使用Wireshark排除Jabber SIP呼叫问题

目录

简介

本文档介绍如何使用Wireshark对Jabber SIP呼叫问题进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- SIP信令
- Jabber呼叫流
- Wireshark和数据包过滤的基本知识

使用的组件

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

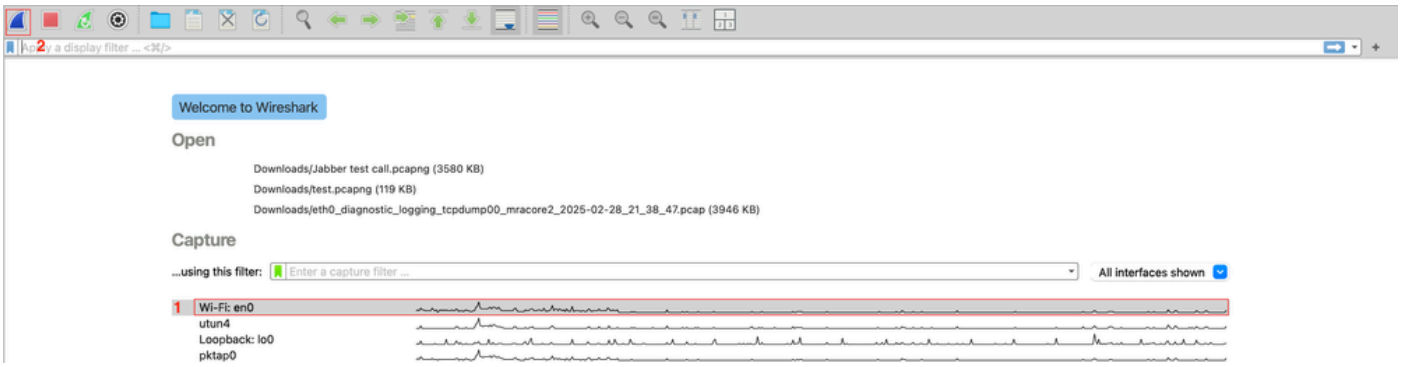
会话初始协议(SIP)是VoIP通信中的信令标准协议。SIP管理呼叫建立、修改和拆卸。当呼叫无法建立时，问题通常出在SIP信令上。在进行语音或视频呼叫时，Cisco Jabber使用SIP进行信令。Wireshark允许工程师捕获和分析SIP消息、识别错误并查明呼叫设置失败的原因。

故障排除

1.确定并隔离受影响的呼叫流，这是一个重要步骤，因为这决定了问题所涉及的网络设备。出于本文档的目的，请使用注册到CUCM的2个Jabber客户端之间的点对点呼叫作为参考，但是，此基本故障排除适用于多个场景。

2.打开Wireshark。

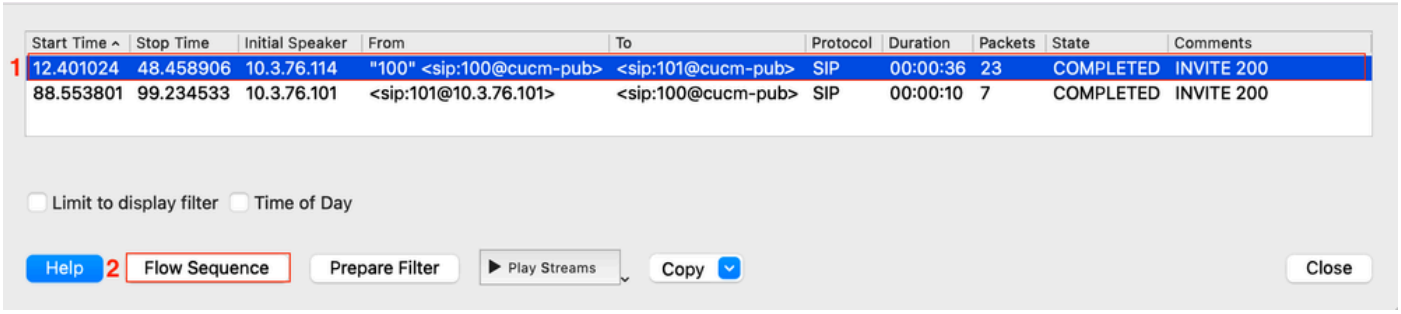
3.选择正确的网络接口并在受影响的设备上启动Wireshark数据包捕获。



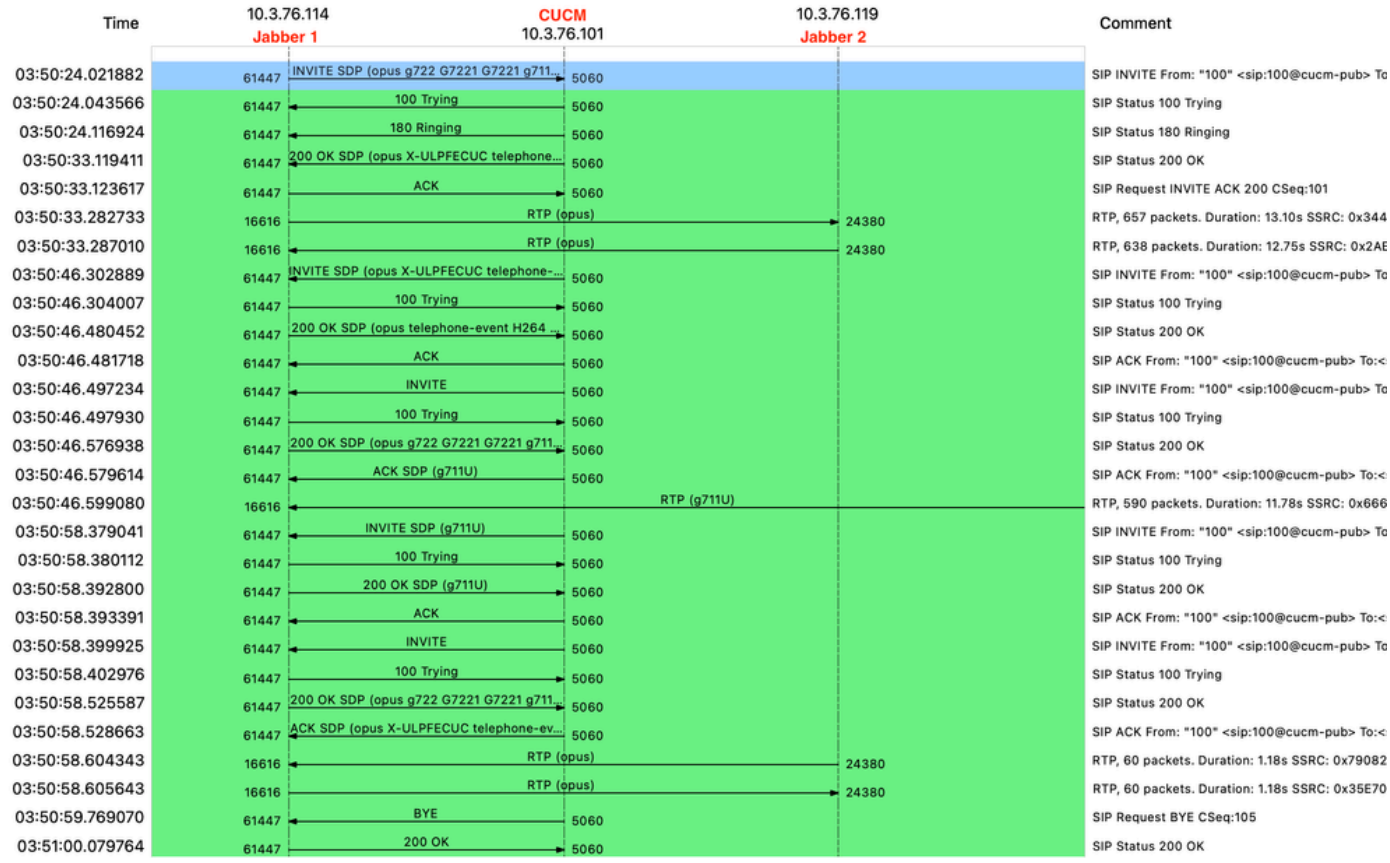
4.复制问题并记录重要信息，例如时间戳、被叫号码、主叫号码以及呼叫过程中的任何特定错误或行为。

5.停止并收集Wireshark数据包捕获。

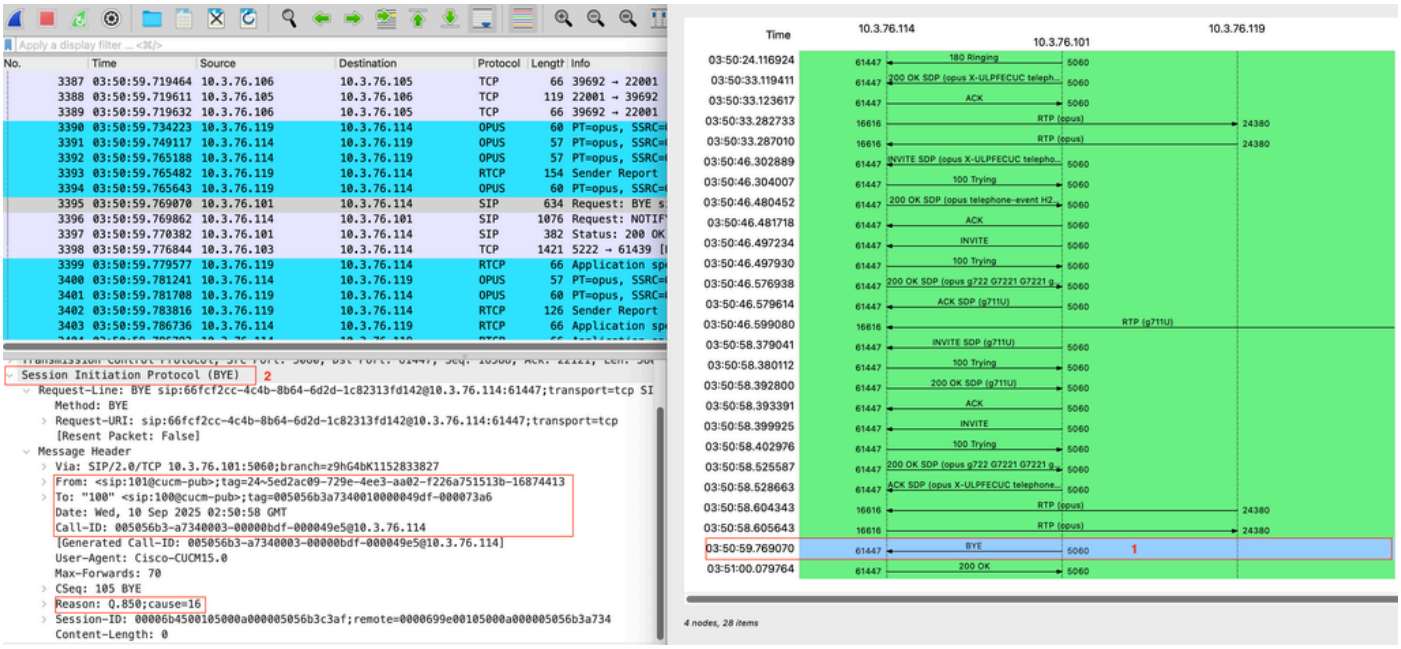
6.打开数据包捕获并导航到Telephony > VoIP Calls > Identify the test call，然后单击Flow Sequence。



7. Wireshark从设备的角度显示呼叫流程图。确定流程中的网络设备部分，并分析SIP信令，以查找SIP错误或任何呼叫终止或未发起原因的指示。



8.如果调查涉及任何SIP消息，请点击该消息，Wireshark将在数据包捕获中自动突出显示该消息。然后，您可以对该特定数据包执行深度检测。请在此处展开相关会话发起协议信息，这些信息可在数据包详细信息中找到。



9. Wireshark的数据包详细信息部分包含该数据包的所有信息。您可以从此处获取详细信息，例如这些错误或消息的Call-ID、From、To、Date、Time、Errors和Reason。如果您需要沿着呼叫流程路径跟踪此呼叫，此信息将相关。

10.下表列出了SIP呼叫最常见的错误：

代码	含义	可能的原因	修复/操作
403禁止	已接受，但请求被拒绝	用户缺少权限，SIP域错误，被策略阻止。	检查拨号方案/权限。
404未找到	找不到用户/分机	用户未创建，未注册，拨打的号码错误。	验证用户是否存在；检查终端注册；确认路由/拨号方案。
408请求超时	没有来自目的地的响应	网络问题、防火墙/NAT阻止、设备脱机。	测试连通性(ping/traceroute);打开SIP/RTP端口；确认设备已联机。
415不支持的媒体类型	媒体类型不受支持。	SDP包括不受支持的编解码器/格式。	调整编解码器；确保兼容的SDP产品/应答。
480暂时不可用	用户无法访问。	设备未注册、请勿打扰、网络丢失。	确认终端状态；支票登记；检验网络连通性。
486在此忙碌	终结点正忙。	其他呼叫的用户，DND处于活动状态。	稍后重试；启用呼叫等待或转发。
488此处不可接受	媒体协商失败。	编解码器不匹配、SRTP与RTP不匹配、不支持的DTMF方法。	调整编解码器列表；检查加密设置；匹配DTMF类型。
500内部服务器错误	服务器端故障。	SIP服务崩溃，配置错误。	检查服务器日志/配置；重新启动SIP服务
503服务不可用	服务器不可用或过载。	服务器停机、维护、过载。	验证服务器运行状况；故障切换至备份；减少负载。

11.此时，您必须了解问题转发的总体情况，常见情况包括：

- Jabber生成错误或终止呼叫。如果出现这种情况，您必须收集Jabber日志，并使用之前获得的数据包详细信息部分中的信息跟踪呼叫。对于Jabber日志分析，建议使用文本编辑器，并且可以使用呼叫ID信息进行过滤，以显示与该呼叫相关的信息，此外，过滤的有用关键字是sipio，以便其显示日志中的所有SIP消息。您必须搜索可能导致问题的SIP故障相关错误或事件。
- Jabber从其他设备或服务器接收错误，在这种情况下，您必须从呼叫流的服务器部分收集其他日志。在某些情况下，Call Manager会记录和跟踪、Expressway日志和网关调试。所需信息因受影响的呼叫流程而异。

SIP的Wireshark显示过滤器

Display filters（显示过滤器）可在Wireshark中用于过滤和显示特定信息、多个呼叫或消息。表中提到了一些示例：

目的	显示过滤器	备注
所有SIP流量	sip	仅显示SIP信令（无媒体）。
邀请消息	sip.Method == "INVITE"	用于呼叫建立分析。
注册消息	sip.Method == "REGISTER"	有关注册/身份验证问题。
所有SIP错误(4xx/5xx/6xx)	sip.Status-Code >= 400	快速隔离失败请求。
特定SIP错误（例如403）	sip.Status-Code == 403	仅检查一种类型的故障。
按呼叫ID过滤	sip.Call-ID == "abcd1234@domain.com"	端到端跟踪单个呼叫/会话。
特定IP的SIP来源/目标	ip.addr == 192.168.1.50和& sip	关注一个终端的SIP流量。
所有RTP流量	rtp	仅显示RTP媒体流。

结论

此结构化工作流程可供工程师用来有效地排除Cisco Jabber SIP呼叫问题。Wireshark结合了SIP流可视化和数据包分析，使其成为解决Jabber呼叫设置问题的重要工具。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。