

Solucionar problemas de chamada SIP do Jabber com o Wireshark

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Troubleshooting](#)

[Filtros de Exibição do Wireshark para SIP](#)

[Conclusão](#)

Introdução

Este documento descreve como solucionar problemas de chamadas SIP Jabber com o Wireshark.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- sinalização SIP
- Fluxos de chamadas Jabber
- Wireshark e conhecimento básico de filtragem de pacotes

Componentes Utilizados

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

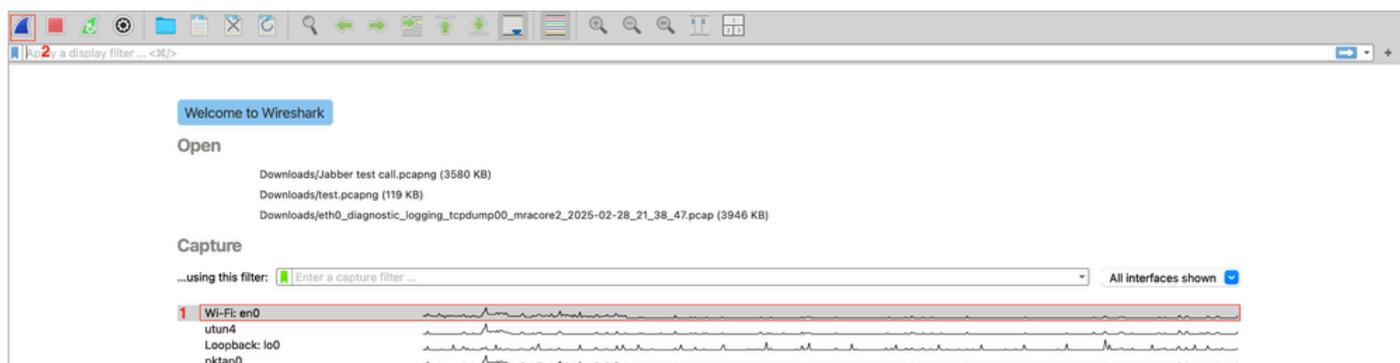
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Session Initiation Protocol (SIP) é o protocolo padrão para sinalização em comunicações VoIP. O SIP gerencia a configuração, a modificação e a desmontagem de chamadas. Quando as chamadas não são estabelecidas, o problema geralmente está na sinalização SIP. O Cisco Jabber usa SIP para sinalização ao fazer chamadas de voz ou vídeo. O Wireshark permite que os engenheiros capturem e analisem mensagens SIP, identifiquem erros e identifiquem a causa de falhas de configuração de chamadas.

Troubleshooting

1. Identifique e isole o fluxo de chamadas afetado. Esta é uma etapa importante, pois determina os dispositivos de rede envolvidos no problema. Para este documento, use como referência uma chamada ponto-a-ponto entre 2 clientes Jabber registrados no CUCM, no entanto, esta solução de problemas básica se aplica a vários cenários.
2. Abra o Wireshark.
3. Selecione a interface de rede correta e inicie as capturas de pacotes do Wireshark no dispositivo afetado.



4. Replique o problema e anote informações importantes, como carimbo de data/hora, número chamado, número chamador e qualquer erro ou comportamento específico durante a chamada.

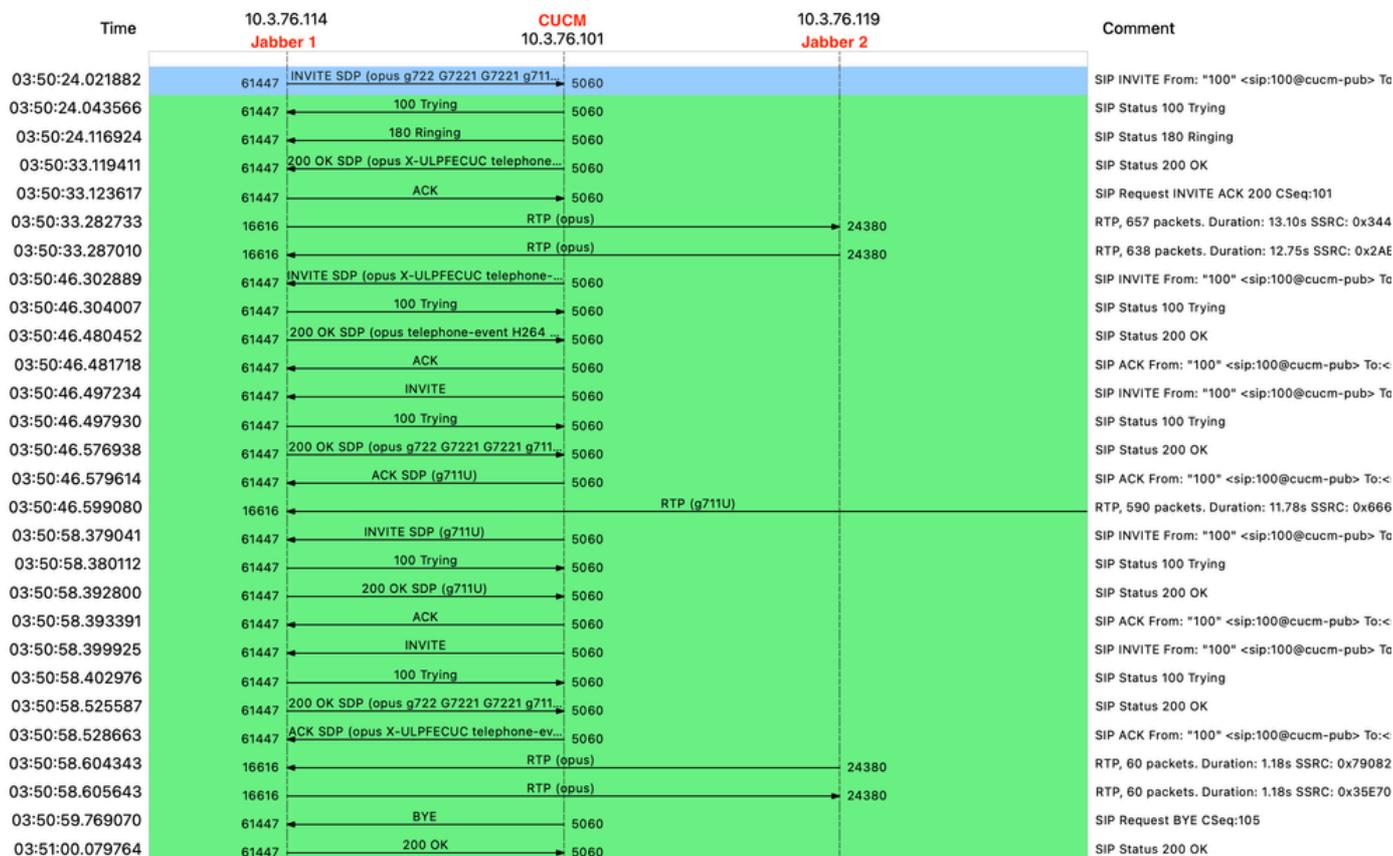
5. Pare e colete a captura de pacotes do Wireshark.



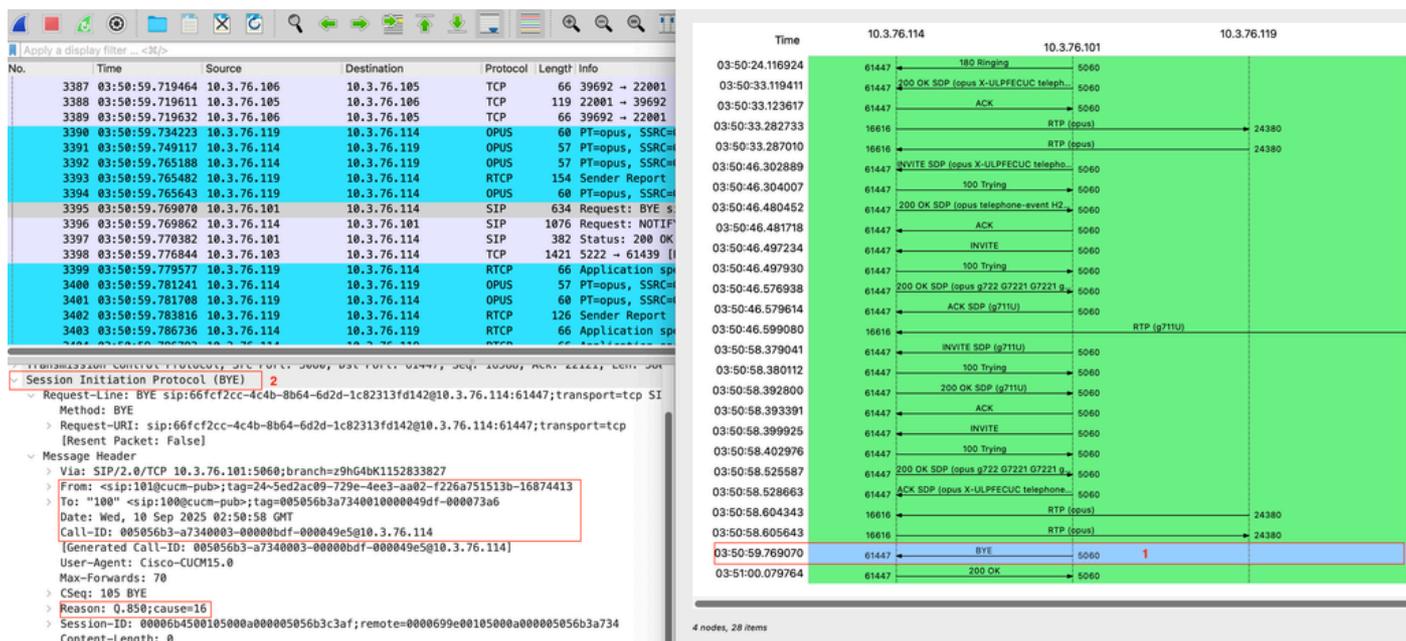
6. Abra a captura de pacotes e navegue até Telefonia > Chamadas VoIP > Identificar a chamada de teste e clique em Sequência de Fluxo.



7. O Wireshark exibe o diagrama do fluxo de chamadas da perspectiva do dispositivo. Identifique a parte dos dispositivos de rede do fluxo e analise a sinalização SIP procurando erros SIP ou qualquer indicação do motivo pelo qual a chamada foi encerrada ou não foi iniciada.



8. Se alguma das mensagens SIP for de interesse para a investigação, clique na mensagem e o Wireshark realçará automaticamente a mensagem na captura de pacotes. Em seguida, você pode executar uma inspeção detalhada desse pacote específico. Expanda aqui as informações do Session Initiation Protocol que são relevantes e que são encontradas nos detalhes do pacote.



9. A seção de detalhes do pacote do Wireshark contém todas as informações desse pacote. A

partir daqui, você pode obter informações detalhadas, como Call-ID, From, To, Date, Time, Errors e Reason desses erros ou mensagens. Essas informações são relevantes caso você precise rastrear essa chamada ao longo do caminho do fluxo de chamada.

10. Os erros mais comuns das chamadas SIP são especificados na tabela abaixo:

Code	Significado	Causa(s) provável(is)	Correção / Ação
403 Proibido	Aceito, mas solicitação negada	O usuário não tem permissão, domínio SIP incorreto, bloqueado pela política.	Verifique o plano de discagem/permisões.
404 Não encontrado	Usuário/ramal não encontrado	Usuário não criado, não registrado, número discado incorreto.	Verificar se o usuário existe; verificar o registro do ponto terminal; confirme o plano de roteamento/discagem.
408 Tempo Limite de Solicitação	Sem resposta do destino	Problema de rede, bloqueio de firewall/NAT, dispositivo offline.	Testar a conectividade (ping/traceroute); portas SIP/RTP abertas; confirmar se o dispositivo está online.
415 Tipo de mídia sem suporte	Tipo de mídia sem suporte.	O SDP inclui codec/formato sem suporte.	Ajustar codecs; garantir que a oferta/resposta do SDP seja compatível.
480 temporariamente indisponível	Usuário inacessível.	Dispositivo não registrado, Não perturbar, perda de rede.	Confirmar o status do ponto final; Verificar o registro; verifique a alcançabilidade da rede.
486 Ocupado Aqui	O ponto de extremidade está ocupado.	Usuário em outra chamada, DND ativo.	Tentar novamente mais tarde; habilitar o encaminhamento ou a espera de chamadas.
488 Não Aceitável Aqui	Falha na negociação de mídia.	Incompatibilidade de codec, incompatibilidade de SRTP vs RTP, método DTMF sem suporte.	Alinhar as listas de codecs; verificar as configurações de criptografia; match DTMF type (corresponder tipo DTMF).

Code	Significado	Causa(s) provável(is)	Correção / Ação
Erro interno do servidor 500	Falha no servidor.	Falha no serviço SIP, erro de configuração.	Verificar a configuração/registros do servidor; reiniciar serviço SIP
Serviço 503 Indisponível	Servidor indisponível ou sobrecarregado.	Servidor inoperante, manutenção, sobrecarga.	Verificar a integridade do servidor; failover para backup; reduzir a carga.

11. Neste ponto, você deve ter uma Visão Geral de onde o problema se retransmite, cenários comuns são:

- O Jabber gera o erro ou encerra a chamada. Se esse for o caso, você deve coletar logs do Jabber e rastrear a chamada com as informações da seção de detalhes do pacote obtidas antes. Para os logs do Jabber, recomenda-se um editor de texto e você pode filtrar usando as informações de ID de chamada para mostrar as informações relevantes para essa chamada. Além disso, uma palavra-chave útil para filtrar é sipio para que ele mostre todas as mensagens SIP nos logs. Você deve procurar erros ou eventos relacionados à falha do SIP que possam causar nosso problema.
- O Jabber recebe um erro de outro dispositivo ou servidor; nesse caso, você deve coletar logs adicionais da parte dos servidores do fluxo de chamadas. Em alguns casos, registros e rastreamentos do Call Manager, registros do Expressway e depurações do Gateway. As informações necessárias variam de acordo com o fluxo de chamadas afetado.

Filtros de Exibição do Wireshark para SIP

Os filtros de exibição podem ser usados no Wireshark para filtrar e exibir informações específicas, várias chamadas ou mensagens. Alguns exemplos são mencionados na tabela:

Propósito	Filtro de exibição	Notas
Todo o tráfego SIP	sip	Mostra apenas a sinalização SIP (sem mídia).
mensagens CONVITE	sip.Method == "CONVITE"	Usado para análise de configuração de chamada.
mensagens REGISTER	sip.Método == "REGISTER"	Para problemas de registro/autenticação.

Propósito	Filtro de exibição	Notas
Todos os erros SIP (4xx/5xx/6xx)	<code>sip.Status-Code >= 400</code>	Isolar rapidamente as solicitações com falha.
Erro SIP específico (como 403)	<code>sip.Status-Code == 403</code>	Verifique apenas um tipo de falha.
Filtrar por ID de chamada	<code>sip.Call-ID == "abcd1234@domain.com"</code>	Acompanhe uma única chamada/sessão de ponta a ponta.
SIP de/para um IP específico	<code>ip.addr == 192.168.1.50 e sip</code>	Concentre-se no tráfego SIP de um endpoint.
Todo o tráfego RTP	<code>rtp</code>	Mostra apenas os fluxos de mídia RTP.

Conclusão

Esse fluxo de trabalho estruturado pode ser usado por engenheiros para solucionar problemas de chamadas SIP do Cisco Jabber de forma eficiente. A combinação do Wireshark de visualização de fluxo SIP e análise de pacotes o torna uma ferramenta crítica para resolver problemas de configuração de chamadas Jabber.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.