International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.460.19

(09/2005)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Supplementary services for multimedia

Traversal of H.323 media across network address translators and firewalls

ITU-T Recommendation H.460.19

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 AND TRIPLE-PLAY MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619

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

ITU-T Recommendation H.460.19

Traversal of H.323 media across network address translators and firewalls

Summary

This Recommendation extends ITU-T Rec. H.323 by defining the NAT/FW traversal mechanism for media. Together with an appropriate mechanism for signalling traversal, such as H.460.18, it may be used as a solution for the NAT/FW traversal problem by H.323.

Source

ITU-T Recommendation H.460.19 was approved on 13 September 2005 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation H.460.19

Traversal of H.323 media across network address translators and firewalls

1 Scope

This Recommendation defines a mechanism for media communication between two H.323 entities, separated by one or more NAT/FW devices.

This Recommendation addresses NAT/FW traversal for RTP; RTP encrypted using H.235 and SRTP media streams only. NAT/FW traversal for media transported by other protocols is for further study.

It also defines a mechanism to use the same transport address for several media channels, which permits reduction of the number of "pinholes" open in the NAT/FW device and reduces the number of Media Channel and Media Control Channel transport addresses used by H.323 entities.

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 Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

– ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication*.

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.

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

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

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

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

3 Definitions

This Recommendation defines the following terms:

3.1 apparent source address: The source IP address received in the IP packet header, combined with the source port number received in the UDP or TCP header of the same packet. The presence of NAT may cause this to differ from the sender's source address and source port number.

3.2 client: An endpoint compliant with H.460.19 specifications and performing H.460.19 client functionality. An H.460.19 client is normally located on the internal network.

3.3 endpoint: An H.323 terminal, Gateway, or MCU. An endpoint can call and be called. It generates and/or terminates information streams.

3.4 external network: A network connected to the firewall through the firewalls public interface. Typically, but not limited to, the Internet.

3.5 **H.460.19 entity**: A client or server.

3.6 **internal network**: A network connected to the NAT/FW through the NAT/FW's private interface.

3.7 **media channel**: An RTP or an SRTP channel.

3.8 **media control channel**: An RTCP or SRTCP channel.

3.9 **multiplexed media mode**: A mechanism which enables managing multiple RTP/RTCP or SRTP/SRTCP sessions on a single pair of transport addresses as described in 7.2. Receivers choose whether or not to multiplex.

3.10 **OLC request**: Any one of:

- the **openLogicalChannel** message;
- the **openLogicalChannel** Fast Connect proposal message for transmission from caller to callee;
- the **openLogicalChannel** Fast Connect proposal accept message for transmission from callee to caller.

3.11 **OLC response**: Any one of:

- the **openLogicalChannelAck** message;
- the **openLogicalChannel** Fast Connect proposal accept message for transmission from caller to callee;
- the **openLogicalChannel** Fast Connect proposal message for transmission from callee to caller.

3.12 **peer**: An H.460.19 entity with which a particular H.460.19 entity is communicating.

3.13 **pinhole**: A temporary binding of an internal and an external transport address in the NAT/FW which allows the bidirectional passage of packets between those addresses.

3.14 **server**: An H.323 entity compliant with H.460.19 specifications and performing H.460.19 server functionality.

3.15 **transport address**: IP address and UDP/TCP port number.

4 Abbreviations

This Recommendation uses the following abbreviations:

LC	Logical Channel (per ITU-T Rec. H.245)
NAT/FW	Network Address Translator and/or Firewall
OID	Object Identifier
OLC	Open Logical Channel
RTCP	Real-Time Control Protocol (according to RFC 3550)
RTP	Real-Time Protocol (according to RFC 3550)
SRTCP	Secure Real-Time Control Protocol (according to RFC 3711)
SRTP	Secure Real-Time Protocol (according to RFC 3711)
SSRC	Synchronization Source
TCP	Transmission Control Protocol
TPKT	Transport Protocol Data Unit Packet

5 Conventions

In this Recommendation the following conventions are used:

"Shall" indicates a mandatory requirement.

"Should" indicates a suggested but optional course of action.

"May" indicates an optional course of action rather than a recommendation that something take place.

6 Architecture

This Recommendation addresses a network which is divided into an internal and external network by a NAT/FW (see Figure 1). Typically, the internal network will be a private network. The external network will typically be a public network such as the Internet, but may alternatively be another private network.

Figures 1, 2 and 3 show possible ways in which this Recommendation may be deployed. Items in bold text: H.323 Endpoint with H.460.19 Client, H.460.19 Client Proxy and H.460.19 Server are referred to in this Recommendation. Other devices are shown for completeness.

The internal network contains an H.323 endpoint (the H.460.19 client) and the external network contains an H.460.19 server. These H.323 endpoints may be terminals, gateways or MCUs. Extensions to H.323 defined in this Recommendation provide modes that permit media streams to traverse NAT/FW devices.

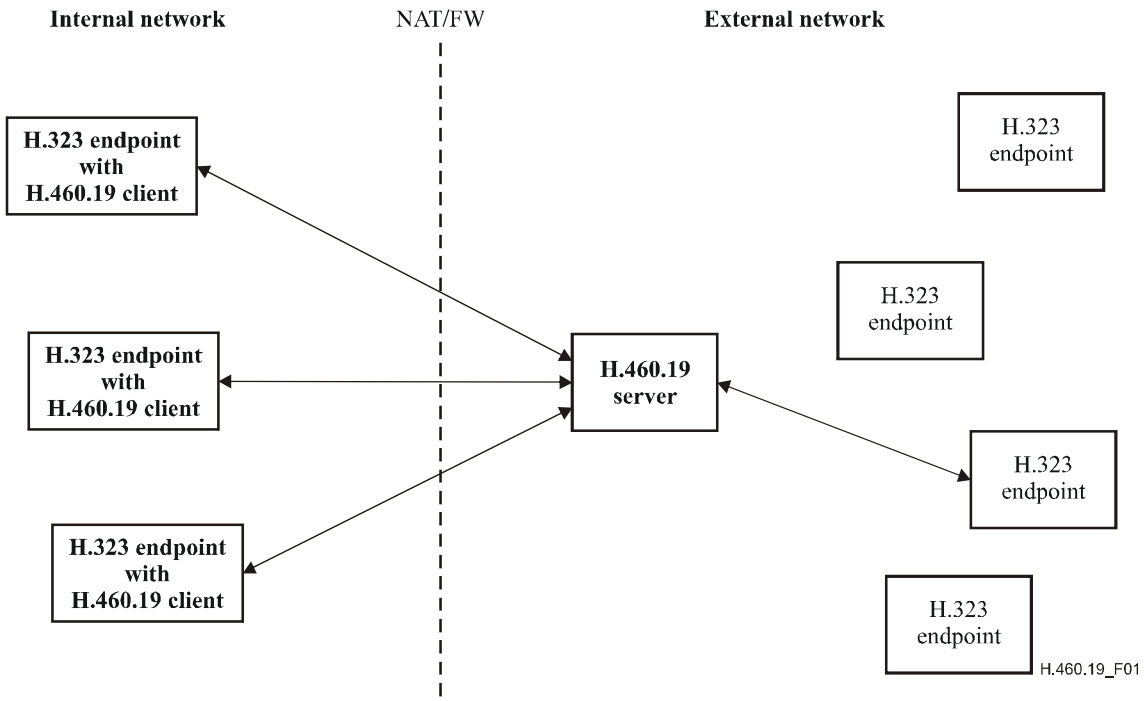

Figure 1/H.460.19 – Combined H.460.19 architecture

This Recommendation defines the "NAT/FW traversal procedure" and the "multiplexed media mode".

For communication between H.460.19 clients and H.460.19 servers, the multiplexed media mode is used together with the NAT/FW traversal procedure. The NAT/FW traversal procedure is used for client-to-server communication but not for client-to-client and server-to-server communication.

NAT/FWs typically permit traffic from the internal network, and typically permit traffic toward the internal network received in response to the original traffic toward the external network.

The Media Control Channel is inherently bidirectional and its packets in the direction toward the external network are used by the NAT/FW traversal procedure to permit Media Control Channel packets to traverse the NAT/FW toward the internal network.

Media Channel traffic is unidirectional. To permit Media Channel packets toward the internal network, this Recommendation defines a Keep Alive Channel. The client sends Keep-Alive media packets to the **keepAliveChannel** transport address provided by the server.

In the NAT/FW traversal procedure, the H.460.19 server sends Media Channel and Media Control Channel packets to the H.460.19 client to the address from which Keep Alive Channel and Media Control Channel packets were received by the H.460.19 server, instead of to the addresses specified in the **H2250LogicalChannelParameters.mediaChannel** and **H2250LogicalChannelParameters.mediaControlChannel** H.245 structures as in normal H.323 operation. The NAT/FW traversal procedure also requires usage of a keep-alive mechanism. The goal of the keep-alive mechanism is to ensure that there are no extended periods of "network silence" between the communicating Transport Addresses, which might result in closure of pinholes by the NAT/FW. The implementation of the Keep-Alive mechanism is mandatory in client to server direction.

The multiplexed media mode enables sending the Media Channel/Media Control Channel packets of several media sessions (which may be part of multiple calls) to the same pair of transport addresses on the H.460.19 client or server (or both), which can significantly reduce the number of pinholes in the NAT/FW. To facilitate multiplexed media mode, the multiplexing layer for use with media and media control packets is defined in this Recommendation.

The capability of a particular entity to send packets with this multiplexing layer is independent of the capability of the same entity to receive such packets. The multiplexed media mode may be supported for transmit and receive directions independently.

The capability of transmitting the multiplexed media mode means the capability to add the multiplexing layer to media and media control packets.

The capability of receiving the multiplexed media mode means the capability to remove the multiplexing layer from media and media control packets.

The procedures in this Recommendation allow negotiation of the support of these extensions and signalling of the specific extension parameters.

In order to support non-H.460.19 enabled (pre-existing) H.323 endpoints, the H.460.19 client functionality may be implemented by a proxy located on the internal network (see Figure 2).

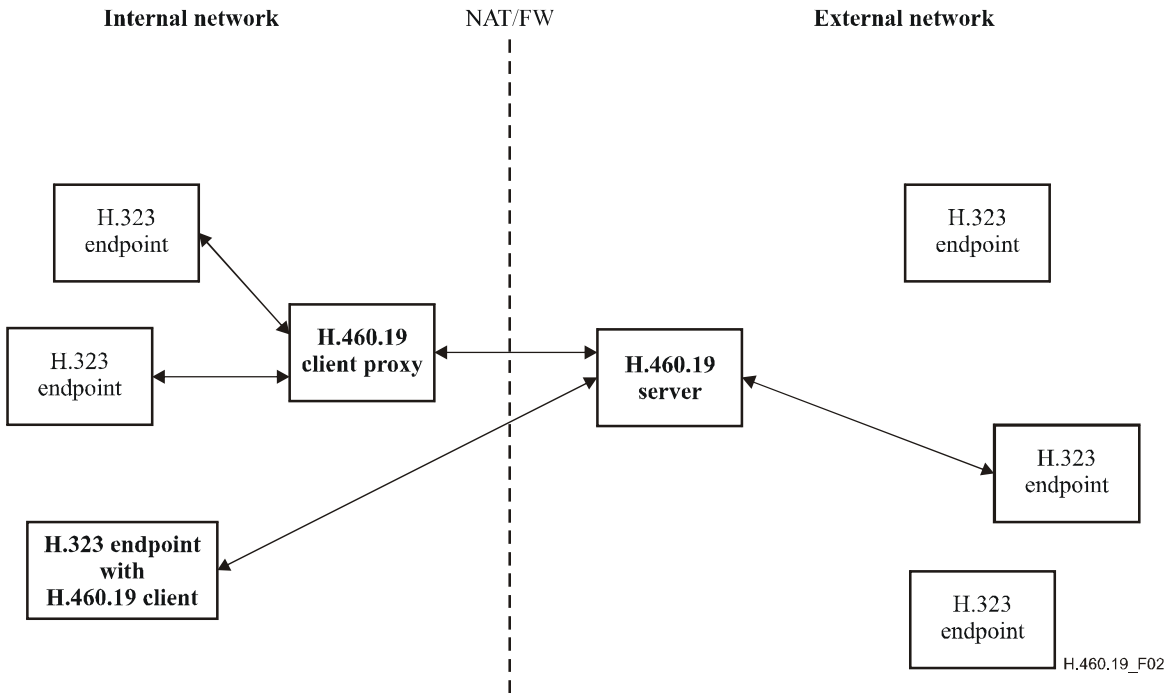

Figure 2/H.460.19 – Decoupled H.460.19 architecture

In Figure 3, Organization A on the left has a mix of H.460.19-enabled endpoints, and of non-H.460.19 H.323 endpoints making use of an H.460.19 proxy. Organization A has an H.460.19 server on their demilitarized zone, which provides media traversal and access to the external network for Organization A endpoints.

Organization B, on the right of Figure 3, has a pair of endpoints communicating with each other on the internal network, and H.460.19-enabled endpoints which communicate with endpoints on the external network (including, indirectly, Organization A endpoints) via a H.460.19 server operated by a service provider.

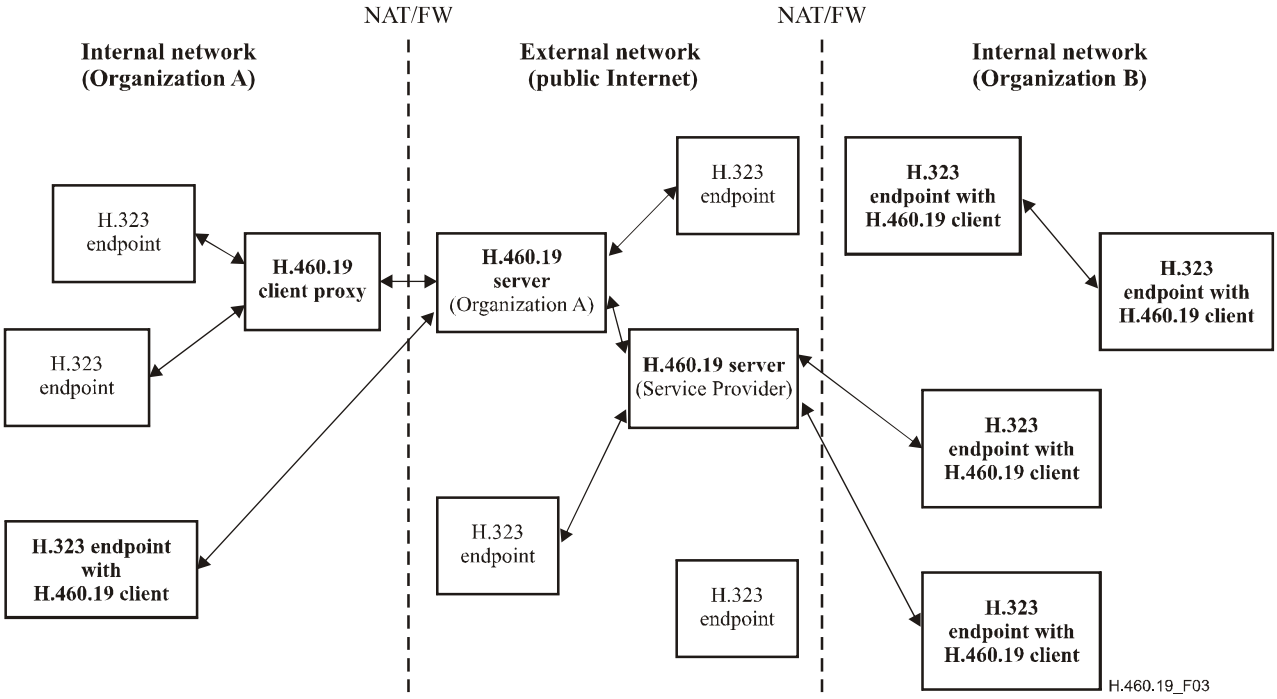

Figure 3/H.460.19 – H.460.19 double NAT/FW architecture

6.1 General requirements

H.460.19 entities shall support ITU-T Rec. H.460.18. Alternative call setup mechanisms may be supported as well.

Support of the NAT/FW traversal procedure, defined in 7.3.1, is mandatory for both H.460.19 clients and H.460.19 servers.

Support of transmission of the multiplexed media mode defined in 7.3.2 is mandatory for H.460.19 clients and optional for H.460.19 servers.

Support of reception of the multiplexed media mode defined in 7.3.2 is optional for both H.460.19 clients and H.460.19 servers.

The use of these procedures with multicast channels is for future study.

7 Procedures

7.1 Signalling procedures

7.1.1 Capabilities signalling

The capability to support H.460.19 functionality shall be signalled by including the **mediaNATFWTraversal** feature identifier defined in 7.4.1 in the **supportedFeatures** field of the following H.225.0 call signalling messages sent in each call:

a) For outgoing calls the feature identifier shall be included in the SETUP message.

b) For incoming calls the feature identifier shall be included in CALL PROCEEDING, ALERTING and CONNECT messages, and in FACILITY messages with **facilityReason** set to **forwardedElements**.

The capability to transmit multiplexed media mode shall be signalled by the servers by including the **supportTransmitMultiplexedMedia** parameter, defined in 7.4.2, in the same **supportedFeatures** field.

Clients shall support transmission of multiplexed media and shall always include the **supportTransmitMultiplexedMedia** parameter in their **supportedFeatures** field.

The capability to receive multiplexed media mode (to de-multiplex) shall be indicated by the presence of the **multiplexID** field in the Traversal Parameters in the OLC Request and OLC Response messages as defined in 7.4.5.

The H.460.19 server shall include the **mediaTraversalServer** parameter, defined in 7.4.3 in the same **supportedFeatures** field.

7.1.2 Logical channel signalling

The use of the procedures defined in this Recommendation shall be negotiated for each Logical Channel (LC) using the H.245 **openLogicalChannel** procedure or in the **openLogicalChannel** request or response in the case of Fast Connect.

To signal a request to use the procedures of this Recommendation on a particular LC, the H.460.19 server shall include the Traversal Parameters field defined in this Recommendation in the **genericInformation** field of the messages defined in Table 1, according to the procedures in 7.4:

Table 1/H.460.19 – Messages used to initiate H.460.19 procedures

LC direction	Message
Toward H.460.19 server	**OLC Response message**
Toward H.460.19 client	**OLC Request message**

H.460.19 entities shall setup LCs according to the procedures given in the following clauses, and using the transport addresses given in Table 2 below.

The H.460.19 server shall include the **keepAliveChannel** field in the **Traversal Parameters** of the OLC Request message.

In all cases, the H.460.19 client shall send Keep-Alive packets as defined in 7.3.1.1.

Table 2/H.460.19 – Transport addresses for channels between H.460.19 client and server

Channel	Source	Source transport address	Dest.	Destination transport address
Media Channel	client	Any port on H.460.19 client.	server	**mediaChannel** destination address on H.460.19 server in server's OLC Response message.
Media Channel	server	**keepAliveChannel** destination address on H.460.19 server in server's OLC Request message.	client	Apparent Keep-Alive source address on H.460.19 client (media sent only after receipt of Keep-Alive from H.460.19 client).
Keep-Alives	client	H.460.19 client's desired Media Channel destination port on H.460.19 client.	server	**keepAliveChannel** destination address on H.460.19 server in server's OLC Request message.
Media Control Channel	client	H.460.19 client's desired Media Control Channel destination port on the client. The **mediaControlChannel** destination address in all OLC Request and OLC Response messages sent by a given client for a given call and value of **sessionID** shall contain this same transport address. NOTE – The H.460.19 server ignores this **mediaControlChannel** value.	server	**mediaControlChannel** destination address on H.460.19 server in server's OLC Request or OLC Response message – whichever was received more recently for the given call and value of **sessionID**.
Media Control Channel	server	**mediaControlChannel** destination address on H.460.19 server in H.460.19 server's OLC Request or OLC Response message – whichever was transmitted more recently for the given call and value of **sessionID**.	client	Apparent Media Control Channel source address on H.460.19 client (media control channel sent only after receipt of media control packet from H.460.19 client).

7.1.2.1 Establishment of LCs from H.460.19 client to H.460.19 server

Figure 4 illustrates the establishment of an LC from an H.460.19 client to an H.460.19 server.

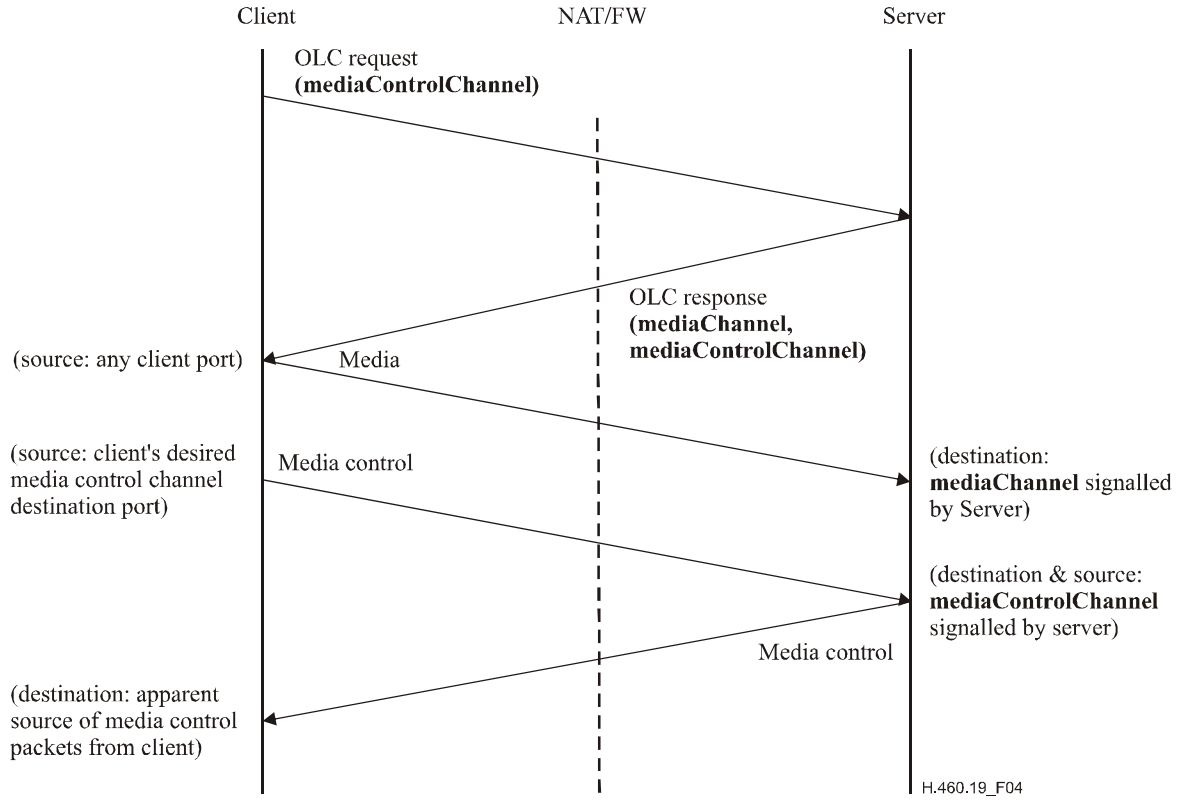

Figure 4/H.460.19 – Opening an LC toward the H.460.19 server

The H.460.19 client shall transmit Media Channel and Media Control Channel packets to the transport addresses indicated in the **mediaChannel** and **mediaControlChannel** fields, respectively, of the H.460.19 server's OLC Response message.

The H.460.19 server shall wait for receipt of at least one Media Control Channel packet from the H.460.19 client for the LC, and then send Media Control Channel packets for the LC to the H.460.19 client, with a destination transport address equal to the apparent source transport address of the Media Control Channel packet received from the H.460.19 client.

7.1.2.2 Establishment of LCs from H.460.19 server to H.460.19 client

Figure 5 illustrates the establishment of an LC from an H.460.19 server to an H.460.19 client.

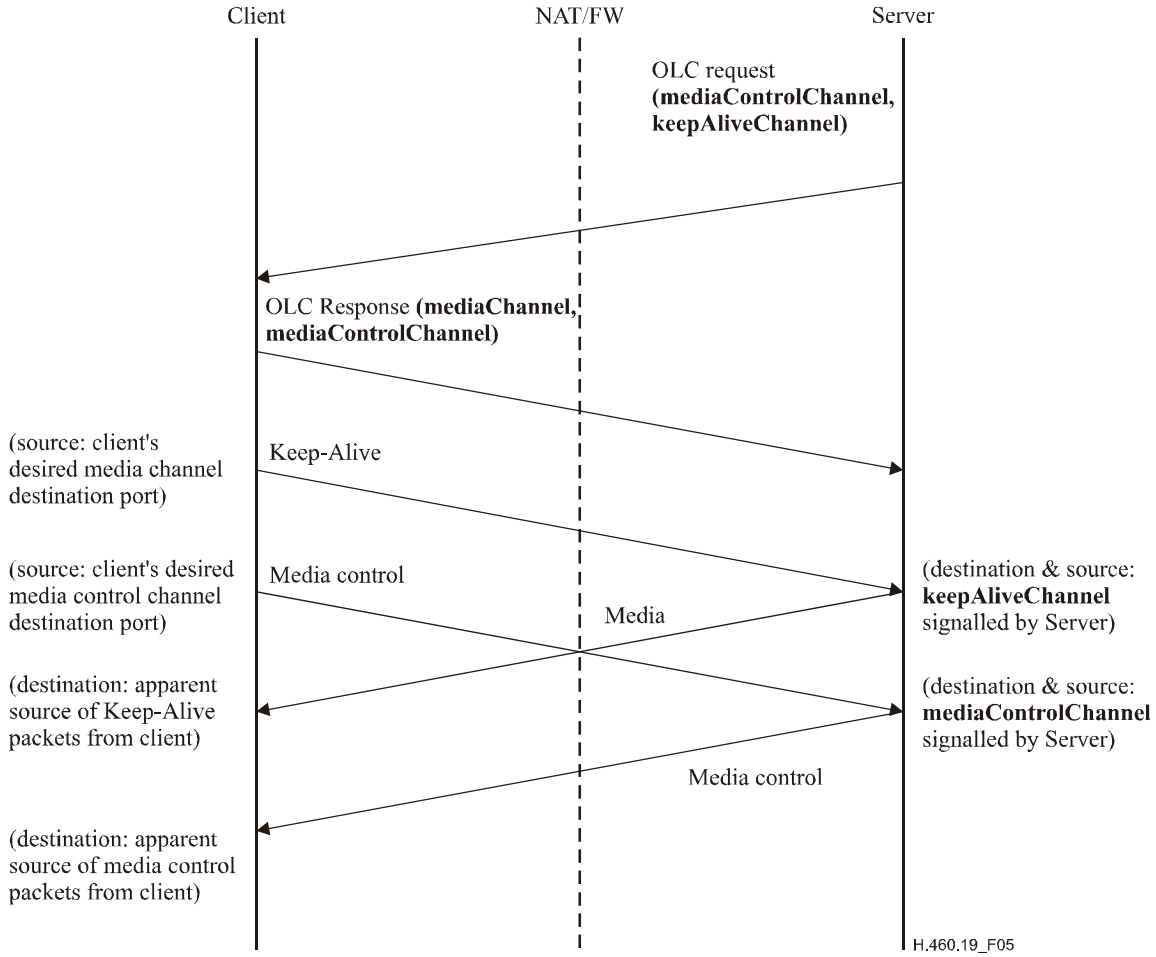

Figure 5/H.460.19 – Opening an LC toward the H.460.19 client

The H.460.19 client shall transmit Media Control Channel and Keep-Alive packets to the transport addresses indicated in the **mediaControlChannel** and **keepAliveChannel** fields, respectively, of the H.460.19 server's OLC Request message.

The H.460.19 server shall wait for receipt of at least one Keep-Alive packet from the H.460.19 client for the LC, and then send Media Channel packets for the LC to the H.460.19 client, with a destination transport address equal to the apparent source transport address of the Keep-Alive packet received from the H.460.19 client.

The H.460.19 server shall wait for receipt of at least one Media Control Channel packet from the H.460.19 client for the LC, and then send Media Control Channel packets for the LC to the H.460.19 client, with a destination transport address equal to the apparent source transport address of the Media Control Channel packet received from the H.460.19 client.

7.1.2.3 Overlapping establishment of LCs between H.460.19 client and H.460.19 server

Figure 6 illustrates the simultaneous establishment of LCs between an H.460.19 client and an H.460.19 server.

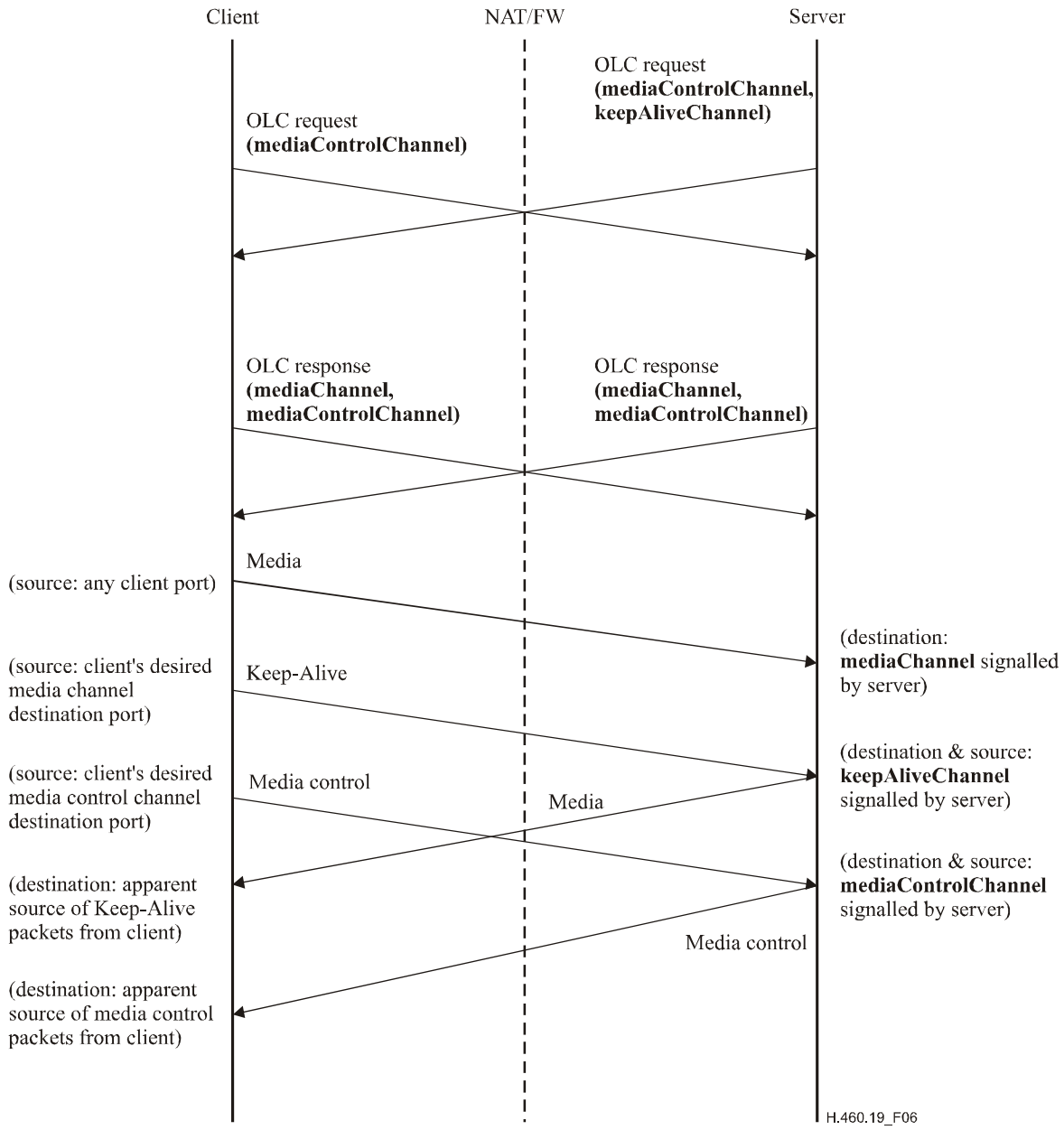

Figure 6/H.460.19 – Overlapping opening of a bidirectional pair of LCs between an H.460.19 server and an H.460.19 client (informative)

The H.460.19 client shall transmit Media Channel, Media Control Channel, and Keep-Alive packets to the transport addresses indicated in the **mediaChannel**, **mediaControlChannel**, and **keepAliveChannel** fields, respectively, of the H.460.19 server's OLC Request or OLC Response message, whichever was received more recently for the same call and using the same value of **sessionID**.

The H.460.19 server shall wait for receipt of at least one Keep-Alive packet from the H.460.19 client for the LC, and then send Media Channel packets for the LC to the H.460.19 client, with a destination transport address equal to the apparent source transport address of the Keep-Alive packet received from the H.460.19 client.

The H.460.19 server shall wait for receipt of at least one Media Control Channel packet from the H.460.19 client for the LC, and then send Media Control Channel packets for the LC to the H.460.19 client, with a destination transport address equal to the apparent source transport address of the Media Control Channel packet received from the H.460.19 client.

7.1.2.4 Establishment of LCs from H.460.19 client to H.460.19 client

Establishment of LCs between two H.460.19 clients shall be according to normal H.323 procedures.

The H.460.19 client shall not transmit Keep-Alive packets when the peer is also H.460.19 client.

The procedures for the multiplexed media mode may be used between two H.460.19 clients.

7.1.2.5 Establishment of LCs from H.460.19 server to H.460.19 server

Establishment of LCs between two H.460.19 servers shall be according to normal H.323 procedures.

The procedures for the multiplexed media mode may be used between two H.460.19 servers.

An H.460.19 server may include the **keepAliveChannel** parameter in its OLC Request message.

The H.460.19 server shall not transmit Keep-Alive packets when the peer is also H.460.19 server.

7.2 Multiplexed media mode

In the multiplexed media mode, multiple RTP/RTCP or SRTP/SRTCP sessions may be carried on a single pair of transport addresses.

In the following clauses, the term multiplexing means the ability to add the multiplexing layer as defined in 7.3.2, and the term de-multiplexing means the ability to understand and remove the multiplexing layer as defined in 7.3.2.

NOTE – Use of the multiplexing layer does not necessarily require or cause actual multiplexing of media or media control packets onto the same transport addresses. Destination transport addresses in all cases are chosen by the receiver of each stream. In the multiplexed media mode, receivers are free to either re-use destination transport address (actual multiplexing) or to choose unique destination transport addresses for each received stream.

Support of multiplexing of Media Channel and Media Control Channel packets is mandatory for H.460.19 clients.

Support of multiplexing of Media Channel and Media Control Channel packets is optional for H.460.19 servers and is signalled by specifying the **supportTransmitMultiplexedMedia** parameter as defined in 7.4.2.

Both H.460.19 clients and H.460.19 servers may support de-multiplexing of received Media Channel and Media Control Channel packets. Support of this optional mode is signalled by including the **multiplexID** field in the Traversal Parameters in the OLC Request and OLC Response messages as defined in 7.4.5. Support of de-multiplexing may be chosen on a LC-by-LC basis.

7.2.1 Requesting the multiplexed media mode

Only H.460.19 entities that support de-multiplexing may initiate use of the multiplexed media mode.

An H.460.19 entity "A" (either an H.460.19 server or an H.460.19 client) may initiate multiplexing of the Media, Media Control and Keep-Alive channels sent from an H.460.19 client to entity A.

An H.460.19 entity "A" (either an H.460.19 server or an H.460.19 client) may initiate multiplexing of the Media, Media Control and Keep-Alive Channels sent from an

H.460.19 server to entity A, only if the H.460.19 server supports multiplexing as indicated by **supportTransmitMultiplexedMedia** parameter of the server's feature identifier as defined in 7.4.2.

To initiate multiplexing toward itself for a given LC, entity A shall include a **multiplexID** field in its OLC Request or OLC Response message sent to the peer H.460.19 entity.

NOTE 1 – A **multiplexID** field may be included in an OLC Request message in order to request multiplexing of the Media Control Channel and Keep-Alive channel in the direction toward the requesting entity.

Entity A shall assign a unique **multiplexID** value for each set of multiplexed LCs for the given call and value of **sessionID**.

NOTE 2 – The pair of LCs for the given call and value of **sessionID** establishes a Media Channel and a Media Control Channel in the direction toward the client and a Keep-Alive Channel and a Media Control Channel in the direction toward the server. The packets, of these channels, sent towards either of the entities include the **multiplexID** provided by the entity.

If the **multiplexID** field was present in the message, the peer H.460.19 entity shall transmit Media Channel, Media Control Channel and Keep-Alive packets for the LCs in the multiplexed mode, identifying each packet with the **multiplexID** value as defined in 7.3.2.

Entity A shall receive Media Channel, Media Control Channel and Keep-Alive packets for the LCs in the multiplexed media mode, and use the received value of the **multiplexID** in each packet as defined in 7.3.2.

If an OLC Request message contains **multiplexID**, then the OLC Response message sent by the same entity for the same call and value of **sessionID** shall contain **multiplexID** with the same value.

NOTE 3 – These OLC Request and OLC Response messages belong to two different LCs established in opposite directions for the given call and **sessionID**.

If an OLC Request message contains a **multiplexID** field, then it also shall contain a **multiplexedMediaControlChannel** field specifying the destination transport address for the multiplexed Media Control packets.

If an OLC Response message contains a **multiplexID** field, then it also shall contain **multiplexedMediaChannel** and **multiplexedMediaControlChannel** fields specifying destination transport address for the multiplexed Media and Media Control packets correspondingly.

If an OLC Request message contains **multiplexID** and **keepAliveChannel** fields, then the **keepAliveChannel** field shall contain the destination transport address for the multiplexed Keep-Alive packets.

If an OLC Request message contains **multiplexID** and **keepAliveChannel** fields, then the **multiplexedMediaChannel** field of the OLC Response message sent by the same entity for the same call and value of **sessionID** shall contain the same value as the **keepAliveChannel** field.

The values of the **multiplexedMediaControlChannel** field signalled by the same entity for all the LCs for the given call and value of **sessionID** shall be identical.

When the Fast Connect caller creates its **openLogicalChannel** proposal message, it does not yet know if the peer entity supports the procedures of this Recommendation. For this case, an H.460.19 entity which desires to use the multiplexed media mode shall include both the **multiplexedMediaChannel** and **multiplexedMediaControlChannel** fields (for the case where the peer supports multiplexing), and the **mediaChannel** and **mediaControlChannel** fields (for the case where the peer does not support multiplexing).

7.3 Media transport

7.3.1 NAT/FW traversal procedure

The NAT/FW traversal procedure shall be used in cases where an H.460.19 server communicates with an H.460.19 client.

The NAT/FW traversal procedure shall not be used in cases where an H.460.19 server communicates with an H.460.19 server, and in the cases where an H.460.19 client communicates with an H.460.19 client.

The Media Channel, Media Control Channel and Keep-Alive Channel are considered established for the purpose of the Keep-Alive procedure when the H.460.19 entity receives the OLC Request or OLC Response message containing the transport address for each respective channel.

NOTE – During establishment of the pair of LCs for a given call and value of **sessionID**, each entity receives the OLC Request and OLC Response messages with the same value of the Media Control Channel transport address. The Media Control Channel is considered established when the first of these two messages is received.

7.3.1.1 NAT/FW traversal procedure – Clients

All H.460.19 clients shall implement the NAT/FW traversal procedure defined in this clause.

The keep-alive mechanism maintains pinholes in any NAT/FW devices located between the H.460.19 client and H.460.19 server.

Upon establishment of each Keep-Alive Channel, the H.460.19 client shall transmit one Media Channel Keep-Alive packet.

Upon establishment of each Media Control Channel, the H.460.19 client shall transmit one Media Control Channel Keep-Alive packet.

For each established Media Control Channel and Keep-Alive Channel, the H.460.19 client shall transmit a Media Channel and Media Control Channel keep-alive packet at intervals of not less than the value specified by the H.460.19 server in the **keepAliveInterval** field in the Traversal Parameters defined in 7.4.5, unless there is other traffic on the channel within the given interval.

A keep-alive interval in the range of 5 to 30 seconds should be used except in cases where it is known (for example, from the specifics of the network) that a longer interval will not result in the closure of pinholes.

7.3.1.1.1 RTP Keep-Alive packet

The RTP keep-alive packet is an RTP packet with an empty payload field. The payload type value shall be equal to the value specified by the client in **keepAlivePayloadType** field in the Traversal Parameters defined in 7.4.5. The sequence number header field shall start from any arbitrary value and increment by one for each Keep-Alive packet.

The SSRC and timestamp header fields may have arbitrary values.

7.3.1.1.2 RTCP Keep-Alive packet

The RTCP keep-alive packet is an RTCP packet containing an SR (sender report) only, as specified in RFC 3550.

7.3.1.1.3 SRTP Keep-Alive packet

The SRTP keep-alive packet is the same as the RTP Keep-Alive packet. In addition, the optional authentication tag (as defined by RFC 3711) should be added to the packet.

7.3.1.1.4 SRTCP Keep-Alive packet

The SRTCP keep-alive packet is an SRTCP packet containing an SR (sender report) authenticated and optionally encrypted with the same parameters which are used for regular SRTCP packets in the same SRTP session.

7.3.1.2 NAT/FW Traversal procedure – Servers

All H.460.19 servers shall implement the NAT/FW Traversal procedure defined in this clause.

H.460.19 servers shall not forward any RTP or SRTP Keep-Alive packet as defined in the previous clause to any H.323 endpoint which has not indicated support for the procedures of this Recommendation.

These packets should be identified by their payload type value.

The H.460.19 server shall ignore the **mediaChannel**, **mediaControlChannel**, **multiplexedMediaChannel** and **multiplexedMediaControlChannel** transport addresses signalled in the **openLogicalChannel** or **openLogicalChannelAck** messages received from the H.460.19 client.

For each established Media Channel, the H.460.19 server entity shall wait for receipt of at least one Keep-Alive media packet from the H.460.19 client and then send media packets destined for the H.460.19 client to the source transport address of the Keep-Alive media packet received from the H.460.19 client.

For each established Media Control Channel, the H.460.19 server entity shall wait for receipt of at least one media control packet from the H.460.19 client and then send media control packets destined for the H.460.19 client to the source transport address of the media control packets received from the H.460.19 client.

NOTE – Security may be increased through the use of authentication (either H.235 anti-spamming or SRTP) in concert with the NAT/FW traversal procedure.

H.460.19 entities which implement SRTP authentication shall also implement H.235 anti-spamming.

7.3.2 Multiplexed media mode – RTP/RTCP

When operating in the multiplexed media mode, a multiplexing layer shall be added by H.460.19 entities between the UDP and RTP/RTCP packet headers as shown in Figures 7 and 8.

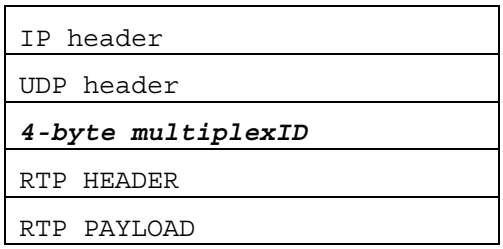

Figure 7/H.460.19 – The multiplexed RTP packet

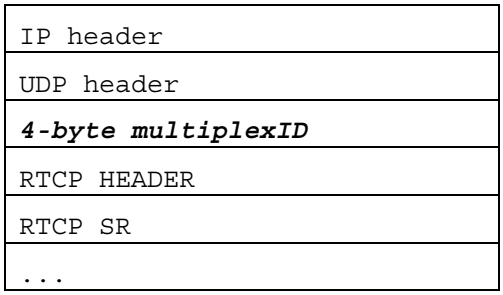

Figure 8/H.460.19 – The multiplexed RTCP packet

The sender of the multiplexed Media Channel/Media Control Channel packet shall create the Media Channel/Media Control Channel packet as specified by RTP/RTCP and then shall insert in the packet the value of **multiplexID** as specified by the peer during the OLC Request or OLC Response procedure as described in 7.2 above.

If the NAT/FW traversal procedure is in use, the packet shall be sent to the addresses discovered by that procedure. Otherwise the packet shall be sent to the addresses either specified by **multiplexedMediaChannel** (for RTP channels) or **multiplexedMediaControlChannel** (for RTCP channels) field.

NOTE – The receiver of the multiplexed packet is the same entity which specified the **multiplexID** to the peer.

When a multiplexed packet is received, the receiver shall verify that the **multiplexID** field has one of the values previously specified by the receiver of the packet.

If the value is valid, the receiver shall associate the packet with the corresponding RTP/RTCP session. It shall then remove the **multiplexID** field from the packet and further process the packet according to normal RTP/RTCP procedures.

Otherwise, the invalid packet shall be discarded.

7.3.3 Multiplexed media mode – SRTP/SRTCP

The multiplexed media mode for SRTP/SRCP is identical to the RTP/RTCP procedure in the previous clause, with the 4-byte **multiplexID** inserted between the UDP header and the SRTP/SRTCP headers.

The information inside the SRTP/SRTCP portion of the packet shall remain intact.

NOTE – The **multiplexID** is not protected by the security mechanisms defined in SRTP/SRTCP.

7.4 Generic data usage

The H.460.19 feature identifier defined in 7.4.1 shall be carried in the **id** subfield of the **supportedFeatures** field of the H323-UU-PDU in the H.225.0 Call Signalling messages.

The **supportTransmitMultiplexedMedia** parameter defined in 7.4.2 and **mediaTraversalServer** parameter defined in 7.4.3 shall be carried in the **parameters** subfield of the **supportedFeatures** field containing the H.460.19 feature identifier in its **id** subfield.

The H.460.19 feature identifier defined in 7.4.4 shall be specified in the **standard** form of the **messageIdentifier** subfield in the **genericInformation** field of the **openLogicalChannel** or **openLogicalChannelAck** H.245 messages. The **messageContent** subfield of the same **genericInformation** field shall include the "Traversal Parameters" parameter.

7.4.1 Feature identifier definition for H.225.0

Table 3/H.460.19 – mediaNATFWTraversal parameter

Feature name:	**mediaNATFWTraversal**
Feature Description:	Declares support of H.460.19 feature.
Feature identifier type:	Standard
Feature identifier value:	19

7.4.2 supportTransmitMultiplexedMedia parameter definition

Table 4/H.460.19 – supportTransmitMultiplexedMedia parameter

Parameter name:	**supportTransmitMultiplexedMedia**
Parameter description:	This is sent together with **mediaNATFWTraversal** feature identifier to signal support for transmission of the multiplexed media mode. NOTE – Support for reception of the multiplexed media mode is signalled inside OLC Request and OLC Response messages.
Parameter identifier type:	Standard
Parameter identifier value:	1
Parameter type:	Empty (Content field shall be omitted)
Parameter cardinality:	One and only one

7.4.3 mediaTraversalServer parameter definition

Table 5/H.460.19 – mediaTraversalServer parameter

Parameter name:	**mediaTraversalServer**
Parameter description:	This is sent together with **mediaNATFWTraversal** feature identifier to signal that the H.460.19 entity is an H.460.19 server
Parameter identifier type:	Standard
Parameter identifier value:	2
Parameter type:	Empty (Content field shall be omitted)
Parameter cardinality:	One and only one

7.4.4 Feature identifier definition for H.245

{ itu-t (0) recommendation (0) h (8) 460 19 version (0) 1}

7.4.5 Traversal Parameters definition

Table 6/H.460.19 – Traversal Parameters parameter

Parameter name:	**Traversal Parameters**
Parameter description:	This parameter shall be sent to provide media parameters necessary for NAT/FW traversal and media multiplexing. The content is a raw field consisting of the ASN.1 aligned variant PER encoded TraversalParameters type as specified in the ASN.1 notation in Annex A.
Parameter identifier value:	1
Parameter status:	Mandatory
Parameter type:	octetString
Supersedes:	This field is not used

7.4.5.1 Traversal Parameters semantics

multiplexedMediaChannel

Media Channel packets shall be sent to the transport address received in this field in the event that the multiplexed media mode is used. If the multiplexed media mode is not used, then the packets shall be sent to the transport address received in the **mediaChannel** field.

Servers performing the NAT/FW traversal procedure should ignore **multiplexedMediaChannel** and **mediaChannel** fields.

multiplexedMediaControlChannel

Media Control Channel packets shall be sent to the transport address received in this field in the event that the multiplexed media mode is used. If the multiplexed media mode is not used, then the packets shall be sent to the transport address received in the **mediaControlChannel** field.

Servers performing the NAT/FW traversal procedure should ignore **multiplexedMediaControlChannel** and **mediaControlChannel** fields.

multiplexID

The presence of this field indicates the intention to use the multiplexed media mode for the logical channel. The value received in this field shall be transmitted in the **multiplexID** field in the multiplexed media mode packets for that logical channel.

keepAliveChannel

Keep-Alive Channel packets shall be sent to the transport address received in this field. This field is used only to specify the address for the Keep-Alive packets which need to be sent in the opposite direction to that of the Media Channel. This field shall be specified only by H.460.19 servers in OLC Request messages.

keepAlivePayloadType

The Keep-Alive Channel packets shall have the payload type value equal to the value specified in this field by the sender of the Keep-Alive packets. This field shall be specified in the OLC Response messages by the H.460.19 client communicating with H.460.19 server or with an entity whose H.460.19 type is still unknown.

keepAliveInterval

This value is signalled by an H.460.19 server and represents the maximum interval, in seconds, of the absence of the Media Channel or Media Control Channel packet traffic, after which the corresponding Keep-Alive packets shall be sent.

Annex A

Media traversal ASN.1 definitions for use inside generic data

A.1 Introduction

This annex contains the ASN.1 definitions used by this Recommendation.

```
MEDIA-TRAVERSAL {itu-t(0) recommendation(0) h(8) 460 19 version (0) 1} DEFINITIONS
AUTOMATIC TAGS ::=

BEGIN

IMPORTS
                TimeToLive

FROM H323-MESSAGES
                TransportAddress

FROM MULTIMEDIA-SYSTEM-CONTROL;

TraversalParameters ::= SEQUENCE
{
      multiplexedMediaChannel             TransportAddress  OPTIONAL,
      multiplexedMediaControlChannel      TransportAddress  OPTIONAL,
      multiplexID                         INTEGER(0..4294967295) OPTIONAL,

      keepAliveChannel                    TransportAddress  OPTIONAL,
      keepAlivePayloadType                INTEGER (0..127)  OPTIONAL,
      keepAliveInterval                   TimeToLive        OPTIONAL,
      ...

}

END -- of ASN.1
```

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	Telephone transmission quality, telephone installations, local line networks
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, 2005