International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.94

(11/2015)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Gateway control protocol: Web-based real-time communication services – ITU-T H.248 protocol support and profile guidelines

Recommendation ITU-T H.248.94

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	**H.240–H.259**
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence	H.420–H.429
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Personal health systems	H.810–H.819
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869

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

Recommendation ITU-T H.248.94

Gateway control protocol: Web-based real-time communication services – ITU-T H.248 protocol support and profile guidelines

Summary

Recommendation ITU-T H.248.94 provides guidelines on the use and configuration of ITU-T H.248 real-time communication in web-browsers (WebRTC) gateways via ITU-T H.248 profiles. These guidelines may be used by other standards developing organizations (SDOs) when defining their ITU-T H.248.1 profiles in support of WebRTC gateways. WebRTC represents an extensive real-time multimedia conversational service with a specific protocol stack in order to address network address translation (NAT) traversal as well as maximize multiplexing support. The WebRTC gateway consequently requires the support of user plane interworking functions (IWFs) for connecting WebRTC clients to non-WebRTC networks. The Recommendation also defines a new package to support the data channel establishment protocol (DCEP).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.248.94	2015-11-29	16	11.1002/1000/12636

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T H.248.94

Gateway control protocol: Web-based real-time communication services – ITU-T H.248 protocol support and profile guidelines

1 Scope

Web-based real-time communication is a service standardized by the IETF and World Wide Web Consortium (W3C) (called real-time communication in web-browsers (WebRTC) or RTCWeb service) and defines a particular protocol suite for IP-based communication in web browser environments. This application is related to multimedia conversational services which cover typical service components such as: telephony, conferencing, instant messaging. The native IETF/W3C WebRTC service (as defined for the public Internet by the IETF) will be embedded in other IP communication infrastructures such as next generation network (NGN)/ IP multimedia subsystem (IMS).

This Recommendation:

– describes example use cases with ITU-T H.248 WebRTC gateway involvement;

– identifies ITU-T H.248 capabilities for such gateways;

– introduces a new ITU-T H.248 package for the support of WebRTC data channel protocol procedures; and

– provides guidelines for the specification of ITU-T H.248 profiles for dedicated ITU-T H.248 WebRTC gateway types.

It is expected that the WebRTC communication service will evolve and be enhanced and/or extended in the future. The next clause provides information about the specific scope of Release 1 of this Recommendation.

1.1 Applicability statements

1.1.1 Release 1

Release 1 provides a basic WebRTC service, but has some limitations due to dependencies on other standards, which are still in progress.

Release 1 supports:

– WebRTC calls with audio and video, the two WebRTC media components are either unbundled or bundled, i.e., using ITU-T H.248 Stream grouping or not;

– WebRTC calls with additional data, but limited to WebRTC-embedded instant messaging (based on message session relay protocol (MSRP)) only.

Release 1 does not yet support:

– WebRTC calls with data applications related to WebRTC conferencing control (based on binary floor control protocol (BFCP)) and WebRTC text conversation (based on [ITU-T T.140);

– full support of datagram transport layer security (DTLS) for WebRTC data: basic establishment and release procedures are supported via ITU-T H.248. However, the ability to influence the DTLS negotiation process and other DTLS capabilities is not supported;

– interactive connectivity establishment (ICE)-based NAT traversal: current ITU-T H.248 WebRTC gateway capabilities support an asymmetric network access model. Additional extensions cannot be excluded for other network configurations, e.g., additional ICE aspects;

– secure RTP (SRTP) key management schemes: the single "DTLS-SRTP"-related key management schemes, as subject of WebRTC, is implicity supported. Additional SRTP key management schemes demand the explicit support of revised [ITU-T H.248.77].

2 References

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

[ITU-T H.248.1] Recommendation ITU-T H.248.1 (2013), *Gateway control protocol: Version 3*.

[ITU-T H.248.37] Recommendation ITU-T H.248.37 (2008), *Gateway control protocol: IP NAPT traversal package*.

[ITU-T H.248.39] Recommendation ITU-T H.248.39 (2014), *Gateway control protocol: H.248 SDP parameter identification and wildcarding*.

[ITU-T H.248.48] Recommendation ITU-T H.248.48 (2012), *Gateway control protocol: RTCP XR block reporting package*.

[ITU-T H.248.50] Recommendation ITU-T H.248.50 (2010), *Gateway control protocol: NAT traversal toolkit packages*.

[ITU-T H.248.52] Recommendation ITU-T H.248.52 (2008), *Gateway control protocol: QoS support packages*.

[ITU-T H.248.53] Recommendation ITU-T H.248.53 (2009), *Gateway control protocol: Traffic management packages*.

[ITU-T H.248.57] Recommendation ITU-T H.248.57 (2014), *Gateway control protocol: RTP control protocol package*.

[ITU-T H.248.71] Recommendation ITU-T H.248.71 (2010), *Gateway control protocol: RTCP support packages*.

[ITU-T H.248.77] Recommendation ITU-T H.248.77 (2010), *Gateway control protocol: Secure real-time transport protocol (SRTP) package and procedures*.

[ITU-T H.248.78] Recommendation ITU-T H.248.78 (2013), *Gateway control protocol: Bearer-level application level gateway*.

[ITU-T H.248.80] Recommendation ITU-T H.248.80 (2014), *Gateway control protocol: Usage of the revised SDP offer/answer model with ITU-T H.248*.

[ITU-T H.248.84] Recommendation ITU-T H.248.84 (2012), *Gateway control protocol: NAT traversal for peer-to-peer services*.

[ITU-T H.248.87] Recommendation ITU-T H.248.87 (2014), *Gateway control protocol: Guidelines on the use of ITU-T H.248 capabilities for performance monitoring in RTP networks in ITU-T H.248 profiles*.

[ITU-T H.248.88] Recommendation ITU-T H.248.88 (2014), *Gateway control protocol: RTP topology dependent RTCP handling by ITU-T H.248 media gateways with IP terminations*.

[ITU-T H.248.89] Recommendation ITU-T H.248.89 (2014), *Gateway control protocol: TCP support packages*.

[ITU-T H.248.90] Recommendation ITU-T H.248.90 (2014), *Gateway control protocol: ITU-T H.248 packages for control of transport security using transport layer security (TLS)*.

[ITU-T H.248.92] Recommendation ITU-T H.248.92 (2014), *Gateway control protocol: Stream endpoint interlinkage package*.

[ITU-T H.248.93] Recommendation ITU-T H.248.93 (2014), *Gateway control protocol: ITU-T H.248 support for control of transport security using datagram transport layer sercurity (DTLS) protocol*.

[ITU-T H.248.96] Recommendation ITU-T H.248.96 (2015), *Gateway control protocol: H.248 Stream grouping and aggregation*.

[ITU-T H.248.97] Recommendation ITU-T H.248.97 (2015), *Gateway control protocol: H.248 support for control of SCTP bearer connections*.

[ITU-T H.320] Recommendation ITU-T H.320 (2004), *Narrow-band visual telephone systems and terminal equipment*.

[ITU-T H.324] Recommendation ITU-T H.324 (2009), *Terminal for low bit-rate multimedia communication*.

[ITU-T H.351] Recommendation ITU-T H.351 (2008), *Semantic web interface for multimedia terminal and system directories (SWIM-D)*.

[ITU-T T.140] Recommendation ITU-T T.140 (1998), *Protocol for multimedia application text conversation*.

[IETF RFC 4103] IETF RFC 4103 (2005), *RTP Payload for Text Conversation*.

[IETF RFC 4571] IETF RFC 4571 (2006), *Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport*.

[IETF RFC 4585] IETF RFC 4585 (2006), *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*.

[IETF RFC 4961] IETF RFC 4961 (2007), *Symmetric RTP / RTP Control Protocol (RTCP)*.

[IETF RFC 5104] IETF RFC 5104 (2008), *Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)*.

[IETF RFC 5109] IETF RFC 5109 (2007), *RTP Payload Format for Generic Forward Error Correction*.

[IETF RFC 5124] IETF RFC 5124 (2008), *Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)*.

[IETF RFC 5506] IETF RFC 5506 (2009), *Support for Reduced-Size Real-Time Transport Control Protocol (RTCP): Opportunities and Consequences*.

[IETF RFC 5576] IETF RFC 5576 (2009), *Source-Specific Media Attributes in the Session Description Protocol (SDP)*.

[IETF RFC 5764] IETF RFC 5764 (2010), *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)*.

[IETF RFC 6525] IETF RFC 6525 (2012), *Stream Control Transmission Protocol (SCTP) Stream Reconfiguration*.

[IETF RFC 7007] IETF RFC 7007 (2013), *Update to Remove DVI4 from the Recommended Codecs for the RTP Profile for Audio and Video Conferences with Minimal Control (RTP/AVP)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation refers to the following document related to all terms used in context of the DTLS protocol: [b-IETF tls-terms].

This Recommendation also uses the following terms defined elsewhere:

3.1.1 media path [b-IETF rtcweb-overview]: The path that media data follows from one WebRTC endpoint to another.

NOTE – Relates to the bearer plane interface (at MG) in case of a WebRTC ITU-T H.248 gateway.

3.1.2 signaling path [b-IETF rtcweb-overview]: The communication channels used between entities participating in signalling to transfer signalling. There may be more entities in the signaling path than in the media path.

NOTE – Relates to the signalling plane call control interface (at MGC) in case of a WebRTC ITU-T H.248 gateway.

3.1.3 web browser [ITU-T H.351]: A software application capable of rendering HTML and XHTML documents.

3.1.4 WebRTC browser [b-IETF rtcweb-overview]: (also called a *WebRTC User Agent* or *WebRTC UA*) is something that conforms to both the protocol specification and the Javascript API.

NOTE – See [b-IETF rtcweb-overview] concerning the referred to "Javascript API specification".

3.1.5 WebRTC endpoint [b-IETF rtcweb-overview]: Is either a WebRTC browser or a WebRTC non-browser. It conforms to the protocol specification.

3.1.6 WebRTC-compatible endpoint [b-IETF rtcweb-overview]: Is an endpoint that is able to successfully communicate with a WebRTC endpoint, but may fail to meet some requirements of a WebRTC endpoint. This may limit where in the network such an endpoint can be attached, or may limit the security guarantees that it offers to others. It is not constrained by this specification; when it is mentioned at all, it is to note the implications on WebRTC-compatible endpoints of the requirements placed on WebRTC endpoints.

NOTE – The self-contained notion of 'endpoint' is consistent with [b-ITU-T H.Sup.13].

3.1.7 WebRTC gateway [b-IETF rtcweb-overview]: Is a WebRTC-compatible endpoint that mediates media traffic to non-WebRTC entities.

3.1.8 WebRTC non-browser [b-IETF rtcweb-overview]: Is something that conforms to the protocol specification, but does not claim to implement the Javascript API. This can also be called a "WebRTC device" or "WebRTC native application".

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 WebRTC ITU-T H.248 gateway: A decomposed gateway according ITU-T H.248 (i.e., an MGC-MG tandem), using an ITU-T H.248 profile with support of web-based real-time communication services.

NOTE 1 – The *WebRTC ITU-T H.248 gateway* could operate in *WebRTC gateway* mode and in *WebRTC endpoint* mode.

NOTE 2 – The particular (ITU-T H.248) gateway type may be further qualified, – based on the application specific profile -, such as WebRTC PSTN gateway, WebRTC border gateway, WebRTC IMS access gateway, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ALG	Application Level Gateway
AN	Access Network
API	Application Programming Interface
B2BRE	Back-to-Back RTP End System
B2BTE	Back-to-Back TCP Endpoint
B2BUA	Back-to-Back User Agent
BFCP	Binary Floor Control Protocol
CNAME	Canonical Name
CS	Capability Set
DC	Data Channel
DCEP	Data Channel Establishment Protocol
DTLS	Datagram Transport Layer Security
DTMF	Dual Tone Multi Frequency
FB	FeedBack
FEC	Forward Error Correction
FW	FireWall
GoS	Grade of Service
HTML	HyperText Markup Language
ICE	Interactive Connectivity Establishment
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IWF	InterWorking Function
Lx	Layer number x
MG	Media Gateway
MGC	Media Gateway Controller
MSRP	Message Session Relay Protocol
MTI	Mandatory To Implement
NACK	(RTP/RTCP) Negative Acknowledgement
NAT	Network Address Translation
NAT-T	NAT Traversal
NGN	Next Generation Network
PCM	Pulse Code Modulation
PPID	(SCTP) Payload Protocol Identifier

PSFB	(RTCP) Payload-Specific Feedback
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
RMCAT	RTP Media Congestion Avoidance Techniques (IETF WG)
RR	(RTCP) Receiver Report
RTCP	RTP Control Protocol
RTCWeb	Real-Time Communication in Web-browsers
RTP	Real-time Transport Protocol
RTPFB	RTCP Transport layer Feedback (message)
SCTP	Stream Control Transmission Protocol
SDES	Source Description (RTCP Packet)
SDP	Session Description Protocol
SEP	(ITU-T H.248) Stream Endpoint
SIP	Session Initiation Protocol
SSRC	Synchronization Source
SR	(RTCP) Sender Report
SRTP	Secure RTP
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TURN	Traversal Using Relays around NAT
UA	User Agent
UDP	User Datagram Protocol
VP8	Video Payload type 8
VP9	Video Payload type 9
W3C	World Wide Web Consortium
WebRTC	Real-Time Communication in Web browsers
XHTML	extensible Hypertext Markup Language
XR	(RTCP) extension Report

5 Conventions

5.1 Acronym usage

The two acronyms RTCWeb and WebRTC denote the initiatives to support real-time communication in web-browsers in the two different SDOs, IETF and W3C. RTCWeb relates to a "protocol specification" (note: it is actually a suite of protocols) while WebRTC provides an application programming interface (API) specification. Both are synonyms from the perspective of ITU-T H.248

entities in their role as "WebRTC-compatible endpoint" or "WebRTC endpoint". This Recommendation uses the acronym WebRTC only for the underlying communication service.

5.2 Prescriptive language

This document provides a list of items, labelled as *R-x/y*, where *x* refers to the clause number and *y* a number within that clause. Such items use the following keywords with meanings as prescribed below:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

5.3 ITU-T H.248 protocol element notation

Elements of the ITU-T H.248 protocol model, e.g., Context, Termination, Stream, Event are represented using the first letter capitalized. Property, Event, Signal and Parameter identities are given in *italics*.

The suffix ".req" added to an ITU-T H.248 command name stands for a command request, while the suffix ".rep" stands for a command reply. For example "Notify.req" represents a Notify Request.

6 WebRTC core technology overview

6.1 WebRTC gateways

The WebRTC communication model considers usage of WebRTC gateways besides the native browser-to-browser scenarios. [b-IETF rtcweb-gateway] describes such gateways in general, whereas the specific instance of an *ITU-T H.248 WebRTC gateway* is in scope of this Recommendation.

6.2 Capabilities

The ITU-T H.248 WebRTC gateway is a peer-to-WebRTC endpoints, given by IP host entities with "WebRTC-capable web browsers" as the application instance. WebRTC endpoints are characterized by following mandatory (and optional) capabilities (according to the "RTCWeb protocol specification" [b-IETF rtcweb-overview]):

– WebRTC as multimedia conversational communication service with application components audio, video and data (which covers again a group of "data services");

– application data transport (see [b-IETF rtcweb-transports]):

  • audio, video: real-time transport protocol (RTP)/RTP control protocol (RTCP) in specific capability sets (CAs) (see [b-IETF rtp-usage]);

  • data: stream control transmission protocol (SCTP)/datagram transport layer security (DTLS) in specific capability sets;

– application data framing and securing (see [b-IETF rtcweb-sec-arch], [b-IETF rtcweb-secur]):

    - audio, video: secure RTP (SRTP);
    - data: (SCTP over) DTLS;
- application data formats:
    - audio codec types (see [b-IETF rtcweb-audio]): Opus [b-IETF RFC 6716] and ITU-T G.711 pulse code modulation (PCM) μ-/A-law [b-ITU-T G.711];
    - video codec types: ITU-T H.264 [b-ITU-T H.264], VP8 [b-IETF RFC 6386] (and their successor technologies ITU-T H.265 [b-ITU-T H.265] and VP9 possibly in future);
    - real-time text conversation (based on [ITU-T T.140]);
    - instant messaging (using message session relay protocol (MSRP) session-mode);
    - image sharing (e.g., data transfer application with binary encoded data);
    - conference / floor control (based binary floor control protocol (BFCP));
- WebRTC data channel (DC) services:
    - two data services are under consideration (see [b-IETF webRTCDC]):
        - unreliable data (non-critical information includes state information);
        - reliable data (both real-time and non-real-time data);
- network address translation traversal (NAT-T) techniques for end-to-end IP media path connectivity:
    - ICE for user datagram protocol (UDP)-based media transport;
    - ICE for alternative TCP-based media transport;
    - latching (in case of hosted NAT traversal support [b-IETF RFC 7362]);
- quality of service (QoS);
- performance monitoring [b-IETF rtcweb-xr].

NOTE – The capabilities listed without any explicit reference are given by the conception of the WebRTC service as well as underlying network architectural assumptions.

6.3 Transport of user plane WebRTC traffic

6.3.1 Objective

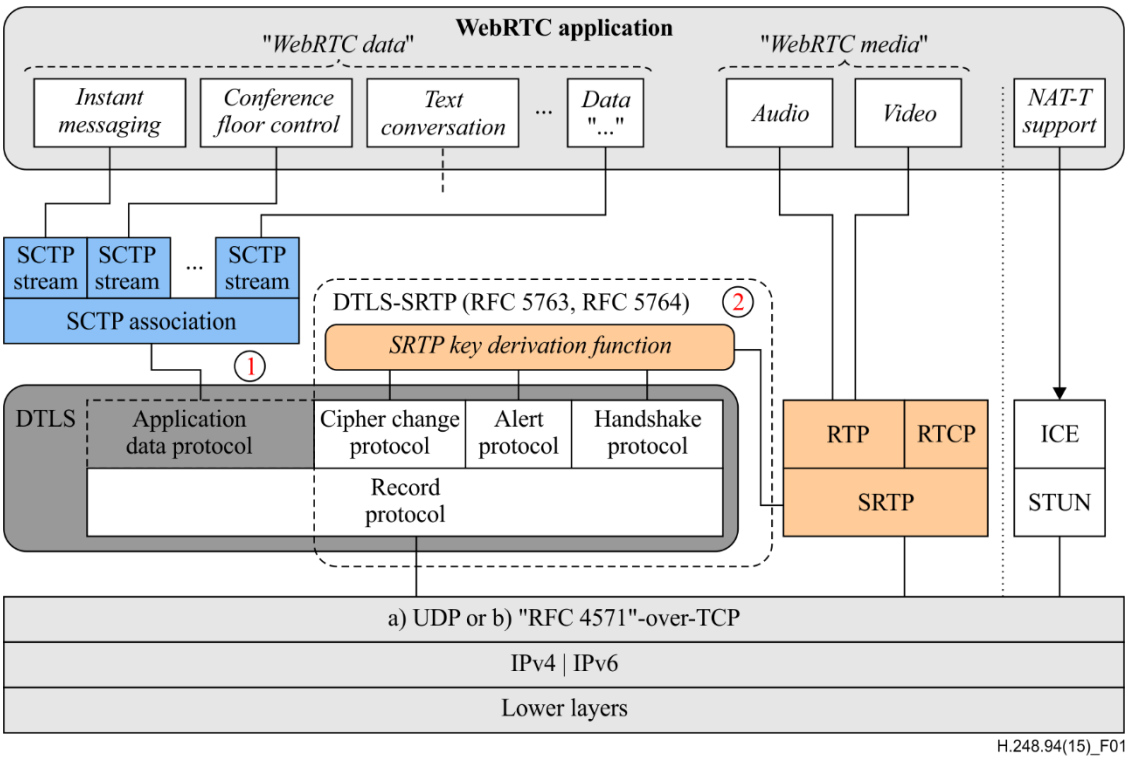
There is the basic assumption that a WebRTC endpoint could be located behind a NAT/firewall (FW) device, and thus needs NAT/FW traversal in order to have end-to-end connectivity at the IP network and transport layer. This objective results mainly in two design aspects:

1) usage of multiplexing methods in order to minimize the number of required IP transport connections; and
2) usage of TCP-based transport as a last resort when the preferred option of UDP-based transport is blocked due to NAT/FW behaviour.

Thus, there are two protocol stacks of consideration from an ITU-T H.248 WebRTC gateway perspective.

6.3.2 Protocol stack for UDP-based transport

See Figure 1:



NOTE 1 – WebRTC data traffic.

NOTE 2 – WebRTC DTLS-based key exchange for SRTP.

Figure 1 – User plane WebRTC protocol stack in case of UDP- and TCP-based transport

Notably, there is:

– a single L4 port used (Figure 1) in case of multiplexing;

– SCTP/DTLS is used for the transport of text conversation according to [ITU-T T.140] (instead of the native RTP-based transport according to [IETF RFC 4103].

6.3.3 Protocol stack for TCP-based transport

See also Figure 1.

Notably, there is:

– DTLS-over-TCP used ("despite the fact of transport layer security (TLS)-over-TCP as native transport security protocol"); and

– SRTP used for securing RTP;

– SRTP key exchange using DTLS with [IETF RFC 4571]-based framing.

Hence, there is a single DTLS connection again as in the case of UDP-based transport. Whether the underlying DTLS session is of type resumable or not, is not specified.

7 ITU-T H.248 WebRTC gateways: example use cases

Some example use cases are described in this clause.

7.1 Point-to-point communication

All examples here are characterized by a *two-party call* (between A and B); the party A always uses a WebRTC browser environment.

7.1.1 Use case #1: WebRTC-to-WebRTC interworking

See Figure 2.

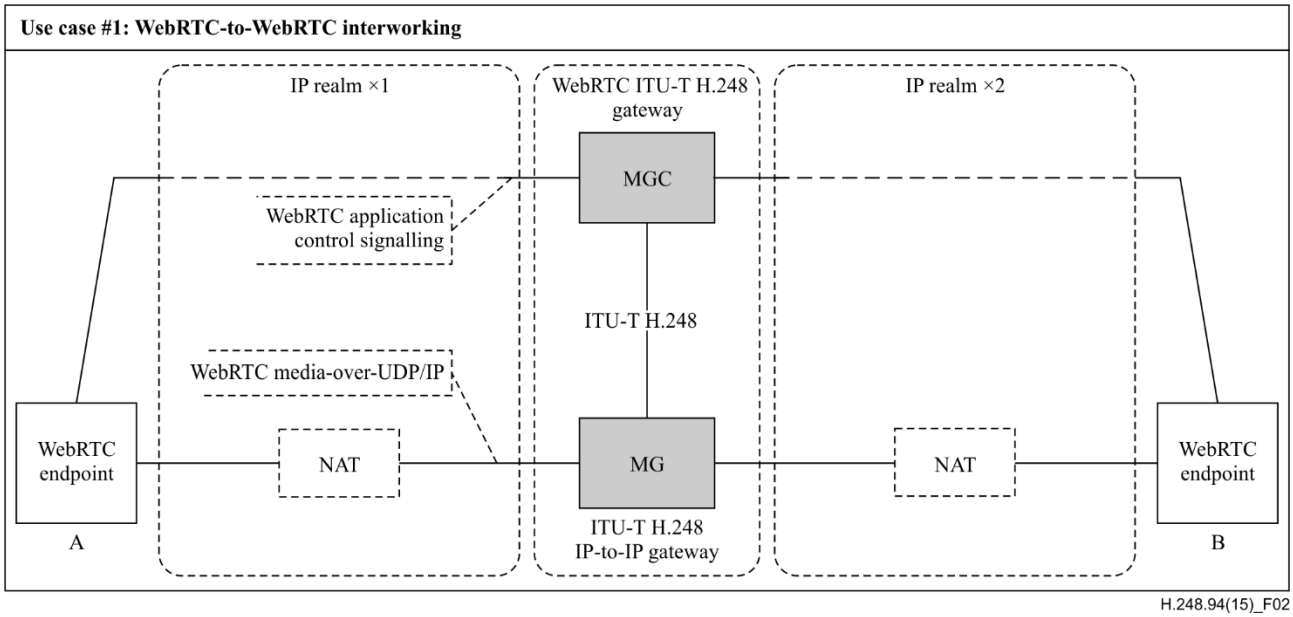


Figure 2 – Use case #1: WebRTC-to-WebRTC interworking

Use case #1 relates to a browser-to-browser scenario: the WebRTC ITU-T H.248 gateway may be needed e.g., due to different NAT-T requirements in the two networks where the WebRTC endpoints reside, due to codec mismatch between both WebRTC endpoints, due to different QoS architecture of the networks where the WebRTC endpoints reside, etc.

7.1.2 Use case #2: WebRTC-to-NGN/IMS interworking

Figure 3 depicts an interworking scenario with next generation network (NGN)/IMS networks.

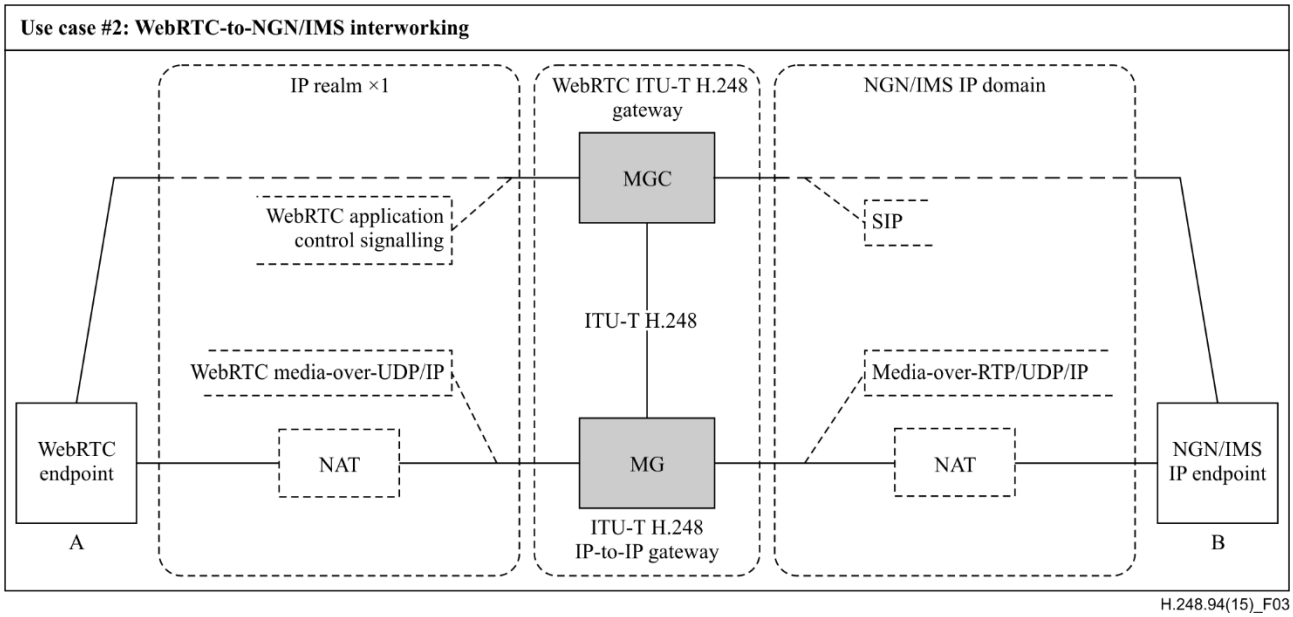


Figure 3 – Use case #2: WebRTC-to-NGN/IMS interworking

Use case #2 is fundamentally motivated by the fact that NGN/IMS IP user equipment is supposed *not* to be fully identical to WebRTC endpoints (in terms of capabilities as listed in clause 8).

7.1.3 Use case #3: WebRTC-to-PSTN/ISDN interworking

Figure 4 outlines an interworking scenario to existing public switched telephone network (PSTN)/ISDN infrastructures.

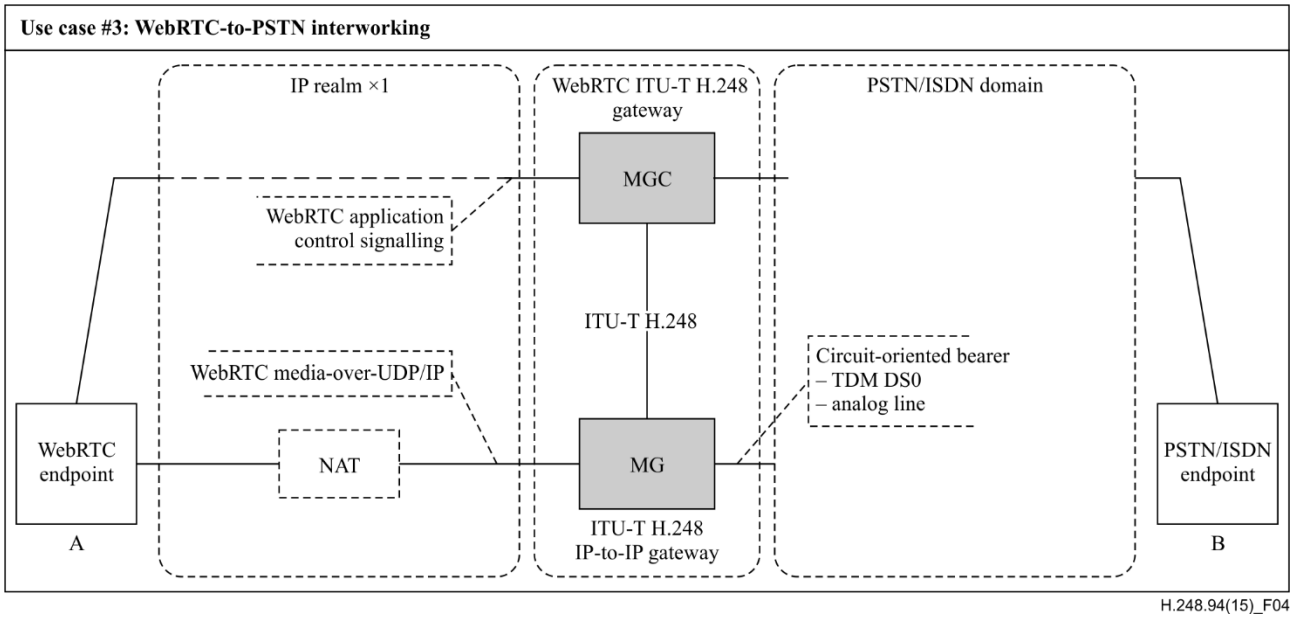


Figure 4 – Use case #3: WebRTC-to-PSTN/ISDN interworking

Use case #3 provides again many variants, such as:

– the down-negotiation of an initial multimedia call request to an audio-only call;

– the transcoding between different audio codecs;

– the support of PSTN/ISDN multimedia terminals (e.g., [ITU-T H.324], [ITU-T H.320]).

7.2 Multipoint communication

Multiparty calls are basically in scope of WebRTC, leading to the usual real-time conferencing support from the network side. For instance, WebRTC components audio and video may demand "RTP mixer" functionality, as e.g., typically provided by media servers. Such a network scenario may therefore relate to ITU-T H.248 profile types concerning media servers (i.e., media resource processors).

The usual connection model of media servers for multiparty call types is given by "back-to-back endpoint" structures, i.e., there are multiple interconnected WebRTC client instances as part of such an ITU-T H.248 Context in a media server.

8 Functional requirements for ITU-T H.248 WebRTC gateways

There are *general* and *use case* specific functional requirements for ITU-T H.248 WebRTC gateways. WebRTC gateway requirements could be classified in subsequent functional areas.

8.1 Requirements related to NAT traversal support

8.1.1 Media latching based NAT traversal support

R-8.1.1/1: The ITU-T H.248 WebRTC gateway is required to support media latching according to the ITU-T H.248 *IP NAPT traversal package* [ITU-T H.248.37].

NOTE – Latching as hosted NAT traversal mechanism (see [b-IETF RFC 7362]) translates to [ITU-T H.248.37] when provided by a decomposed ITU-T H.248 gateway.

R-8.1.1/2: The ITU-T H.248 WebRTC gateway is recommended to support the media latching associated address reporting capability according to the ITU-T H.248 *Address Reporting Package* [ITU-T H.248.37].

NOTE – This is an optional capability and not mandatory for the basic WebRTC call establishment. The media gateway controller (MGC) might use this capability as complementary information, e.g., as part of an overall service concerning the identification of NAT behavioural types.

8.1.2 ICE-based NAT traversal support

IP transport protocols:

R-8.1.2/1: The ITU-T H.248 WebRTC gateway is required to support ICE for UDP connections, according to [ITU-T H.248.50].

R-8.1.2/2: The ITU-T H.248 WebRTC gateway is required to support ICE for TCP connections.

The following [ITU-T H.248.50] building blocks are behind the two L4 protocol type related requirements at minimum:

1) support for MG terminated STUN-based connectivity checks; and
2) session traversal utilities for NAT (STUN) support profile given by the three ITU-T H.248 packages: "MG Act-as STUN server", "Originate STUN continuity check" and "STUN consent freshness".

ICE mode:

R-8.1.2/3: The ITU-T H.248 WebRTC gateway is required to support basically ICE-full mode (see section 3.4 of [b-IETF rtcweb-transports]).

R-8.1.2/4: The ITU-T H.248 WebRTC gateway is required to support ICE-lite mode only, dependent on the location of the ITU-T H.248 WebRTC gateway in the end-to-end path and/or the "NAT traversal" relevant network architecture.

Trickle ICE:

R-8.1.2/5: The ITU-T H.248 WebRTC gateway is required to support the ICE extensions "trickle ICE" (see [b-IETF trickle-ice]).

IPv4/IPv6 dual stack fairness and multihomed extension for ICE:

R-8.1.2/6: The ITU-T H.248 WebRTC gateway can optionally support the ICE extensions "IPv4/IPv6 dual stack fairness" (see [b-IETF ice-dualstack]).

NOTE – The capability is optional for the basic WebRTC call establishment. It is rather a network operator policy concerning IP version preferences.

Additional support of traversal using relays around NAT (TURN) server functionality:

A WebRTC access domain could require additional TURN functionality on top of STUN support. There is then the basic assumption that the IP media path will still be routed via the ITU-T H.248 WebRTC media gateway (MG), which implies that the ITU-T H.248 MG could provide an embedded TURN server function. There seems to be no need for an additional TURN server in the media path.

R-8.1.2/7: The ITU-T H.248 WebRTC gateway can optionally provide TURN support according to [ITU-T H.248.50].

NOTE – The specific TURN related capabilities are for further studies.

8.2 Requirements related to communication topologies

8.2.1 ITU-T H.248 WebRTC gateway for point-to-point interworking

R-8.2.1/1: The ITU-T H.248 WebRTC gateway is required to support an ITU-T H.248 (IP, IP) or (IP, non-IP) connection models (use cases #1, #2 and #3).

8.2.2 ITU-T H.248 WebRTC gateway as WebRTC conferencing point

R-8.2.2/1: The ITU-T H.248 WebRTC gateway is required to support the conferencing extensions for RTP media as indicated in section 5.1 of [b-IETF rtp-usage].

8.3 Requirements related to bearer traffic multiplexing

R-8.3.1/1: The ITU-T H.248 WebRTC gateway is required to support at least one UDP- or TCP-based transport connection for a single, multiplexed WebRTC multimedia call.

NOTE – This is the bearer configuration with a maximum degree of multiplexing. All audio and video traffic are aggregated by usage of RTP transport and RTP media multiplexing. All data traffic is aggregated via a single SCTP Association which is encrypted via DTLS. All three "middle stack" traffic components based on SRTP/SRTCP, DTLS and STUN share a single L4 transport connection.

8.4 Requirements related to RTP-to-RTP type interworking

8.4.1 RTCP control flow component

R-8.4.1/1: The ITU-T H.248 WebRTC gateway is required to always support an RTCP control flow in addition to the RTP media flow (see section 4.1 of [b-IETF rtp-usage]).

Support of RTCP (i.e., the handling and processing of specific RTCP packet types) is dependent on the *RTP topology* used for the ITU-T H.248 WebRTC gateway (see clause 8.4.4). The following requirements are applicable for the example of the RTP topology "*Back-to-back RTP end system (B2BRE)*":

R-8.4.1/2: Basic RTCP services: The ITU-T H.248 WebRTC gateway is required to support sending and receiving RTCP sender report (SR), receiver report (RR), source description (SDES), and BYE packet types.

R-8.4.1/3: RTP profile dependent RTCP services: The ITU-T H.248 WebRTC gateway is required to support sending and receiving RTCP transport layer feedback (RTPFB) (*Generic RTP Feedback*) and *Payload-specific feedback* (PSFB) packet types.

R-8.4.1/4: Supplementary RTCP services: The ITU-T H.248 WebRTC gateway could optionally support sending and receiving RTCP extension report (XR) packet types with respect to performance monitoring of RTP traffic (see also [ITU-T H.248.87]).

8.4.2 RTP profiles

R-8.4.2/1: The ITU-T H.248 WebRTC gateway is required to support RTP profile "RTP/SAVPF" according to [IETF RFC 5124], [IETF RFC 7007] (see section 4.2 of [b-IETF rtp-usage]).

8.4.3 RTP multiplexing

R-8.4.3/1: The ITU-T H.248 WebRTC gateway is required to support RTP media multiplexing ("synchronization source (SSRC) multiplexing") (see section 4.4 of [b-IETF rtp-usage]).

NOTE 1 – The multiplexing mode will only be used when all participants agree. If not, the unmultiplexed mode will be used. Thus, any MGC involved in the call control level end-to-end capability negotiations could actually downgrade to unmultiplexed mode.

R-8.4.3/2: The ITU-T H.248 WebRTC gateway is required to support RTP transport multiplexing ("RTP/RTCP transport multiplexing") (see section 4.5 of [b-IETF rtp-usage]).

NOTE 2 – Same comment as in NOTE 1: backward compatibility requires the support of unmultiplexed mode as well.

8.4.4 RTP topologies

NOTE – All required RTP topologies are already outlined by [ITU-T H.248.88].

R-8.4.4/1: Use case independent: the ITU-T H.248 WebRTC gateway is required to comply with the "RTP topology" behaviour according to [ITU-T H.248.88].

R-8.4.4/2: Use case #1: The ITU-T H.248 WebRTC gateway is required to support topology

a) "*RTP transparent forwarding*";

b) "*RTP transport translator*"; or

c) "*RTP media translator*"

dependent on the call-level end-to-end negotiation of the used "RTP configuration" for WebRTC.

R-8.4.4/3: Use case #2: The ITU-T H.248 WebRTC gateway is required to support, in addition to RTP topologies of use case #1, the topology

a) "Back-to-back RTP end system"

due to the "legacy usage of RTP" in the "NGN/IMS IP domain".

NOTE – All existing ITU-T H.248 profiles for border gateways are not explicit on RTP topologies in detail. Thus, the B2BRE topology represents a default topology (due to the back-to-back IP host configuration of an RTP-RTP H.248 Context).

R-8.4.4/4: Use case #3: The ITU-T H.248 WebRTC gateway is required to support the "*RTP end system*" (RTPE) topology (see clause 7.1 of [ITU-T H.248.88]).

8.4.5 RTCP-based services, report types and packet formats

R-8.4.5/1: The ITU-T H.248 WebRTC gateway is required to support reduced size RTCP according to [IETF RFC 5506] (see section 4.6 of [b-IETF rtp-usage]).

8.4.6 Resource allocation rules for RTP/RTCP

8.4.6.1 Port allocation rules for RTP and RTCP

R-8.4.6.1/1: The ITU-T H.248 WebRTC gateway is required to support symmetric RTP/RTCP according to [IETF RFC 4961] (see section 4.7 of [b-IETF rtp-usage]), which relates to the ITU-T H.248-controlled port allocation as defined by [ITU-T H.248.57].

8.4.6.2 SSRC allocation rules for RTP

R-8.4.6.2/1: The ITU-T H.248 WebRTC gateway is required to support signalled RTP SSRC identifiers according to [IETF RFC 5576] (see section 4.8 of [b-IETF rtp-usage]).

8.4.6.3 CNAME allocation rules for RTP/RTCP

R-8.4.6.3/1: The ITU-T H.248 WebRTC gateway is required to support unique RTCP canonical name (CNAME) value(s) (see section 4.9 of [b-IETF rtp-usage]).

NOTE – A single CNAME might be sufficient for a single ITU-T H.248 MG entity.

R-8.4.6.3/2: The ITU-T H.248 WebRTC gateway can optionally be requested to report received RTCP CNAME value(s) from remote WebRTC clients (according to the *RTCP Source Description* package as defined by [ITU-T H.248.71].

8.5 Requirements related to TCP-based media transport

8.5.1 Requirements related to TCP connection establishment

The establishment of the TCP connection segment between the remote WebRTC client and ITU-T H.248 WebRTC gateway is subject of the overall NAT traversal framework given by ICE/STUN procedures as executed between both WebRTC endpoints. This results in the following TCP specific requirements.

R-8.5.1/1: The ITU-T H.248 WebRTC gateway is required to support autonomous TCP connection establishment according to the implicit results of the ICE candidate selection process.

NOTE – Above requirements translates in active, passive or simultaneous TCP connection establishment procedures. Thus, the TCP-enabled ITU-T H.248 Stream endpoint (SEP) does not use [ITU-T H.248.84] and [ITU-T H.248.89] during the TCP establishment phase.

8.5.2 Requirements related to connectivity checks of TCP connection candidates

R-8.5.2/1: The ITU-T H.248 WebRTC gateway is required to support correspondent STUN-based connectivity checks for TCP (within the overall requirement **R-8.1.2/2**).

8.5.3 Requirements related to TCP connection release

8.5.3.1 Requirements related to immediate TCP connection release in case of non-used ICE candidates

R-8.5.3.1/1: The ITU-T H.248 WebRTC gateway is required to support the immediate release of non-selected TCP connection candidates.

8.5.3.2 Requirements related to regular TCP connection release at the end of the WebRTC call

R-8.5.3.2/1: The ITU-T H.248 WebRTC gateway is required to support the usual TCP connection release capabilities as outlined in [ITU-T H.248.89].

8.5.4 Requirements related to application level framing protocol

R-8.5.4/1: The ITU-T H.248 WebRTC gateway is required to support the L4+ framing scheme according to [IETF RFC 4571] in case of TCP-based WebRTC transport.

8.5.5 Requirements related to MG-internal interworking of TCP traffic

8.5.5.1 Requirements related to TCP-to-UDP interworking

R-8.5.5.1/1: The ITU-T H.248 WebRTC gateway is required to provide a complete termination of the TCP, i.e., a (TCP)-connection-endpoint function.

8.5.5.2 Requirements related to TCP-to-TCP interworking

[ITU-T H.248.84] and [ITU-T H.248.89] describe various modes of operation related to TCP-to-TCP interworking in ITU-T H.248 MGs. Such a TCP-to-TCP connection model is actually only given for the case of a WebRTC call with a single data channel only. The correspondent TCP interworking model would be an "application-aware, stateful TCP" proxy mode (clause 3.2.1 of [ITU-T H.248.89]). However, the general case of multi-data-channel WebRTC calls imply a one-to-many L4 topology, i.e., the *TCP end system* of the WebRTC client might be connected to more than one *TCP end system* at the non-WebRTC Termination.

R-8.5.5.2/1: The ITU-T H.248 WebRTC gateway is required to support basically a *Back-to-Back TCP endpoint* (B2BTE) mode due to:

a) firstly, the "ICE-controlled" TCP connection segment towards remote WebRTC clients (Note 1); and

b) secondly, the principle one-to-many connection endpoint relationship at the TCP layer (Note 2) within an ITU-T H.248 "WebRTC gateway" Context.

NOTE 1 – Background: L4 connectivity issues during the active call phase could lead to ICE refresh procedures, which might impact L4 connection updates.

NOTE 2 – The MG might autonomously transition to a more efficient mode of interworking than B2BTE, however, such MG behaviour is basically conditional and considered to be implementation specific. Example conditions might be the knowledge of the MG of a single-data-channel-only WebRTC call ("which might allow a tighter relationship of the TCP flow controls of each connection segment"), or required application level interworking ("such as transparent forwarding or not of IP application protocol data").

8.5.5.3 Requirements related to MG-internal buffering of TCP data and TCP flow control

This requirements area is implementation specific and out of scope of this Recommendation due to the variety of B2BTE topologies (see clause 8.5.5.2) and the general assumption that MG-internal TCP data forwarding behaviour is out of scope of standardization.

Some general considerations might be given:[1]

1) TCP flow control *during establishment* phase

   a) Without early application data

      Is the normal case for the ITU-T H.248 WebRTC Termination due to the initial ICE phase. Hence, there would be a pure TCP connection establishment phase without any application data transfer (either SRTP-related media or DTLS messages for DTLS connection establishment) at this stage. There is consequently not any TCP data for MG-internal forwarding (and thus buffering) in WebRTC to non-WebRTC ITU-T H.248 Termination directions.

   b) With early application data

      The TCP establishment processes at the TCP connection segments of the WebRTC and non-WebRTC Termination are basically asynchronous, i.e., one side is ready for data transfer earlier than the other side. It is up to the MG to buffer or discard TCP data at this stage of the WebRTC call phase, but it is important that an MG discarding TCP data has to indicate such "loss" via TCP AN acknowledgement process towards the remote TCP endpoint.

2) TCP flow control during active data transfer phase

   It is up to the MG to minimize the amount of internal buffered TCP data by active intervention in the TCP AN acknowledgement processes of all TCP connection endpoints within the ITU-T H.248 "WebRTC gateway" Context.

8.6 Requirements related to media-aware type of interworking

8.6.1 Requirements related to WebRTC audio

8.6.1.1 Requirements related to media format (audio)

R-8.6.1.1/1: The ITU-T H.248 WebRTC gateway is required to support audio transcoding between the WebRTC mandatory to implement (MTI) audio codec(s) and other audio codecs as typically used in NGNs.

[1] There were already similar discussions for non-WebRTC related TCP media, e.g. TLS-based transport security [ITU-T H.248.90] and the interworking of TLS-to-TLS, TLS-to-non-TLS in a particular TCP interworking mode.

8.6.1.2 Requirements related to media adaptation and rate control (audio)

Requirements are subject of section 7 of [b-IETF rtp-usage]; however, there are not yet any explicit capabilities identified for the first phase of WebRTC service deployment. Correspondent capabilities are currently developed by IETF working group *RTP media congestion avoidance techniques* (RMCAT), see e.g., requirements in [b-IETF rmcat-cc], which are planned to be integrated later on in WebRTC.

8.6.2 Requirements related to WebRTC video

8.6.2.1 Requirements related to media format (video)

R-8.6.2.1/1: The ITU-T H.248 WebRTC gateway acting as IP-IP MG is not required to support video transcoding because, if required at all, it is provided by centralized media servers.

R-8.6.2.1/2: The ITU-T H.248 WebRTC gateway as media server can optionally support video transcoding between the WebRTC video codec(s) and other video codecs as typically used in NGNs.

NOTE – The optional tagging of this requirement is due to the fact that it is expected that potential scenarios for video transcoding might be fairly low and exceptional. It is rather expected that WebRTC endpoints will negotiate a common video codec, or fallback to a default codec, or even not use video.

8.6.2.2 Requirements related to media adaptation and rate control (video)

See clause 8.6.1.2.

8.6.3 Requirements related to WebRTC data

8.6.3.1 Requirements for MSRP-based instant messaging

R-8.6.3.1/1: The ITU-T H.248 WebRTC gateway is required to support transparent forwarding of MSRP protocol data units ("MSRP messages"), independent of the underlying (WebRTC specific or legacy) transport (protocol stack). This includes interworking between WebRTC clients or a WebRTC and non-WebRTC client.

R-8.6.3.1/2: The ITU-T H.248 WebRTC gateway is required to support the underlying transport relay function in interworking between "SCTP/DTLS/UDP" to "TCP" for MSRP traffic.

R-8.6.3.1/3: The ITU-T H.248 WebRTC gateway can optionally support a bearer-level application level gateway (ALG), (B-ALG) at MSRP layer according to [ITU-T H.248.78]. Such a capability relates to a specific MSRP back-to-back user agent (B2BUA) function with the purpose of a L4+ level NAT traversal support.

8.6.3.2 Requirements for BFCP-based conference control

R-8.6.3.2/1: The ITU-T H.248 WebRTC gateway is required to support transparent forwarding of BFCP protocol data units ("BFCP messages"), independent of the underlying (WebRTC specific or legacy) transport (protocol stack). This includes interworking between WebRTC clients or a WebRTC and non-WebRTC client.

R-8.6.3.2/2: The ITU-T H.248 WebRTC gateway is required to support the underlying transport relay function in interworking between "SCTP/DTLS/UDP" to "TCP" for BFCP traffic.

R-8.6.3.2/3: The ITU-T H.248 WebRTC gateway can optionally support the underlying transport relay function in interworking between "SCTP/DTLS/UDP" to "UDP" for BFCP traffic (see [b-IETF bfcpbis]).

8.6.3.3 Requirements for binary-encoded WebRTC data

R-8.6.3.3/1: The ITU-T H.248 WebRTC gateway is required to support transparent forwarding of binary data units (images), independent of the underlying (WebRTC specific or legacy) transport

(protocol stack). This includes interworking between WebRTC clients or a WebRTC and non-WebRTC client.

R-8.6.3.3/2: The ITU-T H.248 WebRTC gateway is required to support the underlying transport relay function in interworking between "SCTP/DTLS/UDP" to an applicable transport e.g., "TCP" for binary traffic.

8.6.4 Requirements related to WebRTC text

WebRTC text telephony (text conversation) is considered as "data traffic" (despite the fact of the usual RTP-based transport in non-WebRTC environments).

R-8.6.4/1: The ITU-T H.248 WebRTC gateway is required to support transparent forwarding of ITU-T T.140 protocol data units (according to [ITU-T T.140]), independent of the underlying (WebRTC specific or legacy) transport (protocol stack). This includes interworking between WebRTC clients or a WebRTC and non-WebRTC client.

R-8.6.4/2: The ITU-T H.248 WebRTC gateway is required to support the underlying transport relay function in interworking between "SCTP/DTLS/UDP" to "RTP/UDP" for ITU-T T.140 traffic.

R-8.6.4/3: The ITU-T H.248 WebRTC gateway is required to emulate an "ITU-T T.140/RTP" endpoint in the non-WebRTC domain, which implies an RTP source/RTP sink behaviour according to [IETF RFC 4103]. Hence, the ITU-T H.248 WebRTC gateway is required to be aware of the ITU-T T.140 IP application protocol despite of the use of a transparent forwarding mode. The "ITU-T T.140 awareness" by the ITU-T H.248 WebRTC gateway is limited to the detection of active/silence periods related to the transfer of ITU-T T.140 PDUs, as well as a "packet loss concealment" method related to incoming ITU-T T.140/RTP packets. Appendix II provides more background information on that interworking aspect.

8.7 Requirements related to bearer security

8.7.1 Requirements related to transport security

8.7.1.1 Protocol stacks with DTLS

R-8.7.1.1/1: The ITU-T H.248 WebRTC gateway is required to support transport security for UDP using DTLS, according to [ITU-T H.248.93].

R-8.7.1.1/2: The ITU-T H.248 WebRTC gateway is required to support transport security for TCP using DTLS (according to [ITU-T H.248.93]) and [IETF RFC 4571] as the interim framing protocol.

R-8.7.1.1/3: The ITU-T H.248 WebRTC gateway is required to use a shared DTLS connection for SCTP-encapsulated WebRTC data traffic, according to [ITU-T H.248.93], [ITU-T H.248.97].

R-8.7.1.1/4: The ITU-T H.248 WebRTC gateway is required to use a shared DTLS connection for SRTP-related key exchange procedures (for WebRTC audio and video traffic), according to [ITU-T H.248.93], [ITU-T H.248.77].

8.7.1.2 DTLS interworking scenarios

Transport of data traffic in a native WebRTC domain relates to the protocol layering of "data-over-SCTP/DTLS/UDP/IP", whereas transport of data traffic in the native Internet uses basically "data-over-TCP/IP". The ITU-T H.248 WebRTC gateway needs to address interworking between both network paradigms (see also use cases #1 and #2 in clause 7.1), leading to the following requirements:

R-8.7.1.2/1: The ITU-T H.248 WebRTC gateway is required to support *DTLS transparent forwarding* for the interworking between two network domains with SCTP/DTLS/UDP based WebRTC data transport. This relates to the use case according to clause 6.2.2.1 of [ITU-T H.248.93].

R-8.7.1.2/2: The ITU-T H.248 WebRTC gateway is required to support *DTLS-to-non-DTLS interworking* for the interworking between two network domains with SCTP/DTLS/UDP and

(TLS)/TCP based WebRTC data transport. This relates to the use case #1.2 according to clause 6.2.1 of [ITU-T H.248.93].

8.7.1.3 TLS support

R-8.7.1.3/1: The ITU-T H.248 WebRTC gateway is required to support TLS termination in case of the DTLS interworking scenario according to **R-8.7.1.2/2** and transport security usage in the TCP domain.

8.7.2 Requirements related to media security

8.7.2.1 Encryption method

R-8.7.2.1/1: The ITU-T H.248 WebRTC gateway is required to support media security for RTP using SRTP, according to [b-IETF RFC 3711].

8.7.2.2 Key exchange scheme for SRTP

R-8.7.2.2/1: The ITU-T H.248 WebRTC gateway is required to support the media-path coupled SRTP key exchange (using DTLS-SRTP [IETF RFC 5764], see [b-IETF RFC 5763]).

R-8.7.2.2/2: The ITU-T H.248 WebRTC gateway can optionally support the signalling-path coupled SRTP key exchange, i.e., the "SDES" (session description protocol (SDP) security descriptions) related method according to [ITU-T H.248.77].

R-8.7.2.2/3: The ITU-T H.248 WebRTC gateway can optionally support multiple key exchange schemes for SRTP within a single ITU-T H.248 profile. The ITU-T H.248 WebRTC gateway is then required to indicate the applied SRTP key exchange scheme according to [ITU-T H.248.77].

8.8 Requirements related to WebRTC emergency and priority services

8.8.1 Emergency services within WebRTC calls

From the IETF side, WebRTC emergency services are so far contained in draft [b-IETF rtcweb-ecrit]. No additional requirements for ITU-T H.248 WebRTC gateways are derived taking this initial document as baseline.

8.8.2 Priority services within WebRTC calls

This Recommendation does not provide any (explicit) requirements related to priority services.

NOTE – There appears to be no discussion or method to communicate priority in javascript session establishment protocol (JSEP) [b-IETF rtcweb-jsep]. Therefore, it appears WebRTC does not support priority in SDP form. Priority is able to be specified as part of data channel [b-IETF DCEP]. [b-IETF rtp-usage] indicates that the WebRTC API also allows prioritisation of MediaStreamTrack but there is no discussion in the API document.

8.9 Requirements related to QoS support

8.9.1 IP traffic control: QoS marking

R-8.9.1/1: The ITU-T H.248 WebRTC gateway is required to support DiffServ based QoS marking according to [ITU-T H.248.52] (see section 12.1.3 of [b-IETF rtp-usage]).

NOTE 1 – The ITU-T H.248 WebRTC MG provides the so-called "DS pre-marker" role (see Appendix IV of [ITU-T H.248.52]).

NOTE 2 – QoS marking takes effect at IP level, i.e., on the complete aggregate of all WebRTC traffic components. Any kind of application protocol individual QoS markings is not required for initial WebRTC service support.

8.9.2 IP traffic control: traffic policing – IP byte rate policing

R-8.9.2/1: The ITU-T H.248 WebRTC gateway is required to support IP byte rate policing according to [ITU-T H.248.53].

NOTE 1 – Traffic policing takes effect at IP level, i.e., on the complete aggregate of all WebRTC traffic components.

8.9.3 Improved transport robustness for RTP

See section 6 of [b-IETF rtp-usage].

8.9.3.1 Negative acknowledgements

In general:

R-8.9.3.1/1: The ITU-T H.248 WebRTC gateway is recommended to support negative acknowledgements (NACKs) for RTP data packets [IETF RFC 4585] (see section 6.1 of [b-IETF rtp-usage]).

In particular:

The origination and termination of RTCP feedback (FB) messages is subject of RTP sender and RTP receiver entities [IETF RFC 4585], thus tightly coupled to "RTP topologies" (see clause 8.4.4 of this Recommendation). Hence, an ITU-T H.248 WebRTC gateway, as located within an end-to-end RTP media path, is normally only partially involved in the processing of RTCP FB messages. The following high-level behaviour is derived:

R-8.9.3.1/2: The ITU-T H.248 WebRTC gateway is recommended to support the forwarding of RTCP FB messages when using a *RTP translator* topology.

R-8.9.3.1/3: The ITU-T H.248 WebRTC gateway is recommended to originate and terminate RTCP FB messages when using a *Back-to-back RTP end system* topology.

8.9.3.2 Forward error correction

In general:

R-8.9.3.2/1: The ITU-T H.248 WebRTC gateway can optionally support forward error correction (FEC) for RTP [IETF RFC 5109] (see section 6.2 of [b-IETF rtp-usage]).

In particular:

In general, an RTP sender generates the usual RTP "media packets" plus RTP "FEC packets", which are evaluated again by the RTP receiver in case of lost RTP "media packets". There is an underlying assumption of unmodified RTP packets along the RTP media path. Thus, FEC becomes useless in case of interim RTP entities which would modify RTP packets. Leading to following high-level behaviour:

R-8.9.3.2/2: The ITU-T H.248 WebRTC gateway is required to support the transparent forwarding of RTP traffic when using a *RTP translator* topology, – i.e., when FEC is required, then only RTP transport translator topology would be allowed.

R-8.9.3.2/3: The ITU-T H.248 WebRTC gateway is recommended to originate and terminate RTP "FEC packets" when using a *Back-to-back RTP end system* topology.

8.10 Requirements related to bearer-path coupled congestion controls

These requirements are tightly coupled with the capability of "media adaptation and rate control" (see clause 8.6). Specific requirements are not yet settled from IETF side for the first release of this Recommendation (see also [b-IETF rmcat-cc]).

8.11 Requirements related to performance monitoring

The requirements framework in this clause follows the [ITU-T H.248.87] "*Guidelines on the use of ITU-T H.248 capabilities for performance monitoring in RTP networks*".

Browser-based WebRTC endpoints may likely support the local generation of measurements for performance metrics according to [b-IETF rtcweb-xr]. The bowser-embedded measurement point (MP) and the set of supported *WebRTC's statistics* are defined by [b-W3C webrtc-stats].

8.11.1 Requirements related to measurement point

Generally, the set of performance measurements typically differs between WebRTC endpoints (such as a WebRTC browser) and WebRTC gateways, e.g., because the observation of *application level* performance metrics is primary subject of communication endpoints and normally questionable or even meaningless in case of "in-path equipment".

R-8.11.1/1: The ITU-T H.248 WebRTC gateway is recommended to execute measurements for *transport level* performance metrics (term definition see clause 3.2.6 of [ITU-T H.248.87]).

R-8.11.1/2: The ITU-T H.248 WebRTC gateway can optionally execute measurements for *application level* performance metrics (definition see clause 3.2.1 of [ITU-T H.248.87]), – under the condition of a valuable semantic of the concerned metric.

Example metrics:

1) RTP-based WebRTC traffic:
   - see Appendix III of [ITU-T H.248.87] for a general overview;
   - RTCP XR related metrics are recommended (e.g., RTCP XR metrics are used instead of ITU-T H.248 *nt/rtp* package statistics).
2) non-RTP-based WebRTC traffic: e.g., transport level metrics related to:
   - DTLS (see [ITU-T H.248.93]);
   - SCTP (see [ITU-T H.248.97]);
   - TLS (see [ITU-T H.248.90]); and
   - TCP (see [ITU-T H.248.84], [ITU-T H.248.90]).

The actual set of performance metrics for a particular ITU-T H.248 "WebRTC gateway" profile depends, as usual, on the specific purpose, such as:

a) usage metering (relates typically to the traffic volume on the application level);

b) reporting of user experience related metrics (i.e., QoS/quality of experience (QoE) related metrics);

c) reporting of network condition related metrics (i.e., grade of service (GoS) related metrics);

d) recording of successful, unsuccessful or specific policing actions; or

e) validation of network capacity allocations (relates typically to the traffic volume on the lowest layer of transport capacity reservation).

The primary focus is most likely (c) in case of an ITU-T H.248 WebRTC gateway due to its positioning at the border of network domains (with typically different GoS conditions).

8.11.2 Requirements related to collection point

The set of supported performance metrics, which should be measured by WebRTC endpoints (as peered by ITU-T H.248 WebRTC gateway) is still undefined in this Recommendation. It is e.g., expected that [b-IETF rtcweb-xr] might be supported for the RTP-based WebRTC traffic components. Performance metrics for non-RTP WebRTC traffic is still unclear.

When WebRTC endpoints support the measurement of RTCP XR-based metrics, then it is expected that they report their measurements via RTCP along the WebRTC media path.

R-8.11.2/1: The ITU-T H.248 WebRTC gateway is required to collect remote measurement data via incoming RTCP reports.

8.11.3 Requirements related to reporting point

R-8.11.3/1: The ITU-T H.248 WebRTC gateway is required to support the reporting of RTCP XR-related ITU-T H.248 statistics according to the *RTCP XR block reporting* package [ITU-T H.248.48].

8.11.4 Requirements related to filtering point

Measurement data carried by RTCP XR reports could be filtered by ITU-T H.248 WebRTC gateways, see [ITU-T H.248.87]. However, the particular ITU-T H.248 WebRTC gateway filter behaviour is subject of operator policies, thus out of scope of this Recommendation.

8.11.5 Requirements related to loopback point

None.

8.12 Requirements related to SDP-based description, declaration and negotiation of WebRTC media configurations

8.12.1 Requirements related to supported SDP elements – Overall media descriptions

The ITU-T H.248 WebRTC gateway is required to support SDP elements (for the purpose of media gateway control) according to Tables 1, 2 and 3:

Table 1 – Requirements related to supported SDP elements – Part I SDP "m="-line

Requirement	SDP "m=" line element	Purpose
Media type values (in case of media type aware interworking modes):		
R-8.12.1.1/1:	media type = audio	WebRTC audio component
R-8.12.1.1/2:	media type = video	WebRTC video component
R-8.12.1.1/3:	media type = application	WebRTC data component
Transport protocol (stack) values:		
R-8.12.1.1/4:	proto = RTP/SAVPF	RTP profile for all RTP-based traffic components
R-8.12.1.1/5:	proto = UDP/DTLS/SCTP proto = TCP/DTLS/SCTP	WebRTC data traffic components (Note 1) and L4-aware NAT traversal support ("MGC knows the L4 protocol used at the start of communication phase")
R-8.12.1.1/6:	proto = DTLS/SCTP	WebRTC data traffic components (Note 1) and L4-agnostic NAT traversal support ("MG autonomously concludes whether UDP or TCP will be used at the start of communication phase")
Media format values (in case of *media format aware* interworking modes) (Note 2): a) audio formats (from WebRTC endpoint perspective, see [b-IETF rtcweb-audio]):		
R-8.12.1.1/7:	OPUS	Internet audio codec [b-IETF RFC 6716]
R-8.12.1.1/8:	PCMA / PCMU & CN	voice ITU-T G.711 μ/A-law with optional comfort noise
R-8.12.1.1/9:	telephone-event (event codepoints 0 to 11)	audio/telephone-event media format as specified in [b-IETF RFC 4733] for dual tone multi frequency (DTMF)

Table 1 – Requirements related to supported SDP elements – Part I SDP "m="-line

Requirement	SDP "m=" line element	Purpose
b) audio formats (optional, from NGN/IMS endpoint perspective, see use case #2):		
R-8.12.1.1/10:	AMR-WB	Adaptive multi-rate wideband [b-IETF RFC 4867]
R-8.12.1.1/11:	EVRC	Enhanced variable rate codec [b-IETF RFC 4788]
c) video formats (for consideration, see [b-IETF rtcweb-video]):		
R-8.12.1.1/12:	VP8	video codec [b-IETF RFC 6386], [b-IETF rtp-vp8]
R-8.12.1.1/13:	ITU-T H.264	video codec [b-IETF RFC 6184]
R-8.12.1.1/14:	VP9	video codec [b-IETF codec-vp9]
R-8.12.1.1/15:	ITU-T H.265	video codec [b-IETF rtp-h265]
d) text formats (for consideration):		
R-8.12.1.1/16:	ITU-T T.140	conversational text [IETF RFC 4103]
e) WebRTC data channel formats		
R-8.12.1.1/17:	webrtc-datachannel	generic data channel, realized as SCTP Stream over a DTLS session (Note 3).
NOTE 1 – SDP element defined by [b-IETF sdp-sctp]. There might be a subset of the protocol stack related name used in case of specific ITU-T H.248 Stream grouping models. NOTE 2 – Codec technologies are continuously improving, leading to a limited timeline of usage and their future replacement by evolved codecs. Thus, all listed media format specific types are not mandatory, but are listed in order to provide concrete use cases for the SDP-based parameterization of such codecs in ITU-T H.248 WebRTC gateways (see clause 8.12.2). MTI type of media formats are out of scope of this Recommendation, rather they are subject of concrete ITU-T H.248 profile specifications. NOTE 3 – SDP "m="-line media format value is defined by [b-IETF sdp-sctp].		

Table 2 – Requirements related to supported SDP elements – Part II SDP "a="-line

Requirement	SDP element	Purpose
NAT traversal support for media / bearer path:		
R-8.12.1.2/1:	a=ice-ufrag	ICE credentials for media level STUN authentication procedure
R-8.12.1.2/2:	a=ice-pwd	
R-8.12.1.2/3:	a=candidate: … TCP …	in case of last resort of TCP-based media transport (instead of UDP)
Security in the media / bearer path:		
R-8.12.1.2/4:	a=fingerprint	Authentication procedure for WebRTC DTLS sessions.
R-8.12.1.2/5:	a=crypto	in case of optional SDES-based SRTP
Indication of bearer establishment direction:		
R-8.12.1.2/6:	a=setup	This SDP attribute is used at session initiation protocol (SIP)-based WebRTC call control level, but not required for WebRTC gateway control (Note 1).
Traffic multiplexing in the media / bearer path:		
R-8.12.1.2/7:	a=group:BUNDLE	

Table 2 – Requirements related to supported SDP elements – Part II SDP "a="-line

Requirement	SDP element	Purpose
R-8.12.1.2/8:	a=mid:	General media grouping using "bundle" (Note 2). [ITU-T H.248.96] defines the usage of these SDP attributes because "SIP/SDP bundling" leads to "ITU-T H.248 Stream grouping", i.e., both SDP attributes are not used for WebRTC gateway control.
R-8.12.1.2/9:	a=rtcp-mux	for transport multiplexed RTP traffic [ITU-T H.248.57]
R-8.12.1.2/10:	a=rtcp	optional, if transport unmultiplexed mode for RTP and explicit RTCP transport address allocation [ITU-T H.248.57]
R-8.12.1.2/11:	a=ssrc:	Not required at ITU-T H.248 interface for basic WebRTC call services (Note 3).
WebRTC usage of RTP / RTCP:		
R-8.12.1.2/12:	a=rtcp-rsize	Support of reduced-size RTCP [IETF RFC 5506]
R-8.12.1.2/13:	a=rtcp-fb	RTP profile "RTP/SAVPF" is mandatory (see R-8.12.1.1/4). There are a number of potential RTCP-feedback based services in WebRTC. This SDP attribute is used to indicate which RTCP FB messages (from [IETF RFC 4585], [IETF RFC 5104]) are required for a specific WebRTC call.
WebRTC data traffic configuration:		
R-8.12.1.2/14:	a=sctp-port:…	The actual SCTP port value of the SCTP Association carried over DTLS/UDP, which is used for "WebRTC data channels" (Note 4)
R-8.12.1.2/15:	a=max-message-size:…	The maximum message size (indicated in bytes) that an SCTP Stream endpoint is willing to receive on the SCTP Association, which is used for "WebRTC data channels" (Note 4)
R-8.12.1.2/16:	a) application-agnostic: a=dcmap*:<SCTP StreamID>*	Assignment of a particual SCTP Stream to a WebRTC data traffic component (Note 5) without any indication of the subprotocol.
R-8.12.1.2/17:	a) application-aware a=dcmap*:<SCTP StreamID>* subprotocol="…"	Assignment of a particual SCTP Stream to a WebRTC data traffic component (Note 5) with indication of the subprotocol.
R-8.12.1.2/18:	a=dcsa:…	application-specific information of a particular subprotocol as WebRTC data channel (Note 5), (Note 6).

Table 2 – Requirements related to supported SDP elements – Part II SDP "a="-line

Requirement	SDP element	Purpose
NOTE 1 – There are primarily two reasons: 1) The SDP attribute is semantically overloaded (because defined for multiple protocols), therefore it is mapped (by the MGC) to ITU-T H.248 Signal/Event-based bearer control procedures; 2) Semantical differences between WebRTC clients and WebRTC gateways. Example: [b-IETF data-channel-msrp] describes the usage of this SDP attribute in context of WebRTC MSRP-based data service. The attribute clarifies, *inter alia*, MSRP role assignments between two WebRTC client instances. However, the MSRP will be not terminated by the ITU-T H.248 WebRTC gateway because it primarily acts as a pure MSRP message forwarding instance, leading to MSRP role agnostic behaviour. NOTE 2 – SDP element defined by [b-IETF sdp-bundle]. NOTE 3 – There might be in future an overlay of well-known supplementary services (such as call transfer) for WebRTC clients, which could require explicit signalling of (RTP) source specific information. However, such WebRTC service extensions are for further studies. NOTE 4 – SDP element defined by [b-IETF sdp-sctp]. NOTE 5 – SDP element defined by [b-IETF DCSDP]. NOTE 6 – See [b-IETF data-channel-msrp] concerning the SDP profiling for the example usage of a WebRTC data channel for application protocol "MSRP".		

Table 3 – Requirements related to supported SDP elements – Part III other SDP lines

Requirement	SDP element	Purpose
Transport capacity reservation and allocation – ITU-T H.248 Stream admission control:		
R-8.12.1.3/1:	"b="-line	See [b-IETF rtp-usage]; The following bandwidth modifier values might be used: RR, RS, AS, CT. The concrete usage at call control level is conditional, dependent on multiplexing, RTCP services and overall QoS architecture. The "b="-line information is typically subject of bandwidth and admission control at ITU-T H.248 interfaces (see e.g., section 5.17.1.5 of [b-ETSI TS 183 018]). The MGC needs to provide sufficient "b="-line information to the MG, to be in concert with any optional traffic policing parameter values (e.g., when [ITU-T H.248.53] is applied).

8.12.2 Requirements related to supported SDP elements – Codec configurations

Table 1 introduced the required *media formats* ("codecs"), which usually include a set of parameters concerning their configuration. These parameters are signalled via SDP from MGC to MG and affect the RTP packet encapsulation ("internal structure of the protocol data unit"), codec processing and RTCP handling, dependent on media-aware / media-agnostic modes of operation of the ITU-T H.248 WebRTC gateway.

8.12.2.1 SDP elements related to the parameterization of audio codec "OPUS"

See section 2.1 of [b-IETF RFC 6716]:

*"The Opus codec includes a number of control parameters that can be **changed dynamically** during regular operation of the codec, **without interrupting the audio stream** from the encoder to the decoder. These parameters **only affect the encoder** since any impact they have on the bitstream is*

signalled in-band *such that a decoder can decode any Opus stream without any out-of-band signalling. Any Opus implementation can add or modify these control parameters without affecting interoperability. The most important encoder control parameters in the reference encoder are listed below."*

The ITU-T H.248 WebRTC gateway, when enabled for media aware interworking, would provide such an encoder and decoder function, hence is required to support SDP elements (for the purpose of media gateway control) according to Table 4. [b-IETF RFC 7587] defines the formal codec parameters (in section 6.1) and their mapping on SDP elements (in section 7.1 of [b-IETF RFC 7587]). The parameter value ranges and default values in Table 4 are defined in section 6.1 of [b-IETF RFC 7587].

Table 4 – SDP parameters for IANA registered media type "audio/opus"

Requirement	Codec parameter	SDP parameter	M/O	Value range	Default	Comments and ITU-T H.248 profile
R-8.12.2.1/1:	rate ("sampling rate")	a=rtpmap:… opus/48000/2	M	8000, 12000, 16000, 24000, 48000	48000	all (Note 2)
R-8.12.2.1/2:	maxplaybackrate	a=fmtp: (Note 1)	O		48000	all
R-8.12.2.1/3:	sprop-maxcapturerate	a=fmtp: (Note 1)	O		48000	all
R-8.12.2.1/4:	maxptime	a=maxptime	O	3, 5, 10, 20, 40, 60, or an arbitrary multiple of a frame size rounded up to the next full integer value, up to a max. value of 120	120 (Note 3)	If "media transcoding" mode, it is recommended to align these parameter values between the OPUS and non-OPUS RTP domain in order to minimize end-to-end latency and to avoid interworking complexity.
R-8.12.2.1/5:	ptime	a=ptime	O		20 (Note 3)	
R-8.12.2.1/6:	maxaveragebitrate	a=fmtp: (Note 1)	O	Any positive integer is allowed, but values outside the range 6000 to 510000 SHOULD be ignored	Dependent on OPUS mode	all
R-8.12.2.1/7:	stereo	a=fmtp: (Note 1)	O	0 (mono), 1 (stereo)	0 (mono)	at least 'mono' (Note 4)
R-8.12.2.1/8:	sprop-stereo	a=fmtp: (Note 1)	O		0 (mono)	at least 'mono' (Note 4)
R-8.12.2.1/9:	cbr	a=fmtp: (Note 1)	O	1 (constant bitrate), 0 (variable bitrate)	0 (vbr)	Specific mode interacts normally with traffic policer settings ([ITU-T H.248.53]).
R-8.12.2.1/10:	useinbandfec	a=fmtp: (Note 1)	O	0 (no FEC), 1 (FEC)	0 (no FEC)	
R-8.12.2.1/11:	usedtx	a=fmtp: (Note 1)	O	0 (no DTX), 1 (DTX)	0 (no DTX)	

Table 4 – SDP parameters for IANA registered media type "audio/opus"

Requirement	Codec parameter	SDP parameter	M/O	Value range	Default	Comments and ITU-T H.248 profile
NOTE 1 – Media type string in the form of a semicolon-separated list of parameter=value pairs, as part of the "a=fmtp" SDP attribute. E.g., a=fmtp:101 maxplaybackrate=16000; sprop-maxcapturerate=16000; maxaveragebitrate=20000; stereo=1; useinbandfec=1; usedtx=0 NOTE 2 – The actual clock rate is signalled in the RTP payload and is not restricted by the control plane signalled values. NOTE 3 – Default values are typically subject of network operator preferences, which lead to correspondent settings in supported user equipment. NOTE 4 – This parameter is only relevant in case of media translation mode, i.e., transcoding OPUS to a different audio codec. The majority of legacy audio codecs only support 'mono'. Transcoding scenarios to other, stereo-capable audio codecs is for further studies.						

Table 4 provides the codec parameter value framework for the usage of OPUS in context of ITU-T H.248 WebRTC gateways.

8.12.3 Requirements related to SDP offer/answer

WebRTC does not mandate a specific call control signalling protocol. Thus, there are no guidelines for SDP offer/answer from the IETF side in case of SIP as WebRTC call control protocol.

In case of SIP networks with ITU-T H.248 WebRTC gateways, handling of SDP offer/answer procedures between call control level and their representation at ITU-T H.248 gateway control level is outlined by [ITU-T H.248.80], particularly when the *revised SDP offer/answer* model is used.

8.13 Requirements related to ITU-T H.248 signalling

There might be additional, ITU-T H.248 specific requirements beyond the pure WebRTC service consideration.

8.13.1 Indication of ITU-T H.248 "WebRTC" Terminations

A WebRTC-enabled ITU-T H.248 Termination fundamentally implies that the MG needs to provide a WebRTC client function for the particular Termination in a Context. Such information might be relevant, e.g., from the MG resource management perspective.

R-8.13.1/1: The ITU-T H.248 WebRTC gateway is not required to support additional ITU-T H.248 signalling capabilities in order to discriminate (in MGC to MG direction) between ITU-T H.248 WebRTC and non-WebRTC Terminations.

NOTE – The above requirement makes the assumption that the Termination type indication could be indirectly derived, e.g., from the Termination naming scheme or Termination/Stream specific ITU-T H.248 Descriptor contents.

9 Data channel establishment protocol support package

Package name: Data channel establishment protocol support ackage

Package ID: dcep (0x0124)

Description: This package allows the support of the data channel establishment protocol (DCEP) [b-IETF DCEP] on an MGC/MG. The package allows the MG to detect the reception of DCEP messages (SCTP payload protocol identifier (PPID)=50) on WebRTC data channels.

Version: 1

Extends: None

9.1 Properties

None.

9.2 Events

9.2.1 Detect DCEP Messages

Event name: Detect DCEP Messages

Event ID: detmess (0x0001)

Description: This event detects the reception of DCEP DATA_CHANNEL_OPEN and DATA_CHANNEL_ACK messages on any of the SCTP Streams on an SCTP Association.

9.2.1.1 EventsDescriptor parameters

9.2.1.1.1 DCEP data channel open response

Parameter name: DCEP data channel open response

Parameter ID: openresp (0x0001)

Description: This parameter indicates to the MG whether it should respond autonomously to the reception of a DCEP data channel open.

Type: Enumeration

Optional: Yes

Possible values:

"auto"	The MG shall accept incoming DCEP DATA_CHANNEL_OPEN request message on an SCTP Stream by sending a DATA_CHANNEL_ACK message on an outgoing SCTP Stream with the same identity. If the incoming DATA_CHANNEL_OPEN results in an error the MG shall generate an SCTP Stream reset.
"deny"	The MG shall deny the incoming DCEP DATA_CHANNEL_OPEN requests by initiating an SCTP Stream reset on the applicable SCTP Stream.
"mgc"	The MGC will decide the action based on the reception of a DCEP DATA_CHANNEL_OPEN. E.g., The MG may issues a "DCEP data channel open response" (*dcep/dcopenresp*) Signal or initiate an SCTP reset via the *sctpreset/initreset* Signal.

Default: "auto"

9.2.1.2 ObservedEventsDescriptor parameters

9.2.1.2.1 SCTP StreamID

Parameter name: SCTP StreamID

Parameter ID: sctpid (0x0001)

Description: This parameter indicates the SCTP StreamID that the DCEP DATA_CHANNEL_OPEN message was received on.

Type: Integer

Optional: No

Possible values: 0 – 65535

Default: None

9.2.1.2.2 Sub-protocol ID

Parameter name: Sub-protocol ID

Parameter ID: protocol (0x0002)

Description: This parameter contains the "Protocol" from the received DCEP DATA_CHANNEL_OPEN message.

Type: String

Optional: Yes

Possible values: As per "Protocol" in section 5.1 of [b-IETF DCEP].

Default: None

9.2.1.2.3 Label

Parameter name: Label

Parameter ID: label (0x0003)

Description: This parameter contains the "Label" from the received DCEP DATA_CHANNEL_OPEN message.

Type: String

Optional: Yes

Possible values: As per "Label" in section 5.1 of [b-IETF DCEP].

Default: None

9.2.1.2.4 Channel Type

Parameter name: Channel Type

Parameter ID: chtype (0x0004)

Description: This parameter contains the "Channel Type" from the received DCEP DATA_CHANNEL_OPEN message.

Type: Integer

Optional: No

Possible values: As per "Channel Type" in section 5.1 of [b-IETF DCEP].

Default: None

9.2.1.2.5 Reliability Parameter

Parameter name: Reliability Parameter

Parameter ID: reli (0x0005)

Description: This parameter contains the "Reliability Parameter" from the received DCEP DATA_CHANNEL_OPEN message.

Type: Integer

Optional: No

Possible values: As per "Reliability Parameter" in section 5.1 of [b-IETF DCEP].

Default: None

9.2.1.2.6 Priority

Parameter name: Priority

Parameter ID: priority (0x0006)

Description: This parameter contains the "Priority" from the received DCEP DATA_CHANNEL_OPEN message.

Type: Integer

Optional: No

Possible values: As per "Priority" in section 5.1 of [b-IETF DCEP].

Default: None

9.2.1.2.7 Error

Parameter name: Error

Parameter ID: error (0x0007)

Description: This parameter indicates that the MG has received a DCEP DATA_CHANNEL_OPEN but has determined it to be erroneous. The action taken by the MG is dependent on the *openresp* parameter.

Type: Boolean

Optional: Yes

Possible values: On An error has been generated.

Off No error has been generated.

Default: Off

9.2.1.2.8 Data Channel Message Type

Parameter name: Data Channel Message Type

Parameter ID: ack (0x0008)

Description: This parameter indicates that the MG has received a DCEP DATA_CHANNEL_ACK.

Type: Enumeration

Optional: Yes

Possible values: ACK A DATA_CHANNEL_ACK was received.

OPEN A DATA_CHANNEL_OPEN was received.

Default: OPEN

9.3 Signals

9.3.1 Send DCEP Open

Signal name: Send DCEP Open

Signal ID: sndopen (0x0001)

Description: This Signal requests the MG to send a DCEP DATA_CHANNEL_OPEN message with the indicated parameters on a particular SCTP Stream.

Signal type: Brief

Duration: Not applicable

9.3.1.1 Additional parameters

9.3.1.1.1 SCTP StreamID

Parameter name: SCTP StreamID

Parameter ID: sctpid (0x0001)

Description: This parameter indicates the SCTP StreamID that the DCEP DATA_CHANNEL_OPEN message is to be sent on.

Type: Integer

Optional: No

Possible values: 0 – 65535

Default: None

9.3.1.1.2 Sub-protocol ID

Parameter name: Sub-protocol ID

Parameter ID: protocol (0x0002)

Description: This parameter contains the "Protocol" to be sent in the DCEP DATA_CHANNEL_OPEN message.

Type: String

Optional: Yes

Possible values: As per "Protocol" in section 5.1 of [b-IETF DCEP].

Default: None

9.3.1.1.3 Label

Parameter name: Label

Parameter ID: label (0x0003)

Description: This parameter contains the "Label" to be sent in the DCEP DATA_CHANNEL_OPEN message.

Type: String

Optional: Yes

Possible values: As per "Label" in section 5.1 of [b-IETF DCEP].

Default: None

9.3.1.1.4 Channel Type

Parameter name: Channel Type

Parameter ID: chtype (0x0004)

Description: This parameter contains the "Channel Type" to be sent in the DCEP DATA_CHANNEL_OPEN message.

Type: Integer

Optional: No

Possible values: As per "Channel Type" in section 5.1 of [b-IETF DCEP].

Default: None

9.3.1.1.5 Reliability Parameter

Parameter name: Reliability Parameter

Parameter ID: reli (0x0005)

Description: This parameter contains the "Reliability Parameter" to be sent in the DCEP DATA_CHANNEL_OPEN message.

Type: Integer

Optional: No

Possible values: As per "Reliability Parameter" in section 5.1 of [b-IETF DCEP].

Default: None

9.3.1.1.6 Priority

Parameter name: Priority

Parameter ID: priority (0x0006)

Description: This parameter contains the "Priority" to be sent in the DCEP DATA_CHANNEL_OPEN message.

Type: Integer

Optional: No

Possible values: As per "Priority" in section 5.1 of [b-IETF DCEP].

Default: None

9.3.2 DCEP Open Response

Signal name: DCEP Open Response

Signal ID: dcopenresp (0x0002)

Description: This Signal requests the MG to send a DCEP DATA_CHANNEL_ACK message on a particular SCTP Stream.

Signal type: Brief

Duration: Not applicable

9.3.2.1 Additional parameters

9.3.2.1.1 SCTP StreamID

Parameter name: SCTP StreamID

Parameter ID: sctpid (0x0001)

Description: This parameter indicates the SCTP StreamID that the DCEP DATA_CHANNEL_ACK message is to be sent on.

Type: Integer

Optional: No

Possible values: 0 – 65535

Default: None

9.4 Statistics

None.

9.5 Error codes

None.

9.6 Procedures

9.6.1 Auditing

An MGC may determine if an MG supports the use of DCEP by auditing packages. If the MG returns the "dcep" package, then the DCEP is supported.

9.6.2 Pre-conditions

In order to detect DCEP messages the MGC shall first establish a UDP/DTLS/SCTP Association for WebRTC data channel. See [ITU-T H.248.97] for details on the establishment of an SCTP Association. The establishment of an SCTP Association may also require the use of [ITU-T H.248.96] and a deaggregation stream. A single ITU-T H.248 component stream is used for an incoming and outgoing SCTP Stream with the same identity. The Signals and Events in the "dcep" package are applied to the ITU-T H.248 Stream representing the SCTP Association as a whole (i.e., a deaggregation stream and not to the component streams). When setting these Signals and Events the MGC shall provide the ITU-T H.248 StreamID of the deaggregation stream representing the SCTP Association. Notifications of ObservedEvents shall also indicate the ITU-T H.248 StreamID of the deaggregation stream representing the SCTP Association.

NOTE – In addition, the Signals and the Observed Event specified in this package contain the identifier of the SCTP StreamID where the DCEP messages are sent or received.

9.6.3 Opening a data channel based on a remote request

In order to detect DCEP DATA_CHANNEL_OPEN and DATA_CHANNEL_ACK messages on the SCTP Association the MGC shall set the "Detect DCEP Data Channel Open" (*dcep/detmess*) Event on the ITU-T H.248 Stream on the applicable Termination. Setting this Event indicates that the Termination/Stream shall support the procedures specified in section 6 of [b-IETF DCEP] . The MG shall monitor the SCTP Association for the reception of a DCEP DATA_CHANNEL_OPEN and DATA_CHANNEL_ACK messages (indicated by SCTP PPID=50) on the SCTP Streams in the SCTP Association.

On reception of a DCEP DATA_CHANNEL_OPEN message, the MG shall generate a *dcep/detmess* ObservedEvent and notify the MGC. If the MG detects an error, it shall include the "error" ObservedEvent parameter and any other relevant parameters. Further action taken by the MG in response to the detection of a DCEP DATA_CHANNEL_OPEN message is dependent on the "DCEP data channel open response" (*openresp*) Event parameter. If *openresp* is set to "mgc" then the MGC will accept the open request by sending the *dcep/dcopenresp* Signal or deny the open request by initiating an SCTP Stream reset via the *sctpreset/initreset* signal. If *openresp* is set to "auto" then the MG shall respond autonomously as per clause 9.2.1.1.1.

As the DCEP DATA_CHANNEL_OPEN sender may immediately send data on the SCTP Stream the MG should preferably have the capability to buffer incoming SCTP user data during short periods until the MGC creates a component stream to deliver the data internal to the Context.

NOTE: SCTP offers reliable transmission, therefore it can recover from an eventual loss of user messages, but at the cost of retransmission.

The MGC, in turn, should react with no delay to the notification of the reception of the DCEP DATA_CHANNEL_OPEN from the peer (i.e., by creating the component stream and setting the *sctpid* property to the correct value) in order not to exhaust the buffering capabilities of the MG.

On reception of a DCEP DATA_CHANNEL_ACK message the MG shall generate a *dcep/detmess* ObservedEvent with the "Data Channel Acknowledgement" (*ack*) parameter and notify the MGC. In order to instantiate the data channel and to allow data to flow into the Context, the MGC should create a new ITU-T H.248 Stream and assign the SCTP StreamID received in the ObservedEvent DCEP DATA_CHANNEL_OPEN message to it via the *sctp/sctpid* property (see clause 8.1.2 of [ITU-T H.248.97]). The MGC should add the ITU-T H.248 Stream as a component stream of a deaggregation stream via the *mgroup/strdeagg* property and add it to the "SCTP" semantic via the *mgroup/groupse* property. See [ITU-T H.248.96] for more details. Once created any buffered data should be delivery internally to the Context via the component stream.

The following clauses show an example information flow.

9.6.3.1 Remote open request example step 1

The MGC sends an Add.request to the MG adding a UDP/DTLS/SCTP Association and requests the MG to detect DCEP DATA_CHANNEL_OPEN messages.

Table 5 – Remote open request example step 1

Step 1	Comments
MEGACO/3 [123.123.123.4]:55555 **Transaction = 10000 {** **Context = 1 {** **Add = T1 {** Events = 1235 {**dcep/detmess**{stream=1,openresp=mgc}}, **Media {** **Stream = 1 {** **Local {** v=0 c= IN IP4 $ m=application $ UDP/DTLS/SCTP webrtc- datachannel a=max-message-size: 100000 a=sctp-port:5000 **}** **},** **}** **}** **}** }	An ITU-T H.248 Stream is added to a Termination representing the UDP/DTLS/SCTP Association used for WebRTC datachannel. The MGC sets the *dcep/detmess* event to detect DCEP DATA_CHANNEL_OPEN messages. The MG will notify the MGC when the open is detected and await a response from the MGC. NOTE – The RemoteDescriptor and SDP regarding the DTLS establishment e.g., a=connection, a=fingerprint is not shown.

On reception of the Add.request, the MG starts monitoring the SCTP Streams for DCEP DATA_CHANNEL_OPEN messages. It sends an Add.reply.

9.6.3.2 Remote open request example step 2

The MG detects a DCEP DATA_CHANNEL_OPEN message related to SCTP StreamID = 5. It generates a notification to the MGC.

Table 6 – Remote open request example step 2

Step 2	Comments

MEGACO/3 [125.125.125.111]:55555
Transaction = 2000 {
Context = 1 {
Notify = T1 {ObservedEvents =12345 {
20150115T22020002:**dcep/detmess**{
stream=1,sctpid=5,
chtype=0,reli=0,priority=1}}}
}
}
	The MG reports that a DCEP DATA_CHANNEL_OPEN has been received on SCTP Stream 5. It reports the SCTP StreamID, Channel Type, Reliability Parameter and Priority.

The MGC sends a Notify.reply.

9.6.3.3 Remote open request example step 3

The MGC decides to allow the DCEP channel open request and adds the SCTP Stream as a component of a deaggregation stream.

Table 7 – Remote open request example step 3

Step 3	Comments
MEGACO/3 [123.123.123.4]:55555 **Transaction = 10001 {** **Context = 1 {** **Modify = T1 {** Signals {**dcep/dcopenresp**{Stream=1, sctpid=5}}, Events = 1235 {**dcep/detmess**{Stream=1}}, **Media {** **TerminationState {** **mgroup/groupse**= [”SCTP 2”] **},** **Stream = 1 {** **LocalControl {** **mgroup/strdeagg**=[2] **}** **},** **Stream = 2 {** **LocalControl {** **sctpbcc/sctpid**=5 **}** **}** **}** **}** **}** }	The MGC modifies ITU-T H.248 StreamID = 1 and indicates that it is a deaggregation stream. The group semantic is indicated as "SCTP" ITU-T H.248 StreamID = 2 is added to represent the data in SCTP Stream 5.

On reception of the Modify.request the MG will create a new component stream for ITU-T H.248 StreamID = 2 and start to pass data received in SCTP StreamID = 5 internally to the Context.

9.6.4 Local request to open a data channel

Once the MGC has added an ITU-T H.248 Stream that establishes a UDP/DTLS/SCTP Association for WebRTC data channels with the remote peer, it can request via the "Send DCEP Open" (*dcep/sndopen*) Signal that the MG send a DCEP DATA_CHANNEL_OPEN on a certain SCTP Stream. The MGC shall include the SCTP StreamID, Channel Type, reliability parameter and priority parameters in the signal. The Signal shall be set on the Stream representing the whole SCTP Association (i.e., the deaggregation stream).

The MGC should also set an Event to detect the DCEP DATA_CHANNEL_ACK message for the incoming SCTP Stream with the same ID as used in the Signal. See clause 9.6.3 for the procedures for setting Events. It should also set an Event to detect SCTP resets indicating a failure of the channel open.

In order to prepare the MG to send data on the SCTP Stream and to allow the reception of data from the remote peer once it sends a DCEP DATA_CHANNEL_OPEN, the MGC should:

– indicate that the ITU-T H.248 Stream representing the SCTP Association is a deaggregation stream;

– indicate that the grouping semantic for the deaggregation stream is "SCTP";

– add a component stream representing the SCTP StreamID that the DCEP DATA_CHANNEL_OPEN message is sent on.

The MG shall then forward any data received on the SCTP StreamID internally in the Context via the component stream.

The following clauses show an example message sequence.

9.6.4.1 Local open request example step 4

The MGC sends a Modify.request to the MG requesting that the MG send a DCEP DATA_CHANNEL_OPEN message on a particular stream. A deaggregation and component stream is also added in order to receive data from the remote peer.

NOTE – This example builds on the example in clause 9.6.3.

Table 8 – Local open request example step 4

Step 4	Comments
MEGACO/3 [123.123.123.4]:55555 **Transaction = 1004 {** **Context = 1 {** **Modify = T1 {** Signals {**dcep/sndopen**{Stream=1, sctpid=7,chtype=0,reli=0,priority=1}}, **Media {** **TerminationState {** **mgroup/groupse**= [”SCTP 2 3”] **},** **Stream = 1 {** **LocalControl {** **mgroup/strdeagg**=[2,3] **}** **},** **Stream = 3 {** **LocalControl {** **sctpbcc/sctpid**=7 **}** **}** **}** **}** **}** }	The MGC requests the MG to send a DCEP DATA_CHANNEL_OPEN message on SCTP StreamID = 7. It creates ITU-T H.248 StreamID = 3 as a component stream and assigns it to SCTP StreamID = 7. It adds ITU-T H.248 StreamID = 3 to the SCTP grouping semantic and adds it to the deaggregation stream.

On reception of the Modify.request the MG sends DCEP DATA_CHANNEL_OPEN message message on SCTP StreamID = 7 and monitors the SCTP Stream for data. It also sends a Modify.reply.

9.6.4.2 Local open request example step 5

The MG sends a notify request to the MGC indicating that it has received a DCEP DATA_CHANNEL_ACK message on SCTP Stream 7. It indicates that the DCEP DATA_OPEN_REQUEST was successful.

Table 9 – Local open request example step 5

Step 5	Comments

MEGACO/3 [125.125.125.111]:55555
Transaction = 2010 {
Context = 1 {
Notify = T1 {ObservedEvents =12345 {
20150115T22020012:**dcep/detmess**{
stream=1,sctpid=7,ack="ACK"}}}
}
}
	The MG reports that a DCEP DATA_CHANNEL_ACK has been received on SCTP Stream 7.

9.6.5 Data channel closure

WebRTC data channels are closed according to the procedures in section 6.7 of [b-IETF webRTCDC]. The procedures use the mechanism in [IETF RFC 6525] to support the closure of an SCTP Stream. The "SCTP Re-configuration Stream Reset Package" (*sctpreset*) allows for the support of the RE-CONFIG outgoing SCTP Stream reset. This package shall be implemented if the *dcep* package is used.

To initiate a channel closure the MGC shall use the "Initiating an outgoing SCTP Stream reset" procedures defined in clause 9.6.2 of [ITU-T H.248.97].

The MGC shall also use the "Responding to an outgoing SCTP Stream reset request" procedures in clause 9.6.3 of [ITU-T H.248.97] in order to respond to remote channel closure requests.

If the MGC requires that an MG respond to a received outgoing stream reset request by autonomously sending its own outgoing reset request the MGC shall set the *sctpreset/initreset* Signal parameter *outresp* to "accint".

9.6.6 Termination of DCEP messages

The use of this package on an ITU-T H.248 SEP implies that DCEP messages are terminated in the SEP, i.e., incoming DCEP messages are not transferred internally to the other SEP, even if the Context Topology would allow the transfer of SCTP user messages.

10 Out-of-band WebRTC data channel negotiation

The use of individual data channels may be negotiated by out-of-band procedures such as those defined by [b-IETF DCSDP]. The individual channels are assigned a protocol and SCTP Stream deaggregation is applied via the "SCTP grouping semantic" procedures of clause 11.2 of [ITU-T H.248.97].

In order to send and receive data on the individual data channels the MGC should use [ITU-T H.248.78] to:

– backhaul the relevant bearer-level application protocol across ITU-T H.248 and on to the relevant ITU-T H.248 Stream/SCTP StreamID; or

– request the MG to perform bearer-level ALG functions (i.e., by utilizing the *mgbalg* package [ITU-T H.248.78].

11 ITU-T H.248 profile specification guidelines

This clause provides guidelines for ITU-T H.248 profile specifications. The structure follows the profile template according to Appendix III of [ITU-T H.248.1].

The template elements which are not applicable in this Recommendation are indicated by "*Subject to profile specification*".

Any profile guidelines are primarily dependent on the concerned network configuration and use case. The guidelines in this clause are therefore basically conditional. Some exemplary use cases are considered (as described in Appendix I), termed as capability sets: CS_A, CS_B, CS_C and CS_D. Tag 'CS*' indicates unconditional profile elements, which are either generic because they are basic WebRTC capabilities or required for all four CS examples.

11.1 Profile identification

Subject to profile specification.

11.2 Summary

Subject to profile specification.

11.3 Gateway control protocol version

Subject to profile specification.

11.4 Connection model

Maximum number of Contexts:	*Subject to profile specification.*
Maximum number of Terminations per Context:	*Subject to profile specification.* Examples: IF CS_A OR CS_B OR CS_C THEN "2". IF CS_D THEN "N".
Allowed termination type combinations in a Context:	*Subject to profile specification.*

11.5 Context attributes

Subject to profile specification.

11.6 Terminations

Subject to profile specification.

11.7 Descriptors

11.7.1 TerminationState Descriptor

IF CS* THEN following table:

TerminationState: Group semantics (*mgroup/groupse*)	See clause 11.14.3.8.
TerminationState: …	…

All other aspects related to TerminationState Descriptor (e.g., ServiceState, EventBuffer Control) are "*Subject to profile specification*".

11.7.2 Stream Descriptor

Subject to profile specification.

Note that an ITU-T H.248 IP Termination for the WebRTC service may carry additional ITU-T H.248 *(de-)aggregation streams* besides the legacy ITU-T H.248 component streams. There are then additional, dedicated Stream Descriptors at *(de-)aggregation stream* level.

11.7.3 Events Descriptor

IF CS_A OR CS_B OR CS_C THEN use the following table:

Events settable on termination types and stream types:		Yes	
If yes	**Event ID**	**Termination type**	**Stream type**
	See clause 11.14.3.4 stnconfres/constate stnconfres/confail	IP	IP-enabled
	See clause 11.14.3.5 tlsbsc/BNCChange	IP	DTLS-enabled
	See clause 11.14.3.6 sctpbcc/BNCChange	IP	SCTP-enabled
	See clause 11.14.3.7 sctpreset/detreset sctpreset/result	IP	SCTP-enabled

IF CS_A THEN use the following table:

Events settable on termination types and stream types:		Yes	
If yes	**Event ID**	**Termination type**	**Stream type**
	See clause 11.14.3.3 – ostuncc/ccr – ostuncc/nprc	IP	IP-enabled
NOTE – These *ostuncc* events are only required for ICE full mode.			

IF CS_A OR CS_B THEN use the following table:

Events settable on termination types and stream types:		Yes	
If yes	**Event ID**	**Termination type**	**Stream type**
	See clause 11.14.3.13 – srtp/mke	IP	SRTP-enabled
	See clause 11.14.3.16 – tlsm/mgea	IP	DTLS-enabled
	See clause 11.14.3.18 – adr/rtac	IP	IP-enabled

IF CS_A OR CS_D THEN use the following table:

Events settable on termination types and stream types:		Yes	
If yes	**Event ID**	**Termination type**	**Stream type**
	See clause 11.14.3.9 – dcep/detmess	IP	SCTP-enabled
	See clause 11.14.3.10 – mcbalg/det	IP	SCTP-enabled

All other aspects related to Events Descriptor (e.g., EventBuffer Control, KeepActive, Notification Behaviour) are "*Subject to profile specification*".

11.7.4 EventBuffer Descriptor

Subject to profile specification.

11.7.5 Signals Descriptor

IF CS_A OR CS_B OR CS_C THEN use the following table:

The setting of signals is dependent on termination or streams types:		Yes	
If yes	**Signal ID**	**Termination type**	**Stream type/ID**
	See clause 11.14.3.1 – ipnapt/latch	IP	IP-enabled
	See clause 11.14.3.4 – stnconfres/contst	IP	IP-enabled
	See clause 11.14.3.5 – tlsbsc/EstBNC – tlsbsc/RelBNC	IP	DTLS-enabled
	See clause 11.14.3.6 – sctpbcc/EstBNC – sctpbcc/RelBNC	IP	SCTP-enabled
	See clause 11.14.3.7 – sctpreset/initreset – sctpreset/resetresp	IP	SCTP-enabled

IF CS_A THEN use the following table:

The setting of signals is dependent on termination or streams types:		Yes	
If yes	**Signal ID**	**Termination type**	**Stream type/ID**
	See clause 11.14.3.3 – ostuncc/scc – ostuncc/sacc	IP	IP-enabled
NOTE – These *ostuncc* signals are only required for ICE full mode.			

IF CS_A OR CS_B THEN use the following table:

The setting of signals is dependent on termination or streams types:		Yes	
If yes	**Signal ID**	**Termination type**	**Stream type/ID**
	See clause 11.14.3.16 – tlsm/mgcea	IP	DTLS-enabled

IF CS_A OR CS_D THEN use the following table:

The setting of signals is dependent on termination or streams types:		Yes	
If yes	**Signal ID**	**Termination type**	**Stream type/ID**
	See clause 11.14.3.9 – dcep/sndopen – dcep/dcopenresp	IP	SCTP-enabled
	See clause 11.14.3.10 – mcbalg/sblm	IP	SCTP-enabled

All other aspects related to Signals Descriptor (e.g., Signal direction, Signal list) are "*Subject to profile specification*".

11.7.6 DigitMap Descriptor

Subject to profile specification.

11.7.7 Statistics Descriptor

IF CS_B OR CS_C OR CS_D THEN none.

IF CS_A THEN following table entries: see clauses 11.14.3.13, 11.14.3.17 and 11.14.3.19.

11.7.8 ObservedEvents Descriptor

Subject to profile specification.

11.7.9 Topology Descriptor

Subject to profile specification.

11.7.10 Error Descriptor

IF CS* THEN use the following table:

Error codes sent by the MGC:

Supported ITU-T H.248.8 error codes:	…
Supported error codes defined in packages:	…

Error codes sent by the MG:

Supported ITU-T H.248.8 error codes:	…
Supported error codes defined in packages:	#489 "Invalid aggregation and/or deaggregation"

IF CS_A THEN the following table in addition:

Error codes sent by the MGC:

Supported ITU-T H.248.8 error codes:	…
Supported error codes defined in packages:	…

Error codes sent by the MG:

Supported ITU-T H.248.8 error codes:	…
Supported error codes defined in packages:	#488 "Incorrect stream endpoint interlinkage"

All other error codes are "*Subject to profile specification*".

11.8 Command API

NOTE – It is assumed that an Error Descriptor may be returned in any command reply.

11.8.1 Add

Subject to profile specification.

11.8.2 Modify

Subject to profile specification.

11.8.3 Subtract

Subject to profile specification.

11.8.4 Move

Subject to profile specification.

11.8.5 AuditValue

Subject to profile specification.

11.8.6 AuditCapabilities

Subject to profile specification.

11.8.7 Notify

Subject to profile specification.

11.8.8 ServiceChange

Subject to profile specification.

11.8.9 Manipulating and auditing Context attributes

Subject to profile specification.

11.9 Generic command syntax and encoding

Subject to profile specification.

11.10 Transactions

Subject to profile specification.

NOTE – There is no impact on Transactions.

11.11 Messages

Subject to profile specification.

11.12 Transport

Subject to profile specification.

NOTE – Usage of bearer security may demand for a secured ITU-T H.248 transport mode, too.

11.13 Security

Subject to profile specification.

11.14 Packages

11.14.1 Mandatory packages

Mandatory: specifies the packages that shall be supported in this profile.

Examples:

IF CS_A OR CS_B OR CS_C THEN use the following table:

Mandatory packages:			
Package name	**PackageID**	**Version**	**Termination types supported (Note)**
"IP NATT traversal package" [ITU-T H.248.37]	ipnapt (0x0099)	v1	IP
"MG act-as STUN server package" [ITU-T H.248.50]	mgastuns (0x00c2)	v1	IP
"Originate STUN continuity check package" [ITU-T H.248.50]	ostuncc (0x00c3)	v1	IP
"STUN consent freshness package" [b-IANA H.248 Packages]	stnconfres (0x0120)	v1	IP
"TLS basic session control package" [ITU-T H.248.90]	tlsbsc (0x0117)	v1	IP; Stream type: "DTLS-enabled UDP or TCP connection"
"SCTP basic connection control package" [ITU-T H.248.97]	sctpbcc (0x0121)	v1	IP; Stream type: "DTLS-enabled L4 connection"
"SCTP reconfiguration stream reset package" [ITU-T H.248.97]	sctpreset (0x0122)	v1	IP; Stream type: "DTLS-enabled L4 connection"
"Media grouping package" [ITU-T H.248.96]	mgroup (0x011f)	v1	IP
NOTE – Termination types: an ITU-T H.248 profile might further differentiate IP-based ITU-T H.248 Terminations in "WebRTC" and "non-WebRTC" Terminations (see also clause 8.12). This note applies also for the tables in following clause 11.14.2.			

11.14.2 Optional packages

Examples:

IF CS_A OR CS_B THEN use the following table:

Optional packages:			
Package name	**PackageID**	**Version**	**Termination types supported**
"Stream endpoint interlinkage package" [ITU-T H.248.92]	seplink (0x011b)	v1	IP
"TLS capability negotiation package" [ITU-T H.248.90] (Note 1)	tlscn (0x0118)	v1	IP
"TLS session maintenance package" [ITU-T H.248.90] (Note 2)	tlsm (0x0119)	v1	IP
NOTE 1 – Applied for DTLS-enabled stream endpoints (in context of the SCTP/DTLS/UDP protocol layering). NOTE 2 – Related to DTLS layer.			

Examples:

IF CS_A OR CS_B OR CS_C THEN use the following table:

Optional packages:			
Package name	**PackageID**	**Version**	**Termination types supported**
"Secure RTP package" [ITU-T H.248.77] (Note)	srtp (0x0107)	v2	IP
NOTE – Selection of key management scheme for SRTP.			

Examples:

IF CS_A OR CS_D THEN use the following table:

Optional packages:			
Package name	**PackageID**	**Version**	**Termination types supported**
"MGC Controlled Bearer Level ALG package" [ITU-T H.248.78] (Note 1), (Note 2)	mcbalg (0x0108)	v2	IP
"Data channel establishment protocol support package" [this Recommendation] (Note 1)	dcep (0x0124)	v1	IP
NOTE 1 – There are two options related to the end-to-end control of WebRTC data channels: 1) "out-of-band" method using call control signalling, or 2) "in-band" method. The first approach seems to be default for WebRTC support in SIP networks (such as IMS), and the baseline in this Recommendation. ITU-T H.248 WebRTC gateways which would need to support the second method would require an ITU-T H.248 profile with *dcep* v1 and *mcbalg* v2 packages support. NOTE 2 – In case of CLUE-based WebRTC conferencing control.			

Examples:

IF CS_A THEN use the following table:

Optional packages:			
Package name	**PackageID**	**Version**	**Termination types supported**
"Address Reporting Package" [ITU-T H.248.37]	adr (0x00ac)	v1	IP
"Statistics for discarded packets due to latching package" [ITU-T H.248.37]	lstat (0x00e4)	v1	IP
"Advanced SDP Wildcarding Package" [ITU-T H.248.39] (Note 1)	aswp (0x011c)	v1	IP
"TLS traffic volume metrics package" [ITU-T H.248.90] (Note 2)	tlstv (0x011a)	v1	IP
NOTE 1 – When MGC and MG agree to benefit from advanced SDP wildcarding. NOTE 2 – Related to DTLS layer.			

11.14.3 Package usage information

The following is a non-exhaustive list of package usage indications.

11.14.3.1 IP NAPT traversal package

Example:

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provision-ed value:**	**Termination/ Stream types supported:**
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
Latching (ipnapt/latch, 0x0099/0x0001)	M	ADD, MOD		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	napt (0x0001)	**M**	ALL	–	
Events	**Mandatory/ Optional**	**Used in command:**			
None.	–	–			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

11.14.3.2 MG act-as STUN server package

Example:

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**	**Termination/ Stream types supported:**
Act-as STUN Server (mga-stuns/astuns, 0x00c2/0x0001)	M	ADD, MOD	ALL	–	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
None.	–	–		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Events	**Mandatory/ Optional**	**Used in command:**			
None.	–	–			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

11.14.3.3 Originate STUN continuity check package

Example:

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**	**Termination/ Stream types supported:**
Host Candidate Realm (ostuncc/hcr, 0x00c3/0x0001)	O	ADD, MOD	ALL	Yes	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
Send Connectivity Check (ostuncc/scc, 0x00c3/0x0001)	M	ADD. MOD		not applicable	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	cntrl (0x0001)	O	controlling, controlled	not applicable	
Send Additional Connectivity Check (ostuncc/sacc, 0x00c3/0x0002)	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
	M	MOD		not applicable	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	cntrl (0x0001)	O	controlling, controlled	not applicable	
Events	**Mandatory/ Optional**	**Used in command:**			
Connectivity Check Result (ostuncc/ccr, 0x00c3/0x0001)	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	ctp (0x0001)	M	ALL	not applicable	
New Peer Reflexive Candidate (ostuncc/nprc, 0x00c3/0x0002)	**Mandatory/ Optional**	**Used in command:**			
	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	can (0x0001)	M	ALL	not applicable	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

11.14.3.4 STUN consent freshness package

Example:

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**	**Termination/ Stream types supported:**
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
Consent Test (stnconfres/const, 0x0120/0x0001)	M	ADD. MOD		not applicable	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	tstint (0x0001)	O	ALL	'5000 ms'	
Events	**Mandatory/ Optional**	**Used in command:**			
Consent State (stnconfres/constate, 0x0120/0x0001)	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	reqstate (0x0001)	O	ALL	'B'	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	state (0x0001)	M	ALL	not applicable	
STUN Consent Request Failure (stnconfres/confail, 0x0120/0x0002)	**Mandatory/ Optional**	**Used in command:**			
	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

11.14.3.5 TLS basic session control package

Example:

<table>
<tr><th>Properties</th><th>Mandatory/ Optional</th><th>Used in command:</th><th>Supported values:</th><th>Provisioned value:</th><th>Termination/ Stream types supported:</th></tr>
<tr><td>Incoming security session establishment blocking (tlsbsc/bceb, 0x0117/0x0001)</td><td>O (Note 1)</td><td>ADD, MOD</td><td>ALL</td><td>"Unblocked "</td><td>DTLS</td></tr>
<tr><th>Signals</th><th>Mandatory/ Optional</th><th colspan="2">Used in command:</th><th colspan="2">Duration provisioned value:</th></tr>
<tr><td rowspan="3">Establish BNC (tlsbsc/EstBNC, 0x0117/0x0001)</td><td>M</td><td colspan="2">ADD. MOD</td><td colspan="2">–</td></tr>
<tr><th>Signal parameters</th><th>Mandatory/ Optional</th><th>Supported values:</th><th colspan="2">Provisioned value:</th></tr>
<tr><td>–</td><td>–</td><td>–</td><td colspan="2">–</td></tr>
<tr><td rowspan="4">Release BNC (tlsbsc/RelBNC, 0x0117/0x0002)</td><th>Mandatory/ Optional</th><th colspan="2">Used in command:</th><th colspan="2">Duration provisioned value:</th></tr>
<tr><td>O (Note 2)</td><td colspan="2">ADD, MOD</td><td colspan="2">–</td></tr>
<tr><th>Signal parameters</th><th>Mandatory/ Optional</th><th>Supported values:</th><th colspan="2">Provisioned value:</th></tr>
<tr><td>–</td><td>–</td><td>–</td><td colspan="2">–</td></tr>
<tr><th>Events</th><th>Mandatory/ Optional</th><th colspan="4">Used in command:</th></tr>
<tr><td rowspan="5">TLS session state change (tlsbsc/BNCChange, 0x0117/0x0001)</td><td>O (Note 3)</td><td colspan="4">ADD, MOD, NOTIFY</td></tr>
<tr><th>Event parameters</th><th>Mandatory/ Optional</th><th>Supported values:</th><th colspan="2">Provisioned value:</th></tr>
<tr><td>Type</td><td>M</td><td>Est (0x01), Rel (0x05)</td><td colspan="2">–</td></tr>
<tr><th>ObservedEvent parameters</th><th>Mandatory/ Optional</th><th>Supported values:</th><th colspan="2">Provisioned value:</th></tr>
<tr><td>Type</td><td>M</td><td>Est (0x01), Rel (0x05)</td><td colspan="2">–</td></tr>
<tr><th>Statistics</th><th>Mandatory/ Optional</th><th>Used in command:</th><th colspan="2">Supported values:</th><th>Termination/ Stream types supported:</th></tr>
<tr><td>None.</td><td>–</td><td>–</td><td colspan="2">–</td><td>–</td></tr>
<tr><th>Error codes</th><th colspan="5">Mandatory/Optional</th></tr>
<tr><td>None.</td><td colspan="5">–</td></tr>
<tr><td colspan="6">NOTE 1 – Required for example, too-early incoming DTLS messages (due to security threat), or delayed DTLS session establishment (due to multiple SDP offer/answer cycles, ITU-T H.248 two-stage resource reservation, to await firstly successful L4 connectivity, etc.).
NOTE 2 – When the MGC wants to explicitly trigger the DTLS bearer session release procedure (instead of the implicit trigger related to the removal of the ITU-T H.248 Stream (via a MODify.request or SUBtract.request command)).
NOTE 3 – When the MGC wants to monitor the execution of DTLS bearer control procedures.</td></tr>
</table>

11.14.3.6 SCTP basic connection control package

Example:

Properties	Mandatory/ Optional	Used in command:	Supported values:	Provisioned value:	Termination/ Stream types supported:
Incoming bearer connection establishment blocking (sctpbcc/bceb, 0x0121/0x0001)	O (Note 1)	ADD, MOD	ALL	"Un-blocked"	SCTP
SCTP StreamID (sctpbcc/sctpid (0x0121/0x0002)	M	ADD, MOD	ALL	None.	SCTP

Signals	Mandatory/ Optional	Used in command:		Duration provisioned value:
Establish BNC (sctpbcc/EstBNC, 0x0121/0x0001)	M	ADD. MOD		–
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	–	–	–	–
Release BNC (sctpbcc/RelBNC, 0x0121/0x0002)	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**
	O (Note 2)	ADD, MOD		–
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	–	–	–	–

Events	Mandatory/ Optional	Used in command:		
SCTP connection state change (sctpbcc/BNCChange, 0x0121/0x0001)	O (Note 3)	ADD, MOD, NOTIFY		
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	Type	M	Est (0x01), Rel (0x05)	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	Type	M	Est (0x01), Rel (0x05)	–

Statistics	Mandatory/ Optional	Used in command:	Supported values:	Termination/ Stream types supported:
None.	–	–	–	–

Error codes	Mandatory/Optional
None.	–

NOTE 1 – Required for blocking incoming SCTP Association establishment requests.

NOTE 2 – When the MGC wants to explicitly trigger the SCTP Association shutdown procedure (instead of the implicit trigger related to the removal of the ITU-T H.248 Stream (via a MODify.request or SUBtract.request command)).

NOTE 3 – When the MGC wants to monitor the execution of SCTP bearer control procedures.

11.14.3.7 SCTP Re-configuration Stream Reset package

Example:

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**	**Termination/ Stream types supported:**
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
Initiate Outgoing SCTP Stream Reset (sctpreset/initreset, 0x0122/0x0001)	M	ADD. MOD		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	sctpid (0x0001)	M	ALL	None.	
Outgoing SCTP Stream Reset Response (sctpreset/resetresp, 0x0122/0x0002)	M	ADD. MOD		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	sctpid (0x0001)	M	ALL	None.	
Events	**Mandatory/ Optional**	**Used in command:**			
Detect outgoing SCTP Stream reset (sctpreset/detreset, 0x0122/0x0001)	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	outresp (0x0001)	O	ALL	"accept"	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	sctpid (0x0001)	M	ALL	None.	
Outgoing SCTP Stream reset result (sctpreset/result, 0x0122/0x0002)	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	None.	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	sctpid (0x0001)	M	ALL	None.	
	result (0x0002)	M	ALL	None.	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

11.14.3.8 Media grouping package

Example:

Properties	Mandatory/ Optional	Used in command:	Supported values:	Provisioned value:	Termination/ Stream types supported:
Group semantics (mgroup/groupse, 0x011f/0x0001)	M	ADD, MOD	'BUNDLE', 'SCTP'	None	ALL (Note 1)
Stream aggregation (mgroup/stragg, 0x011f/0x0002)	M (Note 2)	ADD, MOD	ALL	None	ALL (Note 1)
Stream deaggregation (mgroup/strdeagg, 0x011f/0x0003)	M (Note 3)	ADD, MOD	ALL	None	ALL (Note 1)

Signals	Mandatory/ Optional	Used in command:	Duration provisioned value:
None.	–	–	–

	Signal parameters	Mandatory/ Optional	Supported values:	Provisioned value:
	–	–	–	–

Events	Mandatory/ Optional	Used in command:
None.	–	–

	Event parameters	Mandatory/ Optional	Supported values:	Provisioned value:
	–	–	–	–

	ObservedEvent parameters	Mandatory/ Optional	Supported values:	Provisioned value:
	–	–	–	–

Statistics	Mandatory/ Optional	Used in command:	Supported values:	Termination/ Stream types supported:
None.	–	–	–	–

Error codes	Mandatory/Optional
#489	M

NOTE 1 – Some stream grouping semantic values are only applicable for specific protocols (stacks).
NOTE 2 – Required for RTP media multiplexing ('BUNDLE').
NOTE 3 – Required for WebRTC data channel stack.

11.14.3.9 Data channel establishment protocol support package

Example:

Properties	Mandatory/ Optional	Used in command:	Supported values:	Provisioned value:	Termination/ Stream types supported:
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
Send DCEP Open (dcep/sndopen, 0x0124/0x0001)	M	ADD. MOD		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	sctpid (0x0001)	M	ALL	None.	
	protocol (0x0002)	M	ALL	None.	
	label (0x0003)	O	ALL	None.	
	chtype (0x0004)	M	ALL	None.	
	reli (0x0005)	M	ALL	None.	
	priority (0x0006)	M	ALL	None.	
DCEP Open Response (dcep/ dcopenresp, 0x0124/0x0002)	M	ADD. MOD		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	sctpid (0x0001)	M	ALL	None.	
Events	**Mandatory/ Optional**	**Used in command:**			
Detect DCEP Messages (dcep/detmess, 0x0124/0x0001)	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	None.	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	sctpid (0x0001)	M	ALL	None.	
	protocol (0x0002)	M	ALL	None.	
	label (0x0003)	O	ALL	None.	
	chtype (0x0004)	M	ALL	None.	
	reli (0x0005)	M	ALL	None.	
	priority (0x0006)	M	ALL	None.	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

11.14.3.10 MGC Controlled Bearer Level ALG package

Example:

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**	**Termination/ Stream types supported:**
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
Send bearer level message (mcbalg/sblm, 0x0108/0x0001)	M	ADD. MOD		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	Message content (mc)	M	ALL	–	
	Sent application protocol (sap)	O	ALL	–	
	Label (lbl)	O	ALL	–	
Events	**Mandatory/ Optional**	**Used in command:**			
Detect bearer level message (mcbalg/det, 0x0108/0x0001)	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	Protocol Filter (pf)	M	ALL (Note)	–	
	Message Filter (mf)	O	ALL	"*"	
	Forwarding Flag (ff)	O	ALL	FALSE	
	Enhanced Protocol Filter (ehpf)	O	–	–	
	Label (lbl)	O	ALL	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	Message content (mc)	M	ALL	–	
	Detected protocol (dtp)	O	ALL	–	
	Label (lbl)	O	ALL	–	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				
NOTE – At least codepoint '2855' (MSRP) is in scope of Release 1 of this Recommendation.					

11.14.3.11 Stream endpoint interlinkage package

Example:

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**	**Termination/ Stream types supported:**
Interlinkage topology (sep-link/linktopo, 0x011b/0x0001)	M	ADD, MOD	ALL	_	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
None.	–	–		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Events	**Mandatory/ Optional**	**Used in command:**			
None.	–	–			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
#488	–				

11.14.3.12 MG located bearer level ALG package

Example:

Properties	Mandatory/ Optional	Used in command:	Supported values:	Provisioned value:	Termination/ Stream types supported:
Protocol type bearer level ALG (mgbalg/ptbalg, 0x011d/0x0001)	M	ADD, MOD	ALL	_"OFF"	–
Upper layer protocol filter (mgbalg/ulpf, 0x011d/0x0002)	O (Note)	ADD, MOD	ALL	WebRTC related codepoints only.	"0"
Upper Layer Enhanced Protocol Filter (mgbalg/ulepf, 0x011d/0x0005)	O (Note)	ADD, MOD	ALL	WebRTC related codepoints only.	–
Source of replaced source address information part (mgbalg/sosaip, 0x011d/0x0003)	O (Note)	ADD, MOD	ALL	"SD"	–
Source of replaced destination address information part (mgbalg/sodaip, 0x011d/0x0004)	O (Note)	ADD, MOD	ALL	"SD"	–

Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**
None.	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	–	–	–	–

Events	**Mandatory/ Optional**	**Used in command:**		
None.	–	–		
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	–	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	–	–	–	–

Statistics	Mandatory/ Optional	Used in command:	Supported values:	Termination/ Stream types supported:
None.	–	–	–	–
Error codes	**Mandatory/Optional**			
None.	–			
NOTE – When B-ALG service configuration is provisioned in ITU-T H.248 MG.				

11.14.3.13 Secure RTP package

Not supported in Release 1 of this Recommendation.

11.14.3.14 Advanced SDP Wildcarding package

Example:

Properties	Mandatory/ Optional	Used in command:	Supported values:	Provisioned value:	Termination/ Stream types supported:
Advanced Wildcarding Support (aswp/aws, 0x011c/0x0001)	M	AuditValue	ALL	–	Root only
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
None.	–	–		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Events	**Mandatory/ Optional**	**Used in command:**			
None.	–	–			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

11.14.3.15 TLS capability negotiation package

Example:

Properties	Mandatory/ Optional	Used in command:	Supported values:	Provisioned value:	Termination/ Stream types supported:
TLS Domain Profile Identifier (tlscn/dpid, 0x0118/0x0001)	O (Note 1)	ADD, MOD, AUDITVALUE	ALL	_	Root or non-Root '(D)TLS', but not both
TLS Versions (tlscn/tlsv, 0x0118/0x0002)	O (Note 1)	ADD, MOD, AUDITVALUE	ALL	_	Root or non-Root '(D)TLS', but not both
Chipher Suites (tlscn/cs, 0x0118/0x0003)	O (Note 1)	ADD, MOD, AUDITVALUE	ALL	_	Root or non-Root '(D)TLS', but not both
Compression Methods (tlscn/cm, 0x0118/0x0004)	O (Note 1)	ADD, MOD, AUDITVALUE	ALL	_	Root or non-Root '(D)TLS', but not both
Support for Renegotiation of the Security Context (tlscn/srsc, 0x0118/0x0005)	O (Note 1)	ADD, MOD, AUDITVALUE	ALL	_	Root or non-Root '(D)TLS', but not both
Renegotiation Period (tlscn/rp, 0x0118/0x0006)	O (Note 1)	ADD, MOD, AUDITVALUE	ALL	_	Root or non-Root '(D)TLS', but not both
Client Authen-tication Requir-ed (tlscn/car, 0x0118/0x0007)	O (Note 1)	ADD, MOD, AUDITVALUE	ALL	_	Root or non-Root '(D)TLS', but not both

Signals	Mandatory/ Optional	Used in command:		Duration provisioned value:
None.	–	–		–
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	–	–	–	–

Events	Mandatory/ Optional	Used in command:		
None.	–	–		
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	–	–	–	–
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**
	–	–	–	–

Statistics	Mandatory/ Optional	Used in command:	Supported values:	Termination/ Stream types supported:
None.	–	–	–	–

Error codes	Mandatory/Optional
None.	–
NOTE 1 – When tagged as 'optional', then property value(s) needs to be provisioned.	

11.14.3.16 TLS session maintenance package

Example:

Properties	Mandatory/ Optional	Used in command:	Supported values:	Provisioned value:	Termination/ Stream types supported:
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
MGC triggered TLS error alert (tlsm/mgcea, 0x0119/0x0001)	M	ADD. MOD		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	al (0x0001)	M	ALL	–	
	ad (0x0002)	M	ALL	–	
Events	**Mandatory/ Optional**	**Used in command:**			
TLS error alert (tlsm/mgea, 0x0119/0x0001)	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	None.	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	blai (0x0001)	M	ALL	–	
	eat (0x0002)	M	ALL	–	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

11.14.3.17 TLS traffic volume metrics package

Example:

<table>
<tr><td>Properties</td><td>Mandatory/ Optional</td><td>Used in command:</td><td>Supported values:</td><td>Provisioned value:</td><td>Termination/ Stream types supported:</td></tr>
<tr><td>None.</td><td>–</td><td>–</td><td>–</td><td>–</td><td>–</td></tr>
<tr><td>Signals</td><td>Mandatory/ Optional</td><td colspan="2">Used in command:</td><td colspan="2">Duration provisioned value:</td></tr>
<tr><td rowspan="3">None.</td><td>–</td><td colspan="2">–</td><td colspan="2">–</td></tr>
<tr><td>Signal parameters</td><td>Mandatory/ Optional</td><td>Supported values:</td><td colspan="2">Provisioned value:</td></tr>
<tr><td>–</td><td>–</td><td>–</td><td colspan="2">–</td></tr>
<tr><td>Events</td><td>Mandatory/ Optional</td><td colspan="4">Used in command:</td></tr>
<tr><td rowspan="5">None.</td><td>–</td><td colspan="4">–</td></tr>
<tr><td>Event parameters</td><td>Mandatory/ Optional</td><td>Supported values:</td><td colspan="2">Provisioned value:</td></tr>
<tr><td>–</td><td>–</td><td>–</td><td colspan="2">–</td></tr>
<tr><td>ObservedEvent parameters</td><td>Mandatory/ Optional</td><td>Supported values:</td><td colspan="2">Provisioned value:</td></tr>
<tr><td>–</td><td>–</td><td>–</td><td colspan="2">–</td></tr>
<tr><td>Statistics</td><td>Mandatory/ Optional</td><td>Used in command:</td><td colspan="2">Supported values:</td><td>Termination/ Stream types supported:</td></tr>
<tr><td>(Note 1)
(tlstv/*, 0x011a/*)</td><td>O</td><td>ADD, MOD, SUBTRACT, NOTIFY</td><td colspan="2">ALL</td><td>(D)TLS enabled</td></tr>
<tr><td>Error codes</td><td colspan="5">Mandatory/Optional</td></tr>
<tr><td>None.</td><td colspan="5">–</td></tr>
<tr><td colspan="6">NOTE 1 – There are 20 statistics available, where usually just a subset is often sufficient. See clause 12.6.1.3 of [ITU-T H.248.90] on "Profile selection guidelines".</td></tr>
</table>

11.14.3.18 Address reporting package

Example:

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**	**Termination/ Stream types supported:**
Current Remote Transport Address Value (adr/crta, 0x00ac/0x0001)	M	ADD, MOD	ALL	None.	IP
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
None.	–	–		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Events	**Mandatory/ Optional**	**Used in command:**			
Remote Transport Address Change (adr/rtac, 0x00ac/0x0003)	M	ADD, MOD, NOTIFY			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	None.	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	nrta (0x0001)	M	ALL	–	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

11.14.3.19 Latch statistics package

Example:

Properties	**Mandatory/ Optional**	**Used in command:**	**Supported values:**	**Provisioned value:**	**Termination/ Stream types supported:**
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command:**		**Duration provisioned value:**	
None.	–	–		–	
	Signal parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Events	**Mandatory/ Optional**	**Used in command:**			
None.	–	–			
	Event parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
	ObservedEvent parameters	**Mandatory/ Optional**	**Supported values:**	**Provisioned value:**	
	–	–	–	–	
Statistics	**Mandatory/ Optional**	**Used in command:**	**Supported values:**		**Termination/ Stream types supported:**
Discarded Packets (lstat/dp, 0x00e4/0x0001)	M	ADD, MOD, SUBTRACT, NOTIFY	ALL		IP
Error codes	**Mandatory/Optional**				
None.	–				

11.15 Mandatory support of SDP and ITU-T H.248.1 Annex C information elements

At least the following:

Supported Annex C and SDP information elements:		
Information Element	**Annex C Support**	**SDP Support**
"m="-line <type>	not supported (in this example)	Value(s): – application-aware: 'audio', 'video and 'application' – application-agnostic: '-'
"m="-line <proto>	not supported (in this example)	Value(s): 'RTP/SAVPF' Purpose: ITU-T H.248 components streams at ITU-T H.248 WebRTC Termination for media types 'audio' and 'video'. Value(s): '-' (if "m="-line inserted in Stream Descriptor) Purpose: ITU-T H.248 components streams at ITU-T H.248 WebRTC Termination for media type 'application'. Value(s): 'DTLS/SCTP' or '…/DTLS/SCTP' Purpose: ITU-T H.248 deaggregation streams at ITU-T H.248 WebRTC Termination for media type 'application'.
"m="-line <fmt>	not supported (in this example)	Value: 'webrtc-datachannel'
"a=fingerprint:"	not supported (in this example)	Value(s): all Purpose: DTLS authentication procedures
" a=sctp-port"		Value(s): all Purpose: The actual SCTP port value of the SCTP Association carried over DTLS/UDP, which is used for "WebRTC data channels"
"a= max-message-size:"		Value(s): all Purpose: The maximum message size (indicated in bytes) that an SCTP Stream endpoint is willing to receive on the SCTP Association, which is used for "WebRTC data channels".
"a=dcmap*:<SCTP StreamID>"*		Value(s): all Purpose: application-agnostic WebRTC data channels
"a=dcmap*:<SCTP StreamID>* subprotocol="…""		Value(s): MSRP (Note) Purpose: application-aware WebRTC data channels
"a=dcsa:…"		Value(s): all Purpose: application-specific information of a particular subprotocol as WebRTC data channel
NOTE – The additional potential values "ITU-T T.140" and "BFCP" are currently under discussion, thus out of scope of this Release.		

All other aspects are subject to profile specification.

11.16 Optional support of SDP and ITU-T H.248.1 Annex C information elements

At least the following:

Supported Annex C and SDP information elements:		
Information Element	**Annex C Support**	**SDP Support**
"a=setup:"	not supported (in this example)	Not applicable for ITU-T H.248 Streams of ITU-T H.248 WebRTC Terminations (Note 1).
"a=rtcp-rsize:"	not supported (in this example)	Value(s): no value Purpose: support of reduced size RTCP (Note 2)
"a=rtcp-fb:"	not supported (in this example)	Value(s): for further studies (Note 3) Purpose: RTCP feedback based services for a specific WebRTC call.
NOTE 1 – Call control signalling level "a=setup:" information is mapped by the MGC on ITU-T H.248 Signal/Event-based bearer control procedures. NOTE 2 – Support of reduced size RTCP is mandatory for WebRTC clients, but has to be negotiated call-individually due to backward compatibility (see section 4.6 of [b-IETF rtp usage]). Thus, the MGC could require every new WebRTC call to use "compound RTCP package" mode only. More detailed ITU-T H.248 profile guidelines are subject of a future release of this Recommendation. NOTE 3 – There are multiple potential RTCP feedback based services for WebRTC, see [b-IETF rtp-usage]. The identification of rtcp-fb codepoints for WebRTC deployments is a subject for a future release of this Recommendation. Furthermore, there might be a split of mandatory and optional RTCP feedback message types in future for WebRTC.		

IF CS_A OR CS_B OR CS_C THEN "following table":

Supported Annex C and SDP information elements:		
Information element	**Annex C support**	**SDP support**
"a=ice-ufrag:"	not supported (in this example)	Value(s): all Purpose:
"a=ice-pwd:"		Value(s): all Purpose:

IF CS_A OR CS_B THEN "following table":

Supported Annex C and SDP information elements:		
Information element	**Annex C support**	**SDP support**
"a=group:BUNDLE"	not supported (in this example)	Value(s): "BUNDLE" Purpose: general media grouping using "bundle" ITU-T H.248 usage: SDP attribute not used, but *value* mapped on [ITU-T H.248.96] property *mgroup/groupse* in order to indicate ITU-T H.248 Stream grouping.
"a=mid:"		Value(s): not used Purpose: general media grouping using "bundle" ITU-T H.248 usage: correspondent SDP media descriptions are mapped on individual ITU-T H.248 component streams, see clause 8.6.2 of [ITU-T H.248.96]
"a=rtcp-mux":		Value(s): all Purpose: for transport multiplexed RTP traffic
"a=rtcp:"		Value(s): all Purpose: optional, if transport unmultiplexed mode for RTP and explicit RTCP transport address allocation
"a=ssrc:"		Value(s): all Purpose: for RTCP supplementary service with source specific information.

All other aspects are subject to profile specification.

11.17 Procedures

The initial release of this Recommendation focuses on the previous profile elements. Specific guidelines for the procedural section are for further studies with exception of following package-independent procedures.

11.17.1 Package-independent NAT-T procedures

11.17.1.1 Support for MG terminated STUN-based connectivity checks

IF CS_A OR CS_B OR CS_C THEN the specific NAT traversal procedures need to be supported.

11.17.2 Example procedures for communication establishment phase

WebRTC as a multimedia communication service is characterized by the fact that individual media components might be dynamically added and removed during the lifetime of the overall WebRTC call. There are consequently many variations of media configurations how a WebRTC call might start and evolve over the timeline. For example, a later added media component might somehow "reuse gateway resources" or start from scratch. Some high-level use cases are outlined.

11.17.2.1 Use case #1: audio and video only, unbundled

It is expected that the majority of WebRTC calls will always use at least audio due to its positioning as "conversational / telephony" service. The likelihood of video might be in the same range or lower. Thus, a WebRTC call would typically start as "audio only" or "audio and video only", – and if "audio only" then video might be added (and removed again) at a later point in time.

Table 10 indicates the main use case #1.0 (as further discussed below) as well as some example variations:

Table 10 – Use case #1 and variations

UC:	Characteristic:	Comments:
#1.0	• audio and video only • unbundled (i.e., no RTP media multiplexing) • no RTP transport multiplexing • media security model: "e2ae" • IWF "audio": transcoding (TC) • IWF "video": transparent forwarding (TF) • NAT-T (AN side): stable connectivity (i.e., no ICE updates) • SRTP key exchange: only once, DTLS connection remains established in order not to lose the security context • DTLS: non-resumable DTLS session	number of L4 connections: • four (2 x RTP and 2 x RTCP) • ICE/STUN procedures: four times, for each L4 connection number of DTLS connections: • four (because non-resumable DTLS sessions) • thus, four DTLS full handshakes, leading to four DTLS connections • enhancement option: a single resumable DTLS session … number of SRTP key exchange procedures: • four (SRTP master key negotiation for each RTP and RTCP stream) • enhancement option: SRTCP keys derived from SRTP keys
#1.1	as #1.0 with following change: • media security model: "e2e"	i.e., SRTP-to-SRTP interworking in a B2BRE topology with two different SRTP key management schemes (ITU-T H.248 Terminations T1: DTLS-SRTP; T2: SDES)
#1.2	as #1.0 with following change: • DTLS connection remains in "data transfer ready state"	
#1.3	as #1.0 with following change: • IWF "audio": also transparent forwarding	

Figure 5 outlines a correspondent ITU-T H.248 Context model for use case category #1 (for the case of a IMS-embedded WebRTC):

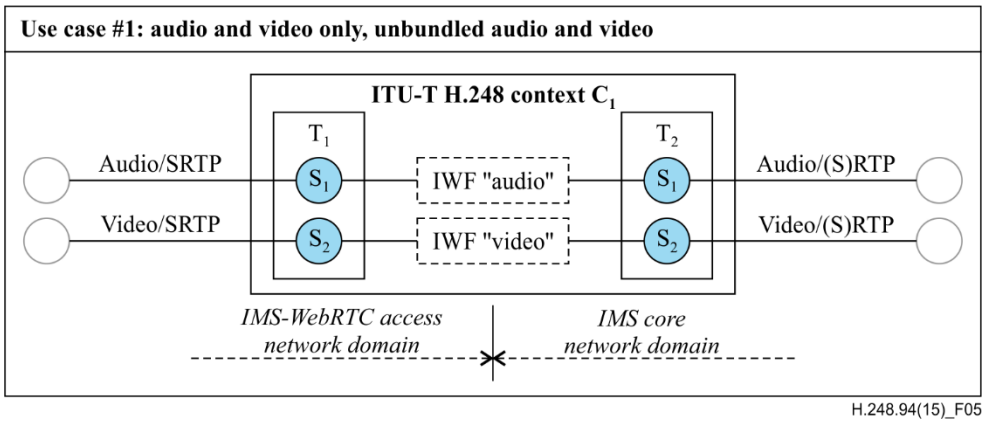


Figure 5 –ITU-T H.248 WebRTC gateway – ITU-T H.248 Context model – Use case #1: audio and video only, unbundled audio and video

ITU-T H.248 Termination T1 is connected with the "WebRTC domain", Termination T2 to the "non-WebRTC domain". There are two ITU-T H.248 Streams for audio and video. Each ITU-T H.248 Stream contains two UDP connections (RTP and RTCP). ICE/STUN procedures need to be executed on each individual UDP connection. After successful STUN connectivity checks, the DTLS connections need to be established for SRTP key exchange.

The worst case (and the assumption here) is the usage of non-resumable DTLS sessions, which lead to the execution of full DTLS handshake procedures on each UDP connection, resulting in finally *four DTLS connections*.

Figure 6 outlines an example signalling flow:

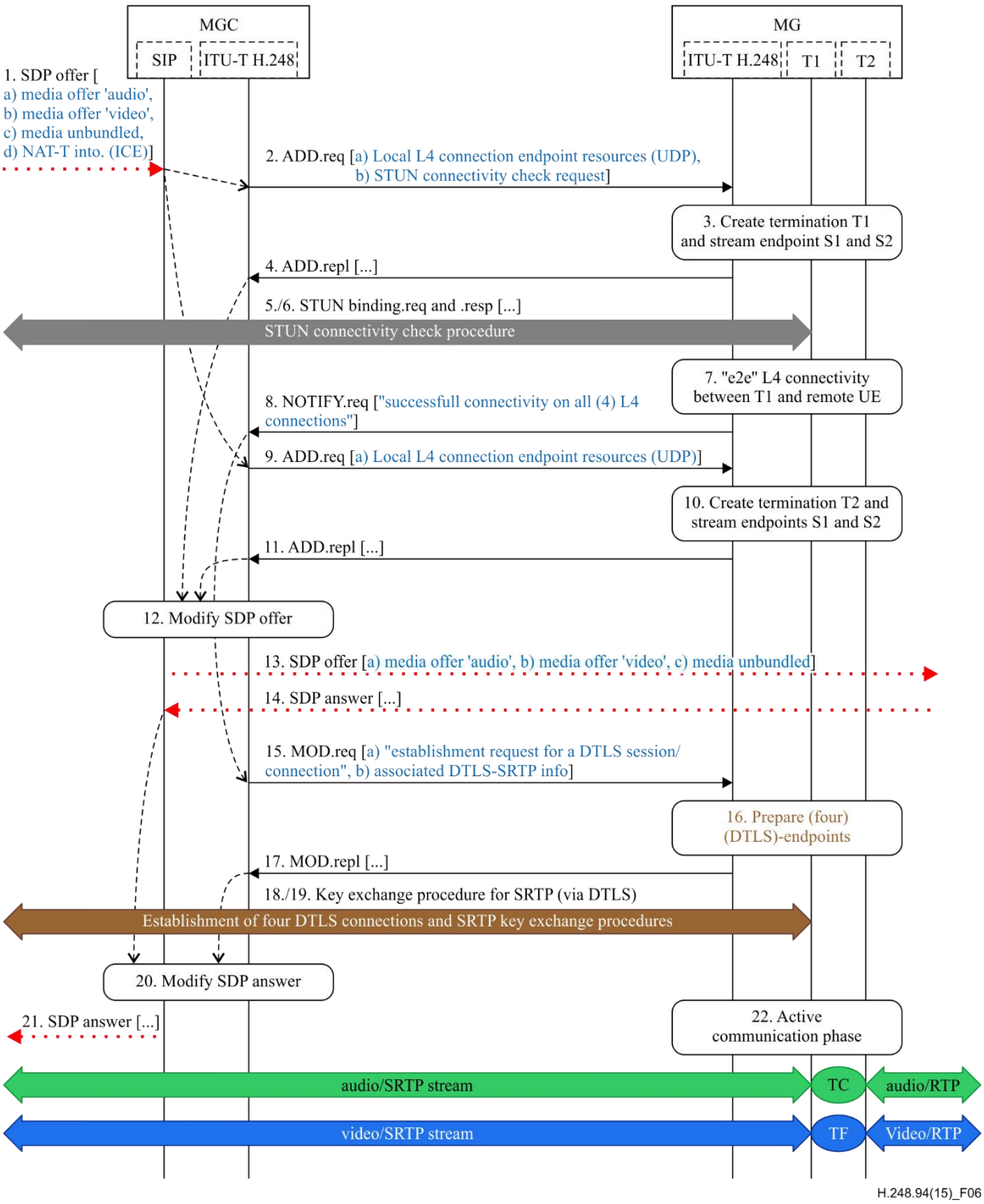


Figure 6 – Example signalling flow for use case #1.0

Observations/discussion of selected signalling steps:

Step:	Comments:
15	The establishment (incoming or outgoing) of the DTLS (non-resumable) session / DTLS connections is here explicitly triggered, dependent on successfully reported L4 connectivity on all four UDP connections between UE and MG. Thus, alternatively step 15 might be merged into step 2.

11.17.2.2 Use case #2: audio and video only, bundled

Additional bundling requires support of ITU-T H.248 Stream grouping based Context models. Table 11 indicates the main use case #2.0 as well as some example variations:

Table 11 – Use case #2 and variations

UC:	Characteristic:	Comments:
#2.0	as #1.0 with following changes: • bundled (i.e., RTP media multiplexing, also known as RTP SSRC multiplexing) • also RTP transport multiplexing	number of L4 connections: • one (both RTP media flows and associated RTCP control flows multiplexed on a single UDP connection) • ICE/STUN procedures: once number of DTLS connections: • one number of SRTP key exchange procedures: • one (SRTP master key negotiation and then key derivation for all RTP media and RTCP control flows)
#2.1	as #2.0 with following change: • media security model: "e2e"	

Figure 7 shows two options of a correspondent ITU-T H.248 Context model for use case category #2:

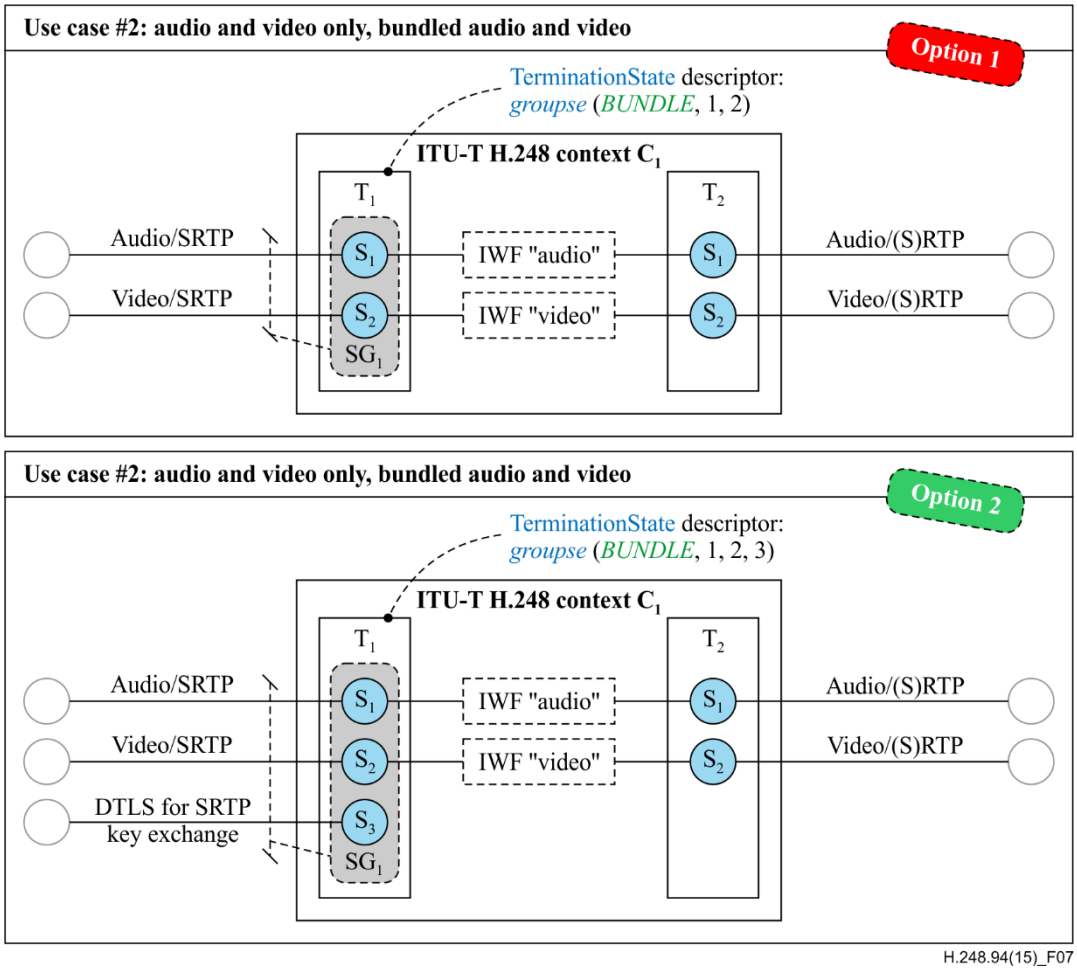


Figure 7 – ITU-T H.248 WebRTC gateway – ITU-T H.248 Context model – Use case #2: audio and video only, bundled audio and video

Bundling implies the usage of ITU-T H.248 Stream grouping with [ITU-T H.248.96] semantic "BUNDLE" (which indicates to the MG that multiple ITU-T H.248 *Streams* share common resources). There are two ITU-T H.248 Streams in case of option 1. The ITU-T H.248 Stream Descriptor of each Stream describes the RTP media and RTCP control flow components for a particular media type. However, there is only a single UDP connection, thus only single ICE/STUN procedures and a single DTLS session as well, inclusive of a single DTLS connection and only a single SRTP key exchange procedure, which are shared by audio and video. This leads to the question of whether ICE, STUN, DTLS and SRTP-related information should be associated to ITU-T H.248 Stream T1(S1) or T1(S2) (in case of option 1). Option 1 is basically feasible; an ITU-T H.248 profile specification should indicate a rule where the DTLS and lower-layer procedures would be signalled via ITU-T H.248, for example, using the ITU-T H.248 Stream with the lowest StreamID value.

That issue could also be addressed by a dedicated ITU-T H.248 Stream T1(S3), see option 2. The [ITU-T H.248.96] "BUNDLE" stream group would then cover all three ITU-T H.248 Streams due to the common usage of the same and single UDP connection.

Observations/discussion of selected signalling steps, – versus use case #1.0 (Figure 6):

Step	Comments
2, 3	ITU-T H.248 stream group SG1 is created, containing three streams.
13	SDP offer with "media bundled" forwarded
18	Start of DTLS procedures at Stream endpoint T1(S3)
22	Active communication phase: • audio IWF in transcoding mode • video IWF in transparent forwarding mode; This semantic implies that the media format for video is not changed (despite the other SRTP-to-RTP interworking functions)

11.17.2.3 Use case #3: additional data component(s), preparation of transport

The description of a protocol stack for WebRTC data and associated ITU-T H.248 Stream/Termination models requires the usage of the ITU-T H.248 media grouping (*mgroup*) package.

The initial SDP Offer could contain a media description for WebRTC data ,but still miss information elements for a concrete WebRTC data application (i.e., the SDP attributes "a=dcmap" and "a=dcsa" are omitted in the SDP Offer). This is a valid scenario because the WebRTC user may want to start with audio only or audio/video telephony first before a potential, later addition of a data service.

Independent of the SIP-level signalling for the establishment of a WebRTC call, the MGC could prepare the ITU-T H.248 Context for a later usage of additional WebRTC data. The level of preparation of correspondent MG resources is usually dependent on MGC local policies (e.g., traffic distribution between WebRTC calls with and without data, expected WebRTC data application(s), expected NAT traversal support at application protocol level) as well as the amount of SDP information signalled in call control signalling.

Table 12 indicates the main use case #3.0 as well as some example variations:

Table 12 – Use case #3 and variations

UC:	Characteristic:	Comments:
#3.0	• SIP: SDP offer indicates "…/DTLS/SCTP" transport, but still missing SDP attributes for a WebRTC data application • L4 protocol: UDP, expected successful NAT traversal • single SCTP Association per DTLS connection (default for WebRTC) • preparation of three ITU-T H.248 Streams for potential future WebRTC data applications in the ITU-T H.248 WebRTC gateway; the preparation includes already the local reservation and assignment of SCTP StreamIDs for each DC candidate	• the preparation and establishment of a **DTLS session/DTLS connection** for SCTP traffic is already feasible • the preparation and establishment of an **SCTP Association** after successful DTLS connectivity is also feasible • however, the preparation of **local DC resource**s is conditional, dependent on **pro-active** or **on-demand** resource management strategies of MGW resources • the pro-active strategy is selected for this use case due to expected later WebRTC data applications
#3.1	as #3.0 with following change: • no preparation of WebRTC data channels	• thus, only the ITU-T H.248 deaggregation stream will be established, but no ITU-T H.248 component streams for DCs are be created

The purpose of the consideration of the two use cases #3.0 and #3.1 is to emphasize the feedback on the ITU-T H.248 handling of Stream group SG2: the size is fixed and static in #3.0, but dynamic in #3.1 (NOTE – 'dynamic' implies future ITU-T H.248 modifications of the TerminationState property *mgroup/groupse* of T1).

Figure 8 illustrates a correspondent ITU-T H.248 Context model for use case category #3.0:

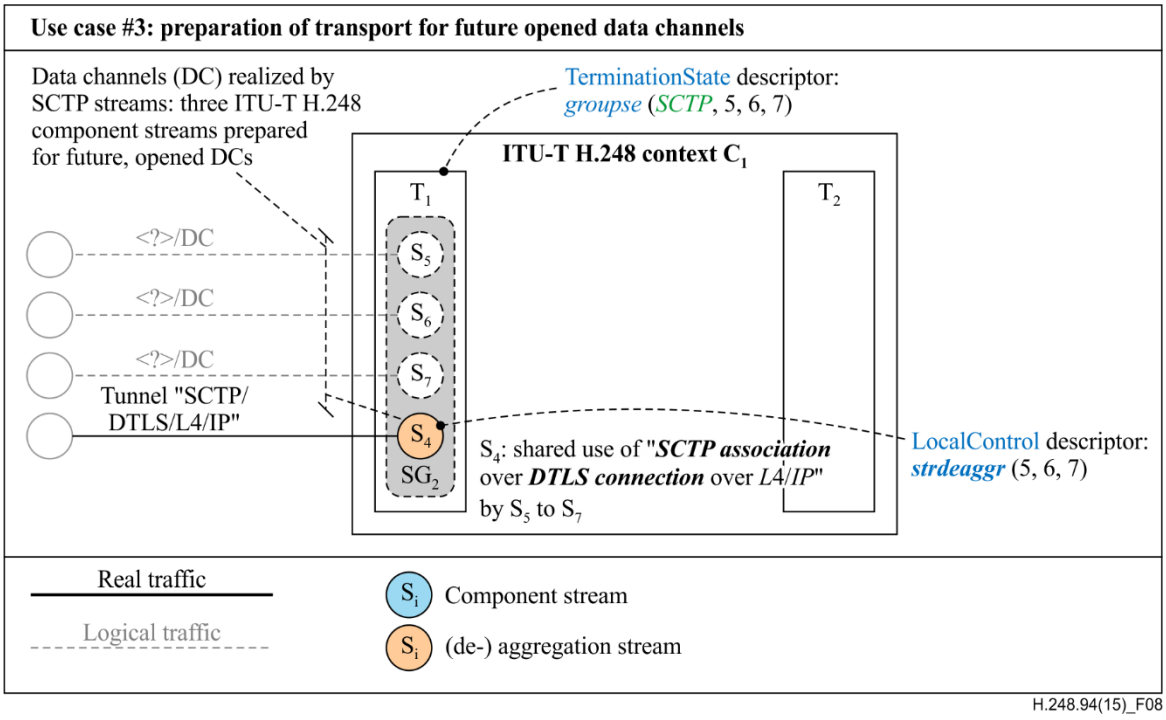


Figure 8 – ITU-T H.248 WebRTC gateway – ITU-T H.248 Context model – Use case #3.0: additional data, preparation of transport

The ITU-T H.248 Stream endpoint T1(S4) represents the ITU-T H.248 deaggregation stream. The protocol stack segment "SCTP Association over DTLS connection over L4 over IP" is allocated to this SEP. The three potential future WebRTC data channels would be provided by the three ITU-T H.248 component streams: S5, S6 and S7 at Termination T1. There are no SEP counterparts at T2 (in this example). The four ITU-T H.248 Streams for WebRTC data are denoted as Stream group SG2 in Figure 6. The name SG2 is only used for illustration purposes; it does not appear in any ITU-T H.248 signalling syntax.

Figure 9 outlines an example signalling flow:

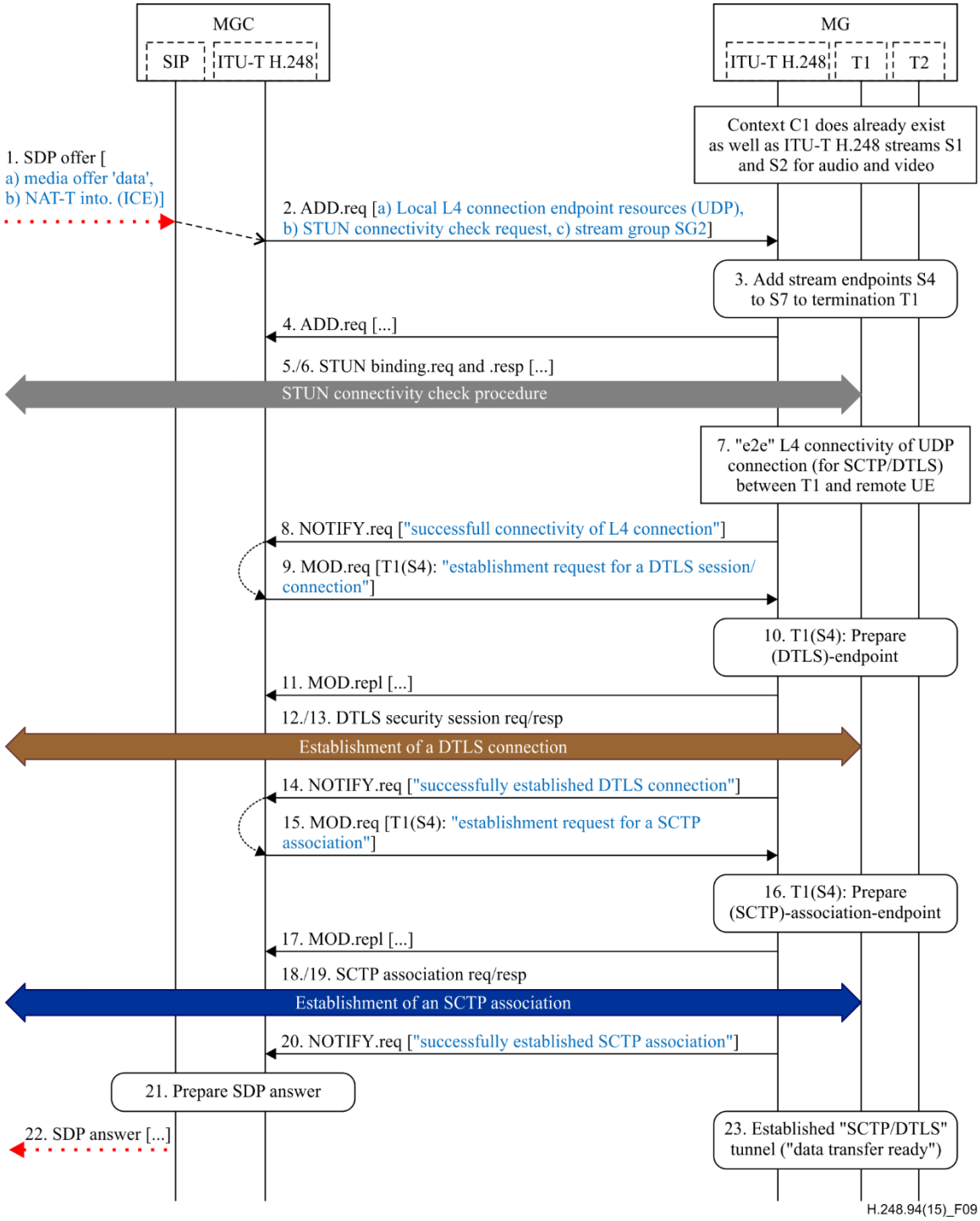


Figure 9 – Example signalling flow for use case #3.0

Observations/discussion of selected signalling steps:

Step:	Comments:
0	Context C1 and Termination T1 already exists as a result of the previous establishment of audio/SRTP and video/SRTP streams. There are three major types concerning the start of a WebRTC call: O1) audio and video only, without any data indication at all; O2) audio and video, plus indication of data but not yet any specific data application; and O3) audio, video and data. The example in Figure 9 provides a scenario from category "initial audio and video only without any initial data indication at all" (due to the history of Context C1). However, the option "of an initial, additional indication of an application-agnostic data indication" seems to be more likely from WebRTC client perspective, hence that option should be considered from profile specification perspective rather than the first scenario. It has to be noted that the third option of a WebRTC call starting already with "audio, video plus data" is applicable in general,.
2	NOTE – The concrete ITU-T H.248 command type depends on the signalling history (e.g., a MOD.req instead of an ADD.req). However, that level of detail is out of scope of this Recommendation. Signalled information: protocol stack segment indication, ICE/STUN info (as well as explicit notification about successful STUN connectivity check), stream group SG2. With regard to ITU-T H.248 Stream group SG2: • ITU-T H.248 *deaggregation stream* T1(S4) could be already fully specified (apart from the usual ITU-T H.248 wildcarding of local MG resources); • the three ITU-T H.248 *component streams* T1(S5, S6, S7) would be prepared by signalling at least the binding information between ITU-T H.248 StreamID and SCTP StreamID (i.e., [ITU-T H.248.97] property *sctpbcc/sctpid* in the LocalControl Descriptor of each component stream; SCTP StreamID value might be wildcarded or explicitly provided by MGC).
8	The MGC is notified upon successful L4 connectivity (here: one UDP connection for SCTP-over-DTLS because the UDP connection is NOT shared with audio and video in this use case). NOTE – Step 8 dependent on 9, see next row.
9	The establishment of the DTLS session/connection is here explicitly triggered (using the [ITU-T H.248.90] *tlsbsc* package) by the MGC. That request could be of course already be combined with step 2. The DTLS protocol profile (actually the concept of the "TLS domain profile", see [ITU-T H.248.90], as applied to the DTLS protocol) is out of scope here, i.e., expected to be pre-provisioned in the MG. For instance, a non-resumable DTLS session, etc.
12, 13	The establishment direction of the DTLS connection is out of scope here.
14	The MGC is notified of the successful establishment of the DTLS connection (i.e., the local *(DTLS)-connection-endpoint* is in state "ESTABLISHED").
15	Here, the establishment of the SCTP Association is explicitly triggered (using the [ITU-T H.248.97] *sctpbcc* package) by the MGC. This request could already be combined with step 9, or the usage of [ITU-T H.248.92] stream endpoint interlinkage might be applied.
18, 19	The establishment direction of the SCTP Association is out of scope here.
20	The MGC is notified about the successful establishment of the SCTP Association (i.e., the local *(SCTP)-association-endpoint* is in state "ESTABLISHED").

11.17.2.4 Use case #4: dynamic establishment of data channels

There is already an existing end-to-end WebRTC communication with audio and video and a prepared "tunnel" (realized as SCTP Association over a DTLS connection) for data. A WebRTC endpoint or

WebRTC-compatible endpoint wants to add a first data application, for instance MSRP-based instant messaging.

Table 13 indicates the main use case #4.0 as well as some example variations:

Table 13 – Use case #4 and variations

UC:	Characteristic:	Comments:
#4.0	• SIP reINVITE: SDP offer provides a media description containing at least, e.g.: m=application <…> UDP/DTLS/SCTP webrtc-datachannel a=dcmap:1 label="…"; subprotocol="MSRP" … • ITU-T H.248 component stream S5 (of SG2) is used for MSRP traffic	this use case highlights the following aspects: • data channel "open": no usage of the DCEP (Data Channel Establishment Protocol) due to the alternative of complete out-of-band DC signalling; • a (WebRTC)-DC-endpoint could immediately send data, which implies the allocation of buffer resources in the MG; • ITU-T H.248 WebRTC gateway interworking function: "MSRP transparent forwarding" or with a B-ALG function in case of L4+ NAT-T support.
#4.1	as #4.0 with following change: • #3.1 as the starting point (i.e., there wasn't yet any preparation of the "tunnel" in the user plane, thus no ITU-T H.248 Stream group SG2 …)	
#4.2	as #4.0 with following change: • immediate establishment of three (instead of just one) WebRTC data channels	

Figure 10 shows an example ITU-T H.248 Context model for use case #4.0:

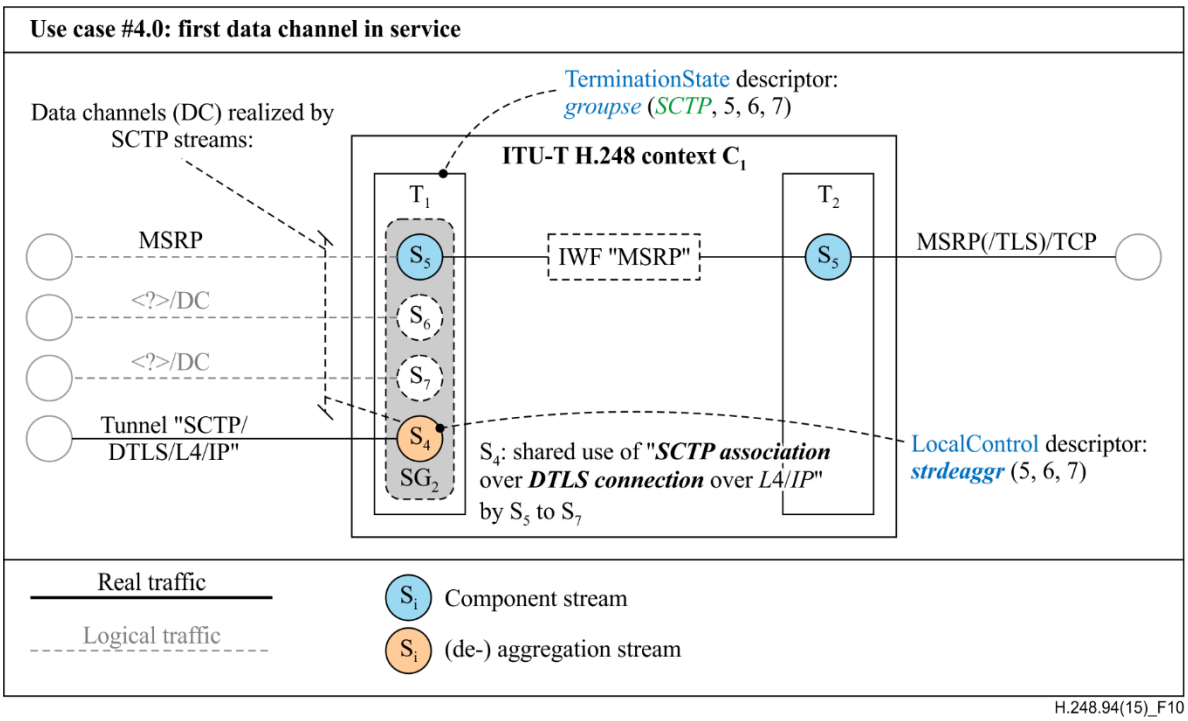


Figure 10 – ITU-T H.248 WebRTC gateway – ITU-T H.248 Context model – Use case #4.0: first data channel in service

ITU-T H.248 Stream endpoint T1(S5) represents the ITU-T H.248 component stream for "MSRP" in the WebRTC domain. Figure 11 outlines an example signalling flow:

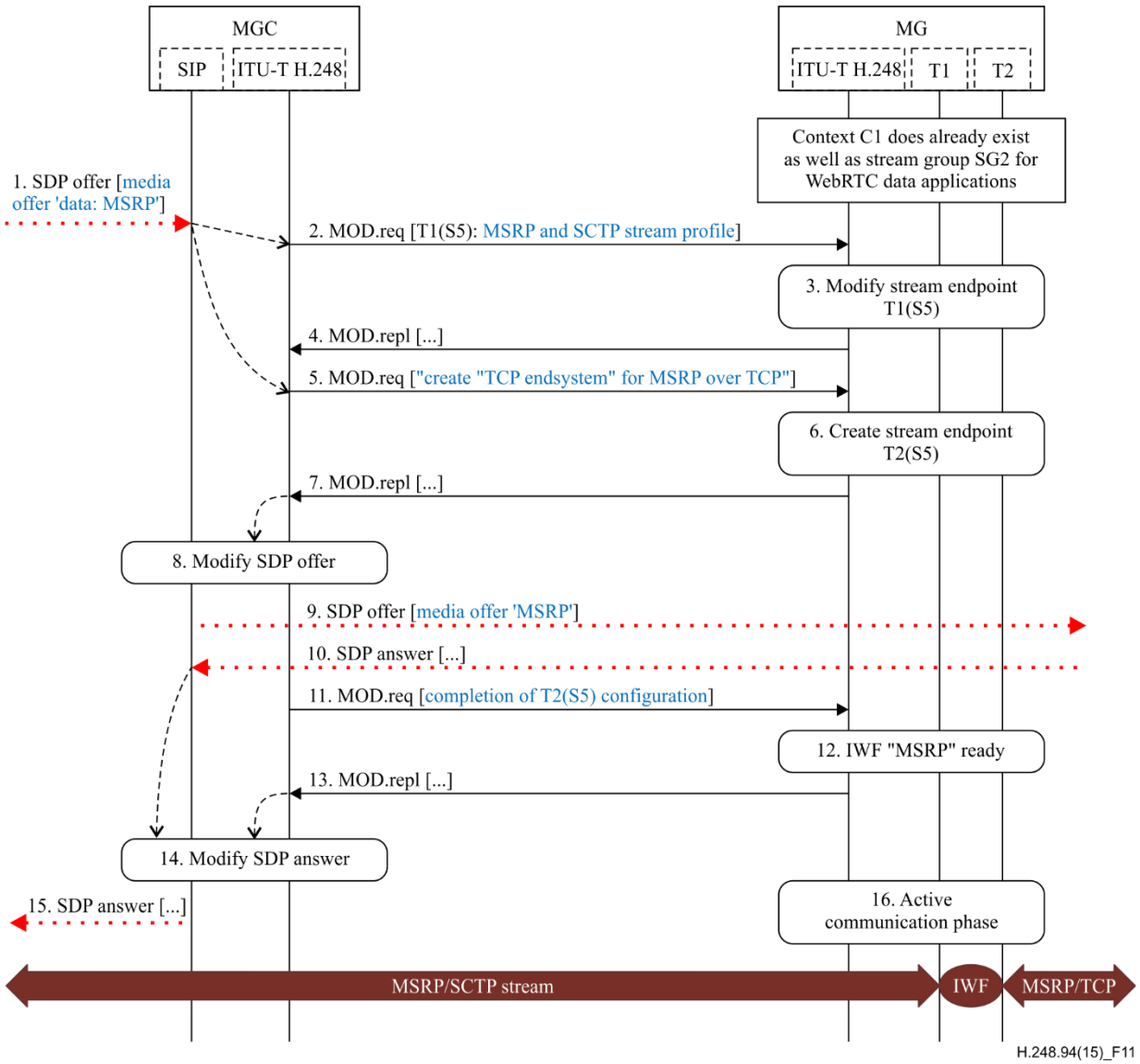


Figure 11 – Example signalling flow for use case #4.0

Observations/discussion of selected signalling steps:

Step:	Comments:
0	Context C1 and Termination T1 already exist due to the previous establishment of audio/SRTP and video/SRTP streams as well as Stream group SG2 for WebRTC data applications. ("same comment as in use case #3.0")
1	The SIP reINVITE / SDP offer provides a media description containing at least, e.g.: m=**application** <…> UDP/DTLS/SCTP **webrtc-datachannel** a=**dcmap**:1 label="…"; subprotocol="**MSRP**"
2	ITU-T H.248 Stream endpoint T1(S5): the associated SCTP Stream is configured. NOTE – Any originally allocated local SCTP StreamID value might be overwritten or renewed ("in case of wildcarding").
5, 11	ITU-T H.248 Stream endpoint T2(S5): the (MSRP(/TLS)/TCP)-connection-endpoint is configured

Figure 12 illustrates the ITU-T H.248 Context model in case of three established and active ITU-T H.248 component streams for WebRTC data services (NOTE – DC application ITU-T T.140 and BFCP are subject of a future Release of this Recommendation):

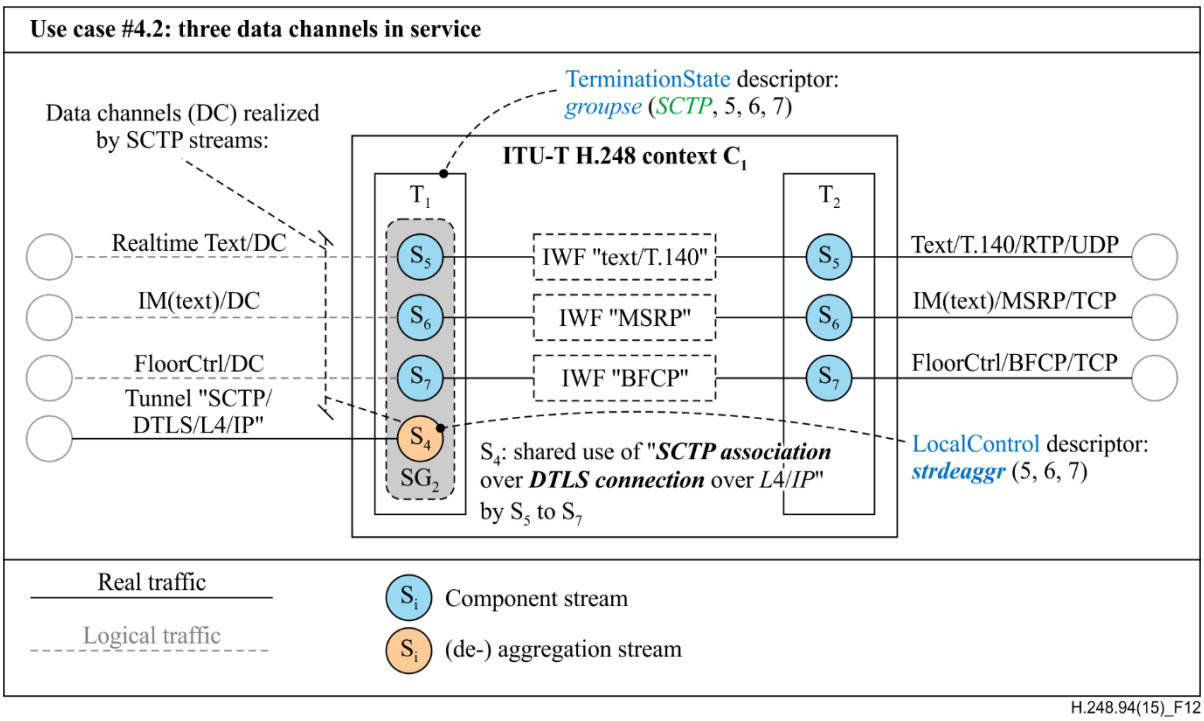


Figure 12 – ITU-T H.248 WebRTC gateway – ITU-T H.248 Context model – Use case #4.2: three data channels in service

A correspondent signalling example for use case #4.2 is not discussed further.

11.17.2.5 Use case #5: data IWF and B-ALG for MSRP

MSRP-based instant messaging allows also to demonstrate: a) the additional usage of an (optional) B-ALG (see [ITU-T H.248.78]) function for L4+ NAT traversal support (due to address information at MSRP message level) and b) TCP-related interworking. Concrete use cases are not detailed in this Release of the Recommendation.

11.17.2.6 Use case #6: MG enhancement – additional usage of stream interlinkage

[ITU-T H.248.92] is applicable in principle whenever a protocol uses explicit bearer control procedures. This is basically the case for ITU-T H.248 WebRTC gateway interworking functions, given by *connection-oriented* protocols DTLS, SCTP (and possibly DCEP) and TCP (if used as L4 protocol) at an "ITU-T H.248 WebRTC Termination", and TCP and TLS at the "ITU-T H.248 non-WebRTC Termination". Concrete use cases with stream interlinkage are not detailed in this Release of the Recommendation.

11.17.3 Example procedures for release of data channels and call release

There are multiple levels of release procedures due to the hierarchical protocol stack as well as the nature of the communication service (see initial comments in clause 11.17.3.1). Only a few examples are discussed in this Recommendation (clauses 11.17.3.2 to 11.17.3.4).

11.17.3.1 Service cancellation for WebRTC data in ITU-T H.248 WebRTC MGs

The hierarchical protocol stack for WebRTC data ("DC/SCTP/DTLS/(UDP|TCP)/IP") contains up to four levels of user plane bearer control procedures, from top to bottom:

1) DC: SCTP Stream reconfiguration procedures for resetting SCTP Streams;
2) SCTP Association: shutdown procedure;
3) DTLS: DTLS connection release procedure (apart from resumption and renegotiation procedures); and

4) TCP (if not UDP): TCP connection release procedure.

There are two options of service cancellation, attributed as "forced" and "graceful".

11.17.3.1.1 Forced service cancellation for WebRTC data in ITU-T H.248 WebRTC MGs

A situation where the MGC removes an ITU-T H.248 SEP for a particular protocol layer or protocol stack segment, an ITU-T H.248 Stream group or even the complete subtraction of the Termination from the Context, without execution (by the MG) at all of the protocol specific bearer control procedures for releasing protocol endpoints. Such a forced service cancellation represents an incorrect service Termination in the user plane because this will cause protocol failure indications at the remote endpoint.

11.17.3.1.2 Graceful service cancellation for WebRTC data in ITU-T H.248 WebRTC MGs

This is the normal behaviour of the MG as a communication endpoint by executing bearer release procedures (by the MG) protocol correctly and in the right order. Some examples follow:

- the ITU-T H.248 command request for releasing the DTLS connection (despite the fact of a still established SCTP Association and still open DCs) should first lead to the execution of an SCTP Association shutdown procedure before starting the DTLS connection release procedure;
- the ITU-T H.248 command request for releasing the SCTP Association (despite the fact of still open data channels) might benefit from first resetting all SCTP Streams before starting the SCTP Association shutdown;
- the ITU-T H.248 command request for subtracting the ITU-T H.248 WebRTC Termination (despite the fact of still open data channels).

11.17.3.2 Use case #7: release of a data channel without call release

Data channels might be removed before the overall end of the WebRTC call. There are multiple variations possible because the "CLOSURE of a data channel" results in a *reset* of the SCTP Stream (see section 6.7 of [b-IETF webRTCDC], i.e., the concerned SCTP Stream still exists. Such a reset SCTP Stream could be *reused* again (for the same or another WebRTC data application). There are consequently two options from the MGC perspective: the correspondent ITU-T H.248 Stream endpoint is still kept, i.e., remains allocated and part of the ITU-T H.248 Stream group, or the ITU-T H.248 Stream endpoint is completely removed from the Termination.

Table 14 indicates the main use case #7.0 as well as some example variations:

Table 14 – Use case #7 and variations

UC:	Characteristic:	Comments:
#7.0	• existing ITU-T H.248 Stream group with three active data channels (i.e., three ITU-T H.248 component streams) (see Figure 13, "Phase 0") • closing of 1-out-of-3 data channels • underlying SCTP Stream is kept after the SCTP Stream reset procedure ("Phase 1") • later, the MGC decides to remove also the unused SCTP Stream ("Phase 2")	• the level of detail concerning the directionality of the DC closure procedure is not considered here • MGC removes SEP at the non-WebRTC Termination T2, but keeps SEP at WebRTC Termination T1 (of the original ITU-T H.248 SEP)
#7.1	as #7.0 with following change: • resetted SCTP is not intended to be reused, thus, the MGC removes ITU-T H.248 SEP	• there are two options again: the ITU-T H.248 Stream group SG2 is either not modified or is updated according the actual Stream group size

Table 14 – Use case #7 and variations

UC:	Characteristic:	Comments:
#7.2	as #7.0 with following change: • closing of 2-out-of-3, or 3-out-of-3 data channels	• the [IETF RFC 6525] SCTP Stream re-configuration procedure allows the reset of multiple streams in parallel … • … hence, that "SCTP bearer control procedure" is actually running at the ITU-T H.248 deaggregation stream T1(S4) and not at the affected ITU-T H.248 component streams
#7.3	• release of all data channels and subsequent shutdown of the SCTP Association	• there are two options again: either the underlying DTLS connection is also immediately released or in future

Figure 13 illustrates a correspondent ITU-T H.248 Context model for use case #7.0 (using ITU-T H.248 Stream S_6 as example), highlighting the three phases of Context modification:

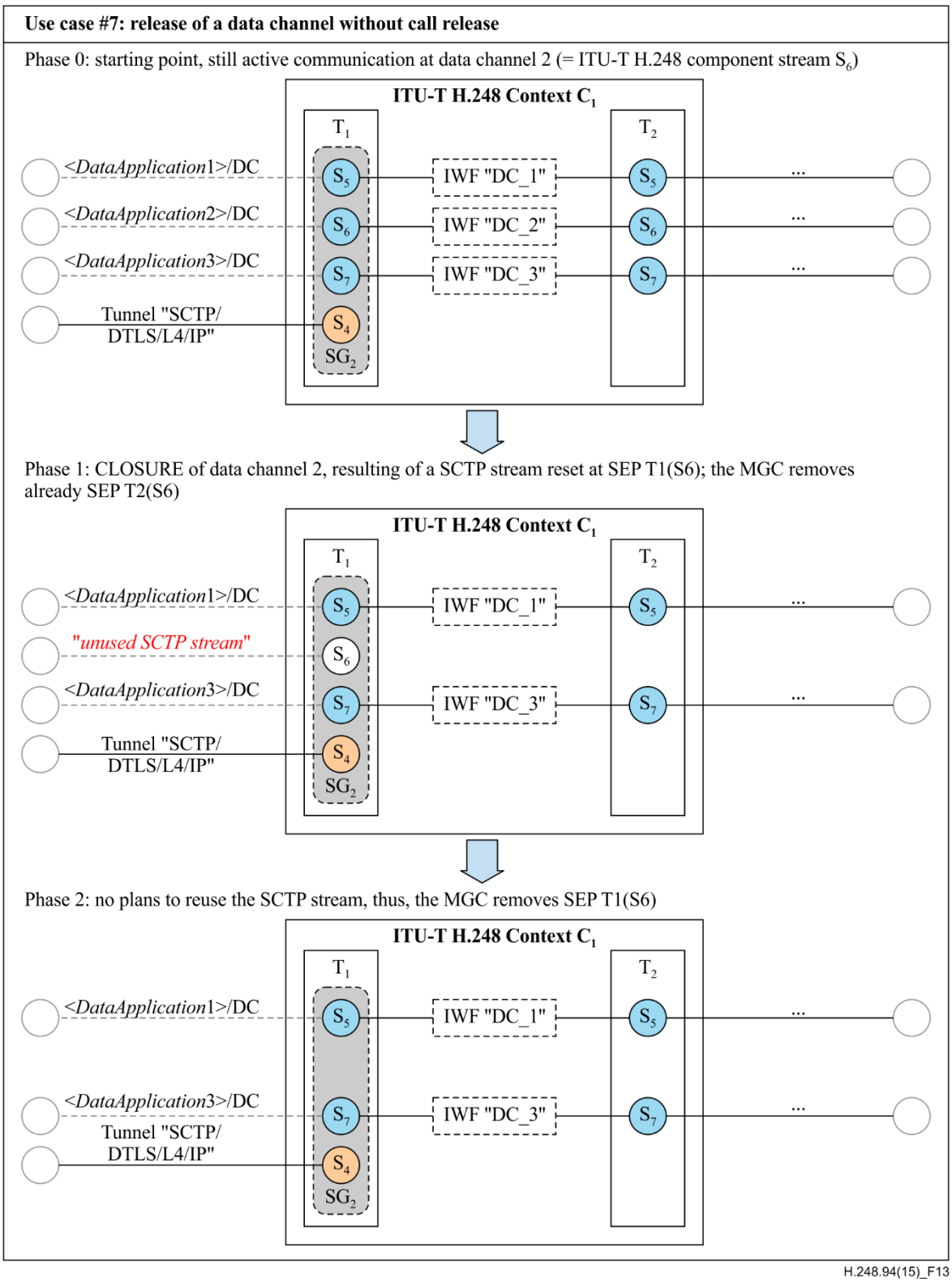


Figure 13 – ITU-T H.248 WebRTC gateway – ITU-T H.248 Context model – Use case #7.0: release of a data channel without call release

Figure 14 outlines an example signalling flow:

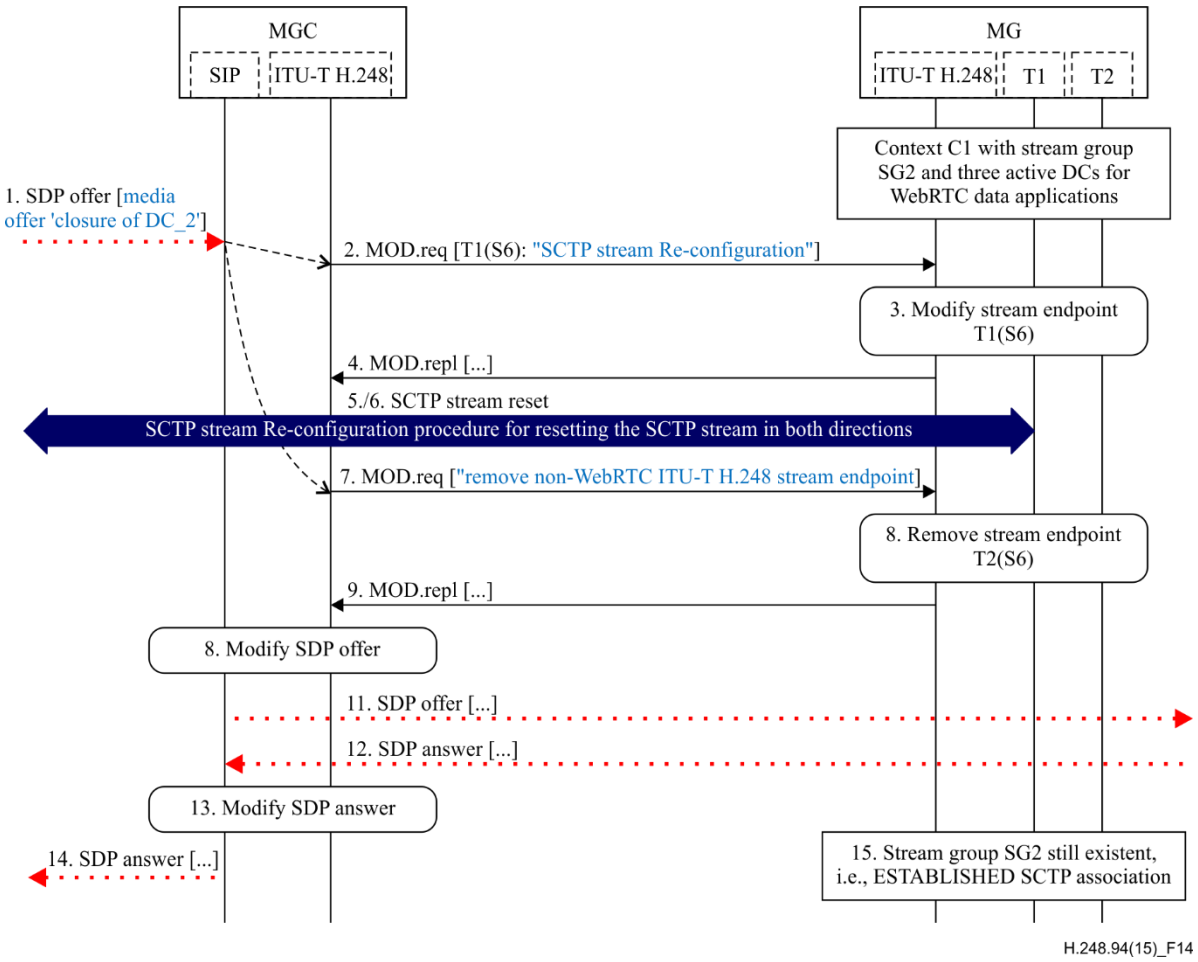


Figure 14 – Example signalling flow for use case #7.0

Observations/discussion of selected signalling steps:

Step:	Comments:
1	the SDP ffer does not contain the SDP attributes of the original data channel and data application
2	the MGC maps the SDP on the [ITU-T H.248.97] *sctpreset* package elements, dependent on an incoming or outgoing SCTP Stream reconfiguration procedure
15	ITU-T H.248 Stream group SG2 is not modified as such, i.e., SEP T1(S6) is still part of the group and allocated SCTP StreamID values (for potential future "reuse")

11.17.3.3 Use case #8: SCTP Association shutdown without DTLS connection release

There might be two reasons for keeping the DTLS connection after a shutdown of the SCTP Association: either the DTLS connection is still used for DTLS-SRTP or there might be WebRTC DCs opened at a future point in time. Such an approach is possible; however, the establishment of a new DTLS connection represents a significant cost factor in terms of CPU cycles and memory, as well as introducing delay.

Table 15 indicates the main use case #8.0 as well as some example variations:

Table 15 – Use case #8 and variations

UC:	Characteristic:	Comments:
#8.0	• existing ITU-T H.248 Stream group with active data channels • closing of all data channels • subsequent shutdown of the SCTP Association without DTLS connection release	• this use case demonstrates the removal of all ITU-T H.248 component streams of Stream group SG2, and the modification of the ITU-T H.248 deaggregation stream T1(S4) (which is kept due to the still established DTLS connection)
#8.1	as #8.0 with following change: • but keeping the Stream group SG2 definition, i.e., unused ITU-T H.248 component streams	• looks feasible from an ITU-T H.248 perspective ("a real-world use case is dependent on "reuse debates" in context of WebRTC data discussions, hence out of scope or Release 1 of this Recommendation")

Figure 15 discusses ITU-T H.248 Context models for use case #8.0:

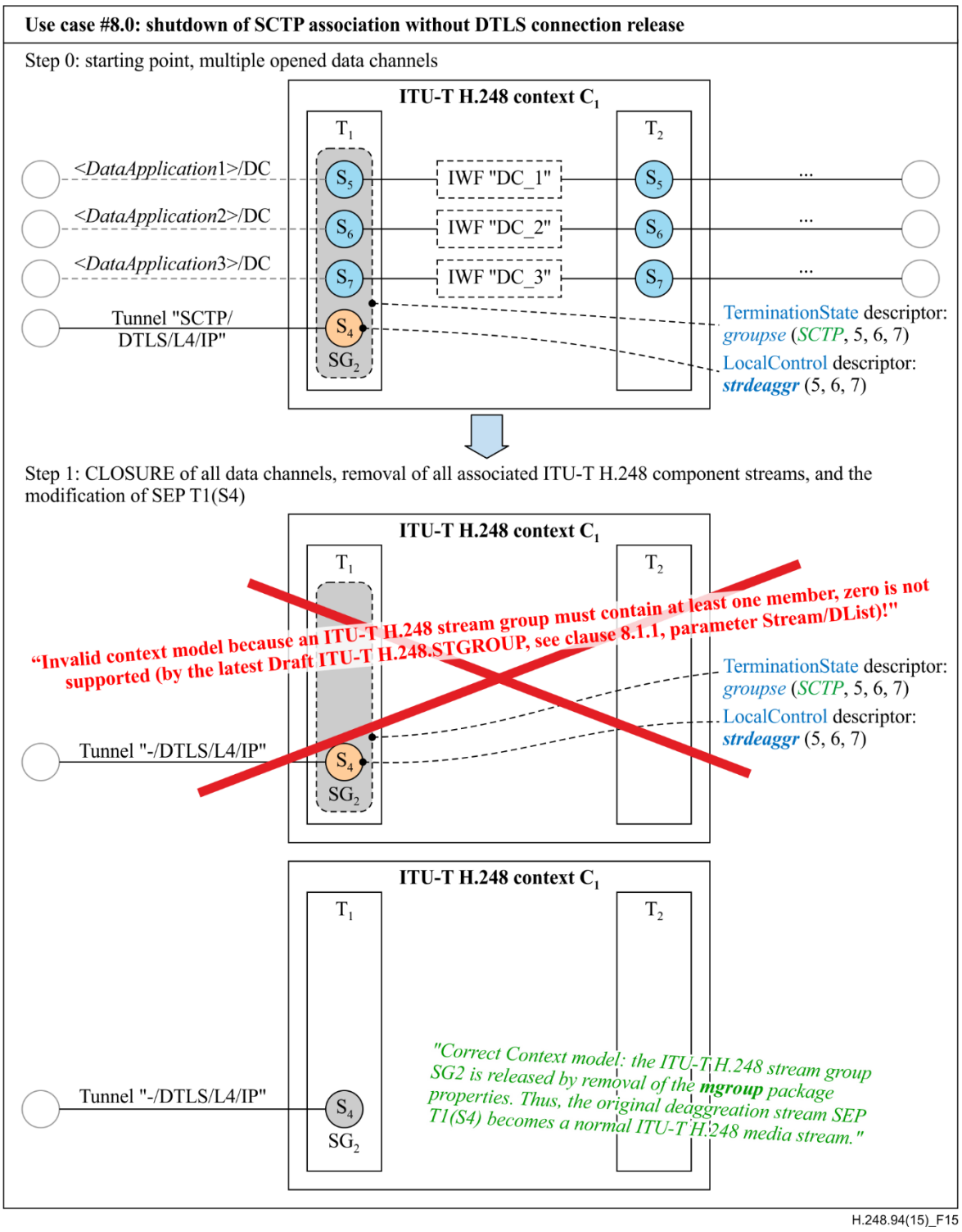


Figure 15 – ITU-T H.248 WebRTC gateway – ITU-T H.248 Context model – Use case #8.0: SCTP Association shutdown without DTLS connection release

Figure 16 outlines an example signalling flow:

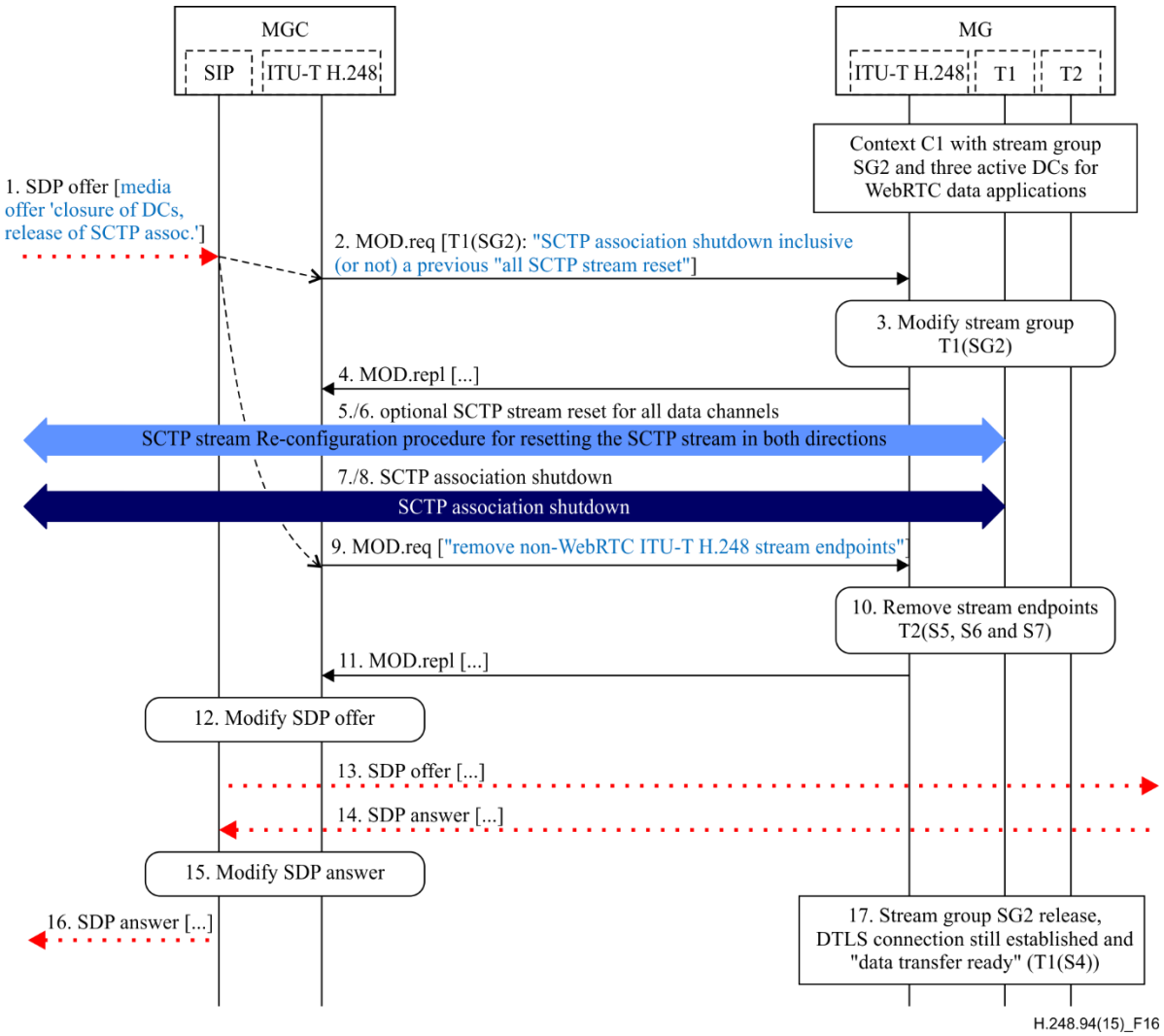


Figure 16 – Example signalling flow for use case #8.0

Observations/discussion of selected signalling steps:

Step:	Comments:
3	the ITU-T H.248 Property *mgroup/groupse* is removed from the TerminationState Descriptor of Termination T1 as well as property *mgroup/strdeaggr* is removed from the LocalControl Descriptor of SEP T1(S4)
5, 6	ITU-T H.248 SEPs T1(S4, S5 and S6) are explicitly removed by the MGC
17	the former ITU-T H.248 deaggreation streams becomes now a "normal" ITU-T H.248 component stream T1(S4), which still contains the protocol stack segment "DTLS/IP/L2"

11.17.3.4 Use case #9: complete call release

Table 16 indicates the main use case #9.0 as well as some example variations:

Table 16 – Use case #9 and variations

UC:	Characteristic:	Comments:
#9.0	• all WebRTC data channels are closed and the underlying transport stack is completely released, but the ITU-T H.248 Termination isn't subtracted	• see general comments in clause 11.17.3.1
#9.1	as #9.0 with following change: • subtraction of ITU-T H.248 WebRTC Termination	• see general comments in clause 11.17.3.1

Figure 17 illustrates an example signalling flow for use case #9.0:

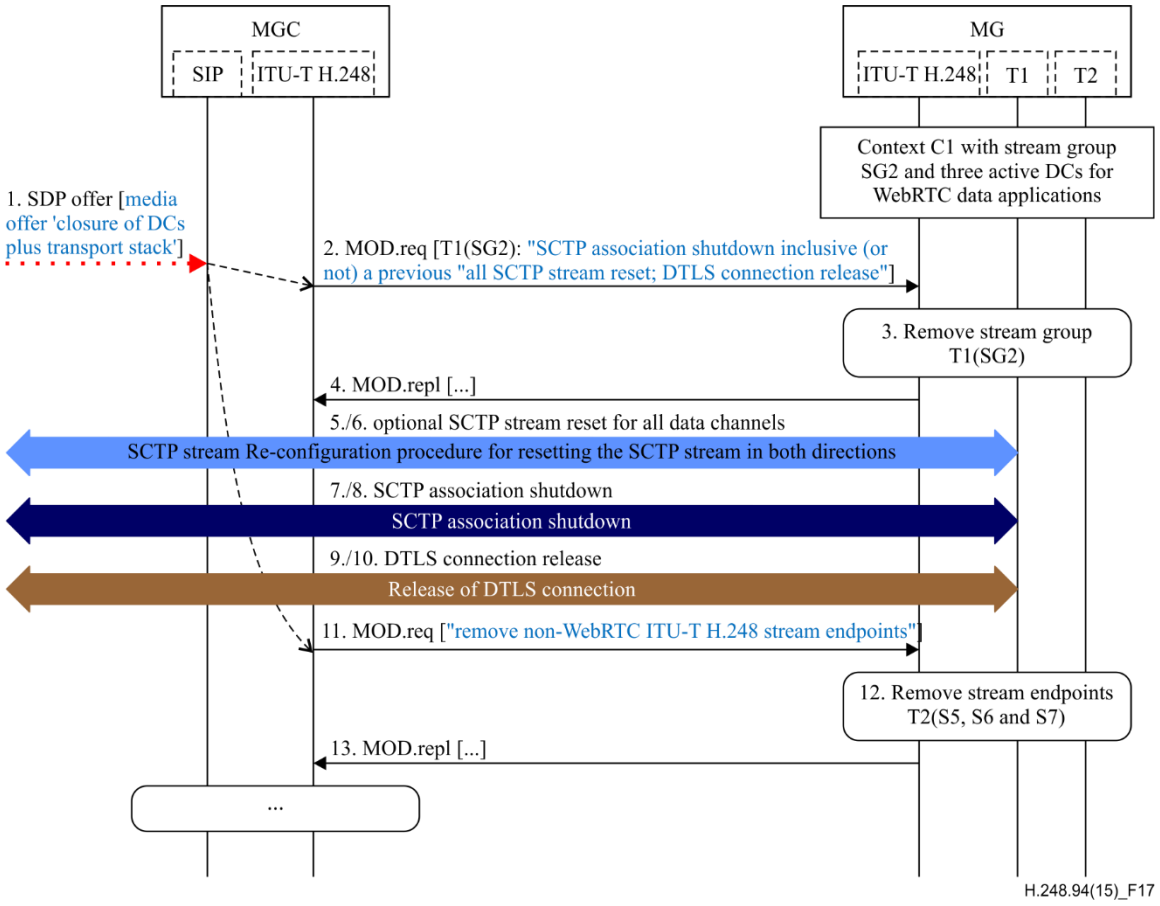


Figure 17 – Example signalling flow for use case #9.0

Observations/discussion of selected signalling steps:

Step:	Comments:
9, 10	NOTE – there might be a subsequent TCP connection release in case of "L4 = TCP"

Appendix I

Use case specific capability sets –Examples

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

I.1 Overview

Profile content is mainly use case dependent (given be the inherent motivation of "protocol profiling"). In order to demonstrate profile specification guidelines in clause 11, this Recommendation considers some exemplary use cases (see Table I.1):

– capability set 'A' (CS_A) – an ITU-T H.248 WebRTC gateway as positioned in use case #1 (see clause 7.1.1):

  use case #1 is based on the assumption that the WebRTC endpoint could request and use all mandatory WebRTC capabilities as defined by the IETF / W3C. Thus, all mandatory and optional capabilities according to [b-IETF rtcweb-gateway] are basically in scope. The ITU-T H.248 WebRTC gateway does then need to support all mandatory requirements as listed in clause 8. Capability set 'A' ($CS_{A)}$ also covers all optional features for enhanced gateway operation;

– capability set 'B' (CS_B) – an ITU-T H.248 WebRTC gateway as positioned in use case #2 with scope on the NGN/IMS domain located WebRTC endpoint (see clause 7.1.2);

– capability set 'C' (CS_C) – an ITU-T H.248 WebRTC gateway again for use case #2, but a light weight capability set in comparison to CS_B, which reflects the service focus at market introduction phase.

Capability set 'A' (CS_A) is therefore a superset of capability set 'B' (CS_B), and 'B' a superset of capability set 'C' (CS_C). Hence, reflecting the usual evolution and phased introduction of new communication services.

Furthermore, besides pure ITU-T H.248 WebRTC gateways with point-to-point connection models due to their network positioning at the edge, access or peering level:

– capability set 'D' (CS_D) – an ITU-T H.248 WebRTC media server with primary scope on WebRTC-based conferencing topologies and support. The correspondent column in Table I.1 indicates a lot of capabilities as *not applicable* (n.a.), e.g., due to assumptions that any kind of NAT traversal support is already provided at the network access segment of the IP paths.

Table I.1 – Examples of use case specific capability sets

Capability	CS_A	CS_B	CS_C	CS_D
NAT-T I: ICE/STUN for UDP	X	X	X	n.a.
NAT-T II: ICE/STUN for TCP	X	X	X	n.a.
NAT-T III: ICE refreshes during active call phase	X	X	-	n.a.
NAT-T IV: ICE lite mode only	X	X	X	n.a.
NAT-T V: ICE full mode	X	-	-	n.a.
NAT-T VI: latching	X	X	X	n.a.
NAT-T VII: B-ALG for L4+ support for WebRTC data applications	X	X	X	n.a.
Multiplexing I: RTP transport multiplexing	X	-	-	X
Multiplexing II: RTP media multiplexing	X	-	-	X
Multiplexing III: UDP payload multiplexing	X	X	-	X
ITU-T H.248 MG type I: WebRTC gateway	X	X	X	-
ITU-T H.248 MG type II: WebRTC media server (media resource function)	-	-	-	X
WebRTC service profile I: audio and video only	X	X	X	X
WebRTC service profile II: audio, video and MSRP-based data only	X	X	X	X
WebRTC service profile III: audio and video and multiple data channels	X	X	-	X
WebRTC service profile IV: CLUE-based conferencing control	X	-	-	X
WebRTC service profile V: performance monitoring	X	-	-	-
WebRTC data channel control I: out-of-band control	X	X	X	X
WebRTC data channel control II: in-band control	X	-	-	X
WebRTC data channel control III: reset of data channels	X	X	-	X
Multiple SRTP key management schemes (due to non-WebRTC SRTP)	X	X	X	X
Enhanced DTLS support (negotiation, maintenance & monitoring)	X	X	-	-
Enhanced ITU-T H.248 control I: stream interlinkage support	X	X	-	n.a.
Enhanced ITU-T H.248 control II: advanced wildcarding	X	X	-	n.a.

Appendix II

Distributed text-over-IP endpoints for WebRTC data 'text'

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

II.1 Purpose

The specific transport of ITU-T T.140 text messages in WebRTC leads to a new interworking model required for WebRTC gateways, resulting in application-specific configurations of the "lower layer protocols" SCTP and RTP in the WebRTC and non-WebRTC domain, as well as dedicated support by the WebRTC gateway in partially emulating a virtual ITU-T T.140 endpoint (i.e., protocol behaviour of [IETF RFC 4103]). Such type of MG-embedded interworking capabilities are usual implementation specific and out of scope of this Recommendation. The purpose of this Appendix is to summarize the problem statement and indicate potential solutions.

II.2 Problem statement

Figure II.1 recalls the reference architecture for the definition of the [b-ITU-T V.151] *text relay mode* ("text-over-IP", ToIP) in case of end-to-end communication between IP user equipment:

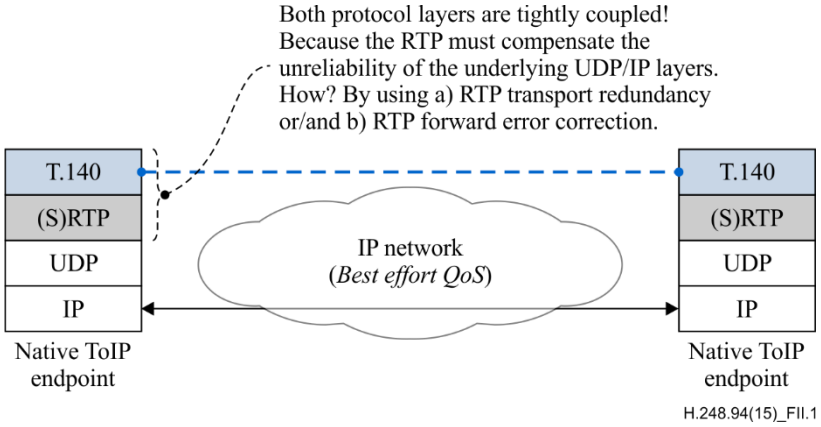


Figure II.1 – Starting point: legacy ToIP in all-IP networks

There are fundamental interactions between the *application level framing protocol* (i.e., RTP) and the *application protocol* (ITU-T T.140), given by the network transport requirements for communication service "text conversation" (or real-time text).

Figure II.2 outlines the two main options which were considered for text conversation embedded in WebRTC:

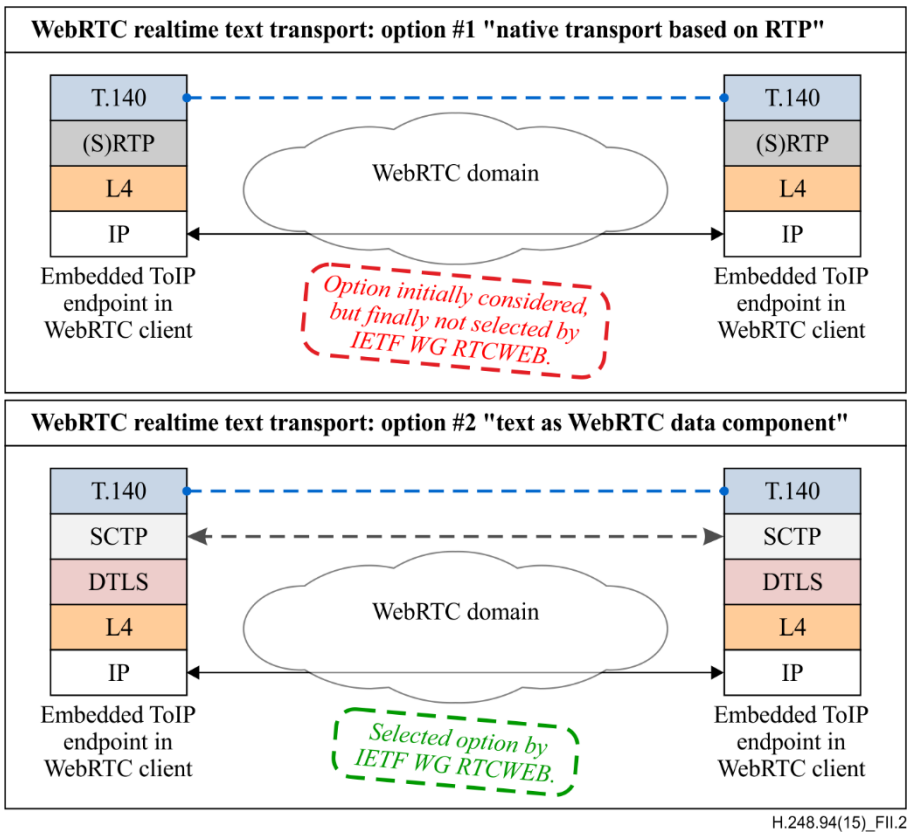


Figure II.2 – peer-to-peer WebRTC: options for WebRTC real-time text transport

Option #1 represents the legacy usage of text-over-RTP (i.e., according to the baseline specification [b-ITU-T V.151]). This approach looks straightforward because:

1) WebRTC already uses audio-over-RTP and video-over-RTP, i.e., text-over-RTP would be just the third application component within the WebRTC "RTP suite"; and

2) text conversation is inherently of type "real-time" as per the two other conversational real-time components audio and video (thus, transport via the real-time transport protocol").

IETF selected option #2, i.e., considering text conversation just as one out of many possible WebRTC data applications.[2] Hence, real-time text in a WebRTC environment uses the WebRTC data channel based transport with its SCTP/DTLS/L4/IP-based stack.

Figure II.3 indicates the associated *WebRTC gateway scenario*, which is the exclusive scope in this Recommendation:

[2] The decision to transport real-time text over a data channel in WebRTC (instead of RTP-based transport) is constituted by use case "U-C 5: *Real-time text chat during an audio and/or video call with an individual or with multiple people in a conference*", see section 3.2 of [b-IETF-rtcweb-data-channel].

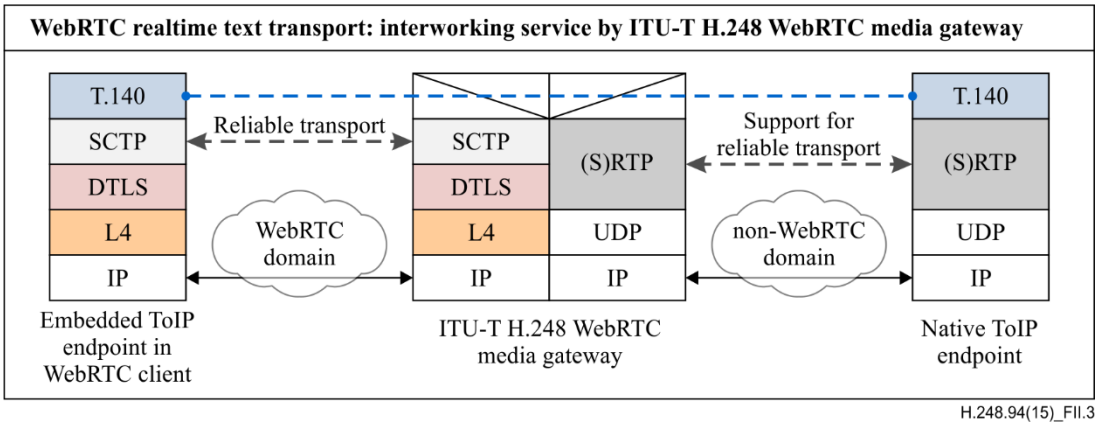


Figure II.3 – WebRTC gateway scenario – protocol stack model in user plane

The required WebRTC gateway service for interworking real-time text between WebRTC and non-WebRTC network domains appears straightforward:

The ITU-T H.248 WebRTC MG must provide (see clause 8.6.4):

a) a "*ITU-T T.140 PDU transparent forwarding*" service besides;

b) the *protocol stack interworking* of "SCTP/DTLS/L4" to "(S)RTP/UDP".

The "ITU-T T.140 transparent forwarding" mode is basically possible, but the WebRTC gateway needs to provide a few support functions in order to address RTP packet loss and ITU-T T.140 inactivity periods. [IETF RFC 4103] defines the required behaviour for *RTP end systems* (i.e., the *RTP source* and *RTP sink* of an ITU-T T.140 stream), which might need a few modifications:

More precisely (using the "RTP grouping taxonomy" terminology): there will be a *distributed model* in case of WebRTC gateways because (NOTE – the referred to processing stages are according to the model in Appendix II of [b-ITU-T H.248.95]):

a) the ITU-T T.140 entities "*media capture*/*media renderer*", "*media source*/*media sink*", "*media encoder*/*media decoder*" and "*media packetizer*/*media depacketizer*" are located at the remote end system (the *WebRTC client*); and

b) the media transport level entities "*SCTP Stream source*/*SCTP Stream sink*" and "*RTP source*/*RTP sink*" represent MG local functions.

Another aspect of consideration is the correct configuration of the underlying protocol stack with respect to support of sufficient reliability for text transport. Figure II.4 provides a summary:

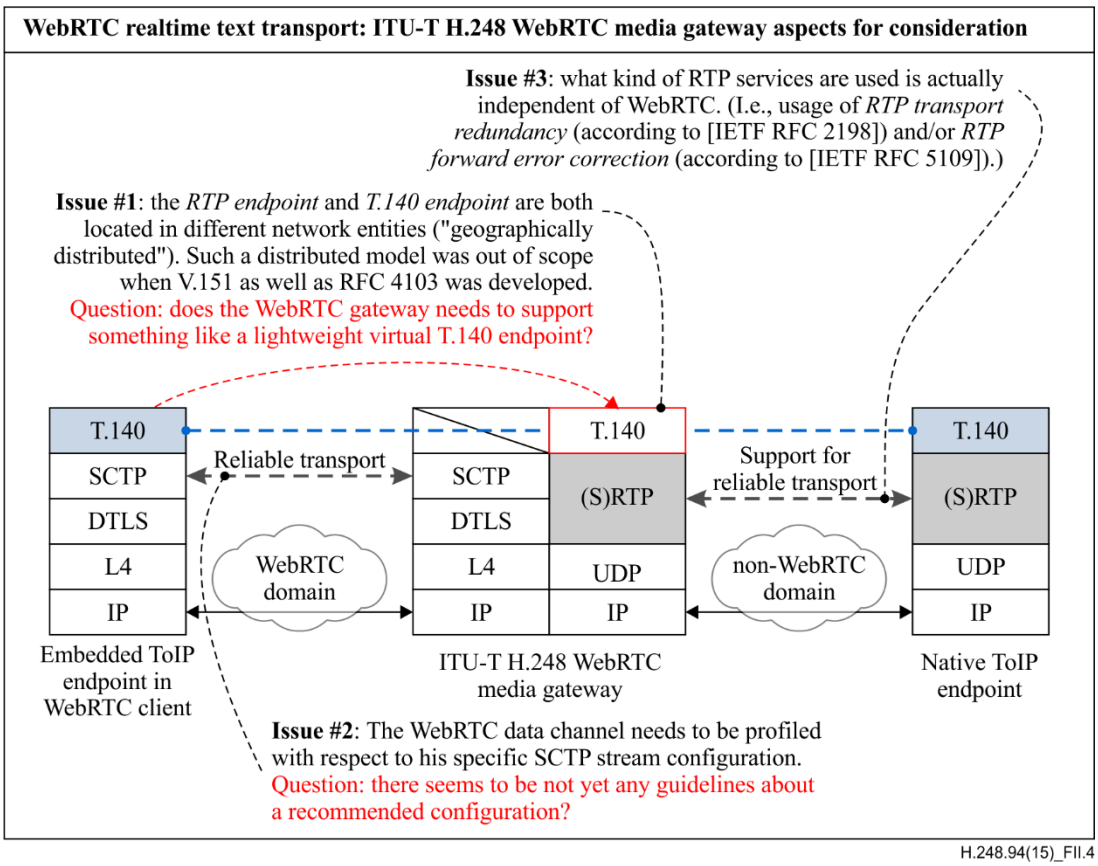


Figure II.4 – WebRTC gateway scenario – Network engineering aspects

Figure II.5 illustrates the complete, unidirectional media processing model in WebRTC to non-WebRTC direction. It underlines the geographical separation (and SCTP-based interruption) of the normally, tightly coupled functions of the "*ITU-T T.140 media endcoder*" (S:3) and the "*RTP media packetizer*" (S:5).

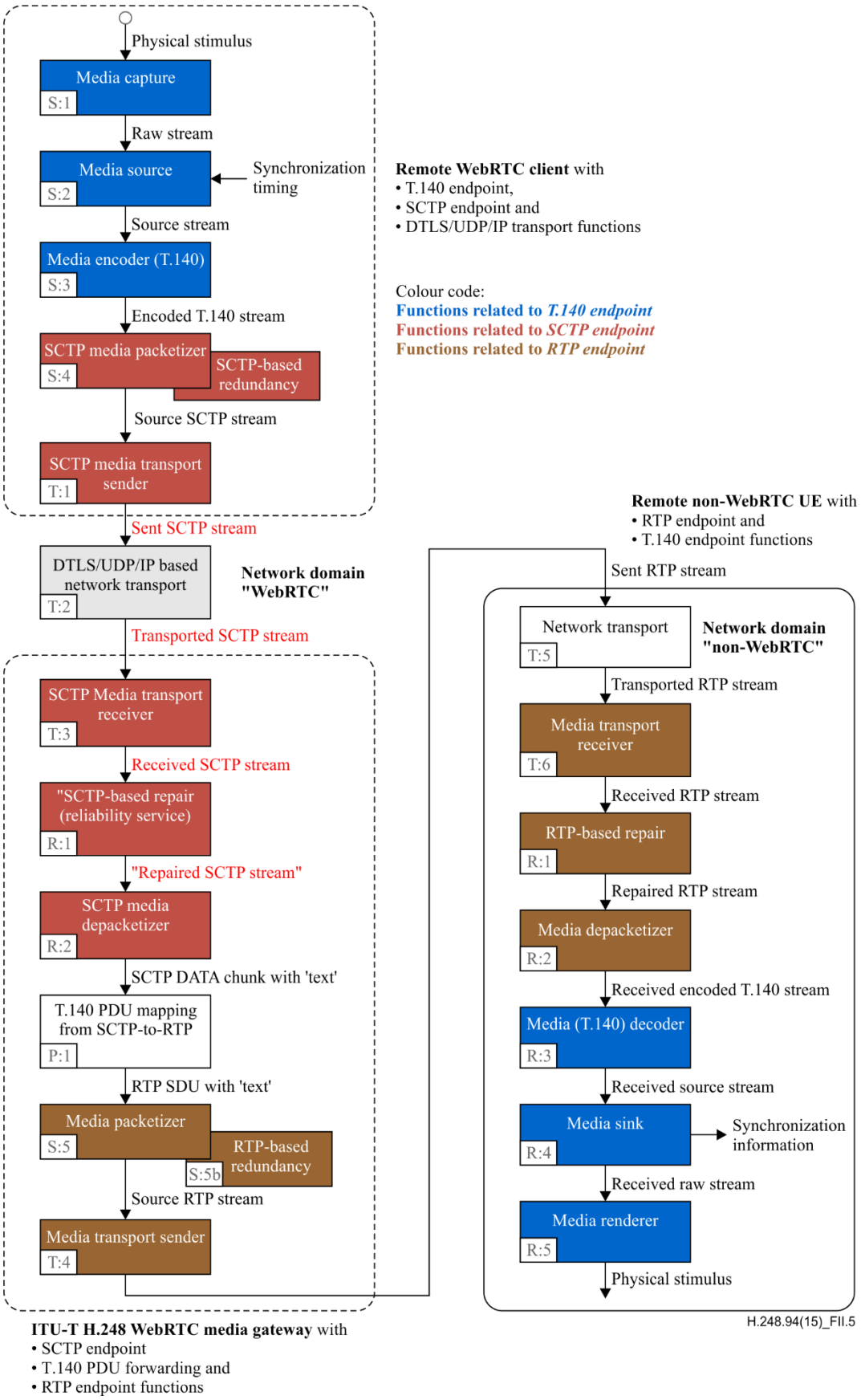


Figure II.5 – WebRTC gateway scenario – Functional processing stages of the distributed "ITU-T T.140-over-RTP endpoint" in WebRTC client to non-WebRTC UE direction

II.3 Solution – Guidelines for the WebRTC MG (ITU-T T.140)-IWF

The WebRTC MG needs to provide some support functions see Table II.1 in order to optimize the end-to-end service quality:

Table II.1 – Policy rules for (ITU-T T.140)-IWF by WebRTC MGs

Rule	Condition(s): If …	Action(s): Then …	Protocol intervention:
$R_{Out,1}$:	C_1: "Inactivity of (ITU-T T.140)-PDU traffic in WebRTC-to-non-WebRTC direction?"	A_1: "MG behaviour: *RTP source* function according to section 5.2 of [IETF RFC 4103], "*Transmission before and after "Idle Periods'*"".	MG sends "empty RTP packets" under consideration of RTP redundancy or/and FEC.
$R_{In,1}$:	C_1: "Incoming RTP packets out of order?"	A_1: "MG behaviour: *RTP sink* function according to section 5.4 of [IETF RFC 4103], "*Compensation for Packets Out of Order*"".	MG delays internal forwarding of RTP payload data (i.e., ITU-T T.140 block) due to required buffering periods.
$R_{In,2}$:	C_1: "Incoming RTP packets lost?"	A_1: "MG behaviour: *RTP sink* function according to section 5.3 of [IETF RFC 4103], "*Detection of Lost Text Packets*"".	MG inserts new ITU-T T.140 blocks with "*missing text marker*" information.

The indicated support functions would be located in processing stage "*ITU-T T.140 PDU mapping between SCTP Stream and RTP*" when using a model such as illustrated in Figure II.5.

Bibliography

[b-ITU-T G.711] Recommendation ITU-T G.711 (1988), *Pulse code modulation (PCM) of voice frequencies*.

[b-ITU-T H.248.95] Recommendation ITU-T H.248.95 (2015), *Gateway control protocol: ITU-T H.248 support for RTP multiplexing*.

[b-ITU-T H.264] Recommendation ITU-T H.264 (2014), *Advanced video coding for generic audiovisual services*.

[b-ITU-T H.265] Recommendation ITU-T H.265 (2013), *High efficiency video coding*.

[b-ITU-T H.Sup.13] Supplement ITU-T H.Suppl. 13 (2015), *Gateway control protocol: Common ITU-T H.248 terminology – Release 2*.

[b-ITU-T V.151] Recommendation ITU-T V.151 (2006), *Procedures for the end-to-end connection of analogue PSTN text telephones over an IP network utilizing text relay*.

[b-IANA H.248 Packages] IANA (2015), Megaco/H.248 Packages. <https://www.iana.org/assignments/megaco-h248/megaco-h248.xhtml>

[b-ETSI TS 183 018] ETSI TS 183 018 V3.5.1 (2009-07), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile Version 3 for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification*. <https://www.etsi.org/deliver/etsi_ts/183000_183099/183018/03.05.01_60/ts_183018v030501p.pdf>

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 4733] IETF RFC 4733 (2006), *RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals*.

[b-IETF RFC 4788] IETF RFC 4788 (2007), *Enhancements to RTP Payload Formats for EVRC Family Codecs*.

[b-IETF RFC 4867] IETF RFC 4867 (2007), *RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs*.

[b-IETF RFC 5763] IETF RFC 5763 (2010), *Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)*.

[b-IETF RFC 6184] IETF RFC 6184 (2011), *RTP Payload Format for H.264 Video*.

[b-IETF RFC 6386] IETF RFC 6386 (2011), *VP8 Data Format and Decoding Guide*.

[b-IETF RFC 6716] IETF RFC 6716 (2012), *Definition of the Opus Audio Codec*.

[b-IETF RFC 7362] IETF RFC 7362 (2014), *Latching: Hosted NAT Traversal (HNT) for Media in Real-Time Communication*.

[b-IETF RFC 7587] IETF RFC 7587 (2015), *RTP Payload Format for Opus Speech and Audio Codec*.

[b-IETF bfcpbis] IETF draft-ietf-bfcpbis-rfc4582bis-16 (2015), *The Binary Floor Control Protocol (BFCP)*.

[b-IETF codec-vp9] IETF draft-grange-vp9-bitstream-00 (2013), *A VP9 Bitstream Overview*.

[b-IETF data-channel-msrp] IETF draft-ietf-mmusic-msrp-usage-data-channel (2015), *MSRP over data channels*.

[b-IETF data-channel-t140] IETF draft-schwarz-mmusic-t140-usage-data-channel-02 (2015), *T.140 Text Conversation over Data Channels*.

[b-IETF data-channel-msrp] IETF draft-ietf-mmusic-msrp-usage-data-channel (2015), *MSRP over data channels*.

[b-IETF DCEP] IETF draft-ietf-rtcweb-data-protocol-09 (2015), *WebRTC Data Channel Establishment Protocol*.

[b-IETF DCSDP] IETF draft-ietf-mmusic-data-channel-sdpneg (2015), *SDP-based data channel negotiation*.

[b-IETF ice-dualstack] IETF draft-ietf-mmusic-ice-dualstack-fairness-02 (2015), *ICE Multihomed and IPv4/IPv6 Dual Stack Fairness*.

[b-IETF rmcat-cc] IETF draft-ietf-rmcat-cc-requirements-09 (2014), *Congestion Control Requirements for Interactive Real-Time Media*.

[b-IETF rtcweb-audio] IETF draft-ietf-rtcweb-audio-10 (2016), *WebRTC Audio Codec and Processing Requirements*.

[b-IETF rtcweb-ecrit] IETF draft-aboba-rtcweb-ecrit-01 (2013), *Emergency Services Support in WebRTC*.

[b-IETF rtcweb-gateway] IETF draft-ietf-rtcweb-gateways-02 (2016), *WebRTC Gateways*.

[b-IETF rtcweb-jsep] IETF draft-ietf-rtcweb-jsep-12 (2015), *Javascript Session Establishment Protocol*.

[b-IETF rtcweb-overview] IETF draft-ietf-rtcweb-overview-15 (2016), *Overview: Real Time Protocols for Brower-based Applications*.

[b-IETF rtcweb-secur] IETF draft-ietf-rtcweb-security-08 (2015), *Security Considerations for WebRTC*.

[b-IETF rtcweb-sec-arch] IETF draft-ietf-rtcweb-security-arch-11 (2015), *WebRTC Security Architecture*.

[b-IETF rtcweb-transports] IETF draft-ietf-rtcweb-transports-11 (2016), *Transports for WebRTC*.

[b-IETF rtcweb-video] IETF draft-ietf-rtcweb-video-06 (2015), *WebRTC Video Processing and Codec Requirements*.

[b-IETF rtcweb-xr] IETF draft-ietf-xrblock-rtcweb-rtcp-xr-metrics-02 (2015), *Considerations for Selecting RTCP Extended Report (XR) Metrics for the WebRTC Statistics API*.

[b-IETF rtp-h265] IETF draft-ietf-payload-rtp-h265-15 (2015), *RTP Payload Format for H.265/HEVC Video*.

[b-IETF rtp-usage] IETF draft-ietf-rtcweb-rtp-usage-25 (2015), *Web Real-Time Communication (WebRTC): Media Transport and Use of RTP*.

[b-IETF rtp-vp8] IETF draft-ietf-payload-vp8-17 (2015), *RTP Payload Format for VP8 Video*.

[b-IETF sdp-bundle] IETF draft-ietf-mmusic-sdp-bundle-negotiation-26 (2015), *Negotiating Media Multiplexing Using the Session Description Protocol (SDP)*.

[b-IETF sdp-sctp] IETF draft-ietf-mmusic-sctp-sdp-15 (2015), *Stream Control Transmission Protocol (SCTP)-Based Media Transport in the Session Description Protocol (SDP).*

[b-IETF tls-terms] IETF draft-guballa-tls-terminology-02 (2015), *Terminology related to TLS and DTLS.* <https://tools.ietf.org/html/draft-guballa-tls-terminology-02>

[b-IETF trickle-ice] IETF draft-ietf-mmusic-trickle-ice-02 (2015), *Trickle ICE: Incremental Provisioning of Candidates for the Interactive Connectivity Establishment (ICE) Protocol*.

[b-IETF webRTCDC] IETF draft-ietf-rtcweb-data-channel-13 (2015), *WebRTC Data Channels.*

[b-W3C webrtc-stats] W3C draft webrtc-stats (2015), *Identifiers for WebRTC's Statistics API*. < http://www.w3.org/TR/webrtc-stats/>

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2016