International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.460.24

Amendment 1

(05/2011)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Supplementary services for multimedia

Point-to-point media through network address translators and firewalls within ITU-T H.323 systems

Amendment 1: Improvements for NAT traversal without intermediary entities

Recommendation ITU-T H.460.24 (2009) – Amendment 1

ITU-T

International Telecommunication Union

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
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.460.24

Point-to-point media through network address translators and firewalls within ITU-T H.323 systems

Amendment 1

Improvements for NAT traversal without intermediary entities

Summary

Recommendation ITU-T H.460.24 enables an ITU-T H.323 gatekeeper to formulate a decision to enable direct media flows between ITU-T H.323 endpoints that reside behind network address translator (NAT)/firewall (FW) devices. This extension is used in conjunction with Recommendation ITU-T H.460.18 to facilitate the traversal of media across NAT/FW devices and Recommendation ITU-T H.460.23 to discover the characteristics of NAT/FW devices sitting in front of ITU-T H.323 endpoints, reducing the frequency with which media proxy devices (as described in Recommendation ITU-T H.460.19) are needed by allowing direct media connectivity between the endpoints. Connectivity is achieved via the formulation of an intelligent media transmission decision and call signalling that instructs endpoints to initiate media flows in such a manner that a reliable direct media pathway is established, even if one or both endpoints reside behind a NAT/FW device.

Amendment 1 to Recommendation ITU-T H.460.24 further improves conditions where media pathways do not require the services of an intermediary to achieve NAT traversal. New Annex B allows endpoints under certain conditions, after first establishing media flows through an intermediary entity, to probe for a direct route and, if detected, change the media pathway to flow directly between the endpoints freeing up the resources of the intermediary entity.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.460.24	2009-12-14	16
1.1	ITU-T H.460.24 (2009) Amd. 1	2011-05-14	16

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T H.460.24

Point-to-point media through network address translators and firewalls within ITU-T H.323 systems

Amendment 1

Improvements for NAT traversal without intermediary entities

1 Scope

This Recommendation defines the capability and procedures for enabling the direct point-to-point media flow between endpoints even if at least one device is behind a network address translator (NAT) or firewall (FW) device. If used in conjunction with [ITU-T H.460.23], this feature can be used to extend the scalability of [ITU-T H.460.19] to allow media, where determined, to flow directly between endpoints and avoid the requirement to proxy media.

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.225.0] Recommendation ITU-T H.225.0 (2009), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[ITU-T H.245] Recommendation ITU-T H.245 (2009), *Control protocol for multimedia communication*.

[ITU-T H.323] Recommendation ITU-T H.323 (2009), *Packet-based multimedia communications systems*.

[ITU-T H.460.1] Recommendation ITU-T H.460.1 (2002), *Guidelines for the use of the generic extensible framework*.

[ITU-T H.460.17] Recommendation ITU-T H.460.17 (2005), *Using H.225.0 call signalling connection as transport for H.323 RAS messages*.

[ITU-T H.460.18] Recommendation ITU-T H.460.18 (2005), *Traversal of H.323 signalling across network address translators and firewalls*.

[ITU-T H.460.19] Recommendation ITU-T H.460.19 (2005), *Traversal of H.323 media across network address translators and firewalls*.

[ITU-T H.460.23] Recommendation ITU-T H.460.23 (2009), *Network address translator and firewall device determination in H.323 systems*.

[IETF RFC 3174] IETF RFC 3174 (2001), *US Secure Hash Algorithm 1 (SHA1)*.

[IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.

NOTE – The IETF published a new RFC that obsoletes [IETF RFC 3489], changing the name of the standard and the procedures defined therein. This Recommendation relies on the protocol and procedures specified in [IETF RFC 3489], and the protocol and procedures defined in the new RFC are neither suitable nor compatible. As such, this Recommendation does not reference the new RFC and deliberately makes reference to the original specification, which is now referred to as "classical STUN".

[IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 transport address [ITU-T H.323]: The transport layer address of an addressable ITU-T H.323 entity as defined by the (inter)network protocol suite in use. The Transport Address of an ITU-T H.323 entity is composed of the Network Address plus the transport layer service access point identifier of the addressable ITU-T H.323 entity.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 P2Pnat media: Indicates that media flows directly (peer-to-peer) between two communicating endpoints through NAT devices without the assistance of a media proxy.

3.2.2 pinhole: A temporary binding of an internal and an external transport address in the network address translator/firewall, which allows the bidirectional passage of packets between those addresses.

3.2.3 STUN server: A server to assist in network address translator type detection.

3.2.4 well-behaved NAT: A network address translator (NAT) that exhibits consistent behaviour over time of a given NAT type as categorized in clause 5 of [IETF RFC 3489].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACF	Admission Confirm
ARJ	Admission Reject
ARQ	Admission Request
CUI	Channel Unique Identifier
EP	Endpoint
FW	Firewall
GEF	Generic Extensibility Framework
LAN	Local Area Network
LCF	Location Confirm
LRQ	Location Request
NAT	Network Address Translator

OID	Object Identifier
OLC	Open Logical Channel message
OLCAck	Open Logical Channel Acknowledge message
PER	Packed Encoding Rules
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SR	Sender Report
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol
STUN	Simple Traversal of User datagram protocol through Network address translators
TCP	Transmission Control Protocol
TSAP	Transport layer Service Access Point
UDP	User Datagram Protocol

5 Feature description

This Recommendation defines a procedure wherein gatekeepers may negotiate between each other to determine a method to traverse media between endpoints where at least one of these endpoints is located behind a NAT/FW device, without requiring the use of an ITU-T H.460.19 server to proxy media.

This Recommendation is designed for use in networks that employ NAT/FW devices with well-behaved NAT characteristics. Networks that do not employ well-behaved NAT devices should continue to utilize [ITU-T H.460.18] and [ITU-T H.460.19] to ensure proper end-to-end media flows.

6 Capability advertisement

Endpoints capable of supporting P2Pnat media shall advertise this capability via the generic extensibility framework (GEF) defined in [ITU-T H.323] and [ITU-T H.460.1].

This feature shall be used in conjunction with ITU-T H.460.23 NAT/FW determination and [ITU-T H.460.18] (or optionally [ITU-T H.460.17]) as an alternative to [ITU-T H.460.19]. Endpoints seeking to support this feature shall also support [ITU-T H.460.23] and [ITU-T H.460.18]/[ITU-T H.460.19] or optionally [ITU-T H.460.17]/[ITU-T H.460.19].

If ITU-T H.460.18 or optionally ITU-T H.460.17 and ITU-T H.460.23 features are unsupported or unavailable, then this feature shall be disabled and shall not advertised.

Endpoints shall advertise the P2Pnat media feature when sending an ARQ to a gatekeeper. The feature indicator shall be included in the **supportedFeatures** field of the **featureSet** field and, if or when instructed by the gatekeeper via the replying ACF message, the feature indicator shall also be to include as a **supportedFeatures** field in the Setup message when placing calls to remote endpoints. The gatekeeper shall also advertise this capability to other gatekeepers via the generic data field contained in the LRQ and responding LCF messages.

NOTE – The advertisement and use of [ITU-T H.460.19] shall be determined by the media strategy of this feature (refer to clause 9).

Table 1 defines the P2Pnat media feature in this Recommendation.

Table 1 – Indication of P2Pnat media feature

Feature name:	P2Pnat media feature
Feature description:	This feature allows a gatekeeper to negotiate with other gatekeepers to calculate a strategy to stream media directly to/from and between NAT/FW endpoints.
Feature identifier type:	Standard
Feature identifier value:	24

Parameters associated with the advertisement of this capability are specified in the following clauses. In consideration of backward compatibility with further revisions to this Recommendation, the recipient shall simply ignore any parameters received other than those specified in this Recommendation.

For the purpose of this Recommendation, where an optional parameter of type **bool** is to be omitted, then it shall automatically be deemed to have a default value of FALSE.

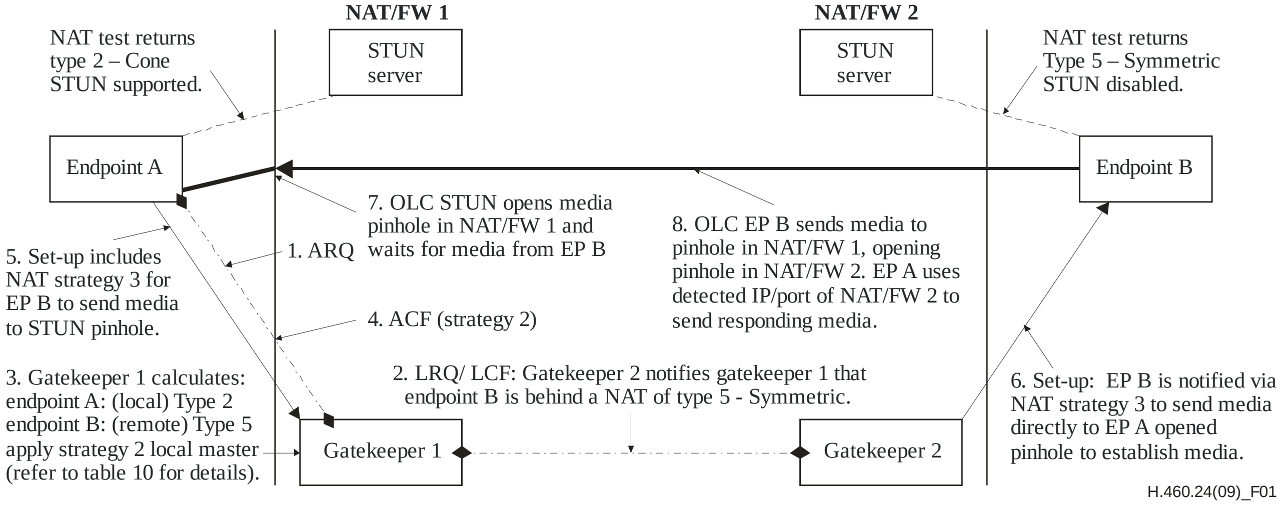
NAT/FW 1
NAT/FW 2
NAT test returns type 2 – Cone STUN supported.
STUN server
STUN server
NAT test returns Type 5 – Symmetric STUN disabled.
Endpoint A
Endpoint B
7. OLC STUN opens media pinhole in NAT/FW 1 and waits for media from EP B
8. OLC EP B sends media to pinhole in NAT/FW 1, opening pinhole in NAT/FW 2. EP A uses detected IP/port of NAT/FW 2 to send responding media.
5. Set-up includes NAT strategy 3 for EP B to send media to STUN pinhole.
1. ARQ
4. ACF (strategy 2)
3. Gatekeeper 1 calculates: endpoint A: (local) Type 2 endpoint B: (remote) Type 5 apply strategy 2 local master (refer to table 10 for details).
2. LRQ/ LCF: Gatekeeper 2 notifies gatekeeper 1 that endpoint B is behind a NAT of type 5 - Symmetric.
6. Set-up: EP B is notified via NAT strategy 3 to send media directly to EP A opened pinhole to establish media.
Gatekeeper 1
Gatekeeper 2
H.460.24(09)_F01

Figure 1 – Sample call flow through double NAT/FW

7 Call establishment procedure

When an endpoint that supports this feature places a call, it shall advertise to the gatekeeper via the supported **FeatureSet** in the ARQ that it supports the P2Pnat media feature.

The gatekeeper, if supporting this feature, shall include the P2Pnat media feature identifier in the **genericData** field when transmitting LRQ to other gatekeepers.

The remote gatekeeper, which supports this feature and is capable of routing the call, shall respond with the **P2Pnat media** feature identifier in the **genericData** field of the LCF and include the following information collected on the remote endpoint.

The parameters exchanged via the LCF can be categorized into three categories:

1) **Gatekeeper parameters** – General information on NAT/FW support for the gatekeeper.

2) **Non-NAT/FW parameters** – General information on the requested endpoint's location, i.e., the endpoint is not behind a NAT/FW and can provide remote NAT support, or whether media must be proxied to reach the endpoint.

3) **NAT/FW-specific parameters** – Specific information on whether the endpoint is behind a NAT/FW device and the characteristics of that device to assist in providing NAT traversal support.

7.1 Gatekeeper parameters

If the responding gatekeeper is capable of providing ITU-T H.460.19 media proxy support, then it shall notify the requesting gatekeeper via the **RemoteProxy** parameter that it can provide media proxy support if required.

Table 2 – RemoteProxy parameter

Parameter name:	RemoteProxy
Parameter description:	Indicates whether the gatekeeper can provide ITU-T H.460.19 media proxy support.
Parameter identifier type:	Standard
Parameter identifier value:	1
Parameter type:	bool
Parameter cardinality:	One and only one

7.2 Non-NAT/FW parameters

If the endpoint is on a public IP address and is capable of receiving NAT client media, then the **RemoteNAT** parameter shall be included, as per Table 3. If this value is set to true, all further included parameters in this clause shall be ignored.

Table 3 – RemoteNAT parameter

Parameter name:	RemoteNAT
Parameter description:	Indicates that the device is not behind a NAT/FW and that the device can support calls from remote endpoints behind a NAT/FW (remote media master, refer to clause 8).
Parameter identifier type:	Standard
Parameter identifier value:	2
Parameter type:	bool
Parameter cardinality:	One and only one

RemoteNAT indicates that the endpoint is on a public IP address and capable of listening and receiving media packets directly from remote endpoints, which reside behind NAT/FW devices, prior to initiating reciprocating media flow. This allows pinholes to be opened in the remote NAT/FW and for the public IP endpoint to detect the apparent source address of the remote media flow to determine a target to which to send media packets. This allows symmetric bidirectional media flows to be initiated between the devices through the remote NAT/FW.

Where the remote party is behind a NAT/FW and all media must be proxied via a network border proxy to reach that endpoint, then this shall be indicated via the **MustProxyNAT** parameter (see Table 4). This shall indicate to the calling party that all media must be proxied to reach the endpoint. If this value is set to TRUE, all further included parameters in this clause shall be ignored.

Table 4 – MustProxyNAT parameter

Parameter name:	MustProxyNAT
Parameter description:	Indicates that media must be proxied to reach the endpoint (i.e., for traversing corporate firewalls).
Parameter identifier type:	Standard
Parameter identifier value:	3
Parameter type:	bool
Parameter cardinality:	One and only one

7.3 NAT/FW-specific parameters

If the remote endpoint is behind a NAT/FW, then the **CalledIsNAT** parameter shall be included (see Table 5).

Table 5 – CalledIsNAT parameter

Parameter name:	CalledIsNAT
Parameter description:	Indicates whether the called endpoint is behind a NAT/FW.
Parameter identifier type:	Standard
Parameter identifier value:	4
Parameter type:	bool
Parameter cardinality:	One and only one

If the **CalledIsNAT** parameter is present, then the **CalledNATType** parameter (refer to Table 6) shall also be present. The values are in accordance with the NATType parameter values (Table 8 of [ITU-T H.460.23]) detected in the ITU-T H.460.23 NAT/FW determination.

Table 6 – CalledNATType parameter

Parameter name:	CalledNATType
Parameter description:	Type of NAT the called party is behind (in accordance with Table 8 of [ITU-T H.460.23]).
Parameter identifier type:	Standard
Parameter identifier value:	5
Parameter type:	number8
Parameter cardinality:	One and only one

If the **CalledIsNAT** parameter is present, then the **ApparentSourceAddress** parameter shall also be present (refer to Table 7). This indicates the apparent public source IP address of the endpoint as detected by the registering gatekeeper. This can be used in determining if the endpoints involved in the call reside behind the same NAT/FW device.

Table 7 – ApparentSourceAddress parameter

Parameter name:	ApparentSourceAddress
Parameter description:	Indicates the apparent public source IP address of the endpoint as detected by the registering gatekeeper.
Parameter identifier type:	Standard
Parameter identifier value:	6
Parameter type:	transport
Parameter cardinality:	One and only one

Optionally, the endpoint may support Annex A. This shall be notified by the **SameNATProbe** parameter (refer to Table 8a).

Table 8a – SameNATProbe parameter

Parameter name:	SameNATProbe
Parameter description:	Indicates whether the endpoint supports probing for the same NAT (supports ITU-T H.460.24 Annex A).
Parameter identifier type:	Standard
Parameter identifier value:	7
Parameter type:	bool
Parameter cardinality:	One and only one

Optionally, the endpoint may support Annex B. This shall be notified by the **ExternalNATProbe** parameter (refer to Table 8b).

Table 8b – ExternalNATProbe parameter

Parameter name:	ExternalNATProbe
Parameter description:	Indicates whether the endpoint supports External NAT probing (supports ITU-T H.460.24 Annex B).
Parameter identifier type:	Standard
Parameter identifier value:	9
Parameter type:	bool
Parameter cardinality:	One and only one

8 Calculating media pathways

On receipt of the LCF from the remote gatekeeper, the local gatekeeper shall calculate, from the information provided, the best method to route media directly between the endpoints.

Possible options are documented below and enumerated in Table 9:

Unknown: This indicates the gatekeeper cannot determine an ITU-T H.460.24 method and shall revert back to the default ITU-T H.460.19 method.

No assistance: This indicates that neither devices require any assistance and that both devices are capable of streaming media between each other directly.

Local media master: This indicates that the local endpoint is to provide assistance directly to the remote endpoint to traverse the remote NAT/FW and stream the media directly.

Remote media master: This indicates that the remote endpoint is to provide assistance directly to the local endpoint to traverse the local NAT/FW and stream the media directly.

Local proxy: This indicates that the local gatekeeper shall provide the required assistance by proxying the media through its assigned ITU-T H.460.19 server.

Remote proxy: This indicates the remote gatekeeper shall provide the required assistance by proxying the media through its assigned ITU-T H.460.19 server.

Full proxy: This indicates that both gatekeepers (or one gatekeeper, if both parties are on the same gatekeeper) shall provide proxy support to the call. This rule generally applies to gatekeepers that act as network border proxies to egress media to/from private local area networks (LANs) to the public Internet.

Same NAT/FW: This indicates that the two endpoints reside behind the same NAT/FW device. Since it is impossible to detect the network topography behind the NAT/FW device, media shall be proxied. However, the devices are to probe a direct media pathway on their own and, if successful, select to send media directly (this requires Annex A support).

External NAT probe: This indicates that the two endpoints reside behind distinct NAT/FW devices and both devices and gatekeeper support Annex B. From media strategy calculations, it was determined that media must be initially proxied and once media is established, the two devices may probe for a direct route via the procedure detailed in Annex B.

NAT media failure: This indicates that there is no resolvable method to stream media between the endpoints and the call will fail to establish bidirectional media flows.

Table 9 – Media strategy indicator

Value	Strategy
0	Unknown
1	No assistance
2	Local media master
3	Remote media master
4	Local proxy
5	Remote proxy
6	Full proxy
7	Same NAT/FW (Annex A)
8	External NAT probe (Annex B)
100	NAT media failure

9 Determining media strategy

The following method shall be used to determine the media path between endpoints that support this feature and, where possible, to support legacy endpoints that do not have this feature.

The following procedure shall be followed in logical order to determine the media pathway.

The required inputs are:

1) NAT/FW type as detected via ITU-T H.460.23 (as per Table 8 of [ITU-T H.460.23]).

2) Whether the gatekeeper can provide ITU-T H.460.19 media proxy support.

3) Whether the endpoint can support remote NAT/FW endpoints.

4) Whether media must be proxied via an ITU-T H.460.19 server to reach the endpoint.

9.1 Compatibility

To support compatibility and provide limited NAT/FW support to non-supporting endpoints, endpoints that do not support this feature shall be assigned NAT type 0 ("**Unknown NAT**") as defined in Table 8 of [ITU-T H.460.23]. It shall also be assigned "**No H.460.19 Proxy Assistance**", "**No Remote NAT support**" and "**No Must Proxy**" as input values into the calculation. It is assumed the non-supporting endpoints' gatekeeper can provide, if required, proxying support to facilitate media flow.

If either endpoint is of NAT type 6 or 7 (see Table 8 of [ITU-T H.460.23]), then it can be assumed that the call will fail and shall be assigned media strategy 100 ("**NAT media failure**") and the call is to be rejected with reason **noRouteToDestination**.

9.2 Same NAT/FW determination

If both endpoints are detected as being behind a NAT/FW device and share the same apparent source IP address, which is detected during registration (refer to clause 7.1 of [ITU-T H.460.17] or clause 8.2 of [ITU-T H.460.18]) and/or transmitted via the **ApparentSourceAddress** parameter contained in the LCF, then it may be assumed that the endpoints reside behind the same NAT/FW device. P2Pnat media cannot determine the network topography behind the shared NAT/FW device and support shall revert back to [ITU-T H.460.19]. This shall be indicated by media strategy indicator 6 (**full proxy**).

Where both endpoints support Annex A (via **SameNATProbe** Parameter), and to avoid unnecessary media proxying, endpoints may elect to attempt, after initiating media proxying via ITU-T H.460.19, to stream media directly. In this case, endpoints shall follow the instructions in Annex A to probe for a direct route and shall instead be notified by media strategy indicator 7 (**same NAT/FW**).

9.3 Must proxy media determination

Below are values to be returned if at least one endpoint must proxy media indicated via the **MustProxyNATIndicator** (refer to Table 4) or has been locally determined.

If both parties must proxy media, then settings are not altered and the gatekeeper is allowed to route the media in full proxy mode via the ITU-T H.460.19 server. All STUN support (if enabled) on either endpoint shall also be disabled for this call. This shall be indicated by media strategy indicator 6 (**full proxy**).

If the local gatekeeper must proxy to reach the local endpoint, indicate this as the preferred method. Any NAT support on the remote gatekeeper (proxy, ITU-T H.245 address rewrites) shall be disabled. All STUN support (if enabled) on the remote endpoint shall also be disabled for this call. Media shall be proxied locally via the local gatekeeper ITU-T H.460.19 server. This shall be indicated by media strategy indicator 4 (**local proxy**).

If the remote gatekeeper must proxy to reach the remote endpoint, indicate this as the preferred method. Any NAT support on the local gatekeeper (proxy, ITU-T H.245 address rewrites) shall be disabled. All STUN support (if enabled) on the remote endpoint shall also be disabled for this call. Media shall be proxied remotely via the remote gatekeeper ITU-T H.460.19 server. This shall be indicated by media strategy indicator 5 (**remote proxy**).

9.4 General NAT strategy determination

Table 10 contains an overview of the general strategy to be employed given the NAT types that are returned from the ITU-T H.460.23 test.

Table 10 – NAT strategy calculation matrix
(for values, refer to Table 9)

		Local type (Table 8 of [ITU-T H.460.23])					
Remote type		0	1	2	3	4	5
	0	0	1	2	4	4	4
	1	1	1	3	3	3	3
	2	3	2	2	3	3	3
	3	5	2	2	~~4~~8	~~4~~8	~~4~~8
	4	5	2	2	~~4~~8	~~4~~8	4
	5	5	2	2	~~4~~8	4	4

NOTE – P2Pnat media is considered strategy 1, 2, ~~or~~ 3 or 8. Strategies 4 and 5 require the support of an ITU-T H.460.19 server.

For the purpose of Table 10, where an ITU-T H.460.19 server is not available for media strategy indicators 4 (**local proxy**), ~~or~~ 5 (**remote proxy**) or 8 (**external NAT probe**), these values shall be deemed to be media strategy indicator 100, indicating call failure (NAT media failure).

Where both parties and the local gatekeeper do not support Annex B, NAT strategy 8 (**external NAT probe**) shall be replaced with NAT strategy 4 (local proxy).

9.5 Example P2Pnat media calculations

If both parties are not behind a NAT/FW (NAT type 1), then no media proxy is required and all proxy functions and ITU-T H.245 address rewrites may be disabled and the media may flow directly between the parties. This shall be indicated by media strategy indicator 1 (**no assistance**).

If the local endpoint is not behind a NAT (NAT type 1) and supports remote NAT or has local NAT type 2 (full cone NAT), then disable all proxy functions and ITU-T H.245 address rewrites in the gatekeeper. STUN support (if enabled) on the remote endpoint shall be disabled. The local endpoint, if behind a NAT/FW, shall perform a STUN routine to open the local real-time transport protocol (RTP)/real-time transport control protocol (RTCP) ports and provide the public IP of the NAT/FW device and the STUN assigned ports in its ITU-T H.245 address. It shall also ignore the ITU-T H.245 address provided to it from the remote endpoint and wait until it receives the first RTP/RTCP packets on the local RTP/RTCP assigned ports. It shall then assign the received apparent source address and port of the remote endpoint as the target to which to send media. Once media is received from the remote endpoint, the pinhole in the remote NAT/FW has been opened and media can then now flow bidirectionally to/from the remote endpoint. This shall be indicated by media strategy indicator 2 (**local media master**).

If the remote endpoint is not behind a NAT (NAT type 1) and supports remote NAT or has remote NAT type 2 (full cone NAT), then disable all proxy functions and ITU-T H.245 address rewrites. STUN support (if enabled) on the local endpoint shall be disabled. The remote endpoint, if behind a NAT/FW, shall perform a STUN routine to open the remote RTP/RTCP ports and provide the public IP of the NAT/FW device and the STUN assigned ports in its ITU-T H.245 address. It shall also ignore the ITU-T H.245 address provided, if any, and wait until it receives the first RTP/RTCP packets on the remote RTP/RTCP assigned ports. It shall then assign the received apparent source address and port of the remote endpoint as the target to which to send media. Once media is received from the local endpoint, the pinhole in the local NAT/FW has been opened and media can then now flow bidirectionally to/from the local endpoint. This shall be indicated by media strategy indicator 3 (**remote media master**).

If matching is not obtained with any of the above and the local gatekeeper supports [ITU-T H.460.19], then disable all proxy functions and ITU-T H.245 address rewrites, and disable STUN support (if enabled) on the remote endpoint. Media shall proxy locally only. This shall be indicated by media strategy indicator 4 (**local proxy**). If, on the condition that both endpoints and the local gatekeeper support Annex B and the NAT type combination is suitable for Annex B (refer to Table B.1), the gatekeeper may provide Annex B support. The endpoints shall follow the procedure prescribed in Annex B to probe for a direct route. This shall be indicated by a media strategy indicator 8 (**external NAT probe**).

If matching is not obtained with any of the above and remote gatekeeper supports [ITU-T H.460.19], then disable all proxy functions and ITU-T H.245 address rewrites, and disable STUN support (if enabled) on the local endpoint. Media shall proxy remotely only. This shall be indicated by media strategy indicator 5 (**remote proxy**).

If none of the above rules apply, then there is a possibility the media streams cannot be established and the call will most likely fail. Upon this condition, the gatekeeper shall immediately send an ARJ to the calling endpoint with call end reason **noRouteToDestination**. This shall be indicated by media strategy indicator 100 (**NAT media failure**).

9.6 Reporting NAT strategy results to the endpoint

The local gatekeeper shall transmit the **MediaStrategy** in either the ACF or ARJ to the local endpoint.

Table 11 – MediaStrategy parameter

Parameter name:	MediaStrategy
Parameter description:	Indicates what method to use to establish media between the ITU-T H.323 devices.
Parameter identifier type:	Standard
Parameter identifier value:	8
Parameter type:	number8
Parameter cardinality:	One and only one

On receipt of any media strategy indicator other than 2 (**local media master**), all NAT support features (including STUN) shall be disabled for this call. In this case, it is assumed that the endpoint does not require assistance, as the media will be proxied via an ITU-T H.460.19 server, or the remote party will provide the assistance directly.

On receipt of a media strategy indicator other than 4 (**local proxy**) or 5 (**remote proxy**), ITU-T H.460.19 support shall be disabled for this call. The ITU-T H.460.19 feature shall not be advertised in accordance with clause 7.1.1 of [ITU-T H.460.19].

On receipt of a media strategy indicator 2 (**local media master**), STUN shall be enabled, the ports shall be opened via STUN procedures and the local ITU-T H.245 address shall be rewritten to the external IP of the NAT box. The endpoint must be placed into **Master Mode**.

In **Master Mode**, the supplied ITU-T H.245 address and port shall be ignored and no RTP/RTCP packets are to be transmitted until the first RTP/RTCP packets are received from the remote endpoint. On receipt of the first packet, the received apparent IP address and port are set as the target to which to send media. This function allows the remote endpoint to open pinholes in its NAT first to establish direct media connectivity.

On receipt of a media strategy parameter 100 (**NAT media failure**), no action shall be taken as the gatekeeper has determined that the call cannot find a suitable media pathway and has rejected the call.

10 Placing the call

Once the appropriate media strategy is determined and reported to the calling endpoint via the ACF, it shall be included in the feature advertisement in the Setup sent to the remote endpoint.

When sending the media strategy indicator to the remote party, it shall be rewritten to change local setting values to remote and vice versa, i.e., 2 (**local media master**) becomes 3 (**remote media master**), 4 (**local proxy**) becomes 5 (**remote proxy**).

Once received by the remote endpoint, the media strategy indicator shall be used to configure the call receiver's endpoint and shall be sent to the receiver's gatekeeper via the ARQ to notify the remote gatekeeper how to configure itself for the proposed media strategy. The rules of clause 9 shall be applied to both the remote endpoint and the remote gatekeeper.

11 Special considerations

11.1 RTP/SRTP/RTCP/SRTCP keep-alive packet

For the purpose of opening and ensuring pinholes in the NAT/FW, the endpoint behind the NAT/FW, which is subject to media strategy indicator 3 (**remote media master**) must send an initial media or a keep-alive packet to open pinholes in the NAT/FW and may send periodic keep-alive packets to ensure the pinholes in the NAT/FW do not close.

For RTP/STRP channels, the keep-alive packet shall have a payload type equal to the media payload type, empty payload size and sequence number starting at any arbitrary value and incrementing by one for each new keep-alive packet.

For RTCP/SRTCP channels, the keep-alive packet shall be an RTCP/SRTCP packet containing an SR (sender report) only and shall comply with the specifications in [IETF RFC 3550] and [IETF RFC 3711], respectively.

The timing to send keep-alive packets may be between 5 s and 30 s of detected silence or some arbitrary continuous interval up to 30 s to ensure the pinholes in the NAT/FW do not close.

11.2 Timeouts waiting for first packet

Where an endpoint uses media strategy indicator 2 (**local media master**) and waits to receive the first packet from the remote endpoint to determine the target to which to send its media packets, a recommended timeout of 3 to 5 s may be employed. If the endpoint fails to detect the media packets from the remote party within that time period, the media shall be considered failed and the media channel closed.

Annex A

Probing for same NAT

(This annex forms an integral part of this Recommendation.)

Due to the nature of NAT/FW devices, it is impossible for a party outside of the NAT/FW to determine with certainty whether two devices behind the same NAT/FW device are able to stream media directly between each other. It may also be impossible for the endpoints to even know whether they are reachable directly, especially if one endpoint is nested behind a subordinate NAT/FW and connectivity establishment is only possible in one direction. This can only be determined by sending a packet and receiving a reply packet. Also, there remains the possibility that they cannot establish connectivity directly at all.

The purpose of this annex is to provide a mechanism to avoid using an ITU-T H.460.19 proxy server. In scenarios where an ITU-T H.460.19 media proxy is to be provided initially, this annex requires that the endpoints probe for a direct route between each other and, once a direct route is verified, media is switched to that direct route and an ITU-T H.460.19 server is no longer required.

Where both endpoints support this annex, and having been notified that they reside behind the same NAT/FW device (via media strategy indicator 7 (**same NAT/FW**)), the endpoints shall follow this annex to determine if direct media connectivity can be established.

A.1 Notification of direct connectivity probing

Endpoints supporting this annex and being notified of media strategy indicator 7 (**same NAT/FW**) shall include in the **GenericInformation** field of the ITU-T H.245 OLC and responding ITU-T H.245 OLCAck, a packed encoding rules (PER) encoded parameter with the object identifier (OID) as specified in Table A.1. The **messageContent** shall contain an array of string representations of the channel unique identifier (CUI) and the alternate RTP and RTCP address and port. The identifiers shall be in accordance with Table A.2.

The channel unique identifier (CUI) shall be an endpoint-generated identifier for the purposes of identifying, authenticating and allocating received direct connectivity RTCP probe packets.

Table A.1 – OID for same NAT generic message

Object identifier value	OID name
{-itu-t (0) recommendation (0) h (8) 460 24 ~~A~~annexA (1)-}	H.460.24 OLC Same NAT probe

Table A.2 – ITU-T H.245 generic parameters

Identifier	Indication	Raw type	Encoded type
0	Channel unique identifier	IA5String	octetString
1	Media channel IP address and port number	TransportAddress (as defined in ITU-T H.245)	octetString
2	Media control channel IP address and port number	TransportAddress (as defined in ITU-T H.245)	octetString

The RTP and RTCP IP address and port in the generic parameters shall mirror the values in the media channel and media control channel parameters contained in the same ITU-T H.245 OLC. The CUI shall be used solely to verify the source of received probe packets.

A.2 Procedure to probe direct connectivity

Once media connectivity has been established via an ITU-T H.460.19 server, each endpoint shall send at least five **RTCP probe packets** (see Table A.3 for format) containing a SHA-1 hash of the ITU-T H.225.0 call identifier with the CUI supplied by the responding endpoint to the alternate RTCP address and port received by the responding endpoint with RTCP subtype 0 (**Request**). This shall indicate that this is a connectivity request. If an endpoint receives an RTCP probe packet with subtype 0 (**Request**) with a matching SHA-1 hash computed by SHA-1(Call Identifier || CUI), it shall indicate that direct connectivity for this call was achieved in at least one direction. The local endpoint shall stop sending request RTCP packets and replace the alternate IP address and port with the detected IP address and port of the received request RTCP packet. It shall return an RTCP packet with subtype 1 (**Reply**) to the detected IP and port. This will notify the remote endpoint of bidirectional connectivity success. Upon receipt of the reply RTCP probe packet, the endpoint originating the successful RTCP probe packet shall also stop sending any further RTCP probe packets.

Once direct connectivity has been verified either by sending or receiving the reply RTCP probe packet, the endpoint shall transmit a **genericIndication** message to the responding endpoint containing the same OID shown in Table A.1. If both endpoints transmit and receive a **genericIndication** message containing the OID from Table A.1, then each endpoint can assume that bidirectional connectivity has been verified. At this point, each endpoint shall stop sending media and control to the supplied ITU-T H.245 OLC/OLCAck address and begin to stream media and control to the verified alternate or detected RTP/RTCP address and port. The RTP channel shall be established in the same order, even if the channel is unidirectional, as the successful RTCP probe packet, that is, the successful RTCP probe packet receiver shall wait for the first RTP packet from the RTCP probe packet sender to enable it to assign the detected IP address and port to send media.

The receipt of the **genericIndication** message from both endpoints shall also indicate to the ITU-T H.460.19 server that media and control will be transmitted directly.

Note that during this brief transition period, RTP or RTCP packets may be received at the ITU-T H.460.19 server or on either the original or alternate/detected port pairs.

A.3 Probe packet format

The probe packet shall be constructed as an Application-Defined RTCP packet in accordance with clause 6.7 of [IETF RFC 3550] with the settings specified in Table A.3.

Table A.3 – Format of RTCP probe packet

Parameter	Value
Packet type	204 (in accordance with clause 12.1 of [IETF RFC 3550])
Subtype	Probe type (values as per Table A.4)
Name	"24.1"
Application data	SHA-1(Call Identifier || CUI)

Table A.4 – Probe types

Parameter	Indication
0	Request
1	Reply

Annex B

External NAT probing

(This annex forms an integral part of this Recommendation.)

With certain configurations, it may be possible, where a call is placed between two endpoints behind distinct NAT/FW devices and neither are Type 2 (full cone NAT), to coerce direct media to flow directly between the endpoints, removing the need to proxy media. Understanding the NAT behaviour as per [IETF RFC 3489] and using an ordered progression of probing with RTP/RTCP probe packets, direct media pathways may be established. Table B.1 indicates the types of NAT combinations supported by this annex.

Table B.1 – NAT type combinations supported for Annex B

Local	**Remote**
3	3, 4, 5
4	3, 4
5	3

Where both endpoints support this annex, and having been signalled a media strategy of 8, (*Cone Nat Probe*), the endpoints shall follow the steps in this annex to establish direct media connectivity.

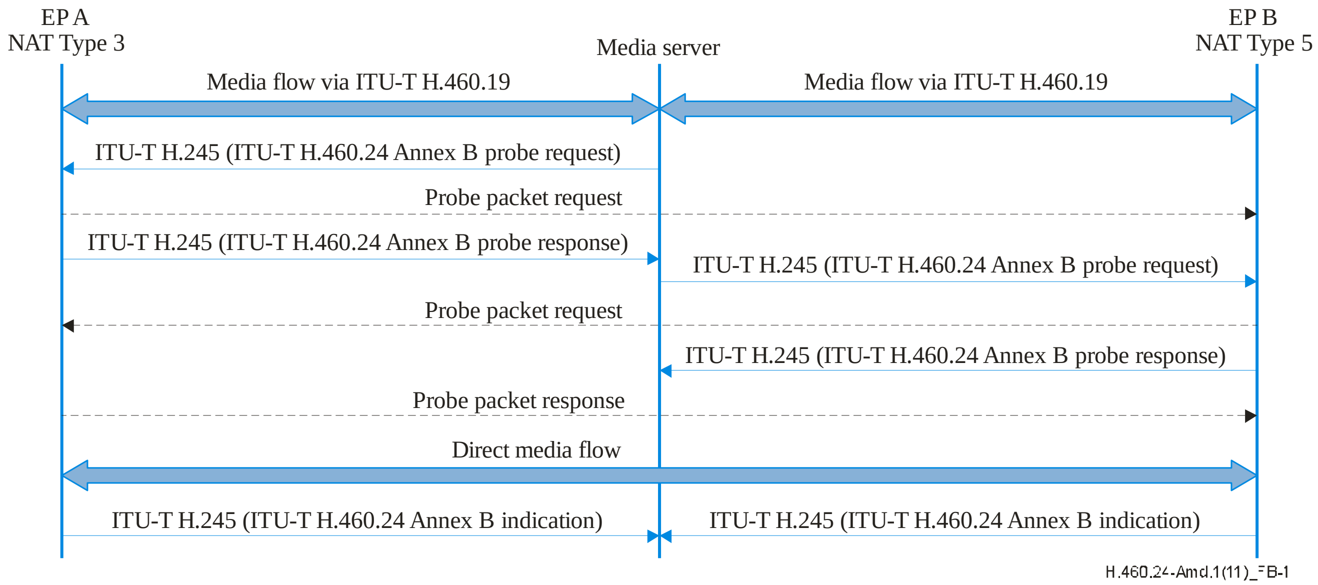
EP A
NAT Type 3
Media server
EP B
NAT Type 5
Media flow via ITU-T H.460.19
Media flow via ITU-T H.460.19
ITU-T H.245 (ITU-T H.460.24 Annex B probe request)
Probe packet request
ITU-T H.245 (ITU-T H.460.24 Annex B probe response)
ITU-T H.245 (ITU-T H.460.24 Annex B probe request)
Probe packet request
ITU-T H.245 (ITU-T H.460.24 Annex B probe response)
Probe packet response
Direct media flow
ITU-T H.245 (ITU-T H.460.24 Annex B indication)
ITU-T H.245 (ITU-T H.460.24 Annex B indication)
H.460.24-Amd.1(11)_FB-1

Figure B.1 – Sample call flow for direct media establishment via Annex B

B.1 Background

NAT behaviour plays a large component in establishing direct media pathways between endpoints. For instance, if either of the endpoints resides behind a Type 2 *full cone NAT* (Table 8 of [ITU-T H.460.23]), then media strategy 2 or 3 (refer to Table 9) may be utilized. In doing so, it takes advantage of the behaviour wherein media may be sent to an opened pinhole in the NAT/FW without the device behind that NAT/FW having first sent a packet out to the originator of the media stream. While Type 2 NAT/FW is common, there are conditions where direct media is not easily established and media would need to proxy. The purpose of this annex is to probe for and establish direct media pathways and remove the requirement to proxy media via an ITU-T H.460.19 server.

Table B.2 – OID for External NAT Probe generic message

Object identifier value	OID name
{-itu-t (0) recommendation (0) h (8) 460 24 annexB (2)-}	H.460.24 OLC External NAT Probe

Table B.3 – ITU-T H.245 generic parameters

Identifier	Request	Raw type	Encoded type
1	Alternate Transport Addresses	H.460.24 Annex B AlternateAddresses	octetString

B.2 Procedure to probe for direct connectivity

Once media connectivity has been established via an ITU-T H.460.19 server, the gatekeeper shall initiate the Annex B direct media probe. The gatekeeper shall make the determination of which endpoint to commence the Annex B procedure with. The selection shall be the calling endpoint, but if the NAT type is Type 5, *Symmetric*, it shall be the called endpoint. All **genericRequest** and **genericResponse** messaging is from gatekeeper to endpoint and visa versa, and shall not be forwarded to the other endpoint. The **genericIndication** messaging shall be routed end-to-end.

The gatekeeper shall transmit a **genericRequest** message containing the OID in Table B.2 and a generic parameter, as per Table B.3, containing an encoded **AlternateAddresses** element. The element shall contain a sequence of **AlternateAddress** fields containing the detected apparent source addresses for media and control and session id for each session requiring direct media probing. The **sessionCUI** field shall be omitted. Once the endpoint has received the **genericRequest,** it shall send at least three RTP/SRTP and three RTCP/SRTCP probe packets (refer to clause B.3 for the format) to the corresponding media/control address for each session from the associated local media/control addresses for that media session.

A response to the probe packets is not expected, as this action is designed merely to open media pinholes in the local NAT/FW to the remote NAT/FW. Once the probe packets have been sent, the endpoint shall respond back to the gatekeeper via a **genericResponse** message containing the OID of Table B.2 and an encoded **AlternateAddresses** element containing a sequence of **AlternateAddress** fields. Each **AlternateAddress** shall contain the applicable session ID and an endpoint generated **sessionCUI** identifier for the purpose of identifying, authenticating and allocating received RTCP probe packets. The media and control address fields shall be omitted.

Upon receipt of the **genericResponse**, the gatekeeper initiates a **genericRequest** to the other endpoint with an encoded **AlternateAddress** element containing a sequence of **AlternateAddress** fields containing the detected apparent source addresses for media and control, session ID and received **sessionCUI** for each session requiring direct media probing of the first NAT/FW. The second endpoint, upon receiving the **genericRequest,** shall send at least three RTP/SRTP and three

RTCP/SRTCP probe packets (refer to clause B.3 for the format) to the corresponding media and media control addresses for each session from the associated local media and media control addresses with the received **sessionCUI** for that media session. Once the probe packets have been sent, the endpoint shall respond back to the gatekeeper via a **genericResponse** message containing the OID in Table B.2. The **AlternateAddress** element shall be omitted.

It is expected that the first endpoint may receive the probe packets from the second endpoint, and it shall authenticate the appropriate RTCP/SRTCP probe packets for each session and respond back with at least 3 response probe packets to the apparent detected source address of the received probe packet. The first endpoint shall send to the gatekeeper a **genericIndication** message containing the OID in Table B.2 with an encoded **AlternateAddress** element containing a sequence of **AlternateAddress** fields with the **sessionID** (optional fields omitted) for each detected direct media pathway. This will notify the gatekeeper that a direct media pathway has been achieved for that session.

Upon receiving the response probe packet, the second endpoint shall signal to the gatekeeper a **genericIndication** containing the OID in Table B.2 with an encoded **AlternateAddress** element containing a sequence of **AlternateAddress** fields with the sessionID (optional fields omitted) for each verified direct media pathway.

The receipt of the **genericIndication** message from both endpoints shall also indicate to the ITU-T H.460.19 server that media and control for the associated session will be transmitted directly.

Note that during this brief transition period, RTP or RTCP packets may be received at the ITU-T H.460.19 server on either the original or alternate/detected port pairs.

B.3 Probe packet format

For RTP/SRTP the probe packet shall have a payload type equal to the media payload type, empty payload size and sequence number starting at some arbitrary value and incrementing by one for each new probe packet.

The RTCP/SRTCP probe packet shall be constructed as an Application-Defined RTCP packet in accordance with clause 6.7 of [IETF RFC 3550] with the settings specified in Table B.4.

Table B.4 – Format of RTCP probe packet

Parameter	**Value**
Packet type	204 (in accordance with clause 12.1 of [IETF RFC 3550])
Subtype	Probe type (values as per Table B.5)
Name	"24.2"
Application data	Call Identifier or SHA-1(Call Identifier || sessionCUI) (Note)
NOTE – SHA-1 is required if **sessionCUI** is supplied in **genericRequest**.	

Table B.5 – Probe types

Parameter	**Indication**
0	Request
1	Response

B.4 Annex B ASN.1 code

```
MEDIA-TRAVERSAL {itu-t(0) recommendation(0) h(8) 460 24 2 asn1-module(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
IMPORTS
               TransportAddress
FROM MULTIMEDIA-SYSTEM-CONTROL -- See Rec. ITU-T H.245;

AlternateAddresses ::= SEQUENCE
{
     addresses     SEQUENCE OF AlternateAddress,
     ...
}

AlternateAddress ::= SEQUENCE
{
     sessionID   INTEGER(0..255),
  sessionCUI   IA5String                OPTIONAL,
     rtpAddress      TransportAddress   OPTIONAL,
     rtcpAddress     TransportAddress   OPTIONAL,
     ...
}

END
```

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