Audia-Nexia Reading a Wireshark trace of a Biamp VoIP device

This article will describe the process of reading a packet capture of communications between a Biamp VoIP device and the VoIP network. A program called Wireshark is a free, open-source packet analyzer that is used for network troubleshooting and analysis.

If a Biamp VoIP device is placed on a VoIP Network, but not registering with the Proxy Server, calls fail or some other issue is being reported determining the point of failure can be difficult using the Biamp software alone. The registration process may be hindered by something beyond the VoIP device itself. Possible causes can include communications issues over the network or issues with the configuration of the Proxy Server. If this is the case, Wireshark can be used to help locate the point of failure.

This article explains how to analyze the Wireshark trace. Analyzing these traces may seem daunting at first however this article aims to simplify the process.

Note that this is a follow up resource to the How to perform a Wireshark trace of a Biamp VoIP device article which covers the procedure for actually obtaining a packet capture.

Basics of VoIP communication

As part of troubleshooting a Wireshark trace it is important to understand the devices and protocols VoIP uses.

The Proxy, sometimes referred to as the Call Manager, Session Manager or VoIP server, is the device responsible for setting up and negotiating the call handling process. This includes registration, authentication and implementing the rules and parameters to establish and route the calls to their correct destinations.

Biamp VoIP devices communicate this call handling information to the Proxy using the Session Initiation Protocol (SIP). SIP is the most commonly used signaling protocol by VoIP devices and vendors today. The protocol is responsible for the establishment, control and termination of VoIP sessions. It does this by the devices exchanging three types of messages – requests, and then responses to those requests, as well as various information and call progress ‘update’ type messages.

Once the SIP protocol has negotiated the connection and a call is initiated, the Real-Time Transport Protocol (RTP) is responsible for packaging the audible voice and any control data (such as DTMF tones) and transporting them across the network.

An endpoint is defined as any VoIP device able to accept incoming or make outgoing VoIP calls. These include Biamp...
VoIP products, a VoIP desk phone, VoIP software (softphone) and other 3rd party manufactures VoIP devices, of which there are many.

Verifying the correct data was captured

To confirm the correct data has been captured, the use of the Wireshark filter field is required. By entering the word ‘sip’ (in lowercase), the SIP negotiation sequence between the Biamp VoIP device and the Proxy can be seen. Note that if no SIP messages are shown, the Wireshark capture has not been performed correctly and will need to be retaken using the correct settings. If necessary, revisit How to perform a Wireshark trace of a Biamp VoIP device to obtain a valid capture file.

A successful SIP negotiation

The capture below shows a Biamp VoIP device at IP Address 10.21.12.73 registering two of its lines to a Proxy at IP Address 10.21.12.20. Within this capture, we can see the sequence of successfully connecting to the Proxy, negotiating the media settings, placing a call, and then terminating the call.

A breakdown of the negotiation process is as follows:

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Biamp VoIP device tries to register Line 1 (ext 520) with the Proxy using anonymous credentials</td>
</tr>
<tr>
<td>2</td>
<td>The Biamp VoIP device tries to register Line 2 (ext 530) with the Proxy using anonymous credentials</td>
</tr>
<tr>
<td>3</td>
<td>Line 1 Registration Denied - The Proxy requests additional data (i.e. Username, Password &amp; other information)</td>
</tr>
<tr>
<td>4</td>
<td>Line 2 Registration Denied - The Proxy requests additional data (i.e. Username, Password &amp; other information)</td>
</tr>
</tbody>
</table>
5 Biamp VoIP device tries to register Line 1 with the Proxy and includes the extra authentication details this time
6 Biamp VoIP device tries to register Line 2 with the Proxy and includes the extra authentication details this time
7 The Proxy reports it has successfully registered Line 1
8 The Proxy reports it has successfully registered Line 2
9 The Biamp VoIP device extension ‘530’ dials and places a call to extension ‘580’
10 The Proxy is configured to rechallenge the Biamp VoIP device for authentication details whenever a call is placed
11 The Biamp VoIP device acknowledges it has been challenged by the Proxy for this extra information
12 The Biamp VoIP device provides the Proxy with the extra information
13 The extra information passes validation and the Proxy indicates that it is trying to call extension ‘580’
14 The Proxy reports to the Biamp VoIP device that at this point the far end is ringing
15 The Proxy reports to the Biamp VoIP device that the far end has answered the call
16 The Biamp VoIP Device confirms with the Proxy that the settings required to begin the call are valid and the call begins
17 Some time later, the Proxy tells the Biamp VoIP device that extension ‘580’ has hung up or disconnected the call
18 The Biamp VoIP device acknowledges the disconnect and gives an indication that its line is ready to make and receive calls once again

As part of the negotiation process some Proxies may report additional or other messages in the Information column. These extra messages listed below can be expected and do not indicate an error. Some examples of common messages that are not shown in the example trace above may include the following;

**Status: 100 Trying**  (0 bindings)
A response from the Proxy or device acknowledging it’s attempt to process the SIP message provided.

**Status: 100 Giving a try**
A response from the Proxy or device acknowledging it’s attempt to process the SIP message provided.

**Request: NOTIFY sip: 101 @ 172.17.203.63:54910;transport=udp**
NOTIFY is a method that a VoIP device can use to relay a change of active state to other devices in a network. This particular notification (transport=udp) means that the SIP end point (at the far end) is using UDP mode for its
transmission of audio and signaling messages. It relays this information to the Proxy using a NOTIFY message. The transport message type could indicate “transport=tcp” as well - this is normal. Another example where a NOTIFY message may be used is if a Gateway device needs to inform an endpoint that the audio CODEC needs to be changed mid-call.

**Status: 183 Session Progress, with session description**
An indication that the call is progressing to an active state. The parameters of the call defined in the Register message would be used to establish this call and a RTP stream may be started.

**Request: OPTIONS sip: 101 @ 192.168.22.202:5060;transport=udp**
Allows one device to query another device about its capabilities. This query can happen regardless of whether or not a call is in place.

**Request: INFO sip: 101 @ 192.168.1.100:5060**
A method that allows the use of the SIP Protocol to deliver information between devices without changing the state of a call. A common use case for SIP INFO is to deliver DTMF in a SIP Packet.

## Error messages

Other messages may indicate a potential issue, especially if you are finding calls cannot be completed or are misbehaving. Different Proxies may word their error messages differently however the overall the message, the error identification number or the message meaning may be similar.

## Additional information

This article is by no means a comprehensive list of all possible issues that can be experienced when implementing a VoIP solution. It is intended to only cover the most commonly seen problems, so if the suggestions in this article do not help or you are seeing an error that is not listed, please email the trace and a description of the issue to support@biamp.com for analysis. The more detail that can be provided, the faster the issue may be resolved.