

Troubleshoot Jabber SIP Call Issues with Wireshark

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Troubleshoot](#)

[Wireshark Display Filters for SIP](#)

[Conclusion](#)

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.

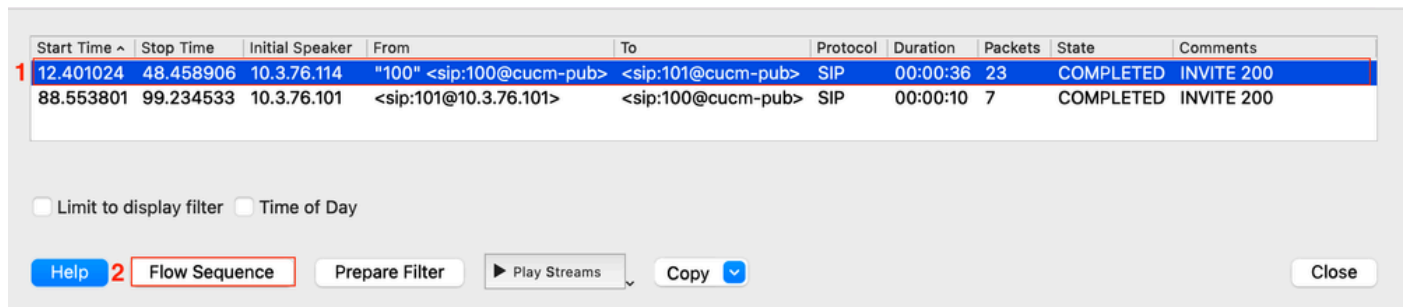


4. Replicate the issue and note important information such as timestamp, called number, calling number and any specific error or behavior during the call.

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.

Time	10.3.76.114 Jabber 1	CUCM 10.3.76.101	10.3.76.119 Jabber 2	Comment
03:50:24.021882	61447	INVITE SDP (opus g722 G7221 G7221 g711...	5060	SIP INVITE From: "100" <sip:100@cucm-pub> To
03:50:24.043566	61447	100 Trying	5060	SIP Status 100 Trying
03:50:24.116924	61447	180 Ringing	5060	SIP Status 180 Ringing
03:50:33.119411	61447	200 OK SDP (opus X-ULPFECUC telephone...	5060	SIP Status 200 OK
03:50:33.123617	61447	ACK	5060	SIP Request INVITE ACK 200 CSeq:101
03:50:33.282733	16616	RTP (opus)	24380	RTP, 657 packets. Duration: 13.10s SSRC: 0x344
03:50:33.287010	16616	RTP (opus)	24380	RTP, 638 packets. Duration: 12.75s SSRC: 0x2AE
03:50:46.302889	61447	INVITE SDP (opus X-ULPFECUC telephone...	5060	SIP INVITE From: "100" <sip:100@cucm-pub> To
03:50:46.304007	61447	100 Trying	5060	SIP Status 100 Trying
03:50:46.480452	61447	200 OK SDP (opus telephone-event H264 ...	5060	SIP Status 200 OK
03:50:46.481718	61447	ACK	5060	SIP ACK From: "100" <sip:100@cucm-pub> To:<
03:50:46.497234	61447	INVITE	5060	SIP INVITE From: "100" <sip:100@cucm-pub> To
03:50:46.497930	61447	100 Trying	5060	SIP Status 100 Trying
03:50:46.576938	61447	200 OK SDP (opus g722 G7221 G7221 g711...	5060	SIP Status 200 OK
03:50:46.579614	61447	ACK SDP (g711U)	5060	SIP ACK From: "100" <sip:100@cucm-pub> To:<
03:50:46.599080	16616	RTP (g711U)	24380	RTP, 590 packets. Duration: 11.78s SSRC: 0x666
03:50:58.379041	61447	INVITE SDP (g711U)	5060	SIP INVITE From: "100" <sip:100@cucm-pub> To
03:50:58.380112	61447	100 Trying	5060	SIP Status 100 Trying
03:50:58.392800	61447	200 OK SDP (g711U)	5060	SIP Status 200 OK
03:50:58.393391	61447	ACK	5060	SIP ACK From: "100" <sip:100@cucm-pub> To:<
03:50:58.399925	61447	INVITE	5060	SIP INVITE From: "100" <sip:100@cucm-pub> To
03:50:58.402976	61447	100 Trying	5060	SIP Status 100 Trying
03:50:58.525587	61447	200 OK SDP (opus g722 G7221 G7221 g711...	5060	SIP Status 200 OK
03:50:58.528663	61447	ACK SDP (opus X-ULPFECUC telephone-ev...	5060	SIP ACK From: "100" <sip:100@cucm-pub> To:<
03:50:58.604343	16616	RTP (opus)	24380	RTP, 60 packets. Duration: 1.18s SSRC: 0x79082
03:50:58.605643	16616	RTP (opus)	24380	RTP, 60 packets. Duration: 1.18s SSRC: 0x35E70
03:50:59.769070	61447	BYE	5060	SIP Request BYE CSeq:105
03:51:00.079764	61447	200 OK	5060	SIP Status 200 OK

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.

Apply a display filter: <K>

No.	Time	Source	Destination	Protocol	Length	Info
3387	03:50:59.719464	10.3.76.106	10.3.76.105	TCP	66	39692 → 22001
3388	03:50:59.719611	10.3.76.106	10.3.76.105	TCP	119	22001 → 39692
3389	03:50:59.719632	10.3.76.106	10.3.76.105	TCP	66	39692 → 22001
3390	03:50:59.734223	10.3.76.119	10.3.76.114	OPUS	60	PT=opus, SSRC=...
3391	03:50:59.749117	10.3.76.114	10.3.76.119	OPUS	57	PT=opus, SSRC=...
3392	03:50:59.765188	10.3.76.114	10.3.76.119	OPUS	57	PT=opus, SSRC=...
3393	03:50:59.765482	10.3.76.119	10.3.76.114	RTCP	154	Sender Report
3394	03:50:59.765643	10.3.76.119	10.3.76.114	OPUS	60	PT=opus, SSRC=...
3395	03:50:59.769070	10.3.76.101	10.3.76.114	SIP	634	Request: BYE s...
3396	03:50:59.769862	10.3.76.114	10.3.76.101	SIP	1076	Request: NOTIF...
3397	03:50:59.770382	10.3.76.101	10.3.76.114	SIP	382	Status: 200 OK
3398	03:50:59.776844	10.3.76.103	10.3.76.114	TCP	1421	5222 → 61439 [I...
3399	03:50:59.779577	10.3.76.119	10.3.76.114	RTCP	66	Application sp...
3400	03:50:59.781241	10.3.76.114	10.3.76.119	OPUS	57	PT=opus, SSRC=...
3401	03:50:59.781708	10.3.76.114	10.3.76.119	OPUS	60	PT=opus, SSRC=...
3402	03:50:59.783816	10.3.76.119	10.3.76.114	RTCP	126	Sender Report
3403	03:50:59.786736	10.3.76.114	10.3.76.119	RTCP	66	Application sp...

Session Initiation Protocol (BYE) 2

Request-Line: BYE sip:66fcf2cc-4c4b-8b64-6d2d-1c82313fd142@10.3.76.114:61447;transport=tcp SI

Method: BYE

Request-URI: sip:66fcf2cc-4c4b-8b64-6d2d-1c82313fd142@10.3.76.114:61447;transport=tcp [Reset Packet: False]

Message Header

Via: SIP/2.0/TCP 10.3.76.101:5060;branch=z9hG4bK1152833827

From: <sip:101@cucm-pub>;tag=24-5ed2ac09-729e-4ee3-aa02-f226a751513b-16874413

To: "100" <sip:100@cucm-pub>;tag=005056b3a7340010000049df-000073a6

Date: Wed, 10 Sep 2025 02:50:58 GMT

Call-ID: 005056b3-a7340003-00000bdf-000049e5@10.3.76.114

[Generated Call-ID: 005056b3-a7340003-00000bdf-000049e5@10.3.76.114]

User-Agent: Cisco-CUCM15.0

Max-Forwards: 70

CSeq: 105 BYE

Reason: 0.850;cause=16

Session-ID: 00006b4500105000a000005056b3c3af;remote=0000699e00105000a000005056b3a734

Content-Length: 0

Time 10.3.76.114 10.3.76.101 10.3.76.119

03:50:24.116924 61447 180 Ringing 5060

03:50:33.119411 61447 200 OK SDP (opus X-ULPFECUC teleph... 5060

03:50:33.123617 61447 ACK 5060

03:50:33.282733 16616 RTP (opus) 24380

03:50:33.287010 16616 RTP (opus) 24380

03:50:46.302889 61447 INVITE SDP (opus X-ULPFECUC teleph... 5060

03:50:46.304007 61447 100 Trying 5060

03:50:46.480452 61447 200 OK SDP (opus telephone-event H2... 5060

03:50:46.481718 61447 ACK 5060

03:50:46.497234 61447 INVITE 5060

03:50:46.497930 61447 100 Trying 5060

03:50:46.576938 61447 200 OK SDP (opus g722 G7221 G7221 g... 5060

03:50:46.579614 61447 ACK SDP (g711U) 5060

03:50:46.599080 16616 RTP (g711U) 24380

03:50:58.379041 61447 INVITE SDP (g711U) 5060

03:50:58.380112 61447 100 Trying 5060

03:50:58.392800 61447 200 OK SDP (g711U) 5060

03:50:58.393391 61447 ACK 5060

03:50:58.399925 61447 INVITE 5060

03:50:58.402976 61447 100 Trying 5060

03:50:58.525587 61447 200 OK SDP (opus g722 G7221 G7221 g... 5060

03:50:58.528663 61447 ACK SDP (opus X-ULPFECUC telephone... 5060

03:50:58.604343 16616 RTP (opus) 24380

03:50:58.605643 16616 RTP (opus) 24380

03:50:59.769070 61447 BYE 5060 1

03:51:00.079764 61447 200 OK 5060

4 nodes, 28 items

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.