Problemen met Jabber SIP-oproepen oplossen met Wireshark

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen met Jabber SIP-oproepen met Wireshark kunt oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SIP-signalering
- Jabber-oproepstromen
- Wireshark en basiskennis van pakketfiltering

Gebruikte componenten

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

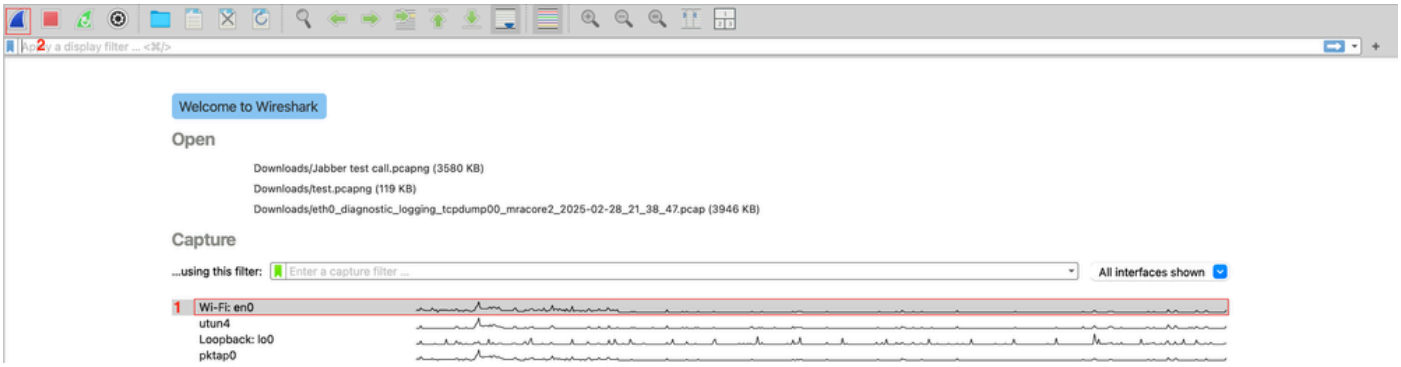
Session Initiation Protocol (SIP) is het standaardprotocol voor signalering in VoIP-communicatie. SIP beheert het instellen, wijzigen en afbreken van oproepen. Wanneer oproepen niet tot stand komen, ligt het probleem vaak in SIP-signalering. Cisco Jabber gebruikt SIP voor signalering bij het voeren van spraak- of videogesprekken. Wireshark stelt ingenieurs in staat om SIP-berichten vast te leggen en te analyseren, fouten te identificeren en de oorzaak van mislukte oproepinstellingen vast te stellen.

Problemen oplossen

1. Identificeer en isoleer de betrokken oproepstroom, dit is een belangrijke stap aangezien dit de netwerkapparaten bepaalt die bij het probleem betrokken zijn. Gebruik voor dit document als referentie een point-to-point call tussen 2 Jabber-clients die zijn geregistreerd bij CUCM, maar deze basisprobleemoplossing is van toepassing op meerdere scenario's.

2. Open Wireshark.

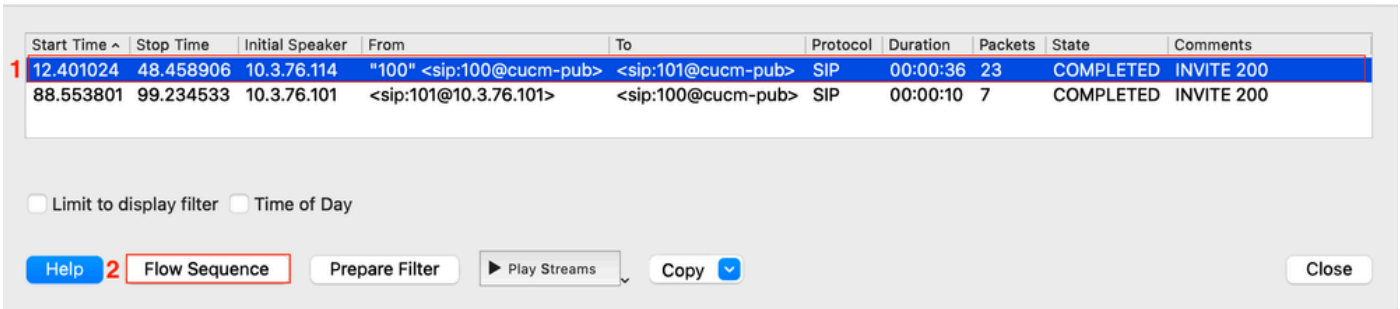
3. Selecteer de juiste netwerkinterface en start Wireshark-pakketopnames op het getroffen apparaat.



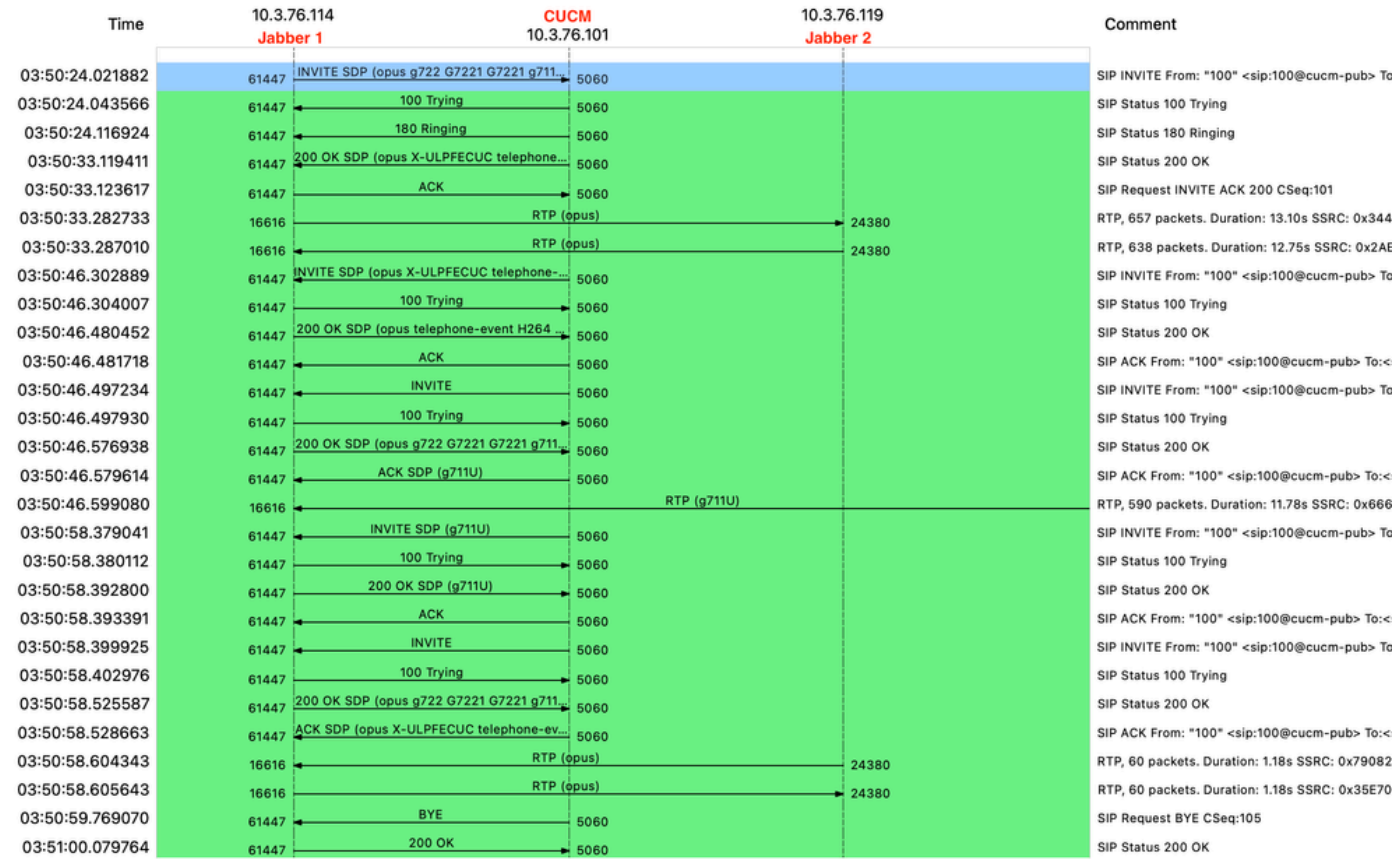
4. Repliceer het probleem en noteer belangrijke informatie zoals tijdstempel, belnummer, oproepnummer en eventuele specifieke fouten of gedrag tijdens het gesprek.

5. Stop en verzamel de Wireshark pakketvangst.

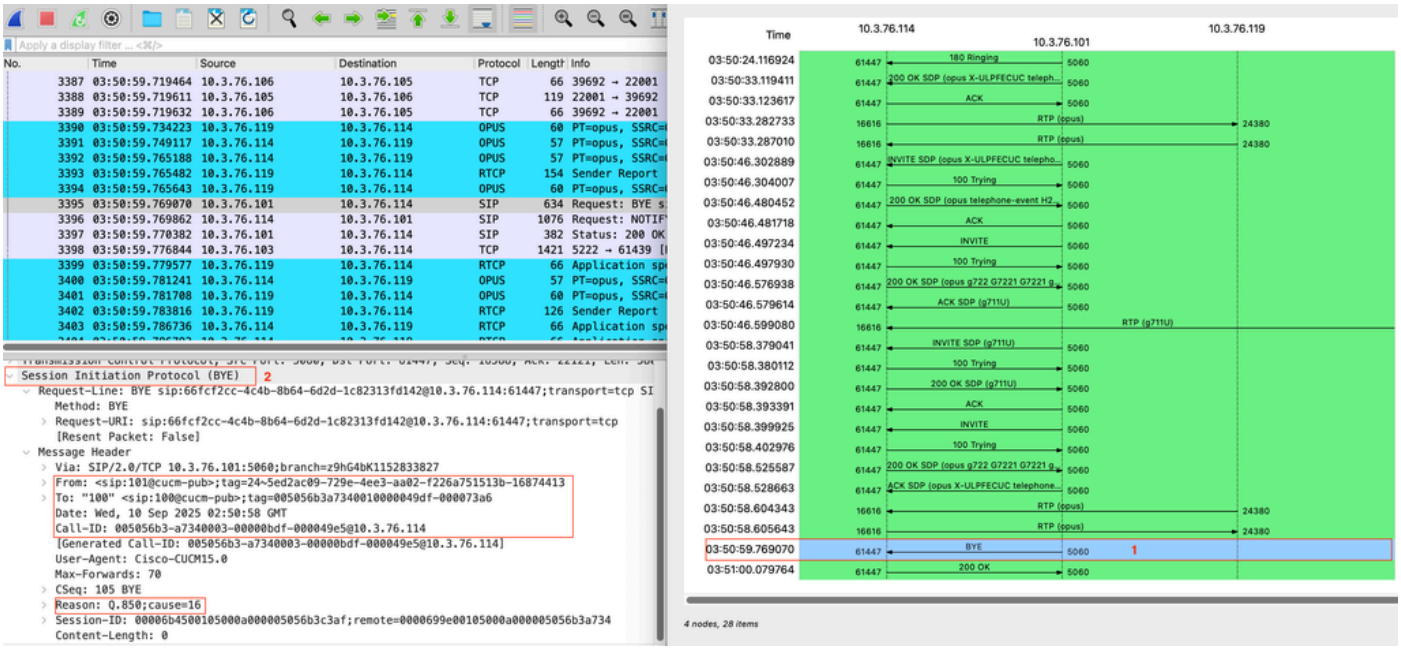
6. Open de pakketopname en navigeer naar Telefonie > VoIP-oproepen > Identificeer de testoproep en klik op Flow Sequence.



7. Wireshark geeft het oproepstroomdiagram weer vanuit het apparaatperspectief. Identificeer de netwerkapparaten die deel uitmaken van de stroom en analyseer de SIP-signalering op zoek naar SIP-fouten of een indicatie waarom de oproep wordt beëindigd of niet wordt geïnitieerd.



8. Als een van de SIP-berichten van belang is voor het onderzoek, klikt u op het bericht en Wireshark markeert automatisch het bericht in de pakketopname. U kunt dan een grondige inspectie uitvoeren op dat specifieke pakket. Vouw hier de informatie over het Sessie-initiatieprotocol uit, die te vinden is in de pakketdetails.



9. Het gedeelte met pakketgegevens van Wireshark bevat alle informatie over dat pakket. Vanaf

hier kunt u gedetailleerde informatie verkrijgen, zoals Call-ID, Van, Tot, Datum, Tijd, Fouten en Reden van die fouten of berichten. Deze informatie is relevant voor het geval u deze oproep langs het callstroompad moet volgen.

10. De meest voorkomende fouten voor SIP-oproepen worden in de onderstaande tabel gespecificeerd:

coderen	Betekenis	Waarschijnlijke oorzaak(en)	Fix / actie
403 Verboden	Aanvaard, maar verzoek afgewezen	Gebruiker mist toestemming, verkeerd SIP-domein, geblokkeerd door beleid.	Controleer kiesplan/machtigingen.
404 niet gevonden	Gebruiker/extensie niet gevonden	Gebruiker niet gemaakt, niet geregistreerd, verkeerd gekozen nummer.	Controleer of de gebruiker bestaat; controleer de registratie van het eindpunt; bevestig de routering/het kiesplan.
408 Time-out voor aanvraag	Geen reactie van bestemming	Netwerkprobleem, firewall/NAT-blok, apparaat offline.	Connectiviteit testen (ping/traceroute); SIP/RTP-poorten openen; bevestigen dat het apparaat online is.
415 Niet-ondersteund mediatype	Mediatype wordt niet ondersteund.	SDP bevat niet-ondersteunde codec/indeling.	Pas codecs aan; zorg voor een compatibel SDP-aanbod/antwoord.
480 Tijdelijk niet beschikbaar	Gebruiker niet bereikbaar.	Apparaat niet geregistreerd, Niet storen, netwerkverlies.	Eindpuntstatus bevestigen; registratie controleren; netwerkbereikbaarheid controleren.
486 druk hier	Het eindpunt is bezet.	Gebruiker bij een ander gesprek, DND actief.	Probeer het later opnieuw; schakel het wachten of doorsturen van oproepen in.
488 Niet	Mediaonderhandelingen	Mismatch van codec,	Codeclijsten uitlijnen;

coderen	Betekenis	Waarschijnlijke oorzaak(en)	Fix / actie
aanvaardbaar	mislukten.	SRTP vs RTP-mismatch, niet-ondersteunde DTMF-methode.	coderingsinstellingen controleren; overeenkomen met het DTMF-type.
500 Interne serverfout	Server-side failure.	SIP-service crash, verkeerde configuratie.	Serverlogs/configuratie controleren; SIP-service opnieuw starten
503 Service niet beschikbaar	Server niet beschikbaar of overbelast.	Server down, onderhoud, overbelasting.	Controleren van de status van de server; failover naar back-up; belasting verminderen.

11. Op dit punt moet u een overzicht hebben van waar het probleem zich voordoet, gemeenschappelijke scenario's zijn:

- Jabber genereert de fout of beëindigt de oproep. Als dat het geval is, moet u Jabber-logs verzamelen en de oproep volgen met de informatie uit de sectie met pakketdetails die u eerder hebt verkregen. Voor de analyse van de Jabber-logs wordt een teksteditor aanbevolen en u kunt filteren met behulp van de Call-ID-informatie om de informatie weer te geven die relevant is voor die oproep, ook is een nuttig zoekwoord om te filteren sipio om alle SIP-berichten in de logs weer te geven. U moet zoeken naar fouten of gebeurtenissen rond de SIP-fout die ons probleem kunnen veroorzaken.
- Jabber ontvangt een fout van een ander apparaat of server, in dit geval moet u extra logs verzamelen van de servers die deel uitmaken van de oproepstroom. In sommige gevallen logt en traceert Call Manager, Expressway-logboeken en Gateway-debugs. De benodigde informatie varieert op basis van de betrokken oproepstroom.

Wireshark Display Filters voor SIP

Weergavefilters kunnen in Wireshark worden gebruikt om specifieke informatie, meerdere oproepen of berichten te filteren en weer te geven. Enkele voorbeelden worden genoemd in de tabel:

Doel	weergavefilter	Opmerkingen
Al het SIP-verkeer	nippen	Geeft alleen SIP-signalering weer (geen media).

Doel	weergavefilter	Opmerkingen
Berichten UITNODIGEN	sip.Methode == "UITNODIGEN"	Gebruikt voor analyse van oproepinstellingen.
Berichten registreren	sip.Methode == "REGISTREREN"	Voor registratie-/authenticatieproblemen.
Alle SIP-fouten (4xx/5xx/6xx)	sip.Status-code >= 400	Snel mislukte aanvragen isoleren.
Specifieke SIP-fout (zoals 403)	sip.Status-code == 403	Controleer slechts één type fout.
Filteren op Call-ID	sip.Call-ID == "abcd1234@domain.com"	Volg één oproep/sessie end-to-end.
SIP van/naar een specifiek IP-adres	IP.addr == 192.168.1.50 & & SIP	Focus op het SIP-verkeer van één eindpunt.
Al het RTP-verkeer	RTP	Toont alleen RTP-mediastromen.

Conclusie

Deze gestructureerde workflow kan door technici worden gebruikt om problemen met Cisco Jabber SIP-oproepen efficiënt op te lossen. Wireshark's combinatie van SIP-stroomvisualisatie en pakketanalyse maakt het een cruciaal hulpmiddel om installatieproblemen van Jabber-oproepen op te lossen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.