International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.40

(03/2013)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Gateway control protocol: Application data inactivity detection package

Recommendation ITU-T H.248.40

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	**H.240–H.259**
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
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

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

Recommendation ITU-T H.248.40

Gateway control protocol: Application data inactivity detection package

Summary

Recommendation ITU-T H.248.40 describes the principle used to detect application data inactivity for IP transport connections in general, like e.g., avoid a potential situation of deadlock if latching was set but no application data stream is incoming to latch on. The solution is based on an event to detect if application data had stopped (or not started).

This revision provides additional information regarding the setting of the detection time for the IP flow stop event.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.248.40	2007-01-13	16
2.0	ITU-T H.248.40	2013-03-16	16

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Page

Recommendation ITU-T H.248.40

Gateway control protocol: Application data inactivity detection package

1 Scope

This Recommendation allows a media gateway controller to request the media gateway to detect that after a certain period of time no Internet protocol application data has flowed on a particular termination/stream. The ability to detect if Internet protocol application data flow has stopped or has not started is useful to avoid deadlock in latching scenarios and also may be of use to detect hanging bearers.

This Recommendation defines an event which is related to one or more IP 2-tuples. An individual 2-tuple is given by <IP address, IP port> of an IP flow of an ITU-T H.248 stream or termination. The set of conditions for inactivity detection is related to IP packet arrival and/or departure events for all 2-tuples of a stream/termination. The condition of packet arrivals or departures respectively is controlled via a dedicated parameter (called "*direction*").

The flexibility of inactivity detection logic configurations allows the usage of ITU-T H.248.40 for various applications (see also the appendices).

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*.

3 Terms and definitions

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ADID	Application Data Inactivity Detection
IP	Internet Protocol
LD	Local Descriptor
MG	Media Gateway
MGC	Media Gateway Controller
NAPT	Network Address and Port Translation
RD	Remote Descriptor
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
RTSP	Real-Time Streaming Protocol

5 Conventions

None.

6 Application data inactivity detection package

Package name: Application data inactivity detection package

Package ID: adid (0x009c)

Description: This package enables the MGC to be notified when the MG has detected that no IP application data flow has been detected on a termination/stream.

Version: 1

Extends: None

6.1 Properties

None.

6.2 Events

6.2.1 IP flow stop detection

Event name: IP flow stop detection

Event ID: ipstop (0x0001)

Description: This event detects if there has been no direction-dependent application data for a set (detection time) interval of time. In cases where it has been indicated that multiple IP ports are associated with a flow (e.g., RTP and RTCP), the detection of no application data flow must be done on all ports before the event is triggered. When applied at a termination level the *adid/ipstop* event shall be notified when it has been determined that application data has stopped on all of the streams associated with the termination.

If, after the initial reporting of the event, and if the event remains active, the detection time elapses without detection of application data, the event is reported again. This may occur multiple times.

This event shall be detected irrespective of the StreamMode. For example, even if the stream is set to SendOnly and packets are received, this will be taken into account.

6.2.1.1 EventDescriptor parameters

6.2.1.1.1 Detection time

Parameter name: Detection time

Parameter ID: dt (0x0001)

Description: This is the interval of time after which if no application data flow is detected, the IP Flow Stop Detection event is triggered. The MG checks over intervals of detection time *dt* if any application data traffic has occurred. If no application data has arrived, then the *adid/ipstop* event is triggered.

NOTE – This may result that more than the detection time has passed between the IP data flow stop and the detection of the event.

Type:	Integer
Optional:	Yes (if default is provisioned).
Possible values:	Any positive number of seconds.
Default:	Provisioned

NOTE:

a) Application-independent versus application-specific values:

Either a single, global default value or multiple, application specific default values may be provisioned. There is typically a single value configured in case of a provisioning approach, valid for all applications. Multiple, application-specific default values could be also provisioned. The value selection could be tied to application information like the LD/RD-embedded media description. The specific selection method is out of scope of this package definition and may be e.g., defined in an ITU-T H.248 profile specification.

b) Stream- versus Termination-level event arming:

When applied at a Termination level, where might be aggregated traffic based on multiple applications (in case of multiple streams). The value selection may be again application-specific or a single value. However in this case value selection must be based on the fact that the event will be notified when only all streams on the Termination have timed out.

6.2.1.1.2 Direction

Parameter name:	Direction
Parameter ID:	dir (0x0002)
Description:	With this parameter, the MGC indicates to the MG which direction of the data flow should be monitored to detect inactivity. Incoming direction means from the outside of the context. Outgoing direction means towards the outside of the context. If direction is set to "BOTH", the MG will generate the event if no data is sent nor received on the termination to/from the outside of the context for an interval of detection time *dt*.
Type:	Enumeration
Optional:	Yes
Possible values:	"IN" (0x0001) Incoming direction "OUT" (0x0002) Outgoing direction "BOTH" (0x0003) Both directions
Default:	Both

6.2.1.2 ObservedEventsDescriptor parameters

None.

6.3 Signals

None.

6.4 Statistics

None.

6.5 Error codes

None.

6.6 Procedures

To detect application data inactivity, the MGC should set the *adid/ipstop* event with an appropriate "detection time" and the appropriate "direction" on the applicable ITU-T H.248 Stream/Termination. The *adid/ipstop* event is notified to the MGC:

- If the MGC has set *dir* to "IN" and no IP data packets have been received by the MG from the network in that stream/termination by the expiry of the detection time (*dt*).
- If the MGC has set *dir* to "OUT" and no IP data packets have been sent by the MG to the network in that stream/termination by the expiry of the detection time (*dt*).
- If the MGC has set direction to "BOTH" and no IP data packets have been sent to nor received from the network in that stream/termination by the expiry of the detection time (*dt*).

On reception of a NOTIFY.req with the *adid/ipstop* event, the MGC should take appropriate action.

The triggered action on MGC level may have to take into account:

- Service features (e.g., unidirectional applications, muted microphone in conference services, etc.).
- Bearer service configuration settings (e.g., enabled silence suppression mode in case of speech telephony, RTP sessions without RTCP, etc.).
- ITU-T H.248 Termination configurations (e.g., ITU-T H.248 StreamMode Property equals "Inactive").

It is recommended to set timer detection time (*dt*) with a relevant value, e.g., a multiple of half the round-trip delay or a multiple of the typical packet interarrival time. The mean interarrival time may be IP application-specific (e.g., codec type), may depend on application level framing protocol usage (e.g., RTP packetization time, RTCP transmission interval, etc.) or service-specific (e.g., muted microphone in case of voice over RTP, or suspended streaming in case of RTSP-controlled multimedia streaming).

Appendix I

Example use case for voice-over-RTP

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

I.1 Introduction

This Recommendation may be applied on ephemeral terminations, which are used for two-party voice-over-RTP (VoRTP) service realizations. The RTP packet transmission interval is here much smaller than the granularity of timer "ipstop/dt".

This appendix illustrates the detection of "RTP media stop". The event of "RTP media stop" relates to the arrival/departure event of an RTP or RTCP packet.

I.2 Abbreviations

This appendix uses the following abbreviations:

FIB	(IP) Forwarding Information Base
IPLR	IP Packet Loss Ratio
RIB	(IP) Routing Information Base
SDL	Specification and Description Language
VoRTP	Voice over RTP

I.3 Assumptions

From the RTP bearer point of view:

- RTCP is enabled.
- Minimum RTCP transmission interval is 5 s (see clause A.7 of [b-IETF RFC 3550]).
- RTP peer endpoints continue to send RTCP packets during "silence phases" (detected voice inactivity, or muted microphone).

From the ITU-T H.248 point of view:

- MGC considers StreamMode setting (in case of Event notification).

I.4 Example detection logic

Figure I.1 illustrates example detection logic. The event is supposed to be continuously enabled (default EventBufferControl setting).

It has to be noted that the event remains active until disabled by the MGC.

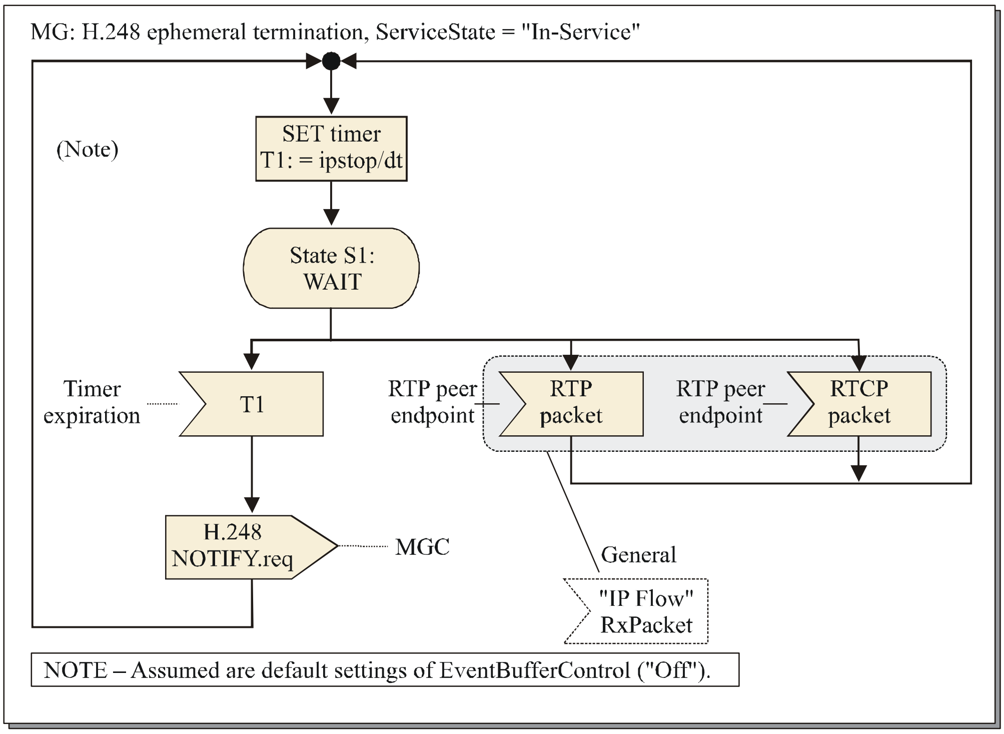


Figure I.1 – Example SDL logic for VoRTP

I.5 Recommendations for timer settings

Some qualitative recommendations; specific settings may depend on the indicated variables.

I.5.1 Objective: "Detect Interrupted IP Route"

Settings of timer "ipstop/dt" may be based on the RTP transmission interval ("estimated maximum interval size").

In case of "fast detection" below, the minimum RTCP report interval is required.

NOTE – Rerouting mechanisms on IP level might be of consideration (e.g., RIB/FIB update intervals due to applied IP routing protocol(s)).

I.5.2 Objective: "Detect Released RTP Endpoint"

Settings of timer "ipstop/dt" may be based on a combination of:

- RTCP transmission interval ("estimated maximum interval size"); and
- IPLR conditions ("estimated loss of RTCP packets").

In case "fast detection" is required, or in case of a more "conservative detection" on (RTP) session holding time (e.g., "estimated Context Holding Time (C_OHT) for VoRTP service").

Appendix II

Example use case for deadlock detection in IP latching scenarios

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

II.1 Introduction

This Recommendation may be applied in the context of [b-ITU-T H.248.37] applications. Figure II.1 shows a potential network configuration.

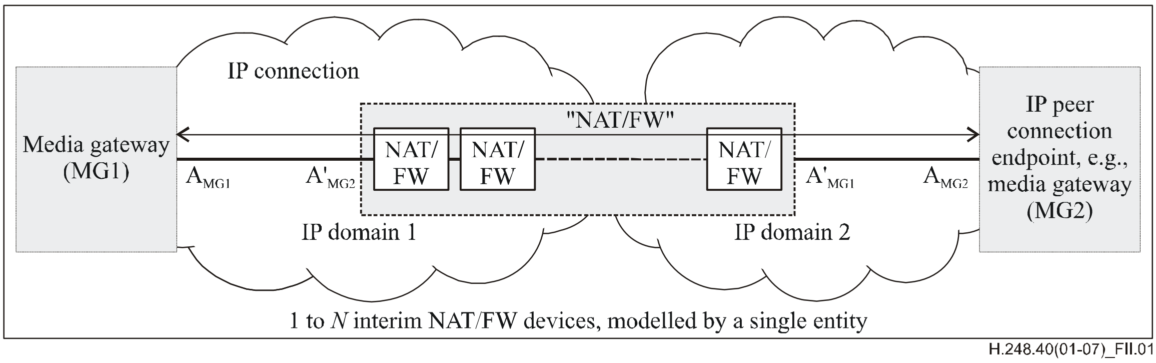


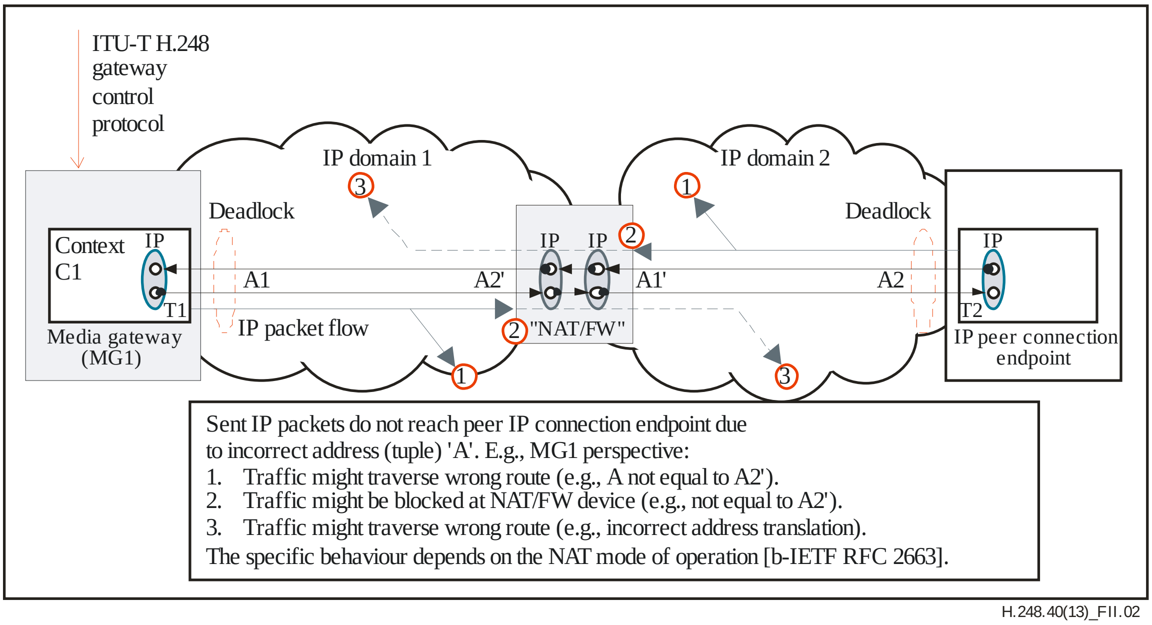
Figure II.1 – Possible network configuration

[b-ITU-T H.248.37] is supporting dynamic IP address adaptations in the user plane (IP-based NGN transport stratum).

This appendix illustrates the detection of a deadlock situation in relation to latching.

II.1.1 Deadlock situation

Sent IP packets may not reach the peer endpoint due to incorrect address information (here: 4-tuple in case of NAPT devices). Figure II.2 illustrates a potential scenario.



Sent IP packets do not reach peer IP connection endpoint due to incorrect address (tuple) 'A'. E.g., MG1 perspective:

1. Traffic might traverse wrong route (e.g., A not equal to A2').
2. Traffic might be blocked at NAT/FW device (e.g., not equal to A2').
3. Traffic might traverse wrong route (e.g., incorrect address translation).

The specific behaviour depends on the NAT mode of operation [b-IETF RFC 2663].

Figure II.2 – Potential deadlock situations

The initially incorrect address tuple requires an inbound IP packet flow in order to adapt to a correct address (also known as "latching" function; see [b-ITU-T H.248.37]).

Deadlock situation:

> "No address update in case of missing inbound flow, accompanied by impossible packet delivery in outbound directions due to incorrect address information, …"

II.2 Assumptions

How such deadlock situations are finally resolved is beyond the scope of this Recommendation. Basic assumption is that such actions might be triggered by MGCs, based on ITU-T H.248.40 event notifications.

From the IP bearer termination point of view:

- None.

From the ITU-T H.248 point of view:

- MGC considers StreamMode setting (in case of Event notification).

II.3 Example detection logic

Activity in outbound direction is irrelevant. The example detection logic according to Figure I.1 is therefore applicable as well. Valid IP packet arrival events are defined by available address tuple information according to the ITU-T H.248 local descriptor (LD).

II.4 Recommendations for timer settings

Some qualitative recommendations; specific settings may depend on the indicated variables.

II.4.1 Objective: "Detect deadlock in IP latching applications"

Settings of timer "ipstop/dt" may be based on "typical, end-to-end session establishment delay" values in case "fast detection" is required.

NOTE – The assumption is stable "device configuration settings" after a completed signalling scenario for session establishment.

Appendix III

Example use case for detection of a hanging voice over RTP session

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

III.1 Introduction

This Recommendation may be used to detect and avoid hanging RTP sessions. An RTP session is characterized by one or two (in case of RTCP) UDP-based IP transport connections between two RTP end systems (see [b-IETF RFC 3550]). For instance, in Figure III.1, the two peer RTP endpoints are located in VoRTP MGs, i.e., the MGs acting as RTP end system. The RTP session endpoint is therefore related to an ephemeral termination.

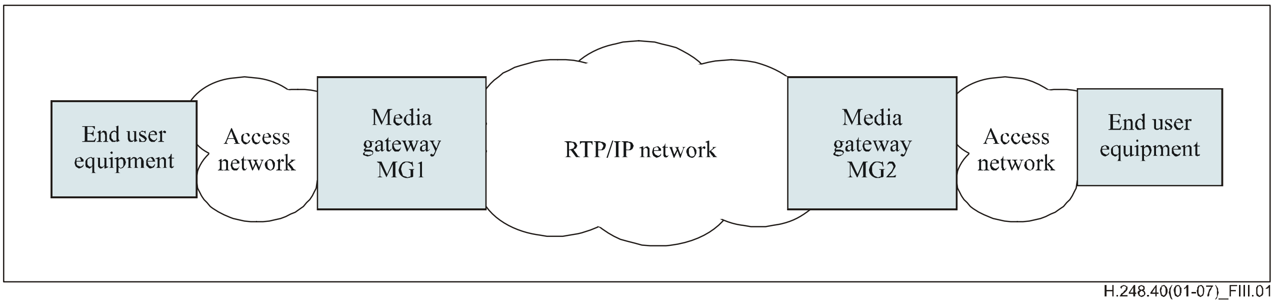


Figure III.1 – Network configuration in a voice over RTP session

The "access network" in Figure III.1 is not necessarily "RTP-based".

III.2 Abbreviations and acronyms

This appendix uses the following abbreviation:

VoIP	Voice over IP

III.3 Incorrect termination of a Voice over RTP session

Figure III.1 shows two user equipment engaged in a VoIP connection.

If one or both of the sides of the session (RTP session and/or call/session control association) is not terminated properly, this may result in some cases in hanging bearer resources or sessions kept alive for unnecessary long time. The operator may protect itself against this situation by using ITU-T H.248.40.

Normally in this case, a hanging situation cannot be assumed only due to lack of data activity in one direction. It is necessary to observe that no RTP stream is received in either direction to assume a hanging situation. Therefore the MGC should arm the ipstop event with direction equals to "both".

III.4 Relation of "hanging RTP session" with "hanging ITU-T H.248 termination"

The hanging session scenario described in clause III.3 may imply hanging resources at call control level, i.e., not only have the bearer resources in the MG not been released, but the corresponding control resources in the MGC have not been released either. This kind of scenarios cannot be resolved with the ITU-T H.248.36 hanging termination detection package, as the scenario does not involve a hanging termination.

Thus, the packages of ITU-T H.248.40 and ITU-T H.248.36 are generally decoupled and complementary because they are both addressing different inactivity conditions in user plane and control plane respectively.

Bibliography

[b-ITU-T H.248.37]	Recommendation ITU-T H.248.37 (2008), *Gateway control protocol: IP NAPT traversal package*.
[b-IETF RFC 2663]	IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.
[b-IETF RFC 3550]	IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications.*

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2013