International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.50

Corrigendum 1

(02/2012)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Gateway control protocol: NAT traversal toolkit packages

Corrigendum 1: Corrections and clarification

Recommendation ITU-T H.248.50 (2010) – Corrigendum 1

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

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

Recommendation ITU-T H.248.50

Gateway control protocol: NAT traversal toolkit packages

Corrigendum 1

Corrections and clarification

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. Any of these packages may be utilized in any order to gather and map addresses, as well as maintain connectivity with and through NATs.

Corrigendum 1 (2012) corrects several defects found in the Recommendation and, in particular, it adds descriptions for packages, properties, signal, events and parameters in order to align with the ITU-T H.248 packages template.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.248.50	2010-09-13	16
1.1	ITU-T H.248.50 (2010) Cor. 1	2012-02-13	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 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.248.50

Gateway control protocol: NAT traversal toolkit packages

Corrigendum 1

Corrections and clarification

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 STUN reflexive address mapping as defined in [IETF RFC 3489] and [IETF RFC 5389].

– Reflected mapping address mapping using the TURN techniques as described in [IETF RFC 5766].

– Comprehensive NAT traversal 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 this Recommendation. Every package is self-contained and does not use the extension principle.

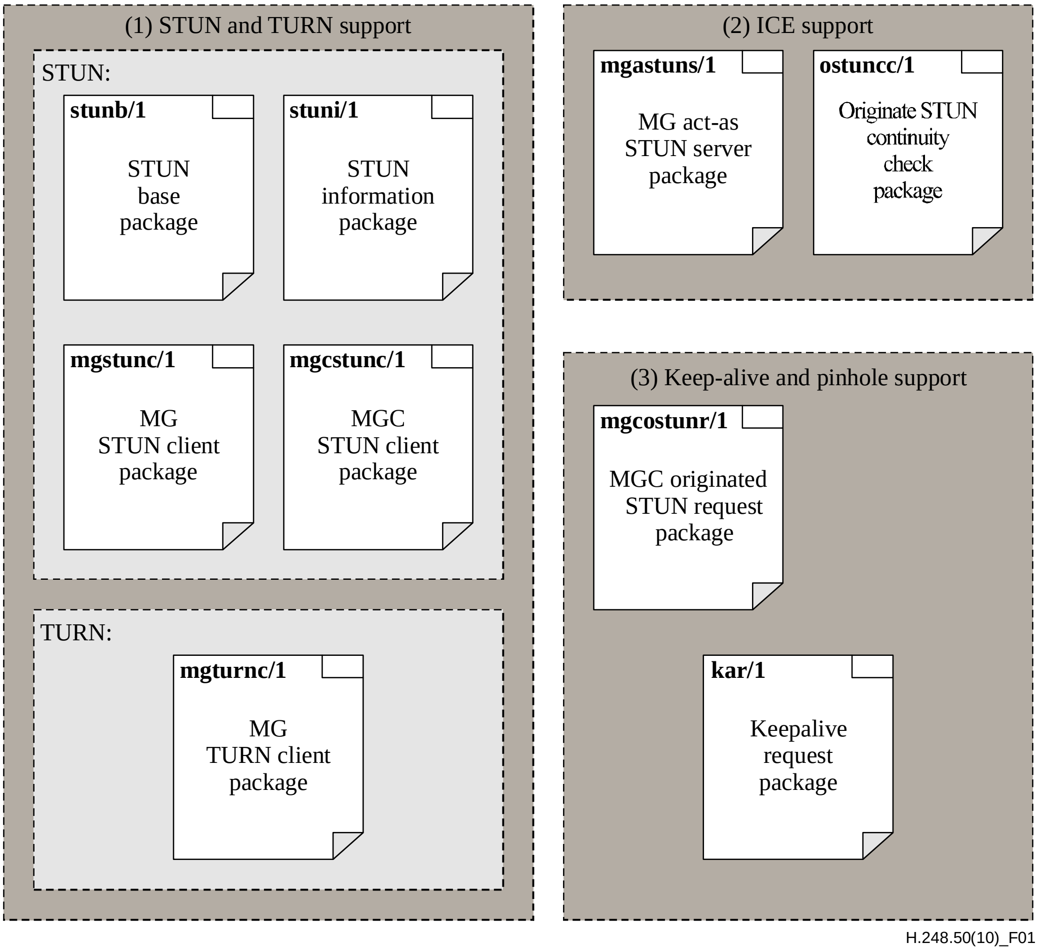


Figure 1 – Landscape of NAT traversal toolkit packages, categorized into three application areas

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 Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in next generation networks*.

[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 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).*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 NAT traversal [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.

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

3.1.3 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).

3.1.4 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.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABNF	Augmented Backus-Naur Form
B2BIH	Back-to-Back IP Host
B2BUA	Back-to-Back User Agent
DCCP	Datagram Congestion Control Protocol
DNS	Domain Name System
FW	FireWall
ICE	Interactive Connectivity Establishment
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IUA	ISDN User Adaptation
MG	Media Gateway

MGC	Media Gateway Controller
NAT	Network Address Translation
PES	PSTN/ISDN Emulation Subsystem
PSTN	Public Switched Telephone Network
RMG	Residential Media Gateway
RMGC	Residential Media Gateway Controller
RTCP	RTP Control Protocol
RTP	Real Time Protocol
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TURN	Traversal Using Relays around NAT
UDP	User Datagram Protocol
UE	User Equipment
UNSAF	UNilateral Self-Address Fixing
VPN	Virtual Private Network

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 media gateway (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.

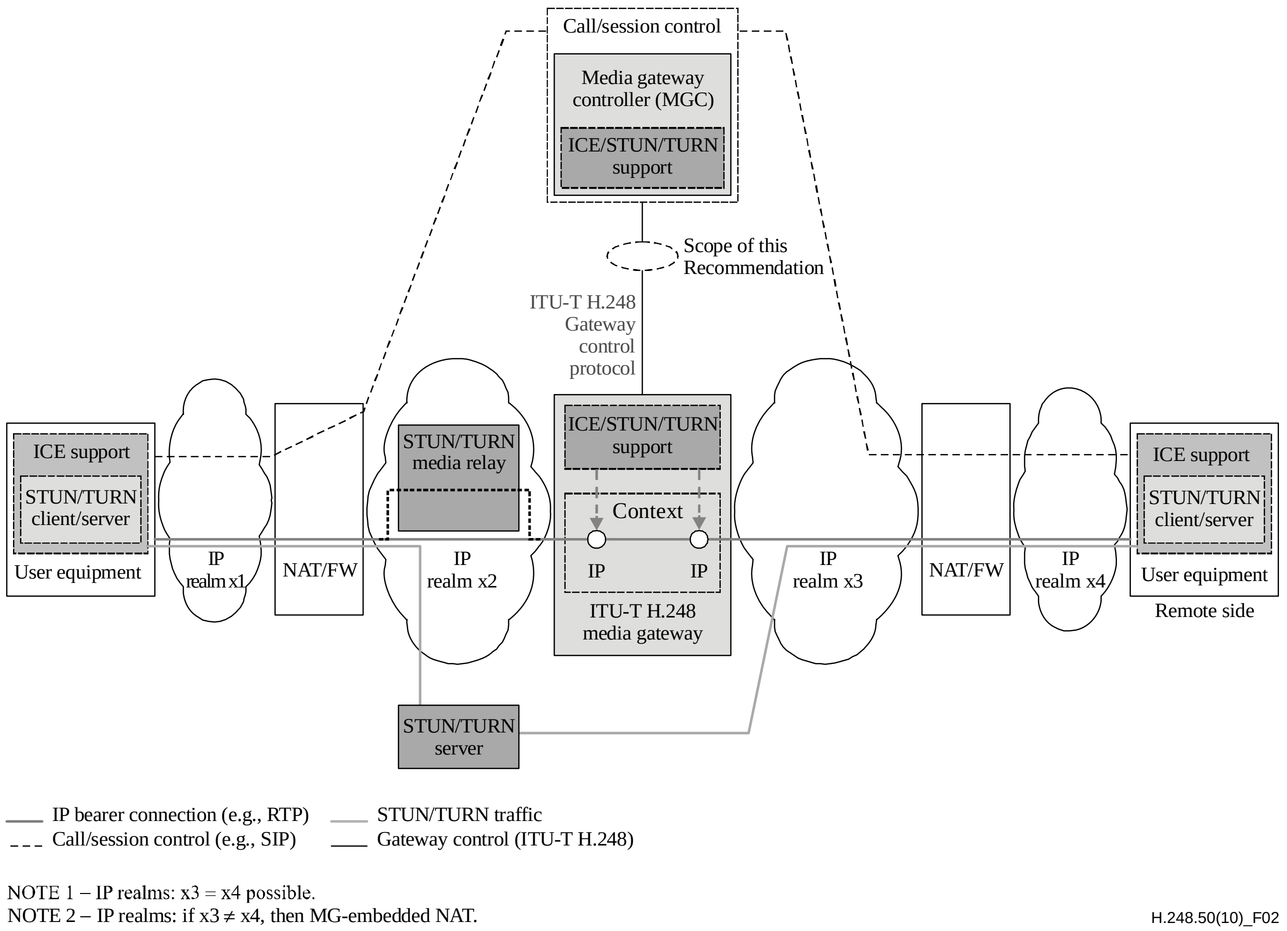


Figure 2 – Network model – ITU-T H.248 MGC/MG as interim nodes in the end-to-end path between user equipment (with STUN client/server and/or ICE support)

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 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 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.

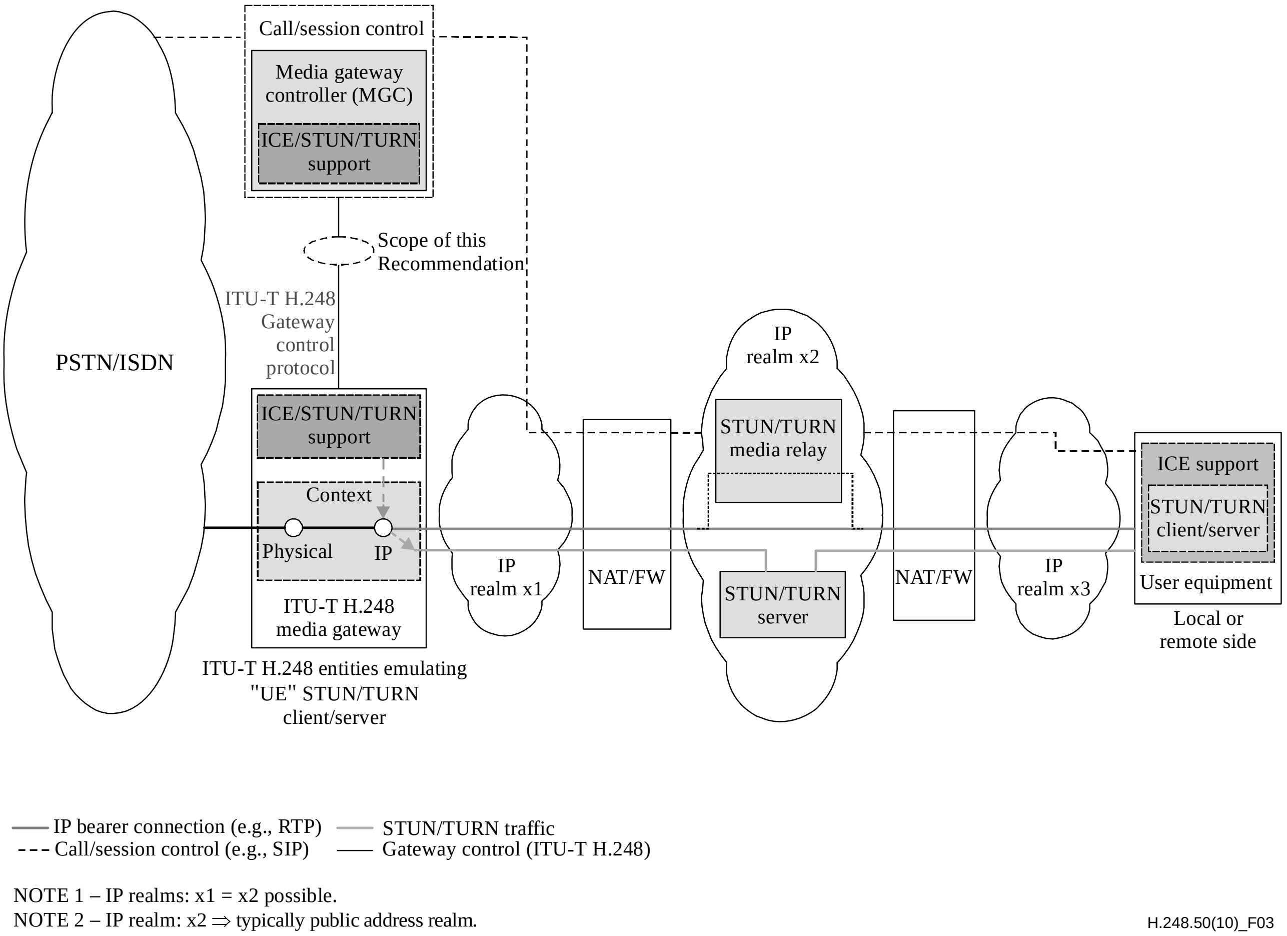

Call/session control
Media gateway controller (MGC)
ICE/STUN/TURN support
Scope of this Recommendation
ITU-T H.248 Gateway control protocol
PSTN/ISDN
ICE/STUN/TURN support
Context
Physical
IP
ITU-T H.248 media gateway
ITU-T H.248 entities emulating "UE" STUN/TURN client/server
IP realm x1
NAT/FW
IP realm x2
STUN/TURN media relay
STUN/TURN server
NAT/FW
IP realm x3
ICE support
STUN/TURN client/server
User equipment
Local or remote side
IP bearer connection (e.g., RTP)
Call/session control (e.g., SIP)
STUN/TURN traffic
Gateway control (ITU-T H.248)
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., 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.

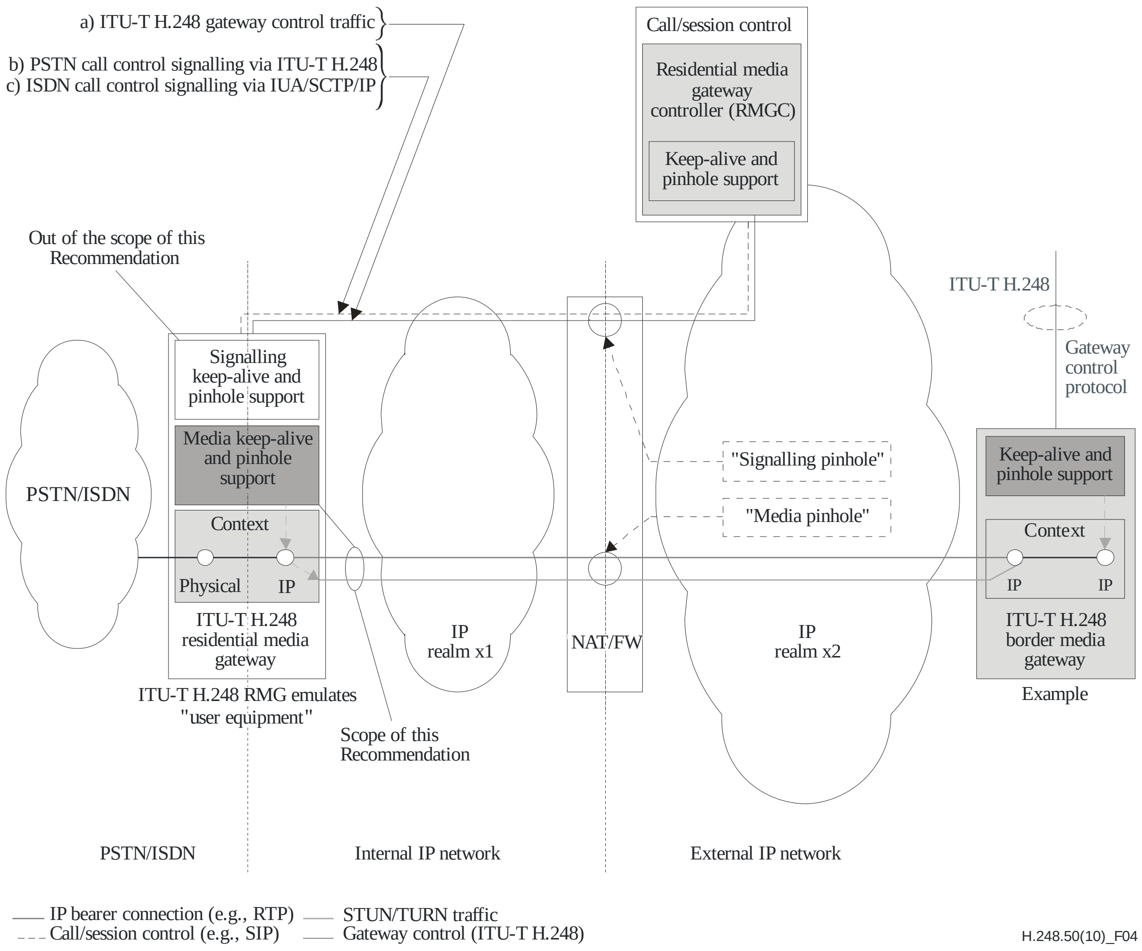
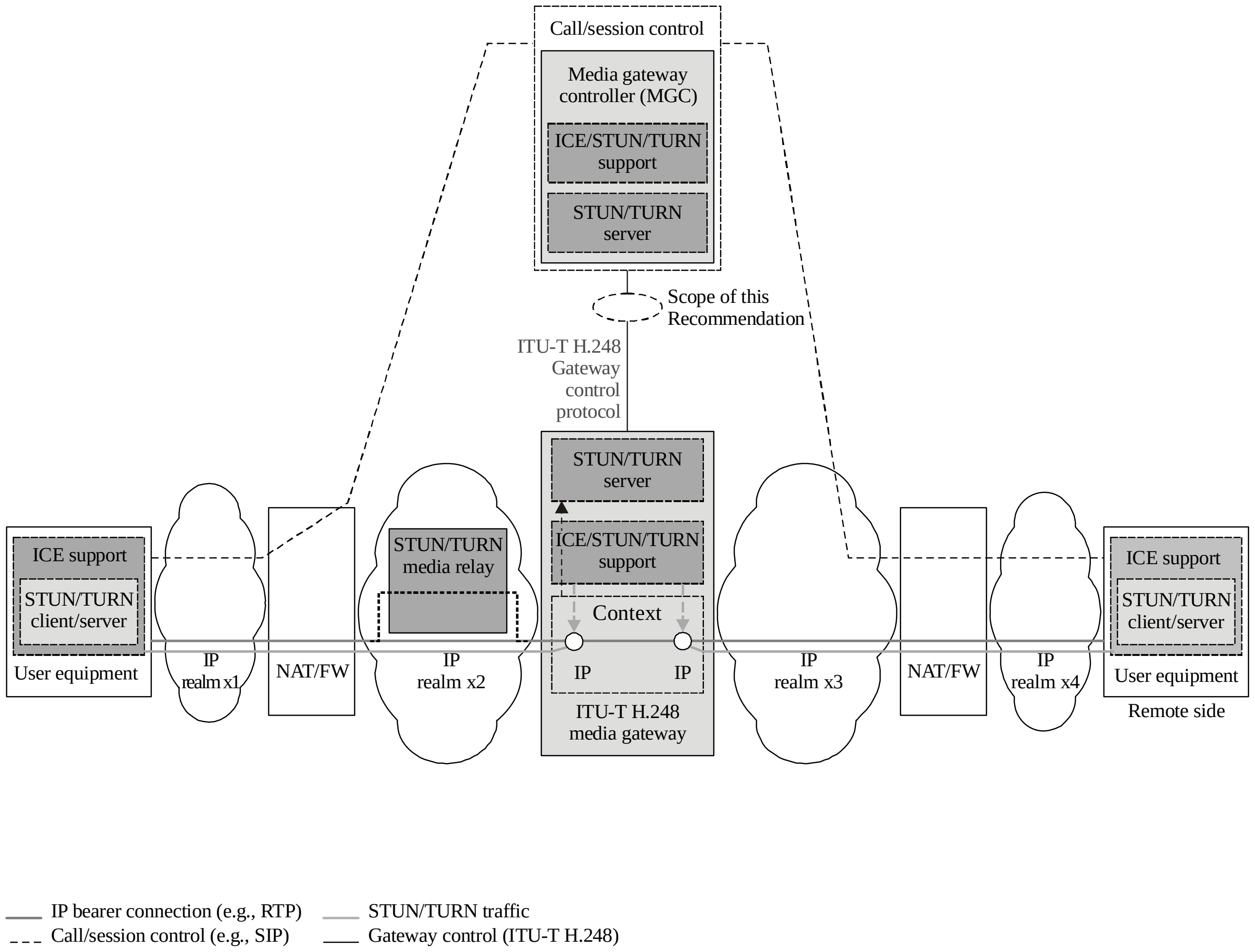

a) ITU-T H.248 gateway control traffic
b) PSTN call control signalling via ITU-T H.248
c) ISDN call control signalling via IUA/SCTP/IP
Call/session control
Residential media gateway controller (RMGC)
Keep-alive and pinhole support
Out of the scope of this Recommendation
ITU-T H.248
Gateway control protocol
Signalling keep-alive and pinhole support
Media keep-alive and pinhole support
Context
Physical
IP
PSTN/ISDN
"Signalling pinhole"
"Media pinhole"
Keep-alive and pinhole support
Context
IP
IP
ITU-T H.248 residential media gateway
IP realm x1
NAT/FW
IP realm x2
ITU-T H.248 border media gateway
Example
ITU-T H.248 RMG emulates "user equipment"
Scope of this Recommendation
PSTN/ISDN
Internal IP network
External IP network
IP bearer connection (e.g., RTP)
Call/session control (e.g., SIP)
STUN/TURN traffic
Gateway control (ITU-T H.248)
H.248.50(10)_F04

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.

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 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.

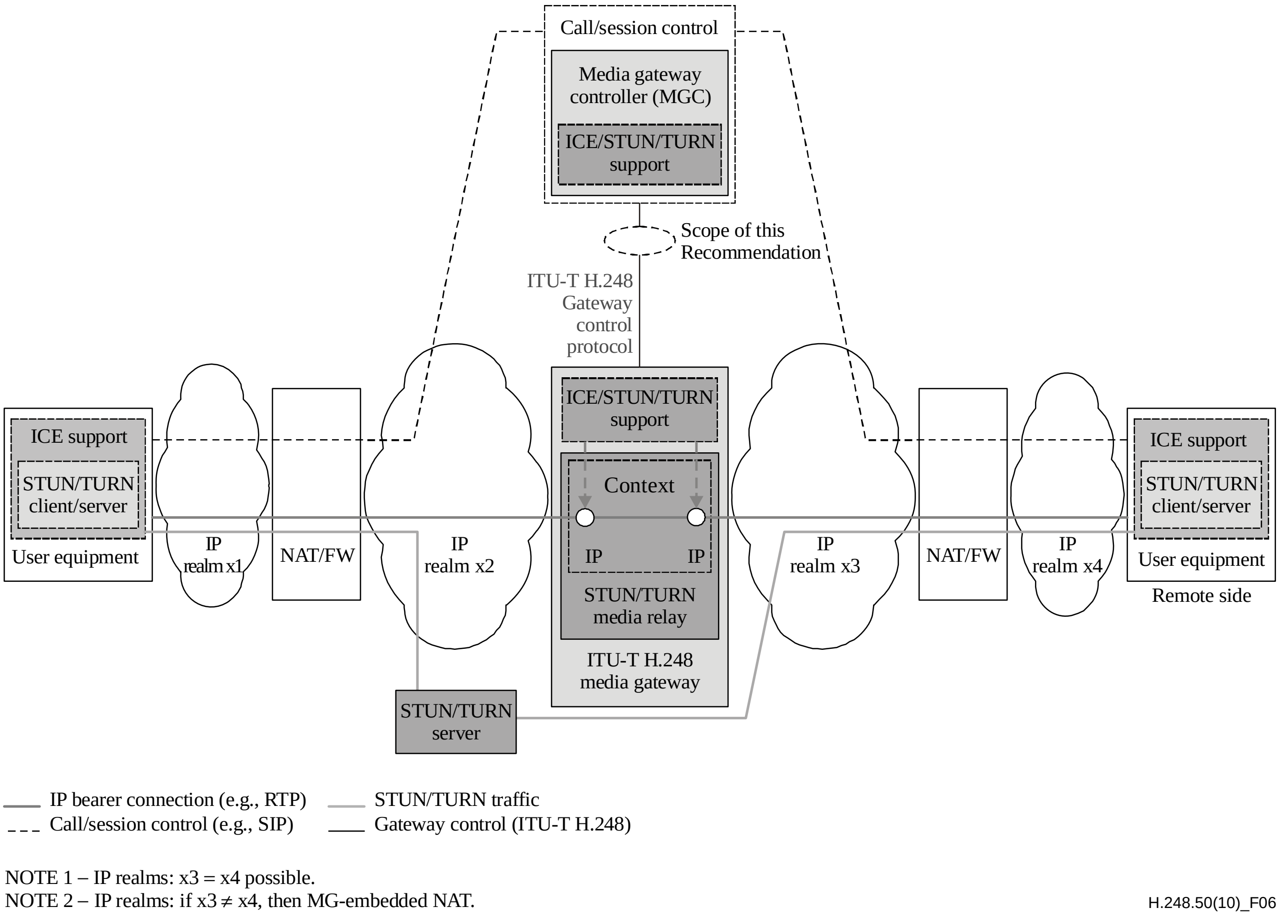


Figure 6 – Network model – ITU-T H.248 MG provides TURN media relay functionality

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].

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., 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 clause 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.

6.4 Specific SDP information elements

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 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.

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

6.5.1 Address latching support

This is covered in the scope of [ITU-T H.248.37].

6.5.2 Basic STUN/TURN support (ICE-less)

See clause 7.

6.5.3 ICE-controlled STUN/TURN

See clause 8. The ICE (interactive connectivity establishment) 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 procedures.

The execution of ICE (from a (SIP) user agent perspective) may be basically divided into a couple of 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) Call/session control signalling: 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 – 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.
3) 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.
4) Bearer connection: check/selection of media streams
   - Used ITU-T H.248.50 packages: None.

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)
Description:	This package describes the mapping between transport addresses defined in the ITU-T H.248 local descriptor and the list position when used for STUN purposes.
Version:	1

Extends: None

7.1.1 Properties

7.1.1.1 Address correlations

Property name: Address Correlation

Property ID: ac (0x0001)

Description: This property details the list position of each IP Address in the ITU-T H.248 Local Descriptor. This package may be used by the MGC to determine the mapping between local IP addresses and list positions for STUN processing purposes.

NOTE – It is not mandatory to implement this package as the MGC may determine the list positions given the logic below. However it provides a mechanism in order to check the list positions.

Type: List of String

Possible values: Each element in the list of string SHALL be type `AddressCorrelation` according to the following ABNF:

```
AddressCorrelation = Listposition "|"
        Groupnumber "|" Instance "|" ComponentID
```

Where:

List position is an integer. The first position of the list shall be 1 and sequentially rising by one.

Groupnumber is an integer and is the ITU-T H.248 group number.

Instance is an integer. The first instance of a media format (as per clause 5.14 of [IETF RFC 4566]) <fmt> field in "m=" line in a particular group shall be 1. For each subsequent media format the instance shall be incremented by one.

ComponentID is the identifier of a component. A component is a piece of a media flow requiring a single transport address. For RTP-based media flows, the RTP itself has a component ID of 1, and RTCP has a component ID of 2. For non RTP-based media flow, the component ID is 1.

The list SHALL contain an element for each IP address in the local descriptor.

For example, the values:

```
"1|1|1|1"
"2|1|1|2"
"3|1|2|1"
"4|1|2|2"
"5|2|1|1"
"6|2|1|2"
```

Would relate to the following SDP in the local descriptor::

```
v=0
c=IN IP4 192.168.1.100
m=audio 10000 RTP/AVP 4 18
v=0
```

```
c=IN IP4 192.168.1.200
m=audio 20000 RTP/AVP 0
```

The values of ReserveValue and ReserveGroup are "on".

Default: Empty String if no IP addresses are present in the local descriptor.

Defined in: LocalControl

Characteristics: ReadOnly

7.1.2 Events

None.

7.1.3 Signals

None.

7.1.4 Statistics

None.

7.1.5 Error codes

None.

7.1.6 Procedures

In order for the MGC to determine in a timely manner the correlation between local IP Address and the STUN processing list positions, the MGC shall perform a CHOOSE ($) on the "*stunb/ac*" property whenever an IP address is added/changed/deleted to/from the ITU-T H.248 local descriptor on a particular Stream/Termination.

7.2 MG STUN client package

Package name: MG STUN Client

Package ID: mgstunc (0x00be)

Description: This package enables an MGC to determine the mapped IP address and port that will be routed back to the media component that sent the request. This package applies to both [IETF RFC 3489] and [IETF RFC 5389].

Version: 1

Extends: None

7.2.1 Properties

7.2.1.1 STUN address

Property name: STUN Address

Property ID: stuna (0x0001)

Description: This property indicates that the MG shall return a STUN mapped IP address and port for each local address indicated. The MGC may send this STUN mapped IP address and port to the peer as its remote IP address and port.

NOTE – Implementors should be aware that each STUN message to a STUN server may imply a 9.5-second delay. This may impact the time in which an ITU-T H.248 command reply can be sent to the MGC. In cases where the STUN delay is excessive the use of TransactionPending is encouraged.

Type: List of String

Possible values: In an ITU-T H.248 command request:

Each element in the list of string SHALL be of type `StunAddressReq` in ABNF format:

```
StunAddressReq = "L"/("B"[COLON Stun-Transport-type])/
("S"[COLON Stun-Transport-type])
Stun-Transport-type = "UDP"/"TCP"/"TLS"
```

Where:

"L": Local Address – Do not perform STUN address mapping for the address in this position.

"B": Binding Request – Perform a STUN binding request on the address in this list position. STUN clients can communicate with a TURN server using UDP, TCP, or TLS over TCP.

"S": Shared Secret/Binding Request – Perform Shared Secret STUN messages before performing a STUN binding request on the address in this list position. The value of *STUN-TRANSPORT-TYPE* is "UDP" , "TCP" or "TLS". These values are for "Binding Requests". "Shared Secret Requests" are always sent over TLS.

In an ITU-T H.248 command reply:

Each element of the string SHALL be of type `StunAddressReply` in ABNF format:

```
StunAddressReply = (IP4-address COLON PortNumber)/ (IP6-
address COLON PortNumber)/EToken [COLON ErrorCode]
PortNumber = UINT16
EToken = "E"
ErrorCode = 1*3(DIGIT); could be extended
```

The ABNF syntax of IP4-address and IP6-address is defined in [IETF RFC 4566].

The MG may reply with an IP4 or IP6 address, for example "192.168.1.10:10000" and "FF1E:03AD::7F2E:172A:1E24:20000",

or reply with an error information in which the Class and Number of the error (see clause 11.2.9 of [IETF RFC 3489] or clause 15.6 of [IETF RFC 5389]) is included.

Default: Empty List

Defined in: LocalControl

Characteristics: Read/Write

7.2.1.2 NAT lifetime

Property name: NAT Lifetime

Property ID: natl (0x0002)

Description: This property requests the MG to return the NAT binding lifetime associated with the transport address at a particular list position.

Type: List of String

Possible values: In an ITU-T H.248 command request:

Each element may be one of the following characters:

T: "Time Request";

N: "No time request".

In an ITU-T H.248 command reply:

An integer (in string form) representing a Lifetime value,

Or:

E: "Error in list position", followed by the Class and Number of the error (clause 11.2.9 of [IETF RFC 3489] or clause 15.6 of [IETF RFC 5389]) is included in the response.

Default: Empty List

Defined in: LocalControl

Characteristics: Read/Write

7.2.1.3 RTO value

Property name: RTO Value

Description: This property requests the MG to set the initial retransmission timer RTO interval as defined in clause 7.2.1 of [IETF RFC 5389].

Property ID: rto (0x0003)

Type: Integer

Possible values: 1 ms to 600000 ms (10 minutes)

Default: 100 ms

Defined in: LocalControl

Characteristics: Read/Write

7.2.2 Events

None.

7.2.3 Signals

None.

7.2.4 Statistics

None.

7.2.5 Error codes

None.

7.2.6 Procedures

To determine a STUN mapped address, the MGC shall issue an ITU-T H.248 Add/Modify/Move.req command containing the "*stuna*" property on the relevant termination/stream. If the MG wants to modify the value of RTO, the "*rto*" property should also be set on the relevant termination/stream. The MGC shall include a value in each position of list of string for each element described in the "*stunb/ac*" property.

For list positions designated with the value "*L*", the MG shall simply return an empty string for that position of the list.

For list positions designated with the value "*B*", the MG shall perform a STUN binding request messaging. If the Binding request is successful, the MG shall return the mapped address in the list position of the reply. If the binding request is unsuccessful, then the STUN error shall be returned in the list position.

For list positions designated with the value "*S*", the MG shall perform a STUN Shared Secret request before issuing binding request messaging. The MG may perform a single Shared Secret request for all Binding requests or issue multiple Shared Secret requests. STUN server implementations based on [IETF RFC 3489] do not support Shared Secret requests.

If the MGC wishes to reset the mappings, then it shall resend the parameter in an ITU-T H.248 request indicating "*L*", "*B*" or "*S*".

If the MGC wishes to receive the period of the binding lifetime with a NAT for an address it shall issue a "*natl*" property requesting "*T*" for each list element it wants a lifetime for and "*N*" for each element it does not want the time for. On receipt of the request, the MG will determine if a binding lifetime has been determined for a particular address. It will return the binding lifetime value if received from the NAT otherwise it will return "0". It is recommended that the "*natl*" property be included after the "*stuna*" property to maximize the possibility that a binding lifetime period is returned.

If the peer side returns error code 300 (Try Alternate), the transport address of the alternate server is in the ALTERNATE-SERVER attribute. The MG should use this transport address to resend the same request message to the alternate server. If the MG cannot send or the request still fails, the MG should indicate the error code to the MGC.

STUN server implementations based on [IETF RFC 3489] may not return a binding lifetime. The STUN information package should be used in this case.

7.3 MG TURN client package

Package name: MG TURN Client

Package ID: mgturnc (0x00bf)

Description: This package enables an MGC to determine the mapped IP address and port used for data relaying through a TURN server. It enables the procedures defined by [IETF RFC 5766] to operate in a split MGC/MG environment.

Version: 1

Extends: None

7.3.1 Properties

7.3.1.1 TURN address

Property name: TURN Address

Property ID: turna (0x0001)

Description: This property requests that, for a particular local transport address and port, the MG send a TURN allocate request to a remote TURN server in order to reserve an address. As per clause 6 of [IETF RFC 5766], the MGC may send this particular local transport address and port to the peer as its remote IP address and port.

Type: List of String

Possible values: In an ITU-T H.248 command request:

Each element in the list of string SHALL be of type `TurnAddressReq` in ABNF format:

```
TurnAddressReq = ("A"
           [RequestedProps][TurnTransportType]
           [Lifetime][ChannelSend])/"N"
RequestedProps = SP "rp" COLON ReqP
TurnTransportType = SP "ttp" COLON TurnTranT
Lifetime = SP "l" COLON LifeT
ChannelSend = SP "c" COLON ChannelS
ReqP = 3* BinChar
BinChar = "0"/"1"
TurnTranT = "UDP"/"TCP"/"TLS"
LifeT = UINT32
ChannelS = "SEND"/"CHANNEL"
```

"A": Allocate Request – Perform a TURN Allocation request on the address in this list position. The REQUESTED-PROPS attribute may be indicated at the same time. The value of REQUESTED-PROPS is "000" to "111". The value of TURN-TRANSPORT-TYPE is "UDP" , "TCP" or "TLS". LIFETIME is the value of the LIFETIME attribute. The value of ChannelS is "SEND" or "CHANNEL". This flag is used to request the MG to send application data using ChannelData messages or using Send and Data indications.

"N": No change – Do not perform TURN address mapping for the address in this position.

In an ITU-T H.248 command reply:

Each element of the string contains a relay address, reflexive address and LIFETIME. Each element in the list of string SHALL be of type `TurnAddressReply` in ABNF format:

```
TurnAddressReply = ((IP4RelayAddr SP IP4ReflexiveAddr) /
(IP6RelayAddr SP IP6ReflexiveAddr) SP LifeT ) / (EToken
[COLON ErrorCode])
IP4RelayAddr = IP4-address COLON PortNumber
IP4ReflexiveAddr = IP4-address COLON PortNumber
IP6RelayAddr = IP6-address COLON PortNumber
IP6ReflexiveAddr = IP6-address COLON PortNumber
PortNumber = UINT16
LifeT = UINT32
EToken = "E"
```

The ABNF syntax of IP4-address and IP6-address is defined in [IETF RFC 4566].

The MG may reply with the relay address, reflex address and the value of LIFETIME attribute, for example "192.168.1.10:10000 192.168.2.100:20000 11000" and "FF1E:03AD::7F2E:172A:1E24:20000 FF1E:03AD::7F2E:2AB3:9AA8:20000 30000". Or it may reply with an error indication in which the class and number of the error (see clause 11.2.9 of [IETF RFC 3489] or clause 15.6 of [IETF RFC 5389]) is included.

Default: Empty List

Defined in: LocalControl

Characteristics: Read/Write

7.3.1.2 TURN refresh

Property name: TURN Refresh

Property ID: turnr (0x0002)

Description: This property requests that, for a particular local transport address and port, the MG send a TURN refresh request to a remote TURN server in order to keep the allocation and change the bandwidth or lifetime. As per clause 7 of [IETF RFC 5766], a Refresh transaction can be used to either (a) refresh an existing allocation and update its time-to-expire, or (b) delete an existing allocation. MG should send periodic refresh request for each local transport address and port automatically. The MGC may request the MG to send a special refresh request to change bandwidth or lifetime via this property.

Type: List of String

Possible values: In an ITU-T H.248 command request:

Each element in the list of string SHALL be of type `RefreshReq` in ABNF format:

```
RefreshReq = ("R"[COLON LifeT])/"N"
LifeT = UINT16
```

"R": Refresh Request – Perform a TURN refresh request on the address in this list position. Lifetime contains the value of the LIFETIME attribute. If the value of LIFETIME attribute is zero, this will cause the IP termination to remove the allocation, and all associated permissions and channel numbers. If a value for lifetime is not included a default lifetime as per [IETF RFC 5766] shall be assumed.

"N": No change – Do not perform TURN refresh request for the address in this position.

In an ITU-T H.248 command reply:

Each element of the string may be LIFETIME. Each element in the list of string SHALL be of type `RefreshReply` in ABNF format:

```
RefreshReply = LifeT/ EToken [:ErrorCode]
```

Lifetime contains the value of the LIFETIME attribute. As per clause 7.2 of [IETF RFC 5766], in a successful response, the LIFETIME attribute indicates the amount of additional time (the number of seconds after the response is received) that the allocation will live without being refreshed.

Or reply with an error information in which the Class and Number of the error (see clause 11.2.9 of [IETF RFC 3489] or clause 15.6 of [IETF RFC 5389]) is included.

Default: Empty List

Defined in: LocalControl

Characteristics: Read/Write

7.3.1.3 NAT lifetime

Property name: NAT Lifetime

Property ID: natl (0x0003)

Description: This property requests the MG to return the NAT binding lifetime associated with the transport address at a particular list position.

Type: List of String

Possible values: In an ITU-T H.248 command request:

Each element may be one of the following characters:

T:"Time Request";

N:"No time request".

In an ITU-T H.248 command reply:

A string based integer representing a Lifetime value,

Or:

E:"Error in list position", followed by the class and number of the error (clause 11.2.9 of [IETF RFC 3489]) is included in the response.

Default: Empty List

Defined in: LocalControl

Characteristics: Read/Write

7.3.2 Events

None.

7.3.3 Signals

None.

7.3.4 Statistics

None.

7.3.5 Error codes

None.

7.3.6 Procedures

To determine a TURN relayed address the MGC shall issue an ITU-T H.248Add/Modify/Move.req command containing the "*turna*" property on the relevant termination/stream. The MGC shall include a value in each position of list of string for each element described in the "*stunb/ac*" property.

For list positions designated with the value "*N*", the MG shall simply return an empty string for that position of the list.

For list positions designated with the value "*A*", the MG shall perform a TURN allocate request messaging. If the allocate request is successful the MG shall return the relayed address, reflex address and the value of LIFETIME attribute in the list position of the reply. The following attributes may be derived from the "*turna*" property:

EVEN-PORT, clause 14.6 of [IETF RFC 5766]

LIFETIME, clause 14.2 of [IETF RFC 5766]

Communication between the TURN client and the TURN server can run over UDP, TCP or TLS. *"TurnTransportType"* in the syntax of the "*turna*" property is used to indicate the desired transport type.

When the TURN client has data to send to a peer, it may use either a ChannelData message or a Send indication. *"ChannelSend"* in the syntax of the "*turna*" property is used to indicate which method should be used.

If the allocate request is unsuccessful then the TURN error shall be returned in the list position.

If the MGC wishes to reset the mappings, then it shall resend the "*turna*" property in an ITU-T H.248 request indicating "*N*" or "*A*".

To refresh an existing allocation and update its time-to-expire, or to delete an existing allocation, the MGC shall issue a Modify/Move.req command containing the "*turnr*" property on the relevant termination/stream.

For list positions designated with the value "*R*" the MG shall perform TURN refresh request messaging. If the MGC wishes the TURN server to set the time-to-expire timer to something other than the default lifetime, the MGC indicates to the MG to include a LIFETIME attribute with the requested value. If the value of the LIFETIME attribute is 0, the TURN server immediately deletes the allocation. If the refresh request is successful the MG shall return the LIFETIME attribute in the list position of the reply. If the refresh request is unsuccessful then the TURN error shall be returned in the list position.

7.4 MGC STUN client package

Package name: MGC STUN Client

Package ID: mgcstunc (0x00c0)

Description: This package enables an MGC to determine the STUN mapped IP address and port for a particular media component. This package allows the STUN client to remain at the MGC level rather than being implemented in the MG.

NOTE – This package has been included for backward compatibility reasons.

Version: 1

Extends: None

7.4.1 Properties

None.

7.4.2 Events

None.

7.4.3 Signals

7.4.3.1 MGC initiated STUN request

Signal name: MGC Initiated STUN Request

Signal ID: mgcistunr (0x0001)

Description: The MGC shall send a signal for each media component address whose address is to be mapped. These signals may occur in the same ITU-T H.248 message.

The STUN response messages are not used in this case. It is used to fulfil the case described in clause 10.3 of [IETF RFC 3489].

Signal type: Brief

Duration: Not applicable

7.4.3.1.1 Binding request message

Parameter name: Binding Request Message

Parameter ID: brm (0x0001)

Description: This parameter contains the MGC constructed STUN request message.

Type: Octet String

Optional: No

Possible values: Any valid STUN request message.

Default: None

7.4.3.1.2 Transport address

Parameter name: Transport Address

Parameter ID: ta (0x0002)

Description: This parameter indicates the IP address of the media component that is to have its address STUN mapped.

Type: Integer

Optional: No

Possible values: Any valid list position from the "stunb/ac" parameter.

Default: None

7.4.4 Statistics

None.

7.4.5 Error codes

None.

7.4.6 Procedures

The MGC provides the STUN message contents, STUN server address and media address to the MG which will send a packet from the media address containing the STUN message contents to the STUN server address. The response will be provided to the MGC, thus any protocol or error handling can remain at the MGC level. This package enables the scenario described in clause 10.3 of [IETF RFC 3489].

7.5 STUN information package

Package name: STUN Information

Package ID: stuni (0x00c1)

Description: This package enables an MGC to determine the type of NAT the MG is behind and the binding lifetime associated with the STUN server. Signals and events may be applied to the Root Termination.

Version: 1

Extends: None

7.5.1 Properties

None.

7.5.2 Events

7.5.2.1 NAT type determination

Event name: NAT Type Determination

Event ID: nattd (0x0001)

Description: This event detects the end of the NAT type determination procedure (initiated by a NAT determination signal) and returns the detected type.

7.5.2.1.1 EventsDescriptor parameters

None.

7.5.2.1.2 ObservedEventsDescriptor parameters

7.5.2.1.2.1 NAT Type

Parameter name: NAT Type

Parameter ID: natt (0x0001)

Description: The determined NAT type (scenario) as per clause 10.1 of [IETF RFC 3489].

Type: Enumeration

Optional: No

Possible values: 0x0000: On the open Internet;

0x0001: Firewall that blocks UDP;

0x0002: Firewall that allows UDP out, and responses have to come back to the source of the request (like a symmetric NAT, but no translation). A symmetric UDP Firewall;

0x0003: Full-cone NAT;

0x0004: Symmetric NAT;

0x0005: Restricted cone NAT;

0x0006: Restricted port cone NAT.

Default: None

7.5.2.2 Binding lifetime determination

Event name: Binding Lifetime Determination

Event ID: bld (0x0002)

Description: This event detects the end of the Binding Lifetime determination procedure (initiated by a Binding Lifetime Determination signal) and returns the time period of the binding.

7.5.2.2.1 EventsDescriptor parameters

None.

7.5.2.2.2 ObservedEventsDescriptor parameters

7.5.2.2.2.1 Binding lifetime

Parameter name: Binding Lifetime

Parameter ID: bl (0x0001)

Description: The period of the life of the binding.

Type: Integer

Optional: No

Possible values: 0-3600 seconds

Default: None

7.5.3 Signals

7.5.3.1 NAT type determination

Signal name: NAT Type Determination

Signal ID: nattd (0x0001)

Description: This signal instructs the MG to detect the type of NAT that a particular media component IP address is behind.

Signal type: Brief

Duration: NA

7.5.3.1.1 Additional parameters

7.5.3.1.1.1 Transport address

Parameter name: Transport Address

Parameter ID: ta (0x0001)

Description: This parameter indicates the IP address of the media component that is to have its address STUN mapped.

Type: Integer

Optional: No

Possible values: Any valid list position from the "*stunb/ac*" parameter.

Default: None

7.5.3.2 Binding lifetime determination

Signal name: Binding Lifetime Determination

Signal ID: bld (0x0002)

Description: This signal instructs the MG to detect the binding lifetime with the NAT.

Signal type: Brief

Duration: NA

7.5.3.2.1 Additional parameters

7.5.3.2.1.1 Transport address

Parameter name:	Transport Address
Parameter ID:	ta (0x0001)
Description:	This parameter indicates the IP address of the media component that is to have its address STUN mapped.
Type:	Integer
Optional:	No
Possible values:	Any valid list position from the "*stunb/ac*" parameter.
Default:	None

7.5.4 Statistics

None.

7.5.5 Error codes

None.

7.5.6 Procedures

This package is used to support the procedures as outlined in clause 10 of [IETF RFC 3489].

8 ICE support

The support of ICE implies that the SDP CANDIDATE attribute is supported. This can facilitate address gathering and description of candidates. However, due to the nature of the ITU-T H.248 connection model, several procedural changes are required.

Address gathering

The MGC may request an MG to perform address discovery through the use of the wildcarding mechanism on the CANDIDATE attribute. In this case the MG is responsible for STUN server discovery. Fully specifying the CANDIDATE attribute will not result in any action. The candidate-attribute is specified by the following ABNF:

```
candidate-attribute = "candidate" ":" foundation SP component-id SP
transport SP
priority SP
connection-address SP     ;from [IETF RFC 4566]
port     ;port from [IETF RFC 4566]
[SP cand-type]
[SP rel-addr]
[SP rel-port]
*(SP extension-att-name SP
       extension-att-value)
```

The MGC shall either include values for, or wildcard mandatory fields. Including values provides a way of narrowing down the selection. For example:

If the MGC wanted a particular candidate type it could specify:

```
a=candidate:1 1 UDP  $ $ typ host
a=candidate:2 1 UDP  $ $ srflx raddr  $ rport $
```

and the host address and server reflexive address would be returned.

If the MGC wanted all candidate types it could specify:

```
a=candidate:$ $ $ $ $ $ typ *
```

and the local, server reflexive address and relay addresses would be returned.

If a request results in multiple candidates then these shall be returned in multiple "a=" lines.

As per clause 4.3 of [IETF RFC 5245], if the MG utilizes RTCP, the MGC and MG MUST encode the RTCP candidate using the a=rtcp attribute as defined in [IETF RFC 3605]. If RTCP is not in use, the MGC and MG MUST signal that by using b=RS:0 and b=RR:0 as defined in [IETF RFC 3556].

If the MGC requires a MG to allocate a port for RTCP, the MGC will send the required information to request an RTCP port (e.g., "a=" line in SDP, a=rtcp $).

A further complication is provided by the selection of the "In-Use candidate" in the SDP media (m=) and connection (c=) lines. In the ITU-T H.248 local descriptor this is a local transport address in the MG. Whereas in ICE this may be another address. Therefore, in order to construct an SDP offer, the MGC shall determine the "In-Use candidate" from the CANDIDATE attributes returned in the response.

The *remote-candidate-att* is related to the SDP (SIP) offer and provides the identity of the remote candidates that the offerer wishes the answerer to use in its answers. It is assumed that the MGC (acting as the offerer) will populate this attribute based on candidate information from the MG.

Similarly the ICE SDP "*ice-pwd-att*" attribute may be wildcarded or provided.

If the MGC asks for candidates, it should provide or ask for credentials in order for the MG to be able to perform the necessary signalling.

If MGC provides credentials, the MGC will send the required "a=" lines in SDP. For example:

```
     a=ice-pwd:asd88fgpdd777uzjYhagZg
     a=ice-ufrag:8hhY
```

If the MGC asks the MG to provide the credentials, the MGC will send the required "a=" lines in SDP. For example:

```
     a=ice-pwd:$
     a=ice-ufrag:$
```

If MGC does not supply the necessary "a=" lines in SDP, the MG may determine these credentials and return them to the MGC in a reply message. This is in order for the MG to be able to send a correct STUN message.

The use of the "*a=ice-lite*" attribute indicates whether or not the agent implements a lite version of ICE. As the agent resides in the MG this information needs to be provided to the MGC in order for the information to be communicated to a peer. Given the structure of the "*a=ice-lite*" attribute the MGC is unable to perform a CHOOSE wildcard operation on the attribute. As such where the MG implements a "lite" version of ICE it shall include the "a=ice-lite" attribute in any command response containing the candidate attribute.

Where a binary encoding of ITU-T H.248 is used, the ICE-related attributes may be realized through the use of [ITU-T H.248.1] Annex C.11 properties. In order to facilitate multiple values the "sub-list of" form should be used.

Connectivity checking

In order for an MG to perform some ICE operations, the remote candidate list is required. This remote candidate list can be provided to the MG in the form of candidate attributes being placed in the appropriate remote descriptors. The MGC may be required to reformat the SDP answer/offer received (i.e., via SIP) in order for it to be applicable to ITU-T H.248 structures. The setting of the candidate attributes in the remote descriptor will not in itself generate any ICE operation such as Connectivity Checking or keep alive mechanisms. ITU-T H.248 packages are used to trigger these operations.

8.1 MG act-as STUN server package

Package name: MG Act-as STUN Server

Package ID: mgastuns (0x00c2)

Description: This package enables an MGC to request that a particular address in an MG act as a STUN server in order to process, initiate binding requests and return STUN binding responses. The purpose of the package is to enable the procedures defined in clause 7.2 of [IETF RFC 5389].

Version: 1

Extends: None

8.1.1 Properties

8.1.1.1 Act-as STUN server

Property name: Act-as STUN Server

Property ID: astuns (0x0001)

Description: This property requests that, for a particular local transport address, the MG be prepared to receive STUN binding requests for the purpose of connectivity checking.

Type: List of String

Possible values: In an ITU-T H.248 command request:

Each element in the list of string SHALL be of type `MGActServer` in ABNF format:

```
MGActServer = GroupID "|" Foundation "|" Component-id "|"
RequestType
GroupID = UINT16
Foundation = UINT16
Component-id = UINT16
RequestType = "N"/"S"
```

GroupId is as per UINT16 in clause B.2 of [ITU-T H.248.1].

Component-id is as per <component-id> in clause 15.1 of [IETF RFC 5245].

Foundation is as per <foundation> in clause 15.1 of [IETF RFC 5245].

RequestType is:

N ("No request"): do not process STUN requests;

S ("STUN Server"): act as a STUN server receiving binding requests.

Default: "STUN Server"

Defined in: LocalControl

Characteristics: Read/Write

8.1.2 Events

None.

8.1.3 Signals

None.

8.1.4 Statistics

None.

8.1.5 Error codes

None.

8.1.6 Procedures

To request the MG to act as a STUN server, the MGC should issue an ITU-T H.248 Add/Modify/Move.req command containing the "*astuns*" property on the relevant Termination/Stream.

8.2 Originate STUN continuity check package

Package name: Originate STUN Continuity Check

Package ID: ostuncc (0x00c3)

Description: This package enables an MGC to initiate a STUN continuity check binding request process. The purpose of the package is to enable the procedures defined in clause 7 of [IETF RFC 5389].

Version: 1

Extends: None

8.2.1 Properties

8.2.1.1 Host candidate realm

Property name: Host Candidate Realm

Property ID: hcr (0x0001)

Description: This property indicates the realm in which the MG allocates the IP address and port for the host candidate. As per clause 1 of [IETF RFC 5245], because ICE exchanges a multiplicity of IP addresses and ports for each media stream, it also allows for address selection for multi-homed and dual-stack hosts. As per clause 4.1.1.1 of [IETF RFC 5245], host candidates are obtained by binding to ports (typically ephemeral) on an IP address attached to an interface (physical or virtual, including VPN interfaces) on the host. The information about the host candidate is described in the local SDP. If the MGC requires the MG to gather more than one host candidate via the local SDP, it uses this property to indicate to the MG to gather each of those host candidates in the indicated IP realm or VPN.

Type: List of String

Possible values: Each element in the list of string SHALL be of type `HostCandRealm` in ABNF format:

```
HostCandRealm = GroupID "|" Foundation "|" Component-id
"|" Realm
GroupID = UINT16
Foundation = UINT16
Component-id = UINT16
Realm = ALPHA 0*63(ALPHA/ DIGIT)
ALPHA = %x41-5A / %x61-7A ; A-Z / a-z
DIGIT = %x30-39; 0-9
```

Where:

GroupId is as per UINT16 in clause B.2 of [ITU-T H.248.1].

Component-id is as per <component-id> in clause 15.1 of [IETF RFC 5245].

Foundation is as per <foundation> in clause 15.1 of [IETF RFC 5245].

Realm is a string used to discriminate overlapping IP address spaces. It is the identifier of the IP domain or VPN.

e.g.,

```
"1|1|1|realm1", "1|2|1|realm2"
```

And MGC sends such a local SDP to a MG:

```
v=0
c=IN IP4 $
a=ice-pwd:YH75Fviy6338Vbrhrlp8Yh
a=ice-ufrag:9uB6
m=audio $ RTP/AVP 0
a=candidate:1 1 UDP 2130706431 $ $ typ host
a=candidate:2 1 UDP 2113929215 $ $ typ host
```

The MG should gather two host candidates. The first one is in IP realm "realm1" and the second one is in IP realm "realm2".

Default: None

Defined in: LocalControl

Characteristics: Read/Write

8.2.2 Events

8.2.2.1 Connectivity check result

Event name: Connectivity Check Result

Event ID: ccr (0x0001)

Description: This event returns the result of an ICE connectivity check.

8.2.2.1.1 EventsDescriptor parameters

None.

8.2.2.1.2 ObservedEventsDescriptor parameters

8.2.2.1.2.1 Candidate/transport pair

Parameter name: Candidate/Transport Pair

Parameter ID: ctp (0x0001)

Description: The list of the successful candidate/transport pairs.

Type: List of String

Optional: No

Possible values: Each element in the list of string SHALL be of type **CandPair** in ABNF format:

```
CandPair = StreamID "|" GroupID "|" Foundation-l "|"
        Foundation-r "|" Component-id [Lp-connection-
        address] [Rp-connection-address] [Rc]
StreamID = UINT16
GroupID = UINT16
Foundation-l = UINT16
Foundation-r = UINT16
Component-id = UINT16
Lp-connection-address = "|lp-" Connection-address COLON
PortNumber
Rp-connection-address = "|rp-" Connection-address COLON
PortNumber
Connection-address = IP4-address
Rc = "|RC"
PortNumber = UINT16
```

The ABNF syntax of IP4-address is defined in [IETF RFC 4566].

Where:

StreamID is as per StreamId in clause B.2 of [ITU-T H.248.1].

GroupID is as per UINT16 in clause B.2 of [ITU-T H.248.1].

Foundation-l (Local Foundation) is as per <foundation> in clause 15.1 of [IETF RFC 5245].

Foundation-r (Remote Foundation) is as per <foundation> in clause 15.1 of [IETF RFC 5245].

Component-id is as per <component-id> in clause 15.1 of [IETF RFC 5245].

Lp (Local) Peer reflexive candidate as described in clause 7.1.3.2 of [IETF RFC 5245].

Rp Peer reflexive remote candidate as described in clause 7.2.1.3 of [IETF RFC 5245].

Rc (Role Change) is a flag to indicate that the control role has changed (i.e., controlled or controlling). Control role is described in clause 7.2.1.1 of [IETF RFC 5245].

e.g.,

```
"1|2|3|4|1|lp-202.2.3.4:1000"
```

Means that StreamID is 1, GroupID is 2, Local Foundation is 3, Remote Foundation is 4 , Component-id is 1, and there is a local peer reflexive candidate in this candidate pair. The IP address of this local peer reflexive candidate is 202.2.3.4, and the port is 1000.

Default: None

8.2.2.2 New peer reflexive candidate

Event name: New Peer Reflexive Candidate

Event ID: nprc (0x0002)

Description: This event indicates that a new peer reflexive candidate was discovered during a connectivity check.

8.2.2.2.1 EventsDescriptor parameters

None.

8.2.2.2.2 ObservedEventsDescriptor parameters

8.2.2.2.2.1 Candidate

Parameter name: Candidate

Parameter ID: can (0x0001)

Description: A list of the newly discovered peer reflexive candidates.

Type: Sub-list of String

Optional: No

Possible values: Each element in the list of string SHALL be of type **peerCand** in ABNF format:

```
peerCand = StreamID "|" GroupID "|" Foundation "|"
          Component-id "|" Connection-address COLON
           PortNumber
StreamID = UINT16
GroupID = UINT16
Foundation = UINT16
Component-id = UINT16
Connection-address = IP4-address
PortNumber = UINT16
```

The ABNF syntax of IP4-address is defined in [IETF RFC 4566].

Where:

StreamID is as per StreamId in clause B.2 of [ITU-T H.248.1].

GroupID is as per UINT16 in clause B.2 of [ITU-T H.248.1].

Foundation is as per <foundation> in clause 15.1 of [IETF RFC 5245].

Component-id is as per <component-id> in clause 15.1 of [IETF RFC 5245].

A newly discovered peer reflexive candidate as described in clause 7.1.3 of [IETF RFC 5245].

e.g.,

```
"1|2|3|4|202.2.3.4:1000"
```

Means that the StreamID is 1, GroupID is 2, Foundation is 3, Component-id is 4, and a new peer reflexive candidate was discovered.

The IP address of this peer reflexive candidate is 202.2.3.4, and the port is 1000.

Default: None

8.2.3 Signals

8.2.3.1 Send Connectivity Check

Signal name: Send Connectivity Check

Signal ID: scc (0x0001)

Description: This signal initiates connectivity checking procedures as defined in clause 7 of [IETF RFC 5245].

Signal type: Brief

Duration: NA

8.2.3.1.1 Additional parameters

8.2.3.1.1.1 Control

Parameter name: Control

Parameter ID: cntrl (0x0001)

Description: This parameter indicates the controlling role defined in clause 7.1.2.2 of [IETF RFC 5245].

Type: Enumeration

Optional: Yes

Possible values: Controlling (0x0001): MG acts as controlling role
Controlled (0x0002): MG acts as controlled role

Default: Controlling

Characteristics: Read

8.2.3.2 Send additional connectivity check

Signal name: Send Additional Connectivity Check

Signal ID: sacc (0x0002)

Description: This signal instructs a MG to initiate additional ICE connectivity check procedures in the case additional candidate/transport address pairs are identified. The MG shall use the CANDIDATE attributes in both the local and remote descriptors to determine the candidate/transport address pairs to use for the connectivity check. The MG shall resume and only perform checks not already performed.

Signal type: Brief

Duration: NA

8.2.3.2.1 Additional parameters

8.2.3.2.1.1 Control

Parameter name: Control

Parameter ID: cntrl (0x0001)

Description: This parameter indicates the controlling role defined in clause 7.1.2.2 of [IETF RFC 5245].

Type: Enumeration

Possible values: Controlling (0x0001): MG acts as controlling role
Controlled (0x0002): MG acts as controlled role

Default: Controlling

Characteristics: Read

8.2.4 Statistics

None.

8.2.5 Error codes

None.

8.2.6 Procedures

When the "Send Connectivity Check" (*scc*) signal is sent, the MGC should initiate the STUN continuity check procedures as outlined in clause 7 of [IETF RFC 5245]. As the ICE agent functionality is split between a MGC and MG and the MG is responsible for sending the connectivity checks, the agent role (controlled or controlling, see clause 5.2 of [IETF RFC 5245]) should be provided. In order for the MGC to obtain the result of the connectivity check, it shall set the "Connectivity Check Result" (*ccr*) event.

The usage of the "Send Connectivity Check" signal shall clear the results of any previous connectivity checking on the Termination/Stream.

If the *ccr* event is set and the *scc* signal is received, the MG shall apply the procedures of clause 7.1.2 of [IETF RFC 5245] to form and prioritize a checklist.

Once the procedures of clause 7.1.3 of [IETF RFC 5245] have been completed, the MG shall then notify the MGC of the result. The MG shall deem the procedures of clause 5.8 of [IETF RFC 5245] completed once all checks have reached the state "succeeded" or "failed". In order to uniquely identify the checks on the termination, the MG shall provide the StreamID, GroupID, foundation of the local candidate, foundation of the remote candidate and the component-id. If the control role of this candidate pair changes, an optional flag "Rc" is included in the end. The MG shall maintain the results of the checking for the lifetime of the Termination/Stream or until they are cleared by a subsequent "Send Connectivity Check" signal.

Where there is only one stream or group the respective ids default to 1.

If there are no successful candidate pairs for one of the particular component-ids in the list, then the connectivity check for that component-id has failed.

If there are more than one successful candidate pairs for a particular component-id in the list, only the candidate pair having the highest priority will be reported. The "Sub-list of" shall be in the same order as the checklist in order to maintain relative priority.

Depending on its connection role, "controlled" or "controlling", the MGC may use the result in the ObservedEventsDescriptor parameter *ccr/ctp* to determine which transport pair to use for the media connection.

If a new peer reflexive candidate is discovered as per the procedure in clause 7.1.3.2.1 of [IETF RFC 5245], and if the "New Peer Reflexive Candidate" (*nprc*) event is set, the MG will notify the MGC with the new peer reflexive candidate. In order to identify this peer reflexive candidate, the MG shall provide the StreamID, GroupID, Foundation, Component-id and the transport IP address and port number of this peer reflexive candidate. If the MGC requires that the peer reflexive candidate be paired with other remote candidates besides the one in the valid pair that will be generated, the MGC may generate an updated offer which includes the peer reflexive candidate. This will cause it to be paired with all other remote candidates. The list of the candidate pairs is updated in this case.

When a new peer reflexive candidate is discovered, the Connectivity Checks procedure continues. If the MGC updates the local candidates via the SDP in the ITU-T H.248 message, the MG will continue with any connectivity checks that are still in progress. It will not perform checks on the new candidates. The MGC shall send the "Send Additional Connectivity Check" (*sacc*) signal to perform checking of the new candidates.

In some kinds of conditions, where the list of the connectivity check candidate pairs is changed (i.e., a new stream is added, an existing stream is modified or a new peer reflexive candidate is discovered) additional connectivity check procedures may be initiated. The MGC may send the "Send Additional Connectivity Check" signal to initiate a connectivity check procedure on any candidate/transport pair not previously checked. In this procedure, the MG shall only perform checks not already performed. Another example is where a new stream is added after the connectivity checks for the existing stream have finished. In this case, the additional connectivity checks will only check the candidate pairs of the newly added stream.

9 Keep-alive and pinhole support

The packages in this clause provide a means of opening a pinhole through a NAT and to maintain a binding with the NAT. It does not rely on ICE techniques.

9.1 MGC-originated STUN request package

Package name: MGC Originated STUN Request

Package ID: mgcostunr (0x00c4)

NOTE 1 – Clause 10 of [IETF RFC 5245] makes use of this mechanism.

Description: The MGC may also periodically request the MG to send a STUN request in order to keep the binding with the NAT "alive". This should be done before the expiry of the keep-alive period.

NOTE 2 – This package is an exception to the rule in the scope that the MG determines the address to which a Binding Request is sent.

Version: 1

Extends: None

9.1.1 Properties

None.

9.1.2 Events

9.1.2.1 STUN binding request failure

Event name: STUN Binding Request Failure

Event ID: fail (0x0001)

Description: This event is triggered if a STUN binding request has failed.

9.1.2.1.1 EventsDescriptor parameters

9.1.2.1.1.1 From address

Parameter name: From Address

Parameter ID: fa (0x0001)

Type: List of String

Optional: No

Possible values: "Y" (Yes): Failure reporting is required for this list position.
"N" (No): Failure Reporting is not required for this list position.

9.1.2.1.2 ObservedEventsDescriptor parameters

9.1.2.1.2.1 Failure

Parameter name: Failure

Parameter ID: fail (0x0001)

Description: This parameter contains the reason for the failure.

Type: String

Optional: No

Possible values: If the response of STUN binding request is "time out", error code 1000 follows the <list position>.

If the mapping address in the response of STUN binding request changes, error code 1001 and the new mapping address follows <list position>. The format is "<list position>:IP address ":" port. e.g., "1:202.1.2.3:1000"

Default: None

9.1.3 Signals

9.1.3.1 Send STUN request

Signal name: Send STUN Request

Signal ID: sstunr (0x0001)

Description: This signal instructs an MG to send a binding request from the local address to the remote address contained in the remote descriptor.

Signal type: Brief

Duration: NA

9.1.3.1.1 From address

Parameter name: From Address

Parameter ID: fa (0x0001)

Description: This parameter contains the addresses from where the binding request should be sent to the corresponding remote address.

Type: List of String

Optional: No

Possible values: *N* ("No Request"): do not perform a STUN binding request from the local address.

Default: None

9.1.3.1.2 Retransmission time interval

Parameter name: Retransmission Time Interval

Parameter ID: rti (0x0002)

Description: This parameter contains the initial retransmission time interval for the STUN request, as RTO defined in clause 7.2.1 of [IETF RFC 5389].

Type: Integer

Optional: Yes

Possible values: 1 ms to 600000 ms (10 minutes)

Default: 100 ms

9.1.4 Statistics

None.

9.1.5 Error codes

None.

9.1.6 Procedures

The MGC should initiate a STUN Binding Request to the remote address when it suspects that the local address is behind a restricted cone NAT. This will have the effect of opening a pinhole, allowing the remote end to send packets to the local end. If the MGC initiates a STUN Binding Request to the remote address, it can keep NAT bindings active. If there are no packets sent between the local and remote address pairs being used for media for Tr seconds (where packets include media and previous keep-alives), the MG MUST generate a keep-alive on that pair. To detect STUN Binding Request failures the *fail* event should be set.

This procedure is distinct from the ICE continuity check procedures.

9.2 Keep alive request package

Package name: Keep Alive Request

Package ID: kar (0x00c5)

Description: This package enables the MGC to request the MG to send a packet in order to open a pinhole through a server or to maintain a binding. This packet goes through the same way as the media flows. For example, it allows the techniques as defined in clause 10 of [IETF RFC 5245].

NOTE – This package is an exception to the rule in the scope that the MG determines the address to which a Binding Request is sent.

Version: 1

Extends: None

9.2.1 Properties

None.

9.2.2 Events

None.

9.2.3 Signals

9.2.3.1 Send keepalive packet

Signal name: Send Keepalive Packet

Signal ID: skap (0x0001)

Description: This signal instructs a MG to send a keepalive packet from the local address to the remote address contained in the remote descriptor.

Signal type: Brief

Duration: NA

9.2.3.1.1 From address

Parameter name: From Address

Parameter ID: fa (0x0001)

Description: This parameter contains the addresses from where the keepalive packet should be sent to the corresponding remote address. The MGC shall include a value in each position of list of string for each element described in the "*stunb/ac*" property.

Type: List of String

Optional: No

Possible values: "Send" (*S*): send a keepalive packet from the local address.

"Not Send" (*N*): do not send a keepalive packet from the local address.

Default: None

9.2.3.1.2 Keep alive transmission interval

Parameter name: Keep Alive Transmission Interval

Parameter ID: ti (0x0002)

Description: This parameter contains transmission time interval for sending the keepalive packet. The value of this parameter corresponds to the Tr timer from [IETF RFC 5245].

Type: Integer

Optional: Yes

Possible values: 15000 ms or more

Default: 15000 ms (15 seconds), unless provisioned otherwise.

9.2.3.1.3 Keep alive packet type

Parameter name: Keep Alive Packet Type

Parameter ID: kapt (0x0003)

Description: This parameter indicates the type of keep alive packet type.

Type: Enumeration

Optional: Yes

Possible values: et (0x0000): Transport (i.e., UDP, DCCP) packet of 0-byte;

rm (0x0001): RTCP packets multiplexed with RTP packets;

sbi (0x0002): STUN binding indication;

cn (0x0003): RTP packet with comfort noise payload;

no (0x0004): Reserved for RTP packet with No-Op payload;

iv (0x0005): RTP packet with incorrect version number;

up (0x0006): RTP packet with unknown payload type.

NOTE – Value no (0x0004) is reserved for a future payload type.

Default: up (0x0006): RTP packet with unknown payload type

9.2.4 Statistics

None.

9.2.5 Error codes

None.

9.2.6 Procedures

In order to open or maintain a binding, the MGC should send the "Send Keep Alive" (*skap*) signal to the MG to initiate sending a keep-alive packet to the remote address. This will have the effect of opening a pinhole (or keeping a binding open) allowing the remote end to send packets to the local end. The "Keep Alive transmission interval" (*ti*) parameter is used in order for the MG to autonomously send a keep-alive packet when no packets have been detected for the address for time interval Tr.

Where a MGC utilizes a Keep alive Request signal with the "RTP packet with unknown payload type", it may be required to communicate this to a peer MGC via the SDP. An MGC on reception of this attribute should then set this attribute in the remote descriptor of the applicable MG Termination/Stream. It indicates to the MG that the remote end will utilize a keep-alive using an RTP packet with an unknown payload type.

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, 2012