Troubleshoot Jabber SIP Call Issues with Wireshark

Contents

Introduction

This document describes how to troubleshoot Jabber SIP calls issues with Wireshark.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SIP signaling
- Jabber call flows
- Wireshark and basic knowledge of packet filtering

Components Used

- Jabber for Windows 15.0.2
- CUCM 15su2
- Wireshark 4.4.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

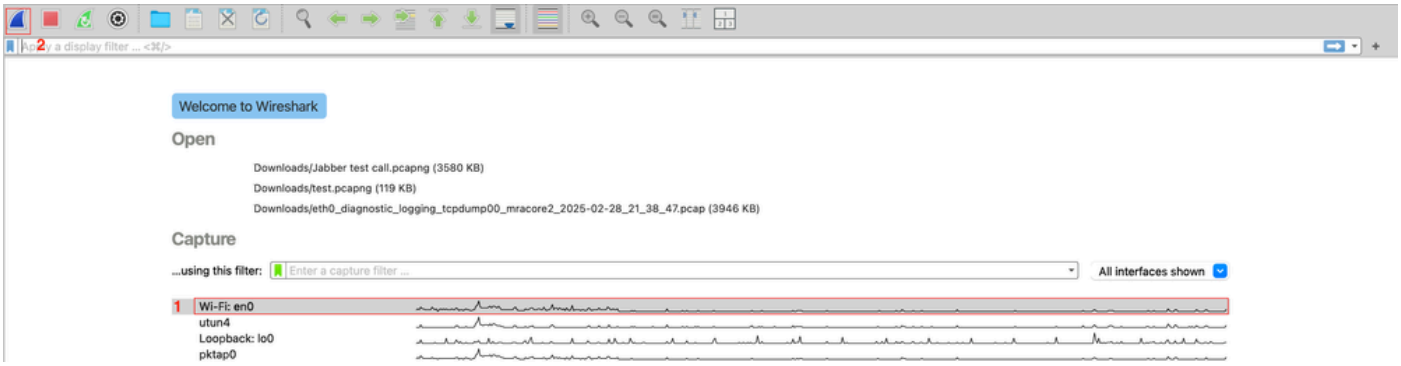
Session Initiation Protocol (SIP) is the standard protocol for signaling in VoIP communications. SIP manages call setup, modification, and teardown. When calls fail to establish, the problem often lies in SIP signaling. Cisco Jabber uses SIP for signaling when making voice or video calls. Wireshark allows engineers to capture and analyze SIP messages, identify errors, and pinpoint the cause of call setup failures.

Troubleshoot

1. Identify and isolate the affected call flow, this is an important step as this determines the network devices involved on the issue. For this document purposes, use as a reference a point-to-point call between 2 Jabber clients registered to CUCM, however, this basic troubleshoot applies to multiple scenarios.

2. Open Wireshark.

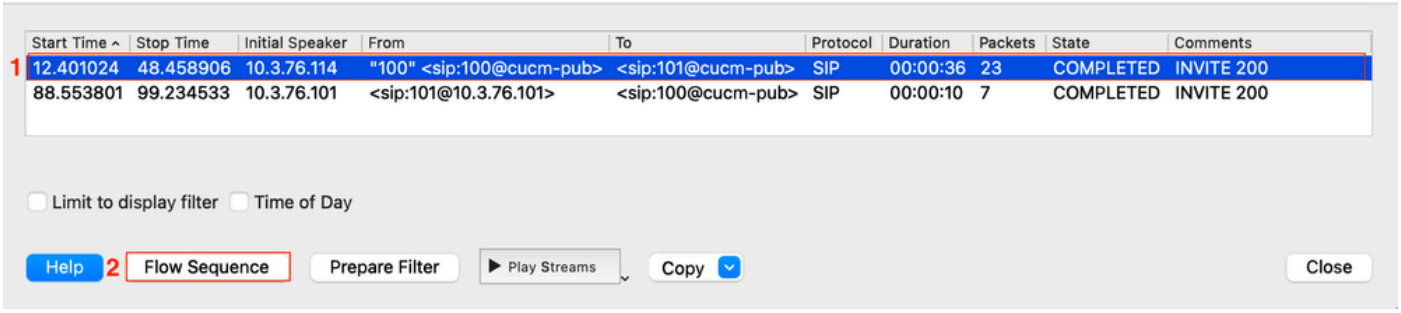
3. Select the correct network interface and start Wireshark packet captures on the affected device.



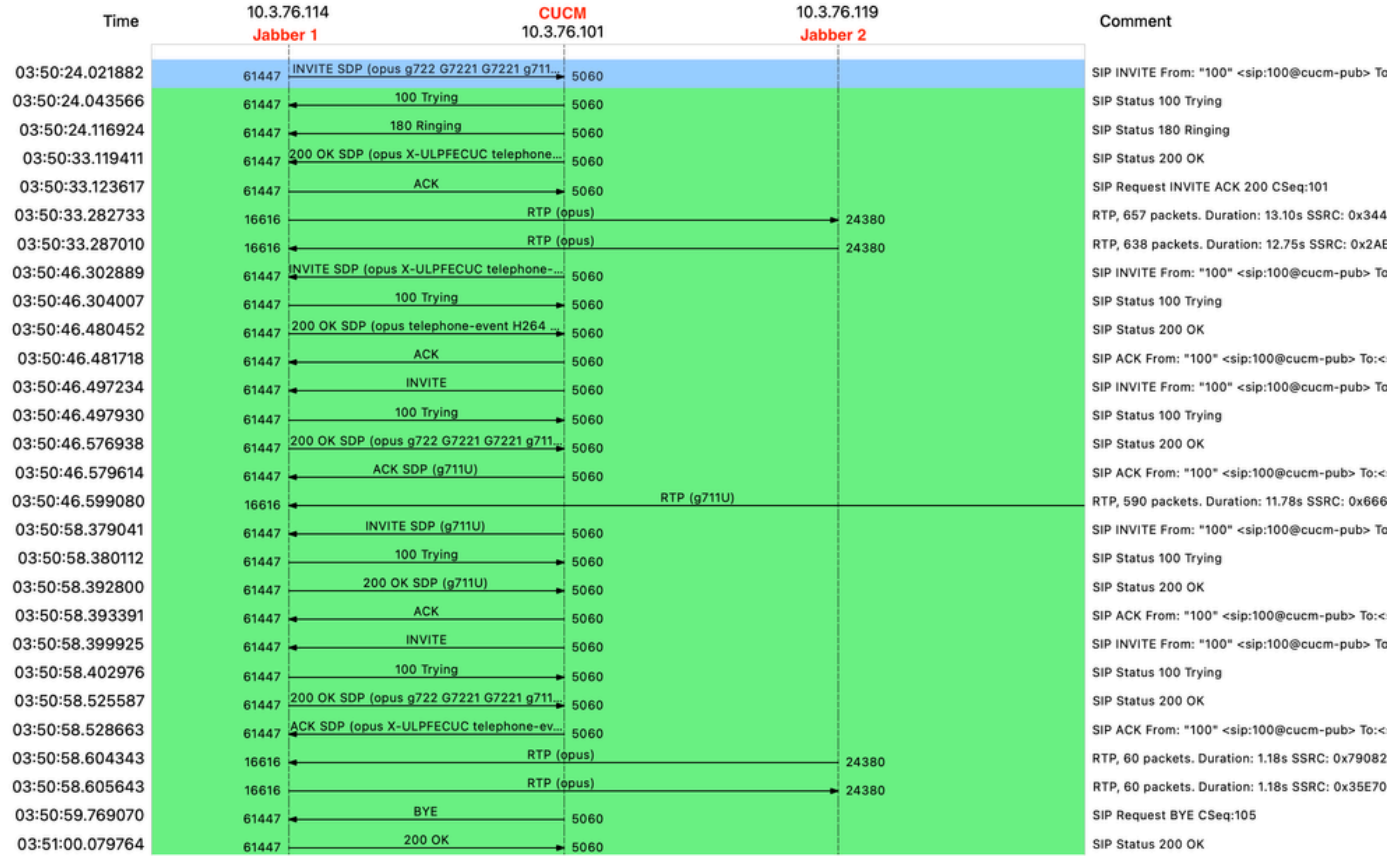
4. Replicate the issue and note important information such as timestamp, called number, calling number and any specific error or behavior during the call.

5. Stop and collect the Wireshark packet capture.

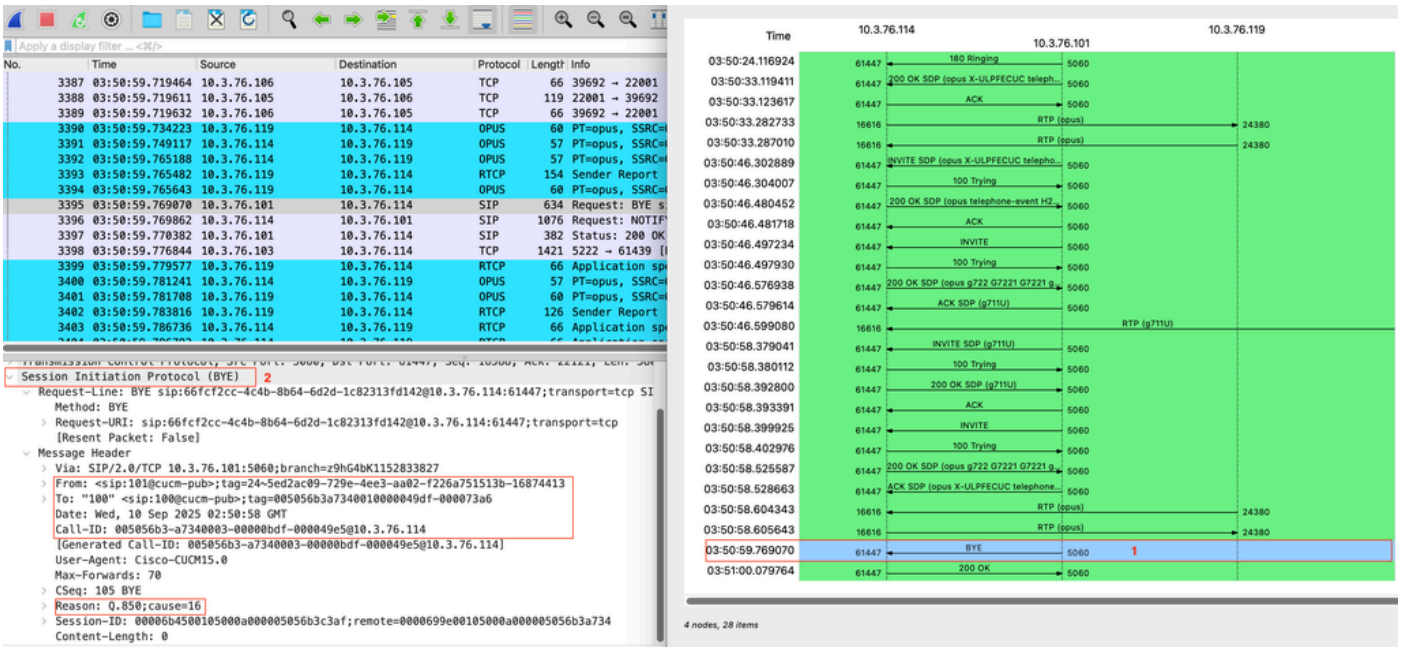
6. Open the packet capture and navigate to **Telephony > VoIP Calls > Identify the test call** and click **Flow Sequence**.



7. Wireshark displays the call flow diagram from the device perspective. Identify the network devices part of the flow and analyze the SIP signaling looking for SIP errors or any indication of why the call is terminated or not initiated.



8. If any of the SIP messages is of interest for the investigation click the message and Wireshark automatically highlights the message in the packet capture. You can then perform a deep inspection to that specific packet. Expand the Session Initiation Protocol information of concern here, which is found in the packet details.



9. The packet details section of Wireshark contains all the information of that packet. From here, you can obtain detailed information such as **Call-ID**, **From**, **To**, **Date**, **Time, Errors** and **Reason** of those errors or messages. This information is relevant in case you need to track this call along the call flow path.

10. Most common errors for SIP calls are specified in the table below:

Code	Meaning	Likely Cause(s)	Fix / Action
403 Forbidden	Accepted but request denied	User lacks permission, wrong SIP domain, blocked by policy.	Check dial plan/permissions.
404 Not Found	User/extension not found	User not created, not registered, wrong dialed number.	Verify user exists; check endpoint registration; confirm routing/dial plan.
408 Request Timeout	No response from destination	Network issue, firewall/NAT block, device offline.	Test connectivity (ping/traceroute); open SIP/RTP ports; confirm device is online.
415 Unsupported Media Type	Media type not supported.	SDP includes unsupported codec/format.	Adjust codecs; ensure compatible SDP offer/answer.
480 Temporarily Unavailable	User not reachable.	Device not registered, Do Not Disturb, network loss.	Confirm endpoint status; check registration; verify network reachability.
486 Busy Here	Endpoint is busy.	User on another call, DND active.	Retry later; enable call waiting or forwarding.
488 Not Acceptable Here	Media negotiation failed.	Codec mismatch, SRTP vs RTP mismatch, unsupported DTMF method.	Align codec lists; check encryption settings; match DTMF type.
500 Internal Server Error	Server-side failure.	SIP service crash, misconfig.	Check server logs/config; restart SIP service
503 Service Unavailable	Server unavailable or overloaded.	Server down, maintenance, overload.	Verify server health; failover to backup; reduce load.

11. At this point, you must have a Big Picture of where the issue relays, common scenarios are:

- Jabber generates the error or terminates the call. If that is the case, you must collect Jabber logs and track the call with the information from the packet details section obtained before. For the Jabber logs analysis is recommended a text editor and you can filter using the Call-ID information to show the information relevant for that call, also, a useful keyword to filter is **sipio** in order for it to show all the SIP messages in the logs. You must search for errors or events around the SIP failure that could cause our issue.
- Jabber receives error from another device or server, in this case, you must collect additional logs from the servers part of the call flow. In some cases, Call Manager logs and traces, Expressway logs and Gateway debugs. The information needed varies based on the affected call flow.

Wireshark Display Filters for SIP

Display filters can be used in Wireshark to filter and display specific information, multiple calls or messages. Some examples are mentioned in the table:

Purpose	**Display Filter**	**Notes**
All SIP traffic	sip	Shows only SIP signaling (no media).
INVITE messages	sip.Method == "INVITE"	Used for call setup analysis.
REGISTER messages	sip.Method == "REGISTER"	For registration/authentication issues.
All SIP errors (4xx/5xx/6xx)	sip.Status-Code >= 400	Quickly isolate failed requests.
Specific SIP error (such as 403)	sip.Status-Code == 403	Check only one type of failure.
Filter by Call-ID	sip.Call-ID == "abcd1234@domain.com"	Track a single call/session end-to-end.
SIP from/to a specific IP	ip.addr == 192.168.1.50 && sip	Focus on one endpoint’s SIP traffic.
All RTP traffic	rtp	Shows only RTP media streams.

Conclusion

This structured workflow can be used by engineers to troubleshoot Cisco Jabber SIP calls issues efficiently. Wireshark’s combination of SIP flow visualization and packet analysis makes it a critical tool to resolve Jabber calls setup problems.