INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.460.18

(09/2005)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Supplementary services for multimedia

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

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/had not] 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.

© ITU 2005

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

ITU-T Recommendation H.460.18

Traversal of H.323 signalling across Network Address Translators and Firewalls

Summary

Recommendation H.460.18 extends H.323 to enable H.323 devices to successfully exchange signalling and establish calls, even when they are placed inside a private network behind NAT/FW devices. These extensions, when used together with the facilities of H.460.19, enable H.323 endpoints to traverse NAT/FW installations with no additional equipment on the customer premises. Alternatively, the H.460.18 extensions may be implemented by a proxy server to support unmodified H.323 endpoints.

Keywords

NAT/FW, H.323, NAT, FW/NAT, firewall, traversal, network address translator

1 Scope

H.460.18 enables H.323 signalling to traverse NAT/FW installations. When used in conjunction with H.460.19, this allows H.323 endpoints to communicate across NAT/FWs which would otherwise be an obstacle to multimedia communications.

The H.460.18 architecture consists of a network which is divided into an internal and an external network by a NAT/FW. Typically the internal network will be a private network, and may be managed by an organization or an individual. The external network will typically be a public network such as the Internet, but may alternatively be another private network.

The H.323 internal endpoint and the external H.460.18 Traversal Server (TS) work together to enable bidirectional communication across the NAT/FW, and discover the transport addresses that have been modified by the NAT/FW.

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.460.19 (2005), *Traversal of H.323 media across Network Address Translators and Firewalls.*
- ITU-T Recommendation X.680 (2002), *Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.*
- ITU-T Recommendation X.691 (2002), *Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER).*

3 Definitions

Client gatekeeper: An H.323 gatekeeper which initiates an H.460.18 channel to an H.460.18 server gatekeeper for the exchange of LRQ/LCF messages.

Client gateway: An H.323 to H.323 gateway which requires the Signalling Traversal Feature.

Client proxy: An H.460.18 client gateway acting as a proxy for non-H.460.18 endpoints.

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

External endpoint: An endpoint located on the external network.

External network: A network connected to the NAT/FW through the public interface of the NAT/FW. Typically, but not limited to, the public Internet.

H.460.18 endpoint: An endpoint with the additional functionality of a H.460.18 client.

Internal endpoint: An endpoint located on the internal network.

Internal network: A network connected to the firewall through the firewall's private interface.

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.

Server gatekeeper: An H.323 gatekeeper which accepts an H.460.18 channel from an H.460.18 client gatekeeper for the exchange of LRQ/LCF messages

Server gateway: An H.323 to H.323 gateway which provides the Signalling Traversal Feature.

Server proxy: An H.460.18 server gateway acting as a proxy for non-H.460.18 gatekeepers.

Transport address: IP address and UDP/TCP port number.

Traversal server: An H.460.18 server gateway logically combined with an H.460.18 server gatekeeper. The Traversal Server is located in the external network.

4 Abbreviations

ACF	Admission Confirmation (H.225.0)
ARQ	Automatic Repeat Request (H.225.0)
LCF	Location Confirm (H.225.0)
LRQ	Location Request (H.225.0)
NAT/FW	Network Address Translator and/or Firewall
RAS	Registration, Admission and Status (H.225.0)
RCF	Registration Confirm (H.225.0)
RRQ	Registration Request (H.225.0)

SCI	Service Control Indication (H.225.0)
SCR	Service Control Response (H.225.0)
TCP	Transport Control Protocol
TPKT	Transport Protocol Data Unit Packet
TS	Traversal Server

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.

Reference is made throughout this Recommendation to two H.323 endpoints: EP$_A$ and EP$_B$. EP$_A$ is an endpoint on the internal network which implements H.460.18. EP$_B$ is located on the external network and is not required to implement H.460.18.

6 Overview

H.460.18 utilizes the fact that NAT/FWs are typically more lenient toward traffic sessions originating from the internal network than traffic sessions originating from the external network. NAT/FWs typically permit traffic that is outbound from the internal network, and typically permit inbound traffic received in response to the original outbound traffic. H.460.18 procedures take advantage of this to open a bi-directional “pinhole” path for a given transport address by originating traffic from the inside network. The pinhole is maintained by the transmission of traffic, or in the absence of traffic by the periodic transmission of “keep-alive” packets.

The Traversal Server (TS) consists of an H.460.18-enabled H.323 server gatekeeper and an H.460.18 server gateway. Communication between the internal endpoint and the external TS starts with the initial outgoing RAS message – (GRQ or RRQ), which establishes a pinhole for RAS traffic. This RAS channel is kept open for the duration of the endpoint’s registration with the external TS.

During call setup, this RAS channel is used to establish an H.225.0 TCP channel, which in turn may be used to establish an H.245 channel.

Outbound calls from the internal endpoint are established according to normal H.323 procedures.

Inbound calls from external endpoints are addressed to the external IP address at the TS. The TS does not simply open a TCP connection for H.225.0 to the internal endpoint because the NAT/FW is likely to block such a connection. Instead, the TS uses a RAS message to request the internal endpoint to open an H.225.0 TCP connection to the TS. This H.225.0 TCP connection is then used for ongoing call control, including establishment of the H.245 control channel if desired.

7 Architecture

H.460.18 makes use of an H.460.18 endpoint or client proxy and an H.460.18 Traversal Server (TS) that work together to enable bidirectional communication across the NAT/FW, and discover the addresses that have been modified by the NAT/FW.

The H.460.18 endpoint acts as an H.323 endpoint combined with an H.460.18 client functionality. The endpoint may be implemented as a single device as shown in Figure 1, which avoids the need for additional equipment on the customer premises, or as a standard H.323 endpoint and a separate H.460.18 client gateway as shown in Figure 2, to support unmodified H.323 endpoints.

The TS may be implemented as a single device as shown in Figure 1, as separate devices interconnected by a unspecified protocol, or as a server proxy and server gatekeeper to support unmodified H.323 gatekeepers as shown in Figure 2. The server gatekeeper operates in gatekeeper routed signalling mode, allowing it to intercept and modify messages. Media from the endpoints is sent via a media relay located in the external network. Bypassing the media relay when certain forms of NAT/FW entities are in use is for further study.

> NOTE - If the TS is implemented as separate devices, as shown in Figure 2, the protocol between them (shown by a dotted arrow in the figure) may be implemented using RAS or a proprietary protocol.

Figures 1, 2 and 3 below show possible ways in which H.460.18 may be deployed. Items in bold text: H.460.18 Endpoint EPA, H.323 Endpoint EPB, Traversal Server, client proxy, server proxy, client gatekeeper and server gatekeeper are referred to in this Recommendation. Other devices are shown for completeness.

For simplicity of description, this Recommendation describes both the H.460.18 endpoint and TS as single devices as in Figure 1 below, but other implementations may be used.

In some deployments H.225.0 LRQ and LCF messages must traverse a NAT/FW boundary. This is accomplished by the H.460.18 client gatekeeper on the internal network maintaining a communication path with an H.460.18 server gatekeeper on the external network using SCI and SCR RAS messages. See Figure 3.

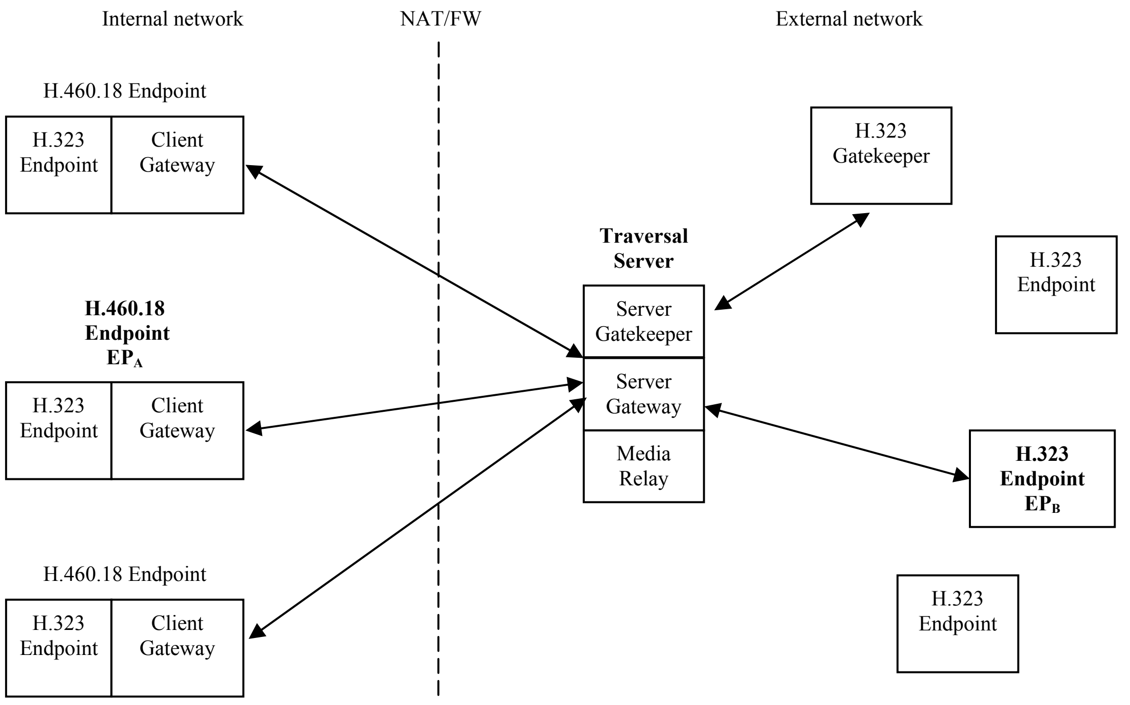

Figure 1/H.460.18 – H.460.18 architecture, single-device Endpoints and TS

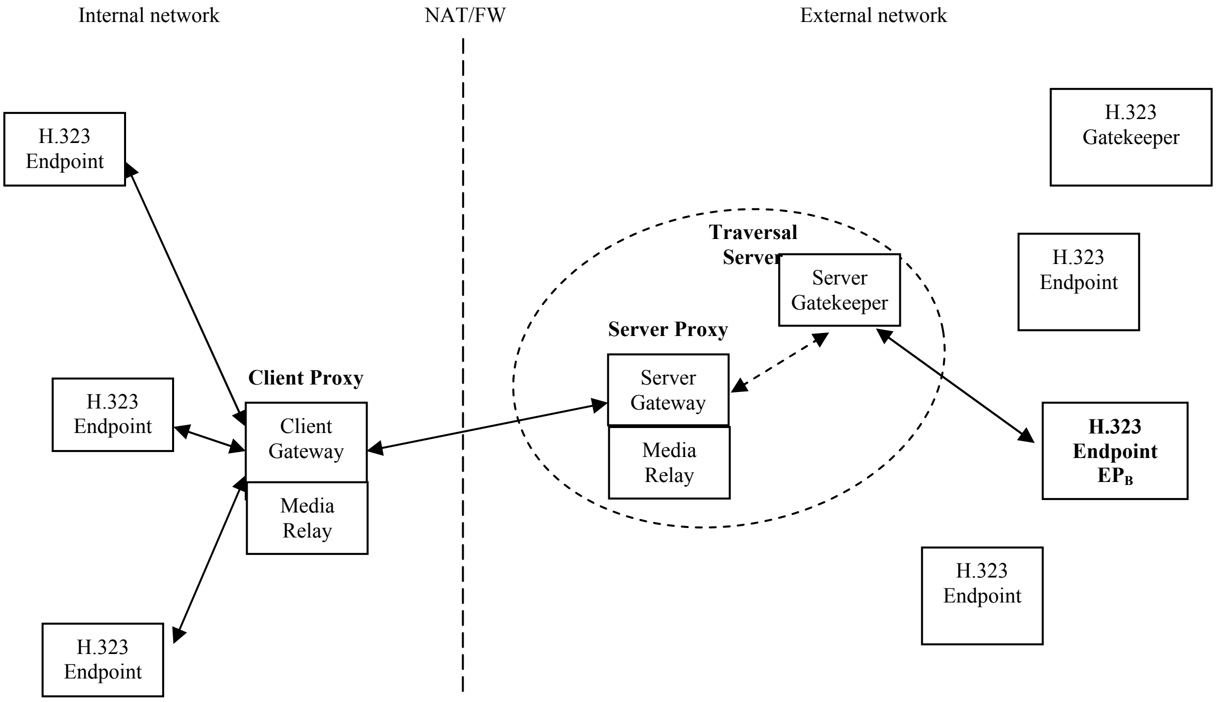

Figure 2/H.460.18 – H.460.18 architecture, fully decomposed implementation

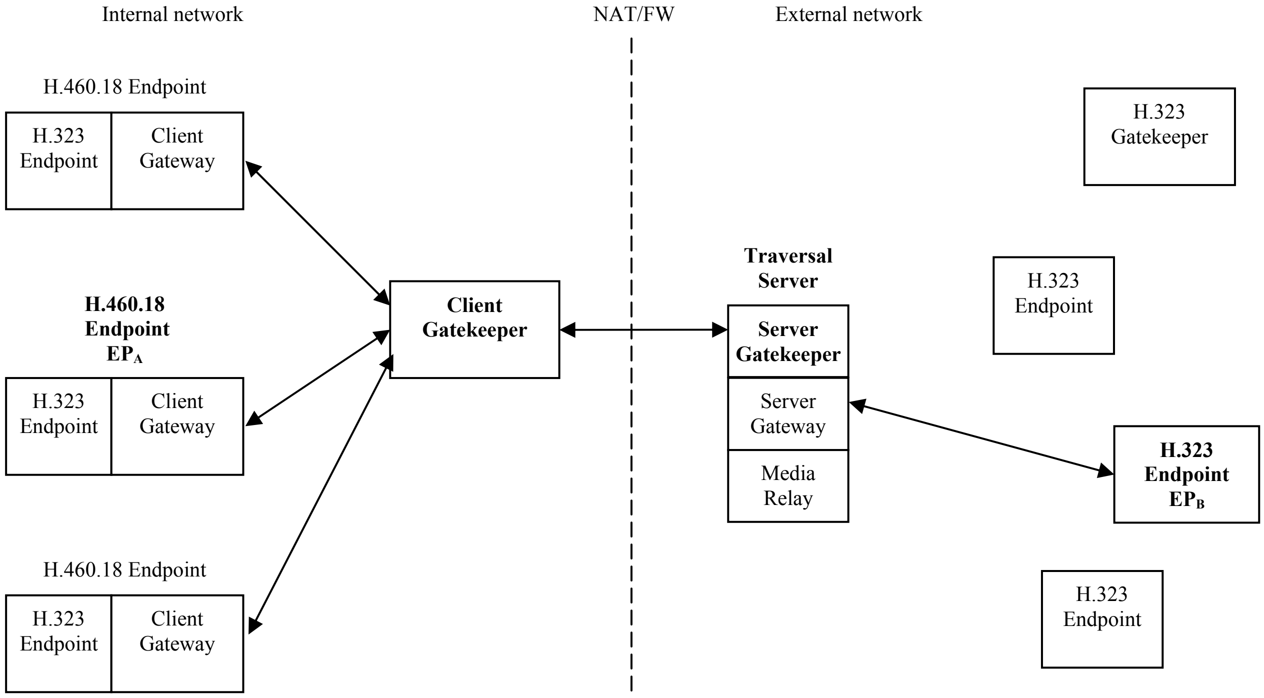

Figure 3/H.460.18 – Gatekeeper communication architecture

8 Registration Procedure

An endpoint which performs gatekeeper discovery shall set the **supportedFeatures** field of its GRQ to include **Signalling Traversal** as defined in clause 15, Table 1. If the TS responds with a GCF, it shall include **Signalling Traversal** in the **supportedFeatures** field.

Endpoints shall send an RRQ to the TS including **Signalling Traversal** in the **supportedFeatures** field. Endpoints may omit **Signalling Traversal** from the **supportedFeatures** field of lightweight RRQ's.

8.1 Traversal Server Mode Selection

If the TS has prior knowledge that there is no NAT/FW between itself and the endpoint, it may elect not to use the procedures described in this Recommendation. If NAT/FW traversal is not required, the TS may omit **Signalling Traversal** from the supported features field of the RCF. Signalling then proceeds without the procedures described in this document.

8.2 Registration when H.460.18 Mode Selected by Traversal Sever

If the TS intends to use the NAT/FW traversal features described in this Recommendation, the TS and endpoint shall follow the procedures as defined in this and the succeeding clauses.

The TS shall ignore any RAS address specified in any GRQ or RRQ which includes **Signalling Traversal** in the **supportedFeatures**. Instead the TS shall use the apparent source transport address from which the GRQ or RRQ was sent as the RAS address.

If the TS accepts a gatekeeper discover or registration, it shall send a GCF or RCF with **Signalling Traversal** in the **supportedFeatures** field. The TS shall set the **timeToLive** in the RCF to a value that is short enough to prevent intermediate NAT/FW devices from blocking connectivity. This value shall be determined as described in clause 14.

An endpoint that is compliant with this Recommendation shall use the same port for sending and receiving all RAS messages. If **Signalling Traversal** is not included in the **supportedFeatures** field of the RCF, the endpoint shall not use the procedures described in this Recommendation.

9. Outgoing Call Procedure

EP$_A$ is located on the internal network, EP$_B$ is on the external network. EP$_B$ is H.323 conformant and outside the scope of this Recommendation.

1. EP$_A$ shall initiate the process, as for a normal call, by sending an ARQ to the TS. If the call is allowed, the TS shall respond with an ACF.
2. EP$_A$ shall initiate a TCP connection to the H.225.0 call signalling address specified in the ACF.
3. EP$_A$ shall send the H.225.0 SETUP message to the TS on the H.225.0 TCP connection. The TS shall forward this to EP$_B$.
4. Any response H.225.0 message from EP$_B$ shall be forwarded by the TS according to the procedures of H.225.0 to EP$_A$. If an **h245Address** field was present in the message received from EP$_B$ by the TS, the TS shall substitute its own transport address in the **h245Address** field of the H.225.0 message forwarded to EP$_A$.

Figure 4 shows an indicative message sequence for an outgoing call.

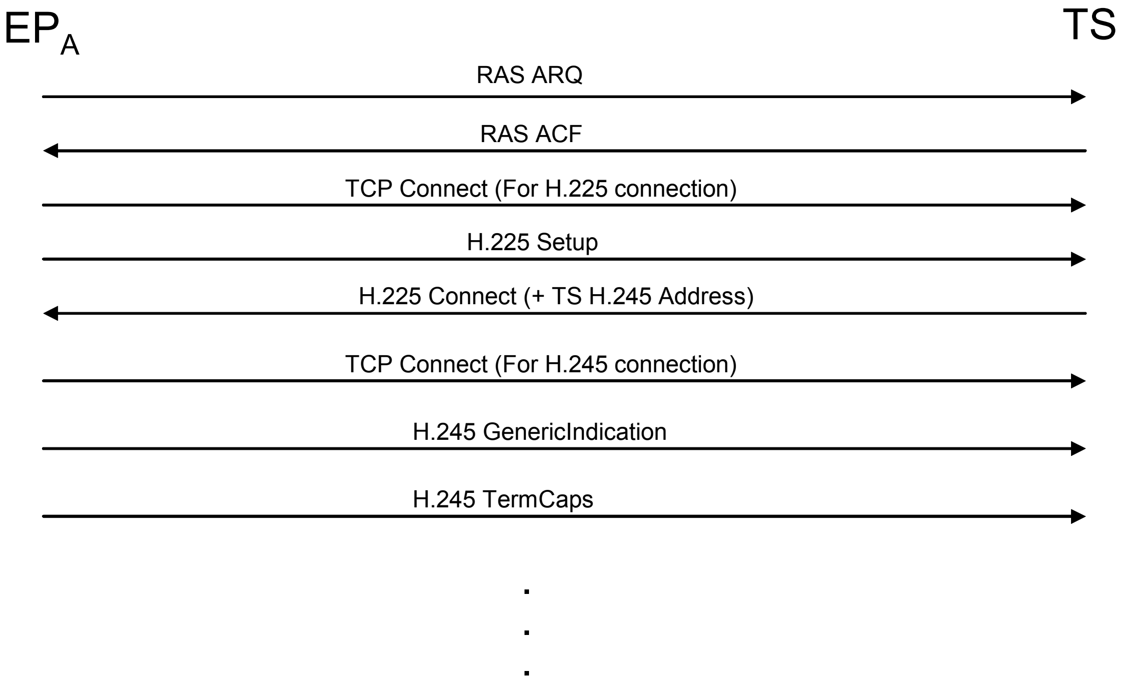
EP_A
TS
RAS ARQ
RAS ACF
TCP Connect (For H.225 connection)
H.225 Setup
H.225 Connect (+ TS H.245 Address)
TCP Connect (For H.245 connection)
H.245 GenericIndication
H.245 TermCaps

Figure 4/H.460.18 Indicative Outgoing Call Message Sequence

10 Incoming Call Procedure

EP$_A$ is located on the internal network, EP$_B$ is on the external network. EP$_B$ is H.323 conformant and is outside the scope of this Recommendation.

1. To establish a call to EP$_A$ in the internal network (for example, in response to an H.225.0 call setup from a EP$_B$), the TS shall send an H.225.0 SCI RAS message to EP$_A$. The **genericData** field of the SCI shall contain an **IncomingCallIndication** as defined in Table 2.
2. On receipt, EP$_A$ shall send an H.225.0 SCR to the TS acknowledging receipt of the SCI.
3. EP$_A$ shall initiate a TCP connection for H.225.0 to the transport address specified in the **callSignalAddress** field of the **IncomingCallIndication**. EP$_A$ shall then send an H.225.0 FACILITY message with the **callIdentifier** field set to the value of the **callIdentifier** sub-field of the **IncomingCallIndication** of the previously received SCI message. The **reason** field shall be set to **undefinedReason** and the **conferenceId** field shall be omitted. The call reference value shall be set to 0, the global call reference.
4. The TS shall not forward the FACILITY message to another entity involved in the call.
5. The TS shall send the H.225.0 SETUP message to EP$_A$ on the just-established H.225.0 TCP connection and call setup shall continue per normal H.323 procedures.

NOTE: The TS can use the callIdentifier received in the FACILITY message of step 3 to determine the call with which the incoming TCP connection is associated.

Figure 5 shows an indicative incoming call message sequence.

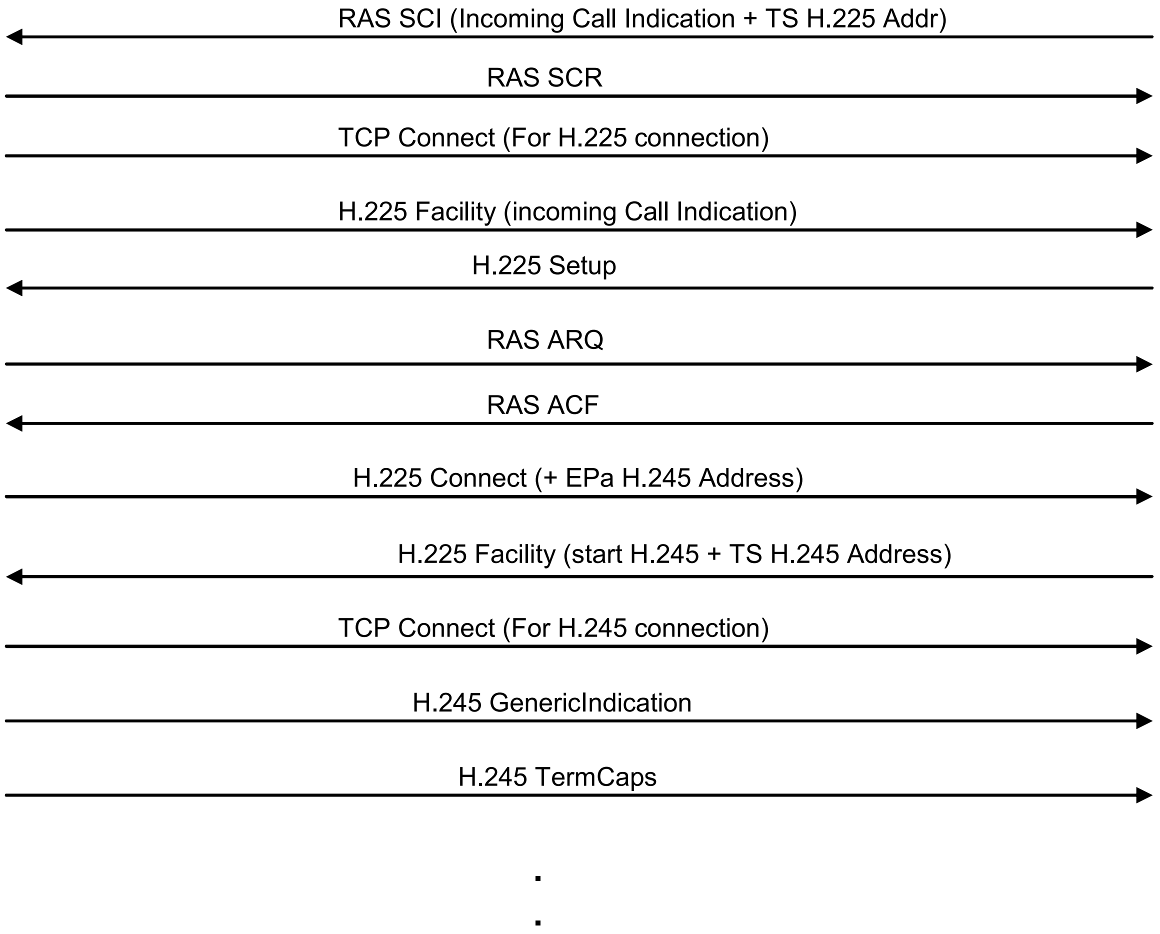
RAS SCI (Incoming Call Indication + TS H.225 Addr)
RAS SCR
TCP Connect (For H.225 connection)
H.225 Facility (incoming Call Indication)
H.225 Setup
RAS ARQ
RAS ACF
H.225 Connect (+ EPa H.245 Address)
H.225 Facility (start H.245 + TS H.245 Address)
TCP Connect (For H.245 connection)
H.245 GenericIndication
H.245 TermCaps

Figure 5/H.460.18 Indicative Incoming Call Message Sequence

11 H.245 Connection Establishment

Traversal Servers may use a single transport address for multiple H.245 TCP connections by specifying the same address in the H.225.0 **h245Address** field of multiple calls.

EP$_{A}$ may establish an H.245 connection any time after receipt of the **h245Address** field. If EP$_{A}$ wishes to establish an H.245 connection and has not received an **h245Address**, EP$_{A}$ shall send an H.225.0 FACILITY message including a **reason** set to **startH245**. EP$_{A}$ may omit the **h245Address** from this message.

On receipt of a FACILITY message containing a **reason** set to **startH245**, the TS shall respond with a FACILITY message with the **reason** set to **startH245** and shall include an **h245Address** field.

NOTE: The presence of a NAT/FW may prevent the TS from creating a TCP connection in response to the request to start H245. The procedure above allows the TS to pass its H245 address to EP$_{A}$ and all connections to be made from internal to external network.

EP$_{A}$ shall establish an H.245 connection with the TS upon receipt of an H.225.0 FACILITY message containing a transport address in the **h245Address** field and including a **reason** set to **startH245**.

The procedure to establish an H.245 connection to the TS is for EP_A to initiate a TCP connection to the transport address given in the **h245Address** field. EP_A shall send an H.245 **genericIndication** containing the **callIdentifier** and **answerCall** as defined in clause 16 as the first message on the TCP connection. The value of the **callIdentifier** shall be the value received during call setup as described in clauses 9 and 10. **answerCall** shall be set to TRUE if the incoming procedure in clause 10 was used, otherwise FALSE.

The TS shall not forward this H.245 **genericIndication** message to another entity involved in the call.

NOTE: The TS can use the **callIdentifier** and **answerCall** to determine which call the incoming TCP connection is associated with. **answerCall** is required for unambiguous identification in some circumstances where both calling and called party are located on the same device, for example a gateway.

If EP_A establishes an H.245 connection to the TS as described above, ~~the TS shall establish an H.245 connection to EP_B. If EP_B has previously signalled an H.245 address the TS shall establish a connection to that address. If no H.245 address has been previously signalled, for example because Fast Connect procedures have been used, the TS shall send an H.225.0 FACILITY message containing a transport address in the **h245Address** field and including a **reason** set to **startH245**~~.

12 Media Setup Procedure

Entities using H.460.18 for signalling traversal shall use the procedures of Rec. H.460.19 for media traversal through the NAT/FW.

13 Location Request (LRQ/LCF) Procedure

An H.460.18 client gatekeeper shall be preconfigured with the address of the TS. In order to establish a connection to the TS, the H.460.18 client gatekeeper on the internal network shall open a NAT/FW pinhole for LRQ and LCF messages by sending an H.225.0 SCI message to the TS. The **featureSet** of the SCI message shall contain **Signalling Traversal** in the **supportedFeatures** list. Other optional fields of the SCI may be omitted. The TS shall respond with an SCR message containing **Signalling traversal** in the **supportedFeatures** list. The SCR shall also contain the **LRQKeepAliveData** parameter defined in this Recommendation in the **GenericData** field.

LRQs and LCFs are then able to flow between the external TS and the internal gatekeeper.

If the TS sends an LRQ to the H.460.18 client gatekeeper, the TS shall insert a **callIdentifier** into the LRQ.

14 Keep-Alives

In order to maintain the NAT/FW pinholes, a keep-alive mechanism is used. After registration, the endpoint shall send keep-alives on each connection if no traffic has been transmitted within the keep-alive interval.

For the RAS channel, the keep-alive is a lightweight RRQ message and the corresponding RCF message.

For the H.225.0 and H.245 channels, the keep-alive is an empty TPKT message.

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. The keep-alive interval for the H.225.0 and H.245 channels shall be equal to the registration **timeToLive**.

Client gateways acting as a client proxy for non-H.460.18 endpoints on the internal network shall send these keep-alives toward the TS at the given interval. H460.18 endpoints communicating directly with a TS shall send these keep-alives toward the TS at the given interval.

For communication between a gatekeeper on the internal network and a TS, the keep-alive is an H.225.0 SCI message sent from the gatekeeper and corresponding SCR message from the TS. The gatekeeper on the internal network shall send the keep-alives to the TS at the interval specified by the **lrqKeepAliveInterval** in the **LRQKeepAliveData** of the SCI received from the TS, as described in clause 13.

Server gateways shall not forward any keep-alives that it receives to another entity in the call.

NOTE: Forwarding of keep-alives is avoided to prevent interoperability problems which might arise if keep-alives on the TCP channel are received by an endpoint which does not recognize them.

NOTE: The choice of keep-alive interval is a trade-off between excessive network traffic and unnecessary message processing which may be caused by an unnecessarily short interval, and the danger that NAT/FWs may close pinholes if too long an interval is used.

NOTE. A client proxy acting on behalf of an H.460.18 endpoint can prevent the endpoint from generating unnecessary keep-alives by omitting the **Signalling Traversal** feature from the RCF as described in clause 8 above.

15 Generic data usage in H.225.0

H.460.18 makes use of the **genericData** field of the H323-UU-PDU and of RAS messages as described in the following sections.

Table 1 below defines the Signalling Traversal feature used in this Recommendation.

Table 1/H.460.18 – Signalling Traversal feature

Feature name:	**Signalling Traversal**
Feature Description:	Shall be indicated by an entity which supports the functions of an H.460.18 client or server.
Feature identifier type:	Standard
Feature identifier value:	18

Table 2 below defines the **IncomingCallIndication** parameter for use with the Signalling Traversal feature.

Table 2/H.460.18 – IncomingCallIndication parameter

Parameter name:	**IncomingCallIndication**
Parameter description:	This shall be sent to request the endpoint to establish a TCP connection for H.225.0 out to the TS. The content is a raw field consisting of the ASN.1 aligned variant PER encoded IncomingCallIndication type as specified in the ASN.1 notation in Annex A.
Parameter identifier type:	Standard
Parameter identifier value:	1
Parameter type:	Raw
Parameter cardinality:	One and only one

Table 3 below defines the LRQKeepAliveData parameter for use with the Signalling Traversal feature.

Table 3/H.460.18 – KeepAliveData parameter

Parameter name:	**LRQKeepAliveData**
Parameter description:	This shall be used to signal keep-alive information for the UDP RAS channel between two gatekeepers. The content is a raw field consisting of the ASN.1 aligned variant PER encoded LRQKeepAliveData type as specified in the ASN.1 notation in Annex A.
Parameter identifier type:	Standard
Parameter identifier value:	2
Parameter type:	Raw
Parameter cardinality:	One and only one

16 Generic Parameters in H.245

As described in clause 11, H.460.18 uses an H.245 **GenericIndication** containing H.245 **GenericParameters**. This shall contain a **GenericMessage.messageIdentifier** with the OID { itu-t (0) recommendation (0) h (8) 460 18 version (0) 1 } and a **subMessageIdentifier** as shown in Table 5.

Table 5/H.460.18 –subMessage identifier values

subMessageIdentifier	Message Name	Message Type
1	connectionCorrelation	GenericIndication

Message content and syntax is given in clause 16.1

16.1 connectionCorrelation

Table 6/H.460.18 —connectionCorrelation syntax

genericParameter identifier	Parameter Name	Required Presence	Type
1	callIdentifier	Mandatory	octetString
2	answerCall	Mandatory	logical

The callIdentifier shall be set to the value of the callIdentifier in the H.225.0 signalling.

answerCall parameter value shall be present if the entity sending the connectionCorrelation received a SETUP message for the corresponding call. It shall be absent if the entity sent a SETUP for the corresponding call.

Annex A

Signalling traversal ASN.1 Definitions for use inside H.245 and H.225.0 Generic Data messages

This annex specifies the syntax of messages using the notation defined in ASN.1 according to Recommendation X.680. Messages shall be encoded for transmission by applying the packed encoding rules specified in Recommendation X.691 using the basic aligned variant. The first bit in each octet which is transmitted is the most significant bit of the octet as is specified in Rec. X.691.

```
SIGNALLING-TRAVERSAL {itu-t(0) recommendation(0) h(8) 460 18 version(0)1}
DEFINITIONS AUTOMATIC TAGS ::=

BEGIN
IMPORTS
     CallIdentifier, TimeToLive, TransportAddress
FROM H323-MESSAGES;

IncomingCallIndication  ::= SEQUENCE
{
     callSignallingAddress   TransportAddress,
     callID                  CallIdentifier,
     ...
}

LRQKeepAliveData        ::= SEQUENCE
{
     lrqKeepAliveInterval    TimeToLive,   -- keep-alive interval (seconds)
     ...
}


END – of ASN.1
```

Appendix I
ASN.1 OIDs defined in this Recommendation

OID	Section Reference
{ itu-t (0) recommendation (0) h (8) 460 18 version (0) 1 }	16