Agilent Technologies

Troubleshooting VoIP Signaling

Application Note 1320

Isolate Signaling and Performance Problems by Decoding H. 323 Traffic

Agilent Technologies
Innovating the HP Way

Contents

Introduction

New communications technologies are developed because they offer some advantage over existing ones. One recent example is Voice Over IP (VoIP) as defined by the International Telecommunication Union H.323 recommendation. But along with the benefits of new communications protocols come new challenges. For example, because H.323 is relatively new, network engineers and administrators struggle with multi-vendor compatibility, standards compliance and interpretation, and a whole host of other issues related to deploying and maintaining VoIP networks.

This Product Application Note provides a brief overview of the ITU-T H.323 recommendation as it relates to Voice Over IP networks. We will discuss some of the most common problems encountered by those deploying and maintaining VoIP networks - many of which are related to signaling. We will then show how to troubleshoot H.323 signaling problems using the Ethernet or Fast Ethernet Agilent Advisor LAN and its H.323 protocol decodes.

Note: although this Product Application Note refers to the Advisor LAN, the Advisor WAN and ATM analyzers provide H.323 decoding capabilities as well. In general, you can use the information and procedures described here in WAN and ATM situations.

How to Use This Product Application Note

You can use this Product Application Note as a resource for general VoIP technology and troubleshooting information. In addition, you can use it to learn how to take advantage of some of the Advisor's powerful analysis features. This Product Application Note's most important benefit, however, is the insight it provides into using protocol decodes to verify and troubleshoot H.323 signaling and signaling performance. Combining this Note with the Advisor's comprehensive on-line Help gives you the tools to isolate and solve H.323 signaling problems quickly and easily.

Overview of VoIP/H.323

This section provides a brief overview of the H.323 recommendation and discusses some of the problems network engineers and administrators will likely face as they work with this new communications technology. Problem solving strategies using the Advisor are presented later.

What is H.323?

ITU-T H.323 is an 'umbrella' recommendation that defines the methods and processes used for multimedia communications over packet networks such as IP-based LANs or WANs. H.323 describes the relevant network entities, various audio and video encoding methods, and how the H.225, Q.931, and H.245 Recommendations are used for call control, call setup, and capability exchange between terminals. H.323 is a flexible standard that provides numerous methods for similar processes. In addition, it is still evolving and will change as more communications providers deploy it and discover ways to standardize and refine its scope.

H.323 Architecture and Call Setup Process

This section briefly covers the basics of a network architecture and call set up process defined by H.323. More complete and detailed information regarding the H.323 recommendation can be obtained from your Agilent Technologies representative or from the Advisor Web site (URL: www.hp.com/go/internetadvisor).

Among other things, H.323 defines a network architecture that allows packetized voice traffic to be transmitted across IP networks that are connected to and interact with other data and voice networks. The main components of an H.323 VoIP network are:

- Terminal - an H.323 terminal is the endpoint on a packet network that provides for real-time, two-way communication with another H.323 entity. Terminals can be H.323 compliant multimedia PCs, Ethernet/IP telephones, or other similar devices.
- Gateway - the Gateway is an endpoint on the packet network that provides real-time, two-way communication between H.323 terminals, other ITU-T terminals, or other Gateways. Gateways also provide the connection path between H.323 terminals and other switched circuit networks (e.g. PSTNs). Gateways perform call setup and clearing between non-H.323 endpoints.
- Gatekeeper - the Gatekeeper provides address translation and controls access to the domain for which it is responsible (for example, a LAN or part of a packet network) for H.323 terminals, Gateways, and MCUs. Gatekeepers are optional, but when used they provide centralized management for authentication, routing, call detail recording, and bandwidth management.
- MCU - an MCU, or multi-point control unit, provides the capability for H.323 entities to participate in a multipoint conference. Troubleshooting the use of MCU functions is not covered in this Product Application Note.

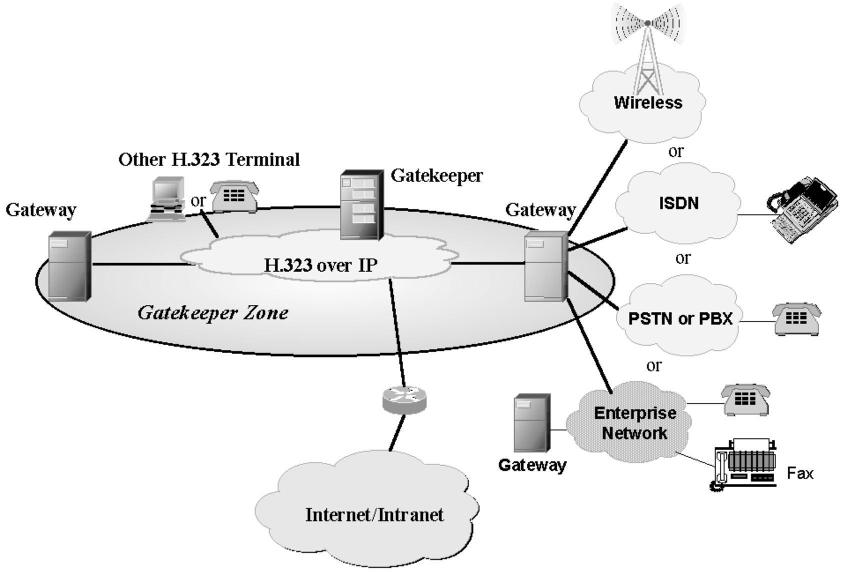


Figure 1.

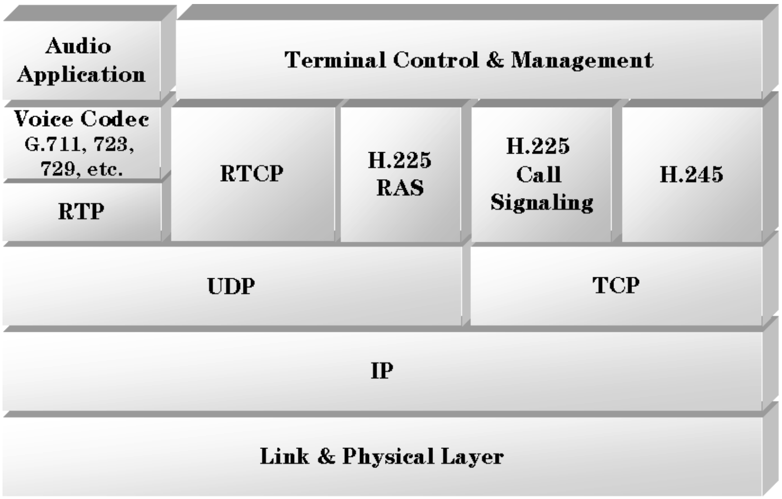


Figure 2.

Figure 1 shows a general H.323 VoIP implementation and how it might interact with other voice and data networks.

One of H.323's most important features is the signaling provided to establish, maintain, and clear a given voice call. Figure 2 shows the protocols used in this process as well as those used to transmit packetized audio. For the subject covered by this Product Application Note, the following protocols are of particular interest and importance:

- H.225 RAS (Registration, Admission, and Status) - used over UDP to transmit registration, admission, bandwidth changes, and status messages.
- H.225 Call Signaling (Q.931) - used over TCP for call setup and termination. It is a subset of the Q.931 messaging used in ISDN.
- RTP (real-time transport protocol) - used over UDP to transmit the digitized voice stream once the call and logical channel has been established.

Figure 3 shows the main steps in the signaling process and correlates these steps with the H.323 protocols used. Typically, the Gatekeeper Discovery and Registration step is performed automatically when H.323 entities are powered on or connected. The Routed Call Signaling step and those that follow occur when an VoIP call is initiated. Because the H.323 recommendation continues to evolve and network equipment manufactures learn more about implementing it, the signaling process shown here is likely to be a subset of signaling processes used. The troubleshooting techniques presented in this Product Application Note are useful regardless of the signaling variations you might encounter.

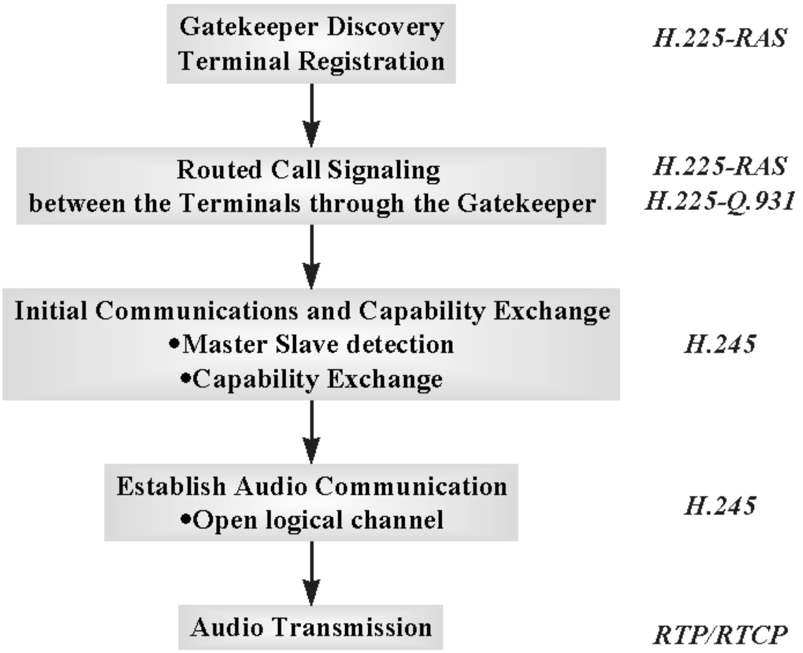


Figure 3.

Common Problems Encountered in H.323 Networks

While VoIP networks are subject to the same problems encountered in other networks - cable plant failure, badly configured or malfunctioning equipment, network congestion - there are a number of problems that are directly related to the characteristics of H.323 VoIP deployment. These fall into one of two categories described next.

Note: this Product Application Note will cover only those problems directly related to the H.323 protocol and voice over packet networks in general. General LAN, WAN, or ATM network troubleshooting techniques are covered in other Agilent Product Application Notes. Please go to the Advisor's Web site for more information.

Interoperability Problems

Interoperability problems caused by various interpretations of the H.323 recommendation can affect the signaling needed for call setup and maintenance. Optional or unclear details in this developing standard can lead to different network implementations by leading equipment vendors. In addition, services provided by one vendor may not be the same as those provided by another. At this early stage of VoIP deployment, interoperability between so called H.323 compliant equipment may prove the be the main source of trouble for network engineers and technicians. Codec compatibility, port number allocation, security concerns, and quality of service enforcement techniques are a few of the issues that are raised as vendors attempt to interoperate.

Performance Problems

Performance problems manifest themselves in a number of ways. Performance during signaling can disrupt a normally functioning process and cause unacceptable call setup delays. Inadequate performance can also affect voice quality - lost packets or excessive and varying packet delay can cause poor sound quality. Low bit rate codecs can adversely affect performance by increasing packet loss.

An aspect of performance not directly related to H.323/IP operation is the affect voice traffic will have on existing IP data traffic. The load imposed by voice traffic can cause sever congestion in a network not designed with VoIP in mind. On the other hand, high utilization not related to voice traffic can affect VoIP performance. Codec choice can affect traffic load. For example, codecs that do not use compression will result in higher overall traffic levels.

How the Advisor Can Help

The Advisor's H.323 decoding capability, coupled with its comprehensive and powerful network analysis features makes it a valuable tool when dealing with signaling or performance problems in a VoIP network. Decoding H.323 signaling messages is the most direct way to see just what is happening when multi-vendor VoIP networks fail.

Troubleshooting Voice Over IP Signaling

This section covers VoIP signaling troubleshooting techniques using the Advisor LAN. The primary tool is the Advisor's H.323 decode capability. The following areas will be covered:

- How to connect and configure the Advisor.
- General VoIP monitoring techniques.
- A brief tour of the Advisor's Decode view and how to recognize VoIP traffic in it.
- An example of how to verify/troubleshoot H.323 signaling messages.
- An example of how to measure signaling performance.

Connecting/Configuring the Advisor

Figure 4 shows the various points within a VoIP network to which the Advisor can be connected in order to monitor conversations between H.323 entities. For the examples shown in this Product Application Note, we assume an Ethernet or Fast Ethernet connection. Note where this topology is located in the larger architecture shown in Figure 1. The Advisor can also monitor conversations between H.323 compliant telephones and H.323 multimedia PC's. Connecting to a Gateway port ensures that all messages between that Gateway, the Gatekeeper, and the remote Gateway can be monitored and captured. If you connect the Advisor to the Gatekeeper only, the Gatekeeper/Gateway exchanges will be captured. Connecting to a network hub lets you monitor VoIP traffic as well as other IP traffic not related to VoIP.

As shown in Figure 4, troubleshooting VoIP networks occurs on the "IP side" of the connection inside a given Gatekeeper zone. Troubleshooting voice traffic on non-H.323 networks is beyond the scope if this document.

There are essentially two ways to connect the Advisor to the network as shown in Figure 4:

- Connect as a Node - you can connect the Advisor LAN to an Ethernet hub or switch so that the Advisor will see all of the network traffic occurring on that network segment. You will likely see non-H.323 traffic interspersed amongst the H.323 traffic in which you are interested. You can use the Advisor's Display Filter to focus on just the VoIP traffic you care about. Display Filtering is covered in more detail in the Advisor's on-line Help and in a later section of this Note.

- Connect Between Network Devices (in a 'through' mode) - you can also connect the Advisor between network devices so that the traffic is passed through. This can result in less extraneous (non-H.323) traffic in the Advisor's Decode view if one of the devices is an H.323 terminal (e.g. an IP/ Ethernet telephone or H.323-enabled PC).

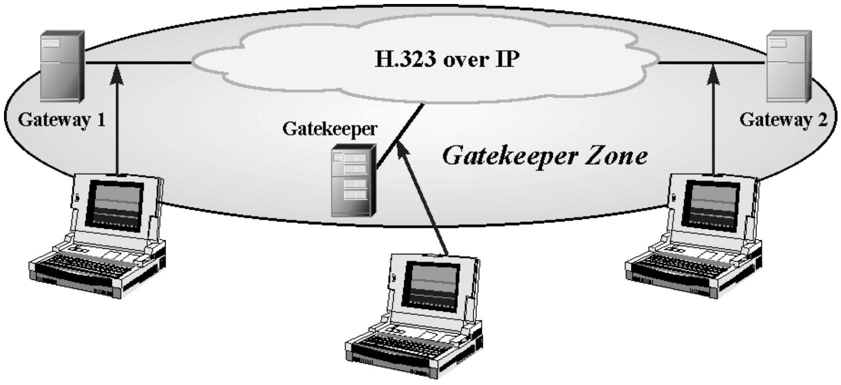


Figure 4.

Remember, these are Ethernet or Fast Ethernet connections. Once you are connected to the network, you will likely need to set or verify the physical interface configuration in the LAN application's Interface/Protocols folder. The Advisor LAN on-line Help provides detailed connection diagrams and configuration information.

Note: if you are using the Advisor WAN or ATM products, look in the on-line Help for connection diagrams and configuration information corresponding to the WAN or ATM interface to which you need to connect. In either one of these applications, you will be monitoring and capturing IP traffic encapsulated in WAN frames (such as frame relay) or segmented into ATM cells.

Basic VoIP/H.323 Monitoring

The most basic VoIP analysis tasks involve simple monitoring to measure things like voice call packets per second, voice call utilization, and packet counts for call setup and disconnect. Typically, these are the kinds of measurements you would perform on an already functioning network. To do this kind of network analysis effectively, you can set up capture filters based on the IP addresses associated with H.323 devices causing the Advisor to capture and gather statistics on incoming VoIP traffic. To learn more about the Advisor LAN's statistical measurement capabilities and about its powerful capture filters, please see the on-line Help or User's Guide.

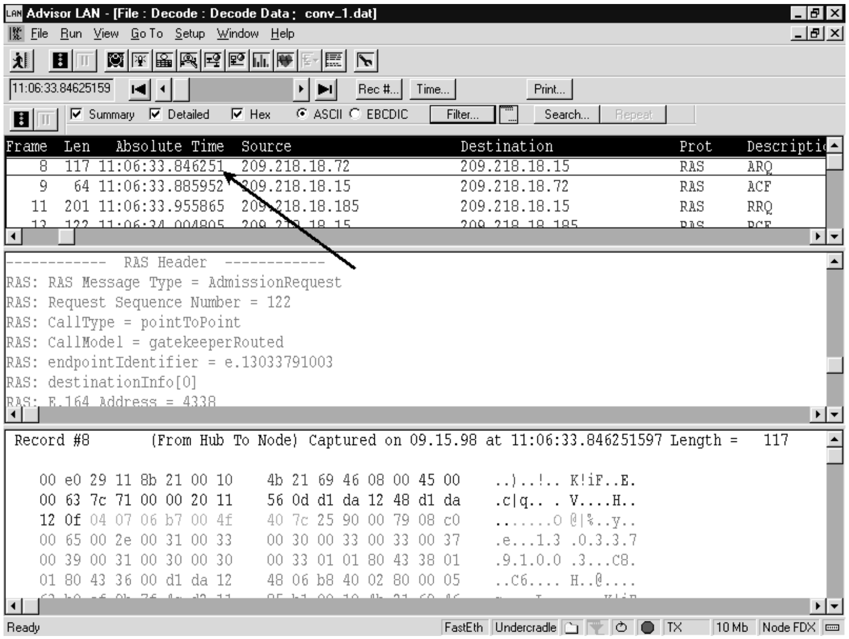
Examining VoIP/H.323 Packets in the Decode View

This section shows you how to use the Advisor's decode capability and how to recognize decoded H.323 packets in the Advisor's Decode measurement view. If you are familiar with the Advisor's operation and how to recognize an H.323 packet in the Decode view, you can go on to the next section.

Figure 5 shows the Advisor LAN's Decode view containing an example of H.323 traffic. The Advisor's Decode view is the main tool used to troubleshoot VoIP signaling because with it you can observe call setup/control messages and the audio packets sent between H.323 entities. While in the Decode view, you can press F1 to display on-line Help directly related to decoding network traffic. Figure 5 shows:

- Decoded traffic shown in Summary, Detail, and Hexadecimal formats.. For H.323 signaling troubleshooting, the Summary and Detail portions of the view are the most useful. You can close the Hex portion by removing the corresponding check mark at the top of the display.
- In the Summary portion of the view, you can see the higher layer protocols used for VoIP signaling. This is a display option that you can evoke by using the right mouse click menu (demonstrated later).
- The Detail portion of the view shows a complete decode of each incoming packets and frames. In this example, you can see the beginnings of the decoded VoIP RAS (H.225) protocol. You can scroll to see the lower layers of the stack, but for most H.323 troubleshooting, the signaling protocols are what you need to focus on.
- IP addresses, port numbers, sequence numbers, and other parameters found in the decoded frames are very important in verifying correct operation and diagnosing problems.
- The Filter button opens the Display Filter Properties dialog box so you can cause the Advisor to display the desired H.323 traffic. In this way, you can focus on upper layer H.323 packets.

Depending on your testing needs and methods, you can examine decoded VoIP in real-time as it is captured, or you can examine it closely frame-by-frame after it has been captured.


Advisor LAN - [File : Decode : Decode Data ; conv_1.dat]
File Run View Go To Setup Window Help
11:06:33.84625159
Rec #...
Time...
Print...
☑ Summary ☑ Detailed ☑ Hex ● ASCII ○ EBCDIC
Filter...
Search...
Repeat
Ready
FastEth
Undercradle
TX
10 Mb
Node FDX

```
Frame  Len   Absolute Time  Source                      Destination                 Prot    Descripti
    8  117 11:06:33.846251  209.218.18.72               209.218.18.15               RAS     ARQ
    9   64 11:06:33.885952  209.218.18.15               209.218.18.72               RAS     ACF
   11  201 11:06:33.955865  209.218.18.185              209.218.18.15               RAS     RRQ
   13  122 11:06:34.004805  209.218.18.15               209.218.18.185              RAS     RCF
```

```
------------  RAS Header  ------------
RAS: RAS Message Type = AdmissionRequest
RAS: Request Sequence Number = 122
RAS: CallType = pointToPoint
RAS: CallModel = gatekeeperRouted
RAS: endpointIdentifier = e.13033791003
RAS: destinationInfo[0]
RAS: E.164 Address = 4338
```

```
 Record #8       (From Hub To Node) Captured on 09.15.98 at 11:06:33.846251597 Length =   117

    00 e0 29 11 8b 21 00 10    4b 21 69 46 08 00 45 00    ..)..!.. K!iF..E.
    00 63 7c 71 00 00 20 11    56 0d d1 da 12 48 d1 da    .c|q.. . V....H..
    12 0f 04 07 06 b7 00 4f    40 7c 25 90 00 79 08 c0    .......O @|%..y..
    00 65 00 2e 00 31 00 33    00 30 00 33 00 33 00 37    .e...1.3 .0.3.3.7
    00 39 00 31 00 30 00 30    00 33 01 01 80 43 38 01    .9.1.0.0 .3...C8.
    01 80 43 36 00 d1 da 12    48 06 b8 40 02 80 00 05    ..C6.... H..@....
```

Figure 5.

Verifying/Troubleshooting H.323 Signaling

Voice conversations over today's packet switched telephone networks require signaling to establish, maintain, and disconnect calls. However, IP does not inherently provide this type of signaling. To enable voice conversations over IP networks, H.323 specifies a relatively complex process. This section shows you how to verify and troubleshoot H.323 call setup signaling.

General Troubleshooting Process

To verify or troubleshoot VoIP signaling, you will usually perform the following general steps:

1. Connect the Advisor to the network such that you can monitor the conversation between H.323 entities. You will also need to make sure the Advisor's physical interface configuration matches the
conditions at the connection point. Connecting and configuring the Advisor is covered in a previous section.

2. Start monitoring the network by clicking the Start tool bar button in the Advisor's tool bar. Go to the Advisor's Decode view and monitor each H.323 exchange to verify correct operation or to see when and/or where the process fails.

The following general tips help with signaling troubleshooting and analysis:

- Use Display Filters - because H.323 traffic is almost always mixed with other types of traffic, you will often want to set up a Display Filter so that you see only the traffic of interest. At first, you will have to look closely at the decoded data to determine which IP addresses are associated with the VoIP traffic. Once you know this, you can set up a Display Filter using those addresses as parameters. You can also set up a Display Filter for the protocols that carry VoIP traffic - for example, TCP and UDP. Another method is to filter on messages that are destined for, or originate from, the IP address of the gateway port to which the Advisor is connected.

- Use Capture Filters - if you are familiar with the VoIP network under test, you may already know which IP addresses are the sources and destinations of VoIP traffic. In this case, you can set up Capture Filters to limit the kinds of traffic the Advisor allows into its buffer. This makes data capture more efficient by only allowing relevant data into valuable buffer space, and makes it easier to collect VoIP-only statistics.

- Along with IP addresses, troubleshooting H.323 signaling almost always revolves around noting the port numbers used for various protocol exchanges and using these numbers to correlate related messages.

- Use the Search Capability - if you need to see a very specific frame or packet, you can set up a decode Search that will target specific information in captured decoded traffic.

- Use Diagnostic Information Provided by the H.323 Protocols - H.323 signaling provides some troubleshooting information in the form of 'reject cause' or 'reject reason' fields in various Reject messages that occur when requests for discovery, registration, and routed call setups fail. In the vast majority of cases, the Advisor decodes these reject causes and displays them in the Detailed portion of the Decode view.

Message Exchange Example

To illustrate the process of verifying or troubleshooting H.323 signaling, we will look at the 'Gatekeeper Routed Call Signaling' portion of the process shown in Figure 2 earlier in this Note. Typically, this is the part of the signaling process that is initiated when a caller takes the telephone 'off the hook' and dials a number. The individual messages exchanged are shown in Figures 6 and 7. Routed Call Signaling is a good example because both H.225 RAS and Q.931 Setup processes - that is, ARQ, ACF, Setup, Call Proceeding, Alerting, and Connect messages - can be shown and discussed. Remember, this example shows only one part of the H.323 signaling process. The following techniques can be altered and applied to other parts of the signaling process as needed.

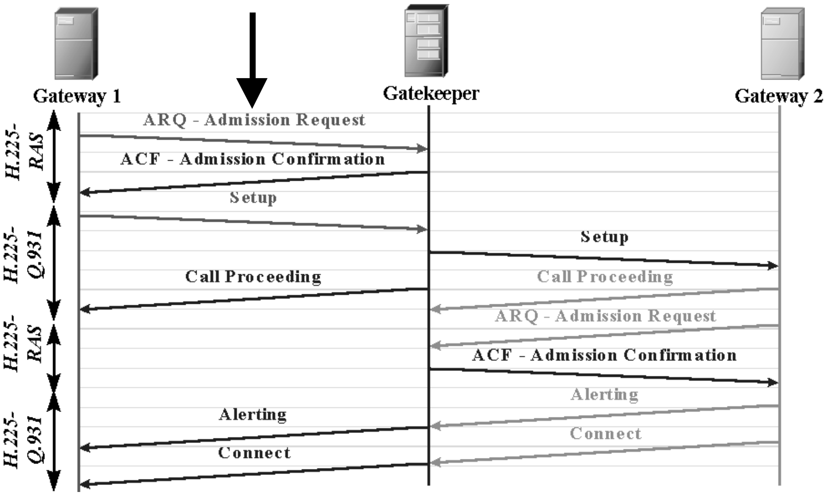


Figure 6.

Figure 6 shows the Gatekeeper Routed Call Signaling process used to establish a call between Gateway 1 and Gateway 2. This process uses the H.225 RAS and Q.931 protocols and sends all messages through the Gatekeeper. For our purposes, we will focus only on the exchange between Gateway 1 and the Gatekeeper because the exchange between the Gatekeeper and Gateway 2 is essentially the same and the test procedure shown here can be similarly applied. Depending on how you are connected, you may or may not be able to capture the Gatekeeper/Gateway 2 conversation.

Figure 7 shows the Gateway 1/Gatekeeper part of the conversation with the IP addresses, message types, and UDP/TCP port numbers added. We will refer to this figure throughout the remaining part of this example and will show how the addresses, message types and port numbers are derived.

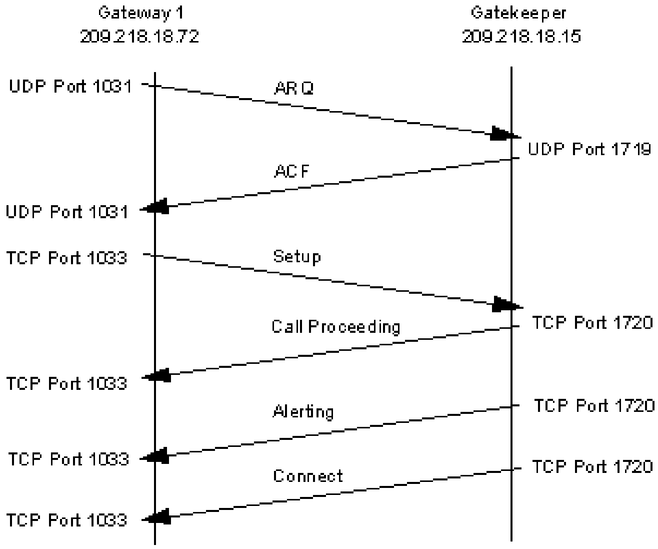


Figure 7.

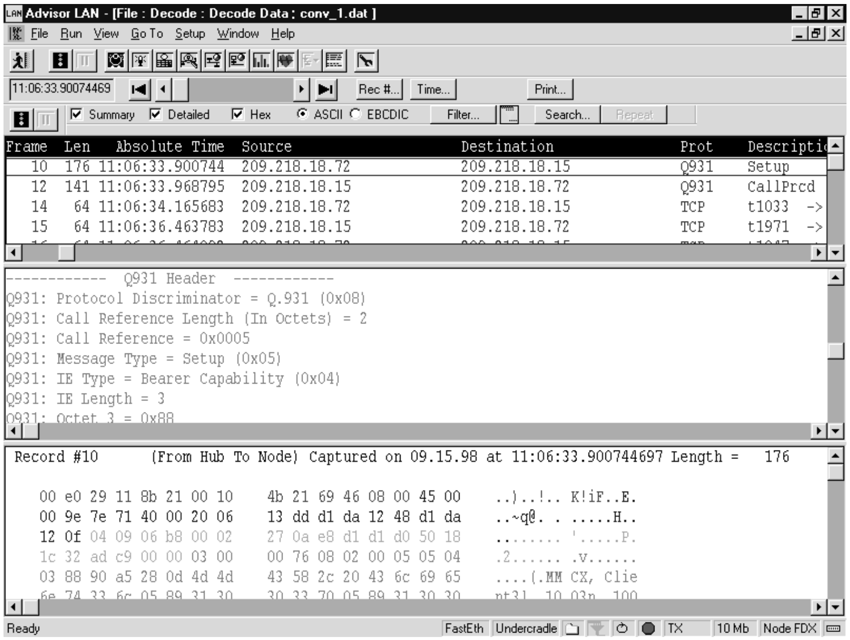
H.225 RAS ARQ (Admission Request) and ACF (Admission Confirmation) Messages

The first messages sent during the Routed Call Signaling process are the RAS Admission Request (ARQ) and Admission Confirmation (ACF) messages. These messages ensure that existing bandwidth and registration conditions will allow a call to be made. Figure 8 shows the ARQ sent from Gateway 1 to the Gatekeeper and the ACF sent from the Gatekeeper to Gateway 1 in the Summary portion of the Decode view.

To easily find the H.225 RAS ARQ and ACF messages in post-process decoded traffic (as shown in Figure 8), position the mouse pointer in the Summary portion of the Decode view, click the right mouse button, and select the 'Top' display option as shown in Figure 9. This causes the protocol and message type at the top of the protocol stack to be shown.

Once you have found the ARQ message, highlight it. Note the Source IP address - 209.218.18.72 in this case. Since we know the Gateway initiates Routed Call Signaling, we can assume that this is the address of Gateway 1. Also note the Destination IP address - 209.218.18.15 . If this is indeed a Gatekeeper Routed Call Signaling process, then this IP address is the Gatekeeper (we will verify this shortly). You will use these addresses (as well as additional decoded data) to identify other messages sent between the Gatekeeper and Gateway 1. Now would also be the time use these addresses to set up two Station Filters using the Advisor's Display Filter capability so that most of the traffic you see is originating either from Gateway 1 or the Gatekeeper. It's a good idea to do this early in the troubleshooting process to simplify subsequent analysis. You set up display filters by clicking the Filter button in the Decode view opening the Display Filter Properties dialog box. Press F1 while in this dialog box for on-line Help related to the subject.

With the ARQ message highlighted in the Summary part of the view, scroll through the data displayed in the Detailed part of the view to find the UDP and RAS Headers associated with it.


Advisor LAN - [File : Decode : Decode Data : conv_1.dat]
File Run View Go To Setup Window Help
11:06:33.90074469
Rec #...
Time...
Print...
☑ Summary ☑ Detailed ☑ Hex ● ASCII ○ EBCDIC
Filter...
Search...
Repeat
Ready
FastEth
Undercradle
TX
10 Mb
Node FDX

```
Frame  Len   Absolute Time  Source                   Destination              Prot    Descripti
   10  176 11:06:33.900744  209.218.18.72            209.218.18.15            Q931    Setup
   12  141 11:06:33.968795  209.218.18.15            209.218.18.72            Q931    CallPrcd
   14   64 11:06:34.165683  209.218.18.72            209.218.18.15            TCP     t1033  ->
   15   64 11:06:36.463783  209.218.18.15            209.218.18.72            TCP     t1971  ->
```

```
-----------  Q931 Header  -----------
Q931: Protocol Discriminator = Q.931 (0x08)
Q931: Call Reference Length (In Octets) = 2
Q931: Call Reference = 0x0005
Q931: Message Type = Setup (0x05)
Q931: IE Type = Bearer Capability (0x04)
Q931: IE Length = 3
Q931: Octet 3 = 0x88
```

```
 Record #10      (From Hub To Node) Captured on 09.15.98 at 11:06:33.900744697 Length =   176

    00 e0 29 11 8b 21 00 10    4b 21 69 46 08 00 45 00    ..)..!.. K!iF..E.
    00 9e 7e 71 40 00 20 06    13 dd d1 da 12 48 d1 da    ..~q@. . .....H..
    12 0f 04 09 06 b8 00 02    27 0a e8 d1 d1 d0 50 18    ........ '.....P.
    1c 32 ad c9 00 00 03 00    00 76 08 02 00 05 05 04    .2...... .v......
    03 88 90 a5 28 0d 4d 4d    43 58 2c 20 43 6c 69 65    ....(.MM CX, Clie
    6e 74 33 6c 05 89 31 30    30 33 70 05 89 31 30 30    nt3l..10 03p..100
```

Figure 8

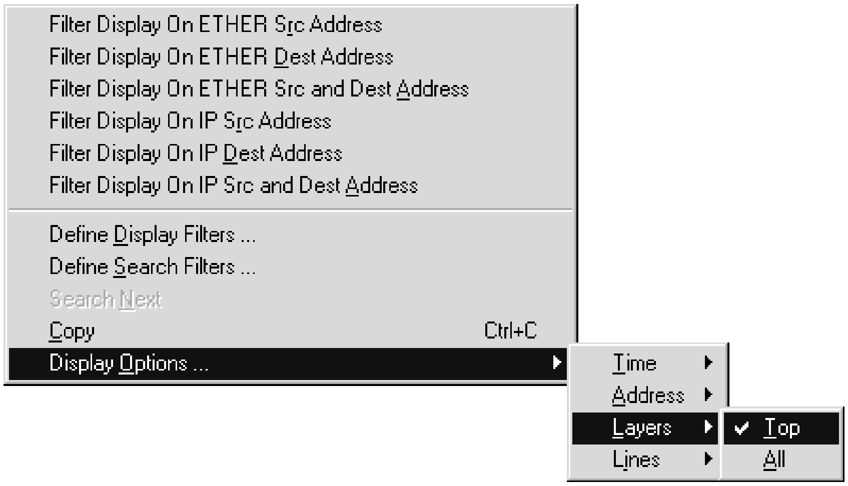

Filter Display On ETHER Src Address
Filter Display On ETHER Dest Address
Filter Display On ETHER Src and Dest Address
Filter Display On IP Src Address
Filter Display On IP Dest Address
Filter Display On IP Src and Dest Address
Define Display Filters ...
Define Search Filters ...
Search Next
Copy
Ctrl+C
Display Options ...
Time
Address
Layers
Lines
✓ Top
All

Figure 9

Figures 10 and 11 show the UDP header and details of the H.225 RAS Admission Request message respectively with important data shown in bold text (the text will **not** be bold in the Advisor's display). The bold items are:

- UDP Source and Destination ports - in this case, 1031 and 1719 respectively. You will use this information to identify the corresponding Admission Confirmation message later.
- RAS Message Type - Admission Request.
- Request Sequence Number - you will use this to ensure the Admission Confirmation message you later identify is the correct one.
- Call Reference Value - this value is assigned at the beginning of each call. You will use this to identify the correct Q.931 messages.

What could go wrong at this point? If you do not see an Admission Request (ARQ) message, you can assume one of two probable causes: (1) either something went wrong earlier in the signaling process - for example, a failed Gateway/Terminal registration - or (2) a call has not been placed. The Gateway could also have some internal software or hardware malfunction. However, if the Gateway has been successfully registered with the Gatekeeper, it is rare that an ARQ is not sent when a call is being initiated.

```
———————   UDP  Header   ———————
UDP: Source port = 1031
UDP: Destination port = 1719
UDP:  Length  =  79
UDP:  Checksum  =  407C
```

Figure 10.

```
———————   RAS  Header   ———————
RAS: RAS Message Type = AdmissionRequest
RAS: |   Request Sequence Number = 122
RAS: |       CallType  =  pointToPoint
RAS: |   CallModel = gatekeeperRouted
RAS: |   endpointIdentifier = e.13033791003
RAS: |     destinationInfo[0]
RAS: |    |     E.164  Address  =  4338
RAS: |     srcInfo[0]
RAS: |    |     E.164  Address  =  4336
RAS: |     srcCallSignalAddress
RAS: |    |     ipAddress
RAS: |    |     ip  =  209.218.18.72
RAS: |    |     port  =  1720
RAS: |     Bandwidth  (in  100s  of  bits)  =  641
RAS: |   CallReferenceValue = 6
RAS: |     Conference  Identifier  =  63B0EF9B7F4CD21185B100104B216946
RAS: |     activeMC  =  0  (FALSE)
RAS: |     answerCall  =  0  (FALSE)
```

Figure 11.

The next step is to find and examine the RAS Admission Confirmation (ACF) message sent from the Gatekeeper to Gateway 1 in response to the ARQ message. Using the information we already have - the IP address of the Gatekeeper and the UDP source and destination port numbers - you should be able to scroll further through the captured decoded traffic until you see the RAS ACF message (IP source address - 209.218.18.15 and UDP source address 1719). Again, look in the Detailed part of the view to see the decoded UDP and RAS frames associated with this message (Figures 12 and 13).

Figure 12 shows the details of the UDP header associated with the ACF message. You can see that the UDP source and destination port numbers are reversed as expected; the ACF message originates from the Gatekeeper this time. Figure 13 shows the decoded ACF message. The following important information is highlighted in bold in both figures:

- UDP source and destination port numbers.
- RAS message type is shown as Admission Confirm.
- Request Sequence Number - confirms that this ACF is associated with the ARQ message shown on the previous page.
- Destination Call Signaling Address - used to identify the corresponding Q.931 Setup message.

What could go wrong at this point? The Gatekeeper sends an a Admission Reject (ARJ) message instead of the Admission Confirmation (ACF) message shown in Figure 13. This would be shown as 'RAS ARJ' in the Summary part of the Decode view sent from the IP address and UDP source port number associated with the Gatekeeper (in our example, 209.218.18.15 and 1719 respectively). If this were to happen, you would need to scroll through the decoded RAS ARJ message to find the Reject Reason field which will give you more information as to why the ARQ message was rejected. Reasons can include:

- The called party is not registered with this 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 Endpoint Identifier is invalid.

```
———————   UDP  Header   ———————
UDP: Source port = 1719
UDP: Destination port = 1031
UDP:  Length  =  22
UDP:  Checksum  =  599A
```

Figure 12.

```
———————   RAS  Header   ———————
RAS: RAS Message Type = AdmissionConfirm
RAS: |    Request Sequence Number = 122
RAS: |    Bandwidth (in 100s  of  bits)  =  641
              ipAddress
RAS: |    CallModel  =  gatekeeperRouted
RAS: |    destCallSignalAddress
RAS: |    |
RAS: |    |   ip = 209.218.18.15
RAS: |    |   port = 1720
```

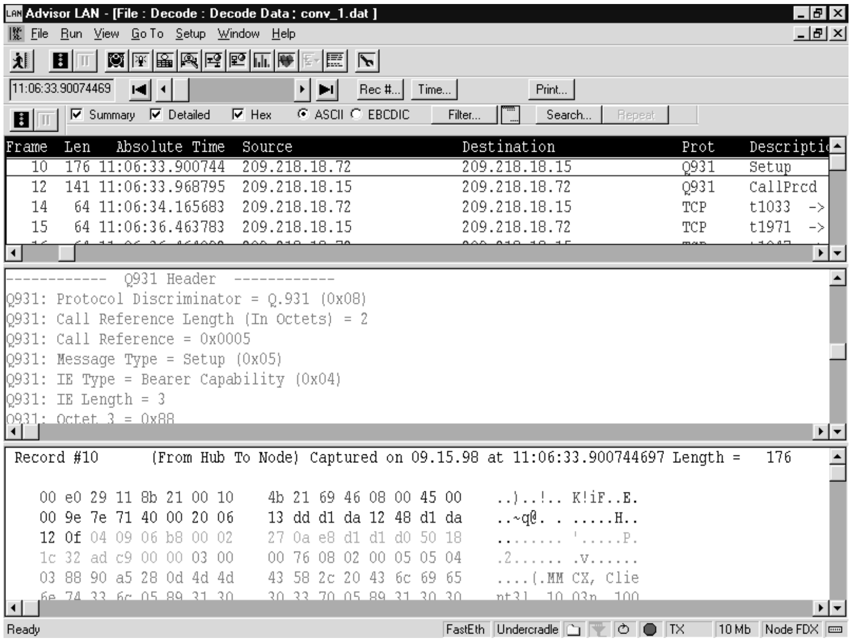
Figure 13.

Q.931 (H.225) Setup and Call Proceeding Messages

The next events in the Routed Call Signaling process are the Q.931 Setup and Call Proceeding messages, again between Gateway 1 and the Gatekeeper. These messages are sent to actually initiate the call. Figure 14 shows the Setup and Call Proceeding messages in the Summary part of the Advisor's Decode view. You can reasonably assume that this Setup message is the one associated with the ARQ and ACF messages because the Destination IP address is the same as that identified in the Destination Call Signaling Address shown in Figure 13. We will confirm this assumption in a moment. Notice that in this example there appears to be a frame missing between these messages (frame 11). This is because a Display Filter has been set up to filter out traffic not originating from Gateway 1 (209.218.18.72) or from the Gatekeeper (201.218.18.15).

Details of the TCP header and Q.931 Setup message are shown in Figures 15 and 16 respectively. Important parts of the decode are highlighted in bold:

- TCP source and destination port numbers (extracted from the previous ACF message) - used to confirm that this is the correct Setup message and to identify corresponding Alerting and Connect messages later on.
- Call Reference Value - since this is the same as the value shown in the ARQ message, we know that this Setup message is indeed the correct one.
- Q.931 Message Type is shown as 'Setup'.
- RAS Transport Addresses - identifies the IP address and TCP port from which subsequent H.245 messages will be sent.


Advisor LAN - [File : Decode : Decode Data : conv_1.dat]
File Run View Go To Setup Window Help
11:06:33.90074469
Rec #...
Time...
Print...
☑ Summary ☑ Detailed ☑ Hex ● ASCII ○ EBCDIC
Filter...
Search...
Repeat
Ready
FastEth
Undercradle
TX
10 Mb
Node FDX

```
Frame  Len   Absolute Time  Source                    Destination               Prot    Descripti
   10  176 11:06:33.900744  209.218.18.72             209.218.18.15             Q931    Setup
   12  141 11:06:33.968795  209.218.18.15             209.218.18.72             Q931    CallPrcd
   14   64 11:06:34.165683  209.218.18.72             209.218.18.15             TCP     t1033  ->
   15   64 11:06:36.463783  209.218.18.15             209.218.18.72             TCP     t1971  ->
```

```
------------  Q931 Header  ------------
Q931: Protocol Discriminator = Q.931 (0x08)
Q931: Call Reference Length (In Octets) = 2
Q931: Call Reference = 0x0005
Q931: Message Type = Setup (0x05)
Q931: IE Type = Bearer Capability (0x04)
Q931: IE Length = 3
Q931: Octet 3 = 0x88
```

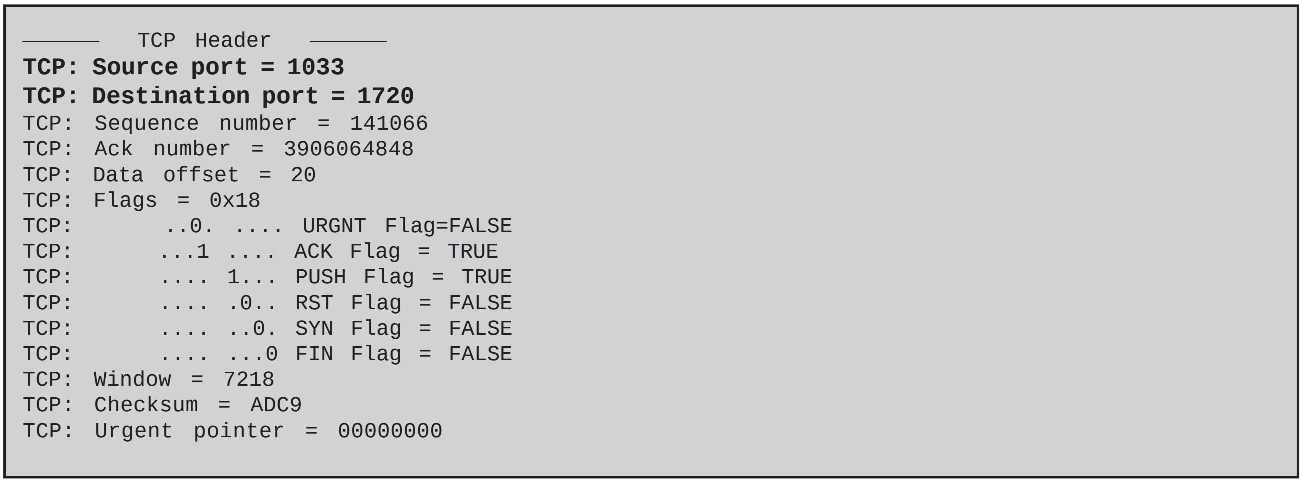
```
 Record #10      (From Hub To Node) Captured on 09.15.98 at 11:06:33.900744697 Length =   176

    00 e0 29 11 8b 21 00 10    4b 21 69 46 08 00 45 00    ..)..!.. K!iF..E.
    00 9e 7e 71 40 00 20 06    13 dd d1 da 12 48 d1 da    ..~q@. . .....H..
    12 0f 04 09 06 b8 00 02    27 0a e8 d1 d1 d0 50 18    ........ '.....P.
    1c 32 ad c9 00 00 03 00    00 76 08 02 00 05 05 04    .2...... .v......
    03 88 90 a5 28 0d 4d 4d    43 58 2c 20 43 6c 69 65    ....(.MM CX, Clie
    6e 74 33 6c 05 89 31 30    30 33 70 05 89 31 30 30    nt3l..10 03p..100
```

Figure 14.

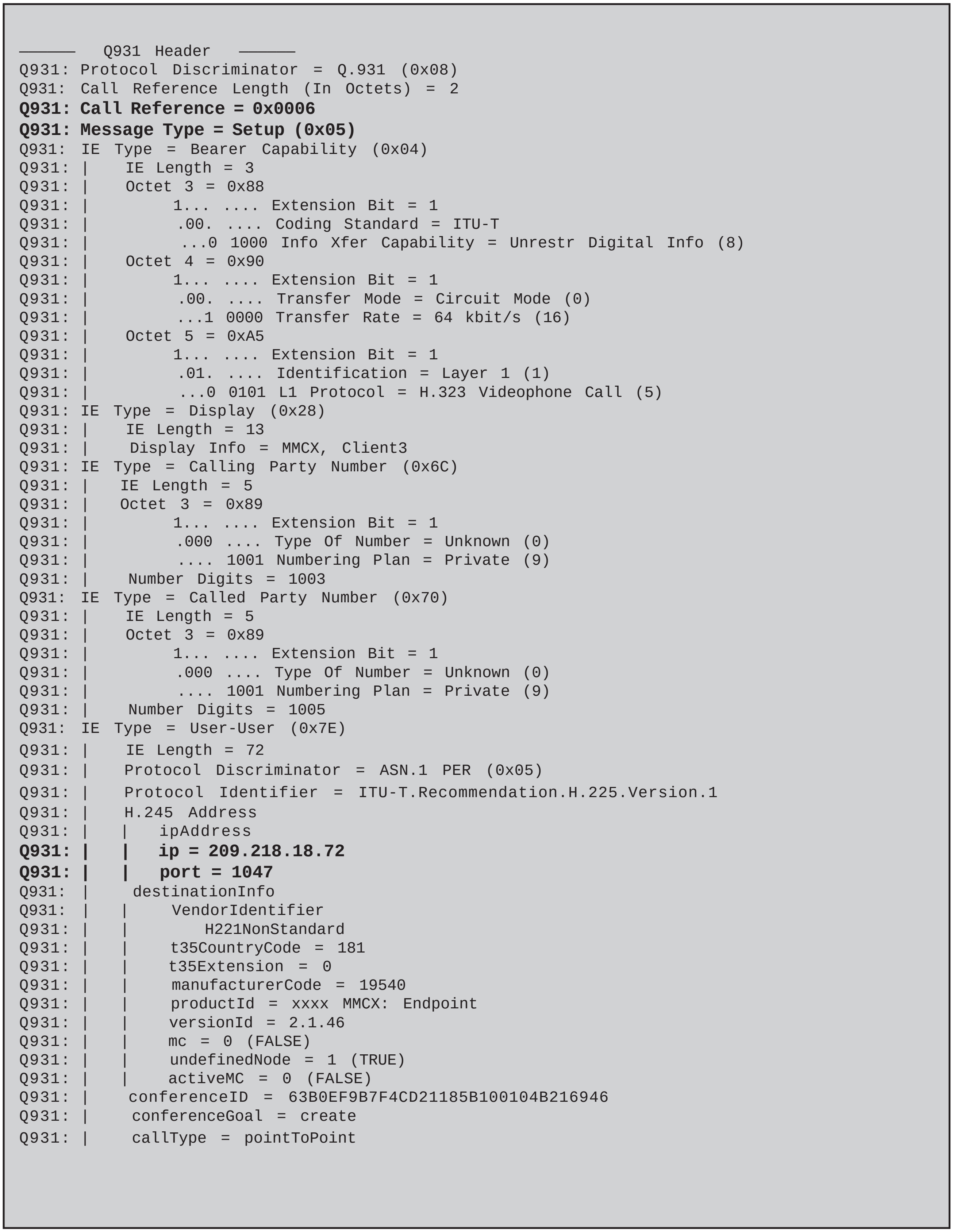
After the Setup message has been sent by the Gateway, a Call Proceeding message is sent back in response from the Gatekeeper. This message is shown decoded in Figures 17 and 18 with important data highlighted:

- TCP Source and Destination port numbers corresponding to the preceding Setup message.
- Call Reference value - matches the value found in the Admission Request and Setup messages.



```
———— TCP Header ————
TCP: Source port = 1033
TCP: Destination port = 1720
TCP: Sequence number = 141066
TCP: Ack number = 3906064848
TCP: Data offset = 20
TCP: Flags = 0x18
TCP:      ..0. .... URGNT Flag=FALSE
TCP:      ...1 .... ACK Flag = TRUE
TCP:      .... 1... PUSH Flag = TRUE
TCP:      .... .0.. RST Flag = FALSE
TCP:      .... ..0. SYN Flag = FALSE
TCP:      .... ...0 FIN Flag = FALSE
TCP: Window = 7218
TCP: Checksum = ADC9
TCP: Urgent pointer = 00000000
```

Figure 15.



```
——————   Q931 Header   ——————
Q931: Protocol Discriminator = Q.931 (0x08)
Q931: Call Reference Length (In Octets) = 2
Q931: Call Reference = 0x0006
Q931: Message Type = Setup (0x05)
Q931: IE Type = Bearer Capability (0x04)
Q931: |    IE Length = 3
Q931: |    Octet 3 = 0x88
Q931: |         1... .... Extension Bit = 1
Q931: |         .00. .... Coding Standard = ITU-T
Q931: |         ...0 1000 Info Xfer Capability = Unrestr Digital Info (8)
Q931: |    Octet 4 = 0x90
Q931: |         1... .... Extension Bit = 1
Q931: |         .00. .... Transfer Mode = Circuit Mode (0)
Q931: |         ...1 0000 Transfer Rate = 64 kbit/s (16)
Q931: |    Octet 5 = 0xA5
Q931: |         1... .... Extension Bit = 1
Q931: |         .01. .... Identification = Layer 1 (1)
Q931: |         ...0 0101 L1 Protocol = H.323 Videophone Call (5)
Q931: IE Type = Display (0x28)
Q931: |    IE Length = 13
Q931: |    Display Info = MMCX, Client3
Q931: IE Type = Calling Party Number (0x6C)
Q931: |    IE Length = 5
Q931: |    Octet 3 = 0x89
Q931: |         1... .... Extension Bit = 1
Q931: |         .000 .... Type Of Number = Unknown (0)
Q931: |         .... 1001 Numbering Plan = Private (9)
Q931: |    Number Digits = 1003
Q931: IE Type = Called Party Number (0x70)
Q931: |    IE Length = 5
Q931: |    Octet 3 = 0x89
Q931: |         1... .... Extension Bit = 1
Q931: |         .000 .... Type Of Number = Unknown (0)
Q931: |         .... 1001 Numbering Plan = Private (9)
Q931: |    Number Digits = 1005
Q931: IE Type = User-User (0x7E)
Q931: |    IE Length = 72
Q931: |    Protocol Discriminator = ASN.1 PER (0x05)
Q931: |    Protocol Identifier = ITU-T.Recommendation.H.225.Version.1
Q931: |    H.245 Address
Q931: |    |   ipAddress
Q931: |    |   ip = 209.218.18.72
Q931: |    |   port = 1047
Q931: |    destinationInfo
Q931: |    |    VendorIdentifier
Q931: |    |        H221NonStandard
Q931: |    |    t35CountryCode = 181
Q931: |    |    t35Extension = 0
Q931: |    |    manufacturerCode = 19540
Q931: |    |    productId = xxxx MMCX: Endpoint
Q931: |    |    versionId = 2.1.46
Q931: |    |    mc = 0 (FALSE)
Q931: |    |    undefinedNode = 1 (TRUE)
Q931: |    |    activeMC = 0 (FALSE)
Q931: |    conferenceID = 63B0EF9B7F4CD21185B100104B216946
Q931: |    conferenceGoal = create
Q931: |    callType = pointToPoint
```

Figure 16.

```
———————   TCP  Header   ———————
TCP: Source port = 1720
TCP: Destination port = 1033
TCP:  Sequence  number  =  3906064848
TCP:  Ack  number  =  141184
TCP:  Data  offset  =  20
TCP:  Flags  =  0x18
TCP:  ..0.  ....  URGENT  Flag  =  FALSE
TCP:  ...1  ....  ACK  Flag  =  TRUE
TCP:  ....  1...  PUSH  Flag  =  TRUE
TCP:  ....  .0..  RST  Flag  =  FALSE
TCP:  ....  ..0.  SYN  Flag  =  FALSE
TCP:  ....  ...0  FIN  Flag  =  FALSE
TCP:  Window  =  16384
TCP:  Checksum  =  0CBF
TCP:  Urgent  pointer  =  00000000
```

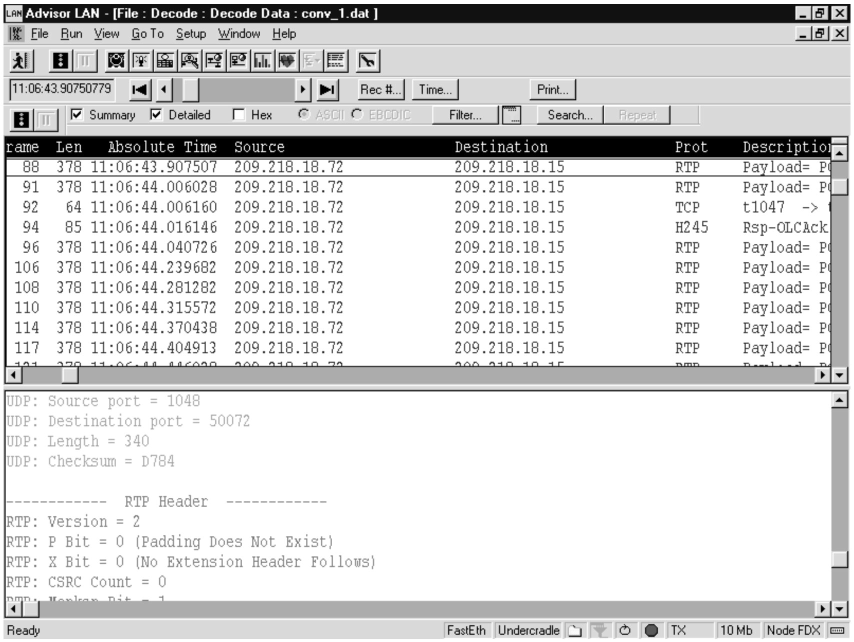
Figure 17.

```
———————   Q931  Header   ———————
Q931:  Protocol  Discriminator  =  Q.931  (0x08)
Q931:  Call  Reference  Length  (In  Octets)  =  2
Q931: Call Reference = 0x0006
Q931: Message Type = Call Proceeding (0x02)
Q931:  IE  Type  =  Bearer  Capability  (0x04)
Q931: |    IE  Length  =  3
Q931: |    Octet  3  =  0x88
Q931: |         1...  ....  Extension  Bit  =  1
Q931: |         .00.  ....  Coding  Standard  =  ITU-T
Q931: |         ...0  1000  Info  Xfer  Capability  =  Unrestr  Digital  Info  (8)
Q931: |    Octet  4  =  0x90
Q931: |         1...  ....  Extension  Bit  =  1
Q931: |         .00.  ....  Transfer  Mode  =  Circuit  Mode  (0)
Q931: |         ...1  0000  Transfer  Rate  =  64  kbit/s  (16)
Q931: |    Octet  5  =  0xA5
Q931: |         1...  ....  Extension  Bit  =  1
Q931: |         .01.  ....  Identification  =  Layer  1  (1)
Q931: |         ...0  0101  L1  Protocol  =  H.323  Videophone  Call  (5)
Q931: IE  Type  =  Display  (0x28)
Q931: |    IE  Length  =  13
Q931: |    Display  Info  =  MMCX,  Client3
Q931: IE  Type  =  User-User  (0x7E)
Q931: |    IE  Length  =  48
Q931: |    Protocol  Discriminator  =  ASN.1  PER  (0x05)
Q931: |    Protocol  Identifier  =  ITU-T.Recommendation.H.225.Version.1
Q931: |    destinationInfo
Q931: |    |    VendorIdentifier
Q931: |    |    H221NonStandard
Q931: |    |    t35CountryCode  =  181
Q931: |    |    t35Extension  =  0
Q931: |    |    manufacturerCode  =  19540
Q931: |    |    productId  =  xxxx  MMCX:  Endpoint
Q931: |    |    versionId  =  2.1.46
Q931: |    |    mc  =  0  (FALSE)
Q931: |    |    undefinedNode  =  1  (TRUE)
```

Figure 18.

What could go wrong here? Q.931 Call Proceeding messages are optional in H.323 signaling, so for some implementations this message may not be sent. This does not necessarily indicate a problem in the network. In some cases, however, the Call Proceeding message prevents the Gateway from timing out while it waits for the Q.931 Alerting message. If this is the case, not getting a Call Proceeding message could cause the signaling process to fail. Another possible problem is when a Release Complete message is sent instead of the Call Proceeding message. Release Complete messages contain a Release Complete Reason field which indicates the cause of the release. Reasons might include:

- Bandwidth withdrawn or Admission Request denied.
- Network resources exhausted.
- No transport path to the called destination.
- Called party, called Gateway, or called Gatekeeper rejected the call.
- Called Gateway is unable to perform ARQ/ACF exchange.



```
rame  Len   Absolute Time  Source                      Destination                 Prot     Descriptio
  88  378 11:06:43.907507  209.218.18.72               209.218.18.15               RTP      Payload= P
  91  378 11:06:44.006028  209.218.18.72               209.218.18.15               RTP      Payload= P
  92   64 11:06:44.006160  209.218.18.72               209.218.18.15               TCP      t1047  ->
  94   85 11:06:44.016146  209.218.18.72               209.218.18.15               H245     Rsp-OLCAck
  96  378 11:06:44.040726  209.218.18.72               209.218.18.15               RTP      Payload= P
 106  378 11:06:44.239682  209.218.18.72               209.218.18.15               RTP      Payload= P
 108  378 11:06:44.281282  209.218.18.72               209.218.18.15               RTP      Payload= P
 110  378 11:06:44.315572  209.218.18.72               209.218.18.15               RTP      Payload= P
 114  378 11:06:44.370438  209.218.18.72               209.218.18.15               RTP      Payload= P
 117  378 11:06:44.404913  209.218.18.72               209.218.18.15               RTP      Payload= P
```

```
UDP: Source port = 1048
UDP: Destination port = 50072
UDP: Length = 340
UDP: Checksum = D784

------------  RTP Header  ------------
RTP: Version = 2
RTP: P Bit = 0 (Padding Does Not Exist)
RTP: X Bit = 0 (No Extension Header Follows)
RTP: CSRC Count = 0
```

Figure 19.

Q.931 (H.225) Alerting and Connect Messages

The final events in the Routed Call Setup process are the Q.931 Alerting and Connect messages both transmitted from the Gatekeeper to Gateway 1. The Alerting message indicates that the called party's "telephone" is ringing, and the Connect message indicates that the connection has been successfully established (several other signaling steps will be performed before audio transmission begins - see Figure 3). Figure 19 shows the Alerting and Connect messages in the Summary Decode view. As in previous sections, the first step to verifying that these are the messages associated with our original ARQ and ACF messages is to note the source IP address - 209.218.18.15, which we know to be the Gatekeeper. You can then verify that you have found the correct messages by looking at the detailed decode.

Note: in the figure, a number of frames seem to be missing between these two messages - again an example of display filters removing unwanted data from the screen. You can change the characteristics of the display filters to see these frames if desired Figures 20 and 21 show the decoded TCP header and Q.931 Alerting message with the important information highlighted:

- TCP source and destination port numbers - 1720 and 1033 - more evidence that this is indeed the correct Alerting message.
- Call Reference value - this confirms that this is the correct Alerting message.

What could go wrong here? One potential problem is if the Alerting message is not received by the Gateway. The H.225 recommendation states in one chapter that this message is required and in another that it is optional. Consequently, some equipment vendors may not include this in their signaling processes. Depending on individual implementations, not receiving an Alerting messages could cause the Gateway to time-out as it waits for the Connect message, thus resulting in a terminated connection.

Figures 22 and 23 show the decoded Q.931 Connect message. Again, we have highlighted important parts of this decode with bold text:

- TCP source and destination ports which should be the same as those in the Alerting message.
- Call Reference value which is the same value that has been maintained throughout the establishment of this call.
- Q.931 message type: Connect message as expected.

What could go wrong here? Simply stated, if the called party does not answer the call, a Connect message will not be sent. Instead, a Release Complete message will be sent which contains a Release Complete Reason field.

Troubleshooting Other Parts of the Signaling Process

Remember, the process we have just described can be applied to the H.225 Gatekeeper Discovery and Terminal Registration, the H.245 Communications and Capability Exchange, and the H.245 Open Logical Channel parts of VoIP signaling. Please see the Troubleshooting H.323 Signaling white paper on the Advisor Web site for more information.

```
——————  TCP Header  ——————
TCP: Source port = 1720
TCP: Destination port = 1033
TCP: Sequence number = 3906064931
TCP: Ack number = 141184
TCP: Data offset = 20
TCP: Flags = 0x18
TCP:       ..0. .... URGENT Flag = FALSE
TCP:       ...1 .... ACK Flag = TRUE
TCP:       .... 1... PUSH Flag = TRUE
TCP:       .... .0.. RST Flag = FALSE
TCP:       .... ..0. SYN Flag = FALSE
TCP:       .... ...0 FIN Flag = FALSE
TCP: Window = 16384
TCP: Checksum = 945D
TCP: Urgent pointer = 00000000
```

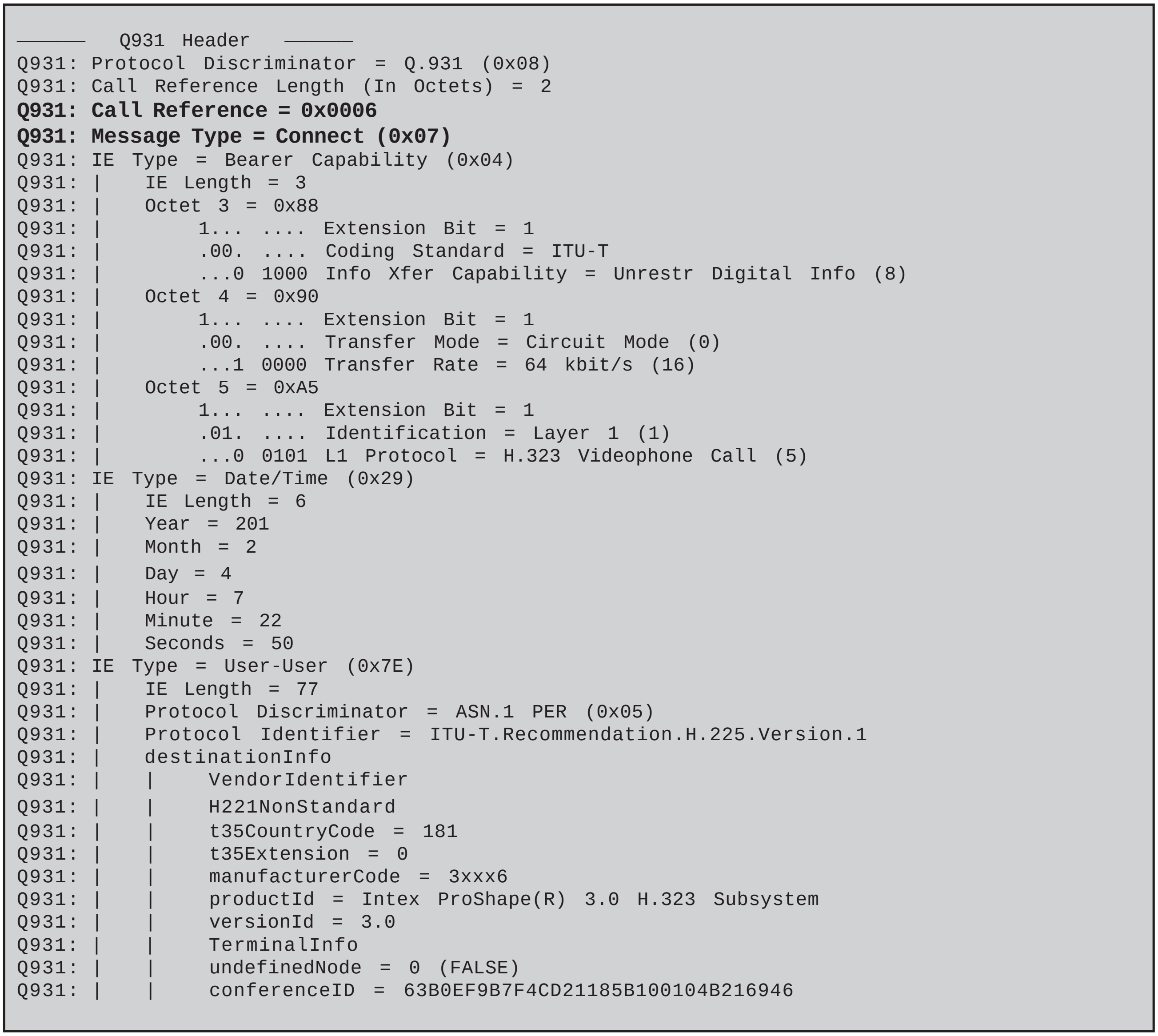
Figure 20.

```
——————  Q931 Header  ——————
Q931: Protocol Discriminator = Q.931 (0x08)
Q931: Call Reference Length (In Octets) = 2
Q931: Call Reference = 0x0006
Q931: Message Type = Alerting (0x01)
Q931: IE Type = Bearer Capability (0x04)
Q931: |   IE Length = 3
Q931: |   Octet 3 = 0x88
Q931: |        1... .... Extension Bit = 1
Q931: |        .00. .... Coding Standard = ITU-T
Q931: |        ...0 1000 Info Xfer Capblty = Unr Digt Info(8)
Q931: |   Octet 4 = 0x90
Q931: |        1... .... Extension Bit = 1
Q931: |        .00. .... Transfer Mode = Circuit Mode (0)
Q931: |        ...1 0000 Transfer Rate = 64 kbit/s (16)
Q931: |   Octet 5 = 0xA5
Q931: |        1... .... Extension Bit = 1
Q931: |        .01. .... Identification = Layer 1 (1)
Q931: |        ...0 0101 L1 Protcl = H.323 Vidphone Call (5)
Q931: IE Type = Display (0x28)
Q931: |   IE Length = 12
Q931: |   Display Info = MMCX Client5
Q931: IE Type = User-User (0x7E)
Q931: |   IE Length = 12
Q931: |   Protocol Discriminator = ASN.1 PER (0x05)
Q931: |   Protocol ID = ITU-T.Recommendation.H.225.Ver.1
Q931: |   destinationInfo
Q931: |   |    TerminalInfo
Q931: |   |    mc = 0 (FALSE)
Q931: |   |    undefinedNode = 0 (FALSE)
```

Figure 21.

```
——————  TCP Header  ——————
TCP: Source port = 1720
TCP: Destination port = 1033
TCP: Sequence number = 3906064974
TCP: Ack number = 141184
TCP: Data offset = 20
TCP: Flags = 0x18
TCP:       ..0. .... URGENT Flag = FALSE
TCP:       ...1 .... ACK Flag = TRUE
TCP:       .... 1... PUSH Flag = TRUE
TCP:       .... .0.. RST Flag = FALSE
TCP:       .... ..0. SYN Flag = FALSE
TCP:       .... ...0 FIN Flag = FALSE
TCP: Window = 16384
TCP: Checksum = 448A
TCP: Urgent pointer = 00000000
```

Figure 22.



```
——————   Q931 Header   ——————
Q931: Protocol Discriminator = Q.931 (0x08)
Q931: Call Reference Length (In Octets) = 2
Q931: Call Reference = 0x0006
Q931: Message Type = Connect (0x07)
Q931: IE Type = Bearer Capability (0x04)
Q931: |   IE Length = 3
Q931: |   Octet 3 = 0x88
Q931: |       1... .... Extension Bit = 1
Q931: |       .00. .... Coding Standard = ITU-T
Q931: |       ...0 1000 Info Xfer Capability = Unrestr Digital Info (8)
Q931: |   Octet 4 = 0x90
Q931: |       1... .... Extension Bit = 1
Q931: |       .00. .... Transfer Mode = Circuit Mode (0)
Q931: |       ...1 0000 Transfer Rate = 64 kbit/s (16)
Q931: |   Octet 5 = 0xA5
Q931: |       1... .... Extension Bit = 1
Q931: |       .01. .... Identification = Layer 1 (1)
Q931: |       ...0 0101 L1 Protocol = H.323 Videophone Call (5)
Q931: IE Type = Date/Time (0x29)
Q931: |   IE Length = 6
Q931: |   Year = 201
Q931: |   Month = 2
Q931: |   Day = 4
Q931: |   Hour = 7
Q931: |   Minute = 22
Q931: |   Seconds = 50
Q931: IE Type = User-User (0x7E)
Q931: |   IE Length = 77
Q931: |   Protocol Discriminator = ASN.1 PER (0x05)
Q931: |   Protocol Identifier = ITU-T.Recommendation.H.225.Version.1
Q931: |   destinationInfo
Q931: |   |    VendorIdentifier
Q931: |   |    H221NonStandard
Q931: |   |    t35CountryCode = 181
Q931: |   |    t35Extension = 0
Q931: |   |    manufacturerCode = 3xxx6
Q931: |   |    productId = Intex ProShape(R) 3.0 H.323 Subsystem
Q931: |   |    versionId = 3.0
Q931: |   |    TerminalInfo
Q931: |   |    undefinedNode = 0 (FALSE)
Q931: |   |    conferenceID = 63B0EF9B7F4CD21185B100104B216946
```

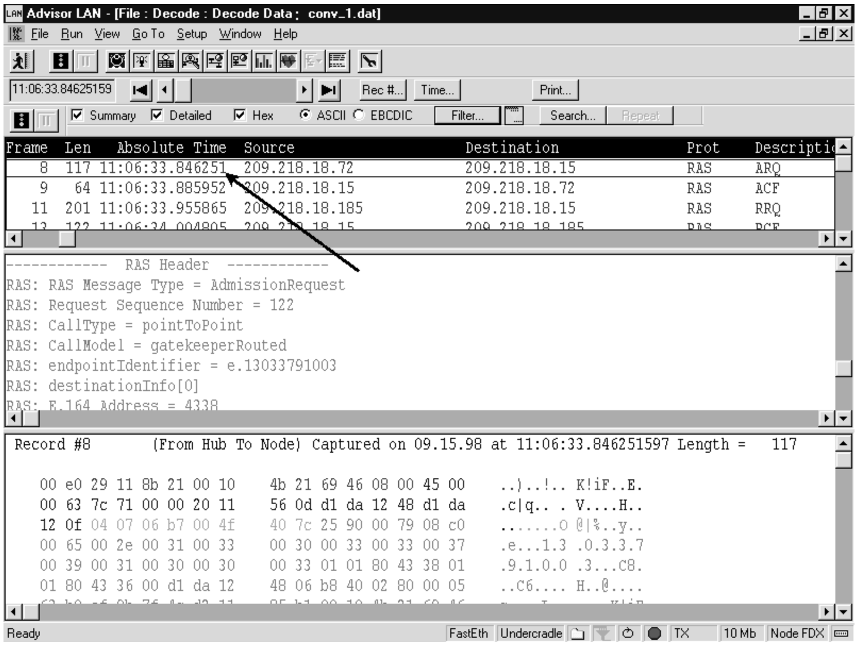
Figure 23.

Verifying/Troubleshooting H.323 Signaling Performance

Like other networking protocols and technologies, VoIP performance must be kept within certain ranges to ensure that communication services can be provided at expected and acceptable levels. For H.323 VoIP networks, there are two areas of performance that interest network engineers:

- Signaling Performance - influences the length of time needed to setup a call between H.323 terminals.
- RTP Performance - influences the delay and overall clarity of the voice signal during a VoIP conversation.

Since this Product Application Note is concerned primarily with H.323 signaling, this section shows how to use the Advisor's H.323 decodes to evaluate signaling performance only. RTP performance and VoIP quality of service are the subjects of another application note and can be tested by another of Agilent's Advisor applications. Please contact your Agilent representative for more information.


Advisor LAN - [File : Decode : Decode Data ; conv_1.dat]
File Run View Go To Setup Window Help
11:06:33.84625159
Rec #...
Time...
Print...
☑ Summary ☑ Detailed ☑ Hex ● ASCII ○ EBCDIC
Filter...
Search...
Repeat
Ready
FastEth
Undercradle
TX
10 Mb
Node FDX

```
Frame  Len   Absolute Time  Source                     Destination            Prot   Descripti
    8  117 11:06:33.846251  209.218.18.72              209.218.18.15          RAS    ARQ
    9   64 11:06:33.885952  209.218.18.15              209.218.18.72          RAS    ACF
   11  201 11:06:33.955865  209.218.18.185             209.218.18.15          RAS    RRQ
   13  122 11:06:34.004805  209.218.18.15              209.218.18.185         RAS    RCF
```

```
------------  RAS Header  ------------
RAS: RAS Message Type = AdmissionRequest
RAS: Request Sequence Number = 122
RAS: CallType = pointToPoint
RAS: CallModel = gatekeeperRouted
RAS: endpointIdentifier = e.13033791003
RAS: destinationInfo[0]
RAS: E.164 Address = 4338
```

```
 Record #8       (From Hub To Node) Captured on 09.15.98 at 11:06:33.846251597 Length =   117

   00 e0 29 11 8b 21 00 10    4b 21 69 46 08 00 45 00    ..)..!.. K!iF..E.
   00 63 7c 71 00 00 20 11    56 0d d1 da 12 48 d1 da    .c|q.. . V....H..
   12 0f 04 07 06 b7 00 4f    40 7c 25 90 00 79 08 c0    .......O @|%..y..
   00 65 00 2e 00 31 00 33    00 30 00 33 00 33 00 37    .e...1.3 .0.3.3.7
   00 39 00 31 00 30 00 30    00 33 01 01 80 43 38 01    .9.1.0.0 .3...C8.
   01 80 43 36 00 d1 da 12    48 06 b8 40 02 80 00 05    ..C6.... H..@....
```

Figure 24.

Measuring Signaling Performance

To evaluate signaling performance, we measure the time needed to establish a connection. There are a number of conditions that can have an adverse affect on the connection setup time. These include:

- Number of network nodes between H.323 endpoints.
- Signaling load at the Gatekeeper or Gateway.
- Processing performance of the Gatekeeper, Gateway, or terminal.
- Overall network traffic load and its affect on packet delay and packet loss.

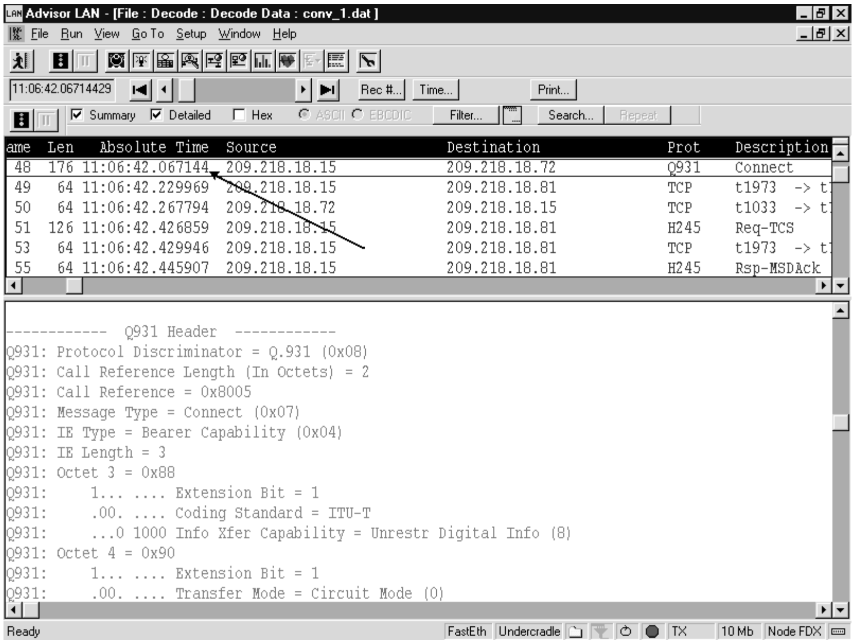
We can use the Advisor's decode capability to isolate signaling performance problems associated with the above conditions by measuring the time it takes network devices to respond to request messages or other network events. The total connection setup time then is the summation of these individual measurements. To illustrate this, we will measure the time required for the completion of the Routed Call Signaling example originally shown in Figure 7.

Recall that the Routed Call Signaling process begins with the H.225 RAS Admission Request (ARQ) message sent from the Gateway to the Gatekeeper, and is completed when the Q.931 Connect message is sent from the Gatekeeper to the Gateway. The easiest way to measure the elapsed time is to use the timestamps assigned to the ARQ and Connect messages when the Advisor captured and decoded them. Figure 24 shows the absolute time of the ARQ message (Frame 8) to be 11:06:33.846251. Figure 25 shows the absolute time of the Connect message (Frame 48) to be 11:06:42.067144. Subtracting the first time stamp from the second, we can see that the Routed Call Signaling exchange between Gateway 1 and the Gatekeeper took nearly 10 seconds (8.220893 seconds). Points of interest:

- Because what we measured is the Routed Call Signaling process, this represents roughly the elapsed time from the point when the destination number is dialed to the point when the called party "answers" the call. Depending upon the user's expectations, this may or may not be considered unacceptable performance.

- This measurement also includes the time elapsed for the Gatekeeper/Gateway 2 exchange; that is, the Connect message is not sent until Gateway 2 sends it through the Gatekeeper. You could find out exactly which message pair took the longest by measuring the Gatekeeper/Gateway 2 exchange and comparing it to the Gatekeeper/Gateway 1 measurement.

- Remember that Routed Call Signaling is only one part of overall signaling process. The times measured here do not include Gatekeeper Discovery and Terminal Registration, Initial Communications and Capability Exchange, and may or may not include the latencies introduced by PSTN/PBX operations.



11:06:42.06714429

☑ Summary ☑ Detailed □ Hex

```
ame  Len   Absolute Time  Source                Destination          Prot    Description
 48  176 11:06:42.067144  209.218.18.15         209.218.18.72        Q931    Connect
 49   64 11:06:42.229969  209.218.18.15         209.218.18.81        TCP     t1973  -> t
 50   64 11:06:42.267794  209.218.18.72         209.218.18.15        TCP     t1033  -> t
 51  126 11:06:42.426859  209.218.18.15         209.218.18.81        H245    Req-TCS
 53   64 11:06:42.429946  209.218.18.15         209.218.18.81        TCP     t1973  -> t
 55   64 11:06:42.445907  209.218.18.15         209.218.18.81        H245    Rsp-MSDAck
```

```
------------  Q931 Header  ------------
Q931: Protocol Discriminator = Q.931 (0x08)
Q931: Call Reference Length (In Octets) = 2
Q931: Call Reference = 0x8005
Q931: Message Type = Connect (0x07)
Q931: IE Type = Bearer Capability (0x04)
Q931: IE Length = 3
Q931: Octet 3 = 0x88
Q931:     1... .... Extension Bit = 1
Q931:     .00. .... Coding Standard = ITU-T
Q931:     ...0 1000 Info Xfer Capability = Unrestr Digital Info (8)
Q931: Octet 4 = 0x90
Q931:     1... .... Extension Bit = 1
Q931:     .00. .... Transfer Mode = Circuit Mode (0)
```

Figure 25.

Contact us with FaxBack

By Returning This FaxBack Page, with the following required information, you can facilitate your initial contact to speak with a Customer Care Representative

Fax to: 1-303-662-2038

OR...

E-mail to: csp_telesales@agilent.com

Visit our web site

www.agilent.com/comms/onenetworks

First Name ____________________
Last Name ____________________
Company Name ____________________
Job Title ____________________

Business Mailing Address ____________________
____

City ____________________
State/Province ____________________
Country ____________________
Zip Code ____________________

E-Mail Address ____________________
____

Phone Number ____________________
(incl. area/country code)

Fax Number ____________________

Do you have a budget set for this application?

□ Yes
□ No
□ In process

What is your time frame to implement this product?

□ 30 days
□ 90 days
□ 180 days
□ Other – (please define) ____________________
____
____

Product(s) of Interest

□ ***The Agilent Advisor*** – Integrated, High-Performance Troubleshooting for:

____ Advisor LAN
____ Advisor WAN
____ Advisor ATM

□ ***The LAN Analyzer*** – Scaleable Ethernet and Token Ring Test Solutions
□ ***Telegra Fax Test*** – Fax Protocol and Low Generation Analysis
□ ***Telegra Voice Quality Tester*** – Detailed Voice Analysis for Clarity, Echo and Delay using PSQM and PAMS
□ ***Telegra Voice and Fax over IP*** – Protocol Analysis
□ ***FASTest*** – Automated Service Verification for PSTN and IP Networks

What is the main problem you need to solve on your network?

____
____
____

Agilent Technologies
Innovating the HP Way

Notes

Notes

Notes

Connect with us!

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

This Product is Y2K Compliant

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) 206 4120

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

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

Latin America:
(Tel) (305) 269 7500
(Fax) (305) 269 7599

Australia:
(Tel) 1-800 629 485
(Fax) (61 3) 9272 0749

New Zealand:
(Tel) 0 800 738 378
(Fax) (64 4) 495 8950

Asia Pacific:
(Tel) (852) 3197 7777
(Fax) (852) 2506 9284

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

Printed in U.S.A. 10/00

Agilent Technologies
Innovating the HP Way