

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.50

(07/2016)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication
procedures

Gateway control protocol: NAT traversal toolkit packages

Recommendation ITU-T H.248.50

ITU-T

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.

Revised Recommendation ITU-T H.248.50

Gateway control protocol: NAT traversal toolkit packages

Summary

Recommendation ITU-T H.248.50 contains a series of ITU-T H.248 packages that enable various network address translator (NAT) traversal techniques to be employed in order to facilitate media flow between networks or user equipment and network-side located media gateways. Any of these packages may be utilized in any order to gather and map addresses, as well as maintain connectivity with and through NATs.

This revision of Recommendation ITU-T H.248.50 adds clarifications and further capabilities, such as:

- a new ITU-T H.248 session traversal utilities for NAT (STUN) consent freshness package;
- package-independent ITU-T H.248 procedures for specific NAT traversal use cases;
- interactive connectivity establishment (ICE) variants (full vs ICE lite; user equipment (UE)-embedded vs gateway-embedded ICE clients; vanilla vs trickle ICE; ICE for user datagram protocol (UDP) vs ICE for TCP; ICE for single-homed vs multi-homed host entities); and
- updates to keep alive support.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.248.50	2010-09-13	16	11.1002/1000/10984
1.1	ITU-T H.248.50 (2010) Cor. 1	2012-02-13	16	11.1002/1000/11542
2.0	ITU-T H.248.50	2016-07-14	16	11.1002/1000/12919

Keywords

FW, Gateway, ITU-T H.248, ICE, NAT, STUN, TURN.

* 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 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/>.

© ITU 2016

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
	1.1 Relation to other ITU-T H.248 related NAT traversal mechanisms	2
2	References.....	3
3	Definitions	4
	3.1 Terms defined elsewhere	4
	3.2 Terms defined in this Recommendation.....	4
4	Abbreviations and acronyms	5
5	Conventions	6
6	Toolkit usage	6
	6.1 ITU-T H.248.50 usage in different network models	6
	6.2 Overview of toolkit NAT traversal techniques	13
	6.3 ITU-T H.248 call/bearer separation, connection model and IP addresses for ephemeral terminations.....	13
	6.4 Specific SDP information elements.....	14
	6.5 Overview of NAT traversal support mechanisms (by ITU-T H.248 entities)	15
7	STUN and TURN support	16
	7.1 STUN base package	16
	7.2 MG STUN client package	18
	7.3 MG TURN client package.....	21
	7.4 MGC STUN client package.....	25
	7.5 STUN information package.....	27
8	ICE support.....	29
	8.1 MG act-as STUN server package	31
	8.2 Originate STUN continuity check package.....	33
	8.3 STUN consent freshness package	39
9	Keep-alive and pinhole support.....	43
	9.1 MGC-originated STUN request package	43
	9.2 Keep alive request package	45
10	Package-independent NAT-T procedures.....	47
	10.1 Support for MG terminated STUN-based connectivity checks.....	47
	Appendix I – Example signalling scenarios for package-independent NAT-T procedures ...	50
	I.1 Example #1: ICE/STUN support by ITU-T H.248 IP access gateways.....	50
	Appendix II – ICE for TCP.....	53
	II.1 Introduction	53
	II.2 MG bearer interface: protocol stack	53
	II.2 Bearer establishment	53
	II.3 TCP address candidates	53



	Page
Appendix III – ICE mode support by gateway-embedded ICE agents.....	55
III.1 Background.....	55
III.2 Main differences between ICE-full and ICE-lite.....	55
Appendix IV – ICE extensions: "Trickle ICE"	58
IV.1 Introduction	58
IV.2 Impact of trickle ICE on ITU-T H.248.50-defined packages.....	59
IV.3 Example signalling flows for trickle ICE	59
IV.4 Summary.....	59
Appendix V – ICE multihomed and IPv4/IPv6 dual stack fairness.....	60
V.1 Introduction	60
V.2 Impact on ITU-T H.248 gateways with ICE support?	60
Appendix VI – ICE restarts.....	61
VI.1 Introduction	61
VI.2 ICE restart procedures	61
VI.2 Impact on ITU-T H.248 gateways with ICE support?	61
Bibliography.....	62

iv

Recommendation ITU-T H.248.50

Gateway control protocol: NAT traversal toolkit packages

1 Scope

This Recommendation describes packages to enable various network address translator (NAT) traversal techniques to be employed in order to facilitate media flow between networks. The media gateway controller (MGC) may utilize any of the packages in any order to gather addresses, map them and then maintain connectivity with and through NATs.

The packages described in this Recommendation allow an ITU-T H.248 MGC and media gateway (MG) to use the techniques defined by:

- simple session traversal utilities for NAT (STUN) reflexive address mapping as defined in [IETF RFC 3489] and [IETF RFC 5389];
- relayed address mapping using the traversal using relays around NAT (TURN) techniques as described in [IETF RFC 5766];
- comprehensive NAT traversal interactive connectivity establishment (ICE) techniques as described in [IETF RFC 5389].

In order to maintain backward compatibility, packages have been produced for both STUN as defined by [IETF RFC 3489] and by [IETF RFC 5389].

Throughout this Recommendation it is assumed that the media gateway performs STUN server discovery through the use of domain name system (DNS) lookup.

Figure 1 summarizes the various packages as defined by the initial Recommendation. Every package is self-contained and does not use the extension principle.

Figure 1

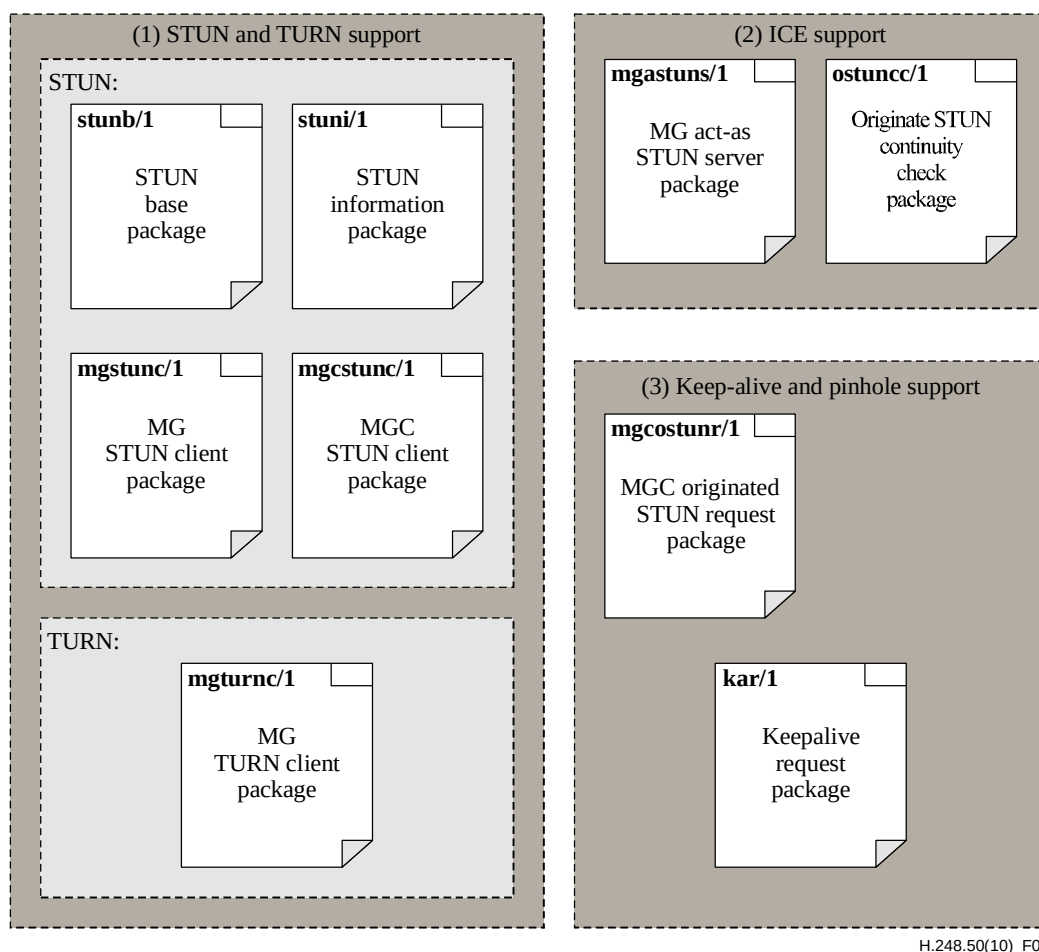


Figure 1 – Landscape of NAT traversal toolkit packages, categorized into three application areas (status of ITU-T H.248.50 (09/2010))

ITU-T H.248.50 (07/2016) adds clarifications and further capabilities, such as:

- a new ITU-T H.248 *STUN consent freshness* package;
- package-independent ITU-T H.248 procedures for specific NAT traversal use cases;
- ICE variants (full vs ICE lite; user equipment (UE)-embedded vs gateway-embedded ICE clients; vanilla vs trickle ICE; ICE for user datagram protocol (UDP) vs ICE for TCP; ICE for single-homed vs multi-homed host entities);
- updates to keep alive support; and
- clarifies support of "ICE restart" procedures.

1.1 Relation to other ITU-T H.248 related NAT traversal mechanisms

The following covers the applicability of this Recommendation versus other ITU-T H.248 supported NAT-T mechanisms:

- Transport protocol generic NAT-T method "media latching" [ITU-T H.248.37]: this is an orthogonal mechanism and may be used in combination with this Recommendation; some of the mechanisms in this Recommendation make "media latching" unnecessary.

NOTE – There is also a bearer plane latching process in the context of ICE, see clause 10.1.5 "STUN-specific media latching". The difference between both latching variants is illustrated in Appendix I. It is further noted that the IETF "media latching" function of [b-IETF RFC 7362] is synonymous to "H.248.37 latching" (because it makes the assumption that ICE/STUN/TURN is not applied for NAT traversal).

- Transport protocol specific NAT-T method "TCP merge mode" [b-ITU-T H.248.84]: this represents a TCP simultaneous open from an end-to-end perspective, which is, if applicable, used before any "ICE for TCP" procedures are selected.

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 (2005), *Gateway control protocol: Version 3*.
- [ITU-T H.248.14] Recommendation ITU-T H.248.14 (2009), *Gateway control protocol: Inactivity timer package*.
- [ITU-T H.248.37] Recommendation ITU-T H.248.37 (2008), *Gateway control protocol: IP NAPT traversal package*.
- [ITU-T H.248.40] Recommendation ITU-T H.248.40 (2013), *Gateway control protocol: Application data inactivity detection package*.
- [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.248.97] Recommendation ITU-T H.248.97 (2016), *Gateway Control Protocol: ITU-T H.248 support for control of SCTP bearer connections*. [IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.
- [IETF RFC 3556] IETF RFC 3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth*.
- [IETF RFC 3605] IETF RFC 3605 (2003), *Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)*.
- [IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol*.
- [IETF RFC 4787] IETF RFC 4787 (2007), *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*.
- [IETF RFC 5245] IETF RFC 5245 (2010), *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols*.
- [IETF RFC 5389] IETF RFC 5389 (2008), *Session Traversal Utilities for NAT (STUN)*.
- [IETF RFC 5766] IETF RFC 5766 (2010), *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*.
- [IETF RFC 5780] IETF RFC 5780 (2010), *NAT Behavior Discovery Using Session Traversal Utilities for NAT (STUN)*.
- [IETF RFC 6544] IETF RFC 6544 (2012), *TCP Candidates with Interactive Connectivity Establishment (ICE)*.
- [IETF RFC 6888] IETF RFC 6888 (2013), *Common Requirements for Carrier-Grade NATs (CGNs)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 full trickle ICE mode [b-IETF trickle-ice]: Regular mode of operation for *trickle ICE* agents, used in opposition to the *half trickle mode* of operation.

3.1.2 half trickle ICE mode [b-IETF trickle-ice]: A *trickle ICE* mode of operation where the *offerer* gathers its first generation of candidates strictly before creating and sending the offer. Once sent, that offer can be processed by *vanilla ICE* agents and does not require support for [b-IETF trickle-ice]. It also allows *trickle ICE* capable *answerers* to still gather candidates and perform connectivity checks in a non-blocking way, thus roughly offering "half" the advantages of trickle ICE. The mechanism is mostly meant for use in cases where support for trickle ICE cannot be confirmed prior to sending a first offer.

3.1.3 NAT traversal [b-ITU-T Y.2111]: The operation of adapting the IP addresses so that the packets in the media flow can pass through a far-end (remote) NAT.

3.1.4 network address translation [b-ITU-T Y.2111]: The operation by which IP addresses are translated (mapped) from one address domain to another address domain.

3.1.5 pinhole [ITU-T H.248.37]: A configuration of two associated H.248 IP terminations within the same context, which allows/prohibits unidirectional forwarding of IP packets under specified conditions (e.g., address tuple).

3.1.6 STUN agent [IETF RFC 5389]: An entity that implements the STUN protocol. The entity can be either a *STUN client* or a *STUN server*.

3.1.7 STUN client [IETF RFC 5389]: An entity that sends STUN requests and receives STUN responses. A *STUN client* can also send indications.

3.1.8 STUN consent freshness [IETF RFC 7675]: Maintaining and renewing *consent* over time. *Consent* relates to the mechanism of obtaining permission from the remote endpoint to send non-ICE traffic to a remote transport address. Consent is obtained using ICE. Note that this is an application-level consent; no human intervention is involved.

3.1.9 STUN server [IETF RFC 5389]: An entity that receives STUN requests and sends STUN responses. A *STUN server* can also send indications.

3.1.10 symmetric NAT [IETF RFC 3489]: A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port.

3.1.11 vanilla ICE [b-IETF trickle-ice]: The Interactive Connectivity Establishment protocol as defined in [IETF RFC 5245].

3.2 Terms defined in this Recommendation

3.2.1 ICE-full (mode, implementation): The ICE protocol capability set that performs the complete set of ICE requirements according to section 4.1 of [IETF RFC 5245].

NOTE – This definition is based on section 3 of [IETF RFC 5245]: "*Full: An ICE implementation that performs the complete set of functionality defined by this specification.*" The RFC uses the term "full ICE" to reference this functionality.

3.2.2 ICE-lite (mode, implementation): The ICE protocol capability set that performs the subset of ICE requirements according to section 4.2 of [IETF RFC 5245].

NOTE – This definition is based on section 3 of [IETF RFC 5245]: "*Lite: An ICE implementation that omits certain functions, implementing only as much as is necessary for a peer implementation that is full to gain the benefits of ICE. Lite implementations do not maintain any of the state machines and do not generate connectivity checks.*"

3.2.3 trickle ICE: The extended ICE protocol capabilities, beyond *vanilla ICE*, as defined in [b-IETF trickle-ice]. Trickle ICE includes half trickle and full trickle ICE modes.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

L4	(Protocol) Layer 4 (= IP transport protocol layer)
L4+	Upper Layers versus L4
ABNF	Augmented Backus-Naur Form
B2BIH	Back-to-Back IP Host
B2BUA	Back-to-Back User Agent
CRLF	Carriage-Return and Line-Feed (sequences)
DCCP	Datagram Congestion Control Protocol
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
FW	FireWall
GFO	Gateway Free Operation
ICE	Interactive Connectivity Establishment
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IUA	ISDN User Adaptation
LD	Local Descriptor
MG	Media Gateway
MGC	Media Gateway Controller
NAT	Network Address Translation (or Translator)
NAT-T	Network Address Translation and Traversal
O/A	Offer/Answer
PES	PSTN/ISDN Emulation Subsystem
PSTN	Public Switched Telephone Network
RD	Remote Descriptor
RMG	Residential Media Gateway
RMGC	Residential Media Gateway Controller
RTCP	RTP Control Protocol



RTO	Retransmission TimeOut [IETF RFC 5389]
RTP	Real Time Protocol
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SEP	Stream Endpoint
SIP	Session Initiation Protocol
SRTP	Secure RTP
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TURN	Traversal Using Relays around NAT
UDP	User Datagram Protocol
UA	User Agent
UE	User Equipment
UNSAF	UNilateral Self-Address Fixing
VPN	Virtual Private Network
WebRTC	Web Real-Time Communication

5 Conventions

None.

6 Toolkit usage

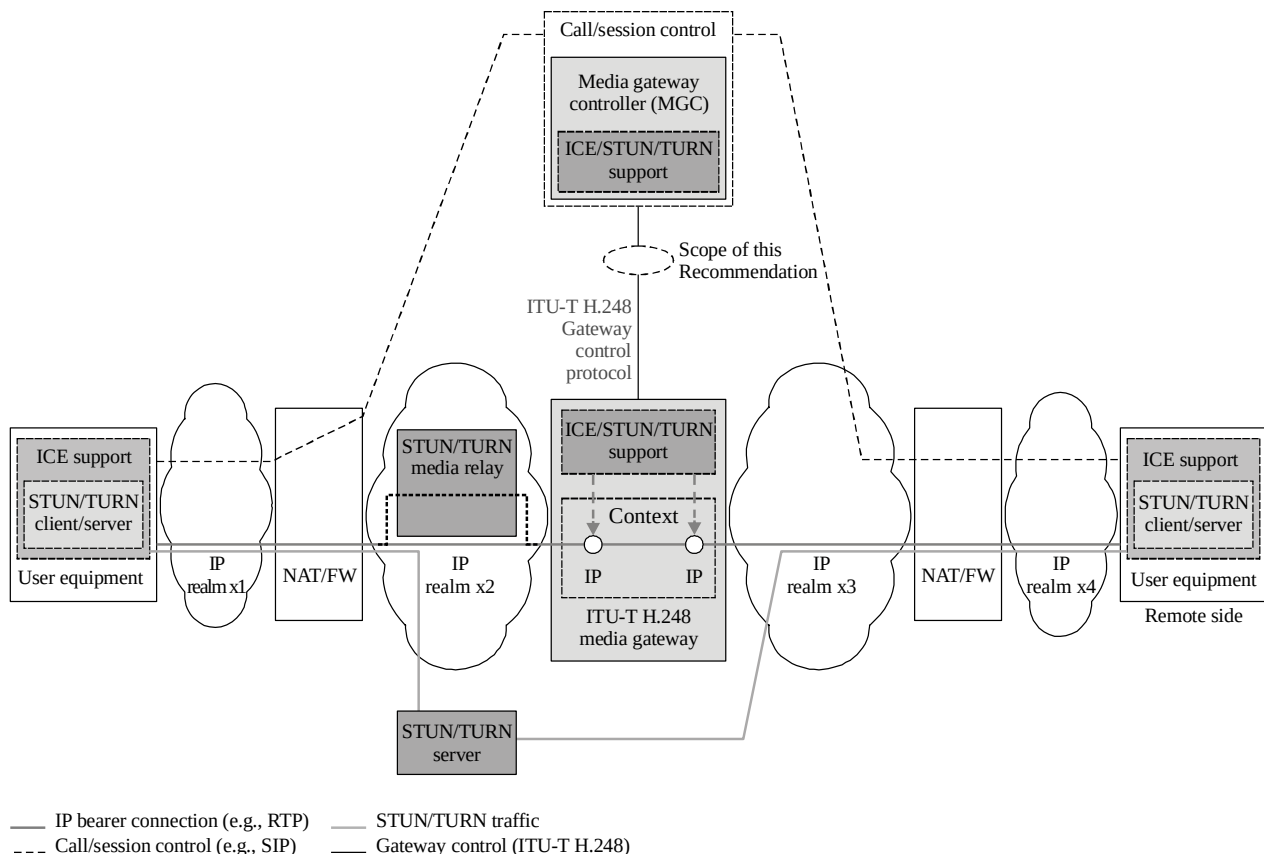
6.1 ITU-T H.248.50 usage in different network models

The ITU-T H.248 packages of this Recommendation may be applied in various network configurations. The clauses below illustrate some main scenarios.

6.1.1 ITU-T H.248 MGC/MG as interim nodes in the end-to-end path between user equipment (with STUN client/server and/or ICE support)

The NAT traversal support protocols: STUN, TURN and ICE are IP application protocols. They are fundamentally deployed in IP hosts (behind NAT device(s)) and IP network servers. The IP host function is located in the user equipment (UE) in Figure 2. The end-to-end IP bearer-path goes through an ITU-T H.248 MG (with an ITU-T H.248 IP-IP Context). There may be multiple NAT devices in the IP bearer-path (and IP signalling path(s)). Figure 2 shows an example with four IP realms, separated by two standalone NAT devices. The third NAT function is provided by the ITU-T H.248 MG.

NOTE – The MG-internal NAT function is realized by the so-called back-to-back IP host (B2BIH) mode.



NOTE 1 – IP realms: $x3 = x4$ possible.

NOTE 2 – IP realms: if $x3 \neq x4$, then MG-embedded NAT.

H.248.50(10)_F02

Figure 2 – Network model – ITU-T H.248 MGC/MG as interim nodes in the end-to-end path between user equipment (with STUN client/server and/or ICE support)

The ITU-T H.248 gateway (MGC and MG entity) may be requested to support particular STUN/TURN/ICE scenarios. For instance, the ITU-T H.248 gateway may be requested to act in a "proxy role" of the STUN client function (e.g., in case that the MG and UE would be both located in the same IP realm and when the UE could not provide the STUN client function itself).

It may be noted that the relation between the assist protocols (STUN, TURN and ICE) and the call/session control protocol (like session initiation protocol (SIP)) may vary between a loose and a tighter coupling mode, e.g., some examples with regard to the time relation:

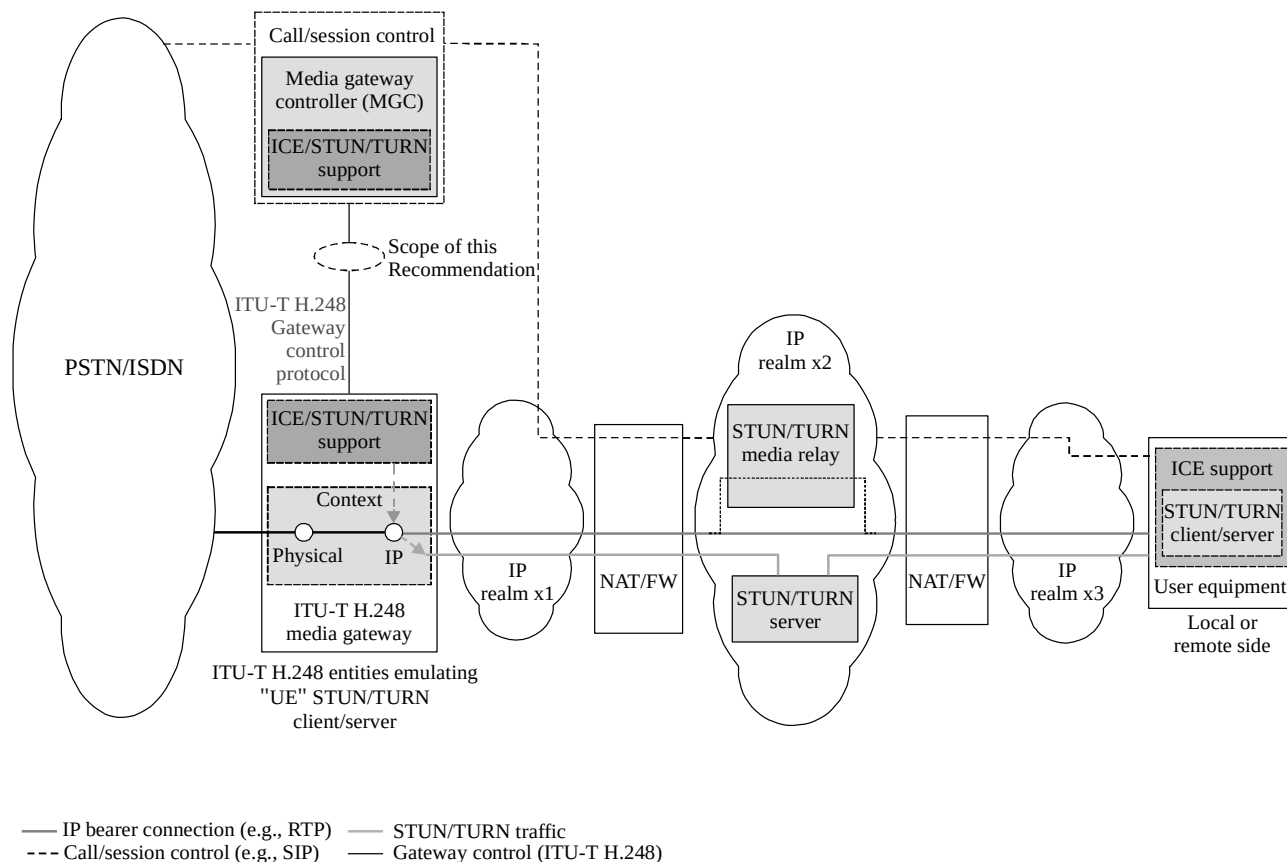
- timely tightly coupled: e.g., the ICE address gathering phase and subsequent SIP INVITE phase (before connectivity check phase);
- timely loosely coupled: e.g., the STUN keep pinhole open mechanism and NAT pinhole timer settings (which may vary between 30 seconds and the timescale of minutes and hours);
- timely de-coupled: e.g., the basic STUN mechanism for analysing the mode of operation(s) of the installed base of NAT devices.

The function of the last bullet item may be decoupled from call/session control phases and done in advance (because network topology and NAT behaviour changes rather slowly). The ITU-T H.248 gateway may be used for a NAT traversal support function on each time-scale.

6.1.2 ITU-T H.248 MGC/MG emulates a user agent (with STUN client/server and/or ICE support)

The evolution from the legacy public switched telephone network/integrated services digital network (PSTN/ISDN) to IP-based networks like the PSTN emulation subsystem (PES) or the IP multimedia

subsystem (IMS) may lead to a network model as depicted in Figure 3. The ITU-T H.248 gateway may be located at the border between the circuit-switched and IP networks. The ITU-T H.248 gateway may be requested to emulate the behaviour of IP user equipment with regard to the NAT traversal support function.



NOTE 1 – IP realms: x1 = x2 possible.
 NOTE 2 – IP realm: x2 ⇒ typically public address realm.

H.248.50(10)_F03

Figure 3 – Network model – ITU-T H.248 MGC/MG emulates a user agent (with STUN client/server and/or ICE support)

It may be noted that the TURN media relay function is outside of the ITU-T H.248 gateway and provided by a separate network server in the previous two examples.

6.1.2.1 Scenario when MG and MGC located in different IP realms

Where the MGC and MG are in different IP realms, the ITU-T H.248 signalling and media flows may traverse the same NAT/firewall (FW) (see also Figure 4, using the example of a residential media gateway (RMG)). The techniques described in this Recommendation may be used for media flow NAT/FW traversal. Signalling (call/session) NAT traversal is generally not in the scope of this Recommendation, however ITU-T H.248 NAT traversal may benefit from the use of ITU-T H.248-based peer-to-peer polling mechanisms (like e.g., [ITU-T H.248.14] or empty audits on ITU-T H.248 level, or e.g., stream control transmission protocol (SCTP) indications on transport connection level) in order to maintain NAT bindings. Opening of the NAT binding for ITU-T H.248 traffic would be subject of the initial ServiceChange messages for MG registration.

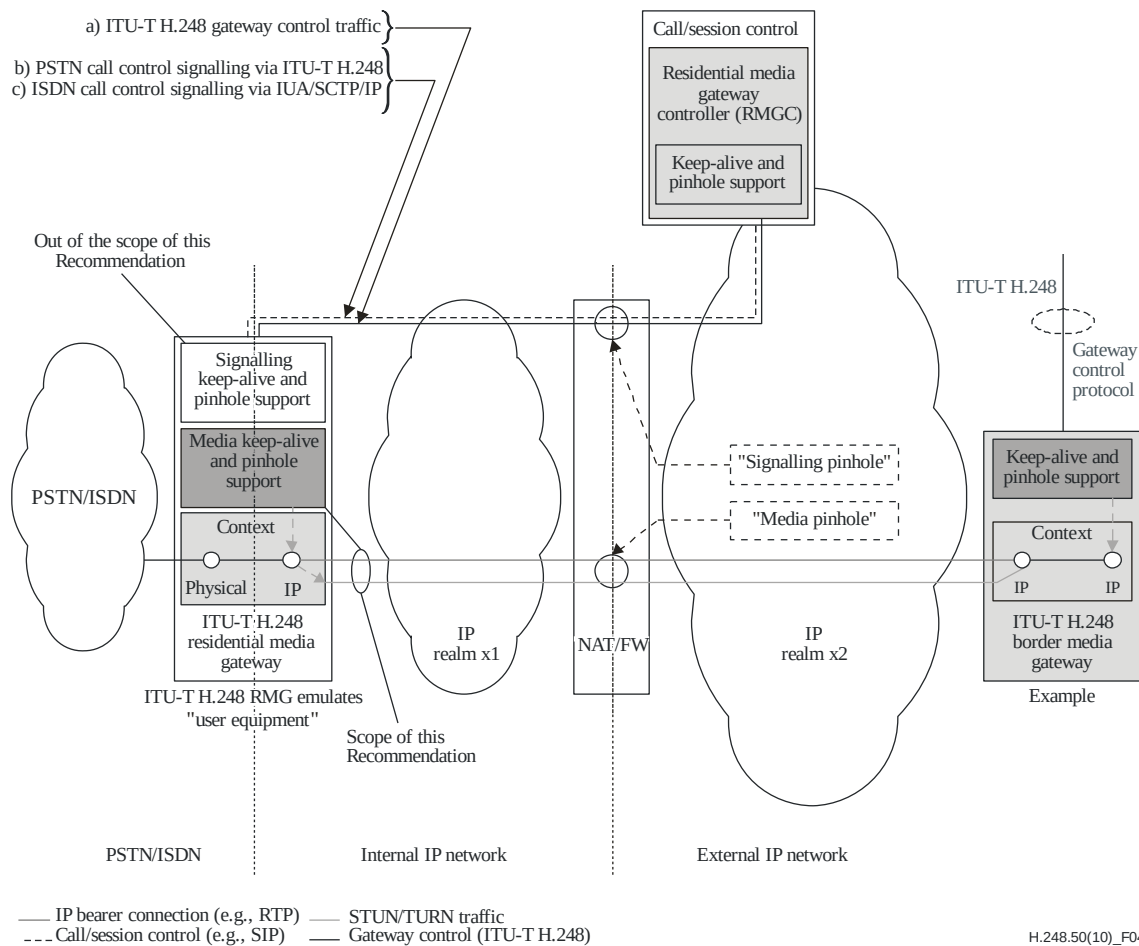
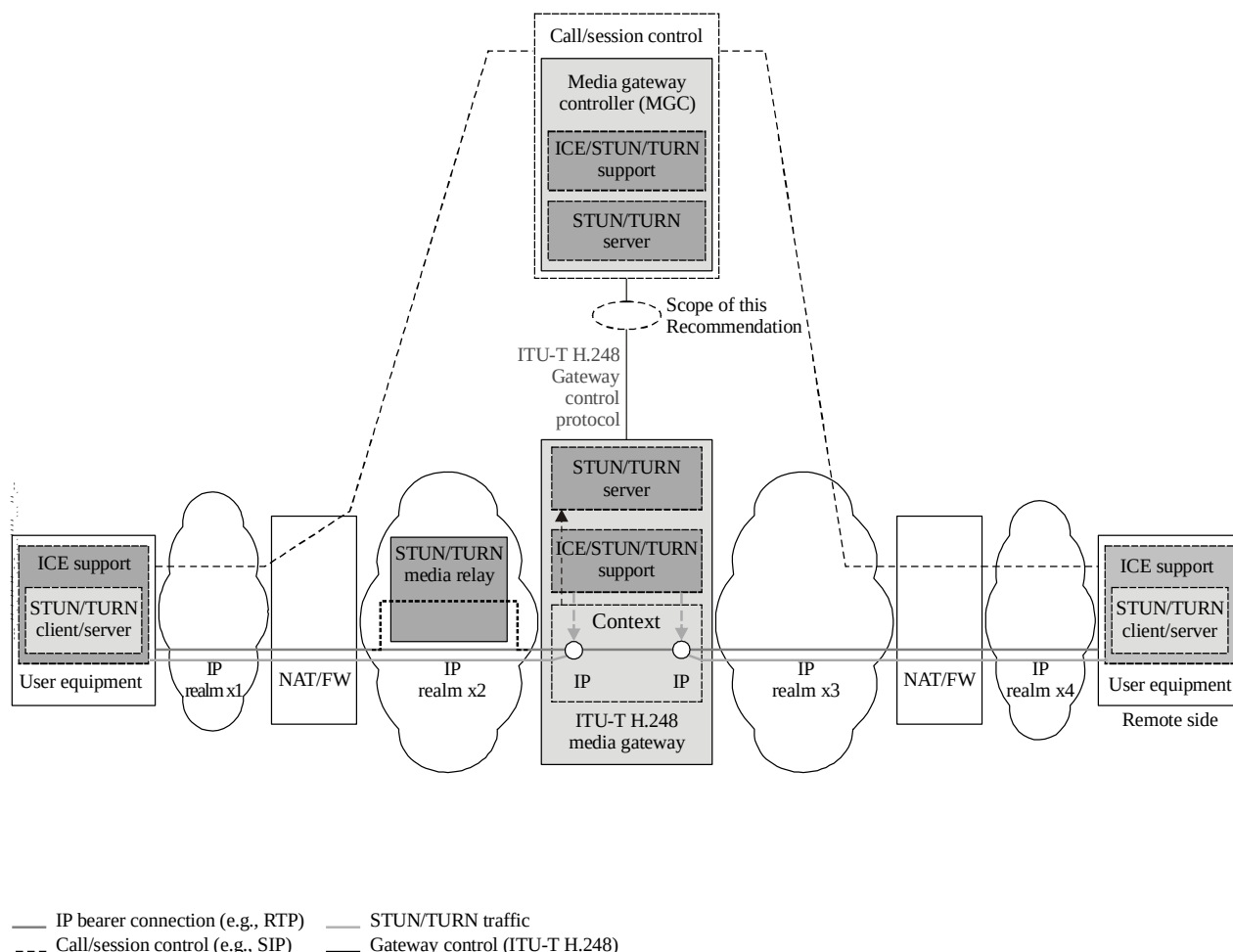


Figure 4 – Network model – Scenario when MG and MGC are located in different IP realms – Keep-alive and pinhole support

Keep "pinhole open" mechanisms for media IP flows are in scope of this Recommendation. Keep "pinhole open" mechanisms for signalling IP flows are out of scope of this Recommendation; such methods may be e.g., addressed by correspondent ITU-T H.248 profile specifications for such ITU-T H.248 gateways.

6.1.3 ITU-T H.248 MGC/MG provides STUN/TURN server functionality

The STUN/TURN server function could be principally embedded in a MG, MGC or gateway (MGC/MG tandem), see Figure 5.



NOTE 1 – IP realms: x3 = x4 possible.

NOTE 2 – IP realms: if x3 ≠ x4, then MG-embedded NAT.

H.248.50(10)_F05

Figure 5 – Network model – ITU-T H.248 MGC/MG provides STUN/TURN server functionality

The STUN server function requires the processing of incoming STUN Binding Request messages and the reply by correspondent STUN Binding Response messages. In case of NAT devices in "symmetric NAT" mode, additional support by TURN is required. The TURN server function requires the processing of TURN messages (Allocate Request, Allocate Response and Send Request).

The STUN server and TURN server functions may be provided by an ITU-T H.248 gateway on a MG or MGC level (as indicated in Figure 5). However, the TURN media relay function should be out of scope of MGC nodes (see clause 6.1.4).

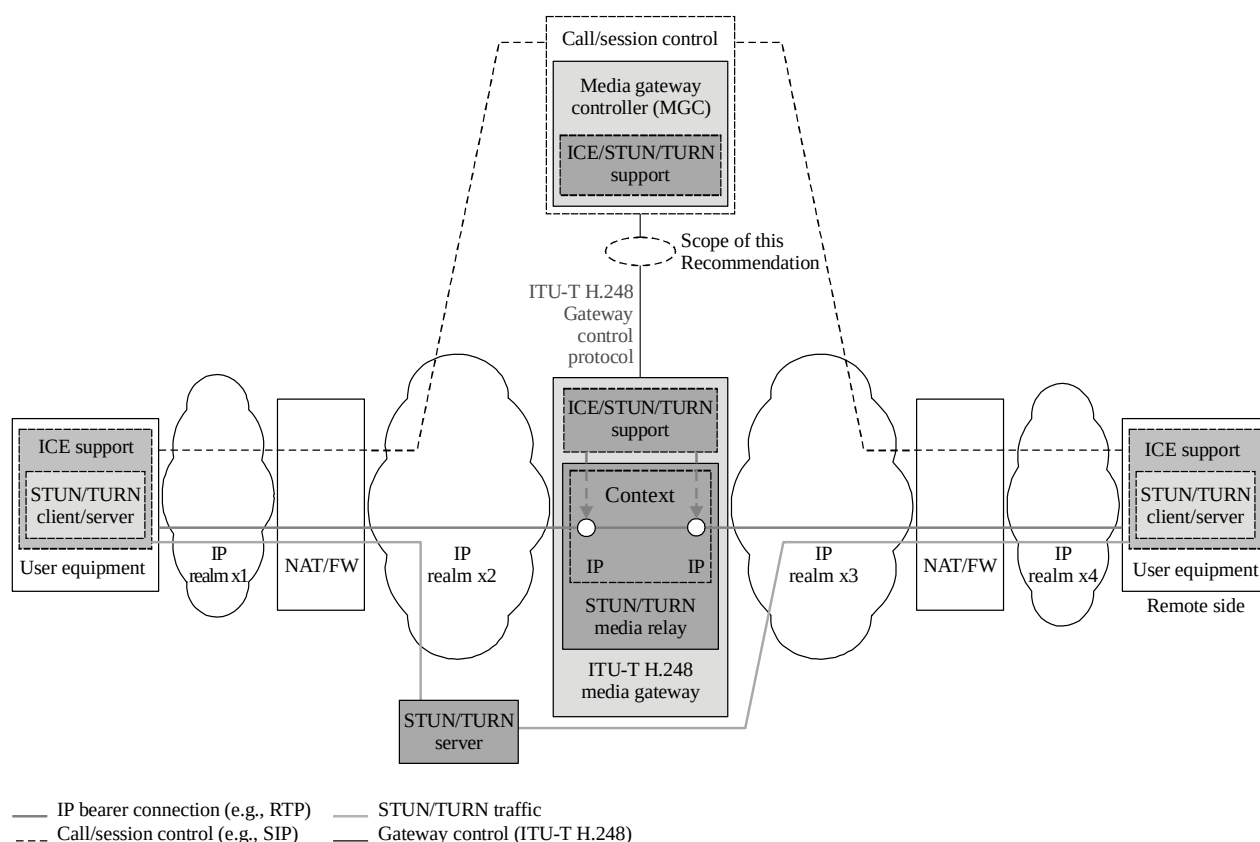
The advantage of a STUN/TURN server at MGC level is the close location to call/session control. For instance, it may be beneficial to have information available concerning interim NAT devices and their behaviour, NAT binding lifetime information (e.g., a TURN attribute) or IP address usage. A close location of possible SIP server function (like a SIP proxy, application level gateway or back-to-back user agent (B2BUA) function) and STUN/TURN servers may also be beneficial.

The advantage of a STUN/TURN server at MG level may be e.g., driven by a functional sharing performance model for off-loading the MGC node from STUN/TURN message processing functions, or e.g., the coupling of a TURN server and TURN media relay in an ITU-T H.248 MG node.

6.1.4 ITU-T H.248 MG provides TURN media relay functionality

The TURN media relay function may be embedded in a MG itself, see Figure 6. The TURN media relay function is inserted in the end-to-end IP bearer-path. The decision for routing the IP bearer connection over a TURN media relay is either already known before call/session establishment, or done during that phase due to a call/session-driven STUN process. The TURN media relay function may require substantial resources for processing and forwarding IP bearer path packets. This is the primary reason for excluding such a function from MGC entities.

There are on the other side many good reasons for combining the TURN media relay function and ITU-T H.248 MG function. For example, this is because the MG may inherently provide the TURN media relay NAT function, or because of a "simpler" IP bearer-path routing process, or due to QoS reasons (e.g., the native TURN media relay provides only coarse support for bearer-path resource reservation by the single attribute "Bandwidth", but is lacking support for session-dependent policing functions per se), or the ability of the MGC to access TURN media relay server information.



NOTE 1 – IP realms: $x3 = x4$ possible.

NOTE 2 – IP realms: if $x3 \neq x4$, then MG-embedded NAT.

H.248.50(10)_F06

Figure 6 – Network model – ITU-T H.248 MG provides TURN media relay functionality

6.1.5 "STUN server" capability

A network domain may provide one or multiple STUN server(s). A STUN server may be realized as a non-ITU-T H.248 network element or as ITU-T H.248 entity-embedded STUN server functions (in context of this Recommendation). For instance, the STUN agent provided by the MG is then called "MG act-as STUN server" function.

The STUN service(s) may be provided by a single or multiple STUN servers; typically, dependent on the network configuration and/or STUN application.

The internal modeling of the STUN protocol in "service categories" (protocol functions) is difficult; however, STUN server functions could be classified in *call-independent* and *call-dependent*

categories. It should be noted that such a classification scheme is not useful in general, but suitable in the context of ITU-T H.248 gateways.

The call-dependent category relates to the ICE connectivity check and has to be performed by the entity in the call/session control path that terminates ICE, either the ICE end point located in a terminal or a gateway, (e.g., a session border gateway). Providing a single STUN server in the network domain thus implies that call control signalling corresponding to all call/sessions using ICE has to be routed through that gateway (such as in Figure 5), unless the end point itself provides the server functionality.

An example of STUN server function distributions for STUN application 'ICE' according to the network model in Figure 2 (see also description of the scenario in clause 6.1.1 or Appendix I.1):

A stand-alone "STUN server" is involved during the STUN-based address gathering phase. And the ITU-T H.248 MG as "STUN server" is involved during the STUN-based connectivity check phase. The first STUN server function is "call-independent" because it actually occurs before any call control signalling (from MGC perspective), and the second STUN server function is "call-dependent" because associated with call control signalling.

The STUN server involved during STUN-based address gathering phase could also be provided by an ITU-T H.248 MG entity (such as in case of Figure 5).

6.1.6 ICE capability set: ICE full vs ICE lite

ICE allows two explicit modes of operations, where "ICE full" represents the complete capability set and "ICE lite" a subset of "ICE full". [IETF RFC 5245] defines an explicit signalling element (session description protocol (SDP) "a=ice-lite" attribute) for ICE mode support indication. The omission / inclusion of this SDP attribute in SIP signalling indicates ICE full / lite support. However, [IETF RFC 5245] does not provide a detailed description of the behaviour of the ICE lite mode; the information is rather distributed across the entire ICE RFC.

NOTE – The rationale behind this is the expectation that ICE lite is only a temporary implementation step which should evolve to ICE full support. This assumption might be valid for terminal-embedded ICE agents, but not necessarily valid for gateway-embedded ICE support as in scope of this Recommendation.

Appendix III describes the differences between the two ICE modes at the level of detail of interest to ITU-T H.248 gateways.

6.1.7 Principal network models concerning location of ICE endpoints

ICE represents a single algorithm, distributed over two ICE agents in a network. There are two main models concerning the mapping of the two ICE agents to the network topology (Table 1):

This aspect should be taken into account when looking at the use cases in clauses 6.1.1 to 6.1.4.

Table 1 – Network models concerning location of ICE endpoints

Model	Characteristics	Comments
Terminal-to-terminal (peer-to-peer)	Both ICE endpoints are located in terminal embedded IP host entities	This is the base model of IETF for the design of ICE. All IETF "ICE RFCs" use this model.
Terminal-to-network	One ICE endpoint is located in IP network infrastructure equipment, such as an ITU-T H.248 IP-to-IP media gateway (acting as B2BIH or IP router) within the end-to-end IP media path. This leads to following consequences: - The end-to-end IP media path is divided (by the ITU-T H.248 MG) in two segments: "ICE segment"; and "another non-ICE based segment". - Special case: both segments use an ICE-based NAT traversal independent of each other.	Major difference to the IETF base model: the MG might not be "located behind a NAT" (from the perspective of ICE), and thus be always reachable ("full IP connectivity without ICE-based NAT traversal support").

6.2 Overview of toolkit NAT traversal techniques

This Recommendation describes the various mechanisms used in order to secure media flow traversal of networks where NATs are used. In essence, the packages described provide a toolkit for the MGC to use in order to: gather a list of potential NAT mapped address (address gathering), check connectivity associated with those addresses, and maintain the connectivity associated with those addresses. The Recommendation is structured around the various techniques that have been defined:

- 1) STUN usage according to [IETF RFC 3489];
- 2) STUN usage according to [IETF RFC 5389];
- 3) TURN usage according to [IETF RFC 5766];
- 4) ICE techniques according to [IETF RFC 5245].

NOTE – At the time of publication of this Recommendation, this RFC was being updated by [b-IETF RFC 5245bis] and [b-IETF ice-sip-sdp]. These updates are out of scope of this Recommendation.

- 5) Other techniques used to maintain connectivity.

These techniques have typically not considered the scenario where the media flows are initiated from a split MGC and MG.

6.3 ITU-T H.248 call/bearer separation, connection model and IP addresses for ephemeral terminations

The splitting of the so-called "user agent" functionality into a control and media components means that there needs to be coordination between the two components. As the MGC usually constructs call and session control messages, it must be able to request information from the MG in order to build these messages. For instance, it would need address and media information to place in an SDP offer.

Media gateways typically support several different source/destination IP address/port combinations per peer-to-peer media connection. This may be due to different media (e.g., audio or video), different single media capabilities (codec A versus codec B) and to handle events (e.g., real time protocol (RTP) control protocol (RTCP)). These capability sets may be advertised to a remote party which selects the appropriate media set to use. In order for media connectivity to be successful for any of the sets, any media stream that encounters a NAT should have its address mapped. At a call/session



level, a correlation is given between the local "native" IP address/ports of the MG and the mapped addresses. Such a scheme is detailed in section 4.3 of [IETF RFC 5245]. The use of ITU-T H.248 between a MGC and MG introduces a connection model that needs to be considered when correlating local "native" addresses and mapped addresses using ICE techniques. Furthermore, some NAT traversal techniques do not use ICE, thus this particular candidate scheme is not appropriate for them.

As such in this Recommendation, where ICE is not used, the correlation is in the form of an ordered list of values, where:

The first position on the list corresponds to the first address in the first group associated with a particular stream. The second position is associated with either a second address in the first group or, if there are no further addresses, it is associated with the first address in the second group. The parameter "Address Correlation" in the Base STUN package describes the mapping between the list position and the place in the Local Descriptor (LD).

6.4 Specific SDP information elements

6.4.1 SDP for vanilla ICE

6.4.1.1 UDP-based address candidates

Where ICE is used, the SDP CANDIDATE attribute [IETF RFC 5245] is used.

The so-called "candidate scheme" does not alter the actual media flows. That is, a MG will use the source address in the Local Descriptor to send from, and the destination address in the Remote Descriptor (RD) to send to. In the text encoding, this is the SDP connection address (c=) and media (m=) lines. Therefore, if the MGC chooses a candidate other than the local address, this shall be reflected in the Local and Remote Descriptors. This may have implications on how the media is sent. For example, if this address is a relay address, then the data may have to be sent using TURN send indications.

6.4.1.2 TCP-based address candidates

Where ICE is used for TCP [IETF RFC 6544] (see also Appendix II), the SDP CANDIDATE attribute from [IETF RFC 5245] is used with its grammar extended according to section 4.5 of [IETF RFC 6544].

6.4.2 SDP for extended ICE

6.4.2.1 Trickle ICE

Appendix IV provides some background information on trickle ICE, from the perspective of ITU-T H.248 gateways.

Where *trickle ICE* is used, the SIP-based call control signalling (according to [b-IETF trickle-ice] and [b-IETF trickle-sip]) uses the following signalling extensions in brief:

1. start of call establishment phase: indication of trickle ICE support via SDP attribute "a=ice-options:trickle";
2. trickling phase: signalling of candidate updates via SIP INFO messages; and
3. stop of trickling phase: announcing end of candidates via SDP attribute "a=end-of-candidates".

The three trickle ICE phases affect the ITU-T H.248 MGCs' SIP-based call control signalling interface only. There are not necessarily correspondent impacts on the ITU-T H.248 gateway control signalling. This seems to be rather conditional, dependent on the network configuration and IP bearer path routes. A detailed analysis of trickle ICE is for further studies.

6.5 Overview of NAT traversal support mechanisms (by ITU-T H.248 entities)

6.5.1 Address latching support

Legacy "media latching" as introduced for network infrastructures without ICE/STUN/TURN (see also [b-IETF RFC 7362]) is covered in the scope of [ITU-T H.248.37]. Clause 10.1.5 describes a STUN-specific media latching function in the context of ICE, which effectively leads to the same autonomous adaptation of IP transport addresses behaviour in the IP bearer plane.

6.5.2 Basic STUN/TURN support (ICE-less)

See clause 7.

6.5.3 ICE-controlled STUN/TURN

See clause 8. The ICE methodology defines a "superior" protocol that uses the STUN/TURN mechanism and other protocols. The use of ICE is also tightly coupled with SIP and in particular with SIP/SDP offer/answer (O/A) procedures. ICE is executed between a pair of ICE agents. There are two device types concerning the embodiment of ICE agents with respect to their location in the IP network infrastructure:

- terminal-embedded ICE agent: user equipment with ICE agent function and SIP UA function;
- gateway-embedded ICE agent: a decomposed ITU-T H.248 gateway provides the ICE agent function in a distributed manner (with the SIP signalling function located at MGC level).

This clause describes the ICE process from the perspective of a generic ICE agent, i.e., it does not differentiate between the above two embodiments (but indicates possible ITU-T H.248 impacts for the gateway-provided ICE agent).

The execution of ICE may be basically divided into several consecutive phases:

- 1) Gather addresses
 - Purpose: Address gathering.
 - This phase may be based on STUN and/or TURN procedures as required.
 - Used ITU-T H.248.50 packages: None.
- 2) Prioritizing addresses
 - Purpose: optimize final IP bearer path (routing).
 - Function provided either by
 - a) MG, in case of a MGC request via SDP CANDIDATE attribute (MG needs to provide then the STUN server discovery, see clause 8); or
 - b) MGC, in its capacity as "ICE endpoint" and SDP O/A processing; or
 - c) external (SIP) server, in case of a network deployment model where the address gathering and prioritization functions are provided by non-ITU-T H.248 entities;
 - Used ITU-T H.248.50 packages: SDP "a=candidate:" attribute and *ostuncc* package (because the STUN connectivity checks result in priority value assignments).
 - Address prioritization rules: The basic rules for address prioritization are described in section 4.1.2.1 of [IETF RFC 5245]. The purpose of ICE multihomed and IPv4/IPv6 dual stack fairness support may require other prioritization algorithms, see [b-IETF ice-dualstack] and Appendix V. The applicable prioritization rules should be explicitly part of an ITU-T H.248 profile specification in case that an ITU-T H.248 entity is responsible for that ICE function.
- 3) Call/session control signalling: generate SDP Offer (for SIP signalling)
 - Purpose: generate SDP Offer content (if originating side).

- Multiple SDP attributes may be involved: the basic ICE protocol introduces seven ICE-specific SDP attributes (see [IETF RFC 5245]).

NOTE 1 – The values of media-level ICE SDP attributes could be requested from the MGC and provided by the MG, whenever the MG is involved in the resource management of such information.

- Used ITU-T H.248.50 packages: None (due to application control protocol related function).
- 4) Call/session control signalling: Negotiations – Offering and Answering (initiate and accept SIP messages)
- Purpose: Address advertisement.
 - This phase is typically related to the initiation of a SIP INVITE (thus, out of scope of this Recommendation).

NOTE 2 – The peer user (called party, invited party) may also start a correspondent "address gathering" procedure (based on STUN and/or TURN as required). These remote procedures would not be visible for the local MGC/MG entities.

- The peer (SIP) user may reply with a SIP OK (thus, out of scope of this Recommendation).
 - Used ITU-T H.248.50 packages: None (due to application control protocol related function).
- 5) Connectivity checks
- This phase is again based on STUN and/or TURN procedures as required.
 - The connectivity checks are based on the same 4-tuple(s) as (later) used for the ITU-T H.248 stream.
 - The STUN/TURN messages may be thus multiplexed into the RTP/RTCP packet flow of the checked ITU-T H.248 stream (of an ITU-T H.248 RTP termination).
 - Used ITU-T H.248.50 packages: mgastuns, ostuncc.
- 6) Completing ICE procedures
- One agent assumes ICE *controlling* role, other agent assumes ICE *controlled* role.
 - Table III.1, table section 6 lists additional functions as part of the ICE completion phase.
 - Used ITU-T H.248.50 packages: None or indirectly because ICE completion is subject of call control signalling between the two ICE endpoints.

NOTE 3 – The ICE completion process could result in the conclusion that the routed IP bearer path could possibly finally bypass the MG instance, which was initially involved in the above ICE procedural steps. The initially created ITU-T H.248 Context would be then obsolete from an ICE perspective, which could result in MGC performing either of the following actions:

- a) the deallocation of the MG (which may be termed as gateway free operation (GFO)), or
 - b) the ITU-T H.248 stream is enabled for a transparent forwarding mode of operation.
- 7) Bearer connection: check/selection of media streams
- Used ITU-T H.248.50 packages: None.

The outlined, high level ICE process is not detailed concerning possible differences from ICE mode perspective. The ICE mode impact on gateway-embedded ICE agents is described in Appendix III.

7 STUN and TURN support

The packages defined in this clause allow the use of STUN and TURN techniques without the need for support of ICE and associated SDP, e.g., Candidates are not used.

7.1 STUN base package

Package name: STUN Base

Package ID: stunb (0x00bd)