ITU Telecommunication Standardization

Sector

Experts Group for Video Coding and Systems in ATM and Other Network Environments

October 23-28, 1995

STUDY GROUP 15

CONTRIBUTION

Source: Mark Reid, PictureTel Corporation

email: reid@pictel.com

voice: +1 (508) 623-4290

fax: +1 (508) 749-2805

Title: Gateway, Gatekeeper and Terminal Procedures in H.323

Date: October 17, 1995

1.0 Introduction

This document is based on the PictureTel ptel7 submission, the current H.323, the current H.22Z, and the Intel submissions entitled Conference Control in H.323 and Gatekeeper and Connection Setup in H.323. I have taken all five documents, combined their information and have included the result as proposed text for the point to point H.323 call setup procedures.

For supporting information, I have included the following sections related to our on-going discussions:

1.1 References

(01) "Draft ITU-T Recommendation H.323" - Thom 5/18/95

(02) "Draft ITU-T Recommendation H.22Z" - Skran 8/19/95

(03) "Draft ITU-T Recommendation H.245" - Nielsen 7/95

(04) "Draft ITU-T Recommendation H.324" - Lindbergh 06/95

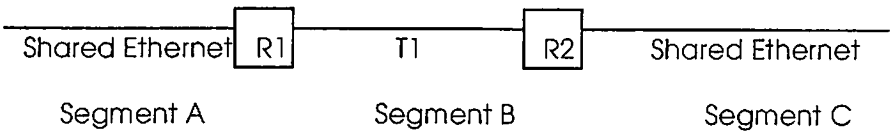
(05) "Gatekeeper and Connection Setup in H.323" - Intel AVC-827

(06) "Conference Control in H.323" - Intel 09/29/95

2.0 Supporting Information

2.1 RSVP and the Gatekeeper

There have been a number of submissions over the past few months indicating that the Gatekeeper was not needed because protocols such as RSVP or ST-II would handle that function. RSVP and ST-II are router protocols which allow for the reservation of bandwidth between routers. Neither protocol handles traversing a shared segment which is not in-between two routers. The following example shows the value of the admission control of the Gatekeeper. Note: The Gatekeeper needs to know the bandwidth in use for each call to be able to make a reasonable determination of the number of simultaneous calls to admit on a given segment at any time.



H.323 systems making calls on Segment A to another system on Segment A or systems on Segment C making calls to systems on Segment C do not benefit from RSVP/ST-II as these calls do not involve a routed link. For Segment A and Segment C, the Gatekeeper can limit the total number of calls to a level that does not interfere with other network traffic.

If we look at Segment B, when calls are placed between Segment A and Segment C both RSVP/ST-II and the Gatekeeper play a role. First, the Gatekeeper is still protecting the overall number of calls on segment A and C during a Segment A to C call. Second, RSVP/ST-II can be used to reserve the required bandwidth between R1 and R2. However, terminals can be configured to make the call from Segment A to Segment C regardless of whether or not they make a successful RSVP or ST-II reservation, so the Gatekeeper can still be useful on Segment B. In this case, Segment B would have an overall call limit (as it does for the other segments) which can be used to prevent the overall number of calls (reserved or not) that traverse Segment B from using an unacceptable amount of bandwidth.

(Note: RSVP/ST-II will guarantee some QoS on Segment B but it cannot guarantee it for the conference as both Segment A and Segment C are shared segments).

2.2 Gateway Management via Gatekeeper

The Gatekeeper should be required to manage the availability and location of Gateway's on a network. Gateway's will come in many flavors, a single card or cards in a server, router, or MCU, or as stand-alone boxes with multiple WAN ports. The management of the number of ports available for use and the management of which network addresses are actually Gateways should not be replicated in each individual terminal.

We have defined how terminals and Gateways register with the Gatekeeper. A single Gateway which may have multiple ISDN ports will register multiple clients with the Gatekeeper. Adding another ISDN port to your Gateway arsenal should be transparent to H.323 terminals.

Gatekeepers know where each Gateway is via the registration process. Gatekeepers know which Gateway's are in use at any given time and already have the E.164 to network address mapping required for in-bound calls.

The Gatekeeper needs to be able to handle three types of calls:

1. H.323 Terminal to H.323 Terminal Call - In this case, the Connection Request (CRQ) PDU contains the network address and/or the E.164 extension of the destination terminal.
2. H.323 Terminal to H.320 Call - In this case, the Connection Request (CRQ) PDU contains between two and six E.164 phone numbers to be dialed by the Gateway. There is no terminal extension because we are calling an H.320 system. (Calls to other H.32x specifications would follow this scenario.)
3. H.323 Terminal to H.323 Terminal via back to back Gateways Call - In this case, the Connection Request (CRQ) PDU would contain both a Terminal extension and between two and six E.164 phone numbers to be dialed by the Gateway.

Upon receiving a Connection Request, a Gatekeeper will look for the presence of WAN dialing information. If it is present, the Gatekeeper will route the call to one of its idle registered Gateways. With this method, terminals do not need to worry about where the Gateway's are and the maintenance and up-keep of the Gateway units can be handled purely from the Gatekeeper.

If the Gatekeeper does not manage this information, clients will have to be updated with an available Gateway list each time the Gateway configuration is changed. Further, when placing an outbound call, each endpoint terminal will need to sequentially test each Gateway for availability. Therefore, to avoid this overhead and configuration problem, the Gatekeeper should manage Gateway availability and location.

2.3 Specific Comments in AVC-827 "Gatekeeper and Connection Setup in H.323"

The following comments relate to the Intel proposal entitled "Gatekeeper and Connection Setup" (4)

Section 5.1, 5.3

MRQ, MCF, and MRJ should be updated to GQQ, GQRS, and GQRJ as specified in Section 7.1 of AVC-827.

Section 7.1

Network Address (page 10)

The subnet mask should be included to allow the IP network number to be extracted from the full IP address (net number + host ID). The extracted number uniquely identifies on which physical segment the terminal resides. You could argue that in a typical organization, the subnet mask is the same through-out all segments; however, there maybe exceptions and as a precaution we would like to have this field included in the registration request.

Guardian Request (page 11)

Should include E.164 extension of terminal.

Registration Request Reject Reasons (page 12)

Add Duplicate Ext Number. A single Gatekeeper cannot have two clients with different network addresses and identical E.164 extensions.

Connection Request (page 14)

Need to include the originating and destination E.164 address.

Need to include a "Request To Answer Call" call type to handle the case shown in Section 5.2 of AVC-827. In this case, the Gatekeeper needs to be signaled that it is not a call setup request, but rather a request to answer a call.

Node Response List (page 23)

Why limit this report to 256 entries?

3.0 H.323 Comments

3.1 Specific Comments on H.323

Section 5.2.4 Video Coding

It states that H.323 terminals shall be capable of operating in asymmetric video bitrates. (e.g. QCIF, CIF). This should not be a requirement as terminals are not required to be able to receive CIF pictures.

Section 5.2.8.1

There are two proposals for H.245 logical channel signaling on the reflector. Ptel7 proposes the establishment of audio, video, control, and data ports for which H.22Z can multiplex the logical channels and Intel's proposal to move the multiplex of logical channels to UDP and have each logical channel running on a separate UDP port. If we chose the Intel proposal there is no H.22Z multiplex and the logical channel number becomes a control mechanism which does not need to be transmitted in packets.

The advantage of the Intel proposal is that the audio and video packets do not need to have a header extension to tag which logical channel they belong to. The disadvantage is that logical channels would be actually tied to physical UDP ports. By the rules of H.245, a mode switch would require the closing and re-opening of the physical UDP port which in implementation would be very slow. (e.g. buffer clean up and reallocation with the system's network drivers)

5.5 MC functions

Note: We need to define the signaling PDU's required to support multipoint operation.

6.1 Terminal Addressing

There are three kinds of terminals which need to be addressed:

1. H.323 Terminals - In this case, the terminal is addressed with an E.164 extension or network address.
2. H.320 or H.324 terminals accessable via a Gateway - In this case, those systems are addressed with between two and six E.164 phone numbers.
3. H.323 Terminals accessable via back to back Gateways - In this case, the terminal is addressed with an E.164 extension and between two and six E.164 phone numbers.

10 Multipoint

Note: We need to add the signaling PDUs to support this type of conference (joining, setup up, terminate, etc.).

Add Section from H.324 (Audio Frame Size 6.7.3)

All H.323 terminals offering audio communication shall support the G.711 codec using H.22Z.

For all frame-oriented audio codecs, receivers shall signal the maximum number of audio frames they are capable of accepting in a single audio packet. Transmitters may send any whole number of audio frames in each packet, up to the maximum stated by the receiver. Transmitters shall not split audio frames across packets, and shall send whole numbers of octets in each audio packet.

Note: Sample based codecs, such as G.711, shall be considered to be frame-oriented, with a frame size of sample one.

For audio algorithms such as G.723 which use more than one size of audio frame, audio frame boundaries within each packet shall be signaled in-band to the audio channel. For audio algorithms which use a fixed frame size, audio frame boundaries shall be implied by the ratio of packet size to audio frame size.

3.2 Gateway, Gatekeeper, and Terminal Procedures for H.323

This section proposes H.323 procedures based on the combination of ptel7, the current H.323, the current H.22Z, and the Intel submissions entitled Conference Control in H.323 and Gatekeeper and Connection Setup in H.323. We support the work proposed in Intel's submissions as they build on the current call setup procedures and propose a solution to the scalability problems with multiple Gatekeepers on a network. They also address terminals without a Gatekeeper and provide a flexible registration policy for terminals and Gateways.

The Intel submission should be supported for the following reasons:

1. Registration is automatic - This allows more flexibility then proposed in Ptel1 or the current draft of H.323.

2. No need to manage Domain spaces for the LAN, no need for System Administration to worry about setting up domains or which domains are neighbors.

3. Terminal signaling continues to be the same with or without a Gatekeeper or Gateway.

4. Gatekeeper to Gatekeeper communication is not required outside of call setup.

<u>The following Sections are proposed for H.323 text:</u>

7 Terminal procedures

The provision of the communication is made in the following steps:

- phase 0: Terminal Registration (subclause 7.1);
- phase A: Call set-up (subclause 7.2);
- phase B: Initial communication and capability exchange (subclause 7.3);
- phase C: Establishment of audio visual communication (subclause 7.4);
- phase D: Call termination (subclause 7.5)

7.1 Phase 0 - Terminal Registration

The registration process associates a terminal's network address with its E.164 address and an optional terminal identifier. Registration may be done statically or dynamically. Static registration includes methods such as manual configuration of the Gatekeeper by an operator or manual entry of the Gatekeeper to register with in each terminal. *{Static Binding in Intel's proposal}* Dynamic registration requires communications between the Terminal and the Gatekeeper as described below.

7.1.1 Registration of H.323 Terminals and Gateway units with a Gatekeeper

7.1.1.1 AutoBinding

As part of their configuration, H.323 terminals and Gateway units, may be configured to Auto Bind to a Gatekeeper. Upon initialization, a terminal or gateway will broadcast a Guardian Request (GRQ) on the H.323 well known port which in effect asks "Who is my gatekeeper?" Any Gatekeeper which receives the GRQ and has not been programmed to ignore the BIND request should respond with a Guardian Confirmation (GCF) "I can be your Gatekeeper". A terminal may now select a Gatekeeper for registration by sending it a Registration Request (RRQ) and following the procedures as outlined in Section 7.1.1.2.

Note: Although terminals can be configured for operation without a Gatekeeper, it is recommended that terminals always broadcast the GRQ message on initialization so that if a Gatekeeper is introduced onto a network, each terminal automatically finds the Gatekeeper and binds to it. Once bound to a Gatekeeper, terminals should require the Gatekeeper to make or place subsequent calls. This procedure will ensure that an IT department can control H.323 terminal equipment by introducing a Gatekeeper on to the network.

7.1.1.2 Static Binding

As part of their configuration, H.323 terminals and Gateway units, may send a Registration Request (RRQ) with the Bind Request flag set to BIND to the appropriate Gatekeeper for their site. The Gatekeeper must respond with either a Registration Confirmation (RCF) or a Registration Rejection (RRJ). The RRQ may be repeated periodically (i.e., at terminal power up) so the Gatekeeper must be able to handle multiple requests from the same terminal. Repeated requests to register (i.e. at terminal power up) should not set the Bind Request flag to BIND. See Figure 2. There is no un-registration message, so the Gatekeeper should have a mechanism to periodically remove inactive terminals. *{Periodic status requests should be used to determine the health of a terminal}*

It is presumed that during install or at some other appropriate point, the user of a H.323 terminal or Gateway will be given the opportunity to enter an address of the appropriate Gatekeeper.

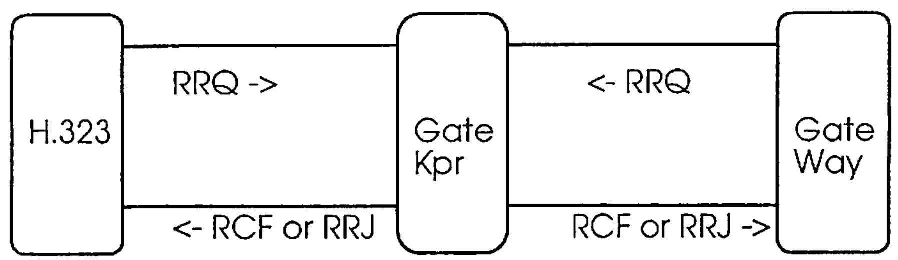


Figure 2

7.1.2 Gatekeeper to Gatekeeper Communications

7.1.2.1 Registration

This section should be deleted. *{With the new proposal, Gatekeeper to Gatekeeper registration and communication outside of call setup are no longer required. The Sub-Domain List Request and Response should be maintained for status reporting and network management query.}*

7.1.2.2 Sub-Domain List Request

Gatekeepers may poll other Gatekeepers in the Super-Domain for the terminals and Gateways in their Sub-Domain using the Sub-Domain list Request (SLR). Gatekeeper's must respond with a Sub-Domain Registered List (SRL) of which the contents are optional. The response may contain a list of their H.323 registered terminals, Gateways, and all of the other Gatekeepers which it has knowledge of, any subset of that information, or no information at all.

Note: As an optional feature, Gatekeepers can accept and respond to terminal list requests from terminals.

7.1.2.3 Termination

(As noted in 7.1.2.1, this section in no longer required)

7.2 Phase A - Call set-up

Call Set-up takes place according to the call control procedures as described below. *(I have followed H.323 and provided the point-to-point procedures first. I did not attempt multipoint procedures.)*

7.2.1 Call Set-up without a Gatekeeper

(All H.22Z defined PDUs RRQ, RCF, RRJ, CRQ, CCF, CRJ, DRQ, DCF, etc. are sent using a unreliable transport on the H.323 well known port. All H.245 messages are sent using a reliable transport on a dynamic port negotiated in the CRQ, CCF exchange. The reliable port represents logical channel zero for H.245. Carrying the H.22Z PDU's on the well known port allows for the removal of the command mux in H.22Z which distinguishes H.245 and H.22Z commands.)

When there is no Gatekeeper on the network, a call is established directly between the terminals or terminal and Gateway unit. This is done by the calling terminal sending a Connection Request (CRQ) to the called terminal on the H.323 well known port. This message is send unreliably and must contain the originating network address (dynamic port) on which the caller wishes to establishing the reliable connection for H.245 logical channel zero.

The called terminal may either answer the call, reject the call, or ignore the call. (e.g. it is ringing and no-one is home) In the reject case, the destination terminal responds with a Connection Rejection (CRJ) on the well known port. If answering, the destination provides the dynamic port to the caller in the Connection Confirmation (CCF).

Between the time the destination receives a Connection Request and the time it answers or rejects the call, it must periodically send a Connection In Progress (CIP) message to the caller to update its status (e.g. ringing). The CIP should be sent every "n" seconds, where "n" is the number of seconds the caller has requested in the CRQ message. The call is now established and phase B is entered.

(I realize the CIP message is essentially taking the status of the Q.931 messages Release, Disconnect, Alerting, and Call Proceeding messages and placing them in a single message. To date I have not have the opportunity (time) to make the proposed PDU's "Q.931 like". I have no issue with using the Q.931 status messages for these cases, but given the complexity of the Q.931, I chose to spend my time on the larger open issues)

If the call is accepted, H.245 communications begin using logical channel zero on the dynamic port negotiated in the CRQ, CCF exchange.

7.2.2 Call Set-up with a Single Gatekeeper

Given that the Gatekeeper is optional, there are three call scenarios: Caller and Callee bound to Gatekeepers, Callee only bound to a Gatekeeper, and Caller only bound to a Gatekeeper. Participation in the mixed mode conference (e.g. only one side bound to a Gatekeeper) is optional.

7.2.2.1 Caller and Callee bound to a single Gatekeeper

When there is a single Gatekeeper on the network, call signaling takes place between the terminals or terminal and Gateway unit through the Gatekeeper. This is done by the calling terminal sending a Connection Request message (CRQ) to the Gatekeeper. The Gatekeeper evaluates the request based on its programmed criteria and if the call is allowed continues as described below. If the Gatekeeper deems the call inappropriate, it will send a Connection Rejection (CRJ) to the caller with the appropriate reason code. {Note: terminal signaling is identical to section 7.2.1} If the Gatekeeper allows the call, the Gatekeeper forwards the CRQ to the destination terminal.

After receiving the CRQ, the destination terminal responds to the Gatekeeper with a CCF or CRJ as described in section 7.1.2. The Gatekeeper forwards the destination's response back to the caller. See Figure 3.

If the call is accepted, H.245 communications begin using logical channel zero on the dynamic port negotiated in the CRQ, CCF exchange.

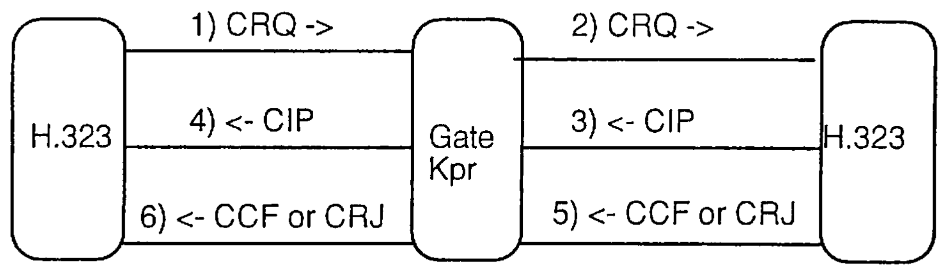


Figure 3

7.2.2.2 Callee bound to Gatekeeper

Support for this mode is optional.

In this case, the callee receives a CRQ with an indication that the caller has no Gatekeeper. The Callee will send a CRQ to its Gatekeeper (CallType set to "Request to Answer"), and if it receives a CCF, continue with call setup as described in section 7.2.1. If a CRJ is received from the Gatekeeper, the terminal will respond to the caller with a CRJ and the appropriate reason code. See Figure 4.

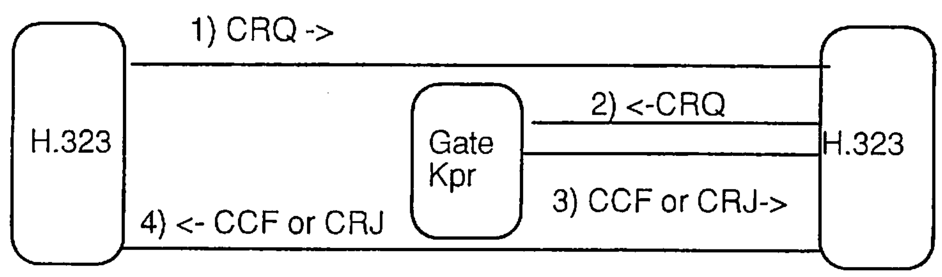


Figure 4

7.2.2.3 Caller bound to Gatekeeper

Support for this mode is optional.

In this case, the signaling follows section 7.2.3 with the exception that the callee responds to the Guardian Query Request (GQQ) with a Guardian Query Reject (GQRJ) indicating that it is not bound to a Gatekeeper. In this case, the Gatekeeper continues with the Call Setup by directly sending a CRQ to the callee. The callee should respond to the Gatekeeper with a CCF or CRJ and the connection should proceed as described in section 7.2.1. See Figure 5.

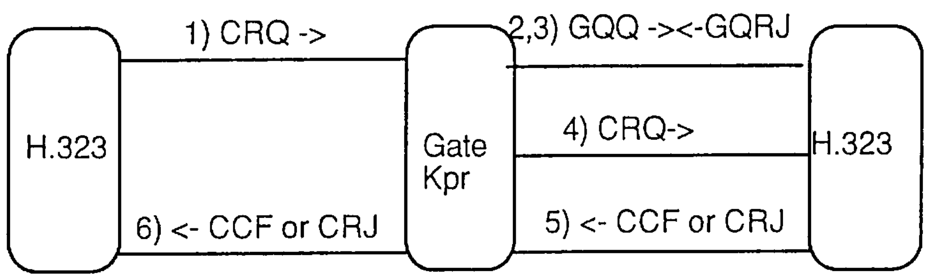


Figure 5

7.2.3 Call Setup with Multiple Gatekeepers Present

When there is multiple Gatekeepers on a network, call signaling takes place between the terminals or terminal and Gateway unit through the Gatekeepers. This is done by the calling terminal sending a Connection Request message (CRQ) to its Gatekeeper. The Gatekeeper evaluates the request based on its programmed criteria and if the call is allowed continues as described below. If the Gatekeeper deems the call inappropriate, it will send a Connection Rejection (CRJ) to the caller with the appropriate reason code. (Note: terminal signaling is identical to section 7.2.1)

The Gatekeeper who receives the CRQ from one of its register clients, sends a Guardian Query Request (GQQ) to the destination network address on the H.323 well known port to ask the question "Who is your Gatekeeper?". A terminal which receives a GQQ, and is bound to a Gatekeeper, must respond with a Guardian Query Response (GQRS) answering "My Gatekeeper is x". Note: If the destination terminal is bound to the same Gatekeeper as the caller, signaling occurs as described in section 7.2.2.

The caller's Gatekeeper now sends the CRQ to the callee's Gatekeeper. The callee's Gatekeeper evaluates the request based on its programmed criteria and if the call is allowed, forwards the CRQ to the destination terminal. If the callee's Gatekeeper deems the call inappropriate, it responds with a Connection Rejection (CRJ) to the caller's Gatekeeper which is then forwarded to the calling terminal.

After receiving the CRQ, the destination terminal responds to its Gatekeeper with a CCF or CRJ as described in section 7.1.2. The Gatekeeper forwards the destination's response back to the caller's Gatekeeper. See Figure 6.

If the call was accepted, H.245 communications begin using logical channel zero on the dynamic port negotiated in the CRQ, CCF exchange.

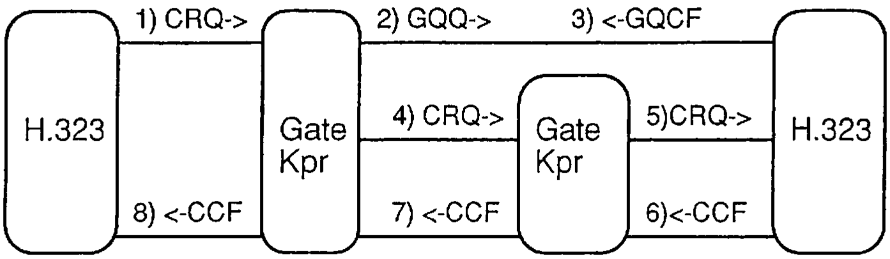


Figure 6

7.2.4 Call Set-up via Gateways

The connection procedure for calling a H.320 system via the Gateway is identical to the description in Sections 7.2.1, 7.2.2, and 7.2.3 with the exception that the H.323 terminals must now pass the WAN dial string information in the Connection Request (CRQ). Inbound calls work in a similar fashion with the Gateway sending the CRQ to its bound Gatekeeper.

Important: The H.323 endpoints do not need to know the location of Gateways. The Gatekeeper will route calls without WAN information in their Connection Requests (CCR) to the specified LAN addresses in the request. The Gatekeeper will route calls with WAN information in their Connection Requests (CRQ) to one of their attached Gateway units. This simple Gatekeeper dialing rule allows terminals to have identical signaling for all calls. If both a network address and WAN information appear in the same connection request, the Gatekeeper will assume the call is to a LAN node on a remote LAN that is being accessed via back to back Gateways.

7.2.4.1 Gateway Inbound Call Set-up

If the call is in-bound from the Gateway, the CRQ message contains an E.164 address which can be mapped to the actual destination by the Gatekeeper.

7.2.4.2 Gateway Outbound Call Set-up

If the call is outbound through the Gateway from a terminal, the CRQ will contain WAN information signaling the Gatekeeper to automatically route the call to a Gateway.

7.3 Phase B - Initial communication and capability exchange

When the connection has been acknowledged, Phase B begins. The Control Channel is immediately opened between the two terminals on the dynamic port negotiated in phase A.

{No proposed change to the remaining 7.3 text}

{No proposed changes to the section 7.4}

7.5 Phase D: Call termination

{Call termination as described in H.323 should remain except item 4) "End Session" which should be modified as described below:}

7.5 1 Call Termination without a Gatekeeper

Either side can disconnect by sending a Disconnect Request (DRQ) directly to the remote terminal on the H.323 well known port. After receiving a Disconnect Request, an endpoint must respond with a Disconnect Confirmation (DCF).

7.5.2 Call Termination with a single Gatekeeper

Disconnect between clients occurs first, followed by a notification to the Gatekeeper that the call has dropped.

Either side can disconnect by sending a Disconnect Request (DRQ) directly to the remote terminal on the H.323 well known port. After receiving a Disconnect Request a terminal must respond with a Disconnect Confirmation (DCF). After sending or receiving the confirmation, each terminal must send a Disconnect Request to its Gatekeeper to notify it that the call has been torn down. The Gatekeeper must respond with a Disconnection Confirmation. If a link is abnormally terminated; thereby preventing the normal disconnect procedure from occurring, the disconnect procedure with the Gatekeeper should still be completed. See Figure 7.

The Gatekeeper can end any conference by sending a Disconnect Request (DRQ) to all of the parties involved in the conference.

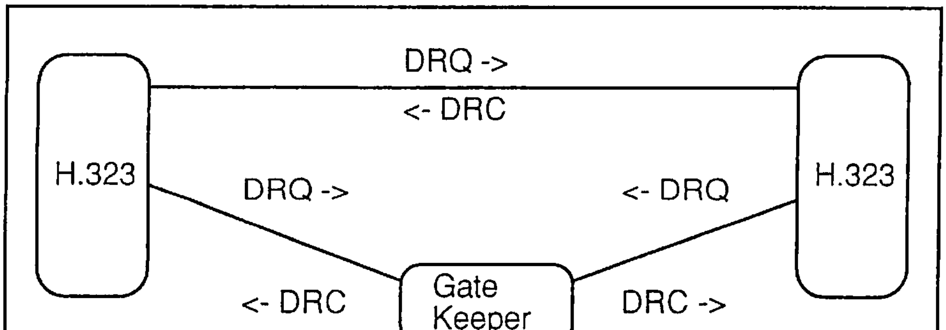


Figure 7

7.5.3 Call Termination with Multiple Gatekeepers

When disconnecting, each terminal and Gateway must notify the Gatekeeper it is registered with about the call termination. See Figure 8.

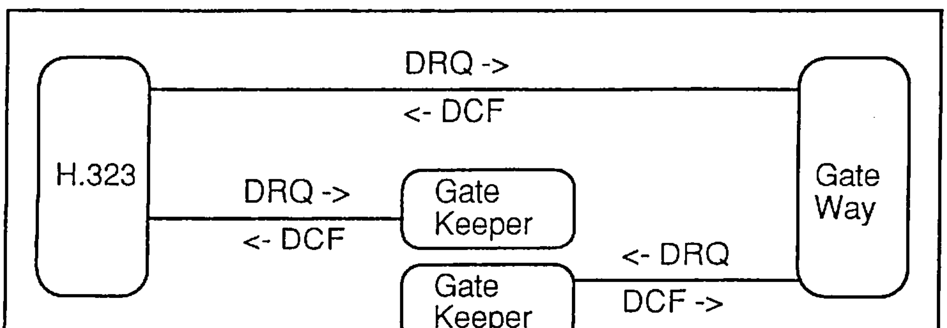


Figure 8