ATGW) to provide the following functions:

- reservation and configuration of IMS-AGW (ATGW) resources for media anchoring during PS session origination or termination;
- reconfiguration of IMS-AGW (ATGW) resources during access transfer to the CS domain;
- release of IMS-AGW (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;
- Indication of IP realm during allocation of transport addresses/resources (the PS and CS accesses may be reachable via different IP realms);
- the ability to configure ECN properties towards the transferred to Access if ECN is supported/requested;
- the ability to reconfigure the ECN mode e.g. from ECN transparent to ECN endpoint towards the IMS CN if ECN transparent cannot be maintained after access transfer to the CS domain;
- provide priority treatment to calls identified as Multimedia Priority Service (see 3GPP TS 22.153 [22]).

See 3GPP TS 23.237 [18] and 3GPP TS 24.237 [19] for a comprehensive description of the ATCF and ATGW functions.

4.4 ePCSCF/eIMS-AGW Function

The Iq reference point is used between the P-CSCF enhanced for WebRTC (eP-CSCF) and the IMS-AGW enhanced for WebRTC (eIMS-AGW), with the following additional functions:

- media plane interworking extensions as needed for WICs;
- media security of type "e2ae" (as specified in 3GPP TS 33.328 [12]) for media protocols specific to WebRTC, including media consent, and DTLS-SRTP as key exchange mechanism for media components using SRTP;
- NAT traversal support including ICE;
- the ability to perform any transcoding needed for audio and video codecs supported by the browser; and
- transport level interworking between DataChannels and other transport options supported by IMS.

See 3GPP TS 23.228 [2] Annex U for a comprehensive description of the eP-CSCF and eIMS-AGW functions.

5 Functional Requirements

5.1 General

A single IMS-ALG may control one or multiple IMS-AGW(s).

5.2 Gate Control & Local NAT

The IMS-ALG shall provide the NAPT control function, i.e. obtain the address binding information (according to IETF RFC 2663 [4]) and perform the NAPT policy control along with gate control (i.e. instruct the opening/closing of a gate).

The IMS-ALG shall request the IMS-AGW to allocate transport addresses/resources to enable media to traverse the IMS-AGW. The IMS-ALG may indicate the corresponding IP realm to the IMS-AGW – see subclause 5.3. The IMS-AGW shall provide the corresponding external transport addresses to the IMS-ALG.

Terminations for the Iq interface may be pre-defined with different levels of granularity for specific IP ports, interfaces, or groups of interfaces. These may then be defined as an IP realm (see subclause 5.3) known by both the IMS-ALG and the IMS-AGW, however IP Realms may also be defined for multiple physical interfaces. In order to efficiently report a failure affecting a large number of terminations associated to specific physical interfaces, the IMS-AGW shall, when allocating a new termination, return to the IMS-ALG an associated Interface ID.

An IMS-AGW not supporting this procedure may allocate the same Interface ID for all IP terminations.

An IMS-AGW supporting the Termination Out-of-Service procedure (see subclause 6.1.15) shall maintain a local mapping of Interface ID to its internal resources.

The IMS-AGW shall provide the NAPT enforcement function, i.e. change the address and port number of the media packets as they traverse the IMS-AGW, along with gate control (i.e. open/close a gate under the control of the IMS-ALG).

The IMS-AGW may provide IP version inter-working.

The IMS-ALG shall request the IMS-AGW to release its transport resources at the end of a session.

5.3 IP realm indication and availability

The IMS-ALG and the IMS-AGW shall support IP realm indication.

The IMS-ALG, when requesting the allocation of transport resources at the IMS-AGW, may indicate the correspondent IP realm to the IMS-AGW. The IMS-AGW 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 cannot be changed after the initial assignment.

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

In order to prevent the IMS-ALG requesting an unavailable IP Realm, the IMS-ALG may audit the list of currently available realms on the IMS-AGW and may request the IMS-AGW to report any changes to that list as they occur over time.

The monitoring of IP realm availability is optional and if supported by IMS-AGW may be requested by the IMS-ALG.

5.4 Remote NAT traversal support

The IMS-ALG and the IMS-AGW shall support remote NA(P)T traversal support using procedures according to the present subclause. In addition they may support remote NA(P)T traversal support using Interactive Connectivity Establishment (ICE) according to subclause 5.17.

The IMS-ALG is responsible for determining whether there is a remote NAT device (the mechanism by which this achieved is out of scope of the current document).

If a remote NAT device is present, the IMS-ALG shall request the IMS-AGW to perform latching or re-latching when requesting the IMS-AGW to reserve transport addresses/resources.

If remote NAT is applicable, the IMS-AGW shall not use the remote media address/port information (supplied by the IMS-ALG) as the destination address for outgoing media. Instead, the IMS-AGW shall dynamically learn the required destination address via the source address/port of incoming media. This mechanism is known as "latching".

When remote NAT Traversal is applied to a stream associated with multiple flows (e.g. RTP and RTCP), the IMS-AGW shall perform individual latching and/or re-latching on the various flows. This means that an RTP and an RTCP flow of a single stream can be latched to different remote addresses and/or ports.

5.5 Remote Source Address/Port Filtering

The IMS-ALG may support and the IMS-AGW shall support policing of the remote source address/port of incoming media flow(s).

The IMS-ALG may determine that the source address/port of received media packets should be policed.

When the IMS-ALG requests the IMS-AGW to reserve transport addresses/resources, the IMS-ALG may indicate to the IMS-AGW that policing of source address and/or port of received media packets is required.

If such policing is applicable, the IMS-AGW shall check the source address and/or port of all received media packets and silently discard any packets that do not conform to the expected source address and/or port.

5.6 Traffic Policing

The IMS-ALG may support traffic policing of incoming media flows.

The IMS-AGW shall support traffic policing of the maximum average bitrate, defined as sustainable data rate (see IETF RFC 2216 [10]) of incoming media flows and may support traffic policing of the peak data rate of incoming media flows.

The IMS-ALG may require the IMS-AGW to police the media flows to ensure that they conform to the expected data rates.

When the IMS-ALG requests the IMS-AGW to reserve transport addresses/resources, the IMS-ALG may indicate to the IMS-AGW that policing of the related media streams is required and provide traffic policing related parameters as detailed in subclause 6.2.5.

If such policing is requested, the IMS-AGW shall police the corresponding media streams as detailed in subclause 6.2.5 by measuring the data rate for the received packets within that media stream. If the permissible data rate provided by the IMS-ALG is exceeded, the IMS-AGW shall discard packets to reduce their data rate to the permissible data rate.

For RTP flows where RTCP resources are reserved together with the RTP resources (see subclause 5.9), the permissible data rate shall include the bandwidth used by RTP and RTCP together.

5.7 Hanging Termination Detection

The IMS-ALG and the IMS-AGW shall support detection of hanging termination.

The IMS-ALG, when requesting the IMS-AGW to reserve an AGW connection point, shall indicate to the IMS-AGW to perform detection of hanging terminations.

The IMS-AGW shall determine a termination to be hanging if there is no signalling sent/received within a specified period.

On being informed of the hanging termination, the IMS-ALG shall check/determine whether the cited termination is valid and initiate any appropriate corrective action, e.g. release an invalid termination.

5.8 QoS Packet Marking

The IMS-ALG may support and the IMS-AGW shall support control via the Iq interface of the setting of the DiffServ Code Point (DSCP) for media packets sent on a termination.

When the IMS-ALG requests the IMS-AGW to reserve transport addresses/resources, the IMS-ALG may indicate to the IMS-AGW that the DSCP of outgoing media packets shall be explicitly set or copied from the DSCP of the corresponding received packet.

If such modification of the DSCP is required by the IMS-ALG, the IMS-AGW shall set the DSCP for outgoing packets on a termination.

5.9 Handling of RTCP streams

The IMS-ALG and the IMS-AGW shall support control via the Iq interface of the specific RTCP behaviour associated to an RTP flow.

When the IMS-ALG requests the IMS-AGW to reserve transport addresses/resources for an RTP flow, the IMS-ALG should also request the IMS-AGW to reserve resources for the corresponding RTCP flow, but may alternatively request the IMS-AGW not to reserve resources for the corresponding RTCP flow. When the IMS-ALG requests the IMS-AGW to reserve transport addresses/resources for a non-RTP flow, the IMS-ALG shall not request the IMS-AGW to reserve resources for an RTCP flow.

To request the IMS-AGW to reserve resources for an RTCP flow, the IMS ALG shall provide the RTCP handling information element with a value indicating that resources for RTCP shall be reserved.

To request the IMS-AGW not to reserve resources for an RTCP flow, the IMS ALG shall either provide the RTCP handling information element with a value indicating that resources for RTCP shall not be reserved or omit the RTCP handling information element.

If the IMS-AGW receives the indication to reserve RTCP resources, the IMS-AGW shall allocate a local port with even number for an RTP flow also reserve the consecutive local port with odd number for the associated RTCP flow, and it shall send and be prepared to receive RTCP.

If the IMS-AGW receives the indication to not reserve RTCP resources, or if it does not receive any indication at all, it shall not allocate an RTCP port when allocating a port for an RTP flow. The IMS-AGW shall not send any RTCP packets and shall silently discard any received RTCP packets.

When RTCP resources are requested, the IMS-ALG may also specify:

- the remote RTCP port, and optionally the remote address, where to send RTCP packets; if not specified, the IMS-AGW shall send RCTP packets to the port contiguous to the remote RTP port;

- bandwidth allocation requirements for RTCP, if the RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556 [6].

NOTE: In line with the recommendations of RFC 3605 [7], separate address or non-contiguous RTCP port numbers will not be allocated by the IMS-ALG / IMS-AGW.

The IMS-AGW shall return an error if it can not allocate the requested RTCP resources.

5.10 Media Inactivity Detection

The IMS-ALG and the IMS-AGW may support the detection of inactive media flows.

The IMS-ALG may require an IMS-AGW that supports media inactivity detection to detect if a media flow is inactive.

NOTE: The decision to apply or not media inactivity is general for all sessions with the same media characteristics (i.e. not user specific). It is for further study under which conditions inactivity media detection may be requested.

When the IMS-ALG requests the IMS-AGW to reserve transport addresses/resources, the IMS-ALG may indicate to the IMS-AGW that detection of an inactive media flow is required and may additional specify inactivity detection time and inactivity detection direction.

The IMS-AGW shall determine a media flow on termination to be inactive if there is no media sent and/or received within the inactivity detection time period.

On being informed of the inactive media, the IMS-ALG shall initiate any appropriate corrective action.

5.11 IMS Media Plane Security

5.11.1 General

The IMS-ALG and the IMS-AGW may support IMS media plane security as specified in 3GPP TS 33.328 [12]. They may support end-to-access edge security, or end-to-end security, or both, for

- RTP based media (such as e.g. audio, video information) using SRTP security, and/or
- TCP based media (such as MSRP and BFCP) using TLS security; and/or
- UDP based media (such as T.38 fax over UDPTL/UDP) using DTLS security.

If supported the IMS-ALG and the IMS-AGW shall use the procedures in the following subclauses.

NOTE: For the support of end-to-end security, the presence of an IMS-ALG is not required.

Procedures for the IMS-ALG to determine if end-to-access edge security or end-to-end security is applicable to a session are specified in 3GPP TS 33.328 [12] and 3GPP TS 24.229[11].

5.11.2 End-to-access-edge Security

5.11.2.1 End-to-access-edge security for RTP based media using SDES

Procedures for the IMS-ALG to determine if end-to-access edge security is applicable to RTP based media and to exchange cryptography related SDP parameters with the served UE during the SIP session setup are specified in 3GPP TS 33.328 [12] and 3GPP TS 24.229[11].

For media lines that can be subject to e2ae security, the IMS-ALG will receive "RTP/AVP" or "RTP/AVPF" as transport protocol in SDP from the core network. When the IMS-ALG determines that e2ae security is applicable, it will indicate "RTP/SAVP" (see IETF RFC 3711 [14]) or "RTP/SAVPF" (see IETF RFC 5124 [15]), respectively, as transport protocol in the corresponding SDP media lines send towards the served UE. When e2ae security is applied, the IMS-ALG will also receive "RTP/SAVP" or "RTP/SAVPF" in SDP from the served UE. The IMS-ALG will then indicate "RTP/AVP" or "RTP/AVPF" respectively, as transport protocol in the corresponding SDP media lines send towards the core network. When the IMS-ALG requests the IMS-AGW to reserve transport addresses/resources for media to which e2ae security is applicable, the IMS ALG shall configure "RTP/SAVP" or "RTP/SAVPF" as transport protocol at the access side termination. The IMS ALG shall configure "RTP/AVP" or "RTP/AVPF" as transport protocol at the core network side termination for media where e2ae security is applicable.

When the IMS-ALG determines that e2ae security is applicable, it will generate appropriate cryptographic context parameters, in particular key(s), and will transfer them to the served UE within SDES SDP "crypto" attribute(s) according to IETF RFC 4568 [13]. The IMS-ALG will also receive cryptographic context parameters, in particular key(s), from the served UE within SDES SDP "crypto" attribute(s). When the IMS-ALG requests the IMS-AGW to reserve or configure transport addresses/resources for media to which e2ae security is applicable, the IMS-ALG shall provide cryptography related parameters as SDES SDP "crypto" attributes applicable at the access side termination.

On the originating side of the SIP session setup, the IMS-ALG shall provide as "Remote cryptographic SDES attribute" the SDES crypto attribute it selected from the ones received from the IMS UE in the SDP Offer . The IMS-ALG shall provide as "Local cryptographic SDES attribute" the SDES crypto attribute the IMS-ALG generated and inserted in the SDP Answer sent to IMS UE.

On the terminating side of the SIP session setup, the IMS-ALG shall provide as "Remote cryptographic SDES attribute" the SDES crypto attribute received from the IMS UE in the SDP Answer. The IMS-ALG shall provide as "Local cryptographic SDES attribute" the SDES crypto attribute selected by the UE from the ones the IMS-ALG generated and inserted in the SDP Offer sent to UE. If the IMS-ALG offers only one SDES crypto attribute to the UE, the IMS-ALG may provide this attribute as "Local cryptographic SDES attribute" within the Reserve AGW Connection Point Procedure before receiving the SDP answer from the UE.In the present release, a modification of an established e2ae crypto session is not supported. Thus, the IMS-ALG shall not modify any previously provided "Local cryptographic SDES attribute" or "Remote cryptographic SDES attribute".

If the IMS-ALG applies e2ae media security for a media stream and receives an SDP bandwidth modifier related to that media stream in SIP/SDP signalling, it should modify this bandwith modifier to adjust the bandwidth overhead due to e2ae security before forwarding the SDP. The IMS-ALG should add the bandwidth overhead caused by e2ae media security to the bandwidth information received from the remote peer. The IMS-ALG should substract the bandwidth overhead caused by e2ae media security from the bandwidth information received from the served UE.

The IMS Access GW shall, upon reception of an SDES crypto attribute, establish an SRTP security context (as described in RFC 4568 [13] and RFC 3711 [14]) and be prepared to convert RTP packets to SRTP packets and vice versa, using the corresponding SRTP security contexts.

5.11.2.2 End-to-access-edge security for TCP based media using TLS

5.11.2.2.1 General

E2ae security for TCP based media using TLS is applicable for MSRP (see IETF RFC 4975 [25]; used in IMS session-based messaging) and BFCP (see IETF RFC 4582 [31]; used in IMS conferencing). The IMS-ALG and IMS-AGW may support e2ae security for MSRP, BFCP, or both protocols.

E2ae protection of MSRP and BFCP media is based on TLS, according to the TLS profile specified in Annex M of 3GPP TS 33.328 [12]. TLS shall be supported over the TCP transport (see IETF RFC 793 [29]).

Key management for e2ae protection of MSRP and BFCP is based on the ciphersuites and session keys negotiated via the TLS handshake protocol between the UE and the IMS-AGW (see 3GPP TS 33.328 [12]).

Procedures for the IMS-ALG to determine if e2ae security for MSRP and/or BFCP is applicable to a session and to exchange the cryptographic information (i.e. certificate fingerprints) over SDP with the served UE during the SIP session setup are specified in 3GPP TS 33.328 [12] and 3GPP TS 24.229 [11]. If e2ae security is not required, the e2e security procedures may apply, see subclause 5.11.3.

If the IMS-ALG applies e2ae media security for a media stream and receives an SDP bandwidth modifier related to that media stream in SIP/SDP signalling, it should modify this bandwith modifier to adjust the bandwidth overhead due to e2ae security before forwarding the SDP. The IMS-ALG should add the bandwidth overhead caused by e2ae media security to the bandwidth information received from the remote peer. The IMS-ALG should substract the bandwidth overhead caused by e2ae media security from the bandwidth information received from the served UE.

For each MSRP or BFCP media stream to be set-up with e2ae security, the P-CSCF (IMS-ALG) shall:

- include the IMS-AGW in the media path and allocate the required resources for the media stream in the IMS-AGW;
- request a certificate fingerprint from the IMS-AGW;
- include the certificate fingerprint received from the IMS-AGW in the SDP it sends to the IMS UE;
- send the certificate fingerprint received in the SDP from the IMS UE to the IMS-AGW;
- instruct the IMS-AGW to perform state-aware TCP handling by including information about the TCP setup direction;
- for each termination determine via SDP negotiation as specified in IETF RFC 4145 [30] if the IMS-AGW needs to act as TCP client or server for the terminations towards the core network and towards the access network;
- indicate to the IMS-AGW how to perform the TCP connection establishment by:
    a) either instructing the IMS-AGW to start a TCP connection establishment on any terminations where it needs to act as TCP client; or
    b) indicating to the IMS-AGW to use an incoming TCP connection establishment request at one termination as a trigger to send a TCP connection establishment request at the interconnected termination in the same context (support of this alternative is optional for the IMS-AGW and IMS-ALG);
- determine via SDP negotiation if the IMS-AGW needs to act as TLS client or server as specified in the subclauses below;

NOTE 2: The determination of the TLS client/server role relies on different rules for MSRP and BFCP.

- if the IMS-AGW needs to act as TLS client, request the IMS-AGW to start the TLS session setup once the TCP connection is established towards the UE; and
- apply additional specific procedures for MSRP in subclause 5.11.2.2.2 or for BFCP in subclause 5.11.2.2.3.

For each MSRP or BFCP media stream to be set-up with e2ae security the IMS-AGW shall:

- upon request from the IMS-ALG, select an own certificate for the media stream, uniquely associate own certificate with the media stream, and send the fingerprint of the own certificate to the IMS-ALG;
- uniquely associate the certificate fingerprint received from the IMS-ALG with the corresponding MSRP or BFCP media stream, and subsequently use the certificate fingerprint (as described in IETF RFC 4975 [25]) to verify the establishment of the TLS session of the corresponding media stream to belong to the served user;
- if the verification of the remote certificate fingerprint during the TLS session establishment fails, regard the remote TLS endpoint as not authenticated, terminate the TLS session and report the unsuccessful TLS session setup to the IMS-ALG;
- negotiate the TLS protocol configurations with the TLS peer based on locally provisioned TLS profile parameters;

- when the TLS session has been established, convert unprotected media received from the network to protected media to send to the served UE and vice versa;
- be capable to support both the TLS server and TLS client roles;
- when being instructed to start the TLS session setup, act as a TLS client and establish the TLS session as soon as the underlying TCP bearer connection is established;
- upon instruction of the IMS-ALG to perform state-aware TCP handling, not forward any TCP connection establishment request received on one termination towards the interconnected termination;
- upon corresponding instructions from the IMS-ALG, start a TCP connection establishment on the indicated termination by sending a TCP SYN, or use an incoming TCP connection establishment request received at one termination as a trigger to send a TCP connection establishment request at the interconnected termination in the same context;
- release the underlying TCP bearer connection as soon as the TLS session is released; and
- apply additional specific procedures for MSRP in subclause 5.11.2.2.2 or for BFCP in subclause 5.11.2.2.3.

5.11.2.2.2 e2ae security for session based messaging (MSRP)

For each MSRP media stream requiring e2ae security, the IMS-ALG shall indicate to the IMS-AGW as transport protocol:

a) for application-agnostic e2ae security support:
   - "TCP" at the termination towards the core network; and
   - "TCP/TLS" at the termination towards the access network; or

b) for application-aware e2ae security support:
   - "TCP/MSRP" at the termination towards the core network; and
   - "TCP/TLS/MSRP" at the termination towards the access network.

The IMS-ALG shall determine via SDP negotiation if the IMS-AGW needs to act as TLS client or TLS server using the IETF RFC 4145 [30] "a=setup" SDP attribute as follows:

- if the IMS-ALG send an "a=setup:active" SDP attribute in an SDP answer towards the UE, the IMS-AGW shall act as TLS client;
- if the IMS-ALG send an "a=setup:passive" SDP attribute in an SDP answer towards the UE, the IMS-AGW shall act as TLS server;
- if the IMS-ALG receives an "a=setup:active" SDP attribute in an SDP answer from the UE, the IMS-AGW shall act as TLS server; and
- if the IMS-ALG receives an "a=setup:passive" SDP attribute in an SDP answer from the UE, the IMS-AGW shall act as TLS client.

5.11.2.2.3 e2ae security for conferencing (BFCP)

For each BFCP media stream requiring e2ae security, the IMS-ALG shall indicate to the IMS-AGW as transport protocol:

- "TCP" at the termination towards the core network; and
- "TCP/TLS" at the termination towards the access network.

The IMS-ALG shall determine via SDP negotiation (see IETF RFC 4583 [27]) if the IMS-AGW needs to act as TLS client or TLS server as follows:

- if the IMS-ALG receives an initial SDP offer from the UE, the IMS-AGW shall act as TLS server; and

- if the IMS-ALG sends an initial SDP offer towards the UE, the IMS-AGW shall act as TLS client.

5.11.2.3 End-to-access-edge security for UDP based media using DTLS

5.11.2.3.1 General

The IMS-ALG and the IMS-AGW may support end-to-access-edge (e2ae) security for an UDP based media. The e2ae protection of the UDP based media relies on the usage of DTLS (see IETF RFC 6347 [32]) and exchange of self-signed certificates as defined in 3GPP TS 33.328 [12].

Key management solution for the e2ae media security of UDP is based on the cipher suites and session keys negotiated via the DTLS handshake protocol between the served UE and the IMS-AGW as specified in 3GPP TS 33.328 [12]. Procedures for the IMS-ALG to determine if e2ae security is applicable to UDP based media and to exchange the cryptographic information (i.e. certificate fingerprints) via SDP negotiation with the served UE during the SIP session establishment are specified in 3GPP TS 33.328 [12] and 3GPP TS 24.229 [11].

If the IMS-ALG applies e2ae media security for a media stream and receives an SDP bandwidth modifier related to that media stream in SIP/SDP signalling, it should modify this bandwith modifier to adjust the bandwidth overhead due to e2ae security before forwarding the SDP. The IMS-ALG should add the bandwidth overhead caused by e2ae media security to the bandwidth information received from the remote peer. The IMS-ALG should substract the bandwidth overhead caused by e2ae media security from the bandwidth information received from the served UE.

Subclause 5.11.2.n.2 defines specific requirements for e2ae protection of T.38 fax media stream over UDPTL/UDP transport. The usage of UDPTL over DTLS is defined in IETF draft-ietf-mmusic-udptl-dtls [33].

5.11.2.3.2 e2ae security for T.38 fax over UDP/UDPTL transport

If the IMS-ALG and the IMS-AGW support e2ae security for the UDP based media using DTLS and certificate fingerprints, then for each T.38 fax media stream over UDPTL/UDP transport to be setup with e2ae security, the IMS-ALG shall:

- include the IMS-AGW in the media path and allocate the required resources for the media stream in the IMS-AGW;
- determine via SDP negotiation with the served UE if the IMS-AGW needs to act as DTLS client or DTLS server as specified in IETF draft-ietf-mmusic-udptl-dtls [33];
- when requesting resources towards the access network:
  a) indicate to the IMS-AGW "UDP/DTLS" as transport protocol;

  NOTE: For IANA registry of "UDP/DTLS" see IETF draft-schwarz-mmusic-sdp-for-gw [34].

  b) send the certificate fingerprint received from the served UE to the IMS-AGW; and
  c) request from the IMS-AGW the certificate fingerprint;
- include the certificate fingerprint received from the IMS-AGW in the SDP body it sends to the served UE;
- request the IMS-AGW to start the DTLS session setup if the IMS-AGW needs to act as DTLS client; and
- when requesting resources towards the core network:
  a) indicate to the IMS-AGW "UDP" as transport protocol.

For each T.38 fax media stream over UDPTL/UDP transport to be setup with e2ae security, the IMS-AGW shall:

- be capable to support both the DTLS server and DTLS client roles;
- upon request from the IMS-ALG, act as DTLS client and start DTLS session establishment;
- upon request from the IMS-ALG, select an own certificate for the T.38 fax media stream, uniquely associate its own certificate with the media stream, and send the fingerprint of the own certificate to the IMS-ALG;

- uniquely associate the certificate fingerprint received from the IMS-ALG with the corresponding T.38 fax media stream; and
- verify during the subsequent DTLS handshake with the served UE (as described in IETF draft-ietf-mmusic-udptl-dtls [33]) that the fingerprint of the certificate passed by the served UE during DTLS handshake matches the certificate fingerprint received from the IMS-ALG:
  a) if the verification fails, the IMS-AGW shall regard the remote DTLS endpoint as not authenticated, terminate the DTLS session and report the unsuccessful DTLS session setup to the IMS-ALG;
  b) otherwise, the IMS-AGW shall continue with DTLS session setup and when the DTLS session is established, the IMS-AGW shall be prepared to receive and convert unprotected media from the core network to the protected media to be sent to the served UE and vice versa.

5.11.2.4 End-to-access-edge security for RTP based media using DTLS-SRTP

The eP-CSCF (IMS-ALG) and eIMS-AGW for WebRTC provide end-to-access edge security by using DTLS-SRTP, where DTLS is used to establish keys for SRTP according to IETF RFC 5763 [42] and IETF RFC 5764 [43].

During the establishment of a WebRTC session, the IMS-ALG receives "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as the transport protocol in SDP from the served WebRTC IMS Client (WIC). The IMS-ALG then shall indicate "RTP/AVP" or "RTP/AVPF" over UDP, respectively, as the transport protocol in the corresponding SDP media lines send towards the core network. When an IMS-ALG receives "RTP/AVP" or "RTP/AVPF" in SDP from the core network, the IMS-ALG shall indicate "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as transport protocol in SDP send torwards the served WIC. When the IMS-ALG requests the eIMS-AGW to reserve transport addresses/resources for e2ae media security, the IMS ALG shall configure "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as transport protocol at the access side termination, and "RTP/AVP" or "RTP/AVPF" over UDP as transport protocol at the core network side termination.

The IMS-ALG shall send the received WIC certificate fingerprint to the eIMS-AGW that is then able to correlate the fingerprint within the media stream uniquely. For each SRTP/SRTCP media stream to be established with e2ae media security, the eIMS-AGW shall send the fingerprint of its certificate via Iq interface to the IMS-ALG.

According to procedures defined in 3GPP TS 24.371 [44], the eIMS-AGW shall act as either a DTLS server or client in the DTLS session.

In DTLS-SRTP case, RTP and RTCP data are encrypted using SRTP and SRTCP as defined in IETF RFC 3711 [14].

When the DTLS session is established between the WIC and the eIMS-AGW, the eIMS-AGW shall be prepared to send and receive SRTP/SRTCP packets of the incoming network side from the WIC, and convert SRTP/SRTCP packets to RTP/RTCP packets to the outgoing network side and vise versa, if the media stream towarding to the IMS core network is using RTP/RTCP.

5.11.3 End-to-end Security

5.11.3.1 End-to-end security for RTP based media

For the support of e2e-security, the IMS-ALG and the IMS-AGW shall support "RTP/SAVP" (see IETF RFC 3711 [14]) and/or "RTP/SAVPF" (see IETF RFC 5124 [15]) as transport protocol.

If the IMS-ALG receives SDP containing media lines with "RTP/SAVP" (see IETF RFC 3711 [14]) or "RTP/SAVPF" (see IETF RFC 5124 [15]) as transport protocol, but did not receive any request for end-to-access-edge security, the IMS-ALG shall:

- forward the SDP with unmodified transport protocol for those media lines;
- provide "RTP/SAVP" or "RTP/SAVPF", as received in the SDP, to the IMS-AGW as transport protocol for all related terminations, and provide no media related information to these terminations, to configure the IMS-AGW to pass media transparently.

If the IMS-ALG receives SDP containing SDES SDP attribute(s) according to IETF RFC 4568 [13], and did not receive any request for end-to-access-edge security, it shall forward the SDP with unmodified SDES SDP attribute(s), but shall not provide the SDES SDP attribute(s) to the IMS-AGW.

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

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 [12].

If the IMS-ALG receives SDP containing media lines with "TCP/TLS/MSRP" (see IETF RFC 4975 [25] and IETF RFC 6714 [26]) and/or "TCP/TLS/BFCP" (see IETF RFC 4583 [27]) as transport protocol but did not receive any request for end-to-access-edge security, the IMS-ALG shall:

- forward the SDP with unmodified transport protocol for those media lines and unmodified TLS related SDP attribute(s);
- indicate "TCP" to the IMS-AGW as transport protocol for all related terminations, and provide no media related information to these terminations, to configure the IMS-AGW to pass media transparently.

Editor's Note: The scenario where both terminals of an e2e security protected media session are located behind firewalls/NATs is FFS.

5.12 Explicit Congestion Notification support

5.12.1 General

An IMS-ALG and IMS-AGW may support Explicit Congestion Notification (see IETF RFC 3168 [16], IETF RFC 6679 [17] and 3GPP TS 26.114 [21]).

An IMS-ALG and IMS-AGW which supports ECN shall support the ECN transparent procedure i.e. the transparent forwarding of ECN bits in the IP header (see IETF RFC 3168 [16]). If the IMS-AGW does not support the transparent forwarding of ECN bits then the IMS-ALG shall not permit ECN in the SDP Offer/Answer negotiation.

The IMS-AGW shall treat RTCP for ECN as a RTP translator with no media translation.

An IMS-ALG and IMS-AGW which supports ECN may then act as an ECN endpoint to enable ECN towards the IMS access network or/and towards the IMS Core Network. The subsequent sub-sections describe the general support for ECN, further details on the support of ECN during PS to CS access transfer is described in sub-clause 6.2.14.3.

NOTE: It is out of the scope of this profile to support interworking with a non-3GPP ECN IP terminal.

An IMS-ALG and IMS-AGW that support ECN Transparent as well as transcoding shall also support the ECN endpoint procedure.

An IMS-ALG/IMS-AGW supporting the ATCF/ATGW function and ECN shall support ECN Endpoint (see sub-clause 6.2.14).

When acting as an ECN endpoint, the IMS-AGW shall be capable of enabling end-to-end rate adaptation between the local terminal and the remote entity by performing the following towards the ECN-capable peer:

- trigger rate adaptation request towards the ECN-capable peer when receiving in the incoming IMS media flow IP packets marked with ECN-CE, regardless of whether the IMS-AGW applies or does not apply transcoding;
- forward adaptation requests between the local and the remote peer when the IMS-AGW bridges compatible codec configurations between the interfaces without applying a transcoding function;
- perform media adaptation (e.g. reduce media bit-rate) towards the ECN-capable peer when receiving from the latter an adaptation request. and the IMS-AGW applies transcoding.

5.12.2 Incoming SDP offer with ECN

The IMS-ALG and IMS-AGW shall apply the requirements specified in clause 10.2.13.2 of 3GPP TS 29.162 [20] replacing the IBCF and TrGW with IMS-ALG and IMS-AGW respectively.

5.12.3 Incoming SDP offer without ECN

The IMS-ALG and IMS-AGW shall apply the requirements specified in clause 10.2.13.3 of 3GPP TS 29.162 [20] replacing the IBCF and TrGW with IMS-ALG and IMS-AGW respectively with the following additions:

- if the IMS-ALG or IMS-AGW does not support the procedure to act as an ECN endpoint, the IMS-ALG shall not include the "a=ecn-capable-rtp" attribute in the SDP offer it forwards to the succeeding node.

5.12.4 Detection of ECN failures by IMS-AGW

An IMS-ALG and IMS-AGW that support the procedure to act as an ECN endpoint shall support the requirements specified in clause 10.2.13.3a of 3GPP TS 29.162 [20] replacing the IBCF and TrGW with IMS-ALG and IMS-AGW respectively.

5.13 Transcoding

The transcoding functionality, where the IMS-AGW processes and possibly converts media data (like e.g. RTP payload) is optional for the P-CSCF and IMS-AGW to support. Transcoding should be supported if the IMS-ALG and IMS-AGW support the ATCF and ATGW functions for use after an SRVCC handover if the media that was used prior to the access transfer is not supported by the MSC Server.

An IMS-ALG and IMS-AGW that support transcoding shall support the requirements specified for Media Control in clause 10.2.5 of 3GPP TS 29.162 [20] respectively for the IBCF and TrGW, with the following additions:

- During an originating or terminating PS session establishment, the IMS-ALG (ATCF) may remove codecs when passing SDP offers (e.g. codecs known not to be supported by either the IMS-AGW (ATGW) or the MSC Server), but the IMS-ALG (ATCF) should pass SDP offers without adding codecs to the SDP offer and pass SDP answers without modification to the contained codecs to avoid the potential need for transcoding in the IMS-AGW (ATGW) before the PS to CS access transfer;

- During the PS to CS access transfer procedure, the IMS-ALG (ATCF) shall preferentially select from the SDP offer it receives from the MSC Server the codec already configured on the corresponding remote leg, if available.

The procedures for the IMS-ALG (ATCF) and IMS-AGW (ATGW) are further detailed in subclause 6.2.14.

5.14 Multimedia Priority Service (MPS) Support

The Multimedia Priority Service (MPS) is specified in 3GPP TS 22.153 [22]. The IMS-ALG and IMS-AGW may support the priority treatment of a call/session identified as an MPS call/session. If MPS is supported, the following functional requirements apply:

- Upon receipt of the MPS priority information in the call control signalling:

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

  - The IMS-ALG shall send the priority information for a context to the IMS-AGW to enable the priority treatment described below related to the IMS-AGW.

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

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

  - If the MPS Priority service requires a specific MPS DSCP setting the IMS-ALG shall configure the IMS-AGW 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 IMS-AGW 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 IMS-AGW assumes an operator uses Diffserv for prioritising user plane traffic related to an MPS call/session.

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

  i) seize priority reserved resources; or

  ii) if resources are congested, indicate that in aCommand 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.

5.15 Coordination of Video Orientation

The IMS-ALG and the IMS-AGW may support the Coordination of Video Orientation (CVO) as defined in 3GPP TS 26.114 [21].

If the IMS-ALG receives an SDP body containing "a=extmap" attribute(s), as defined in IETF RFC 5285 [23], and the "a=extmap" attribute(s) contain 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 [21], then:

- a) if the IMS-ALG and the IMS-AGW support the CVO feature:

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

Editor´s Note: It is ffs if the IMS-ALG needs to include the "extended RTP header for CVO" information element when seizing terminations of a media agnostic IMS-AGW, or if a media agnostic IMS-AGW always passes any RTP header extension.

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

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

NOTE 1: The UE supporting the CVO feature will not send the extended RTP headers for CVO if the UE did not receive any SDP body with the CVO related "a=extmap" attribute.

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

- if the IMS AGW does not apply video transcoding, it shall pass any received RTP CVO header extension to succeeding RTP streams; or
- if the IMS-AGW 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 2: IETF RFC 5285 [23] provides a framework for header extensions and can also be used for non-CVO related purposes. It is an implementation decision of the IMS-AGW 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 3: The behaviour of the IMS-AGW when being instructed with an "extended RTP header for CVO" information element only at one termination is an implementation decision.

NOTE 4: Unknown IETF RFC 5285 [23] RTP header extensions are ignored by the destination RTP end system.

5.16 Generic image attributes

The IMS-ALG and the IMS-AGW may support a media-level SDP image attribute "a=imageattr" defined in IETF RFC 6236 [24] to negotiate the image size for sending and receiving video as required by 3GPP TS 26.114 [21].

NOTE: 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 IMS-ALG:

- supports the negotiation of the image size;
- receives an SDP body containing the image attribute(s) "imageattr" defined in IETF RFC 6236 [24]; and
- does not support or does not apply the video transcoding procedure defined in subclause 5.13;

the IMS-ALG shall forward the SDP body with unmodified image attribute(s).

If the IMS-ALG and the IMS-AGW support the ATCF/ATGW functions then during the access transfer procedures the IMS-ALG may apply the procedure described in subclause 6.2.14.6 to negotiate and adjust the image size for sending and receiving video of the session.

5.17 TCP bearer connection control

5.17.1 Stateless TCP handling

An IMS-ALG and IMS-AGW that supports TCP as transport protocol (see IETF RFC 793 [29] and IETF RFC 4145 [30]) shall support the following procedures.

NOTE 1: It is assumed that pre-Release 12 IMS-ALGs and IMS-AGWs also apply these procedures.

When receiving an SDP offer or answer containing a media line for a new TCP based media stream (e.g. with "TCP", "TCP/MSRP" as transport protocol), the IMS-ALG:

- shall indicate "TCP" (for application-agnostic interworking) or "TCP/MSRP" (for application-aware MSRP interworking) as transport protocol to the IMS-AGW;
- shall indicate the TCP port numbers received in the SDP from the remote peer as destination port in the remote descriptor at the termination towards the SDP sender;
- shall request the IMS-AGW to allocate a TCP port number at the destination towards the SDP receiver;
- shall replace the TCP port in the received SDP with the TCP port number allocated by the IMS-AGW and forward the SDP; and
- shall indicate to the IMS-AGW to perform TCP stateless handling by not including the TCP session setup direction attribute at the interconnected terminations in the same context.

An IMS-AGW receiving an indication of "TCP", or "TCP/MSRP" as transport protocol, but no indication to perform TCP state-aware handling (via information about the directionality of the TCP session setup):

- shall send a TCP SYN when receiving a TCP SYN at the interconnected termination in the same context;
- shall forward received TCP payload; and
- shall use its own port number as TCP source port numbers and the remote port number received from the IMS-ALG as TCP destination port numbers and calculate a new TCP checksum for all TCP packets it sends.

NOTE 2: This mode of operation corresponds to the "TCP Relay" mode in ITU-T Recommendation H.248.84 [38].

5.17.2 State-aware TCP handling

5.17.2.1 General

An IMS-ALG and IMS-AGW that supports TCP as transport protocol (see IETF RFC 793 [29] and IETF RFC 4145 [30]) may support the procedures specified in subclause 5.17.2 for state-aware TCP handling.

NOTE 1: State-aware TCP handling enables modifications of TCP payloads by the IMS-AGW such as changing the size of the payload and inserting extra protocol layers, e.g. for e2ae media security.

An IMS-ALG and IMS-AGW that supports state-aware TCP handling shall support the procedures specified in subclause 5.17.2.2 and may additionally support the procedures specified in subclause 5.17.2.3.

NOTE 2: The procedures in subclause 5.17.2.3 enable TCP connections between two peers behind remote (far-end) NATs without any other intermediate server capable of acting as a TCP B2BUA (such as a messaging server). However, they are not possible if e2e security is applied for MSRP based media.

5.17.2.2 State-aware TCP handling without support of modifying the TCP setup direction

When the IMS-ALG receives an SDP offer containing a media line for a new TCP based media stream (e.g. with "TCP", "TCP/MSRP" as transport protocol), for that TCP based media stream the IMS-ALG:

- if no media security is applied, shall indicate "TCP" (for application-agnostic interworking) or "TCP/MSRP" (for application-aware MSRP interworking) as transport protocol to the IMS-AGW;
- if media security is applied, shall indicate a transport protocol according to subclause 5.11 to the IMS-AGW;
- shall request the IMS-AGW to allocate a TCP port at the destination towards the SDP answerer;
- shall request the IMS-AGW to allocate a TCP port at the destination towards the SDP offerer;
- shall indicate the TCP port numbers received in the SDP offer as destination in the remote descriptor at the termination towards the SDP offerer;
- shall indicate to the IMS-AGW to perform TCP state-aware handling (by indicating the "actpass" TCP session setup direction at both interconnected terminations in the same context in the local descriptor);
- if supported by the IMS-AGW, may indicate to the IMS-AGW for a given termination to use an incoming TCP connection establishment request (TCP SYN) at that termination as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context;
- if supported by the IMS-AGW, may indicate to the IMS-AGW to discard incoming TCP connection establishment requests; and
- shall replace the TCP port in the received SDP offer with the TCP port number allocated by the IMS-AGW at the termination towards the SDP answerer, shall maintain a received "a=setup:active" or "a=setup:passsive" SDP attribute (see IETF RFC 4145 [30]) in the SDP offer without modification, and shall forward the SDP offer.

When the IMS-ALG then receives the SDP answer containing a media line for a new TCP based media stream, for that TCP based media stream the IMS-ALG:

- shall indicate the TCP port numbers received in the SDP answer as destination in the remote descriptor at the termination towards the SDP answerer;
- if supported by the IMS-AGW, may indicate to the IMS-AGW for a given termination to use an incoming TCP connection establishment request (TCP SYN) at that termination as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context;
- if the IMS-ALG did not indicate to the IMS-AGW to use the incoming TCP connection establishment request (TCP SYN) at one termination as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context,

- if the SDP answer contains an "a=setup:active" SDP attribute (see IETF RFC 4145 [30]), shall indicate to the IMS-AGW to start a TCP connection establishment at the termination towards the SDP offerer; and
- if the SDP answer contains an "a=setup:passive" SDP attribute, shall indicate to the IMS-AGW to start a TCP connection establishment at the termination towards the SDP answerer;

NOTE 1: Clients only supporting MSRP according to IETF RFC 4975 [25] will not use the SDP "a=setup" attribute, but will assign the TCP client role to the SDP offerer. However, in 3GPP (Release 8 onwards), OMA and GSMA the support of IETF RFC 6135 [45] is mandated, and the "a=setup" attribute will thus be used.

- if the IMS-ALG previously indicated to the IMS-AGW to discard incoming TCP connection establishment requests, shall indicate to the IMS-AGW to process incoming TCP connection establishment requests; and
- shall replace the destination TCP port in the received SDP answer with the TCP port number allocated by the IMS-AGW at the termination towards the SDP offerer, shall maintain the received "a=setup" SDP attribute (RFC 4145 [30]) in the SDP answer without modification, and shall forward the SDP answer.

An IMS-AGW receiving an indication of "TCP", or "TCP/MSRP" as transport protocol and an indication to perform TCP state-aware handling (via information about the directionality of the TCP session setup):

- if the IMS-ALG indicated to start a TCP connection establishment at a given termination, shall start the TCP connection establishment at that TCP termination by sending a TCP SYN;
- if the IMS-ALG indicated to discard incoming TCP connection establishment requests, shall discard any incoming TCP connection establishment requests (support optional for the IMS-AGW);
- if

  a) the IMS-ALG indicated to use the incoming TCP connection establishment request (TCP SYN) at one termination as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context, and

  b) the IMS-ALG did not indicate to discard incoming TCP connection establishment requests,

  shall send a TCP SYN when receiving a TCP SYN at the interconnected termination in the same context (support optional for the IMS-AGW);
- if

  a) the IMS-ALG did not indicate to use the incoming TCP connection establishment request (TCP SYN) at one termination as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context, and

  b) the IMS-ALG did not indicate to discard incoming TCP connection establishment requests, and

  c) the IMS-ALG already configured the remote IP address and port or requested latching,

  shall answer any received TCP SYN at a given termination with appropriate messages according to TCP procedures;
- shall forward received TCP payload, performing any required modifications on the TCP payload according to procedures in other parts of this specification; and
- shall use its own port number as TCP source port and the remote port number indicated by the IMS-ALG as TCP destination port numbers and shall calculate a new TCP checksum for all TCP packets it sends.

NOTE 2: This mode of operation corresponds to the "TCP Proxy" mode in ITU-T Recommendation H.248.84 [38].

5.17.2.3 State-aware TCP handling with support of modifying the TCP setup direction

The IMS-ALG and IMS-AGW shall perform the same procedures as in subclause 5.17.2.2 with modification according to the present subclause.

When the IMS-ALG receives an SDP offer containing a media line for a new TCP based media stream (e.g. with "TCP", "TCP/MSRP" as transport protocol), for that TCP based media stream the IMS-ALG:

- if an "a=setup:active" SDP attribute (see IETF RFC 4145 [30]) is received in an SDP offer towards a served UE that is possibly behind a remote NAT, the IMS-ALG
    - should replace this attribute with a "a=setup:actpass" or "a=setup:passive" SDP attribute; and
    - shall then not indicate to the IMS-AGW to use the incoming TCP connection establishment request (TCP SYN) at the termination towards the offerer as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context towards the answerer;
- if an "a=setup:active" SDP attribute (see IETF RFC 4145 [30]) is received in an SDP offer from a served UE, the IMS-ALG
    - may replace this attribute with a "a=setup:actpass" SDP attribute; and
    - shall then not indicate to the IMS-AGW to use the incoming TCP connection establishment request (TCP SYN) at the termination towards the answerer as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context towards the offerer;

NOTE 1: Clients only supporting MSRP according to IETF RFC 4975 [25] will not use the SDP "a=setup" attribute, but will assign the TCP client role to the SDP offerer. However, in 3GPP (Release 8 onwards), OMA and GSMA the support of IETF RFC 6135 [45] is mandated, and the "a=setup" attribute will thus be used.

- shall indicate to the IMS-AGW to perform TCP state-aware handling, either by indicating the "actpass" TCP session setup direction at both interconnected terminations in the same context in the local descriptors, or by indicating the "passive" TCP session setup direction at both interconnected terminations in the same context.

When the IMS-ALG then receives the SDP answer containing a media line for a new TCP based media stream, for that TCP based media stream the IMS-ALG:

- if
    a) the IMS-ALG received an "a=setup:active" SDP attribute in the SDP offer, and
    b) the SDP answer containes an "a=setup:active" SDP attribute,

    then

    - if the IMS-ALG previously indicated "actpass" TCP session setup direction at both interconnected terminations to the IMS-AGW, shall indicate to the IMS-AGW the "passive" TCP session setup direction at both interconnected terminations in the same context in the local descriptors, and
    - shall replace the "a=setup:active" SDP attribute in the SDP answer with an "a=setup:passive" SDP attribute before forwarding the answer.
- if
    a) the IMS-ALG received an "a=setup:active" SDP attribute in the SDP offer, and
    b) the SDP answer containes an "a=setup:passive" SDP attribute,

    then

    - if the IMS-ALG previously indicated "passive" TCP session setup direction at both interconnected terminations to the IMS-AGW, shall indicate to the IMS-AGW the "actpass" TCP session setup direction at both interconnected terminations in the same context in the local descriptors, and
    - shall retain the "a=setup:passive" SDP attribute in the forwarded SDP answer;
- if the IMS-ALG did not indicate to the IMS-AGW to use the incoming TCP connection establishment request (TCP SYN) at one termination as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context,
    - if the sent SDP answer towards the offerer contains an "a=setup:active" SDP attribute (RFC 4145 [30]), indicate to the IMS-AGW to start a TCP connection establishment at the termination towards the SDP offerer; and

- if the received SDP answer contains an "a=setup:passive" SDP attribute, indicate to the IMS-AGW to start a TCP connection establishment at the termination towards the SDP answerer.

When the IMS-ALG indicated a "passive" TCP setup direction for a termination, the IMS-AGW shall wait for an incoming TCP connection establishment at that termination and shall not start a TCP connection establishment on its own.

NOTE 2: If the "passive" TCP session setup direction has been indicated to the IMS-AGW at both interconnected terminations, the mode of operation corresponds to the "TCP Merge" mode in ITU-T Recommendation H.248.84 [38]. If the "actpass" TCP session setup direction has been indicated to the IMS-AGW at both interconnected terminations, the mode of operation corresponds to the "TCP Proxy" mode in ITU-T Recommendation H.248.84 [38].

5.18 Interactive Connectivity Establishment (ICE)

5.18.1 General

The IMS-ALG and the IMS-AGW may support ICE functionality as specified in IETF RFC 5245 [39] and 3GPP TS 24.229 [11] to support a UE residing behind a remote NAT. The present subclause describes the requirements for P-CSCF (IMS-ALG) and IMS-AGW when the ICE procedures are supported.

Support of full ICE functionality is optional, but if ICE is supported, the IMS-ALG and IMS-AGW shall at least support ICE lite as specified in IETF RFC 5245 [39].

The IMS-ALG and IMS-AGW shall only use host candidates as local ICE candidates.

NOTE: IMS-ALG and IMS-AGW are not located behind a NAT (from perspective of the ICE deployment model according to Figure 1 in IETF RFC 5245 [39]).

The IMS-ALG with IMS-AGW inserted on the media plane shall perform separate ICE negotiation and procedures with the offerer and the answerer and ICE may be applied independently at either side. Furthermore, the IMS-ALG may be configured to apply ICE procedures only towards the access network side.

When the P-CSCF (IMS-ALG) detects no ICE parameters in the received SDP, it shall not configure the IMS-AGW to apply any ICE and STUN related procedures toward the call leg from where the SDP has been received, and if applicable may apply the remote NAT traversal using latching according to subclause 5.4.

Any IMS-AGW supporting ICE shall advertise its support of incoming STUN continuity check procedures. An IMS-AGW supporting full ICE procedures shall in addition advertise its support for originating STUN connectivity check procedures.

If the IMS-AGW does not indicate the support of STUN procedures, or if the IMS-ALG is configured not to apply ICE toward a call leg, the IMS-ALG:

- shall not configure the IMS-AGW to apply STUN procedures;
- shall remove any received SDP candidate information from the SDP it forwards; and
- may apply remote NAT traversal using latching according to subclause 5.4.

5.18.2 ICE lite

If the IMS-ALG is configured to use ICE lite, or supports only ICE lite, or controls an IMS-AGW that only support ICE lite, the procedures in the present subclause apply.

If the IMS-ALG receives an initial SDP offer with ICE candidate information but no "a=ice-lite" attribute, the IMS-ALG:

- shall not forward the received candidate information in the SDP it sends towards the answerer;
- shall request the IMS-AGW for each media line where it decides to use ICE to reserve an ICE host candidate and provide its address information and a related ICE user name fragment and password;

NOTE 1: Requesting only one host candidate per m-line prevents that the IMS-ALG will receive "a=remote-candidates" SDP attributes in a subsequent SDP. Requesting separate ufrag and password for each media line simplifies H.248 encoding.

- shall configure the IMS-AGW to act as STUN server at the host candidate address, i.e. to answer STUN connectivity checks;
- may provide received remote ICE candidates and the received related ICE user name fragment and password to the IMS-AGW;
- shall include the host candidate and related ICE user name fragment and password received from the IMS-AGW in the SDP answer it forwards;
- shall include the "a=ice-lite" attribute in the SDP answer it forwards; and
- shall not apply the remote NAT traversal using latching according to subclause 5.4.

If the IMS-ALG receives SDP offer with ICE candidate information and an "a=ice-lite" attribute, the IMS-ALG shall not apply ICE towards that call leg and not include any ICE related SDP attributes in the SDP answer.

NOTE 2: This avoids that the ICE lite peer needs to send extra SDP offers to complete ICE procedures.

If the IMS-ALG sends an SDP offer (or forwards a received SDP offer) towards a call leg where ICE is to be applied, the IMS-ALG:

- shall request the IMS-AGW to reserve a host candidate for each media line where it decides to use ICE and provide its address information, user name fragment and password;
- shall configure the IMS-AGW to act as STUN server at the host candidate address, i.e. to answer STUN connectivity checks;
- shall include the host candidate provided by the IMS-AGW and related ICE user name fragment and password in the SDP offer it forwards; and
- shall include the "a=ice-lite" attribute in the SDP offer.

If the IMS-ALG then receives an SDP answer with candidate information from the call leg where ICE is to be applied, the IMS-ALG:

- shall not forward the received candidate information in the SDP it sends towards the offerer;
- may provide received remote ICE candidates and the received related ICE user name fragment and password to the IMS-AGW; and
- shall not apply the remote NAT traversal using latching according to subclause 5.4.

After the initial SDP offer-answer exchange, the IMS-ALG can receive a new offer from the peer that includes updated address and port information in the SDP "c=" line, "m=" line, or "a=rtcp" line SDP attributes. If the ICE user name fragment and password in the SDP offer differ from the ones received in the previous SDP (i.e. the peer restarts ICE), the IMS-ALG shall apply the same procedures as for the initial SDP offer.

When receiving a request for a host candidate for a media line, the IMS-AGW shall allocate one host candidate for that media line and send it to the IMS-ALG within the reply. The IP address and port shall be the same as indicated separately as Local IP Resources. The IMS-AGW shall also indicate that it supports ICE lite in the reply.

When receiving a request for an ICE user name fragment and password, the IMS-AGW shall generate an ICE user name fragment and password and send it to the IMS-ALG within the reply. The IMS-AGW shall store the password and user name fragment to be able to authenticate incoming STUN binding request according to subclause 7.2 of IETF RFC 5245 [39].

When receiving a request to act as STUN server, the IMS-AGW shall be prepared to answer STUN binding request according to subclause 7.2 of IETF RFC 5245 [39]. Once a STUN binding request with the "USE-CANDIDATE" flag has been received, the IMS-AGW may send media towards the source of the binding request.

5.18.3 Full ICE

If the IMS-ALG supports and is configured to use full ICE, and controls an IMS-AGW that supports full ICE, the procedures in the present subclause apply.

If the IMS-ALG receives an initial SDP offer with ICE candidate information, the IMS-ALG:

- shall not forward the received candidate information in the SDP it sends towards the answerer;
- shall request the IMS-AGW for each media line where it decides to use ICE to reserve an ICE host candidate and provide its address information and a related ICE user name fragment and password;

NOTE: Requesting only one host candidate per m-line prevents that the IMS-ALG will receive "a=remote-candidates" SDP attributes in a subsequent SDP. Requesting separate ufrag and password for each media line simplifies H.248 encoding.

- shall configure the IMS-AGW to act as STUN server at the host candidate address, i.e. to answer STUN connectivity checks;
- shall provide received remote ICE candidates and the received related ICE user name fragment and password to the IMS-AGW;
- shall include the host candidate and related ICE user name fragment and password received from the IMS-AGW in the SDP answer it forwards;
- shall determine the role of IMS-ALG in ICE (controlling or controlled) according to subclause 5.2 of IETF RFC 5245 [39];
- shall configure the IMS-AGW to perform connectivity checks in accordance with the determined ICE role;
- shall configure the IMS-AGW to report connectivity check results;
- shall configure the IMS-AGW to report a new peer reflexive candidate if discovered during the connectivity check; and
- shall not apply the remote NAT traversal using latching according to subclause 5.4.

If the IMS-ALG sends an SDP offer (or forwards a received SDP offer) towards a call leg where ICE is to be applied, the IMS-ALG:

- shall request the IMS-AGW to reserve a host candidate for each media line were it decides to use ICE and provide its address information, ICE user name fragment and password;
- shall configure the IMS-AGW to act as STUN server at the host candidate address, i.e. to answer STUN connectivity checks; and
- shall include the host candidate provided by the IMS-AGW and related ICE user name fragment and password in the SDP offer it forwards.

If the IMS-ALG then receives an SDP answer with candidate information from the call leg where ICE is to be applied, the IMS-ALG:

- shall not forward the received candidate information in the SDP it sends towards the offerer;
- shall provide received remote ICE candidates and the received related ICE user name fragment and password to the IMS-AGW;
- shall determine the role of IMS-ALG in ICE (controlling or controlled) according to subclause 5.2 of IETF RFC 5245 [39];
- shall configure the IMS-AGW to perform connectivity checks in accordance with the determined ICE role;
- shall configure the IMS-AGW to report connectivity check results;
- shall configure the IMS-AGW to report a new peer reflexive candidate if discovered during the connectivity check; and

- shall not apply the remote NAT traversal using latching according to subclause 5.4.

When the IMS-ALG is informed by the IMS-AGW about new peer reflexive candidate(s) discovered by the connectivity checks, it shall configure the IMS-AGW to perform additional connectivity checks for those candidates.

When the IMS-ALG is informed by the IMS-AGW about successful candidate pairs determined by the connectivity checks, the IMS-ALG shall send a new SDP offer to its peer with contents according to subclause 9.2.2.2 of IETF RFC 5245 [39] if it has the controlling role and the highest-priority candidate pair differs from the default candidates in previous SDP.

After the initial SDP offer-answer exchange, the IMS-ALG can receive a new offer from the peer that includes updated address and port information in the SDP "c=" line, "m=" line, or "a=rtcp" line SDP attributes. If the ICE user name fragment and password in the SDP offer differ from the ones received in the previous SDP (i.e. the peer restarts ICE), the IMS-ALG shall apply the same procedures as for the initial SDP offer.

When receiving a request for a host candidate for a media line, the IMS-AGW shall allocate one host candidate for that media line and send it to the IMS-ALG within the reply. The IP address and port shall be the same as indicated separately as Local IP Resources.

When receiving a request for an ICE user name fragment and password, the IMS-AGW shall generate an ICE user name fragment and password and send it to the IMS-ALG within the reply. The IMS-AGW shall store the password and user name fragment to be able to authenticate incoming STUN binding request according to subclause 7.2 of IETF RFC 5245 [39].

When receiving a request to act as STUN server, the IMS-AGW shall be prepared to answer STUN binding request according to subclause 7.2 of IETF RFC 5245 [39]. Once a STUN binding request with the "USE-CANDIDATE" flag has been received, the IMS-AGW may send media towards the source of the binding request.

When receiving a request to perform connectivity checks and to report connectivity check results, the IMS AGW:

- shall compute ICE candidate pairs according to subclause 5.7 of IETF RFC 5245 [39];
- shall schedule checks for the ICE candidate pairs according to subclause 5.8 of IETF RFC 5245 [39];
- shall send STUN connectivity checks for the scheduled checks according to subclause 7.1 of IETF RFC 5245 [39];
- shall inform the IMS-ALG about successful candidate pairs determined by the connectivity checks;
- shall inform the IMS-ALG about new peer reflexive candidate(s) discovered by the connectivity checks; and
- should send media using the highest priority candidate pair for which connectivity checks have been completed.

5.19 MSRP handling

5.19.1 General

The IMS-ALG and IMS-AGW may support MSRP handling. If they support MSRP handling, they shall apply the procedures as specified in the present clause 5.19.

The IMS-AGW may operate either in MSRP agnostic and MSRP aware mode. The MSRP agnostic modes relates to "transparent forwarding of MSRP messages" by the IMS-AGW.

The IMS-AGW shall support application-agnostic MSRP handling.

NOTE 1: Application-agnostic MSRP handling suffices when IETF RFC 6714 [26] or IETF draft-ietf-simple-msrp-sessmatch is supported by both ends (e.g. between Rel-8 onwards IMS UEs) and no MSRP relays are used.

NOTE 2: The expired IETF draft-ietf-simple-msrp-sessmatch modifies the session matching procedure defined by IETF RFC 4975 [25]. A peer applying IETF draft-ietf-simple-msrp-sessmatch will only compare the session-id part of the first MSRP URI in the SDP "a=path" attribute with the session-id part of the first MSRP URI in the "To-Path" header field of the received MSRP packets. This draft is still used by OMA and GSMA as an alternative option to IETF RFC 6714 [26].

The IMS-AGW may in addition support application-aware MSRP interworking, as described in Clause 5.18.5.

NOTE 3: Application-aware MSRP interworking enables direct communication:

- between an MSRP client applying IETF RFC 6714 [26] and an MSRP client applying IETF RFC 4975 [25] without extensions by either IETF RFC 6714 [25] or IETF draft-ietf-simple-msrp-sessmatch.
- between an MSRP client applying IETF draft-ietf-simple-msrp-sessmatch and an MSRP client applying IETF RFC 4975 [25] without extensions by either IETF RFC 6714 [26] or IETF draft-ietf-simple-msrp-sessmatch.
- between an MSRP client applying IETF RFC 6714 [26] and an MSRP client applying IETF draft-ietf-simple-msrp-sessmatch.
- between two MSRP clients applying IETF RFC 4975 [25] without extensions by either IETF RFC 6714 [26] or IETF draft-ietf-simple-msrp-sessmatch.

However, to address these scenarios, application aware MSRP interworking can also be applied in other network elements than the IMS-ALG and IMS-AGW, for instance in an CPM Participating Function or CPM Interworking Function as defined in OMA-TS-CPM_Conversation_Function-V2 [46].

NOTE 4: MSRP relays external to the IMS-AGW are not supported in the present release.

The IMS-ALG procedures depend on whether the IMS-AGW applies application-agnostic MSRP interworking or application-aware MSRP interworking, and on the MSRP extensions applied on the interconnected call legs. The support of related procedures in subclauses 5.19.2 to 5.19.4 below are all optional, but the IMS-ALG shall support at least one of them.

Table 5.19.1-1: Behaviour of MSRP clients and related IMS-ALG and IMS-AGW procedures for MSRP with different extensions.

IETF document:	MSRP client takes destination address for TCP connection setup from	Session matching at MSRP client between SDP path and "To-Path" in MSRP messages includes address information	IMS-AGW needs to insert own address into "To-Path" in MSRP messages	IMS-ALG needs to modify SDP path attribute	Support of extension is negotiated
IETF RFC 4975 [25]	SDP MSRP path attribute	Yes	Yes	Yes	-
Expired draft-ietf-simple-msrp-sessmatch	SDP MSRP path attribute	No	No	Yes	No
IETF RFC 6714 [26]	SDP c-line and m-line	Yes	No (Yes if fallback to IETF RFC 4975 [6] occurs and is supported)	No	Yes, via SDP CEMA attribute

5.19.2 IMS-ALG procedures to support IETF RFC 6714 with application agnostic MSRP handling by the IMS-AGW

A peer applying IETF RFC 6714 [26] will include the "a=msrp-cema" SDP attribute in the first SDP offer it sends.

If the "a=msrp-cema" SDP attribute is contained in an SDP offer, the IMS-ALG:

- shall ensure that the IMS-AGW performs application agnostic MSRP handling by not configuring the IMS-AGW to apply application-aware MSRP interworking;
- shall indicate "TCP" or "TCP/TLS" (if e2ae media security is applied) as transport protocol to the IMS-AGW;
- shall forward the "a=path" attribute and the "a=msrp-cema" SDP attribute in the SDP offer without modification; and
- shall forward the "a=path" SDP attribute in the corresponding SDP answer without modification (even if the "a=msrp-cema" SDP attribute is not contained in the answer).

NOTE: If the "a=msrp-cema" SDP attribute is not contained in the SDP answer and the "a=path" SDP attribute is not modified, the offerer will discover a mismatch and send a new SDP offer without the "a=msrp-cema" SDP attribute according to IETF RFC 6714 [26] procedures.

If the "a=msrp-cema" SDP attribute is not contained in an SDP offer, the IMS ALG shall either apply the procedures in subclause 5.19.3 or subclause 5.19.4 (if supported).

5.19.3 IMS-ALG procedures to support IETF draft-ietf-simple-msrp-sessmatch with application agnostic MSRP handling by the IMS-AGW

A peer applying the expired IETF draft-ietf-simple-msrp-sessmatch will not include the "a=msrp-cema" SDP attribute in the SDP it sends, and will only compare the session-id part of the first MSRP URI in the SDP "a=path" attribute with the session-id part of the first MSRP URI in the "To-Path" header field of the first received MSRP packet.

If the "a=msrp-cema" SDP attribute is not contained in an SDP offer, the IMS-ALG:

- shall ensure that the IMS-AGW performs application agnostic MSRP handling by not configuring the IMS-AGW to apply application-aware MSRP interworking;
- shall indicate "TCP" or "TCP/TLS" (if e2ae media security is applied) as transport protocol to the IMS-AGW; and
- shall replace the IP address and TCP port in the only entry of the "a=path" SDP attribute in received SDP offer or answer with the IP address and TCP port allocated for the media stream at the IMS-AGW before forwarding the SDP.

5.19.4 IMS-ALG procedures for application aware MSRP interworking by the IMS-AGW

The IMS ALG:

- shall provide the SDP "a=path" attribute, as received in SIP/SDP signalling, to the IMS-AGW as "MSRP Path" with the remote descriptor of the corresponding call leg;
- shall ensure that the IMS-AGW performs application aware MSRP interworking by configuring the IMS-AGW to apply application-aware MSRP interworking; and
- shall indicate "TCP/MSRP" or "TCP/TLS/MSRP" (if e2ae media security is applied) as transport protocol to the IMS-AGW.

If interworking between an MSRP client applying IETF RFC 6714 [26] and an MSRP client applying IETF RFC 4975 [25] without extensions by either IETF RFC 6714 [26] or IETF draft-ietf-simple-msrp-sessmatch needs to be supported, the IMS ALG should:

- when receiving an SDP offer including the "a=msrp-cema" SDP attribute, include the "a=msrp-cema" SDP attribute in the SDP answer on that call leg;
- when sending an SDP offer, include the "a=msrp-cema" SDP attribute; and
- if the "a=msrp-cema" SDP attribute is not contained in a received SDP answer and the SDP c/m-line address information does not match the "a=path" attribute, send a new SDP offer without the "a=msrp-cema" SDP attribute according to IETF RFC 6714 [26] procedures.

NOTE: The second SDP offer can be omitted if the IMS-ALG knows that there is no SBC in the path (e.g. between the IMS-ALG and the UE).

5.19.5 Application-aware MSRP interworking at the IMS-AGW

The IMS-AGW shall apply application-aware MSRP interworking either if being statically configured to do so, or if being instructed from the IMS-ALG. Support of dynamic instructions from the IMS-ALG is optional.

To apply application-aware MSRP interworking, the IMS-AGW:

- shall modify the MSRP "To-Path" header field in application (i.e. MSRP) data by replacing the IP address and TCP port of the only entry with the corresponding information in the "MSRP path" provided by the IMS_ALG while retaining the MSRP session ID part of the entry as received in the MSRP "To-Path"; and

- shall forward the MSRP data without further modification.

NOTE: MSRP session matching will be performed only be the MSRP clients.

6 IMS-ALG to IMS-AGW Procedures

6.1 Non-Call Related Procedures

6.1.1 General

The non-call related procedures are based on corresponding procedures of 3GPP TS 23.205 [8] where the IMS-ALG takes the place of the MSC server and the IMS-AGW takes the place of the MGW.

6.1.2 IMS-AGW Unavailable

The IMS-ALG server recognises that the IMS-AGW is unavailable in the following 4 cases:

1. The signalling connection is unavailable

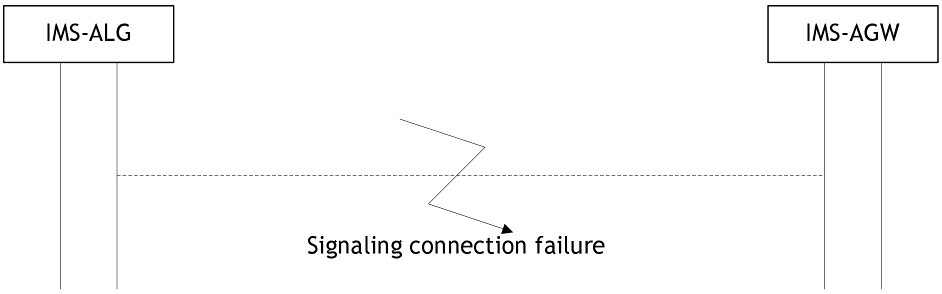


Figure 6.1.2.1: Signalling connection failure

2. The IMS-AGW indicates the failure or the maintenance locking condition to all connected IMS-ALG servers

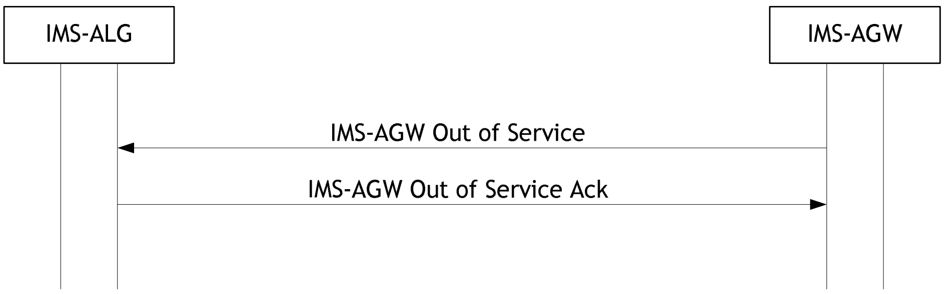


Figure 6.1.2.2: IMS-AGW indicates the Failure/Maintenance locking

The failure or maintenance locking indication indicates that the IMS-AGW is locked for new calls or will soon go out of service and that no new connections should be established using this IMS-AGW. The IMS-AGW can choose between the "graceful" and the "forced" method. In the graceful method the connections are cleared when the corresponding calls are disconnected. In the forced method all connection are cleared immediately.

3. The IMS-ALG recognises that the IMS-AGW is not functioning correctly, e.g. because there is no reply on periodic sending of Audits. The periodic sending of Audits by IMS-ALG should go on.

In all of the above cases the IMS-ALG shall prevent the usage of the IMS-AGW until the IMS-AGW has recovered or the communication with the IMS-AGW is restored.

6.1.3 IMS-AGW Available

The IMS-ALG discovers that the IMS-AGW is available when it receives an IMS-AGW Communication Up message or an IMS-AGW Restoration message. If the IMS-ALG does not wish to sustain an association with the IMS-AGW, the response sent to the IMS-AGW may indicate an alternative IMS-ALG signalling address, in which case the IMS-AGW shall not consider itself registered and should preferably attempt to re-register with this alternative IMS-ALG before any further alternate IMS-ALGs. Otherwise, the response shall not indicate any alternative IMS-ALG signalling address.

When the IMS-ALG discovers that the IMS-AGW is available the following shall occur:

1. Signalling recovery

The IMS-AGW indicates to all connected IMS-ALGs that the signalling connection is restored.

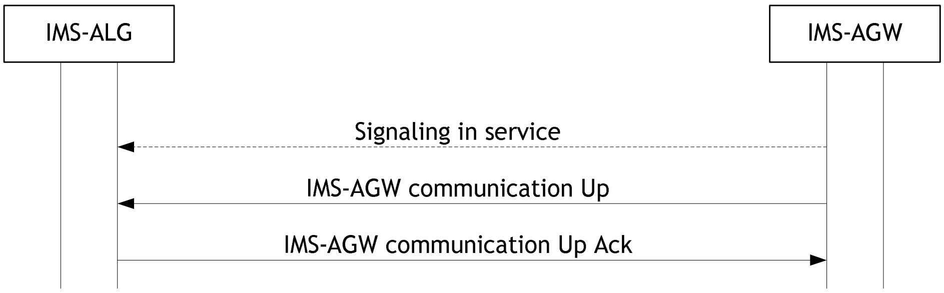


Figure 6.1.3.1: Communication goes up

2. IMS-AGW restoration/maintenance unlocking indication.

   The IMS-AGW indicates to all connected IMS-ALGs that normal operation has resumed.

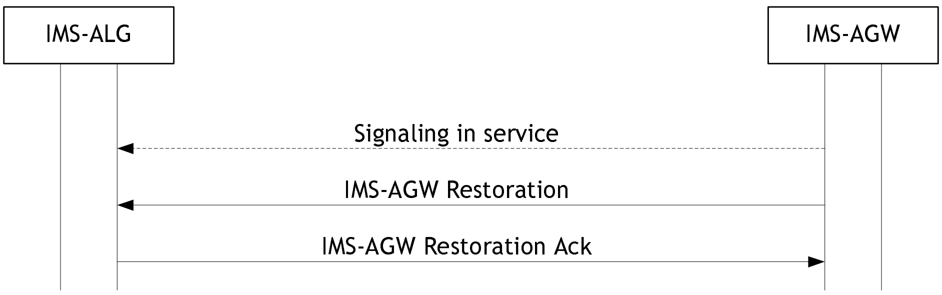


Figure 6.1.3.2: IMS-AGW indicates recovery from a failure/or maintenance unlocking

NOTE: This procedure may be used after recovery from a signalling failure.

3. The IMS-ALG recognises that the IMS-AGW is now functioning correctly, e.g. because there is a reply on periodic sending of Audits.

After this the IMS-ALG can use the IMS-AGW.

If none of 1, 2, and 3 happens the IMS-ALG server can initiate the IMS-ALG Ordered Re-register procedure.

6.1.4 IMS-AGW Recovery

If the IMS-AGW recovers from a failure, is maintenance unlocked, or it has been restarted, it registers to its known IMS-ALGs using the IMS-AGW Restoration procedure or the IMS-AGW Registration procedure. The IMS-AGW can indicate whether the Service has been restored or whether it has restarted with a cold or warm boot. If the IMS-ALG does not wish to sustain an association with the IMS-AGW, the response sent to the IMS-AGW may indicate an alternative IMS-ALG signalling address, in which case the IMS-AGW shall not consider itself registered and should preferably attempt to re-register with this alternative IMS-ALG before any further alternate IMS-ALGs. Otherwise, the response shall not indicate any alternative IMS-ALG signalling address.

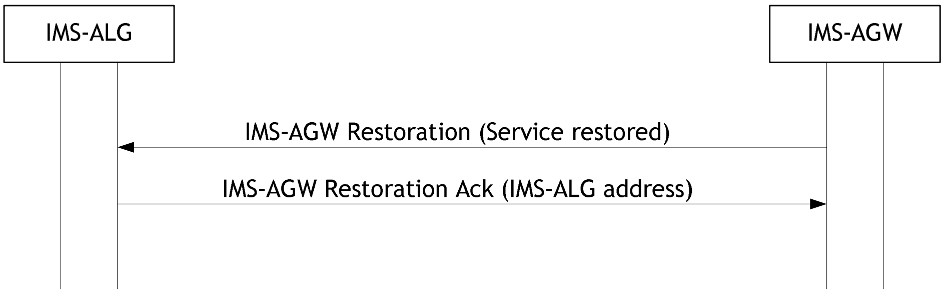


Figure 6.1.4.1: IMS-AGW Restoration

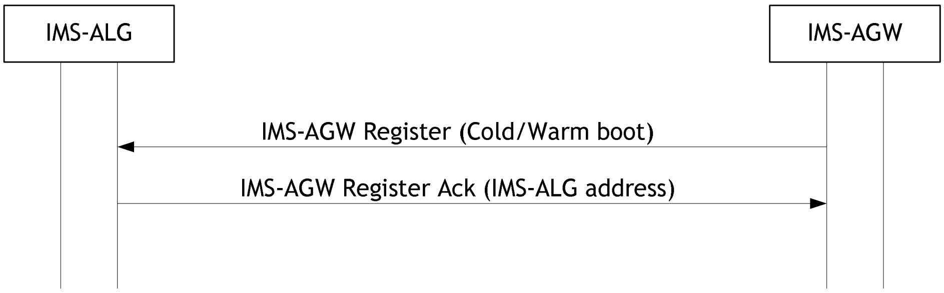


Figure 6.1.4.2 IMS-AGW Registration

After the recovery the IMS-ALG can use the IMS-AGW.

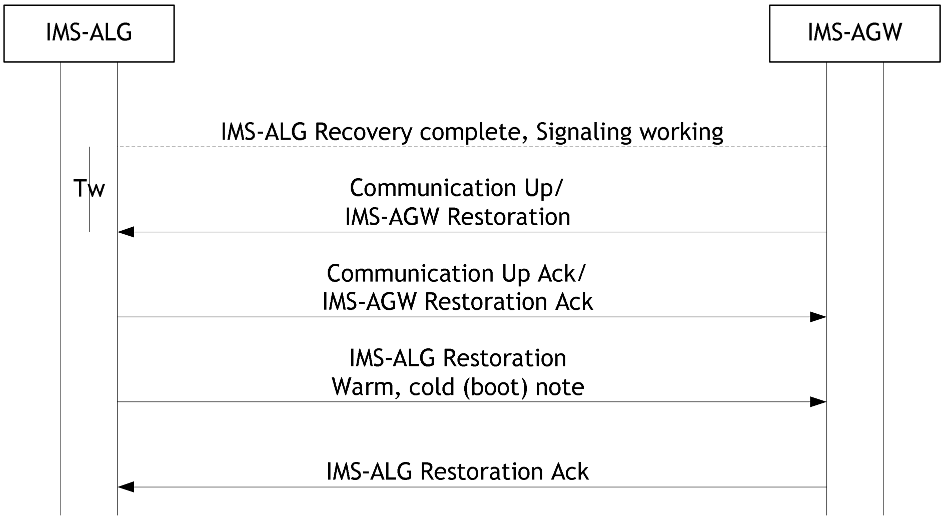
6.1.5 IMS-ALG Recovery

6.1.5.1 General

If an IMS-AGW-unavailable condition is provoked by a failure/recovery action, the IMS-ALG recovery sequence will, from an information flow point of view, look like IMS-AGW unavailable and then IMS-AGW available. If an IMS-AGW-unavailable condition is not provoked, the IMS-ALG recovery sequence will look like IMS-AGW available.

After the information flow, the terminations affected by the recovery action are released.

6.1.5.2 IMS-ALG Restoration



NOTE: Normal release procedure may also be initiated.

Figure 6.1.5.2.1: IMS-ALG Restoration

After the recovery action is complete and it is possible to signal to the IMS-AGW the IMS-ALG starts a timer Tw. If recovery indications are not received (IMS-AGW Communication Up or IMS-AGW Restoration) from the IMS-AGW during Tw an Audit is sent. If the IMS-ALG receives a recovery indication or IMS-AGW communication up indication, it shall acknowledge the indication before the IMS-ALG Restoration may be sent or the release procedure is initiated.

6.1.6 IMS-AGW Re-register

When the IMS-ALG requests an IMS-AGW to perform a registration (see subclauses 6.1.3, 6.1.4 and 6.1.7), the IMS-AGW performs a re-registration to the IMS-ALG which is defined in the IMS-ALG address.

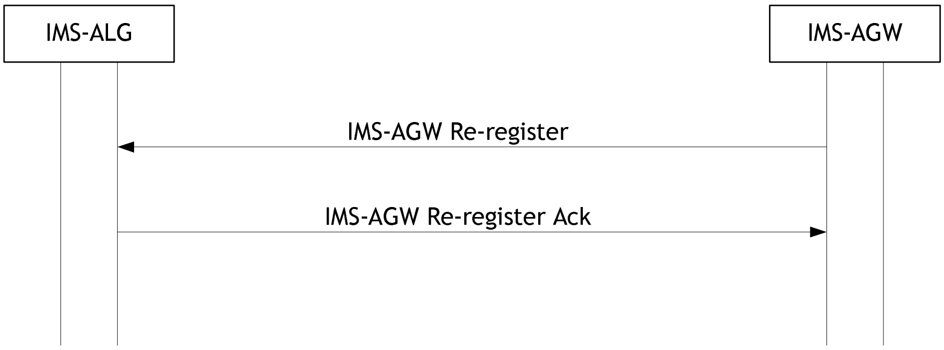


Figure 6.1.6.1: Re-registration of an IMS-AGW

6.1.7 IMS-AGW Re-registration Ordered by IMS-ALG

If the IMS-ALG knows that communication is possible, but the IMS-AGW has not registered, the IMS-ALG can order re-registration of the IMS-AGW.

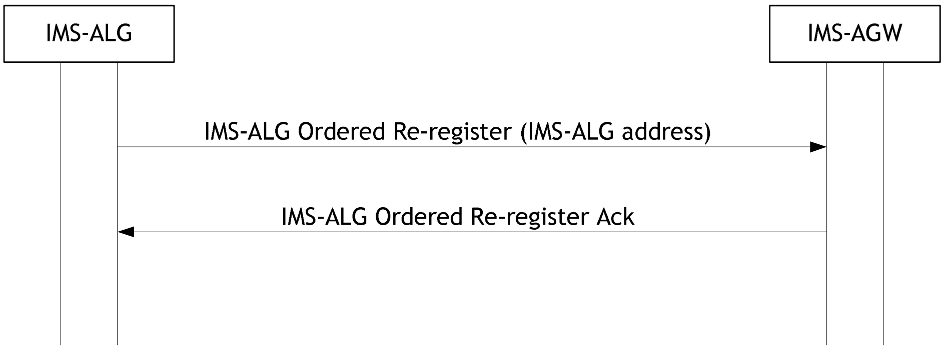


Figure 6.1.7.1: Re-registration ordered by the IMS-ALG

If the re-registration request is accepted the IMS-AGW uses the IMS-AGW Re-register procedure to register with the IMS-ALG.

6.1.8 Audit of IMS-AGW

6.1.8.1 Audit of Value

The IMS-ALG may request the IMS-AGW to report the current values assigned to distinct objects in the IMS-AGW. This procedure may be used when a change has occurred in the IMS-ALG such that the IMS-ALG is unsure of the current Service State of Terminations.

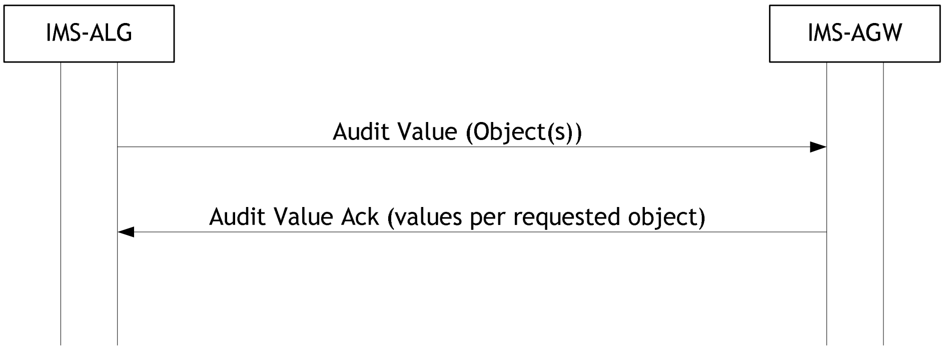


Figure 6.1.8.1.1: Audit Value

6.1.8.2 Audit of Capability

The IMS-ALG may request the IMS-AGW to report the capabilities of distinct objects in the MGW.

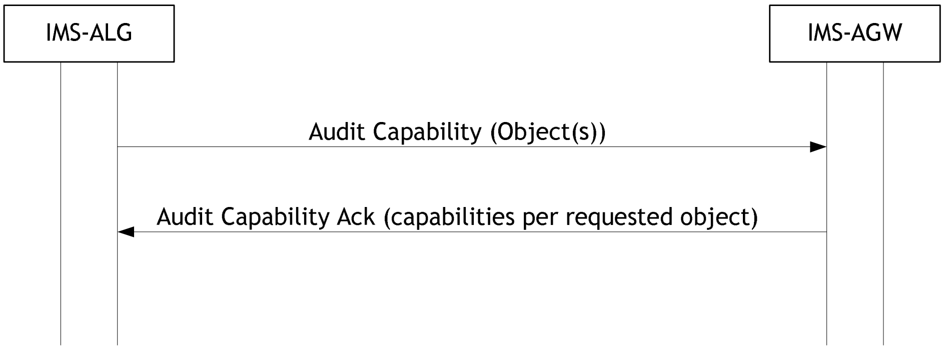


Figure 6.1.8.2.1: Audit Capability

6.1.9 IMS-AGW Capability Change

The IMS-AGW reports a change of capability of distinct objects in the MGW.

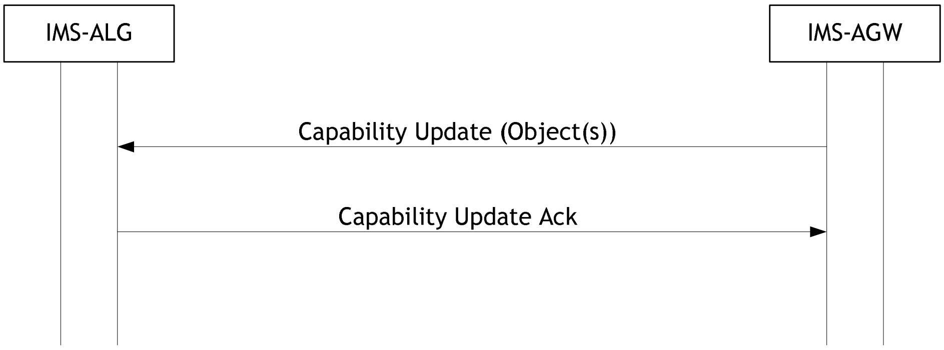


Figure 6.1.9.1: Capability Update

The IMS-ALG may use the Audit Value and/or Audit Capability procedures to obtain further information, about the objects whose capabilities have changed.

6.1.10 IMS-ALG Out of service

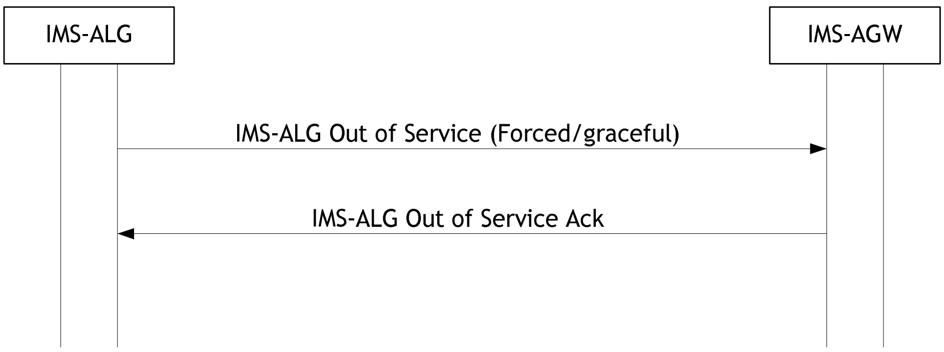


Figure 6.1.10.1: IMS-ALG Out of Service

If an IMS-ALG discovers that it wants to go out of service it may start an IMS-ALG Out of Service procedure. The IMS-ALG can indicate whether it requires the context to be cleared immediately (forced) or cleared as the bearer control protocol clears the bearer (Graceful).

6.1.11 IMS-AGW Resource Congestion Handling - Activate

When the IMS-ALG requires that an IMS-AGW congestion notification mechanism be applied in the MGW, the IMS-ALG shall use the IMS-AGW Resource Congestion Handling - Activate procedure towards the IMS-AGW.

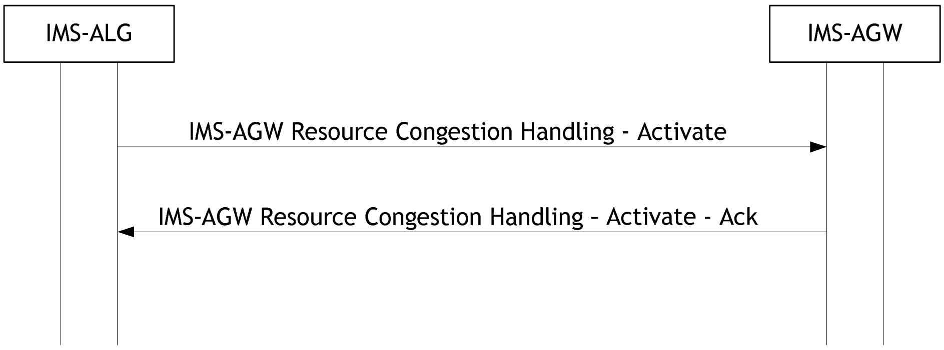


Figure 6.1.11.1: IMS-AGW Resource Congestion Handling - Activate

6.1.12 MGW Resource Congestion Handling -Indication

When the IMS-ALG receives a load reduction notification from the IMS-AGW via the IMS-AGW Resource Congestion Handling - Indication procedure, the IMS-ALG tries to reduce the processing load that the IMS-ALG creates on the IMS-AGW. The IMS-AGW shall decide the actual level of traffic reduction.

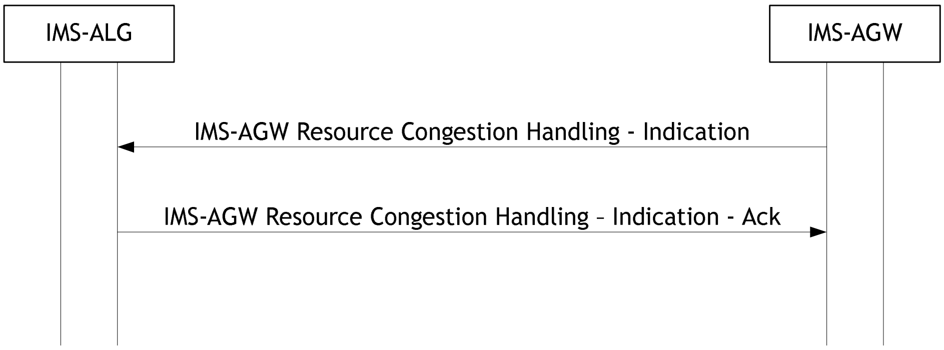


Figure 6.1.12.1: IMS-AGW Resource Congestion Handling – Indication

6.1.13 Control association monitoring

Monitoring of the H.248 control association may be performed by monitoring the status of the transport link association where the transport protocol provides sufficient coupling to the H.248.1 protocol, i.e. if the transport link association is disconnected when no local H.248.1 protocol connection exists.

An alternative method for the IMS-AGW to detect loss of the IMS-ALG may be achieved by requesting the IMS-AGW to poll the IMS-ALG periodically

Upon registration of an IMS-AGW, the IMS-ALG may use the Inactivity Timeout - Activate procedure towards the IMS-AGW to request the IMS-AGW to monitor incoming messages for periods of silence exceeding the maximum inactivity timer value.

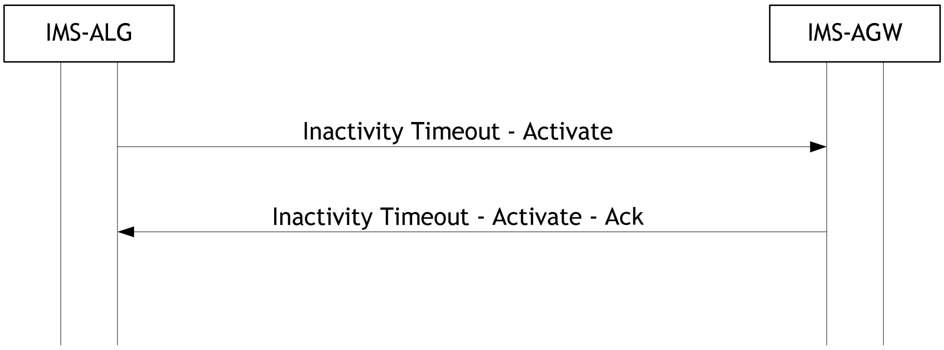


Figure 6.1.13.1: Inactivity Timeout - Activate

Upon receipt of an inactivity timeout notification from the IMS-AGW via the Inactivity Timeout - Indication procedure, the IMS-ALG shall send a reply to the IMS-AGW. If the IMS-ALG has failed, the IMS-AGW will not receive a reply.

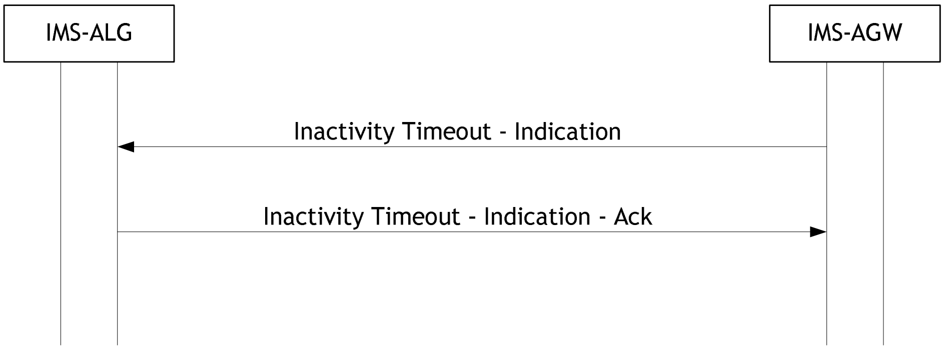


Figure 6.1.13.2: Inactivity Timeout - Indication

If no Inactivity Timeout – Indication Ack reply is received, the IMS-AGW shall consider the IMS-ALG to have failed. The IMS-AGW may then attempt to re-contact its controlling IMS-ALG by performing IMS-AGW Communication Up. If not successful, the IMS-AGW may then attempt to register to a new IMS-ALG.

6.1.14 Realm Availability Monitoring

If the IMS-AGW supports IP Realm Availability monitoring, the IMS-ALG may request the monitoring of the available IP Realms by the IMS-AGW; the IMS-AGW shall inform the IMS-ALG of any changes in realm availability.

NOTE: The IMS-ALG can use the AuditValue procedure to determine which IP realms are currently available.

The IMS-ALG may use the Realm Availability - Activate procedure towards the IMS-AGW to request the IMS-AGW to monitor the status of its IP Realms.

Figure 6.1.14.1: Realm Availability - Activate

The IMS-AGW shall inform the IMS-ALG via the Realm Availability – Notification procedure.

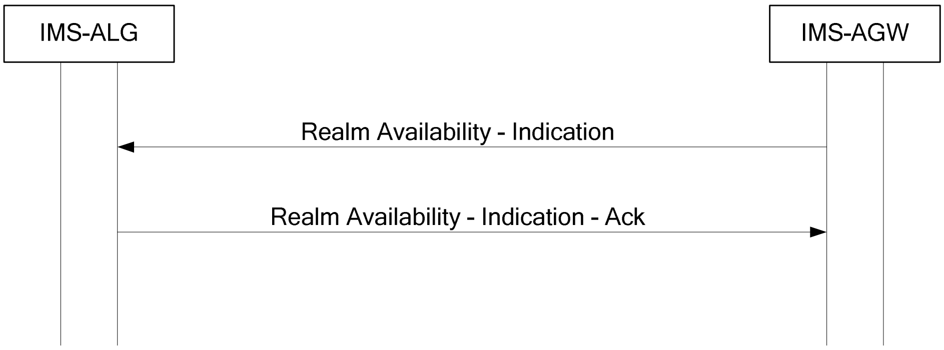


Figure 6.1.14.2: Realm Availability - Indication

On being informed of newly available/unavailable realms, IMS-ALG shall take appropriate action (e.g. update its list of available realms etc.).

6.1.15 Failure of IP Port, Interface or Group of Interfaces

This procedure only applies when text encoding is used on the H.248 interface.

The IMS-ALG shall and the IMS-AGW may support the Termination Out-of-Service procedure.

If the IMS AGW suffers a loss of physical IP device(s) that pertain to a whole IP Realm it may report the IP Realm as unavailable (see subclause 6.1.14). However, it is possible that a failure affects a physical port or group of ports that forms a subset of the IP Realm and therefore many terminations are affected. In such cases the IMS-AGW may initiate a Termination Out of Service procedure to inform the IMS-ALG that the set of terminations is out of service. This is shown in Figure 6.1.15.1.

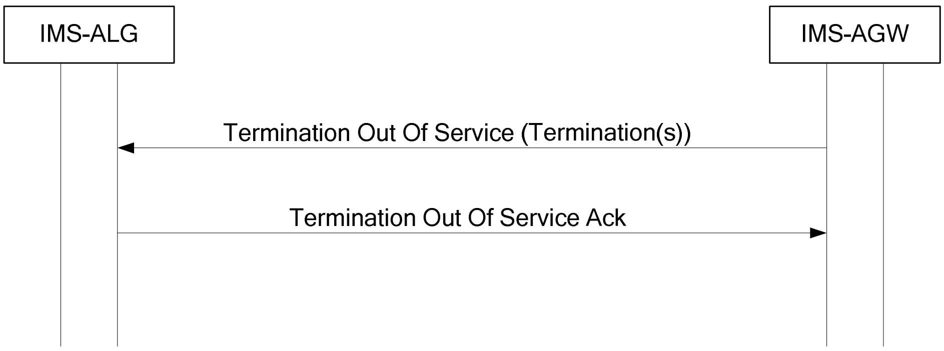


Figure 6.1.15.1: Termination Out of Service

On receipt of the Termination Out Of Service the IMS-ALG shall initiate the appropriate actions, e.g. by subtracting the affected terminations and releasing the affected calls.

NOTE: This procedure provides an alternative failure reporting to the IP Bearer Released procedure (which allows reporting the failure of one IP Bearer / termination). The Termination Out-of-Service procedure avoids sending an avalanche of notifications when the failure affects multiple ephemeral terminations.

6.2 Call Related Procedures

6.2.1 Gate Control & Local NA(P)T procedure

The session establishment and session release procedures are specified in 3GPP TS 23.228 [2] Annex G.4.3 and G.4.

Figure 6.2.1.2 depicts the signalling flow for a session setup from the IMS access network towards the IMS core network when the P-CSCF invokes the IMS-ALG function for a session. The same signalling flow applies for a session setup from the IMS core network towards the IMS access network with the exception that terminations T1 and T2 are then exchanged.

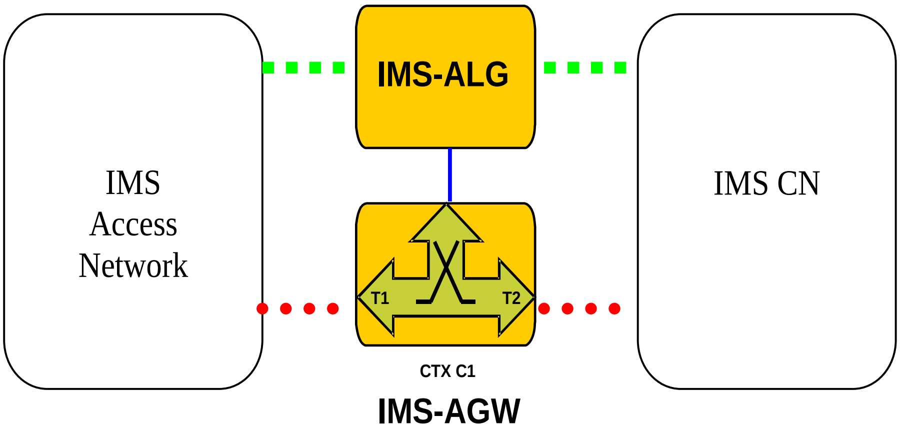


Figure 6.2.1.1: H.248 Context Model

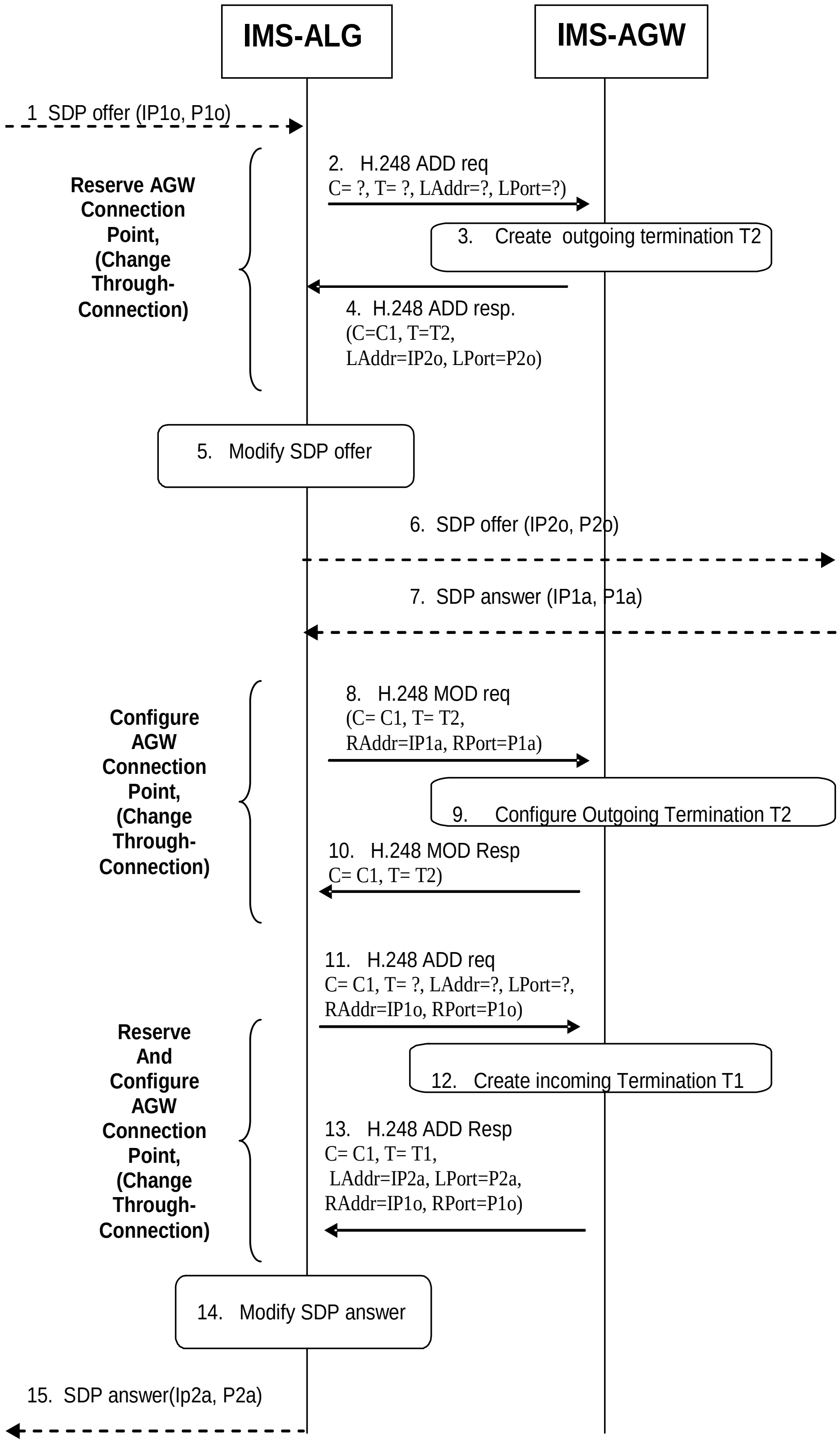


Figure 6.2.1.2: IMS-ALG and IMS-AGW interaction at session establishment

Upon receipt of a session initiation request, the IMS-ALG shall extract the offerer's destination network address(es) and port number(s) from the signalling message body received from the calling party endpoint. It shall then request the IMS-AGW to allocate transport resources (T2) via the Reserve AGW Connection Point procedure. Upon receipt of the response from the IMS-AGW, the IMS-ALG shall modify the offerer's destination address(es) and/or port(s) contained in the application signalling message body and propagate the session establishment toward the terminating party.

On receipt of the terminating end SDP in the session establishment response, the IMS-ALG shall pass the information to the IMS-AGW in the Configure AGW Connection Point procedure and shall request the IMS-AGW to allocate transport resources (T1) via the Reserve and Configure AGW Connection Point. Upon receiving the response from the IMS-AGW, the IMS-ALG shall modify the answerer's destination address(es) and/or port(s) contained in the application signalling message body and pass the information to the originating party.

On session termination, the IMS-ALG shall request the IMS-AGW to release its transport resources via the Release AGW Termination procedure.

6.2.2 IP realm indication procedure

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG optionally specifying the required IP Realm to the IMS-AGW when requesting the allocation of transport resources on the IMS-AGW.

6.2.3 Remote NA(P)T traversal support procedure

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG optionally indicating to the IMS-AGW that the remote media address/port information (supplied by the IMS-ALG) shall not be used as the destination address for outgoing media. Instead, the IMS-AGW shall "latch" or "relatch" onto the required destination address via the source address/port of the incoming media. The IMS-ALG may command the IMS-AGW to latch once (on the first received packet) or to re-latch (i.e. to check for a change of source address on the incoming media stream and latch once on this new address).

6.2.4 Remote Source Address/Port Filtering

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG optionally specifying the required IP address and/or port to be used to screen received media packets on a termination.

This subclause considers when the IMS-ALG is acting as an Entry point and remote source transport address filtering is required towards the external network.

As a security related option, on request from the IMS-ALG, filtering may be enabled to check/validate the source address or source address and port number of incoming packets from the external network. If the IMS-ALG requests address filtering, it may additionally provide an address specification, which may identify either a single address or a range of addresses, against which filtering is to be performed. The absence of such an address specification in the request shall implicitly request filtering against the IP address of the remote connection address. In addition to address filtering, the IMS-ALG may also request port filtering. If the IMS-ALG requests port filtering, it may additionally include either a port or a range of ports, against which filtering is to be performed. The absence of a port specification in the request shall implicitly request filtering against the port of the remote connection address.

If the IMS-AGW is requested to apply source IP address and possibly source port filtering, it shall only pass incoming IP packets from the identified source, and discard IP packets from other sources.

If remote source address filtering is required for the created termination, then the IMS-ALG shall include the information element "Remote source address filtering" in the request sent to the IMS-AGW. In addition, it may also include the information element "Remote source address mask" in order to request filtering of a range of addresses.

If remote source port filtering is required for the created termination (in addition to remote source address filtering), then the IMS-ALG shall include the information element "Remote source port filtering" in the request sent to the IMS-AGW. It may also include one of the information elements "Remote source port" or "Remote source port range".

Subsequently, the IMS-AGW shall apply filtering as requested to the packets arriving from the external network. Any packet arriving, which does not meet the filtering requirement, shall be discarded.

6.2.5 Traffic Policing

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG optionally requesting the IMS-AGW to police the media stream flow according to one or more of the following media policing(s) through the IMS-AGW, in accordance with IETF RFC 2216 [10].

The following media policing shall be supported at the IMS-AGW:

- **Sustainable Data Rate (SDR) Policing:**
  To request policing of the sustainable data rate of a media stream, the IMS-ALG shall request media policing for that media stream and shall provide the sustainable data rate, and shall provide a maximum burst size (MBS) indicating the expected maximum size of packet bursts for that media stream. The IMS-AGW shall then measure the data rate for the received packets within that media stream as per IETF RFC 2216 [10] for "Token Bucket", where r = SDR and b = MBS. If the permissible sustainable data rate is exceeded, the IMS-AGW shall discard packets to reduce the data rate to the permissible sustainable data rate.

NOTE 1: The IMS-ALG can derive the sustainable data rate from bandwidth parameters if it receives them within an SDP description.

The following media policing may be supported in addition at the IMS-AGW ; if supported then the following applies:

- **Peak Data Rate Policing**:
  To request policing of the peak data rate of a media stream, the IMS-ALG shall request media policing for that media stream and shall provide the peak data rate, and may provide a Delay Variation Tolerance indicating the expected maximum delay variation due to jitter for that media stream. The IMS-AGW shall then measure the data rate for the received packets within that media stream. If the permissible peak data rate is exceeded, the IMS-AGW shall discard packets to reduce the data rate to the permissible peak data rate. If both peak data rate and sustainable data rate have been provided for the same media stream, the IMS-AGW shall discard packets to reduce the data rate to the permissible peak data rate and should discard packets to reduce the data rate to the permissible sustainable data rate.

NOTE 2: The decision to apply or not traffic policing is general for all sessions with the same media characteristics (i.e. not user specific). The conditions which media policings to apply are beyond the scope of the specification. This can be based on the media characteristics of the session (e.g. media type).

6.2.6 Hanging Termination Detection

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG requesting the IMS-AGW to periodically report termination heartbeat indications to detect hanging context and termination in the IMS-AGW that may result e.g. from a loss of communication between the IMS-ALG and the IMS-AGW.

When the IMS-ALG receives a termination heartbeat notification from the IMS-AGW via the Termination heartbeat - Indication procedure, the IMS-ALG shall return a Termination heartbeat –Indication Ack (without an error) if the context id / termination identity combination exists in the IMS-ALG. If it does not exist, the IMS-ALG shall return an error and shall correct the mismatch, e.g. by requesting the IMS-AGW to subtract the indicated termination and to clear any associated context.

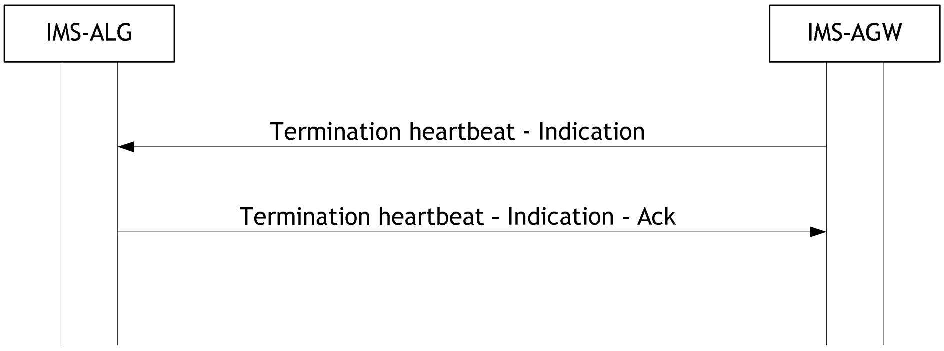


Figure 6.2.6.1: Termination heartbeat – Indication

6.2.7 QoS Packet Marking

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG optionally specifying the setting of the DSCP for outgoing packets on a termination. The DSCP value may be explicitly set by the IMS-AGW or else copied from that received in the corresponding received packet.

If differentiated services are required for the created termination, then the IMS-ALG shall include the information elements "DiffServ Code Point" and/or "DiffServ Tagging Behaviour" in the request sent to the IMS-AGW.

Subsequently, for all egress packets, the IMS-AGW shall set the DiffServ Code Point in the IP header as specified by the IMS-ALG:

- If the DiffServ Tagging Behaviour information element was received with a value to indicate that the DiffServ Code Point should be copied, then the DiffServ Code Point in the IP header of the egress packet is copied from the ingress packet.
- If the Diffserv Tagging Behaviour information element was not received, or was received with a value to indicate that the DiffServ Code Point should be set to a specific value, then:
  - If the DiffServ Code Point information element was received, then the DiffServ Code Point in the IP header of the egress packet shall be set to the value received in the DiffServ Code Point information element.
  - If the DiffServ Code Point information element was not received, then the DiffServ Code Point in the IP header of the egress packet shall be set to a configured default value.

6.2.8 Media Inactivity Detection

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG optionally requesting the IMS-AGW to detect inactive media.

If media inactivity detection is required for the created termination, the IMS-ALG may include the information elements "Inactivity detection time" and "Inactivity detection direction" in the request sent to the IMS-AGW. The IMS-ALG may request the detection of media inactivity on a termination or a stream basis.

When the IMS-ALG receives a notification of inactive media from the IMS-AGW via the Media Inactivity Notification procedure, the IMS-ALG shall return a Media Inactivity Notification Ack and shall take appropriate action (e.g. release the termination).

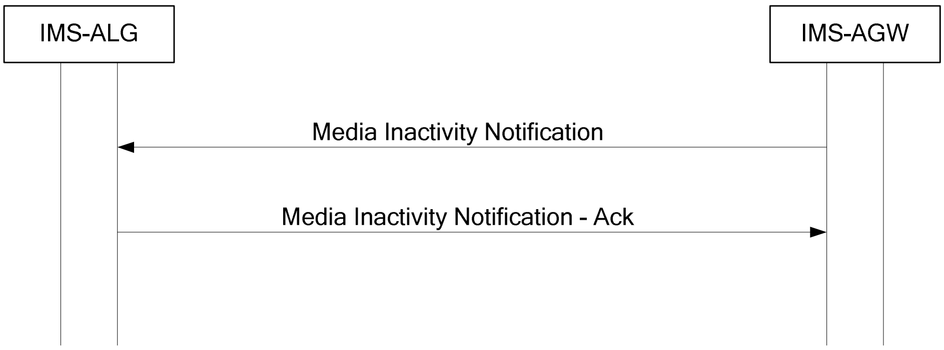


Figure 6.2.8.1: Media Inactivity Notification

6.2.9 Handling of RTCP streams

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG optionally requesting the IMS-AGW to allocate or not allocate RTCP resources, and if RTCP is requested, optionally specifying the remote RTCP port and address, and bandwidth allocation for RTCP.

6.2.10 IMS end-to-access-edge Media Plane Security

6.2.10.1 General

All message sequence charts in this clause are examples.

The H.248 context model is defined in Figure 6.2.1.1.

6.2.10.2 End-to-access-edge security for RTP based media using SDES

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG optionally requesting the IMS-AGW to provide IMS media plane security in accordance with 3GPP TS 33.328 [12].

The IMS-ALG shall provide the following media plane security related parameters to the IMS-AGW:

- the SDES crypto attributes

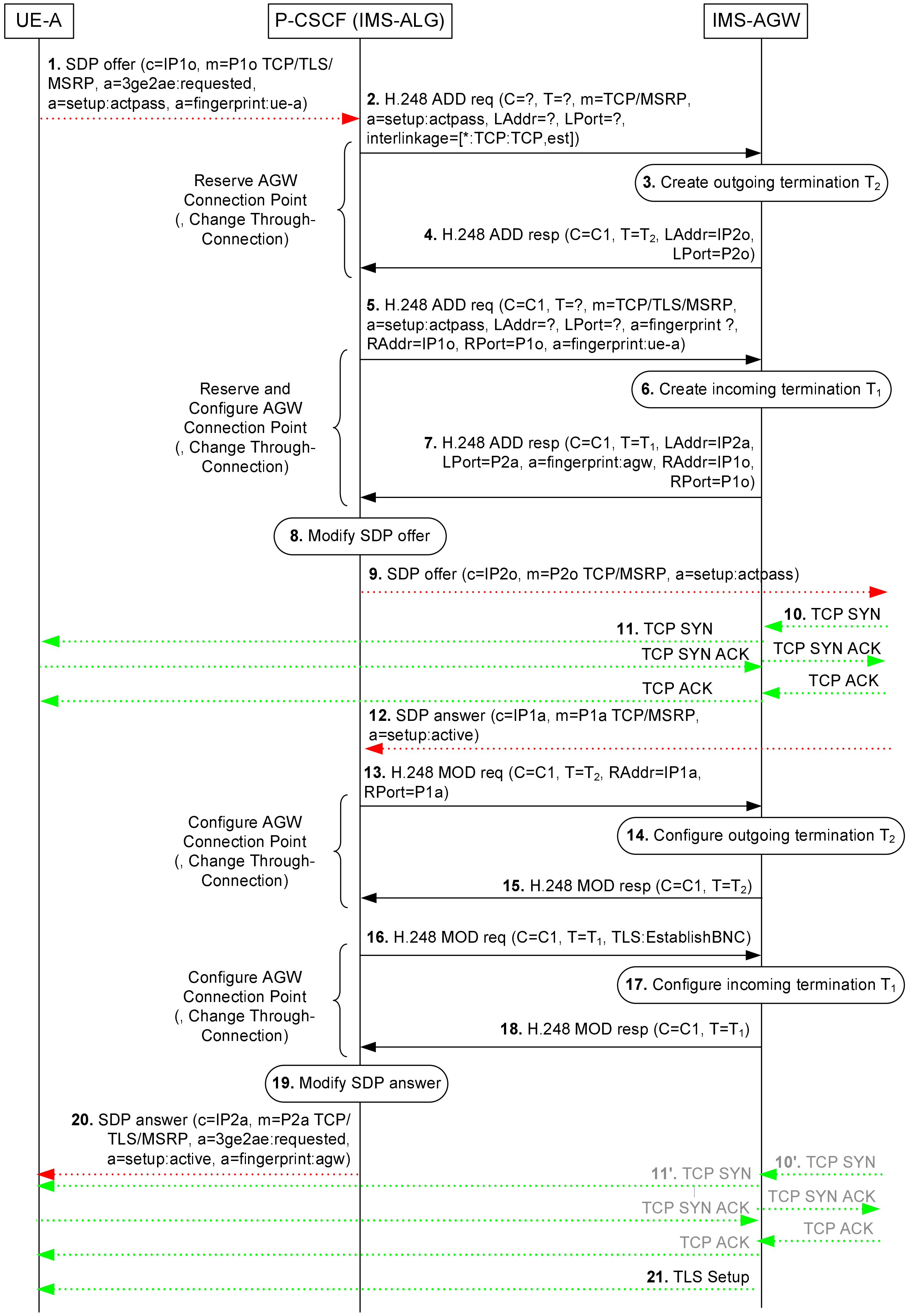
6.2.10.3 End-to-access-edge security for TCP-based media using TLS

6.2.10.3.1 End-to-access-edge security for session based messaging (MSRP)

6.2.10.3.1.1 IMS UE originating procedures for e2ae

6.2.10.3.1.1.1 Incoming TCP bearer establishment triggers an outgoing TCP bearer establishment

Figure 6.2.10.3.1.1.1.1 shows an example call flow for the originating session set-up procedures for one MSRP media stream using e2ae security, where an incoming TCP bearer establishment triggers an outgoing TCP bearer establishment.



UE-A
P-CSCF (IMS-ALG)
IMS-AGW
1. SDP offer (c=IP1o, m=P1o TCP/TLS/MSRP, a=3ge2ae:requested, a=setup:actpass, a=fingerprint:ue-a)
2. H.248 ADD req (C=?, T=?, m=TCP/MSRP, a=setup:actpass, LAddr=?, LPort=?, interlinkage=[*:TCP:TCP,est])
Reserve AGW Connection Point (, Change Through-Connection)
3. Create outgoing termination T_2
4. H.248 ADD resp (C=C1, T=T_2, LAddr=IP2o, LPort=P2o)
5. H.248 ADD req (C=C1, T=?, m=TCP/TLS/MSRP, a=setup:actpass, LAddr=?, LPort=?, a=fingerprint ?, RAddr=IP1o, RPort=P1o, a=fingerprint:ue-a)
Reserve and Configure AGW Connection Point (, Change Through-Connection)
6. Create incoming termination T_1
7. H.248 ADD resp (C=C1, T=T_1, LAddr=IP2a, LPort=P2a, a=fingerprint:agw, RAddr=IP1o, RPort=P1o)
8. Modify SDP offer
9. SDP offer (c=IP2o, m=P2o TCP/MSRP, a=setup:actpass)
10. TCP SYN
11. TCP SYN
TCP SYN ACK
TCP SYN ACK
TCP ACK
TCP ACK
12. SDP answer (c=IP1a, m=P1a TCP/MSRP, a=setup:active)
13. H.248 MOD req (C=C1, T=T_2, RAddr=IP1a, RPort=P1a)
Configure AGW Connection Point (, Change Through-Connection)
14. Configure outgoing termination T_2
15. H.248 MOD resp (C=C1, T=T_2)
16. H.248 MOD req (C=C1, T=T_1, TLS:EstablishBNC)
Configure AGW Connection Point (, Change Through-Connection)
17. Configure incoming termination T_1
18. H.248 MOD resp (C=C1, T=T_1)
19. Modify SDP answer
20. SDP answer (c=IP2a, m=P2a TCP/TLS/MSRP, a=3ge2ae:requested, a=setup:active, a=fingerprint:agw)
10'. TCP SYN
11'. TCP SYN
TCP SYN ACK
TCP SYN ACK
TCP ACK
TCP ACK
21. TLS Setup

Figure 6.2.10.3.1.1.1.1: Originating example call flow for e2ae security for MSRP where an incoming TCP bearer establishment triggers an outgoing TCP bearer establishment

The IMS UE A performs an IMS originating session set-up according to 3GPP TS 23.228 [2], with modifications as described in 3GPP TS 33.328 [12].

The procedure in the above figure for requesting e2ae security for a media stream is described step-by-step with an emphasis on the additional aspects for IMS-ALG and IMS-AGW of media protection using TLS.

1. IMS UE A sends an SDP offer for a media stream containing cryptographic information, together with an "a=3ge2ae:requested" SDP attribute for the MSRP-related SDP m-line, to the P-CSCF (IMS-ALG). For e2ae protection of MSRP the cryptographic information contained in the SDP offer consists of the fingerprint of the certificate of IMS UE A in accordance to IETF RFC 4975 [25]. For each media stream that uses transport "TCP/TLS/MSRP", the P-CSCF (IMS-ALG) checks for the presence of the "a=3ge2ae:requested" SDP attribute. If that indication is present and the P-CSCF (IMS-ALG) indicated support of e2ae-security for MSRP during registration, the P-CSCF (IMS-ALG) allocates the required resources, includes the IMS-AGW in the media path and proceeds as specified in this clause.

NOTE 1: An operator can choose to terminate TLS in the IMS-AGW according to the following steps for all media streams that are signalled in SIP INVITE messages with transport TCP/TLS/MSRP and a certificate fingerprint attribute, even if the UE did not indicate support for e2ae security during registration and did not indicate usage of e2ae security for the respective media streams in the INVITE. This can lead to session failures for pre-Rel-12 IMS UEs or non-IMS UEs due to a mismatch of security parameters sent by the network and expected by the UE, but on the other hand, it will ensure compatibility with GSMA RCS 5.1 [35, 36], which specifies that TLS for MSRP is always terminated in the network.

2.-4. The IMS-ALG uses the "Reserve AGW Connection Point" procedure to request a termination for "TCP" media (for application-agnostic interworking) or "TCP/MSRP" media (for application-aware interworking) towards the core network. To indicate that the IMS-AGW shall operate in TCP Proxy mode, the IMS-ALG provides "a=setup:actpass" attribute. The IMS-ALG sets the interlinkage topology on the termination T2 to configure the IMS-AGW to use the TCP connection establishment request (TCP SYN) received at the termination T2 as a trigger to send a TCP connection establishment on the termination T1.

NOTE 2: If "a=setup:passive" is received in the SDP answer in step 12, the IMS-ALG then needs to set the interlinkage topology on the termination T1 (not depicted).

5.-7. The IMS-ALG uses the "Reserve And Configure AGW Connection Point" procedure to request a termination for "TCP/TLS" media (for application-agnostic interworking) or "TCP/TLS/MSRP" media (for application-aware interworking) towards the access network. In the remote descriptor, it provides the IP address, port and fingerprint attribute received from the UE containing the fingerprint of the UE´s certificate in accordance to IETF RFC 4975 [25]. This instructs the IMS-AGW to verify during the subsequent TLS handshake with the IMS UE that the fingerprint of the certificate passed by the IMS UE during this TLS handshake matches the fingerprint passed by the P-CSCF (IMS-ALG) to the IMS-AGW. In turn, the IMS-AGW communicates the fingerprint of the certificate it is going to use for setting up protection for this media stream to the P-CSCF (IMS-ALG). To indicate that the IMS-AGW shall operate in TCP Proxy mode, the IMS-ALG provides "a=setup:actpass" attribute.

NOTE 3: These steps could be combined with steps 16.-18. This saves H.248 signalling interactions but can delay the TCP connection setup.

8. The P-CSCF (IMS-ALG) changes the transport from "TCP/TLS/MSRP" to "TCP/MSRP" in the SDP offer, removes the "a=3ge2ae:requested" SDP attribute and the fingerprint SDP attribute, and inserts the address information received from the IMS-AGW.

9. The P-CSCF (IMS-ALG) forwards the SDP offer.

10. The remote peer chooses to become the active party in the TCP connection establishment and sends a TCP SYN to establish the TCP connection. If the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall ignore any incoming TCP connection establishment requests (TCP SYN), e.g. to enable a remote source transport address filtering, or if the P-CSCF (IMS-ALG) did not indicate to the IMS-AGW at step 2 that it shall latch onto the required destination address via the source address/port of the incoming media, the IMS-AGW shall drop the TCP SYN received from the remote peer.
If the TCP SYN is not answered before a timer expiry, the remote peer will send the TCP SYN a second time

(step 10'). The IMS-AGW will answer a repeated TCP SYN if it is received after step 13 (step 10'). The IMS-AGW answers the TCP SYN and the remote peer completes the TCP connection establishment.

11. The IMS-AGW uses the TCP SYN received at the termination T2 (at step 10 or step 10' if the TCP SYN is dropped at step 10) as a trigger to send a TCP SYN towards the UE to establish a TCP connection (effectively making the IMS-AGW acting as the TCP client towards the UE).. The UE answers the TCP SYN and the IMS-AGW completes the TCP connection establishment.

12. The P-CSCF (IMS-ALG) receives the SDP answer.

13.-15.The IMS-ALG uses the "Configure AGW Connection Point" procedure to configure the termination towards the core network with remote address information. If the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall ignore any incoming TCP connection establishment requests (TCP SYN), the IMS-ALG indicates to the IMS-AGW to accept incoming TCP connection establishment (TCP SYN) only from the indicated remote transport address.

NOTE 4: For "a=setup:active" in the SDP answer, these steps could possibly be skipped if the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall latch onto the required destination address via the source address/port of the incoming media, as the IMS-AGW will then use the address information in the TCP SYN when replying.

16.-18.The IMS-ALG uses the "Configure AGW Connection Point" procedure to configure the termination towards the access network with the request to establish the TLS session once the TCP connection is established (effectively making the IMS-AGW acting as the TLS client), in accordance with the information in the "a=setup" attribute in the SDP answer.

19. The P-CSCF (IMS-ALG) modifies the SDP answer before sending it to the UE A. The P-CSCF (IMS-ALG) sets the transport to "TCP/TLS/MSRP" and includes the fingerprint of the IMS-AGW´s certificate in accordance to IETF RFC 4975 [25].

20. The P-CSCF (IMA-ALG) then sends the updated SDP answer to IMS UE A. After receiving this message IMS UE A completes the media security setup.

21. Upon completion of the TCP connection establishment, the IMS-AGW starts the establishment of the TLS session.

6.2.10.3.1.1.2 IMS-ALG requests sending an outgoing TCP bearer establishment

Figure 6.2.10.3.1.1.2.1 shows an example call flow for the originating session set-up procedures for one MSRP media stream using e2ae security, where the IMS-ALG requests sending an outgoing TCP bearer establishment.

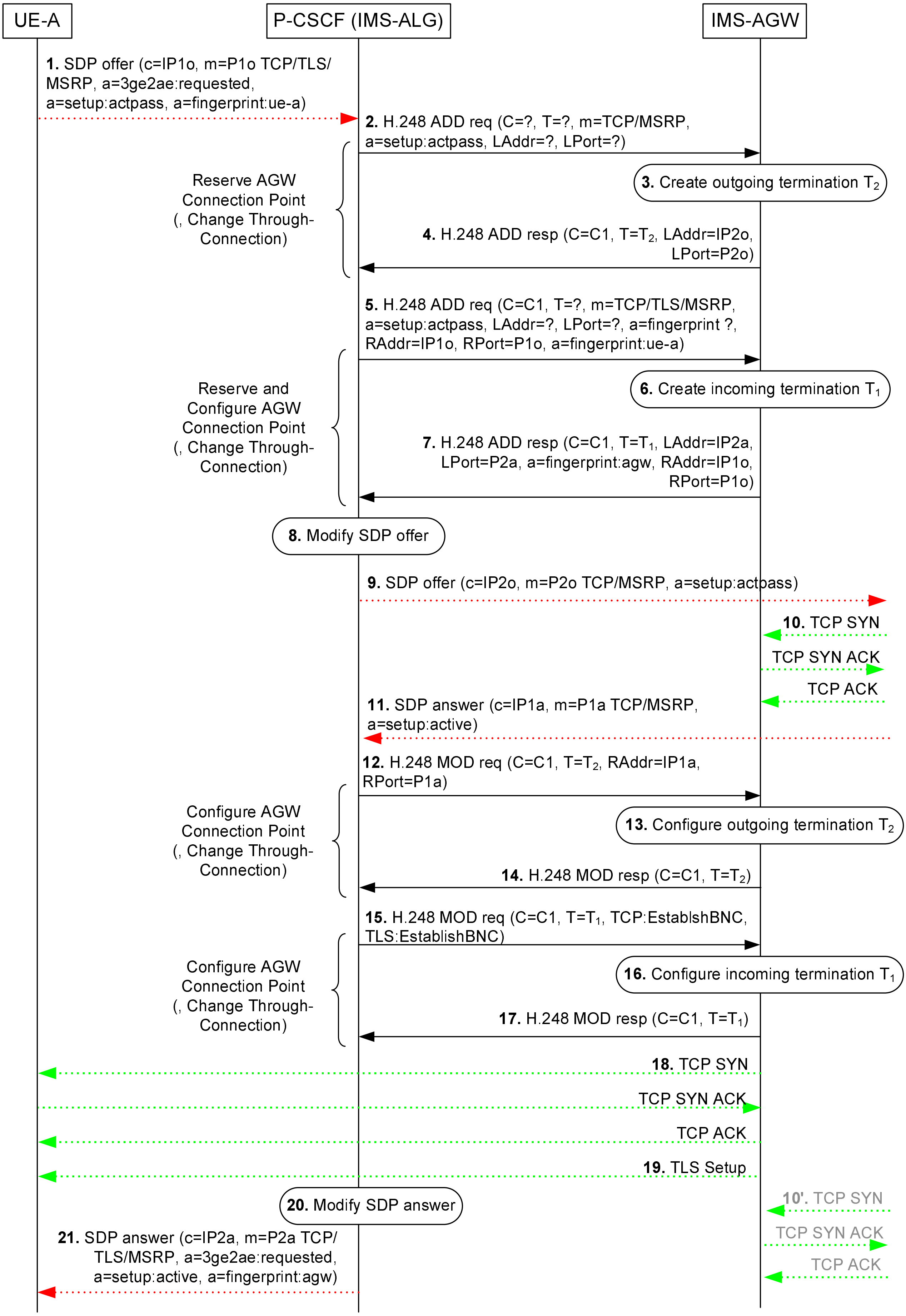

UE-A
P-CSCF (IMS-ALG)
IMS-AGW
1. SDP offer (c=IP1o, m=P1o TCP/TLS/MSRP, a=3ge2ae:requested, a=setup:actpass, a=fingerprint:ue-a)
2. H.248 ADD req (C=?, T=?, m=TCP/MSRP, a=setup:actpass, LAddr=?, LPort=?)
Reserve AGW Connection Point (, Change Through-Connection)
3. Create outgoing termination T_2
4. H.248 ADD resp (C=C1, $T=T_2$, LAddr=IP2o, LPort=P2o)
5. H.248 ADD req (C=C1, T=?, m=TCP/TLS/MSRP, a=setup:actpass, LAddr=?, LPort=?, a=fingerprint ?, RAddr=IP1o, RPort=P1o, a=fingerprint:ue-a)
Reserve and Configure AGW Connection Point (, Change Through-Connection)
6. Create incoming termination T_1
7. H.248 ADD resp (C=C1, $T=T_1$, LAddr=IP2a, LPort=P2a, a=fingerprint:agw, RAddr=IP1o, RPort=P1o)
8. Modify SDP offer
9. SDP offer (c=IP2o, m=P2o TCP/MSRP, a=setup:actpass)
10. TCP SYN
TCP SYN ACK
TCP ACK
11. SDP answer (c=IP1a, m=P1a TCP/MSRP, a=setup:active)
12. H.248 MOD req (C=C1, $T=T_2$, RAddr=IP1a, RPort=P1a)
Configure AGW Connection Point (, Change Through-Connection)
13. Configure outgoing termination T_2
14. H.248 MOD resp (C=C1, $T=T_2$)
15. H.248 MOD req (C=C1, $T=T_1$, TCP:EstablshBNC, TLS:EstablishBNC)
Configure AGW Connection Point (, Change Through-Connection)
16. Configure incoming termination T_1
17. H.248 MOD resp (C=C1, $T=T_1$)
18. TCP SYN
TCP SYN ACK
TCP ACK
19. TLS Setup
10'. TCP SYN
TCP SYN ACK
TCP ACK
20. Modify SDP answer
21. SDP answer (c=IP2a, m=P2a TCP/TLS/MSRP, a=3ge2ae:requested, a=setup:active, a=fingerprint:agw)

Figure 6.2.10.3.1.1.2.1: Originating example call flow for e2ae security for MSRP where the IMS-ALG requests sending an outgoing TCP bearer establishment

The IMS UE A performs an IMS originating session set-up according to 3GPP TS 23.228 [2], with modifications as described in 3GPP TS 33.328 [12].

The procedure in the above figure for requesting e2ae security for a media stream is described step-by-step with an emphasis on the additional aspects for IMS-ALG and IMS-AGW of media protection using TLS.

1. As step 1 in figure 6.2.10.3.1.1.1.1.

2.-4. As steps 2-4 in figure 6.2.10.3.1.1.1.1 with the exception that the IMS-ALG does not set the interlinkage topology on the termination T2.

5.-7. As steps 5-7 in figure 6.2.10.3.1.1.1.1.

8. As step 8 in figure 6.2.10.3.1.1.1.1.

9. As step 9 in figure 6.2.10.3.1.1.1.1.

10. As step 10 in figure 6.2.10.3.1.1.1.1.

NOTE: The incoming TCP SYN does not trigger the sending of an outgoing TCP SYN, and step 11 in figure 6.2.10.3.1.1.1.1thus does not apply.

11. As step 12 in figure 6.2.10.3.1.1.1.1.

12.-14. As steps 13-15 in figure 6.2.10.3.1.1.1.1.

15.-17. As steps 16-18 in figure 6.2.10.3.1.1.1.1with the exception that the IMS-ALG uses the "Configure AGW Connection Point" procedure also to configure the termination towards the access network with the request to establish the TCP connection (effectively making the IMS-AGW acting as the TCP client), in accordance with the information in the "a=setup" attribute in the SDP answer.

18. The IMS-AGW sends a TCP SYN towards the UE to establish a TCP connection. The UE answers with a TCP SYN ACK and the IMS-AGW replies with a TCP ACK, completing the TCP connection establishment.

19. As step 21 in figure 6.2.10.3.1.1.1.1.

20. As step 19 in figure 6.2.10.3.1.1.1.1.

21. As step 20 in figure 6.2.10.3.1.1.1.1.

6.2.10.3.1.2 IMS UE terminating procedures for e2ae

6.2.10.3.1.2.1 Incoming TCP bearer establishment triggers an outgoing TCP bearer establishment

Figure 6.2.10.3.1.2.1.1 shows an example call flow for the terminating session set-up procedures for one MSRP media stream using e2ae security, where an incoming TCP bearer establishment triggers an outgoing TCP bearer establishment.

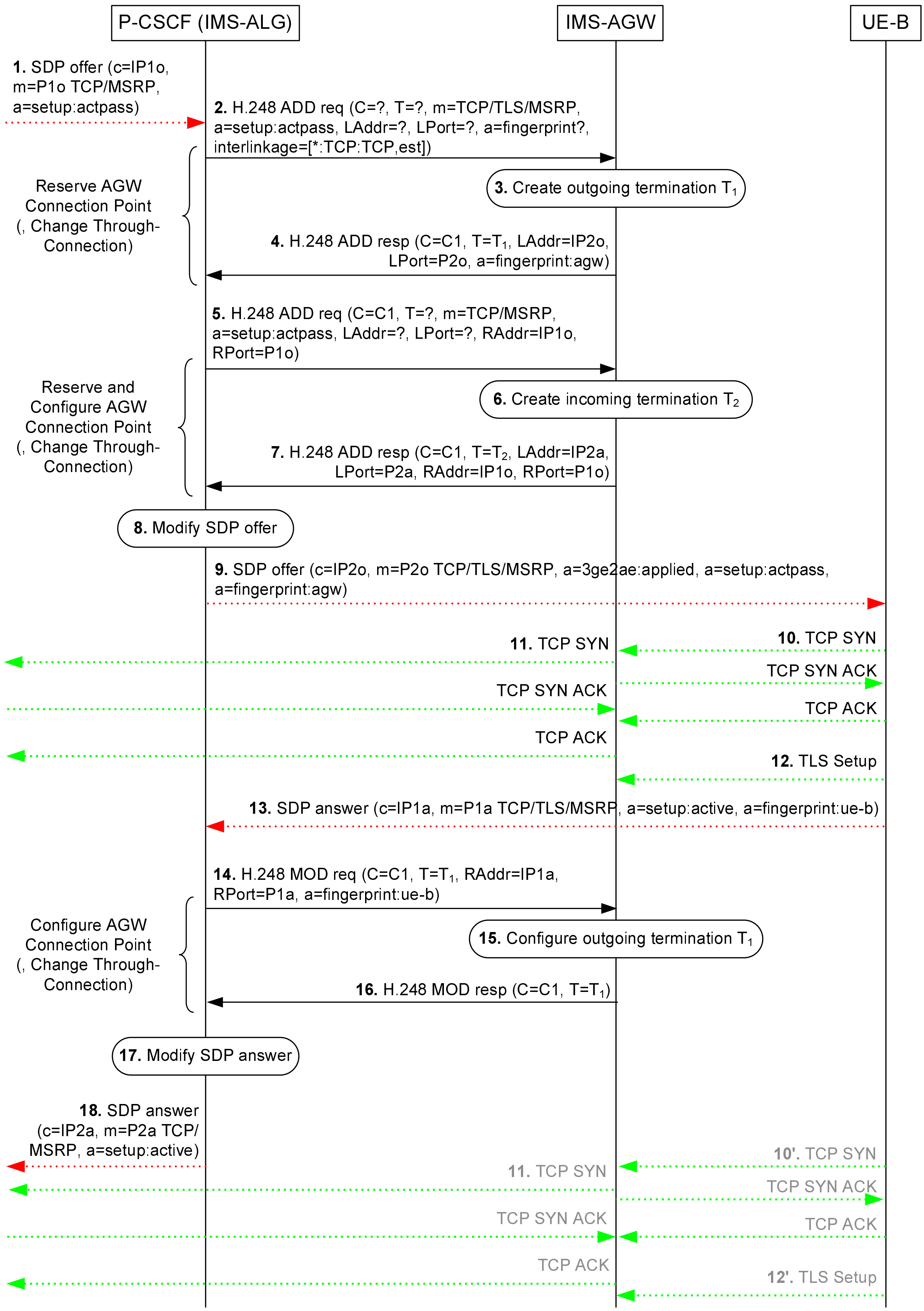

P-CSCF (IMS-ALG)
IMS-AGW
UE-B
1. SDP offer (c=IP1o, m=P1o TCP/MSRP, a=setup:actpass)
2. H.248 ADD req (C=?, T=?, m=TCP/TLS/MSRP, a=setup:actpass, LAddr=?, LPort=?, a=fingerprint?, interlinkage=[*:TCP:TCP,est])
Reserve AGW Connection Point (, Change Through-Connection)
3. Create outgoing termination T_1
4. H.248 ADD resp (C=C1, $T=T_1$, LAddr=IP2o, LPort=P2o, a=fingerprint:agw)
5. H.248 ADD req (C=C1, T=?, m=TCP/MSRP, a=setup:actpass, LAddr=?, LPort=?, RAddr=IP1o, RPort=P1o)
Reserve and Configure AGW Connection Point (, Change Through-Connection)
6. Create incoming termination T_2
7. H.248 ADD resp (C=C1, $T=T_2$, LAddr=IP2a, LPort=P2a, RAddr=IP1o, RPort=P1o)
8. Modify SDP offer
9. SDP offer (c=IP2o, m=P2o TCP/TLS/MSRP, a=3ge2ae:applied, a=setup:actpass, a=fingerprint:agw)
10. TCP SYN
11. TCP SYN
TCP SYN ACK
TCP SYN ACK
TCP ACK
TCP ACK
12. TLS Setup
13. SDP answer (c=IP1a, m=P1a TCP/TLS/MSRP, a=setup:active, a=fingerprint:ue-b)
14. H.248 MOD req (C=C1, $T=T_1$, RAddr=IP1a, RPort=P1a, a=fingerprint:ue-b)
Configure AGW Connection Point (, Change Through-Connection)
15. Configure outgoing termination T_1
16. H.248 MOD resp (C=C1, $T=T_1$)
17. Modify SDP answer
18. SDP answer (c=IP2a, m=P2a TCP/MSRP, a=setup:active)
10'. TCP SYN
11. TCP SYN
TCP SYN ACK
TCP SYN ACK
TCP ACK
TCP ACK
12'. TLS Setup

Figure 6.2.10.3.1.2.1.1: Terminating example call flow for e2ae security for MSRP where an incoming TCP bearer establishment triggers an outgoing TCP bearer establishment

The IMS UE B performs an IMS terminating session set-up according to 3GPP TS 23.228 [2], with modifications as described in 3GPP TS 33.328 [12].

The procedure in the above figure for requesting e2ae security for a media stream is described step-by-step with an emphasis on the additional aspects for IMS-ALG and IMS-AGW of media protection using TLS.

1. The P-CSCF (IMS-ALG) receives an SDP offer for an MSRP media stream. For each MSRP media stream offered with transport "TCP/MSRP", if both the IMS UE and P-CSCF (IMS-ALG) indicated support for e2ae-security for MSRP during registration, the P-CSCF (IMS-ALG) allocates the required resources, includes the IMS-AGW in the media path and proceeds as specified in this clause.

NOTE 1: An operator can choose to terminate TLS in the IMS-AGW according to the following steps for all media streams that are signalled in SIP INVITE messages with transport TCP/MSRP, even if the UE did not indicate support for e2ae security during registration. This can lead to session failures for pre-Rel-12 IMS UEs or non-IMS UEs due to a mismatch of security parameters sent by the network and expected by the UE, but on the other hand, it will ensure compatibility with GSMA RCS 5.1 [35, 36], which recommends to always use e2ae security for MSRP on the terminating leg.

2.-4. The IMS-ALG uses the "Reserve AGW Connection Point" procedure to request a termination for "TCP/TLS" media (for application-agnostic interworking) or "TCP/TLS/MSRP" media (for application-aware interworking) towards the access network. In turn, the IMS-AGW communicates the fingerprint of the certificate it is going to use for setting up protection for this media stream to the P-CSCF (IMS-ALG). To indicate that the IMS-AGW shall operate in TCP Proxy mode, the IMS-ALG provides "a=setup:actpass" attribute. The IMS-ALG sets the interlinkage topology on the termination T1 to configure the IMS-AGW to use the TCP connection establishment request (TCP SYN) received at the termination T1 as a trigger to send a TCP connection establishment on the termination T2.

NOTE 2: If "a=setup:passive" is received in the SDP answer in step 13, the IMS-ALG then needs to sets the interlinkage topology on the termination T2 (not depicted)

5.-7. The IMS-ALG uses the "Reserve And Configure AGW Connection Point" procedure to request a termination for "TCP" media (for application-agnostic interworking) or "TCP/ MSRP" media (for application-aware interworking) towards the core network. To indicate that the IMS-AGW shall operate in TCP Proxy mode, the IMS-ALG provides "a=setup:actpass" attribute.

8. The P-CSCF (IMS-ALG) changes the transport from "TCP/ MSRP" to "TCP/TLS/MSRP" in the SDP offer, adds the "a=3ge2ae:applied" SDP attribute and the fingerprint SDP attribute received from the IMS-AGW, and inserts the address information received from the IMS-AGW.

9. The P-CSCF (IMS-ALG) forwards the SDP offer.

10. The UE B chooses to become the active party in the TCP connection establishment and sends a TCP SYN to establish the TCP connection. If the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall ignore any incoming TCP connection establishment requests (TCP SYN), e.g. to enable a remote source transport address filtering, or if the P-CSCF (IMS-ALG) did not indicate to the IMS-AGW at step 2 that it shall latch onto the required destination address via the source address/port of the incoming media, the IMS-AGW shall drop the TCP SYN received from the UE.
If the TCP SYN is not answered before a timer expiry, the UE will send the TCP SYN a second time (step 10'). The IMS-AGW will answer a repeated TCP SYN if it is received after step 14 (step 10').
The IMS-AGW answers the TCP SYN and the remote peer completes the TCP connection establishment.

11. The IMS-AGW uses the TCP SYN received at the termination T1 (at step 10 or step 10' if the TCP SYN is dropped at step 10) as a trigger to send a TCP SYN towards the core network to establish a TCP connection (effectively making the IMS-AGW acting as the TCP client towards the core network). The remote peer answers the TCP SYN and the IMS-AGW completes the TCP connection establishment.

12. Upon completion of the TCP connection establishment, the UE B starts the establishment of the TLS session. The IMS-AGW needs to wait until step 14 to verify the received fingerprint.

13. The P-CSCF (IMS-ALG) receives the SDP answer. It contains the fingerprint attribute with the UE´s certificate in accordance to IETF RFC 4975 [25].

14.-16. The IMS-ALG uses the "Configure AGW Connection Point" procedure to configure the termination towards the UE B with remote address information. In the remote descriptor, it also provides fingerprint attribute received from the UE. This instructs the IMS-AGW to verify during the subsequent TLS handshake with the IMS UE that the fingerprint of the certificate passed by the IMS UE during this TLS handshake matches the fingerprint passed by the P-CSCF (IMS-ALG) to the IMS-AGW. If the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall ignore any incoming TCP connection establishment requests (TCP SYN), the IMS-ALG indicates to the IMS-AGW to accept incoming TCP connection establishment (TCP SYN) only from the indicated remote transport address.

17. The P-CSCF (IMS-ALG) modifies the SDP answer before sending it to the core network. The P-CSCF (IMS-ALG) sets the transport to "TCP/ MSRP" and removes the SDP fingerprint attribute.

18. The P-CSCF (IMA-ALG) then sends the updated SDP answer to core network.

6.2.10.3.1.2.2 IMS-ALG requests sending an outgoing TCP bearer establishment

Figure 6.2.10.3.1.2.2.1 shows an example call flow for the terminating session set-up procedures for one MSRP media stream using e2ae security, where the IMS-ALG requests sending an outgoing TCP bearer establishment.

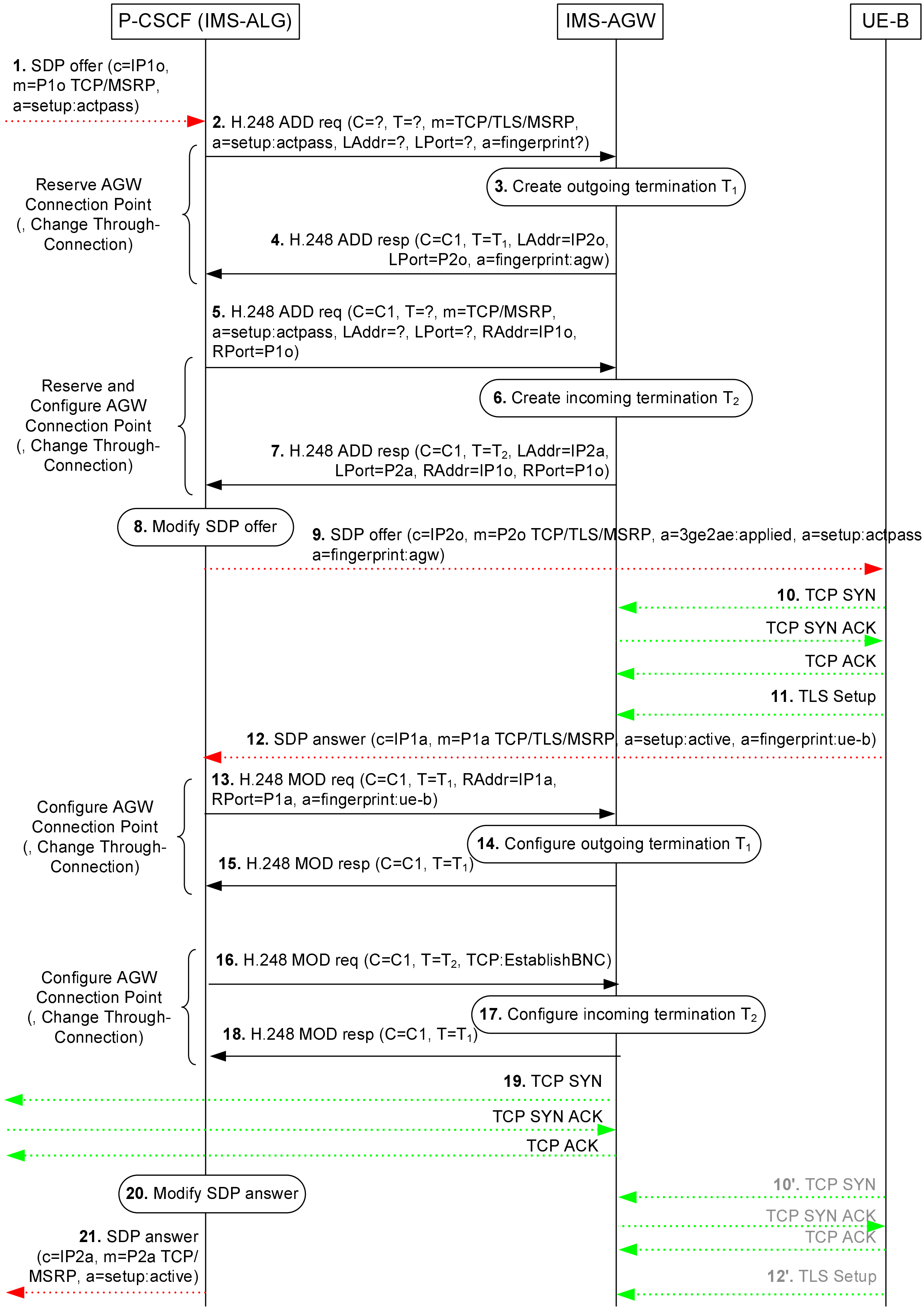

P-CSCF (IMS-ALG)
IMS-AGW
UE-B
1. SDP offer (c=IP1o, m=P1o TCP/MSRP, a=setup:actpass)
2. H.248 ADD req (C=?, T=?, m=TCP/TLS/MSRP, a=setup:actpass, LAddr=?, LPort=?, a=fingerprint?)
Reserve AGW Connection Point (, Change Through-Connection)
3. Create outgoing termination T1
4. H.248 ADD resp (C=C1, T=T1, LAddr=IP2o, LPort=P2o, a=fingerprint:agw)
5. H.248 ADD req (C=C1, T=?, m=TCP/MSRP, a=setup:actpass, LAddr=?, LPort=?, RAddr=IP1o, RPort=P1o)
Reserve and Configure AGW Connection Point (, Change Through-Connection)
6. Create incoming termination T2
7. H.248 ADD resp (C=C1, T=T2, LAddr=IP2a, LPort=P2a, RAddr=IP1o, RPort=P1o)
8. Modify SDP offer
9. SDP offer (c=IP2o, m=P2o TCP/TLS/MSRP, a=3ge2ae:applied, a=setup:actpass a=fingerprint:agw)
10. TCP SYN
TCP SYN ACK
TCP ACK
11. TLS Setup
12. SDP answer (c=IP1a, m=P1a TCP/TLS/MSRP, a=setup:active, a=fingerprint:ue-b)
13. H.248 MOD req (C=C1, T=T1, RAddr=IP1a, RPort=P1a, a=fingerprint:ue-b)
Configure AGW Connection Point (, Change Through-Connection)
14. Configure outgoing termination T1
15. H.248 MOD resp (C=C1, T=T1)
16. H.248 MOD req (C=C1, T=T2, TCP:EstablishBNC)
Configure AGW Connection Point (, Change Through-Connection)
17. Configure incoming termination T2
18. H.248 MOD resp (C=C1, T=T1)
19. TCP SYN
TCP SYN ACK
TCP ACK
20. Modify SDP answer
21. SDP answer (c=IP2a, m=P2a TCP/MSRP, a=setup:active)
10'. TCP SYN
TCP SYN ACK
TCP ACK
12'. TLS Setup

Figure 6.2.10.3.1.2.2.1: Terminating example call flow for e2ae security for MSRP where the IMS-ALG requests sending an outgoing TCP bearer establishment

The IMS UE B performs an IMS terminating session set-up according to 3GPP TS 23.228 [2], with modifications as described in 3GPP TS 33.328 [12].

The procedure in the above figure for requesting e2ae security for a media stream is described step-by-step with an emphasis on the additional aspects for IMS-ALG and IMS-AGW of media protection using TLS.

1. As step 1 in figure 6.2.10.3.1.2.1.1.

2.-4. As steps 2-4 in figure 6.2.10.3.1.2.1.1 with the exception that the IMS-ALG does not set the interlinkage topology on the termination T1.

5.-7. As steps 7-7 in figure 6.2.10.3.1.2.1.1.

8. As step 8 in figure 6.2.10.3.1.2.1.1.

9. As step 9 in figure 6.2.10.3.1.2.1.1.

10. As step 10 in figure 6.2.10.3.1.2.1.1.

NOTE: The incoming TCP SYN does not trigger the sending of an outgoing TCP SYN, and step 11 in figure 6.2.10.3.1.2.1.1 thus does not apply.

11. As step 12 in figure 6.2.10.3.1.2.1.1.

12. As step 13 in figure 6.2.10.3.1.2.1.1.

13.-15. As steps 14-16 in figure 6.2.10.3.1.2.1.1.

16.-18. The IMS-ALG uses the "Configure AGW Connection Point" procedure to configure the termination towards the core network with the request to establish the TCP connection, in accordance with the information in the "a=setup" attribute in the SDP answer.

19. The IMS-AGW sends a TCP SYN towards the core network to establish a TCP connection. The remote peer answers with a TCP SYN ACK and the IMS-AGW replies with a TCP ACK, completing the TCP connection establishment.

20. As step 17 in figure 6.2.10.3.1.2.1.1.

21. As step 18 in figure 6.2.10.3.1.2.1.1.

6.2.10.3.2 End-to-access-edge security for conferencing (BFCP)

6.2.10.3.2.1 IMS UE originating procedures for e2ae

6.2.10.3.2.1.1 Incoming TCP bearer establishment triggers an outgoing TCP bearer establishment

Figure 6.2.10.3.2.1.1.1 shows the originating session set-up procedures for one or more BFCP media stream(s) using e2ae security.

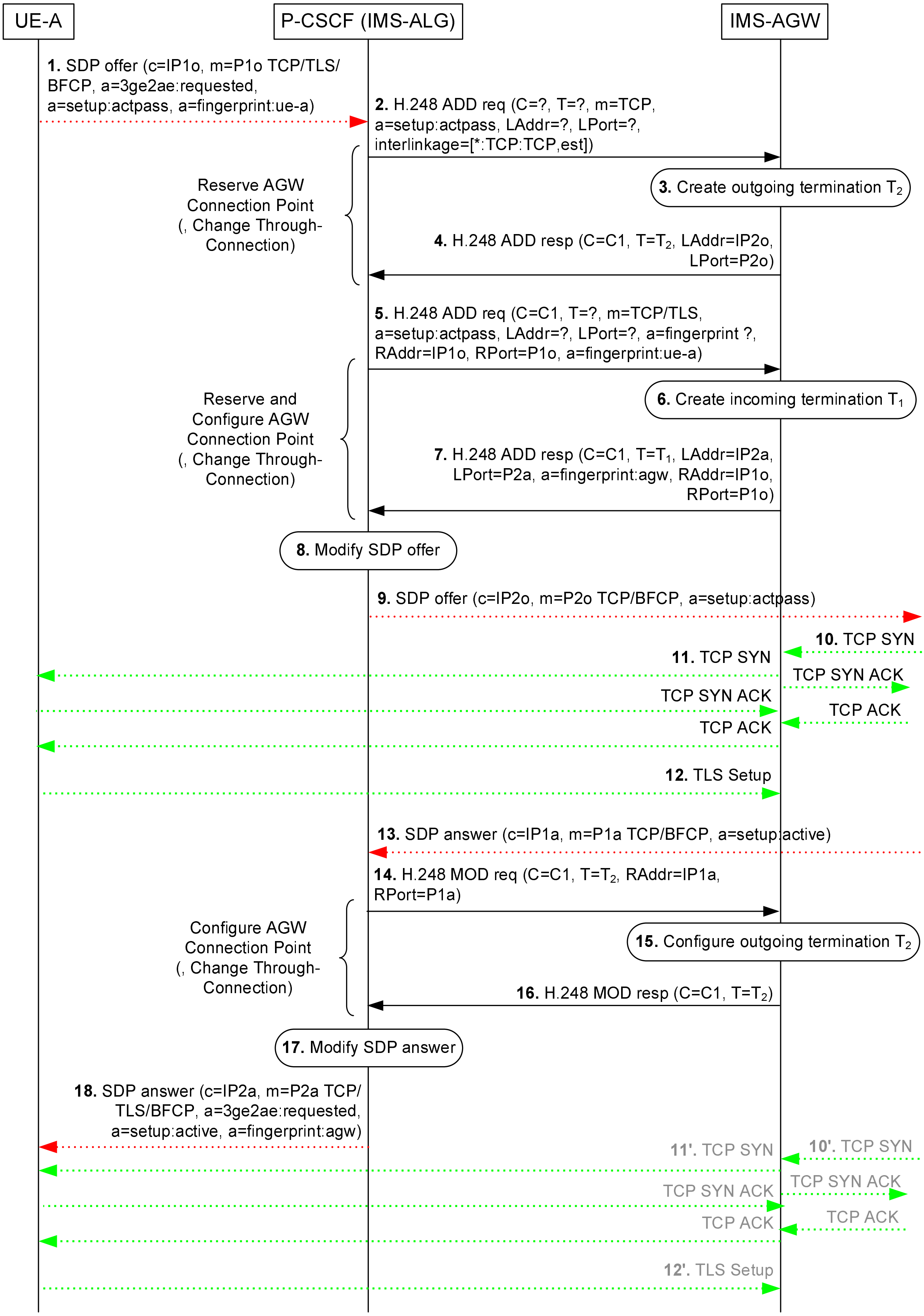

UE-A
P-CSCF (IMS-ALG)
IMS-AGW
1. SDP offer (c=IP1o, m=P1o TCP/TLS/BFCP, a=3ge2ae:requested, a=setup:actpass, a=fingerprint:ue-a)
2. H.248 ADD req (C=?, T=?, m=TCP, a=setup:actpass, LAddr=?, LPort=?, interlinkage=[*:TCP:TCP,est])
Reserve AGW Connection Point (, Change Through-Connection)
3. Create outgoing termination T_2
4. H.248 ADD resp (C=C1, $T=T_2$, LAddr=IP2o, LPort=P2o)
5. H.248 ADD req (C=C1, T=?, m=TCP/TLS, a=setup:actpass, LAddr=?, LPort=?, a=fingerprint ?, RAddr=IP1o, RPort=P1o, a=fingerprint:ue-a)
Reserve and Configure AGW Connection Point (, Change Through-Connection)
6. Create incoming termination T_1
7. H.248 ADD resp (C=C1, $T=T_1$, LAddr=IP2a, LPort=P2a, a=fingerprint:agw, RAddr=IP1o, RPort=P1o)
8. Modify SDP offer
9. SDP offer (c=IP2o, m=P2o TCP/BFCP, a=setup:actpass)
10. TCP SYN
11. TCP SYN
TCP SYN ACK
TCP SYN ACK
TCP ACK
TCP ACK
12. TLS Setup
13. SDP answer (c=IP1a, m=P1a TCP/BFCP, a=setup:active)
14. H.248 MOD req (C=C1, $T=T_2$, RAddr=IP1a, RPort=P1a)
Configure AGW Connection Point (, Change Through-Connection)
15. Configure outgoing termination T_2
16. H.248 MOD resp (C=C1, $T=T_2$)
17. Modify SDP answer
18. SDP answer (c=IP2a, m=P2a TCP/TLS/BFCP, a=3ge2ae:requested, a=setup:active, a=fingerprint:agw)
11'. TCP SYN
10'. TCP SYN
TCP SYN ACK
TCP SYN ACK
TCP ACK
TCP ACK
12'. TLS Setup

Figure 6.2.10.3.2.1.1.1: Originating example call flow for e2ae security for BFCP where an incoming TCP bearer establishment triggers an outgoing TCP bearer establishment

The IMS UE A performs an IMS originating session set-up according to 3GPP TS 23.228 [2], with modifications as described in 3GPP TS 33.328 [12].

The procedure in the above figure for requesting e2ae security for a media stream is described step-by-step with an emphasis on the additional aspects for IMS-ALG and IMS-AGW of media protection using TLS.

1. IMS UE A sends an SDP offer for a media stream containing cryptographic information, together with an "a=3ge2ae:requested" SDP attribute for the BFCP-related SDP m-line, to the P-CSCF (IMS-ALG). For e2ae protection of BFCP the cryptographic information contained in the SDP offer consists of the fingerprint of the certificate of IMS UE A in accordance to IETF RFC 4975 [25]. For each media stream that uses transport "TCP/TLS/BFCP", the P-CSCF (IMS-ALG) checks for the presence of the "a=3ge2ae:requested" SDP attribute. If that indication is present and the P-CSCF (IMS-ALG) indicated support of e2ae-security for BFCP during registration, the P-CSCF (IMS-ALG) allocates the required resources, includes the IMS-AGW in the media path and proceeds as specified in this clause.

2.-4. The IMS-ALG uses the "Reserve AGW Connection Point" procedure to request a termination for "TCP" media towards the core network. To indicate that the IMS-AGW shall operate in TCP Proxy mode, the IMS-ALG provides "a=setup:actpass" attribute. The IMS-ALG sets the interlinkage topology on the termination T2 to configure the IMS-AGW to use the TCP connection establishment request (TCP SYN) received at the termination T2 as a trigger to send a TCP connection establishment on the termination T1.

NOTE 1: If "a=setup:passive" is received in the SDP answer in step 13, the IMS-ALG then needs to set the interlinkage topology on the termination T1 (not depicted).

5.-7. The IMS-ALG uses the "Reserve And Configure AGW Connection Point" procedure to request a termination for "TCP/TLS" media towards the access network. In the remote descriptor, it provides the IP address, port and fingerprint attribute received from the UE containing the fingerprint of the UE´s certificate in accordance to IETF RFC 4975 [25]. This instructs the IMS-AGW to verify during the subsequent TLS handshake with the IMS UE that the fingerprint of the certificate passed by the IMS UE during this TLS handshake matches the fingerprint passed by the P-CSCF (IMS-ALG) to the IMS-AGW. In turn, the IMS-AGW communicates the fingerprint of the certificate it is going to use for setting up protection for this media stream to the P-CSCF (IMS-ALG). To indicate that the IMS-AGW shall operate in TCP Proxy mode, the IMS-ALG provides "a=setup:actpass" attribute.

8. The P-CSCF (IMS-ALG) changes the transport from "TCP/TLS/BFCP" to "TCP/BFCP" in the SDP offer, removes the "a=3ge2ae:requested" SDP attribute and the fingerprint SDP attribute, and inserts the address information received from the IMS-AGW.

9. The P-CSCF (IMS-ALG) forwards the SDP offer.

10. The remote peer chooses to become the active party in the TCP connection establishment and sends a TCP SYN to establish the TCP connection. If the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall ignore any incoming TCP connection establishment requests (TCP SYN), e.g. to enable a remote source transport address filtering, or if the P-CSCF (IMS-ALG) did not indicate to the IMS-AGW at step 2 that it shall latch onto the required destination address via the source address/port of the incoming media, the IMS-AGW shall drop the TCP SYN received from the remote peer.
If the TCP SYN is not answered before a timer expiry, the remote peer will send the TCP SYN a second time (step 10'). The IMS-AGW will answer a repeated TCP SYN if it is received after step 14 (step 10').
The IMS-AGW answers the TCP SYN and the remote peer completes the TCP connection establishment.

11. The IMS-AGW uses the TCP SYN received at the termination T2 (at step 10 or step 10' if the TCP SYN is dropped at step 10) as a trigger to send a TCP SYN towards the UE to establish a TCP connection (effectively making the IMS-AGW acting as the TCP client towards the UE). The UE answers the TCP SYN and the IMS-AGW completes the TCP connection establishment.

12. Upon completion of the TCP connection establishment, the UE B starts the establishment of the TLS session. The IMS-AGW needs to wait until step 14 to verify the received fingerprint.

13. The P-CSCF (IMS-ALG) receives the SDP answer.

14.-16. The IMS-ALG uses the "Configure AGW Connection Point" procedure to configure the termination towards the core network with remote address information. If the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall ignore any incoming TCP connection establishment requests (TCP SYN), the IMS-ALG indicates to the IMS-AGW to accept incoming TCP connection establishment (TCP SYN) only from the indicated remote transport address.

NOTE 2: For "a=setup:active" in the SDP answer, these steps could possibly be skipped if the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall latch onto the required destination address via the source address/port of the incoming media, as the IMS-AGW will then use the address information in the TCP SYN when replying.

17. The P-CSCF (IMS-ALG) modifies the SDP answer before sending it to the UE A. The P-CSCF (IMS-ALG) sets the transport to "TCP/TLS/BFCP" and includes the fingerprint of the IMS-AGW´s certificate in accordance to IETF RFC 4975 [25].

18. The P-CSCF (IMA-ALG) then sends the updated SDP answer to IMS UE A. After receiving this message IMS UE A completes the media security setup.

6.2.10.3.2.2 IMS UE terminating procedures for e2ae

6.2.10.3.2.2.1 Incoming TCP bearer establishment triggers an outgoing TCP bearer establishment

Figure 6.2.10.3.2.2.1.1 shows the terminating session set-up procedures for one or more BFCP media stream(s) using e2ae security.

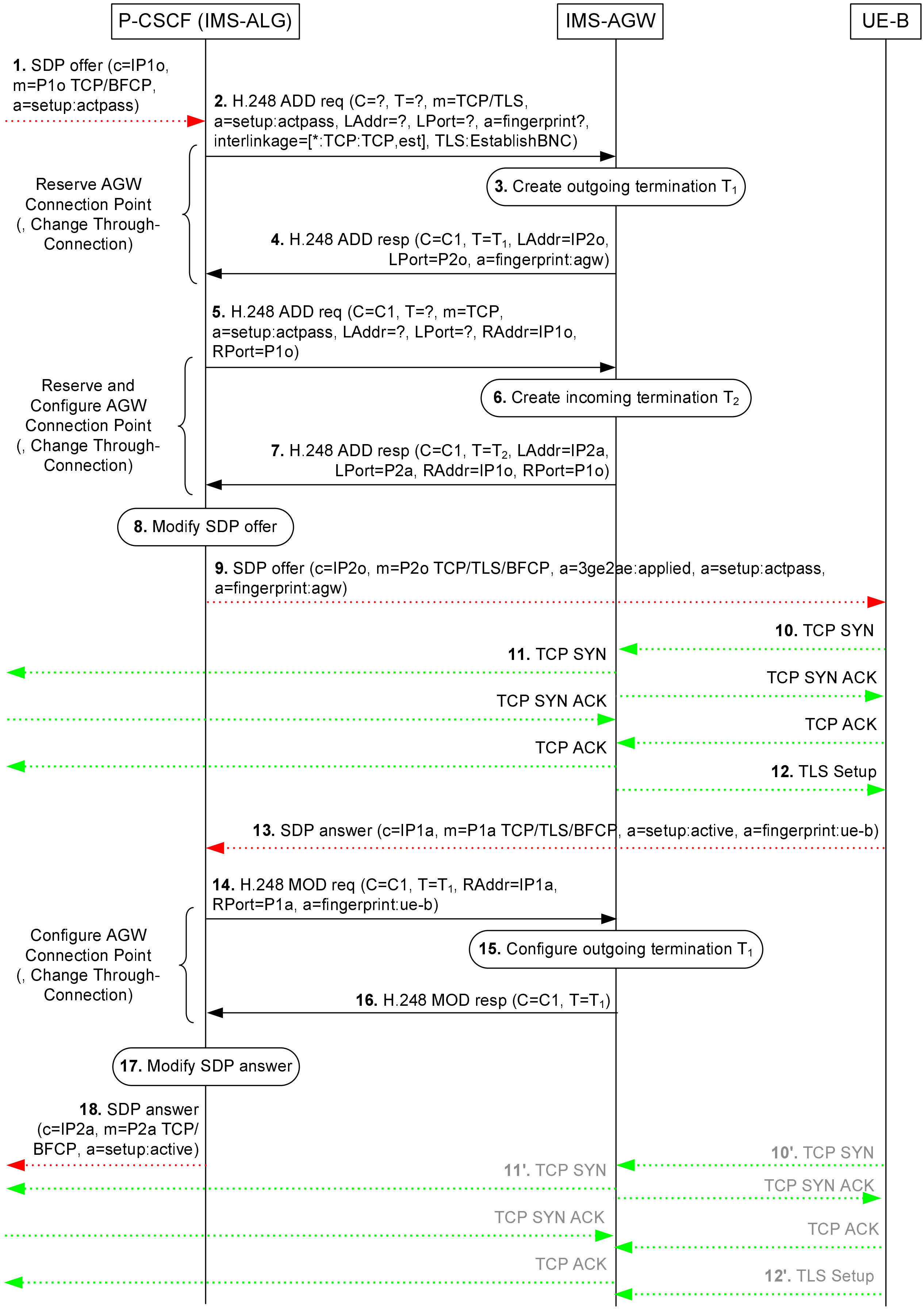

P-CSCF (IMS-ALG)
IMS-AGW
UE-B
1. SDP offer (c=IP1o, m=P1o TCP/BFCP, a=setup:actpass)
2. H.248 ADD req (C=?, T=?, m=TCP/TLS, a=setup:actpass, LAddr=?, LPort=?, a=fingerprint?, interlinkage=[*:TCP:TCP,est], TLS:EstablishBNC)
Reserve AGW Connection Point (, Change Through-Connection)
3. Create outgoing termination T_1
4. H.248 ADD resp (C=C1, $T=T_1$, LAddr=IP2o, LPort=P2o, a=fingerprint:agw)
5. H.248 ADD req (C=C1, T=?, m=TCP, a=setup:actpass, LAddr=?, LPort=?, RAddr=IP1o, RPort=P1o)
Reserve and Configure AGW Connection Point (, Change Through-Connection)
6. Create incoming termination T_2
7. H.248 ADD resp (C=C1, $T=T_2$, LAddr=IP2a, LPort=P2a, RAddr=IP1o, RPort=P1o)
8. Modify SDP offer
9. SDP offer (c=IP2o, m=P2o TCP/TLS/BFCP, a=3ge2ae:applied, a=setup:actpass, a=fingerprint:agw)
10. TCP SYN
11. TCP SYN
TCP SYN ACK
TCP SYN ACK
TCP ACK
TCP ACK
12. TLS Setup
13. SDP answer (c=IP1a, m=P1a TCP/TLS/BFCP, a=setup:active, a=fingerprint:ue-b)
14. H.248 MOD req (C=C1, $T=T_1$, RAddr=IP1a, RPort=P1a, a=fingerprint:ue-b)
Configure AGW Connection Point (, Change Through-Connection)
15. Configure outgoing termination T_1
16. H.248 MOD resp (C=C1, $T=T_1$)
17. Modify SDP answer
18. SDP answer (c=IP2a, m=P2a TCP/BFCP, a=setup:active)
10'. TCP SYN
11'. TCP SYN
TCP SYN ACK
TCP SYN ACK
TCP ACK
TCP ACK
12'. TLS Setup

Figure 6.2.10.3.2.2.1.1: Terminating example call flow for e2ae security for MSRP where an incoming TCP bearer establishment triggers an outgoing TCP bearer establishment

The IMS UE B performs an IMS terminating session set-up according to 3GPP TS 23.228 [2], with modifications as described in 3GPP TS 33.328 [12].

The procedure in the above figure for requesting e2ae security for a media stream is described step-by-step with an emphasis on the additional aspects for IMS-ALG and IMS-AGW of media protection using TLS.

1. The P-CSCF (IMS-ALG) receives an SDP offer for an MSRP media stream. For each BFCP media stream offered with transport "TCP/BFCP", if both the IMS UE and P-CSCF (IMS-ALG) indicated support for e2ae-security for BFCP during registration, the P-CSCF (IMS-ALG) allocates the required resources, includes the IMS-AGW in the media path and proceeds as specified in this clause.

2.-4. The IMS-ALG uses the "Reserve AGW Connection Point" procedure to request a termination for "TCP/TLS" media towards the access network. The IMS-ALG configures the IMS-AGW with the request to start the establishment of the TLS session once the TCP connection is established (effectively making the IMS-AGW acting as the TLS client). . To indicate that the IMS-AGW shall operate in TCP Proxy mode, the IMS-ALG provides "a=setup:actpass" attribute. The IMS-ALG sets the interlinkage topology on the termination T1 to configure the IMS-AGW to use the TCP connection establishment request (TCP SYN) received at the termination T1 as a trigger to send a TCP connection establishment on the termination T2.
The IMS-AGW communicates the fingerprint of the certificate it is going to use for setting up protection for this media stream to the P-CSCF (IMS-ALG).

NOTE: If "a=setup:passive" is received in the SDP answer in step 13, the IMS-ALG then needs to sets the interlinkage topology on the termination T2 (not depicted)

5.-7. The IMS-ALG uses the "Reserve And Configure AGW Connection Point" procedure to request a termination for "TCP" media towards the core network. To indicate that the IMS-AGW shall operate in TCP Proxy mode, the IMS-ALG provides "a=setup:actpass" attribute.

8. The P-CSCF (IMS-ALG) changes the transport from "TCP/ BFCP" to "TCP/TLS/BFCP" in the SDP offer, adds the "a=3ge2ae:applied" SDP attribute and the fingerprint SDP attribute received from the IMS-AGW, and inserts the address information received from the IMS-AGW.

9. The P-CSCF (IMS-ALG) forwards the SDP offer.

10. The UE B chooses to become the active party in the TCP connection establishment and sends a TCP SYN to establish the TCP connection. If the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall ignore any incoming TCP connection establishment requests (TCP SYN), e.g. to enable a remote source transport address filtering, or if the P-CSCF (IMS-ALG) did not indicate to the IMS-AGW at step 2 that it shall latch onto the required destination address via the source address/port of the incoming media, the IMS-AGW shall drop the TCP SYN received from the UE.
If the TCP SYN is not answered before a timer expiry, the UE will send the TCP SYN a second time (step 10'). The IMS-AGW will answer a repeated TCP SYN if it is received after step 14 (step 10').
The IMS-AGW answers the TCP SYN and the remote peer completes the TCP connection establishment.

11. The IMS-AGW sends a TCP SYN towards the core network to establish a TCP connection. The remote peer answers the TCP SYN and the IMS-AGW completes the TCP connection establishment.

12. Upon completion of the TCP connection establishment, the IMS-AGW starts the establishment of the TLS session. The IMS-AGW needs to wait until step 14 to verify the received fingerprint.

13. The P-CSCF (IMS-ALG) receives the SDP answer. It contains the fingerprint attribute with the UE´s certificate in accordance to IETF RFC 4975 [25].

14.-16.The IMS-ALG uses the "Configure AGW Connection Point" procedure to configure the termination towards the UE B with remote address information. In the remote descriptor, it also provides fingerprint attribute received from the UE. This instructs the IMS-AGW to verify during the TLS handshake with the IMS UE (see step 12) that the fingerprint of the certificate passed by the IMS UE during this TLS handshake matches the fingerprint passed by the P-CSCF (IMS-ALG) to the IMS-AGW. If the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall ignore any incoming TCP connection establishment requests (TCP SYN), the IMS-ALG indicates to the IMS-AGW to accept incoming TCP connection establishment (TCP SYN) only from the indicated remote transport address.

17. The P-CSCF (IMS-ALG) modifies the SDP answer before sending it to the core network. The P-CSCF (IMS-ALG) sets the transport to "TCP/ BFCP" and removes the SDP fingerprint attribute.

18. The P-CSCF (IMS-ALG) then sends the updated SDP answer to core network.

6.2.10.4 End-to-access-edge security for UDP based media using DTLS

6.2.10.4.1 General

The IMS-ALG and the IMS-AGW may support e2ae security for the UDP based media using DTLS and certificate fingerprints.

The following subclauses describe extensions to the Iq signalling procedures and their interactions with SIP signalling in the control plane and with user plane procedures if the e2ae security for the UDP based media using DTLS and certificate fingerprints is supported by the IMS-ALG and the IMS-AGW and if the IMS-ALG indicated support of e2ae security for the UDPTL using DTLS and certificate fingerprints during registration.

6.2.10.4.2 Session establishment from IMS access network for T.38 fax using "UDP/TLS/UDPTL"

Upon receipt of an SDP offer from the IMS access network containing T.38 fax media using the "UDP/TLS/UDPTL" transport protocol with the associated:

- 3ge2ae SDP attribute, as defined in 3GPP TS 24.229 [11], with a value "requested";
- fingerprint SDP attribute as defined in IETF RFC 4572 [37]; and
- setup SDP attribute as defined in IETF RFC 4145 [30];

the IMS-ALG shall:

- check the received value of the setup SDP attribute to determine if the IMS-AGW needs to act as DTLS client or DTLS server. When the received value is equal to:

  a) "active" the IMS-AGW needs to act as DTLS server;

  b) "passive" the IMS-AGW needs to act as DTLS client; or

  c) "actpass" the IMS-ALG shall decide if the IMS-AGW needs to act as DTLS client or DTLS server;

- when reserving the transport addresses/resources towards the IMS access network:

  a) indicate to the IMS-AGW "UDP/DTLS" as transport protocol;

  b) if the IMS-AGW needs to act as DTLS client, include the Establish (D)TLS session information element to request the IMS-AGW to start the DTLS session setup;

  c) include the Notify (D)TLS session establishment Failure Event information element to request the IMS-AGW to report the unsuccessful DTLS session setup;

  d) include the Remote certificate fingerprint information element with the value of the received fingerprint SDP attribute; and

  e) include the Local certificate fingerprint Request information element to request the certificate fingerprint of the IMS-AGW; and

- indicate to the IMS-AGW "UDP" as transport protocol when reserving the transport addresses/resources towards the IMS core network.

When modifying an SDP answer that will be sent to the IMS access network, the IMS-ALG shall:

- in the "m=" line indicating T.38 fax using UDPTL, change the transport protocol to "UDP/TLS/UDPTL";
- insert the fingerprint SDP attribute with the value of the Local certificate fingerprint information element received from the IMS-AGW; and

- insert the setup SDP attribute with the value:

  a) "active" if the IMS-ALG requested the IMS-AGW to act as DTLS client; or

  b) "passive" if the IMS-AGW shall take the DTLS server role.

The message sequence chart shown in the figure 6.2.10.4.2.1 gives an example of a session establishment from the IMS access network with an emphasis on the additional aspects for the IMS-ALG and the IMS-AGW for the e2ae protection of the T.38 fax media using UDPTL over DTLS.

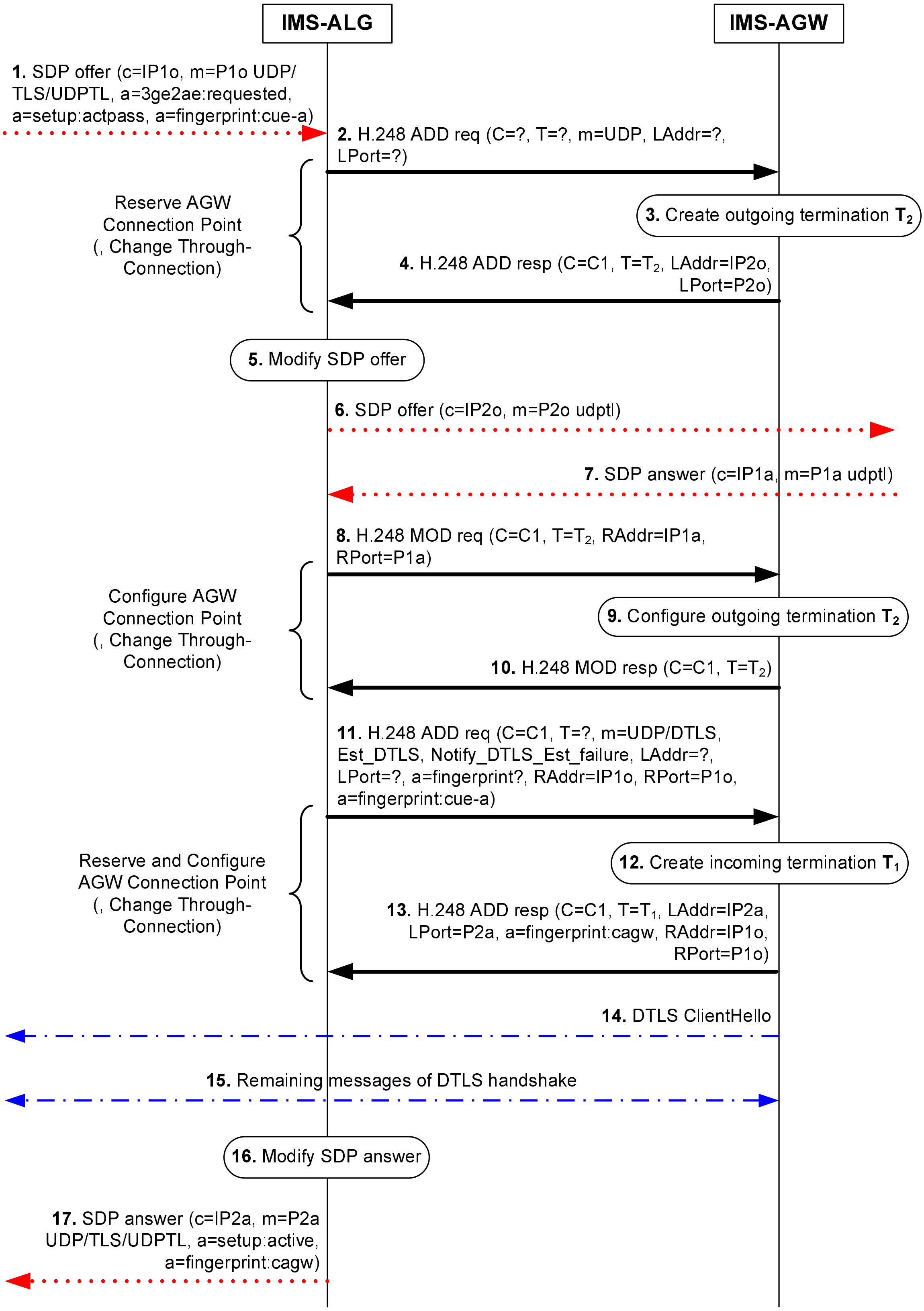


Figure 6.2.10.4.2.1: Session setup from the IMS access network with e2ae protection of T.38 fax

6.2.10.4.3 Session establishment towards IMS access network for T.38 fax using "UDP/TLS/UDPTL"

Upon receipt of an SDP offer from the IMS core network containing T.38 fax media using the "UDPTL" transport protocol the IMS-ALG shall:

- when reserving the transport addresses/resources towards the IMS access network:

  a) indicate to the IMS-AGW "UDP/DTLS" as transport protocol;

  b) include the Notify (D)TLS session establishment Failure Event information element to request the IMS-AGW to report the unsuccessful DTLS session setup; and

NOTE 1: The IMS-ALG may omit this information element when reserving resources and instead send it to the IMS-AGW when modifying the resources towards the IMS access network.

  c) include the Local certificate fingerprint Request information element to request the certificate fingerprint of the IMS-AGW; and

- when reserving the transport addresses/resources towards the IMS core network indicate to the IMS-AGW "UDP" as transport protocol.

When modifying the SDP offer that will be sent to the IMS access network, the IMS-ALG shall:

- in the "m=" line indicating T.38 fax using UDPTL, change the transport protocol to "UDP/TLS/UDPTL";

- insert the 3ge2ae SDP attribute, as defined in 3GPP TS 24.229 [11], with a value "applied";

- insert the fingerprint SDP attribute, as defined in IETF RFC 4572 [37], with the value of the Local certificate fingerprint information element received from the IMS-AGW; and

- insert the setup SDP attribute, as defined in IETF RFC 4145 [30], with the value "actpass".

NOTE 2: Alternatively, the IMS-ALG can set the value of the setup SDP attribute to "active" if the IMS-ALG wants that the IMS-AGW provides DTLS client role or to "passive" if the IMS-ALG wants that the IMS-AGW provides DTLS server role.

Upon receipt of an SDP answer from the IMS access network containing T.38 fax media using the "UDP/TLS/UDPTL" transport protocol with the associated fingerprint and setup SDP attributes, the IMS-ALG shall:

- check the value of the received setup SDP attribute to determine if the IMS-AGW needs to act as DTLS client or DTLS server. When the received value is equal to:

  a) "active" the IMS-AGW needs to act as DTLS server; or

  b) "passive" the IMS-AGW needs to act as DTLS client; and

- when modifying the transport addresses/resources towards the IMS access network:

  a) if the IMS-AGW needs to act as DTLS client, include the Establish (D)TLS session information element to request the IMS-AGW to start the DTLS session setup;

  b) include the Remote certificate fingerprint information element with the value of the received fingerprint SDP attribute; and

  c) if not already provided, include the Notify (D)TLS session establishment Failure Event information element to request the IMS-AGW to report the unsuccessful DTLS session setup.

The message sequence chart shown in the figure 6.2.10.4.3.1 gives an example of a session establishment towards the IMS access network with an emphasis on the additional aspects for the IMS-ALG and the IMS-AGW for the e2ae protection of the T.38 fax media using UDPTL over DTLS.

NOTE 3: In the shown example it is assumed that the IMS-ALG requested the IMS-AGW at step 2 to latch onto the address of the received media packets to determine the corresponding destination address. Otherwise, the DTLS ClientHello message received at the step 10 will be dropped until the IMS-AGW receives a repeated DTLS ClientHello message after the step 13.

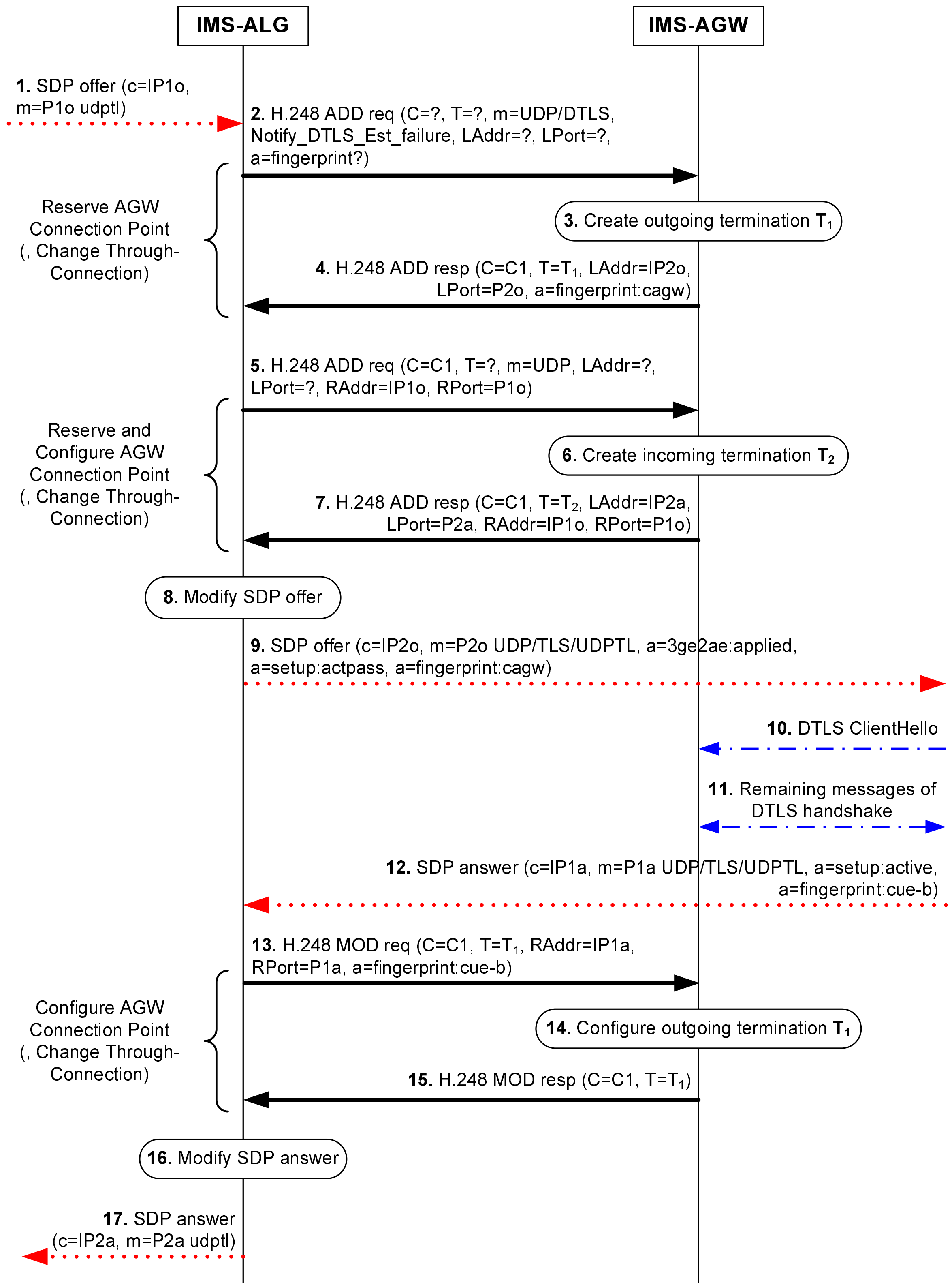


Figure 6.2.10.4.3.1: Session setup towards the IMS access network with e2ae protection of T.38 fax

6.2.10.4.4 IMS-AGW procedure for e2ae security of T.38 fax using "UDP/TLS/UDPTL"

The IMS-AGW shall:

- upon reception of the Local certificate fingerprint Request information element, select an own certificate for the T.38 fax media stream, uniquely associate the own certificate with the T.38 media stream, and send to the IMS-ALG the Local certificate fingerprint information element with the fingerprint of the own certificate;

- uniquely associate the value of the Remote certificate fingerprint information element, received from the IMS-ALG, with the corresponding T.38 fax media stream;
- take a DTLS server role and be prepared to receive a DTLS ClientHello message from the served UE;
- upon reception of the Establish (D)TLS session information element, take a DTLS client role and start DTLS session establishment by sending the DTLS ClientHello message to the served UE; and
- verify during the subsequent DTLS handshake with the served UE (as described in IETF draft-ietf-mmusic-udptl-dtls [33]) that the fingerprint of the certificate passed by the served UE during DTLS handshake matches the value of the Remote certificate fingerprint information element received from the IMS-ALG:
  a) if the verification fails, the IMS-AGW shall regard the remote DTLS endpoint as not authenticated, terminate the DTLS session and as specified in subclause 6.2.10.4.5, shall report the unsuccessful DTLS session setup to the IMS-ALG; or
  b) if the verification succeeds, the IMS-AGW shall continue with DTLS session setup and when the DTLS session is established, the IMS-AGW shall be prepared to receive and convert the protected media from the served UE to the unprotected media to be sent to the core network and vice versa.

6.2.10.4.5 DTLS session establishment failure indication

The IMS-AGW shall use a Notify (D)TLS session establishment Failure Indication procedure to report DTLS session establishment related failures.

The figure 6.2.10.4.5.1 shows the message sequence chart example when the IMS-AGW reports the unsuccessful DTLS session setup to the IMS-ALG.

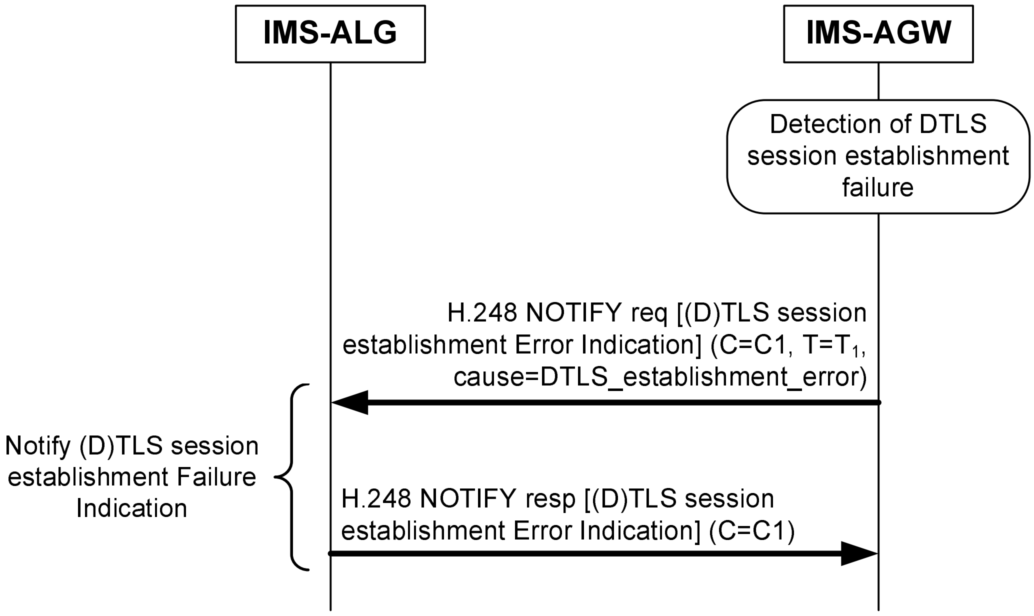


Figure 6.2.10.4.5.1: DTLS session establishment failure indication

6.2.10.5 End-to-access-edge security for RTP based media using DTLS-SRTP

Editor's Note: There are two served user instances of the DTLS service within WebRTC: the data channel and the key exchange for SRTP. Thus, there are either two DTLS connections behind a single DTLS session, or two separate DTLS sessions.

The procedures are similar to that of subclause 6.2.10 apart from the IMS-ALG optionally requesting the eIMS-AGW to provide IMS media plane security using DTLS.

Upon receipt of an SDP offer from the IMS access network, the IMS-ALG shall:

- when reserving the transport addresses/resources towards the IMS access network:

a) indicate to the eIMS-AGW "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as transport protocol;

b) include the Remote certificate fingerprint information element with the value of the received fingerprint SDP attribute from the WIC;

c) include the Local certificate fingerprint Request information element to request the certificate fingerprint of the eIMS-AGW; and

- indicate to the eIMS-AGW "RTP/AVP" or "RTP/AVPF" over UDP as transport protocol when reserving the transport addresses/resources towards the IMS core network.

When modifying an SDP answer that will be sent to the IMS access network, the IMS-ALG shall:

- in the "m=" line indicating the use of SRTP, change the transport protocol to "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF"; and

- insert the fingerprint SDP attribute with the value of the Local certificate fingerprint information element received from the eIMS-AGW.

Figure 6.2.10.5.1 shows the message sequence chart example of WIC originated procedure using DTLS-SRTP.

NOTE: Below establishment procedures are based on the assumption that there wasn't yet any DTLS procedure triggered from WebRTC data channel side.

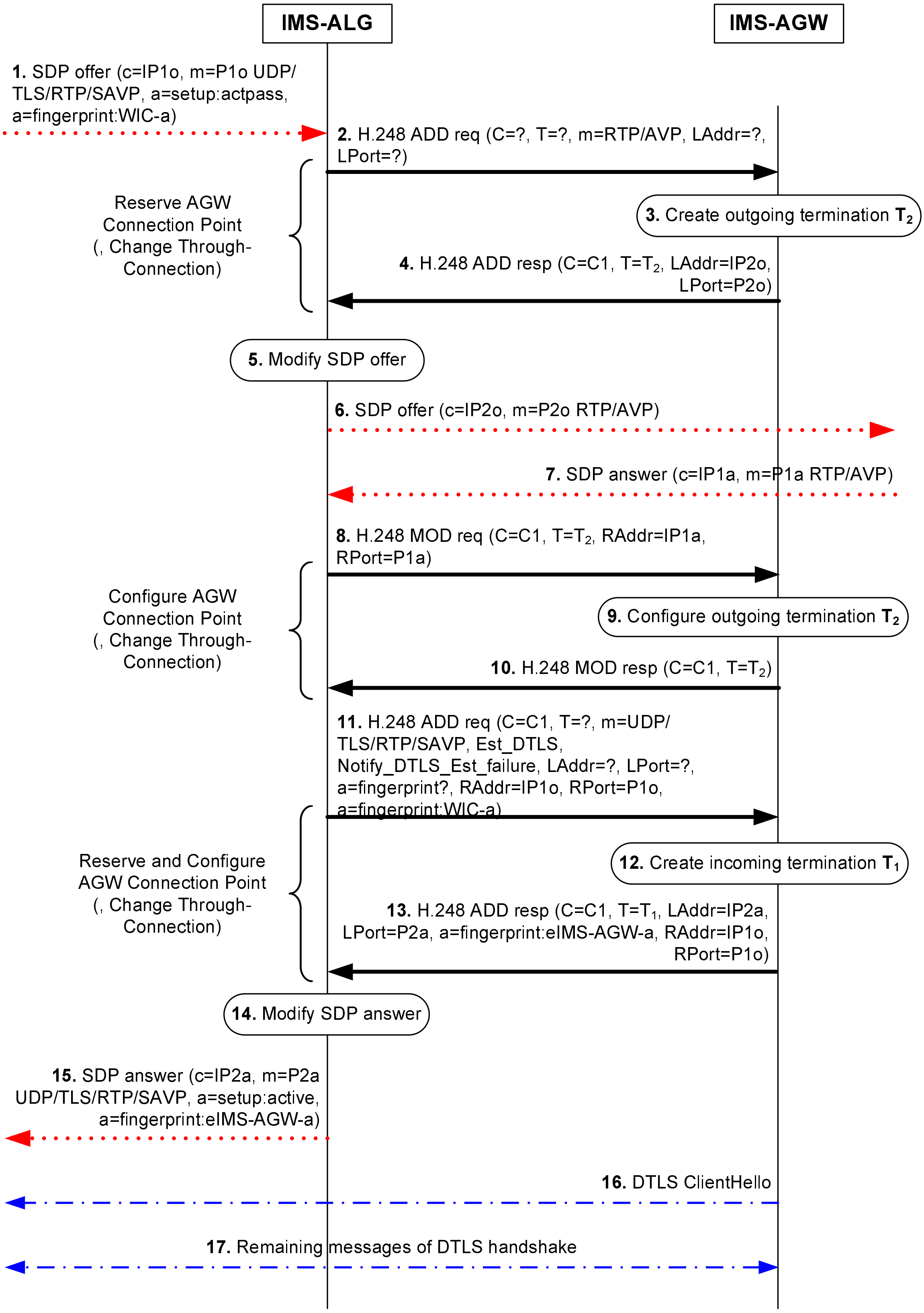


Figure 6.2.10.5.1: WIC originated procedure using DTLS-SRTP

NOTE: The WIC may receive the ClientHello prior the SDP answer, thus the handshake might be initiated, but the handshake will not complete until the SDP answer has been received by the WIC.

Upon receipt of an SDP offer from the IMS core network using the "RTP/AVP" or "RTP/AVPF" over UDP as transport protocol the IMS-ALG shall:

- when reserving the transport addresses/resources towards the IMS access network:

  a) indicate to the eIMS-AGW "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as transport protocol;

  b) include the Local certificate fingerprint Request information element to request the certificate fingerprint of the eIMS-AGW; and

- when reserving the transport addresses/resources towards the IMS core network indicate to the eIMS-AGW "RTP/AVP" or "RTP/AVPF" over UDP as transport protocol.

When modifying the SDP offer that will be sent to the IMS access network, the IMS-ALG shall:

- in the "m=" line indicating the use of SRTP, change the transport protocol to "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF"; and

- insert the fingerprint SDP attribute with the value of the Local certificate fingerprint information element received from the eIMS-AGW.

Upon receipt of an SDP answer from the IMS access network containing the use of the "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" transport protocol with the associated fingerprint and setup SDP attributes, the IMS-ALG shall:

- when modifying the transport addresses/resources towards the IMS access network:

  a) include the Remote certificate fingerprint information element with the value of the received fingerprint SDP attribute.

The message sequence chart shown in the figure 6.2.10.5.2 shows the message sequence chart example of WIC terminated procedure using DTLS-SRTP.

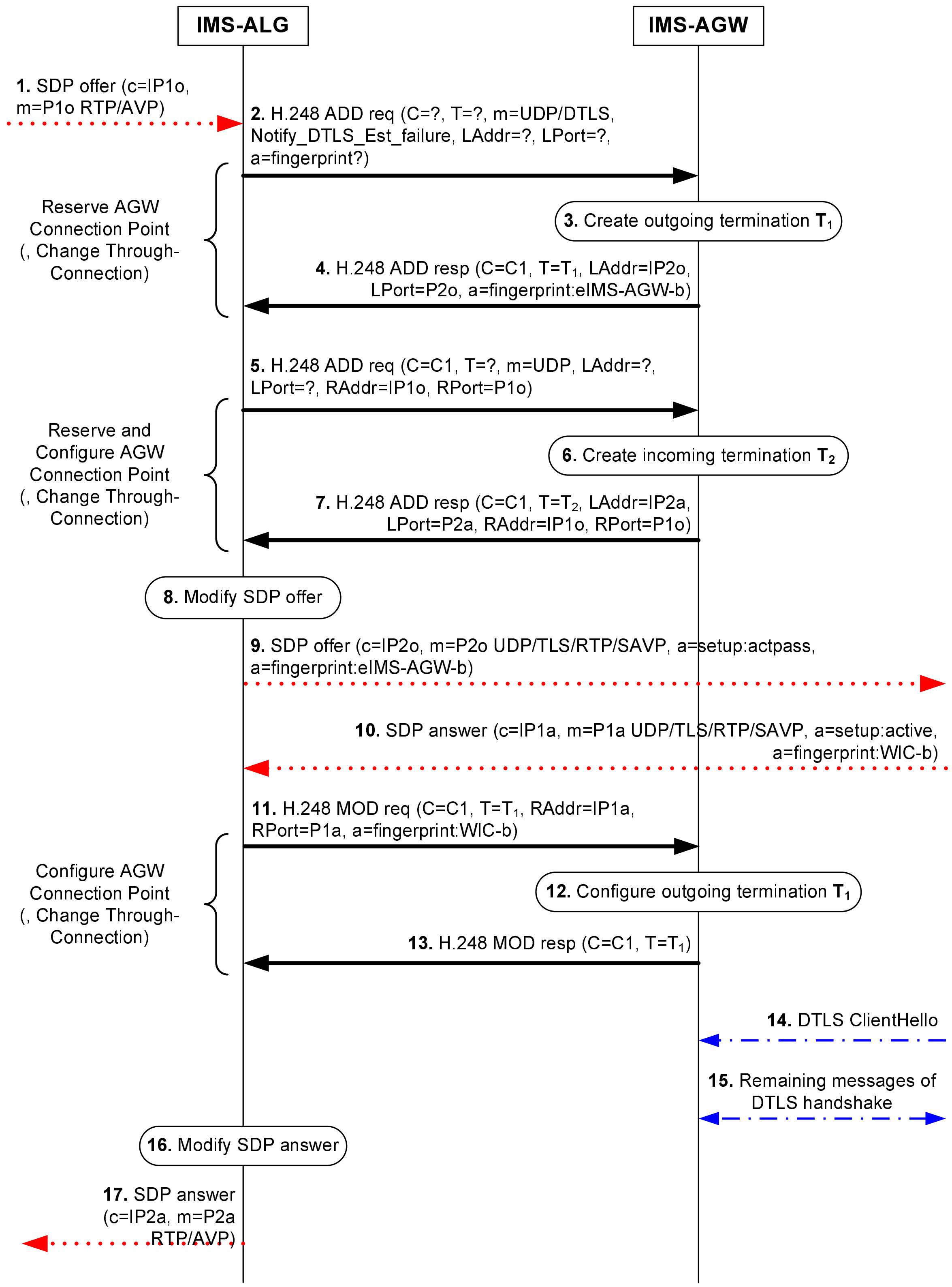


Figure 6.2.10.5.2: WIC terminated procedure using DTLS-SRTP

NOTE: The eIMS-AGW might receive the ClientHello prior receiving the MOD-request, but the DTLS handshake will not finish before the MOD-request (more specific: the fingerprint from WIC-b) has been received.

6.2.10A IMS end-to-end Media Plane Security

6.2.10A.1 End-to-end security for RTP based media using SDES

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG providing "RTP/SAVP" or "RTP/SAVPF", as received in the SDP, to the IMS-AGW as transport protocol and not providing any other media related information to the corresponding terminations, and configuring the IMS-AGW to pass media transparently.

The IMS-ALG shall forward the SDP with unmodified transport protocol for those media lines and unmodified SDES SDP attribute(s).

6.2.10A.2 End-to-end security for TCP-based media using TLS

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG providing "TCP" to the IMS-AGW as transport protocol and not providing any TLS related information nor any other media related information to the corresponding terminations, and configuring the IMS-AGW to pass media transparently.

The IMS-ALG shall forward the SDP with unmodified transport protocol for those media lines and unmodified TLS related SDP attribute(s).

Editor's Note: The scenario where both terminals of an e2e security protected media session are located behind firewalls/NATs is FFS.

6.2.11 Change Through-Connection

The Change Through-Connection procedure is used for opening and closing of gates and is mandatory for IMS-ALG and IMS-AGW to support. The IMS-ALG sets the Stream mode parameter using the Change Through-Connection procedure to request the IMS-AGW to one-way or both-way through-connect or block media streams on a termination.

The IMS-ALG may combine the Change Through-Connection procedure with the Reserve and Configure AGW Connection Point, Reserve AGW Connection Point or Configure AGW Connection Point procedure as in Figure 6.2.1.2., or may apply this procedure separately.

6.2.12 Emergency Calls

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG requesting the IMS-AGW to treat the call as emergency call with a preferential handling by including the information element "Emergency Call Indicator" within the "Reserve and Configure AGW Connection Point" or "Reserve AGW Connection Point procedure".

6.2.13 Explicit Congestion Notification support

6.2.13.1 General

An IMS-ALG may configure the IMS-AGW to transfer the ECN bits in the IP header transparent (see subclause 6.2.13.2) or to act as an ECN endpoint (see subclause 6.2.13.3). See subclause 5.12.

6.2.13.2 ECN Active Indicated (ECN transparent)

Figure 6.2.13.2.1 shows the message sequence chart example for indicating ECN transparent.

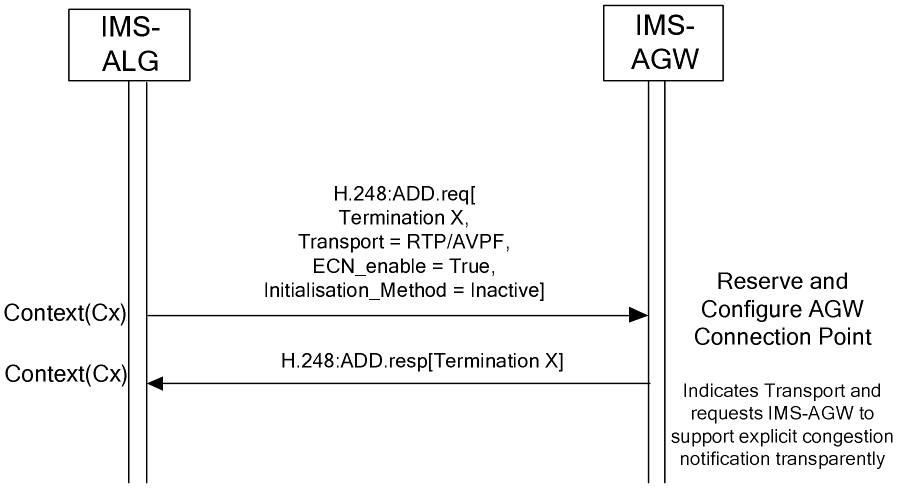


Figure 6.2.13.2.1: Procedure to indicate ECN transparent negotiated

Upon receipt of the indication that ECN transparent has been negotiated, the IMS-AGW shall forward ECN bits within IP packets unmodified. Any RTCP feedback received shall be passed unchanged.

6.2.13.3 ECN support requested (ECN endpoint)

Figure 6.2.13.3.1 shows the message sequence chart example for requesting ECN endpoint.

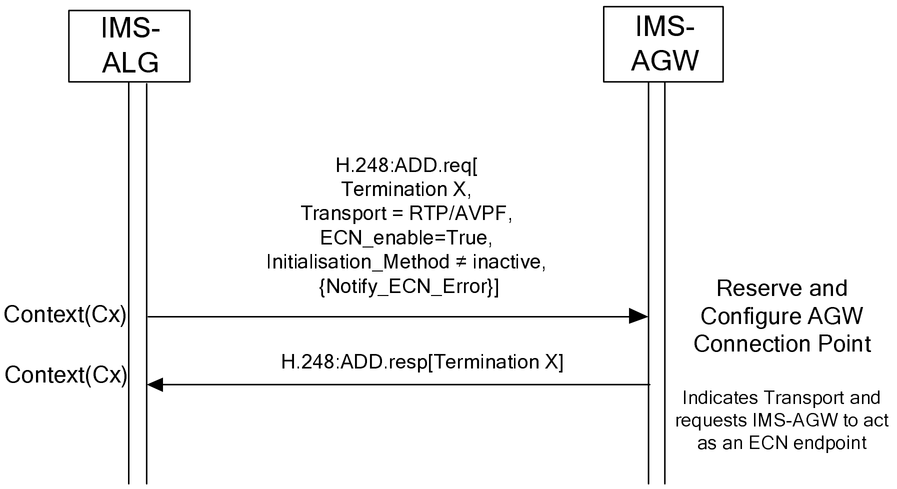


Figure 6.2.13.3.1: Procedure to Request ECN endpoint

Upon receipt of a request to apply ECN the IMS-AGW shall set the ECN field of the IP header in accordance with 3GPP TS 26.114 [21] when sending any data packets.

Upon receipt of any IP headers indicating ECN Congestion Experienced (ECN-CE) the IMS-AGW shall trigger rate adaptation in accordance with 3GPP TS 26.114 [21].

NOTE: ECN endpoint requires the IMS-ALG to configure the IMS-AGW with all media attributes to allow rate adaptation even if no transcoding is required/supported in the IMS-AGW.

6.2.13.4 ECN Failure Indication (ECN endpoint)

Figure 6.2.13.4.1 shows the message sequence chart example for an ECN Failure Event.

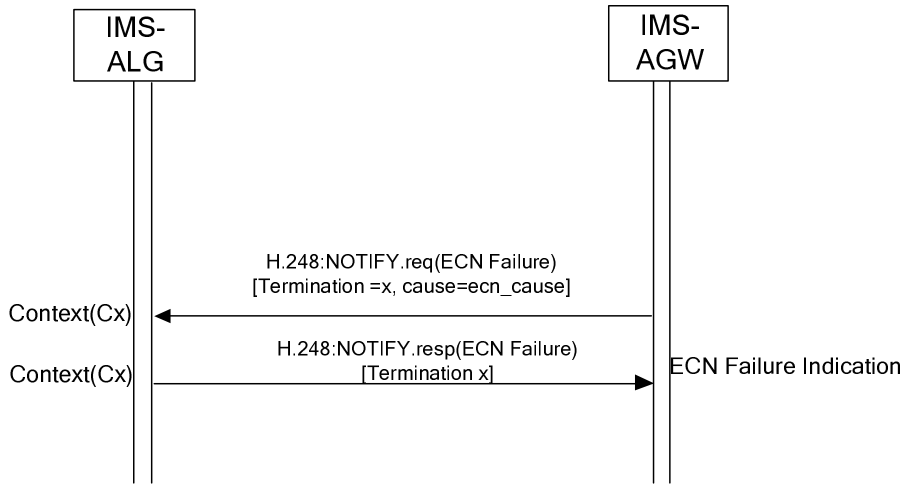


Figure 6.2.13.4.1: Procedure to Report ECN Failure

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

6.2.14 Access Transfer procedures with media anchored in IMS-AGW (ATGW)

6.2.14.1 General

This clause describes extensions to the Iq signalling procedures and their interactions with SIP signalling in the control plane and with user plane procedures to support the "SRVCC enhanced with ATCF" procedures between the IMS-ALG (ATCF) and IMS-AGW (ATGW) when the IMS-ALG and IMS-AGW support the ATCF and ATGW functionality, as specified in 3GPP TS 23.237 [18] and 3GPP TS 24.237 [19].

The Access Transfer procedures are optional to support on the Iq reference point. The requirements in this clause shall apply if these procedures are supported.

All message sequence charts in this clause are examples.

6.2.14.2 H.248 context model

Figure 6.2.14.2.1 shows the H.248 context model after the PS originating or terminating session establishment and before the PS to CS access transfer procedure. The "squared" line represents the call control signalling. The "dotted" line represents the bearer. The bearer termination T1 is used for the media path of the PS access leg, the bearer termination T2 is used for the media path of the remote leg.

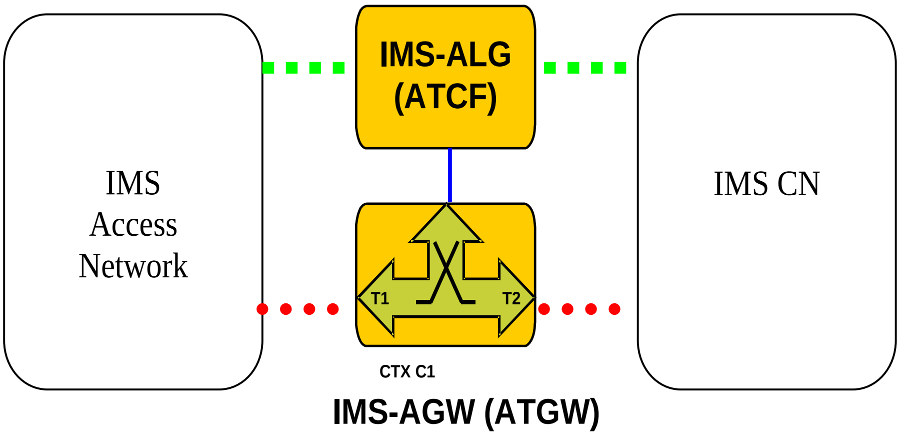


Figure 6.2.14.2.1: H.248 Context Model before Access Transfer

Figure 6.2.14.2.2 shows the H.248 context model during the PS to CS access transfer procedure. The IMS-ALG (ATCF) may seize a new bearer termination T3 for the new media path of the CS access leg, e.g. if the PS and CS nodes before and after the handover are reachable via different IP realms or use a different IP version. The IMS-ALG (ATCF) may alternatively reconfigure the T1 termination with the new remote configuration (e.g. IP address and media) instead of seizing a new termination; in that case, the H.248 context model remains as before access transfer.

Bi-casting is not supported during access transfer, i.e. the IMS-AGW (ATGW) does not duplicate downlink media packets received from the remote leg to the source and target access legs simultaneously.

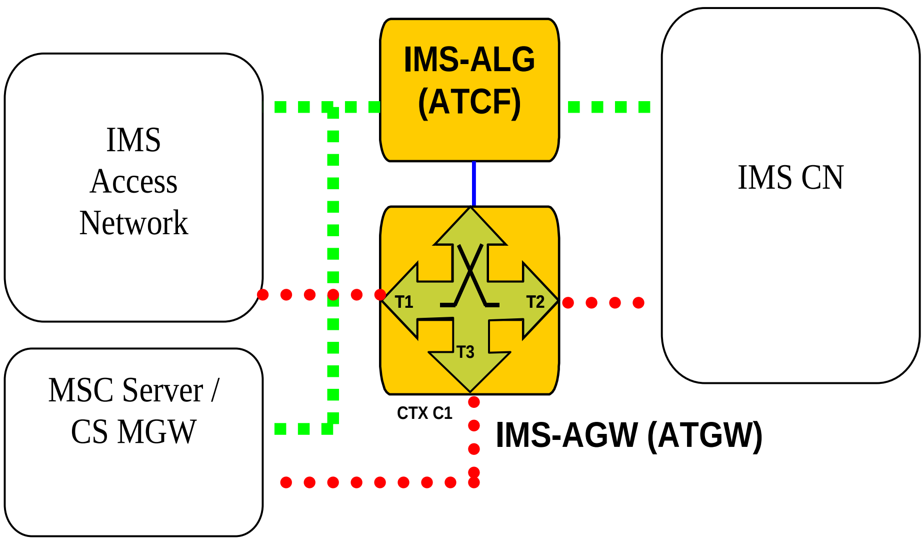


Figure 6.2.14.2.2: H.248 Context Model during Access Transfer

Figure 6.2.14.2.3 shows the H.248 context model after the PS to CS access transfer procedure if the source access leg is released. If the UE chooses to retain some media flow(s) in the transferred-out access, the H.248 context model remains as during access transfer.

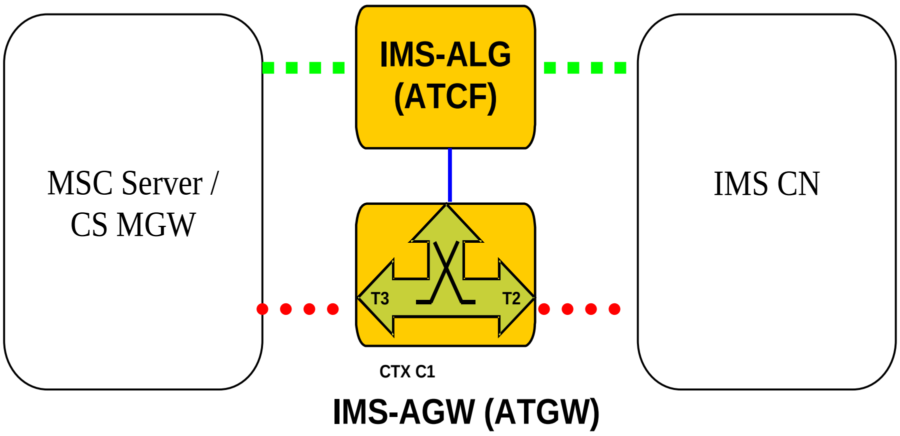


Figure 6.2.14.2.3: H.248 Context Model after Access Transfer

6.2.14.3 PS session origination or termination with media anchoring in IMS-AGW (ATGW) signaling procedures

If the IMS-ALG (ATCF) decides to anchor the media of a session in the IMS-AGW (ATGW) the call related procedures shall follow the basic procedures for IMS ALG (i.e. as specified in clause 6.2.1) with the following differences:

- The IMS-ALG (ATCF) shall seize a termination towards the terminating user, using the "Reserve AGW Connection Point" procedure before sending a SDP offer to the terminating user. The IMS-ALG (ATCF) may signal media related information to the IMS-AGW (ATGW) or omit media when adding the IP termination at this stage.

NOTE : 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 IMS-AGW (ATGW) does not need to reserve any associated resources at this stage.

- When the IMS-ALG (ATCF) receives the SDP answer from the terminating user, the IMS-ALG (ATCF) shall configure the IMS-AGW (ATGW) accordingly by either supplying the same media related information for all interconnected terminations or by omitting the media related information.

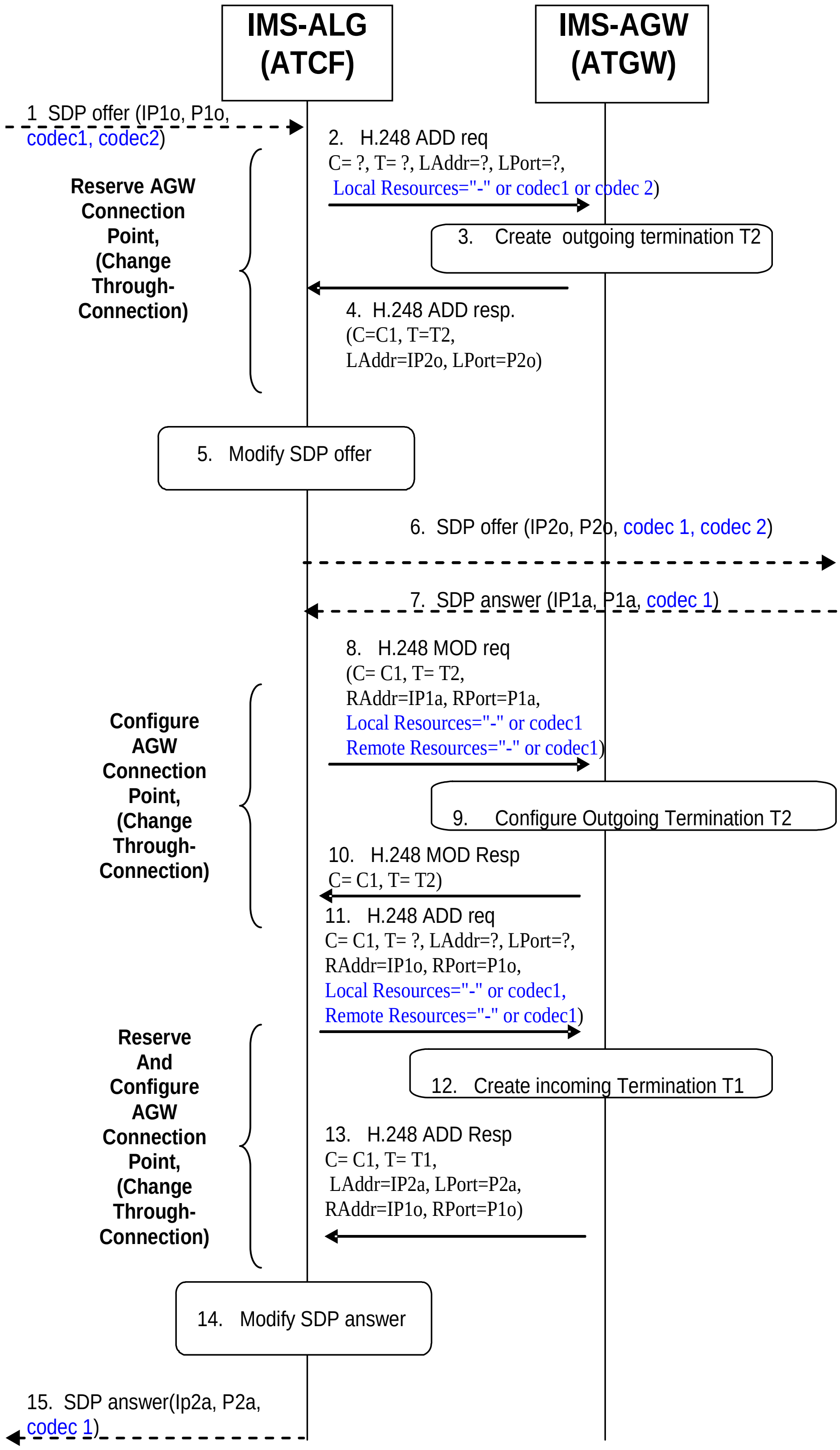


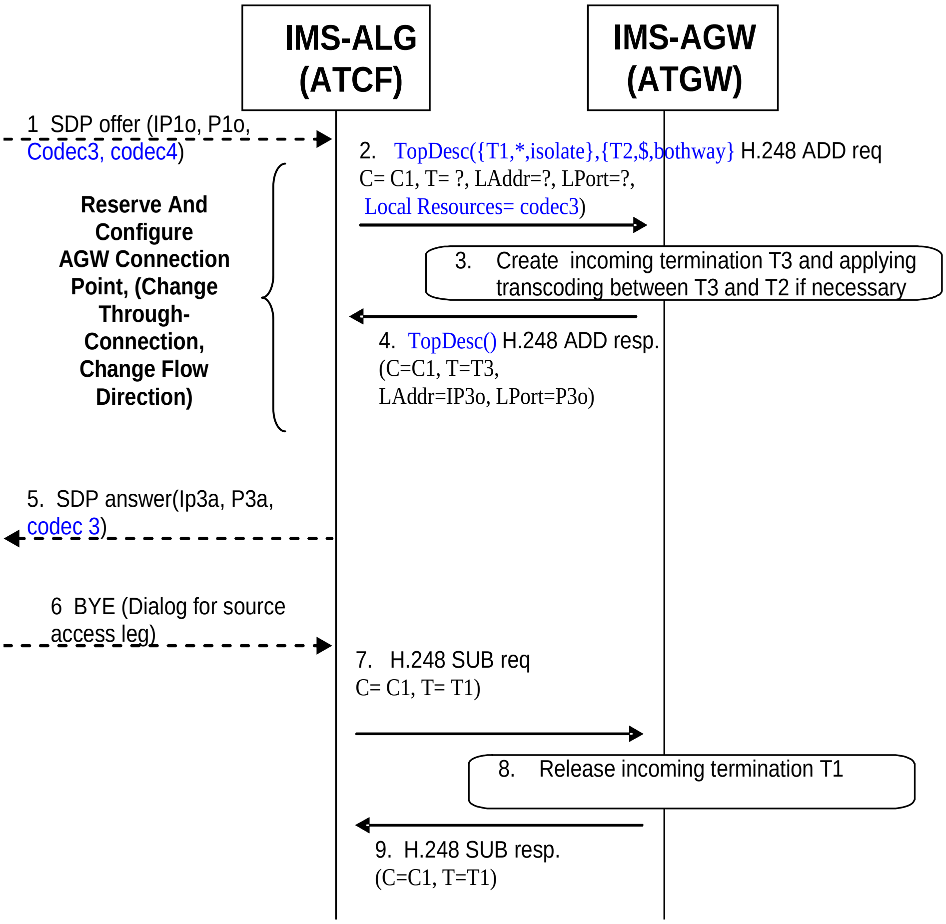
Figure 6.2.14.3.1: PS session establishment with media anchoring in IMS-AGW (ATGW)

1. The IMS-ALG (ATCF) receives an SDP offer in SIP signalling. The IMS-ALG (ATCF) requires an IMS-AGW (ATGW) for media anchoring (or for another IMS-AGW use case) but does not offer transcoding.
2. The IMS-ALG (ATCF) sends a H.248 ADD request command to create the outgoing termination and to request IP resources to execute ATGW 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 IMS-ALG (ATCF) selects an IMS-AGW (ATGW) that does not support transcoding, the IMS-ALG (ATCF) may signal media related sub-fields in the media descriptor to the IMS-AGW (ATGW) if the IMS-AGW (ATGW) supports media encoding. The IMS-AGW (ATGW) shall accept the ADD request even though it cannot reserve any transcoding resources for the indicated media.
3. The IMS-AGW (ATGW) creates the outgoing termination.
4. The IMS-AGW (ATGW) replies to IMS-ALG (ATCF) with a H.248 ADD reply command and provides the local address and port of the outgoing termination.
5. The IMS-ALG (ATCF) replaces the IP address inside the SDP using the information coming from IMS-AGW (ATGW).
6. The IMS-ALG (ATCF) forwards the new offer to the succeeding node.
7. The SDP answer is received by IMS-ALG (ATCF). In this example the codec1 received in the original SDP offer in step1 has been selected.
8. The IMS-ALG (ATCF) 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.
9. The IMS-AGW (ATGW) configures the outgoing termination.
10. The IMS-AGW (ATGW) replies to IMS-ALG (ATCF) with a H.248 MOD reply command.
11. The IMS-ALG (ATCF) 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 ATGW 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 7 (Codec 1).
12. The IMS-AGW (ATGW) creates the incoming termination.
13. The IMS-AGW (ATGW) replies to the IMS-ALG (ATCF) with a H.248 ADD reply command and provides the local address and port of the incoming termination.
14. The IMS-ALG (ATCF) replaces the IP address inside the SDP answer using the information coming from IMS-AGW (ATGW).
15. SDP answer is sent to the network at the incoming side.

Similar principles shall apply during the establishment of a mobile terminating session.

6.2.14.4 PS to CS Access Transfer procedure with media anchored in IMS-AGW (ATGW)

The signalling flow shown in figure 6.2.14.4.1 gives an example for PS to CS access transfer with media anchored in the IMS-AGW (ATGW). In this case, the media has been anchored in IMS-AGW (ATGW) as specified in subclause 6.2.14.3.



1. The IMS-ALG (ATCF) receives an SDP offer in SIP signalling from the MSC Server. The IMS-ALG (ATCF) checks whether transcoding is required.2. The IMS-ALG (ATCF) sends a H.248 ADD request command to create the target access leg termination and to request IP resources to execute ATGW function. Topology is changed and media reconfigured to connect media between T2 and T3.
If no media transcoding is required this may be indicated by signalling "-" or by signalling the same media information on T3 as is configured on T2, following the principles specified in subclause 6.2.14.3.
If media transcoding is required (as illustrated in this example), the IMS-ALG (ATCF) signals media related sub-fields in the media descriptor to the IMS-AGW (ATGW). The IMS-AGW (ATGW) determines from the media configuration whether transcoding is required on a stream between two terminations between which data flow is permitted.
3. The IMS-AGW (ATGW) creates the target access leg termination T3 and starts to apply transcoding between T2 and T3 (if required).
4. The IMS-AGW (ATGW) replies to IMS-ALG (ATCF) with a H.248 ADD reply command and provides the local address and port of the outgoing termination.
5. The IMS-ALG (ATCF) returns an SDP answer to the MSC Server; the IP address inside the SDP uses the information coming from IMS-AGW (ATGW).
6. Upon successful completion of the access transfer procedure, the IMS-ALG (ATCF) receives a BYE request from the SCC AS if there is no more media flows on the PS access.
7. The IMS-ALG (ATCF) sends a H.248 SUB request command to subtract the source access leg termination.
8. The IMS-AGW (ATGW) releases the source access leg termination.
9. The IMS-AGW (ATGW) replies to IMS-ALG (ATCF) with a H.248 SUB reply command.

Figure 6.2.14.4.1: PS to CS Access Transfer with transcoding in IMS-AGW (ATGW)

6.2.14.5 ECN support during PS to CS Access Transfer procedure with media anchored in IMS-AGW (ATGW)

The signalling flow shown in figure 6.2.14.4.1 gives an example for PS to CS access transfer with media anchored in the IMS-AGW (ATGW). The following additional actions are required if ECN is supported by the IMS-ALG/IMS-AGW:

1.

a) If ECN was supported during the PS session transparently and the SDP offer received from the MSC Server does not indicate ECN support, it is not possible to maintain transparent ECN support to the IMS CN. The IMS-ALG (ATCF) shall modify the Termination T2 to act as an ECN endpoint toward the IMS CN (see Subclause 5.12). Additionally the IMS-ALG (ATCF) shall disable ECN on the termination T3 (or T1).

b) If ECN was supported during the PS session transparently and the SDP offer received from the MSC Server does indicate ECN support and no transcoding is required (codec types and modes are aligned between ICS side and IMS CN), then the IMS-ALG (ATCF) shall request ECN transparent properties when seizing T3 and respond to the MSC Server with ECN supported in the SDP answer (step 5).

c) If ECN was supported during the PS session transparently and the SDP offer received from the MSC Server does indicate ECN support and transcoding is required between the CS leg and the IMS-CN, then the IMS-ALG (ATCF) shall request ECN endpoint properties when seizing T3 (or modify the termination T1 with ECN endpoint properties) and respond to the MSC Server with ECN supported in the SDP answer (step 5). Additionally the IMS-ALG (ATCF) shall modify the Termination T2 to act as an ECN endpoint toward the IMS CN (see Subclause 5.12).

d) If ECN was not supported during the PS session and the SDP Offer received from the MSC Server indicates ECN support, the IMS-ALG (ATCF) shall not accept ECN support in the SDP answer (step 5).

6.2.14.6 Support of generic image attributes

6.2.14.6.1 General

The IMS-ALG (ATCF) and the IMS-AGW (ATGW) may support a media-level SDP image attribute "a=imageattr" defined in IETF RFC 6236 [24] to negotiate the image size for sending and receiving video.

The list of image sizes per payload type supported by the IMS-AGW (ATGW) shall be preconfigured in the IMS-ALG (ATCF). If the image sizes received within an SDP body on the Mw/Mx interface are not all supported by the IMS-AGW (ATGW) then the IMS-ALG (ATCF) shall only send the list of corresponding IMS-AGW (ATGW) supported image sizes to the IMS-AGW (ATGW). If no image size is supported by the IMS-AGW (ATGW), the IMS-ALG (ATCF) shall not send the generic image attribute parameter to the IMS-AGW (ATGW).

The signalling flow shown in figure 6.2.14.3.1 gives an example for a PS session establishment with media anchored in the IMS-AGW (ATGW). The following additional actions may be performed if the negotiation of the image size is supported by the IMS-ALG/IMS-AGW:

a) upon receipt of an SDP offer containing the image attribute(s) and if the received image sizes are supported by the IMS-AGW (ATGW) then the IMS-ALG (ATCF) may send the generic image attribute parameters for the send and receive directions to the IMS-ALG (ATCF) (step 2 or step 8) when seizing or modifying an outgoing termination;

NOTE 1: If the offered image attributes are not supported by the IMS-AGW (ATGW) then the IMS-ALG (ATCF) will not send the generic image attribute parameter to the IMS-AGW (ATGW).

b) the IMS-ALG (ATCF) shall include the SDP image attribute(s) "a=imageattr" indicating the supported image sizes in the modified SDP offer (step 5);

c) upon receipt of an SDP answer containing the generic image attribute(s) and if the received image sizes are supported by the IMS-AGW (ATGW) then the IMS-ALG (ATCF) may include the generic image attribute parameter to the IMS-AGW (ATGW) (step 11) when seizing an incoming termination; and

d) the IMS-ALG (ATCF) shall include the SDP image attribute(s) "a=imageattr" indicating the supported image sizes in the modified SDP answer (step 14).

NOTE 2: The IMS-ALG (ATCF) not supporting the negotiation of generic image attributes will ignore the SDP image attribute received in the SDP offer and will send the SDP offer/answer without any associated SDP image attribute.

When sending the SDP body with image attribute(s) on the Mw/Mx interface the IMS-ALG (ATCF) shall include in the "a=imageattr":

- "recv" keyword and corresponding image sizes which the IMS-AGW (ATGW) supports in the receiving direction; and

- "send" keyword and corresponding image sizes which the IMS-AGW (ATGW) supports in the sending direction.

The signalling flow shown in figure 6.2.14.4.1 gives an example for PS to CS access transfer with media anchored in the IMS-AGW (ATGW). The following additional actions may be performed if the negotiation of the image size is supported by the IMS-ALG/IMS-AGW:

a) if the image sizes were negotiated during the PS session and if the IMS-AGW (ATGW) applies the video transcoding (step 3) and if the IMS-AGW (ATGW) 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 [21] when sending media.

NOTE 3: The relation between the negotiated image sizes and CVO are specified in 3GPP TS 26.114 [21].

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.

6.2.14.6.2 Indication of generic image attributes

The IMS-ALG (ATCF) may include the generic image attributes to the IMS-AGW (ATGW). The example sequence is shown in figure 6.2.14.6.2.1.

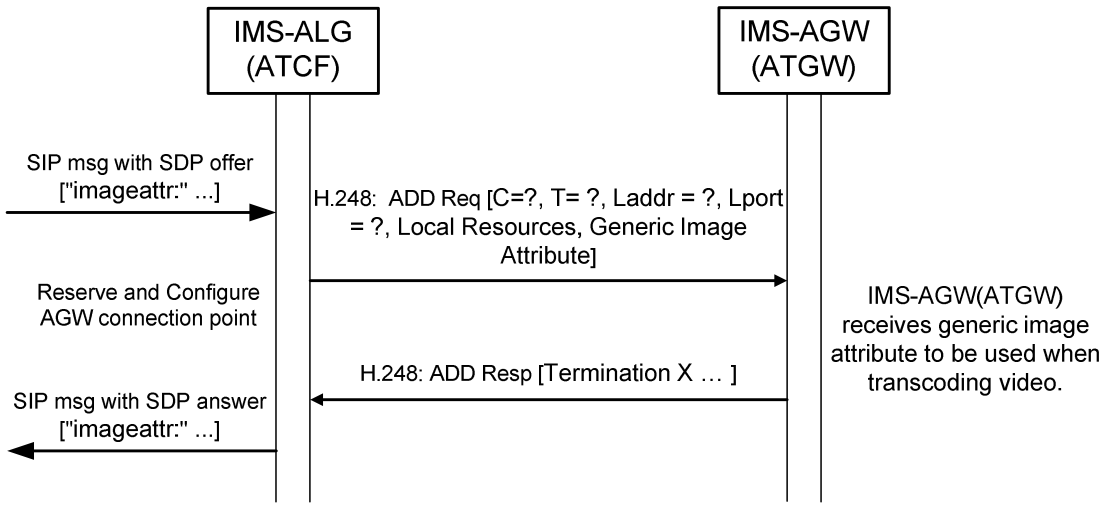


Figure 6.2.14.6.2.1: Request to reserve AGW connection point with generic image attribute

6.2.15 Multimedia Priority Congestion Control Procedures

6.2.15.1 General

The IMS-ALG and IMS-AGW may support the priority treatment of a call/session identified as an MPS call/session. This clause describes the Iq signalling procedures and their interactions with SIP signalling in the control plane and with user plane procedures to support the requirements for Multimedia Priority Service. These Iq signalling procedures may or may not apply depending on the network configuration (e.g. whether the IMS-AGW is shared by multiple IMS-ALGs or whether the IMS-ALG controls multiple IMS-AGWs for a given route – Media Gateway Group).

The IMS-ALG can receive a SIP INVITE with MPS priority information (see 3GPP TS 23.228 [2], subclause 5.21).

6.2.15.2 IMS-AGW Resource Congestion in ADD response, request is queued

If the IMS-ALG requests a resource via the procedure Reserve and Configure AGW Connection Point or Reserve AGW Connection Point and receives an error indicating that the requested resource could not be seized (e.g. H.248 error code #510 "insufficient resources") and the IMS-ALG does not have alternative IMS-AGW through which it can route the call it queues the priority session and gives it priority over any further Reserve and Configure AGW Connection Point or Reserve AGW Connection Point procedures for lower priority sessions towards this IMS-AGW until the requested resource for this queued session is successful seized. The example sequence is shown in Figure 6.2.15.2.1.

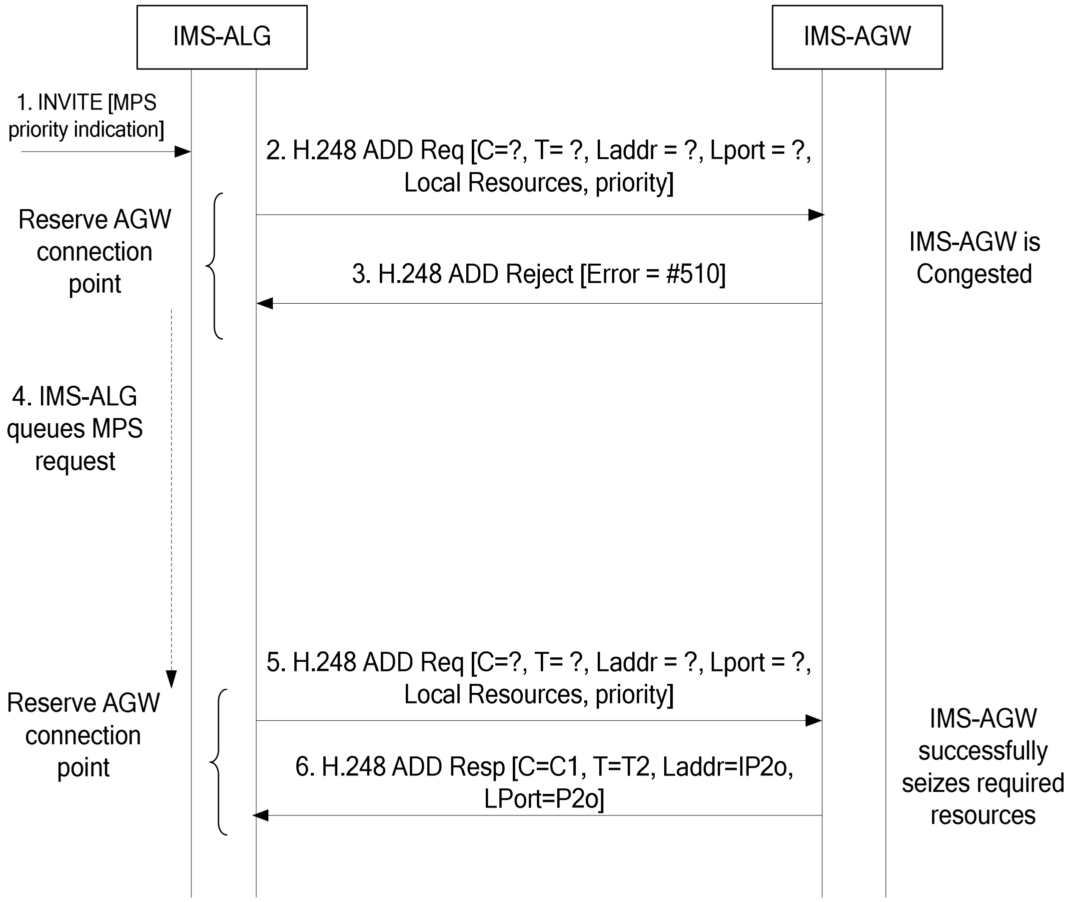


Figure 6.2.15.2.1: Request to reserve IMS-AGW MPS Priority call resources when IMS-AGW is congested

6.2.15.3 IMS-AGW Resource Congestion in ADD response, IMS-ALG seizes new IMS-AGW

If the IMS-ALG requests a resource via the procedure Reserve and Configure AGW Connection Point or Reserve AGW Connection Point and receives an error indicating that the requested resources could not be seized (e.g. H.248 error code #510 "insufficient resources") and Media Gateway Groups are implemented it should seize a new IMS-AGW from the same Media Gateway Group before resorting to any queuing of the priority session (as described in 6.2.15.2) to enable the MPS call/session to proceed as early as possible.

6.2.15.4 IMS-AGW Priority Resource Allocation

If the IMS-AGW supports the Priority information (e.g. determined through provisioning or package profile) the IMS-ALG requests a resource via the procedure Reserve and Configure AGW Connection Point or Reserve AGW Connection Point and includes the Priority information. The IMS-AGW may then provide priority allocation of resources once a congestion threshold is reached. If the IMS-AGW is completely congested it shall indicate this to the IMS-ALG as described in 6.2.15.2. The example sequence is shown in Figure 6.2.15.4.1.

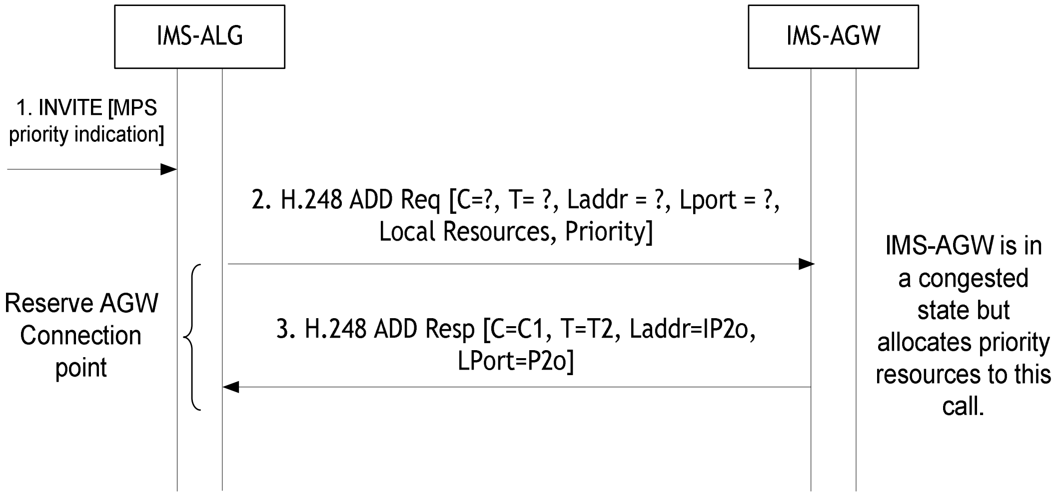


Figure 6.2.15.4.1: Request to reserve IMS-AGW MPS Priority call resources when IMS-AGW is congested, priority resources are allocated

6.2.15.5 IMS-AGW Priority User Data marking

The IMS-ALG may request the streams associated to an MPS Priority Call to be marked with certain priority code point as described in subclause 6.2.7. The IMS-AGW shall then mark each IP packet header accordingly. The example sequence is shown in Figure 6.2.15.5.1.

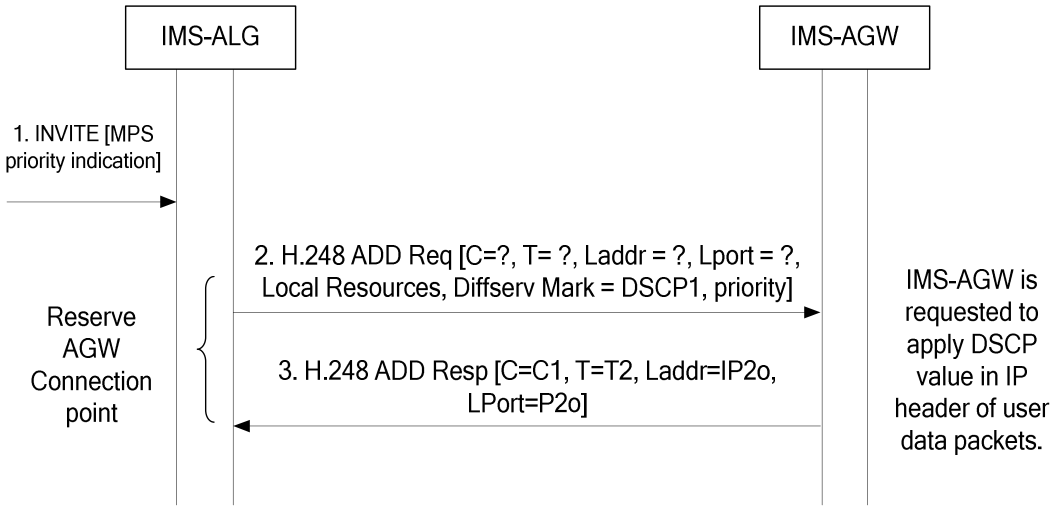


Figure 6.2.15.5.1: Request to reserve IMS-AGW call resources and apply DCSP marking for MPS

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

6.2.15.6 IMS-AGW Priority Modification

If the IMS-ALG 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 IMS-AGW (e.g. subject to subsequent authorisation by an authorisation point, see 3GPP TS 24.229 [11] subclause 4.11), the IMS-ALG 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 IMS-AGW via the Configure AGW Connection Point Procedure.

NOTE: The specific Iq related call sequence which details the handling to support the requirements defined in 3GPP TS 24.229 [11], subclause 4.11 and 3GPP TS 23.228 [2], 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 Iq interface.

6.2.16 Coordination of Video Orientation

Figure 6.2.16.1 shows the message sequence chart example for indicating extended RTP header for Coordination of Video Orientation.

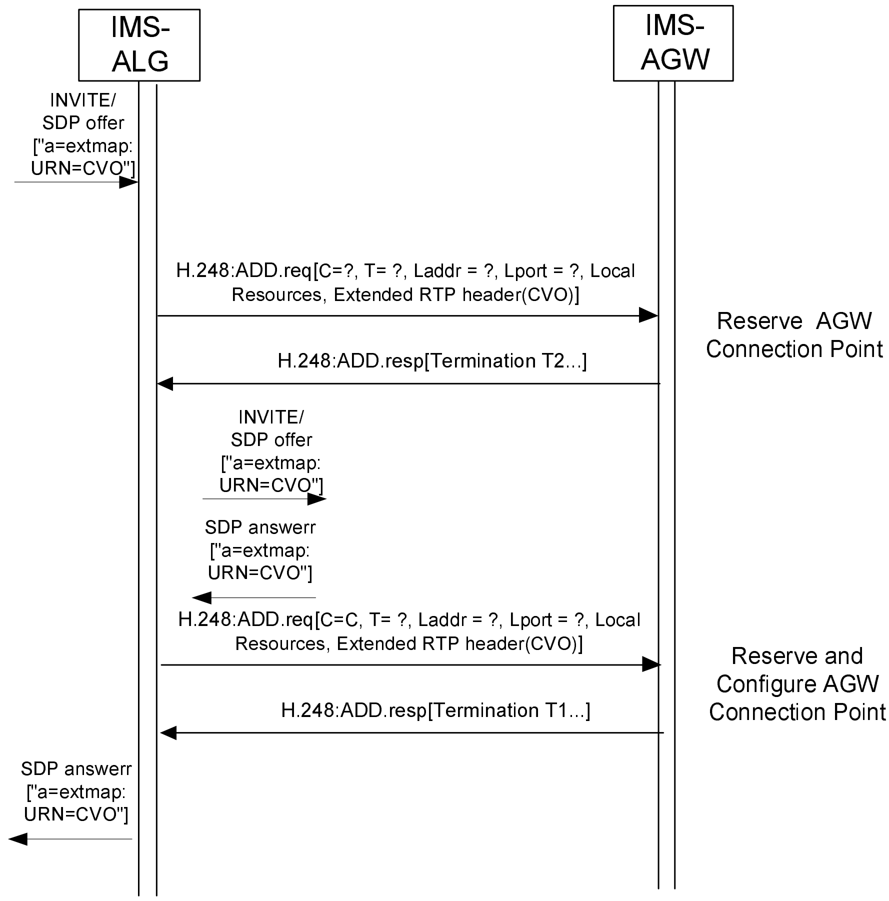


Figure 6.2.16.1: Procedure to indicate RTP extension header for CVO

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG optionally requesting the IMS-AGW to support the RTP Header Extension capability as defined in IETF RFC 5285 [23].

NOTE: If the IMS-ALG receives an SDP answer, which includes the "a=extmap" attribute with a CVO URN with a granularity that the IMS-AGW 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 IMS-AGW settings for this reason alone. Doing that would only add unnecessary signalling without requiring any action or changes in the IMS-AGW. However, if the IMS-ALG needs to modify the media attributes for other purposes, in particular due to transcoding, then the IMS-AGW is updated in accordance with the received SDP answer, that is, either with the received CVO related "a=extmap" attribute if present in the received SDP answer or without it if not included in the received SDP answer (thus removing the requirement for supporting "a=extmap" and for sending the header and CVO bits for the transcoded stream).

6.2.17 Procedures for Interactive Connectivity Establishment (ICE)

6.2.17.1 ICE lite

Figure 6.2.17.1.1 shows a message sequence chart example for performing the ICE lite procedure towards the offerer.

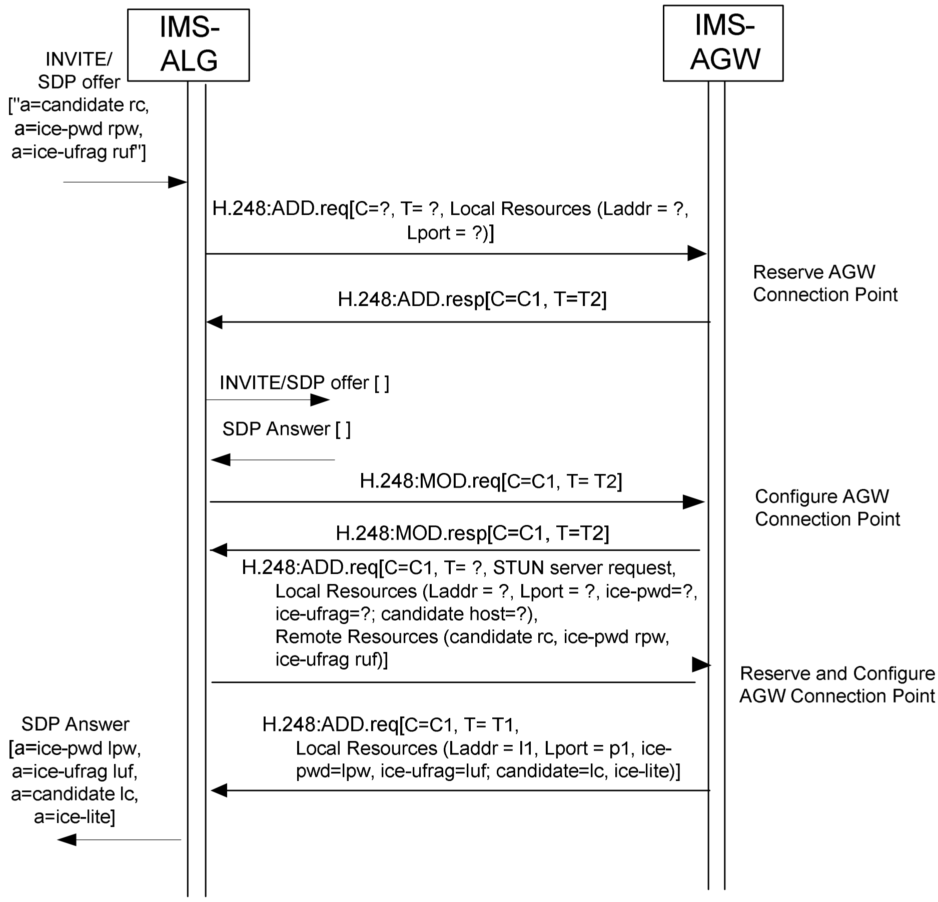


Figure 6.2.17.1.1: Procedure for interactive connectivity establishment using ICE lite towards the offerer

6.2.17.2 Full ICE

Figure 6.2.17.2.1 shows a message sequence chart example for performing the full ICE procedure towards the offerer.

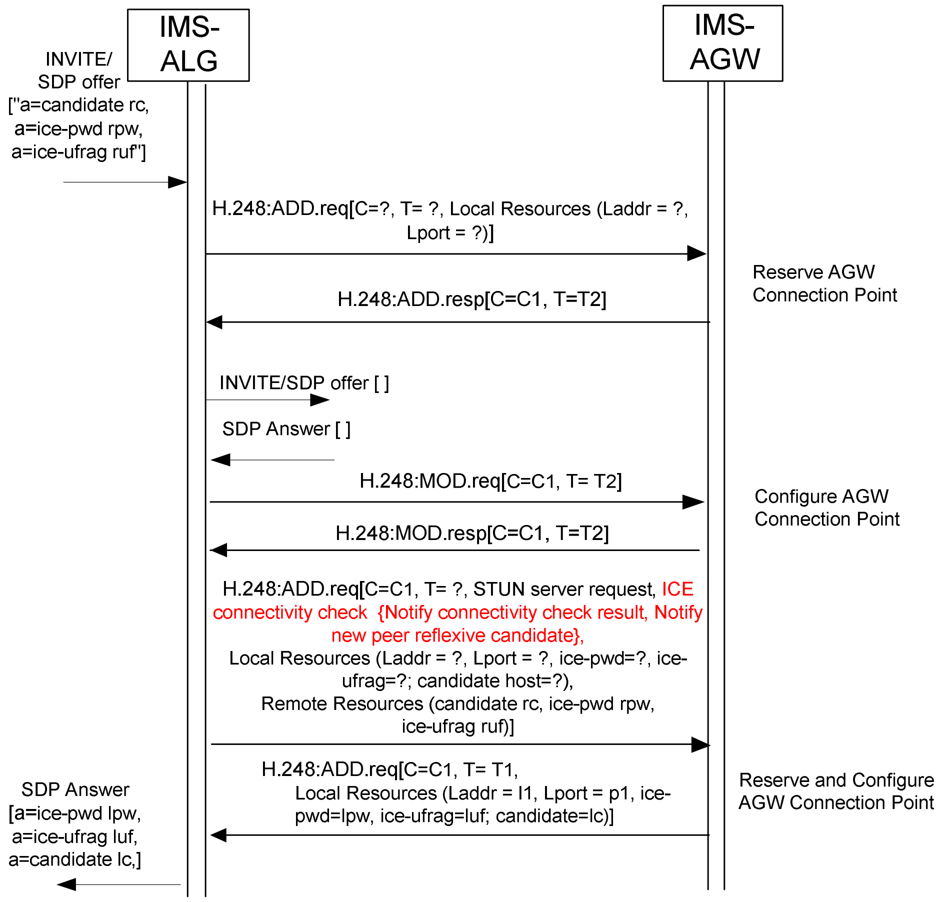


Figure 6.2.17.2.1: Procedure for interactive connectivity establishment using full ICE towards the offerer

6.2.17.3 Connectivity check result notification (full ICE)

Figure 6.2.17.3.1 shows the message sequence chart example for an ICE connectivity check result Event.

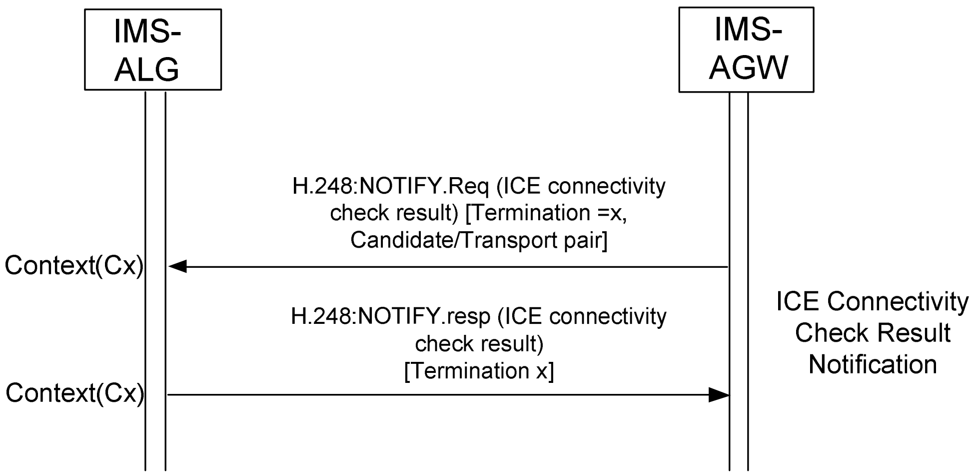


Figure 6.2.17.3.1: Procedure to report ICE connectivity check result

6.2.17.4 New peer reflexive candidate notification (full ICE)

Figure 6.2.17.4.1 shows the message sequence chart example for additional connectivity check when new peer reflexive candidate is discovered in full ICE.

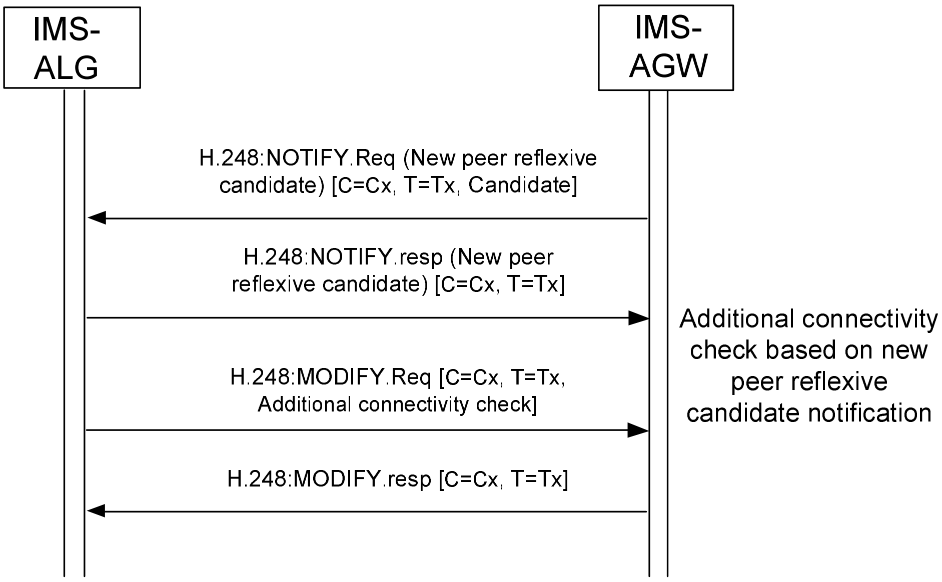


Figure 6.2.17.4.1: Procedure to perform additional connectivity check upon the report of new peer reflexive candidate

6.2.18 TCP bearer connection control

6.2.18.1 General

All message sequence charts in this clause are examples. The H.248 context model is defined in Figure 6.2.1.1.

6.2.18.2 Stateless TCP handling

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG and IMS-AGW applying the requirements specified in subclause 5.16.1.

6.2.18.3 State-aware TCP handling without support of modifying the TCP setup direction

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG and IMS-AGW applying the requirements specified in subclause 5.16.2.2.

Subclause 6.2.10.3.1 provides example call flows for TCP bearer connection establishment without modyfing the TCP setup direction.

6.2.18.4 State-aware TCP handling with support of modifying the TCP setup direction

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG and IMS-AGW applying the requirements specified in subclause 5.16.2.3.

Figure 6.2.18.4.1 shows an example call flow for a terminating session set-up procedure, where the IMS-ALG receives an incoming SDP offer containing media line for a new MSRP media stream with an "a=setup:active" SDP attribute towards a served UE located behind a remote NAT.

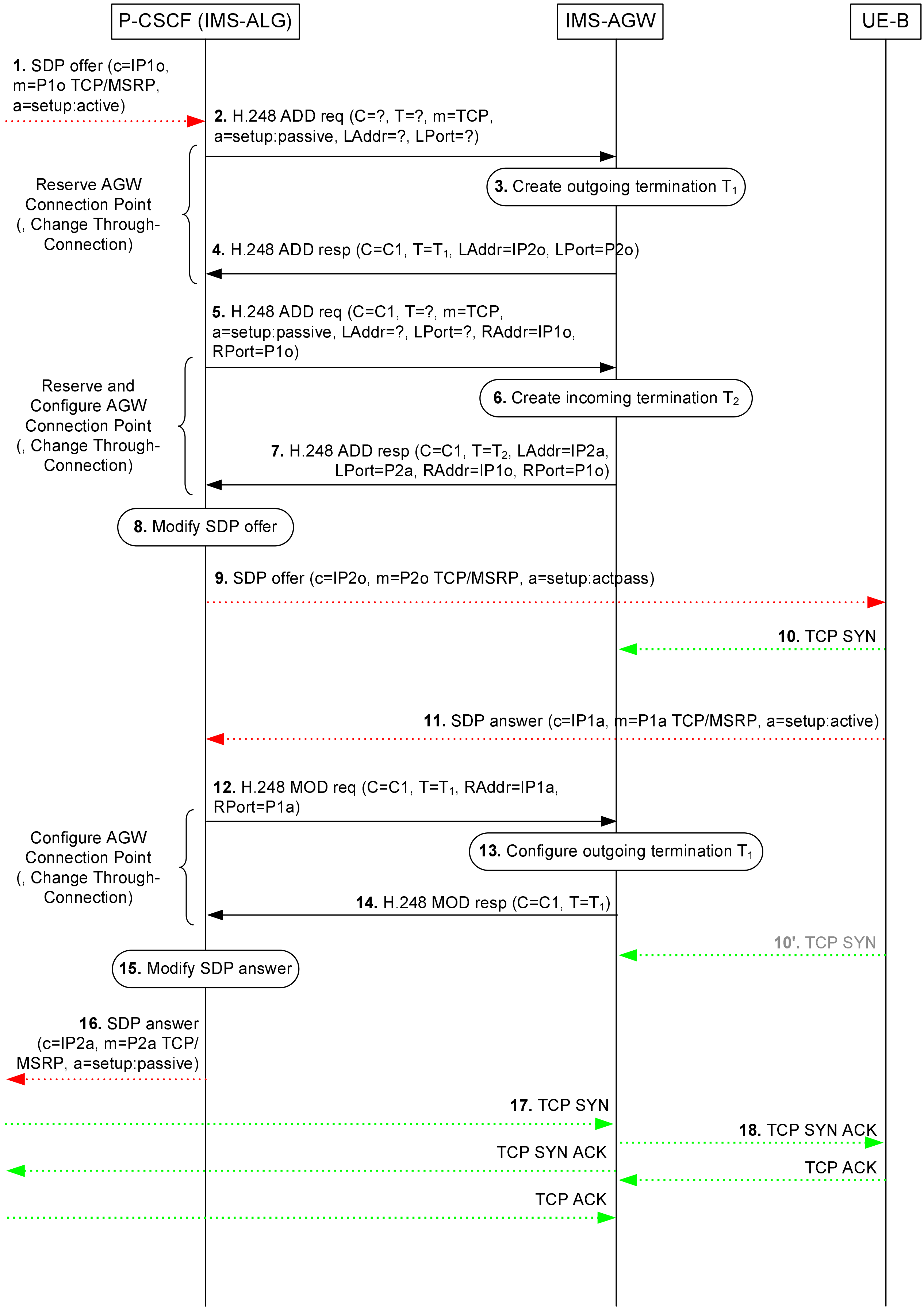


Figure 6.2.18.4.1: Terminating example call flow for MSRP between UEs located behind NAT

The IMS UE B performs an IMS terminating session set-up according to 3GPP TS 23.228 [2], with modifications as described in 3GPP TS 33.328 [12].

The procedure in the above figure is described step-by-step with an emphasis on the additional aspects for IMS-ALG and IMS-AGW of TCP bearer connection control.

1. The P-CSCF (IMS-ALG) receives an SDP offer for an MSRP media stream with an "a=setup:active" attribute. For the MSRP media stream offered with transport "TCP/MSRP", the P-CSCF (IMS-ALG) allocates the required resources, includes the IMS-AGW in the media path and proceeds as specified in this clause.

2.-4. The IMS-ALG uses the "Reserve AGW Connection Point" procedure to request a termination for "TCP" media (for application-agnostic interworking) or "TCP/MSRP" media (for application-aware interworking) towards the access network. The IMS-ALG preconfigures the IMS-AGW to operate in TCP merge mode by providing the "a=setup:passive" attribute.

5.-7. The IMS-ALG uses the "Reserve And Configure AGW Connection Point" procedure to request a termination for "TCP" media (for application-agnostic interworking) or "TCP/ MSRP" media (for application-aware interworking) towards the core network. The IMS-ALG preconfigures the IMS-AGW to operate in TCP Merge mode by providing the "a=setup:passive" attribute.

8. The P-CSCF (IMS-ALG) changes the "a=setup" SDP attribute to "actpass" in the SDP offer and inserts the address information received from the IMS-AGW.

9. The P-CSCF (IMS-ALG) forwards the SDP offer.

10. The UE B chooses to become the active party in the TCP connection establishment and sends a TCP SYN to establish the TCP connection. If the P-CSCF (IMS-ALG) indicated to the IMS-AGW at step 2 that it shall ignore any incoming TCP connection establishment requests (TCP SYN), e.g. to enable a remote source transport address filtering, or if the P-CSCF (IMS-ALG) did not indicate to the IMS-AGW at step 2 that it shall latch onto the required destination address via the source address/port of the incoming media, the IMS-AGW shall drop the TCP SYN received from the UE.
If the TCP SYN is not answered before a timer expiry, the UE will send the TCP SYN a second time (step 10').

11. The P-CSCF (IMS-ALG) receives the SDP answer. It contains the SDP answer with an "a=setup:active" attribute.

12.-14.The IMS-ALG uses the "Configure AGW Connection Point" procedure to configure the termination towards the UE B with remote address information.

15. The P-CSCF (IMS-ALG) modifies the SDP answer before sending it to the core network. The P-CSCF (IMS-ALG) sets the "a=setup:passive" SDP attribute.

16. The P-CSCF (IMA-ALG) then sends the updated SDP answer to core network.

17. The IMS-AGW answers the TCP SYN and the remote peer completes the TCP connection establishment.

18. The IMS-AGW answers the TCP SYN and UE B completes the TCP connection establishment.

6.2.19 Application-aware MSRP interworking at the IMS-AGW

This procedure is identical to that of subclause 6.2.1 apart from the IMS-ALG:

- indicating "TCP/MSRP" or "TCP/TLS/MSRP" (if e2ae media security is applied) as transport protocol to the IMS-AGW;

- configuring the IMS-AGW to apply application-aware MSRP interworking; and

- providing the SDP "a=path" attribute, as received in SIP/SDP signalling, to the IMS-AGW as "MSRP Path" with the remote descriptor of the corresponding call leg.

The IMS-AGW applies application-aware MSRP interworking if being instructed from the IMS-ALG. Support of dynamic instructions from the IMS-ALG is optional.

If the IMS-AGW applies application-aware MSRP interworking, it modifies the MSRP "To-Path" header field in MSRP packets by replacing the IP address and TCP port of the only entry with the corresponding information in the "MSRP path" provided by the IMS_ALG while retaining the MSRP session ID part of the entry as received in the MSRP "To-Path" and then forward the MSRP data without further modification.

7 Charging

The charging is specified in 3GPP TS 32.260 [5]. No requirements are identified for the Iq interface.

8 Messages/Procedures and Contents

8.1 General

This clause describes logical signalling procedures between the IMS-ALG and IMS-AGW. The procedures within this clause are intended to be implemented using the standard H.248 procedure as defined in ITU recommendation H.248.1 [9] with appropriate parameter combinations.

NOTE: Whenever the stage 2 description is referring to a "(stage 2) information element", then there is the premise of a one-to-one mapping to a stage 3 signalling element.

8.2 Reserve and Configure AGW Connection Point

This procedure is used to reserve multimedia-processing resources for the Iq interface connection.

Table 8.2.1: Procedures between IMS-ALG and IMS-AGW: Reserve and Configure AGW Connection Point

Procedure	Initiated	Information element name	Information element required	Information element description
Reserve and Configure AGW Connection Point	IMS-ALG	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 IMS-AGW to apply priority treatment for the terminations and bearer connections in the specified context.
		Bearer Termination Request	M	This information element indicates the existing bearer termination or requests a new bearer termination for the bearer to be established.
		Local IP Resources	O	This information element indicates the resource(s) for which the IMS-AGW shall be prepared to receive user data. May be excluded (i.e. "-" is used in SDP m-line) if no transcoding or media related functions are required. For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream.
		ReserveValue	O	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.
		Remote IP Resources	O	This information element indicates the resource(s) for which the IMS-AGW shall send data. For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream. May be excluded (i.e. "-" is used in SDP m-line) if no transcoding or media related functions are required.
		Local Connection Address Request	M	This information element requests an IP address and port number(s) on the IMS-AGW that the remote end can send user plane data to. For terminations supporting any combination of video, audio and messaging this may contain multiple addresses.

		Remote Connection Address	M	This information element indicates the remote IP address and port number(s) that the IMS-AGW can send user plane data to. For terminations supporting any combination of video, audio and messaging this may contain multiple addresses.
		Notify termination heartbeat	M	This information element requests termination heartbeat indications. This information element shall be included when requesting a new bearer termination. Otherwise the information element is optional.
		Notify Released Bearer	O	This information element requests a notification of a released bearer.
		Latching Requirement	O	This information element indicates that the IMS-AGW should (re)latch onto the address of received media packets to determine the corresponding destination address.
		IP Realm Identifier	O	This information element indicates the IP realm of the bearer termination.
		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 is required if a range of remote source address filtering is required.
		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. (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. (NOTE 1)
		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 bearer termination.
		DiffServ Tagging Behaviour	O	This information element indicates whether the Diffserv code point in the IP header in packets sent on the bearer termination shall 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.

		Media Inactivity Detection Time	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection time.
		Media Inactivity Detection Direction	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection direction.
		RTCP handling	O	This information element is present if IMS-ALG wants explicitly control the reservation of RTCP resources by the IMS-AGW.
		Local cryptographic SDES attribute	C	This information element is present if IMS-ALG wants that the media is encrypted and/or integrity protected by the IMS-AGW (NOTE 3). It indicates the SDES local cryptographic parameters such as key(s)
		Remote cryptographic SDES attribute	C	This information element is present if IMS-ALG wants that the media is decrypted, and/or integrity checked by the IMS-AGW (NOTE 3). It indicates the SDES remote cryptographic parameters such as key(s)
		ECN Enable	O	This information element requests the IMS-AGW to apply ECN procedures.
		ECN Initiation Method	C	This information element specifies the ECN Initiation method and requests the IMS-AGW 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.
		Notify ECN Failure Event	C	This information element requests a notification if a ECN failure occurs due to ECN. It may only be supplied if ECN is enabled and the IMS-AGW acts as ECN endpoint.
		Extended RTP Header for CVO	O	This information element requests the IMS-AGW to pass on the CVO extended RTP header as defined by IETF RFC 5285 [23].
		Generic Image Attributes	O	This information element indicates image attributes (e.g. image size) as defined by IETF RFC 6236 [24].
		Local certificate fingerprint Request	O	This information element is present if the IMS-ALG wants that the media is decrypted, and/or integrity protected by the IMS-AGW (NOTE 3). It requests the IMS-AGW to provide a local certificate fingerprint.
		Remote certificate fingerprint	O	This information element is present if the IMS-ALG wants that the media is decrypted, and/or integrity checked by the IMS-AGW (NOTE 3). It indicates the remote certificate fingerprint.
		Establish (D)TLS session	O	This information element requests the IMS-AGW to take the (D)TLS client role and to initiate the establishment of the (D)TLS session. (NOTE 3)
		Notify (D)TLS session establishment Failure Event	O	This information element requests a notification if a (D)TLS session establishment failure occurs. (NOTE 3)
		TCP State-aware Handling Indicator and Setup Direction	C	This information element indicates that TCP state-aware handing is required and indicates the TCP setup direction. It may only be included if the IMS-AGW supports TCP state-aware handling.
		Discard Incoming TCP Connection Establishment Requests Indicator	C	This information element indicates whether incoming TCP connection establishment requests (TCP SYN) shall be discarded. It may only be included if the IMS-AGW supports TCP state-aware handling and discarding incoming TCP connection establishment requests.

		Forward Incoming TCP Connection Establishment Requests Indicator	C	This information element indicates for a given termination to use the incoming TCP connection establishment request (TCP SYN) at that termination as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context. It may only be included if the IMS-AGW supports TCP state-aware handling and the Forward Incoming TCP Connection Establishment Requests Indicator.
		Notify TCP Connection Establishment Failure Event	C	This information element requests a notification if a TCP connection establishment failure occurs. It may only be included if the IMS-AGW supports TCP state-aware handling.
		STUN server request	O	This information element is present if IMS-ALG requests the IMS-AGW to answer STUN connectivity checks for ICE.
		ICE Connectivity Check	C	This information element requests the IMS-AGW to perform ICE connectivity check as defined by IETF RFC 5245 [39]. 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 IMS-ALG requests an ICE password.
		ICE Ufrag request	O	This information element is present if IMS-ALG requests an ICE ufrag.
		ICE host candidate request	O	This information element is present if IMS-ALG requests an ICE host candidate.
		ICE received candidate	O	This information element is present if IMS-ALG indicates a received candidate for ICE.
		ICE received password	O	This information element is present if IMS-ALG indicates a received password for ICE.
		ICE received Ufrag	O	This information element is present if IMS-ALG 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 IMS-AGW shall insert in the MSRP layer "To-Path" Information element.
		Application-aware MSRP interworking request	O	This information element is present if IMS-ALG requests the IMS-AGW to perform application-aware MSRP Interworking.
Reserve and Configure AGW Connection Point Ack	IMS-AGW	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.
		Local IP Resources	C	This information element indicates the resource(s) for which the IMS-AGW shall be prepared to receive user data. This IE shall be present if it was contained in the request. If the IE was not contained in the request, it may be present in the reply. For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream.

		Remote IP Resources	O	This information element indicates the resource(s) for which the IMS-AGW shall send data. For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream.
		Local Connection Address	M	This information element indicates the IP address and port number(s) the IMS-AGW shall receive user plane data from IMS. For terminations supporting any combination of video, audio and messaging this may contain multiple addresses.
		Remote Connection Address	O	This information element indicates the remote IP address and port number(s) that the IMS-AGW can send user plane data to. For terminations supporting any combination of video, audio and messaging this may contain multiple addresses.
		Local cryptographic SDES attribute	C	This information element may be present only if it was contained in the request. It indicates the SDES local cryptographic parameters such as key(s)
		Remote cryptographic SDES attribute	C	This information element may be present only if it was contained in the request. It indicates the SDES remote cryptographic parameters such as key(s)
		Local certificate fingerprint	C	This information element may be present only if the Local certificate fingerprint Request was contained in the request. It indicates the local certificate fingerprint. (NOTE 3)
		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 IMS-AGW.
		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 IMS-AGW.
		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 IMS-AGW.
		ICE lite indication	C	This information element shall be present only if an ICE host candidate request was contained in the request, and the IMS-AGW supports ICE lite, but not full ICE. It indicates that the IMS-AGW only supports ICE lite.
NOTE 1: Remote Source Port and Remote Source Port Range are mutually exclusive. NOTE 2: One of those IEs shall at least be present when policing is required. NOTE 3: This IE may only be present for access network terminations.				

8.3 Reserve AGW Connection Point Procedure

This procedure is used to reserve local connection addresses and local resources in IMS-AGW.

Table 8.3.1: Procedures between IMS-ALG and IMS-AGW: Reserve AGW Connection Point

Procedure	Initiated	Information element name	Information element required	Information element description
Reserve AGW Connection Point	IMS-ALG	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 IMS-AGW to apply priority treatment for the terminations and bearer connections in the specified context.
		Bearer Termination Request	M	This information element requests a new bearer termination
		Local IP Resources	O	This information element indicates the resource(s) for which the IMS-AGW shall be prepared to receive user data. For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream. May be excluded (i.e. "-" is used in SDP m-line) if no transcoding or media related functions are required.
		ReserveValue	O	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(s) on the IMS-AGW that the remote end can send user plane data to. For terminations supporting any combination of video, audio and messaging this may contain multiple addresses.
		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.
		Latching Requirement	O	This information element indicates that the IMS-AGW should (re)latch onto the address of received media packets to determine the corresponding destination address.
		IP Realm Identifier	O	This information element indicates the IP realm of the bearer termination.
		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 is required if a range of remote source address filtering is required.

		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. (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. (NOTE 1)
		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 bearer termination.
		DiffServ Tagging Behaviour	O	This information element indicates whether the Diffserv code point in the IP header in packets sent on the bearer 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.
		Media Inactivity Detection Time	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection time.
		Media Inactivity Detection Direction	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection direction.
		RTCP handling	O	This information element is present if IMS-ALG wants explicitly control the reservation of RTCP resources by the IMS-AGW.
		Local cryptographic SDES attribute	C	This information element is present if IMS-ALG wants that the media is encrypted and/or integrity protected by the IMS-AGW (NOTE 3). It indicates the SDES local cryptographic parameters such as key(s).
		ECN Enable	O	This information element requests the IMS-AGW to apply ECN procedures.
		ECN Initiation Method	C	This information element specifies the ECN Initiation method and requests the IMS-AGW 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.
		Notify ECN Failure Event	C	This information element requests a notification if a ECN failure occurs due to ECN. It may only be supplied if ECN is enabled and the IMS-AGW acts as ECN endpoint.

		Extended RTP Header for CVO	O	This information element requests the IMS-AGW to pass on the CVO extended RTP header as defined by IETF RFC 5285 [23].
		Generic Image Attributes	O	This information element indicates image attributes (e.g. image size) as defined by IETF RFC 6236 [24].
		Local certificate fingerprint Request	O	This information element is present if the IMS-ALG wants that the media is decrypted, and/or integrity protected by the IMS-AGW (NOTE 4). It requests the IMS-AGW to provide a local certificate fingerprint.
		Establish (D)TLS session	O	This information element requests the IMS-AGW to take the (D)TLS client role and to initiate the establishment of the (D)TLS session. (NOTE 4)
		Notify (D)TLS session establishment Failure Event	O	This information element requests a notification if a (D)TLS session establishment failure occurs. (NOTE 4)
		TCP State-aware Handling Indicator and Setup Direction	C	This information element indicates that TCP state-aware handing is required and indicates the TCP setup direction. It may only be included if the IMS-AGW supports TCP state-aware handling.
		Discard Incoming TCP Connection Establishment Requests Indicator	C	This information element indicates whether incoming TCP connection establishment requests (TCP SYN) shall be discarded. It may only be included if the IMS-AGW supports TCP state-aware handling and discarding incoming TCP connection establishment requests.
		Forward Incoming TCP Connection Establishment Requests Indicator	C	This information element indicates for a given termination to use the incoming TCP connection establishment request (TCP SYN) at that termination as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context. It may only be included if the IMS-AGW supports TCP state-aware handling and the Forward Incoming TCP Connection Establishment Requests Indicator.
		Notify TCP Connection Establishment Failure Event	C	This information element requests a notification if a TCP connection establishment failure occurs. It may only be included if the IMS-AGW supports TCP state-aware handling.
		ICE password request	O	This information element is present if IMS-ALG requests an ICE password.
		ICE Ufrag request	O	This information element is present if IMS-ALG requests an ICE ufrag.
		ICE host candidate request	O	This information element is present if IMS-ALG requests an ICE host candidate.
		STUN server request	O	This information element is present if IMS-ALG requests the IMS-AGW to answer STUN connectivity checks for ICE.
		Application-aware MSRP interworking request	O	This information element is present if IMS-ALG requests the IMS-AGW to perform application-aware MSRP Interworking.
Reserve AGW Connection Point Ack	IMS-AGW	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.

		Local IP Resources	C	This information element indicates the resource(s) for which the IMS-AGW shall be prepared to receive user data. This IE shall be present if it was contained in the request. If the IE was not contained in the request, it may be present in the reply. For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream.
		Local Connection Address	M	This information element indicates the IP address and port number(s) the IMS-AGW shall receive user plane data from IMS. For terminations supporting any combination of video, audio and messaging this may contain multiple addresses.
		Local cryptographic SDES attribute	C	This information element may be present only if it was contained in the request. It indicates the SDES local cryptographic parameters such as key(s)
		Local certificate fingerprint	C	This information element may be present only if the Local certificate fingerprint Request was contained in the request. It indicates the local certificate fingerprint. (NOTE 4)
		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 IMS-AGW.
		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 IMS-AGW.
		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 IMS-AGW.
		ICE lite indication	C	This information element shall be present only if an ICE host candidate request was contained in the request, and the IMS-AGW supports ICE lite, but not full ICE. It indicates that the IMS-AGW only supports ICE lite.
NOTE 1: Remote Source Port and Remote Source Port Range are mutually exclusive. NOTE 2: One of those IEs shall at least be present when policing is required. NOTE 3: This IE may only be present for access network terminations, and only if the IMS-ALG includes only one SDES crypto attribute in the SDP sent towards the served UE. NOTE 4: This IE may only be present for access network terminations.				

8.4 Configure AGW Connection Point Procedure

This procedure is used to select or modify multimedia-processing resources for the Iq interface connection.

Table 8.4.1: Procedures between IMS-ALG and IMS-AGW: Configure AGW Connection Point

Procedure	Initiated	Information element name	Information element required	Information element description
Configure AGW Connection Point	IMS-ALG	Context	M	This information element indicates the context for the bearer termination.
		Priority information	O	This information element shall be present if the priority information needs to be modified, it may be present otherwise.
		Bearer Termination	M	This information element indicates the existing bearer termination.
		Local IP Resources	O	This information element indicates the resource(s) for which the IMS-AGW shall be prepared to receive user data. For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream. May be excluded (i.e. "-" is used in SDP m-line) if no transcoding or media related functions are required.
		Remote IP Resources	O	This information element indicates the resource(s) for which the IMS-AGW shall send data. For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream. May be excluded (i.e. "-" is used in SDP m-line) if no transcoding or media related functions are required.
		Local Connection Address	O	This information element indicates the IP address and port number(s) on the IMS-AGW that the IMS user can send user plane data to. For terminations supporting video any combination of video, audio and messaging may contain multiple addresses.
		Remote Connection Address	O	This information element indicates the remote IP address and port number(s) that the IMS-AGW can send user plane data to. For terminations supporting any combination of video, audio and messaging this may contain multiple addresses.
		Latching Requirement	O	This information element indicates that the IMS-AGW should (re)latch onto the address of received media packets to determine the corresponding destination address.
		IP Realm Identifier	O	This information element indicates the IP realm of the bearer termination. (NOTE 3)

		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 is required if a range of remote source address filtering is required.
		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. (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. (NOTE 1)
		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 bearer termination.
		DiffServ Tagging Behaviour	O	This information element indicates whether the Diffserv code point in the IP header in packets sent on the bearer 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.
		Media Inactivity Detection Time	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection time.
		Media Inactivity Detection Direction	C	This information element may be present if Inactive Media Detection is required and specifies the Inactivity Detection direction.

		RTCP handling	O	This information element is present if IMS-ALG wants explicitly control the reservation of RTCP resources by the IMS-AGW.
		Local cryptographic SDES attribute	C	This information element is present if IMS-ALG wants that the media is encrypted and/or integrity protected by the IMS-AGW (NOTE 4). It indicates the SDES local cryptographic parameters such as key(s).
		Remote cryptographic SDES attribute	C	This information element is present if IMS-ALG wants that the media is decrypted, and/or integrity checked by the IMS-AGW (NOTE 4). It indicates the SDES remote cryptographic parameters such as key(s).
		ECN Enable	O	This information element requests the IMS-AGW to apply ECN procedures.
		ECN Initiation Method	C	This information element specifies the ECN Initiation method and requests the IMS-AGW 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.
		Notify ECN Failure Event	C	This information element requests a notification if a ECN failure occurs due to ECN. It may only be supplied if ECN is enabled and the IMS-AGW acts as ECN endpoint.
		Extended RTP Header for CVO	O	This information element requests the IMS-AGW to pass on the CVO extended RTP header as defined by IETF RFC 5285 [23].
		Generic Image Attributes	O	This information element indicates image attributes (e.g. image size) as defined by IETF RFC 6236 [24].
		Remote certificate fingerprint	O	This information element is present if the IMS-ALG wants that the media is decrypted, and/or integrity checked by the IMS-AGW (NOTE 4). It indicates the remote certificate fingerprint.
		Establish (D)TLS session	O	This information element requests the IMS-AGW to take the (D)TLS client role and to initiate the establishment of the (D)TLS session. (NOTE 4)
		Release (D)TLS session	O	This information element requests the IMS-AGW to release the (D)TLS session. (NOTE 4)
		Notify (D)TLS session establishment Failure Event	O	This information element requests a notification if a TLS session establishment failure occurs. (NOTE 4)
		TCP State-aware Handling Indicator and Setup Direction	C	This information element indicates that TCP state-aware handing is required and indicates the TCP setup direction. It may only be included if the IMS-AGW supports TCP state-aware handling.

		Discard Incoming TCP Connection Establishment Requests Indicator	C	This information element indicates whether incoming TCP connection establishment requests (TCP SYN) shall be discarded. It may only be included if the IMS-AGW supports TCP state-aware handling and discarding incoming TCP connection establishment requests.
		Forward Incoming TCP Connection Establishment Requests Indicator	C	This information element indicates for a given termination to use the incoming TCP connection establishment request (TCP SYN) at that termination as a trigger for sending a TCP connection establishment request at the interconnected termination in the same context. It may only be included if the IMS-AGW supports TCP state-aware handling and the Forward Incoming TCP Connection Establishment Requests Indicator.
		Send TCP Connection Establishment Requests Indicator	C	This information element indicates for a given termination to send a TCP connection establishment request (TCP SYN). It may only be included if the IMS-AGW supports TCP state-aware handling.
		Notify TCP Connection Establishment Failure Event	C	This information element requests a notification if a TCP connection establishment failure occurs. It may only be included if the IMS-AGW supports TCP state-aware handling.
		ICE Connectivity Check	C	This information element requests the IMS-AGW to perform ICE connectivity check as defined by IETF RFC 5245 [39]. 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 IMS-AGW to perform additional ICE connectivity check as defined by IETF RFC 5245 [39]. It is only applicable for full ICE.
		ICE received candidate	O	This information element is present if IMS-ALG indicates a received candidate for ICE.
		ICE received password	O	This information element is present if IMS-ALG indicates a received password for ICE.
		ICE received Ufrag	O	This information element is present if IMS-ALG 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 IMS-AGW shall insert in the MSRP layer "To-Path" Information element.
Configure AGW Connection	IMS-AGW	Context	M	This information element indicates the context where the command was executed.

Point Ack		Bearer Termination	M	This information element indicates the bearer termination where the command was executed.
		Local IP Resources	O	This information element indicates the resource(s) for which the IMS-AGW shall be prepared to receive user data For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream.
		Remote IP Resources	O	This information element indicates the resource(s) for which the IMS-AGW shall send data. For terminations supporting any combination of video, audio and messaging this IE shall contain separate resources per stream.
		Local Connection Address	O	This information element indicates the IP address and port number(s) on the IMS-AGW that the IMS user can send user plane data to. For terminations supporting any combination of video, audio and messaging this may contain multiple addresses.
		Remote Connection Address	O	This information element indicates the remote IP address and port number(s) that the IMS-AGW can send user plane data to. For terminations supporting any combination of video, audio and messaging this may contain multiple addresses.
		Local cryptographic SDES attribute	C	This information element may be present only if it was contained in the request. It indicates the SDES local cryptographic parameters such as key(s)
		Remote cryptographic SDES attribute	C	This information element may be present only if it was contained in the request. It indicates the SDES remote cryptographic parameters such as key(s)
NOTE 1: Remote Source Port and Remote Source Port Range are mutually exclusive. NOTE 2: One of those IEs shall at least be present when policing is required. NOTE 3: Additional streams may be added by the Configure AGW Connection Point procedure. The additional streams shall then carry the same IP Realm Identifier as the very first Stream. NOTE 4: This IE may only be present for access network terminations.				

Editor's Note : The details of how the transparent indication included in ECN Control is subject of stage 3 specification. It also needs to be determined if this indication is needed on both incoming and outgoing terminations.

8.5 Release AGW Termination

This procedure is used to release a termination towards the IMS and free all related resources.

Table 8.5.1: Procedures between IMS-ALG and IMS-AGW: Release AGW Termination

Procedure	Initiated	Information element name	Information element required	Information element description
Release AGW Termination	IMS-ALG	Context	M	This information element indicates the existing context for the bearer termination.
		Bearer Termination	M	This information element indicates the bearer termination to be released.
Release AGW Termination Ack	IMS-AGW	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.

8.6 Termination heartbeat indication

This procedure is used to report a termination heartbeat.

Table 8.6.1: Procedures between IMS-ALG and IMS-AGW: Termination heartbeat indication

Procedure	Initiated	Information element name	Information element required	Information element description
Termination heartbeat indication	IMS-AGW	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, as defined in 3GPP TS 29.334 [3].
Termination heartbeat indication Ack	IMS-ALG	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.

8.7 IMS-AGW Out-of-Service

This procedure is used to indicate that the IMS-AGW will go out of service or is maintenance locked.

Table 8.7.1: Procedures between IMS-ALG and IMS-AGW: IMS-AGW Out-of-Service

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-AGW Out-of-Service	IMS-AGW	Context	M	This information element indicates the context for the command.
		Root Termination	M	This information element indicates the root termination for the command.
		Reason	M	This information element indicates the reason for service change.
		Method	M	This information element indicates the method for service change.
IMS-AGW Out-of-Service Ack	IMS-ALG	Context	M	This information element indicates the context where the command was executed.
		Root Termination	M	This information element indicates the root termination where the command was executed.

8.8 IMS-AGW Communication Up

This procedure is used to indicate that the IMS-AGW is back in service using an existing control association.

Table 8.8.1: Procedures between IMS-ALG and IMS-AGW: IMS-AGW Communication Up

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-AGW Communication Up	IMS-AGW	Context	M	This information element indicates the context for the command.
		Root Termination	M	This information element indicates the root termination for the command.
		Reason	M	This information element indicates the reason for service change.
		Method	M	This information element indicates the method for service change.
IMS-AGW Communication Up Ack	IMS-ALG	Context	M	This information element indicates the context where the command was executed.
		Root Termination	M	This information element indicates the root termination where the command was executed.
		IMS-ALG Address	O	This information element indicates the IMS-ALG signalling address to which the IMS-AGW should preferably attempt to re-register.

8.9 IMS-AGW Restoration

This procedure is used to indicate the IMS-AGW has recovered from a failure.

Table 8.9.1: Procedures between IMS-ALG and IMS-AGW: IMS-AGW Restoration

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-AGW Restoration	IMS-AGW	Context	M	This information element indicates the context for the command.
		Root Termination	M	This information element indicates the root termination for the command.
		Reason	M	This information element indicates the reason for the service change.
		Method	M	This information element indicates the method for service change.
IMS-AGW Restoration Ack	IMS-ALG	Context	M	This information element indicates the context where the command was executed.
		Root Termination	M	This information element indicates the root termination where the command was executed.
		IMS-ALG Address	O	This information element indicates the IMS-ALG signalling address to which the IMS-AGW should preferably attempt to re-register.

8.10 IMS-AGW Register

This procedure is used to register the IMS-AGW after a cold/warm boot.

Table 8.10.1: Procedures between IMS-ALG and IMS-AGW: IMS-AGW Register

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-AGW Register	IMS-AGW	Context	M	This information element indicates the context for the command.
		Root Termination	M	This information element indicates the root termination for the command.
		Reason	M	This information element indicates the reason for the service change.
		Method	M	This information element indicates the method for service change.
		Protocol Version	M	This information element indicates the protocol version for Iq interface requested by the IMS-AGW.
		Service Change Profile	M	This information element indicates the profile for the Iq interface requested by the IMS-AGW.
IMS-AGW Register Ack	IMS-ALG	Context	M	This information element indicates the context where the command was executed.
		Root Termination	M	This information element indicates the root termination where the command was executed.
		Protocol Version	O	This information element indicates the protocol version for Iq interface supported by the IMS-ALG.
		Service Change Profile	O	This information element indicates the profile for the Iq interface supported by the IMS-ALG.
		IMS-ALG Address	O	This information element indicates the IMS-ALG signalling address to which the IMS-AGW should preferably attempt to re-register.

8.11 IMS-ALG Restoration

This procedure is used to indicate the IMS-ALG has recovered from a failure.

Table 8.11.1: Procedures between IMS-ALG and IMS-AGW: IMS-ALG Restoration

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-ALG Restoration	IMS-ALG	Context	M	This information element indicates the context for the command.
		Root Termination	M	This information element indicates the root termination for the command.
		Reason	M	This information element indicates the reason for the service change.
		Method	M	This information element indicates the method for service change.
IMS-ALG Restoration Ack	IMS-AGW	Context	M	This information element indicates the context where the command was executed.
		Root Termination	M	This information element indicates the root termination where the command was executed.

8.12 IMS-AGW Re-register

This procedure is used to re-register the IMS-AGW (having been requested to do so by the IMS-ALG).

Table 8.12.1: Procedures between IMS-ALG and IMS-AGW: IMS-AGW Re-register

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-AGW Re-register	IMS-AGW	Context	M	This information element indicates the context for the command.
		Root Termination	M	This information element indicates the root termination for the command.
		Reason	M	This information element indicates the reason for the service change.
		Method	M	This information element indicates the method for service change.
		Protocol Version	M	This information element indicates the protocol version for Iq interface requested by the IMS-AGW.
		Service Change Profile	M	This information element indicates the profile for the Iq interface requested by the IMS-AGW.
IMS-AGW Re-register Ack	IMS-ALG	Context	M	This information element indicates the context where the command was executed.
		Root Termination	M	This information element indicates the root termination where the command was executed.
		Protocol Version	O	This information element indicates the protocol version for Iq interface supported by the IMS-ALG.
		Service Change Profile	O	This information element indicates the profile for the Iq interface supported by the IMS-ALG.
		IMS-ALG Address	O	This information element indicates the IMS-ALG signalling address to which the IMS-AGW should preferably attempt to re-register.

8.13 IMS-ALG Ordered Re-registration

This procedure is used by the IMS-ALG to request the IMS-AGW to re-register.

Table 8.13.1: Procedures between IMS-ALG and IMS-AGW: IMS-ALG Ordered Re-register

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-ALG Ordered Re-register	IMS-ALG	Context	M	This information element indicates the context for the command.
		Root Termination	M	This information element indicates the root termination for the command.
		Reason	M	This information element indicates the reason for the service change.
		IMS-ALG Address	O	This information element indicates the IMS-ALG signalling address.
IMS-ALG Ordered Re-register Ack	IMS-AGW	Context	M	This information element indicates the context where the command was executed.
		Root Termination	M	This information element indicates the root termination where the command was executed.

8.14 Audit Value

This procedure is used to audit values of different object(s).

Table 8.14.1: Procedures between IMS-ALG and IMS-AGW: Audit Value

Procedure	Initiated	Information element name	Information element required	Information element description
Audit Value	IMS-ALG	Context	M	This information element indicates the context for the command.
		Bearer Termination	M	This information element indicates the bearer termination(s) for the command.
		Object(s)	M	This information element indicates the object(s) to be audited.
Audit Value Ack	IMS-AGW	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.
		Value(s)	M	This information element indicates the value(s) of the object(s).

8.15 Audit Capability

This procedure is used to audit capabilities of different object(s).

Table 8.15.1: Procedures between IMS-ALG and IMS-AGW: Audit Capability

Procedure	Initiated	Information element name	Information element required	Information element description
Audit Capability	IMS-ALG	Context	M	This information element indicates the context for the command.
		Bearer Termination	M	This information element indicates the bearer termination(s) for the command.
		Object(s)	M	This information element indicates the object(s) which capability is requested.
Audit Capability Ack	IMS-AGW	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.
		Capabilities(s)	M	This information element indicates the capabilities of the object(s).

8.16 Capability Update

This procedure is used to indicate update of an object capability.

Table 8.16.1: Procedures between IMS-ALG and IMS-AGW: Capability Update

Procedure	Initiated	Information element name	Information element required	Information element description
Capability Update	IMS-AGW	Context	M	This information element indicates the context for the command.
		Bearer Termination	M	This information element indicates the bearer termination(s) for the command.
		Reason	M	This information element indicates the reason for service change.
		Method	M	This information element indicates the method for service change.
Capability Update Ack	IMS-ALG	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.

8.17 IMS-ALG Out of Service

This procedure is used to indicate that IMS-ALG has gone out of service.

Table 8.17.1: Procedures between IMS-ALG and IMS-AGW: IMS-ALG Out of Service

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-ALG Out of Service	IMS-ALG	Context	M	This information element indicates the context for the command.
		Root Termination	M	This information element indicates the root termination for the command.
		Reason	M	This information element indicates the reason for the service change.
		Method	M	This information element indicates the method for service change.
IMS-ALG Out of Service Ack	IMS-AGW	Context	M	This information element indicates the context where the command was executed.
		Root Termination	M	This information element indicates the root termination where the command was executed.

8.18 IMS-AGW Resource Congestion Handling - Activate

This procedure is used to activate the congestion handling mechanism.

Table 8.18.1: Procedures between IMS-ALG and IMS-AGW: IMS-AGW Resource Congestion Handling - Activate

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-AGW Resource Congestion Handling – Activate	IMS-ALG	Context	M	This information element indicates that all context are applicable for the root termination.
		Root Termination	M	This information element indicates that root termination is where the congestion mechanism is activated.
		Congestion Activate	M	This information element requests to activate the congestion mechanism.
IMS-AGW Resource Congestion Handling - Activate Ack	IMS-AGW	Context	M	This information element indicates that all context are where the command was executed.
		Root Termination	M	This information element indicates that root termination is where the command was executed.

8.19 IMS-AGW Resource Congestion Handling - Indication

This procedure is used to inform the IMS-ALG that traffic restriction is advised.

Table 8.19.1: Procedures between IMS-ALG and IMS-AGW: IMS-AGW Resource Congestion Handling -Indication

Procedure	Initiated	Information element name	Information element required	Information element description
IMS-AGW Resource Congestion Handling - Indication	IMS-AGW	Context	M	This information element indicates all context are applicable for the root termination.
		Root Termination	M	This information element indicates that root termination is where the congestion mechanism was activated.
		Reduction	M	This information element indicates the load percentage to be reduced.
IMS-AGW Resource Congestion Handling - Indication Ack	IMS-ALG	Context	M	This information element indicates all context are where the command was executed.
		Root Termination	M	This information element indicates that root termination is where the command was executed.

8.20 Inactivity Timeout Activate

This procedure is used to activate the inactivity timeout mechanism.

Table 8.20.1: Procedures between IMS-ALG and IMS-AGW: Inactivity Timeout Activate

Procedure	Initiated	Information element name	Information element required	Information element description
Inactivity Timeout Activate	IMS-ALG	Context	M	This information element indicates all context are applicable for the root termination.
		Root Termination	M	This information element indicates that root termination is where inactivity timeout mechanism was activated.
		Inactivity Timeout Activate	M	This information element activates the Inactivity Timeout request.
		Inactivity Timeout	O	This information element indicates the maximum length of time before triggering the related notification.
Inactivity Timeout Activate Ack	IMS-AGW	Context	M	This information element indicates all context are where the command was executed.
		Root Termination	M	This information element indicates that root termination is where the command was executed.

8.21 Inactivity Timeout Notification

This command is used to notify the IMS-ALG of an inactive control association.

Table 8.21.1: Procedures between IMS-AGW and IMS-ALG: Inactivity Timeout Notification

Procedure	Initiated	Information element name	Information element required	Information element description
Inactivity Timeout Notification	IMS-AGW	Context	M	This information element indicates all context are applicable for the root termination.
		Root Termination	M	This information element indicates that root termination is where the inactivity timeout mechanism was activated.
		Inactivity Timeout Notification	M	This information element notifies the IMS-ALG of an inactivity time period.
Inactivity Timeout Notifcation Ack	IMS-ALG	Context	M	This information element indicates all context are where the command was executed.
		Root Termination	M	This information element indicates that root termination is where the command was executed.

8.22 Command Reject

This command is used to reject the received command request. It may be used as response to any of the procedures.

Table 8.22.1: Procedures between IMS-ALG and IMS-AGW: Command Reject

Procedure	Initiated	Information element name	Information element required	Information element description
Command Reject	Both	Context	O	This information element indicates the context where the command was rejected.
		Bearer Termination	O	This information element indicates the bearer termination where the command was rejected.
		Error	M	This information element indicates the error that caused command rejection.

8.23 Realm Availability Activate

This command is used to request the IMS-AGW to monitor the status of its IP Realms and to report any changes to the IMS-ALG.

Table 8.23.1: Procedures between IMS-ALG and IMS-AGW: Realm Availability Activate

Procedure	Initiated	Information element name	Information element required	Information element description
Realm Availability Activate	IMS-ALG	Context	M	This information element indicates all context are applicable for the root termination.
		Root Termination	M	This information element indicates that root termination is where the realm availability monitoring was activated.
		Realm Availability Activate	M	This information element activates the monitoring of the availability of IP Realms on the IMS-AGW.
Realm Availability Activate Ack	IMS-AGW	Context	M	This information element indicates all context are where the command was executed.
		Root Termination	M	This information element indicates that root termination is where the command was executed.

8.24 Realm Availability Notification

This command is used to notify the IMS-ALG of any changes in the availability of IP Realms on the IMS-AGW.

Table 8.24.1: Procedures between IMS-ALG and IMS-AGW: Realm Availability Notification

Procedure	Initiated	Information element name	Information element required	Information element description
Realm Availability Notification	IMS-AGW	Context	M	This information element indicates all context are applicable for the root termination.
		Root Termination	M	This information element indicates that root termination is where the realm availability monitoring was activated.
		Realm Availability Changes	M	This information element notifies the IMS-ALG of newly available/unavailable IP Realms.
Realm Availability Notifcation Ack	IMS-ALG	Context	M	This information element indicates all context are where the command was executed.
		Root Termination	M	This information element indicates that root termination is where the command was executed.

8.25 IP Bearer Released

Table 8.25.1: Procedures between IMS-ALG and IMS-AGW: IP Bearer Released

Procedure	Initiated	Information element name	Information element required	Information element description
IP Bearer Released	IMS-AGW	Context	M	This information element indicates the context for the bearer termination.
		Bearer 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	IMS-ALG	Context	M	This information element indicates all context are where the command was executed.
		Bearer Termination	M	This information element indicates that Bearer termination is where the command was executed.

8.26 Media Inactivity Notification

This command is used to notify the IMS-ALG of media inactivity on the IMS-AGW.

Table 8.26.1: Procedures between IMS-ALG and IMS-AGW: Media Inactivity Notification

Procedure	Initiated	Information element name	Information element required	Information element description
Media Inactivity Notification	IMS-AGW	Context	M	This information element indicates the existing context for the bearer termination.
		Bearer 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 IMS-ALG of Media inactivity detection on the bearer termination.
Media Inactivity Notification Ack	IMS-ALG	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.

8.27 Termination Out-of-Service

This procedure is used to indicate that a termination on the IMS-AGW has gone out of service

Table 8.27.1: Procedures between IMS-ALG and IMS-AGW: Termination Out-of-Service

Procedure	Initiated	Information element name	Information element required	Information element description
Termination Out-of-Service	IMS-AGW	Context	M	This information element indicates the context for the command.
		Bearer Termination	M	This information element indicates the bearer termination(s) for the command.
		Reason	M	This information element indicates the reason for service change.
		Method	M	This information element indicates the method for service change.
Termination Out-of-Service Ack	IMS-ALG	Context	M	This information element indicates the context where the command was executed.
		Bearer Termination	M	This information element indicates the bearer termination(s) where the command was executed.

8.28 Change Through-Connection

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

Table 8.28.1: Procedures between IMS-ALG and IMS-AGW: Change Through-Connection

Procedure	Initiated	Information element name	Information element required	Information element description
Change Through-Connection	IMS-ALG	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	IMS-AGW	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 AGW Connection Point, Reserve AGW Connection Point or Configure AGW Connection Point procedure. This list of procedures is not exhaustive.

8.29 Change Flow Direction

This procedure is used to change the flow direction between bearer terminations within the context.

Table 8.29: Procedures between IMS-ALG and IMS-AGW: Configure AGW Connection Point

Procedure	Initiated	Information element name	Information element required	Information element description
Change Flow Direction	IMS-ALG	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	IMS-AGW	Context	M	This information element indicates the context where the command was executed.

8.30 ECN Failure Indication

This procedure is used to report ECN related failures (see clause 6.2.13.4).

Table 8.30.1: Procedures between IMS-ALG and IMS-AGW: ECN Failure Indication

Procedure	Initiated	Information element name	Information element required	Information element description
ECN Failure Indication	IMS-AGW	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 Failure Indication Ack	IMS-ALG	Context	M	This information element indicates the context where the command was executed.

8.31 Notify (D)TLS session establishment Failure Indication

This procedure is used to report (D)TLS session establishment failures.

Table 8.31.1: Procedures between IMS-ALG and IMS-AGW: (D)TLS session establishment Failure Indication

Procedure	Initiated	Information element name	Information element required	Information element description
(D)TLS session establishment Failure Indication	IMS-AGW	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 (D)TLS session establishment failure is reported.
		(D)TLS session establishment Error Indication	M	This information element indicates a (D)TLS session establishment failure event.
(D)TLS session establishment Failure Indication Ack	IMS-ALG	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.

8.32 Notify TCP connection establishment Failure Indication

This procedure is used to report TCP connection establishment failures.

Table 8.32.1: Procedures between IMS-ALG and IMS-AGW: TCP connection establishment Failure Indication

Procedure	Initiated	Information element name	Information element required	Information element description
TCP connection establishment Failure Indication	IMS-AGW	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 TCP connection establishment failure is reported.
		TCP connection establishment Error Indication	M	This information element indicates a TCP connection establishment failure event.
TCP connection establishment Failure Indication Ack	IMS-ALG	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.

8.33 ICE Connectivity Check Result Notification

This procedure is used to report ICE connectivity check result for Full ICE (see clause 6.2.17.3).

Table 8.33.1: Procedures between IMS-ALG and IMS-AGW: ICE Connectivity Check Result Notification

Procedure	Initiated	Information element name	Information element required	Information element description
ICE Connectivity Check Result Notification	IMS-AGW	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	M	This information element indicates an ICE Connectivity Check Result event.
ICE Connectivity Check Result Notification Ack	IMS-ALG	Context	M	This information element indicates the context where the command was executed.

8.34 ICE New Peer Reflexive Candidate Notification

This procedure is used to report ICE new peer reflexive candidate for Full ICE (see clause 6.2.17.4).

Table 8.34.1: Procedures between IMS-ALG and IMS-AGW: ICE New Peer Reflexive Candidate Notification

Procedure	Initiated	Information element name	Information element required	Information element description
ICE New Peer Reflexive Candidate Notification	IMS-AGW	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	M	This information element indicates an ICE New Peer Reflexive Candidate event.
ICE New Peer Reflexive Candidate Notification Ack	IMS-ALG	Context	M	This information element indicates the context where the command was executed.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2009-12	CT#46	CP-090822			3GPP TS Presented for approval in CT#46	2.0.0	9.0.0
2009-12					Editiorial clean up	9.0.0	9.0.1
2010-03	CT#47	CP-100050	0001	2	IMS media plane security stage 2	9.0.1	9.1.0
2010-06	CT#48	CP-100289	0003	1	Transport protocol to be indicated to gateway for end-to-end media security	9.1.0	9.2.0
		CP-100284	0004	1	Handling of Through Connection		
			0005	-	Handling of RTCP streams requirement update		
2010-09	CT#49	CP-100461	0006	1	Procedures for Emergency call	9.2.0	9.3.0
			0007	1	Local IP Resources IE: changing of property		
2010-12	CT#50	CP-100685	0008	-	Support of ECN	9.3.0	10.0.0
2011-03	CT#51	CP-110058	0009	2	Handling of ICE Initialisation method for ECN	10.0.0	10.1.0
			0010	2	ECN Support in Iq Interface		
2011-09	CT#53	CP-110573	0011	2	Transcoding at ATCF/ATGW during eSRVCC	10.1.0	10.2.0
2011-12	CT#54	CP-110798	0012	1	Explicit Congestion Notification	10.2.0	10.3.0
		CP-110798	0013	1	Corrections to Stage 2 Procedures for Access Transfer Function		
2012-03	CT#55	CP-120046	0014	2	Functional Requirements for eMPS MGW control	10.3.0	11.0.0
2012-06	CT#56	CP-120239	0015	3	Multimedia Priority Control of Media Gateway resources	11.0.0	11.1.0
2012-06	CT#56	CP-120226	0018	1	Reference update: draft-ietf-avtcore-ecn-for-rtp	11.0.0	11.1.0
2012-11					Version in the header corrected	11.1.0	11.1.1
2012-12	CT#58	CP-120723	0025	-	Reference update: RFC 6679	11.1.1	11.2.0
		CP-120734	0026	3	Support of Multimedia Priority Service (MPS) in Modify over Iq Interface		
2013-06	CT#60	CP-130299	0029	3	Introduction of support for Coordination of Video Orientation (CVO)	11.2.0	12.0.0
2013-09	CT#61	CP-130471	0030	3	Introduction of support for Generic Image Attribute/signalling of image size	12.0.0	12.1.0
		CP-130452	0034	2	CVO Procedural Clarifications		
2013-12	CT#62	CP-130636	0035	1	Usage of generic image attributes	12.1.0	12.2.0
		CP-130636	0038	1	Correction of Image Size description		
		CP-130619	0037	1	Correction of CVO description		
2014-03	CT#63	CP-140025	0040	-	Alignment of IE name for CVO	12.2.0	12.3.0
2014-06	CT#64	CP-140245	0041	1	e2e media security for TCP-based media using TLS – Functional requirements	12.3.0	12.4.0
		CP-140245	0042	4	e2ae media security for TCP based media using TLS – Functional requirements		
		CP-140245	0043	2	e2ae media security for UDP-based media using DTLS – Functional requirements		
		CP-140245	0054	1	e2e media security for TCP-based media using TLS - Procedures		
		CP-140245	0055	2	e2ae media security for TCP-based media using TLS - Procedures		
		CP-140245	0056	1	e2ae media security for UDP-based media using DTLS – procedures		
		CP-140245	0057	3	Iq requirements for end-to-end TCP bearer connection control and related NAT traversal support		
		CP-140256	0045	1	Functional requirements – clarification of "stage 2" convention		
		CP-140248	0046	3	Support for Interactive Connectivity Establishment (ICE)		
		CP-140249	0052	2	WebRTC media security using DTLS-SRTP		
		CP-140249	0053	2	WebRTC support for Iq		
2014-09	CT#65	CP-140504	0058	1	Procedures for TCP bearer connection control	12.4.0	12.5.0
		CP-140504	0060	1	Bandwidth adjustment due to e2ae media security		
		CP-140504	0061	-	MSRP handling		

History

Document history		
V12.5.0	October 2014	Publication