



Agilent Technologies

Troubleshooting H.323 Signaling

White Paper

By Stefan Pracht
Product Marketing Manager

Agilent Technologies
Network Systems Test Division



Agilent Technologies

Contents

Introduction	page 3
Test Configuration	page 3
Gate Keeper Discovery and Registration	page 5
Correlation of Messages	page 6
Problem Identification	page 6
Call Setup	page 7
Call Setup Message Correlation	page 8
Problem Identification Call Setup	page 8
Initial Communications and Capability Exchange	page 9
Message Correlation - Master - Slave Determination Capability Exchange	page 10
Problem Identification Master - Slave Determination Capability Exchange	page 11
Establish Audio Communication	page 11
Message Correlation - Establish Audio Communication	page 12
Problem Identification - Establish Audio Communication	page 12
Audio Transmission	page 13
Collision with Reality	page 13

Introduction

H.323 is known for quite complex signaling, high connection set-up latencies, and implementation difficulties. In addition, compliance by implementers is usually limited to a subset of H.323's functionality. Despite these shortcomings H.323 is widely implemented and is a common method for Voice over IP transport. H.323 is potentially the primary common denominator for all VoIP.

The inability to connect is the *simple* result of some failure in a very *complex* process of protocol exchanges. H.323 defines several protocol exchange stages between the terminals, gateways, and gatekeepers before an audio connection can be established. Furthermore, H.323 signaling messages have dynamically assigned transport addresses which make it difficult to identify and correlate them. This information has to be extracted out of previous signaling messages.

This paper highlights the potential signaling problems during connection setup and how to identify them. It will show the information to look for in specific signaling messages and how to identify subsequent messages.

Test Configuration

To simplify the discussion and to focus on the most common problems, we will work with a simple test scenario. Figure 1 shows two H.323 gateways that are connected to the same gatekeeper through an IP network such as a LAN. Both gateways belong to the same gatekeeper management domain or zone. We will focus on the protocol exchange on the IP side; interworking between the telephone network and IP signaling is not discussed. Since the scenario described focuses on the IP side, we would see the same messages as if there were end-user terminals such as PCs running Microsoft® NetMeeting instead of the gateways.

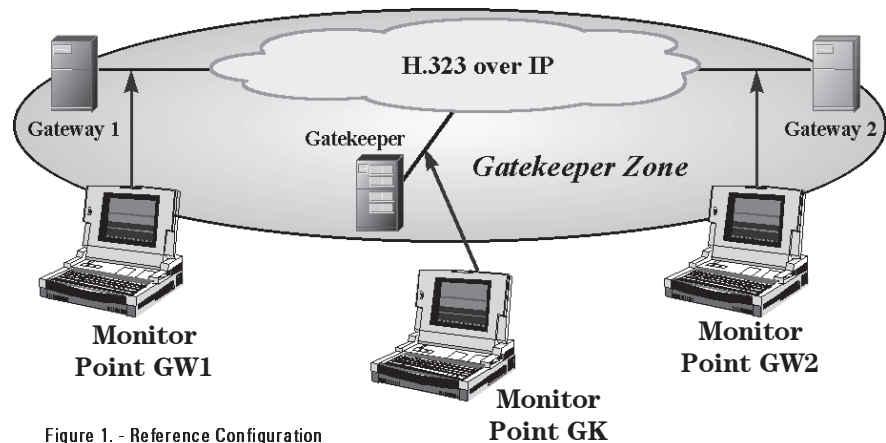


Figure 1. - Reference Configuration

Some conventions:

- The tests described are based on H.323 version 2.
- Multicast connections and Multicast Control Units are not discussed.
- Expressions in italics are message or field names used in the ITU-T Recommendations.

Figure 2 depicts the protocols defined in H.323 and how they are carried over IP. The protocols highlighted in blue are discussed in this paper.

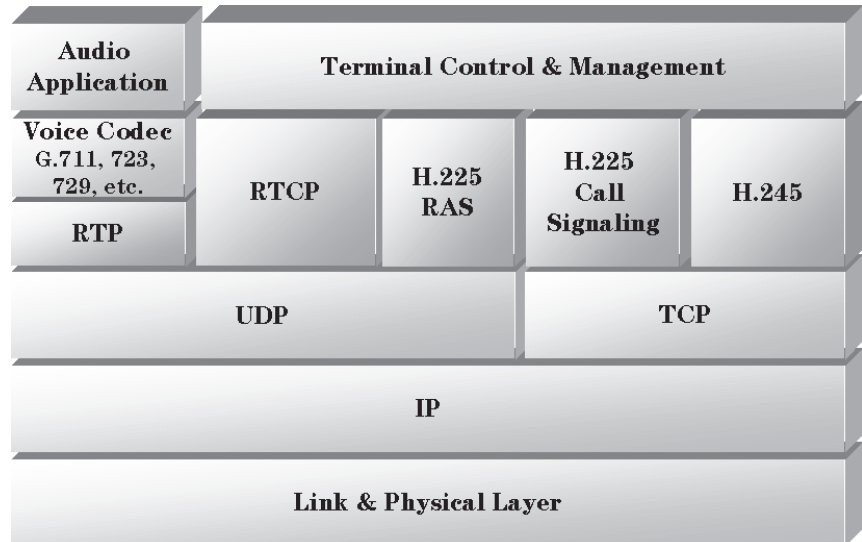


Figure 2. H.323 Protocol Stack

H.323 has defined several protocol exchange stages between the terminals, gateways, and gatekeepers before an audio connection can be established. In order to set up a connection between the two terminals, the steps in Figure 3 have to be performed successfully:

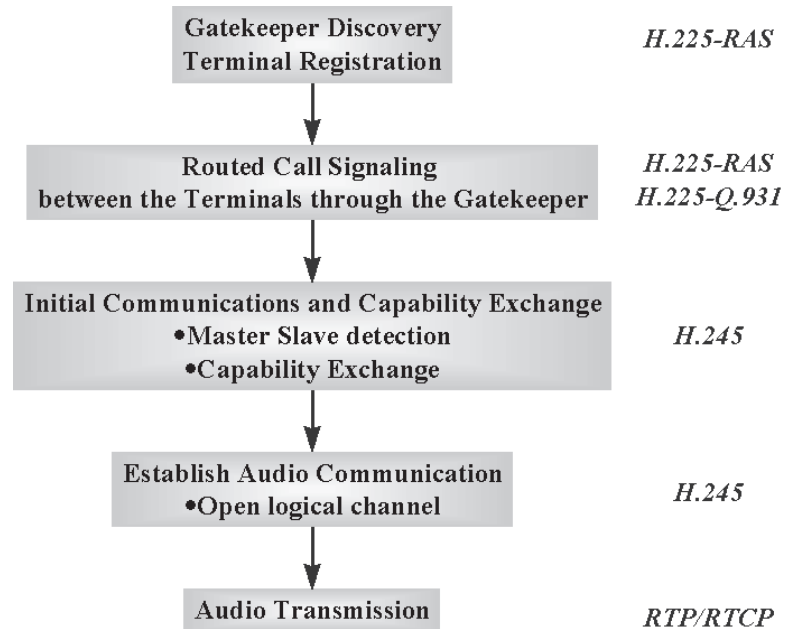


Figure 3. H.323 Connection and Session Setup

Gatekeeper Discovery and Registration

For gatekeeper discovery and registration, the gateway uses H.225-RAS signaling. The RAS signaling channel is opened before any of the other channels between gateways are established, and is independent from the H.245 control channel.

When a gateway first connects to the network, it needs to register with a gatekeeper. This can be done manually or automatically. In our example, we assume it is done automatically. After the gateway successfully discovers its gatekeeper, it then joins this particular gatekeeper zone by informing the gatekeeper of its IP address and related alias addresses. These alias addresses can be phone numbers (E.164 address), names, or Internet addresses.

A successful discovery and registration process is shown in Figure 4:

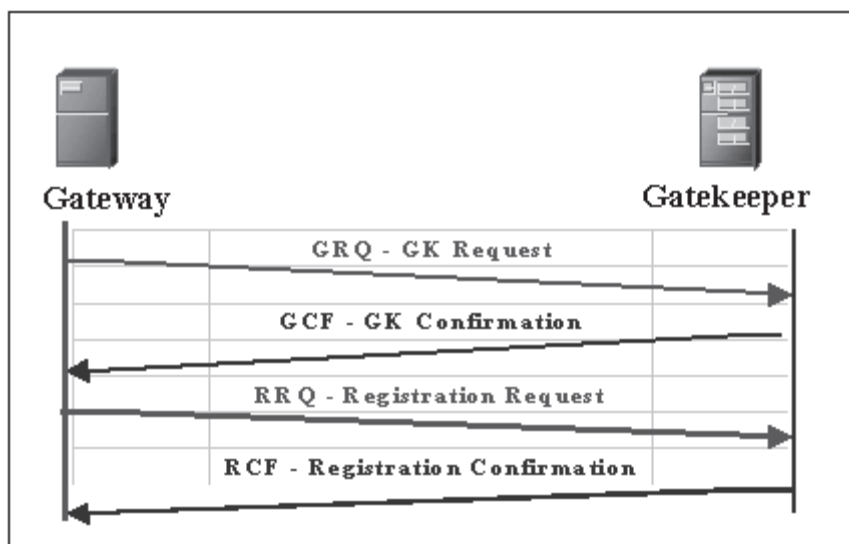


Figure 4. H.225-RAS - Auto discovery and registration

Correlation of the Messages

When monitoring an H.323 Voice over IP link, one of the challenges is to identify which responses belong to which requests. The following table shows the information necessary to identify messages that belong to a particular protocol exchange. For each message, the table shows:

- “Identification Information” - the information contained in an earlier message that can be used to identify the current message.
- “Correlation Information” - the information contained in the current message that is needed to correlate later messages.

Message	Identification Information from <u>previous</u> messages	Correlation Information for <u>later</u> messages
GRQ Gatekeeper Request	Gatekeeper IP Discovery Multicast Address 224.0.1.41, UDP Port 1718	<ul style="list-style-type: none"> • Gateway <i>RAS Address</i>* • <i>Request Sequence Number</i>
GCF Gatekeeper Confirmation	<i>GRQ</i> message <ul style="list-style-type: none"> • Gateway <i>RAS Address</i>* • <i>Request Sequence Number</i> 	<ul style="list-style-type: none"> • gatekeeper <i>RAS Address</i>*
RRQ Registration Request	<ul style="list-style-type: none"> • Either Gatekeeper UDP Discovery Multicast Address* 224.0.1.41, Port 1719 • Or <i>GCF</i> message - gatekeeper <i>RAS Address</i>* 	<ul style="list-style-type: none"> • <i>Request Sequence Number</i> • Gateway <i>RAS Address</i>* • Gateway <i>Call Signal Address</i>*
RCF Registration Confirmation	<i>RRQ</i> message <ul style="list-style-type: none"> • Gateway <i>RAS Address</i>* • <i>Request Sequence Number</i> 	<ul style="list-style-type: none"> • Gateway <i>End-Point Identifier</i> • gatekeeper <i>Call Signal Address</i>*

* IP address and UDP port number

1.1 Problem Identification Gatekeeper Discovery and Registration

Several problems may arise that prevent the gateway from registering:

- The gatekeeper does not reply.
- The gatekeeper rejects the registration.

In the first case, the gatekeeper either did not receive the request or did not confirm the request. Some of the reasons might be:

- LAN or IP connectivity problems.
- Incorrect configuration of the gatekeeper Discovery Multicast IP Address and port number in the gateway or gatekeeper.
- Packet loss - H.225-RAS messages are sent via UDP, an unreliable transport mechanism.

The simplest way to check connectivity is to send a ping to the IP address of the Gatekeeper. This validates both its address and the ability to connect to it.

The second reason the gateway cannot register (i.e. the gatekeeper rejects the registration attempt) can be determined by looking at the *Reject Reason* field in the *Gatekeeper Reject* message and *Registration Reject* message. Connecting a protocol analyzer to the gateway connection (monitor point GW1) and gatekeeper connection (monitor point GW2) allows you to monitor the link and to analyze the messages that are exchanged.

- In the case of *Gatekeeper Reject* message and *Registration Reject* message, examples are:
 - The gateway has no permission to join this zone based on the IP address submitted.
 - The gateway has a different version of the H.323 protocol than is supported by the gatekeeper and is therefore not able to join.
- In the case of the *Registration Reject* message, examples are:
 - Invalid H.225 call signaling address.
 - The gateway submitted H.225 RAS address is invalid.
 - The gateway submitted an H.225 call signaling address that is invalid.
 - The gateway uses an alias already registered to another gateway.
 - The gatekeeper does not support this particular gateway type.

Further Information

More detailed information can be obtained from the ITU-T Recommendations:

- H.323 - Chapter 6.2.9, 7.1, 7.2, 8.1
- H.225 - Chapter 7.6 - 7.11, Appendix IV.1

Call Setup

H.225.0 call signaling is used to establish a connection between two gateways. In this example, we will use the gatekeeper “Routed Call Signaling”. In this method, all H.225 signaling messages are routed via the gatekeeper to the gateways. Another method is “Direct gateway Call Signaling” as described in H.225. In this case, the H.225 signal messages are exchanged directly between the gateways after having received admission from the gatekeeper for this particular connection setup procedure. A successful call set up is shown in the next figure.

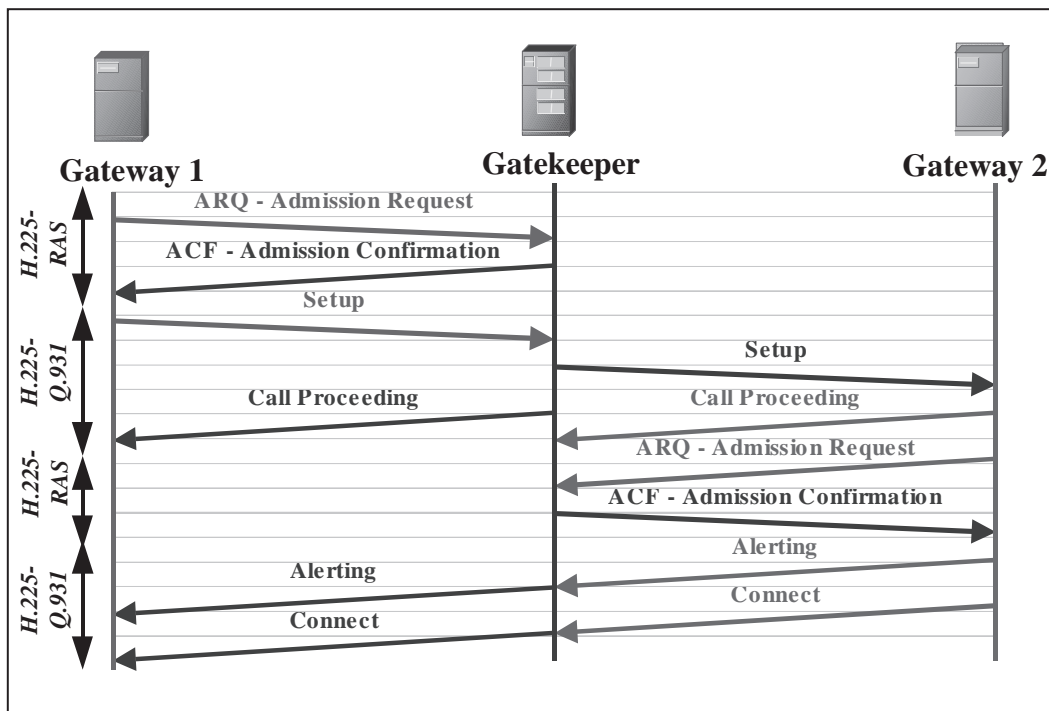


Figure 5. H.225-RAS - Gatekeeper Routed Call Signaling

Call Setup Message Correlation

The following table shows the information necessary to identify messages that belong to a particular protocol exchange.

	H.225 Message	Identification Information from previous messages	Message Information For later message correlation
RAS	ARQ Admission Request	<ul style="list-style-type: none"> • GCF message - gatekeeper RAS Address* • RCF message - End-Point Identifier 	<ul style="list-style-type: none"> • Request Sequence Number • Gateway End point Identifier • Gateway RAS Address* • Call Reference Value
RAS	ACF Admission Confirmation	<ul style="list-style-type: none"> • ARQ message • Gateway RAS Address* • Request Sequence Number 	<ul style="list-style-type: none"> • Gatekeeper Destination Call Signaling Address*
Q.931	Setup 1 - Gateway 1 to gatekeeper	<ul style="list-style-type: none"> • ACF message - gatekeeper Destination Call Signaling Address* • ARQ message Call Reference Value 1 	<ul style="list-style-type: none"> • Call Reference Value 1 Gateway 1 information, all optional: • E.164 Calling party number • H.245 Address* • Source Address* (H.323 alias Address*)
Q.931	Setup 2 - gatekeeper to Gateway 2	<ul style="list-style-type: none"> • RRQ message - Gateway 2 Call Signaling Address* Optional Setup 1 message: • Gateway 1 E.164 Calling party number • Gateway 1 H.245 Address* • Gateway 1 Source Address* (H.323 alias Address*) 	<ul style="list-style-type: none"> • Call Reference Value 2 • Gateway 1 H.245 Address*
Q.931	All other H.225 Call signaling messages destined to gatekeeper	<ul style="list-style-type: none"> • ACF message - gatekeeper Destination Call Signaling Address* • ARQ message Call Reference Value 1 when Gateway 1 source • Setup message 2 Call Reference Value 2 when Gateway 2 source 	<ul style="list-style-type: none"> • H.245 Address*
	All other H.225 Call signaling messages destined to Gateway	<ul style="list-style-type: none"> • Different values depending whether sent to Gateway 1 or 2 • RRQ message - Gateway Call Signaling Address* • Setup message Call Reference Value 	<ul style="list-style-type: none"> • H.245 Address*

* IP address and UDP port number for RAS or TCP port number for Q.931 messages

Problem Identification Call Setup

The following problems may arise:

A) Admission is rejected.

Instead of receiving an *Admission Confirmation* message the gatekeeper replies with an *Admission Reject* message. This can be caused by:

- The called party is not registered with this gatekeeper zone or a remote gatekeeper zone to which the local gatekeeper has access.
- There is no bandwidth available.
- The calling gateway is not registered.
- The calling gateway is no longer registered with the gatekeeper.
- Invalid calling gateway *Endpoint identifier*.

The *Admission Reject* message has the same identification information as described for the *Admission Confirmation* message. The *Admission Reject* message contains a field called *Reject Reason* that provides the cause for the rejection.

B) No *Call Proceeding* message. The Call Proceeding message is optional.

C) No *Alerting* message received. Alerting indicates that at the far end “phone” is ringing. Not every vendor might implement this because the H.225 Recommendation states in one chapter as mandatory and in another as optional.

D) Release complete is received after setup was sent. Release complete indicates that the call could not be completed. The Release Complete message indicates the reason in its *Release Complete Reason* field:

- Bandwidth taken away or *Admission Request* denied.
- Gatekeeper, gateway, or network resources exhausted.
- No transport path to destination.
- Called party rejected call.
- Called gateway's gatekeeper rejected.
- Called gateway cannot reach gatekeeper for *Admission Request*.
- Bad address format.

Release Complete message indicates the reason in its *Release Complete Reason* field:

- Bandwidth taken away or *Admission Request* denied.
- Gatekeeper, gateway, or network resources exhausted.
- No transport path to destination.
- Called party rejected call.
- Called gateway's gatekeeper rejected.
- Called gateway cannot reach gatekeeper for *Admission Request*.
- Bad address format.

E) Calling gateway does not react to *Connect* message.

The most likely cause is that the Q.931 "Setup timer" expired. This timer defines how long the calling gateway shall wait for Alert, Call Proceeding, and Connect messages. The timer is usually set to 4 seconds. If the timer expires the first time, the Setup is sent again. If it expires the second time, the call is cleared in the gateway call reference table and no further messages are sent.

Another timer is the Q.931 "establishment timer" which defines how long the calling gateway shall wait for the called gateway to respond. When the connect message is not received within 4 minutes after *Alerting* message is received, the call is cleared.

Further Information

More detailed information can be obtained from the ITU-T Recommendations:

- H.323 - Chapter 6.2.10, 7.3 - 7.5, 8.1
- H.225 - Chapter 7.1 - 7.5
- Q.931

Initial Communications and Capability Exchange

After the connection is successfully established, end-to-end control messages are exchanged that determine the operation of the H.323 gateways. In our example, H.245 signaling is established between the two gateways directly. H.323 also allows the messages to be forwarded via the gatekeeper.

For each of the calls established using H.225 there is one H.245 control channel. This control channel is carried on logical channel 0. This channel is open during the entire call and does not need to be opened or closed the way that other channels are.

In this step, we consider two procedures:

- Master slave determination. This is used to avoid two gateways initiating similar events simultaneously.
- Capability exchange. This is used to ensure that the two gateways exchange only signals that can be processed by the receive gateway. This requires that both gateways agree on common formats for the number of audio, visual, and data streams on which they can simultaneously send and receive. They must also agree on the encoding and decoding mechanism to be used, whether encryption is used, the type of encryption (if used), and so on.

The following figure shows a successful master slave determination and capability exchange:

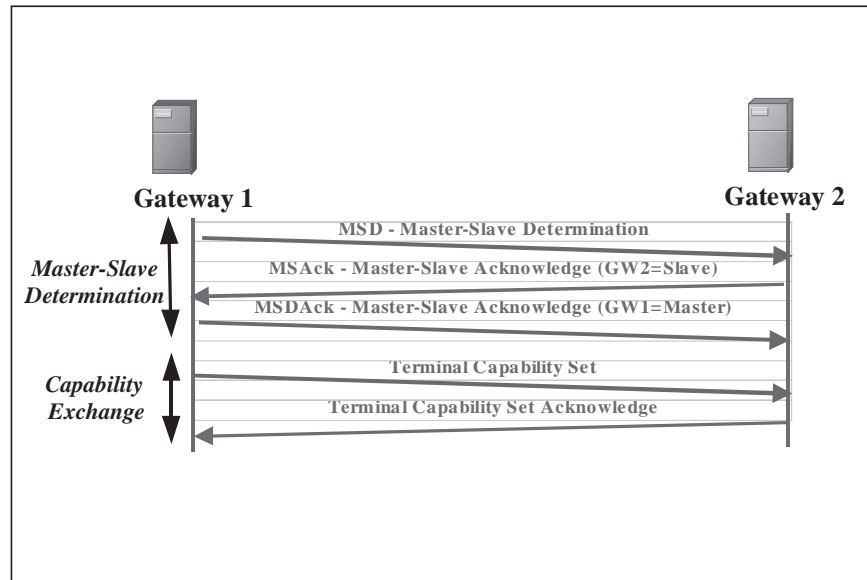


Figure 6. H.245 - Master slave determination and capability exchange

As shown in the above figure, Gateway 1 sends a *Master Slave Determination* message to Gateway2. Gateway2 compares its *Gateway Type* and *Status Determination Number* field values with the values contained in the received *Master Slave Determination* message and determines whether it is the master or slave. This is communicated and confirmed via the *Master Slave Acknowledge* message.

Message Correlation - Master-Slave Determination Capability Exchange

The following table shows the information necessary to identify messages that belong to a particular protocol exchange.

H.245 Message	Identification Information from previous messages	Message Information For later message correlation
All <i>Master Slave Determination</i> messages	H.225-Q.931 <i>Connect</i> message - <i>H.245Address*</i> for each gateway	None
<i>Gateway Capability Set</i>	<ul style="list-style-type: none"> H.225-Q.931 <i>Connect</i> message - <i>H.245Address*</i> for each gateway Previous <i>Gateway Capability Set</i> message <i>Sequence Number</i> +1 	<ul style="list-style-type: none"> Sequence Number
<i>Gateway Capability Set Acknowledge</i> and <i>Reject</i>	<ul style="list-style-type: none"> H.225-Q.931 <i>Connect</i> message - <i>H.245Address*</i> for each gateway Last <i>Gateway Capability Set</i> message <i>Sequence Number</i> 	None

* IP address and TCP port number

Problem Identification - Master-Slave Determination and Capability Exchange

The following problems may arise:

A) Master-Slave Determination (MSD) failed. This can be identified through the following messages monitored on the link:

- One gateway receives MSDReject message received at another gateway site - *gateway Type* and *Status Determination Number* values of both gateways are the same and no master or slave can be determined.
- Initiating gateway generates MSDRelease message - initiating side has not received a response from the other gateway within the time set for timer T106.

B) Gateway Capability exchange failed. This can be identified through the following messages monitored on the link:

- The initiating gateway receives a *Gateway Capability Set Reject* message indicating the other gateway is incapable of handling the request. Causes are identified in the Cause field of the message:
 - An undefined table entry.
 - The gateway was incapable of storing all description or table information provided in the gateway Capability Set message.
- The initiating gateway sends a *gateway Capability Set Release* message indicating that the initiating gateway did not receive a *gateway Set Acknowledge* or *gateway Capability Set Reject* message in the time set in the T101 timer since sending the *gateway Capability Set* message.

Further Information

More detailed information can be obtained from the ITU-T Recommendations:

- H.323 - Chapter 6.2.8, 8.2, Annex A
- H.245 - Chapters 5.1-2, 6., 7.1-2, 8.2-3, Appendix II.2-3, Appendix, III.1

Establish Audio Communication

After the master and slave operation is determined and the capabilities are exchanged, the logical channels can be established between the two gateways to carry the audio and video streams. This procedure is also defined in H.245 and is called “open logical channels”.

One logical channel is opened for every individual audio and video stream. Every request to open a logical channel contains a full description of the content of the logical channel. This includes media type, algorithm used, options, and all other information needed for the receiver to interpret the content of the logical channel. This mechanism ensures that the gateway is ready to receive and decode the data on this particular channel.

In our example, we set up unidirectional channels, which allows a different number of channels to be established from gateway 1 to 2 than from 2 to 1. The logical channel is opened and received from the transmitter side.

The following figure shows a successful channel opening:

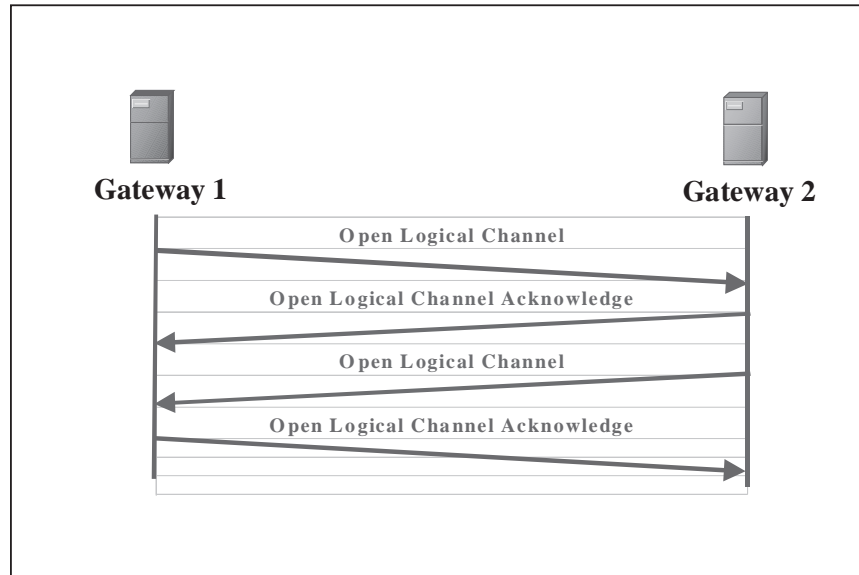


Figure 7. H.245 - Open Logical Channel

Message Correlation - Establish Audio Communication

The following table shows the information necessary to identify messages that belong to a particular protocol exchange.

H.245 Message	Identification Information from previous messages	Message Information For later message correlation
Open Logical Channel	H.225-Q.931 <i>Connect</i> message - <i>H.245Address*</i> for gateway 2	<ul style="list-style-type: none"> • <i>Logical Channel Number</i> • <i>Session ID</i> - RTP Session identifier • <i>Media Control Channel</i> - reverse RTCP transport Address* • <i>Transport Address*</i> - RTP IP Address* and UDP port number
Open Logical Channel Acknowledge	<ul style="list-style-type: none"> • H.225-Q.931 <i>Connect</i> message - <i>H.245Address*</i> for gateway 1 • <i>OLC</i> message - <i>Logical Channel Number</i> 	

* IP address and TCP port number

Problem Identification - Establish Audio Communication

The following problems may arise when establishing a logical channel:

A) Receiving gateway rejects opening of channel. This requires the gateway to send an *Open Logical Channel Reject* message back to the initiator. The *cause* field in the reject message indicates:

- Data type unknown, not supported or unavailable.
- Multicast channel not allowed.
- Insufficient bandwidth.
- Invalid session ID.
- Master slave conflict.

B) The initiating gateway sends a *Close Logical Channel* message to its peer before receiving *Open Logical Channel Acknowledge*. In the case when the initiating gateway does not receive the acknowledge message in time, the gateway will release this call. The gateway timer H.245-T103 determines this duration.

Further Information

More detailed information can be obtained from the ITU-T Recommendations:

- H.323 - Chapter H323: 6.2.8.2, 8.3, Annex A
- H.245 - Chapters 5.3, 7.3, 8.4, Appendix II.4, Appendix III.1

Audio Transmission

After all of the above steps audio packets can now be exchanged. Two protocols are used for the exchange of audio:

- Audio data is sent via RTP packets to the IP address and UDP port number defined in the *Open Logical Channel* message.
- The quality of the audio received is communicated via RTCP, the RTP Control Protocol. This allows the sending gateway to control an adaptive encoder. It can also be used to indicate problems to the user. Unfortunately, not every vendor is necessarily supporting RTCP generation.

RTCP packets are sent to the IP address and UDP port number defined in the *Open Logical Channel* message. Another way to correlate the RTCP packet stream with the RTP stream is via the SSRC (Synchronization Source) identifier contained in both RTP and RTCP packets.

H.323 - Collision with Reality

This description probably proved the point that H.323 is quite a complex protocol. In our example, we just addressed simple connection and session setup procedures, assuming that both implementations work compliant with the ITU-T Recommendation. However in reality, implementations are rarely fully compliant. The challenge then is to deal with problems such as hardcoded UDP or TCP port numbers for certain protocol types, invalid RTP payload types, or large call setup delay that exceeds internal timers and terminates the connection before the setup is finished. These types of problems are difficult to address in this paper, especially with all that could be implemented in a non-compliant manner.

In this paper, we discussed how systems should behave based on H.323 and how to identify the various messages that, in the correct order and coding, lead to a successful connection setup. With this information at hand, it is possible to identify non-compliant behavior and to explain why a connection setup failed. Even if two non-compliant gateways are still able to setup a connection, chances are that they will not necessarily interoperate with a gateway from a different vendor. Protocol analyzers are important tools to examine H.323 signaling behavior and to identify problems that may arise.

About the Authors

Stefan Pracht

Stefan Pracht is a Product Marketing Manager for Agilent Technologies' Network Systems Test Division focusing on voice, fax, and IP test solutions for next generation networks. Stefan has been instrumental in the development of Agilent's VoIP business and is managing the definition and market deployment of the Telegra line of fax, voice quality, and VoIP test and analysis products.

During the last six years with Hewlett-Packard Company and now Agilent Technologies, he has worked on the definition and introduction of several products and services focusing on digital communications and telephony test and analysis systems. Stefan has developed cable modem and IP analysis system business strategies for a range of HP/Agilent products.

Prior to joining Hewlett-Packard/Agilent Technologies, Stefan worked as a project manager for Deutsche Telekom's national and international ATM trials. Stefan holds a Bachelors of Science in Telecommunications degree from the University of Dieburg, Germany and has several years of experience in product definition, development, and introduction.

Notes:

**Agilent Technologies'
Test and Measurement Support,
Services, and Assistance**

Agilent Technologies aims to maximize the value you receive, while minimizing your risk and problems. We strive to ensure that you get the test and measurement capabilities you paid for and obtain the support you need. Our extensive support resources and services can help you choose the right Agilent products for your applications and apply them successfully. Every instrument and system we sell has a global warranty. Support is available for at least five years beyond the production life of the product. Two concepts underlie Agilent's overall support policy: "Our Promise" and "Your Advantage."

Our Promise

Our Promise means your Agilent test and measurement equipment will meet its advertised performance and functionality. When you are choosing new equipment, we will help you with product information, including realistic performance specifications and practical recommendations from experienced test engineers. When you use Agilent equipment, we can verify that it works properly, help with product operation, and provide basic measurement assistance for the use of specified capabilities, at no extra cost upon request. Many self-help tools are available.

Your Advantage

Your Advantage means that Agilent offers a wide range of additional expert test and measurement services, which you can purchase according to your unique technical and business needs. Solve problems efficiently and gain a competitive edge by contracting with us for calibration, extra-cost upgrades, out-of-warranty repairs, and on-site education and training, as well as design, system integration, project management, and other professional engineering services. Experienced Agilent engineers and technicians worldwide can help you maximize your productivity, optimize the return on investment of your Agilent instruments and systems, and obtain dependable measurement accuracy for the life of those products.

By internet, phone or fax, get assistance with all your Test and Measurement needs.

Online assistance:

<http://www.agilent.com/find/assist>

United States:

(Tel) 1 800 452 4844

Canada:

(Tel) 1 877 894 4414
(Fax) (905) 282 6495

China:

(Tel) 800-810-0189
(Fax) 1-0800-650-0121

Europe:

(Tel) (31 20) 547 2323
(Fax) (31 20) 547 2390

Japan:

(Tel) (81) 426 56 7832
(Fax) (81) 426 56 7840

Korea:

(Tel) (82-2) 2004-5004
(Fax) (82-2) 2004-5115

Latin America:

(Tel) (305) 269 7500
(Fax) (305) 269 7599

Taiwan:

(Tel) 080-004-7866
(Fax) (886-2) 2545-6723

Other Asia Pacific Countries:

(Tel) (65) 375-8100
(Fax) (65) 836-0252

Product specifications and descriptions in this document subject to change without notice.

©Agilent Technologies, Inc. 2000-2001
Printed in U.S.A. October 5, 2001



5968-3642E

Use this link to go directly to our network troubleshooting solutions:

<http://www.agilent.com/comms/onenetworks>

