VAF | BUNDESVERBAND TELEKOMMUNIKATION

SIP- und RTP-Troubleshooting

Teil 1:Technische Grundlagen – Protokollaufbau, Dialoge und Servertypen

Bild: unsplash.com / @bermixstudio

www.vaf.de

Impressum

SIP- und RTP-Troubleshooting
Teil 1: Technische Grundlagen – Protokollaufbau, Dialoge und Servertypen

Ausblick
Teil 2: Werkzeuge
Teil 3: Methoden, Planung und Praxisbeispiele

Autor
Benjamin Pfister, Rotenburg an der Fulda

Redaktion
Martin Bürstenbinder (V.i.S.d.P.), Uwe Klenner (Layout, Titelseite und Bildbearbeitung), Dr. Christian Jerger (Lektorat). Beratende Unterstützung: VAF-Fachkreis Technik mit den Mentoren Bernd Rücker und Jens Wilkens.

Bilder
Benjamin Pfister; Titelseite unsplash.com/@bermixstudio; Bildbearbeitungen: VAF

Herausgeber
VAF Bundesverband Telekommunikation e. V.
Otto-Hahn-Straße 16
40721 Hilden
www.vaf.de

Daniel Brosend (1. Vorsitzender), Martin Bürstenbinder (Geschäftsführer)

1. Auflage, November 2023

Inhaltsverzeichnis

Editorial

Die zuverlässige und nach Bedarf flexible Verfügbarkeit der Telekommunikation ist für jedes Unternehmen ein grundlegendes Erfordernis. Treten Funktionsstörungen auf, so müssen sie in möglichst kurzer Zeit behoben werden. Allerdings bergen die Komplexität der aktuellen Netztechnik und die spezifischen Eigenschaften des zentralen Session Initiation Protocol einige Herausforderungen für die Fehlersuche und Fehlerbehebung.

Hier setzt die dreiteilige Fachheftreihe des VAF an. Sie vermittelt aus der praktischen Erfahrung heraus grundlegendes Wissen zu der Fehleranalyse im besonderen Anwendungsbereich der Kommunikationstechnik. Sie leistet damit einen unterstützenden Beitrag, um die Effektivität und Effizienz des SIP/RTP-Troubleshootigns für ITK-Integratoren und Administratoren zu steigern.

Der vorliegende Teil 1 behandelt die technischen Grundlagen. Der kommende Teil 2 hat die Werkzeuge zum Thema und der Teil 3 wird neben den Methoden einen umfangreichen Part mit Praxisfällen beisteuern. Die Heftreihe darf jedoch nicht als Ersatz für das allgemeine Grundlagenwissen zur Netzwerktechnik, zu den einschlägigen Protokollen, zu SIP-Trunks usw. verstanden werden. Sie setzt vielmehr darauf auf. Für interessierte Einsteiger sei darum auf die Fachschulungen des VAF hingewiesen, zu denen auch diese Publikation als begleitendes Lehrheft dienen kann.

Der Autor ist aktiver Troubleshooting-Experte im ITK-Bereich und wirkt für den VAF als technischer Berater und Trainer. Die Idee zu der Heftreihe entstand im VAF-Fachkreis Technik, und Vertreter aus Mitgliedsunternehmen haben an der Entwicklung von Konzept und Inhalt beratend mitgewirkt.

Das ITK-Systemhaus als Problemlöser für den Kunden positioniert sich erfolgsorientiert am Markt. Letztlich zielt die Heftreihe darauf, den Mitgliedern in dem relevanten Kompetenzbereich des spezifischen Troubleshootings eine kompakte Wissenssammlung für die Fortbildung an die Hand zu geben.

Hilden, November 2023

Martin Bürstenbinder
Geschäftsführer
VAF Bundesverband Telekommunikation e. V.

1. Einleitung

Über 20 Jahre nach der Veröffentlichung des ersten Request for Comments (RFC) spielt die Kombination aus dem Session Initiation Protocol (SIP) und dem Real-Time Transport Protocol (RTP) eine zentrale Rolle in den Telekommunikationsnetzen. Sei es in internen Netzen zur Anbindung von Hardware- und Softwaretelefonen an eine IP-PBX, zur Kopplung von IP-PBXen untereinander oder mit Applikationsservern über SIP-Trunks. SIP-Trunks stellen dabei den aktuellen technischen Stand für die Kopplung mit den öffentlichen Telefonnetzen dar.

Jedoch birgt die Kombination der beiden Protokolle auch eine Vielzahl von Herausforderungen. Die Aufteilung in zwei zueinander in Beziehung stehende Datenströme, die bidirektional fließen müssen, steigert die Komplexität. Mit RTCP sind es sogar drei Datenströme. Außerdem kann der Initiator auf beiden Seiten der Kommunikationsbeziehung stehen. Jeder User Agent hält die Funktionalitäten als Client (UAC) und Server (UAS) vor und muss entsprechend über das zugrunde liegende Datennetzwerk kommunizieren können. Die dynamische Aushandlung der Codecs, Adressierungsinformationen und Zusatzinformationen über das Session Description Protocol (SDP) innerhalb des SIP-Dialogs bringt zwar Flexibilität, kann jedoch auch zu Aushandlungsfehlern führen. Hinzu kommt, dass es inzwischen über 100 (!) RFCs gibt, die sich ganz oder in Teilen mit SIP beschäftigen, viele davon mit einigen »Sollte«- anstatt »Muss«-Empfehlungen zur Implementierung. Dies alles zusammengenommen führt in der Praxis immer wieder zu Inkompatibilitäten.

Gerade das SIP bewerten einige Experten, wie selbst dessen ursprünglicher Entwickler Jonathan Rosenberg, inzwischen kritisch aufgrund seiner Komplexität in der Integration. Gleichwohl prägen SIP und RTP weiterhin die Kommunikationsnetze und mit dem SIP/RTP-spezifischen Know-how zum Troubleshooting lassen sich die Effektivität und Effizienz in der Fehlererkennung und -behebung wesentlich verbessern. Dieser erste Teil der dreiteiligen Heftreihe des VAF behandelt die spezifischen technischen Grundlagen des SIP/RTP-Troubleshootings. Als Erstes vergegenwärtigen wir uns kurz die Einordnung im OSI-Schichtenmodell sowie das SIP-Trapezoid. Die weiteren Kapitel erläutern die für das Troubleshooting wichtigsten Aspekte der Protokolle und die SIP-Servertypen.

1.1 OSI-Modell

Sowohl SIP, inklusive des SDP, als auch RTP bewegen sich im OSI-7-Schichten-Modell auf der Sitzungsschicht **(Tabelle 1)**. Diese logische Eingruppierung stellt einen wichtigen Aspekt im Troubleshooting dar, da Fehlerbilder auf einer Schicht auch auf Probleme bzw. Fehler in einer der unteren Schichten zurückzuführen sein können. Die Fehlerwahrnehmung des Anwenders bezieht sich naturgemäß auf die Applikationen, betrifft also die oberste Schicht. Letztlich muss der Troubleshooter, der die Ursache eines Fehlers aufspüren und diesen beheben will, alle Schichten im Blick behalten. Wie man dabei methodisch vorgeht, wird im dritten Teil dieser Heftreihe dargelegt. Die Einordnung im OSI-Modell gehört jedoch auch zum Verständnis der technischen Grundlagen des Troubleshootings.

OSI-Schicht	Protokoll / Applikation
Applikation	Sprach-/Videovermittlung, Sprach-/Videoübertragung
Präsentation	G.711, G.722, H.263, H.264
Sitzung	SIP inkl. SDP, RTP
Transport	UDP, TCP
Vermittlung	IPv4, IPv6
Sicherung	Ethernet, PPP
Bitübertragung	xDSL, Ethernet

Tabelle 1: Einsortierung von SIP mit dem darin eingebetteten SDP und RTP im OSI-Modell

1.2 Trapezoid

SIP und RTP haben unterschiedliche Datenströme, was auch im Troubleshooting Beachtung finden muss. Eine plakative Beispieldarstellung auf Basis des sogenannten SIP-Trapezoids findet sich in **Bild 1**. SIP kommt zur Signalisierung zum Einsatz, also beispielsweise beim Anrufauf- und -abbau, der Beendigung oder der Weiterleitung einer Session. RTP hingegen wird genutzt für den Austausch der Medieninformationen wie Sprache und Video.

Jedoch sind die Grenzen im Troubleshooting-Prozess häufig fließend. So wird die Beschreibung der Medieninformationen, wie beispielsweise der zugehörigen IP-Adressen und des UDP-Ports sowie der Codecs für RTP, über das SDP ausgetauscht. Daher muss der Analyst auch bei Fehlern der Übertragung von Medieninformationen einen genauen Blick auf die Signalisierung werfen.

Zudem folgt der RTP-Datenstrom beim Einsatz von Session Border Controllers (SBCs) an Sicherheitsübergängen oder beim Einsatz von Medienrelay aufgrund von Kompatibilitätsproblemen dem Netzwerkpfad der Signalisierung.

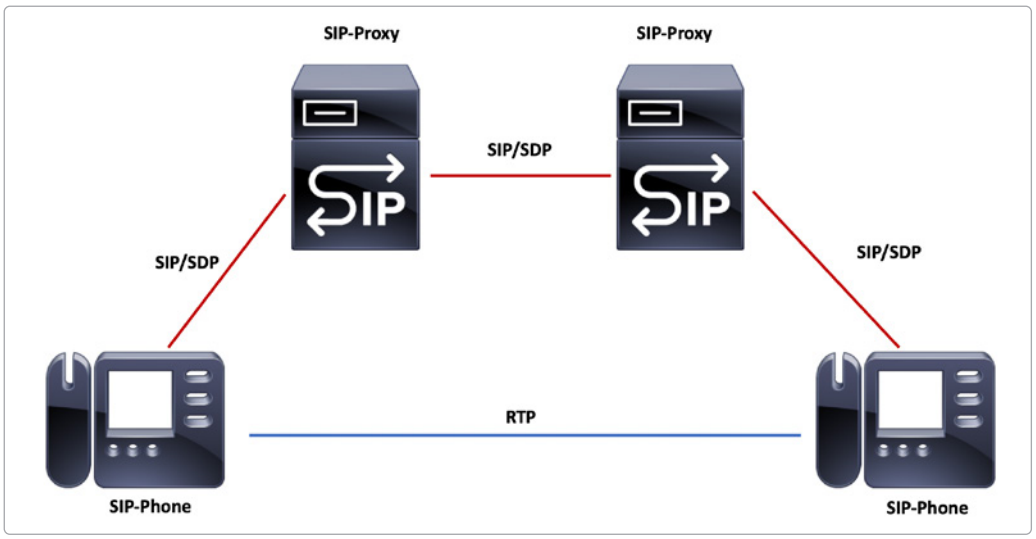

Bild 1: SIP-Trapezoid zur Verdeutlichung der unterschiedlichen Datenströme für die Signalisierung und die Sprachdaten

2. Protokollaufbau

Der Analyst benötigt zunächst ein Grundverständnis für die Protokolle. Daher stellt das Fachpapier zunächst die Protokollbasis vor und konzentriert bzw. beschränkt sich dabei auf die Bestandteile und Charakteristika, die für das Troubleshooting von besonderer Bedeutung sind.

2.1 SIP

Das SIP ist sehr flexibel. Aufgrund seiner Wandelbarkeit stellt es an den Analysten jedoch auch spezifische Anforderungen im Troubleshooting. Dies bedeutet, ihm müssen die Zusammenhänge zwischen den darunterliegenden Transportprotokollen, dem eigentlichen Nachrichtenaufbau und der Adressierung über die SIP-URI bekannt sein. Die folgenden Abschnitte veranschaulichen dies.

2.1.1 Transportprotokoll

Das SIP kann entweder auf dem verbindungslosen User Datagram Protocol (UDP) oder dem verbindungsorientierten Transmission Control Protocol (TCP) aufbauen. Beides ist in RFC 3261 definiert. Einen entscheidenden Vorteil der Übertragung mittels UDP stellt dessen Schnelligkeit dar, da kein Handshake stattfinden muss und der Header schlanker ist. Jedoch bietet nur TCP eine Fehlerkorrektur bzw. Wiederholungen bei Paketverlusten. Zudem ist UDP unter Sicherheitsaspekten anfälliger für IP-Spoofing-Attacken, also die Vortäuschung anderer Quell-IP-Adressen, und es besteht keine Möglichkeit der TLS-Verschlüsselung über UDP. TCP hat eine initial höhere Latenz aufgrund des notwendigen Handshakes. Beim Einsatz von TLS-Verschlüsselung braucht es im Nachgang auch noch einen TLS-Handshake. **Bild 2** zeigt beispielhaft eine Verbindung in Wireshark.

Das auf UDP aufbauende Quick UDP Internet Connections (QUIC), das auch eine zwingende TLS-1.3-Verschlüsselung bietet, ist noch nicht für SIP standardisiert.

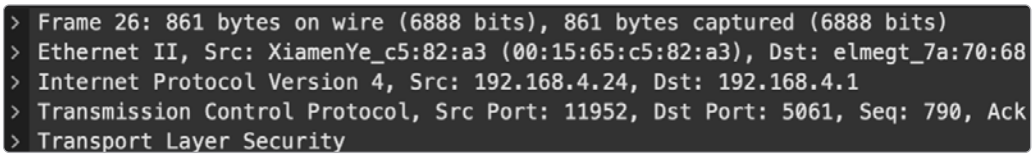

Bild 2: Screenshot einer SIP-over-TLS-Signalisierung. Man sieht den Protokollstapel mit Ethernet II, IPv4, TCP und darauf aufbauendem TLS.

2.1.2 SIP-Nachrichtenaufbau

Eine SIP-Nachricht besteht grundsätzlich aus drei Teilen. Diese sind die Request- oder Statuszeile, der Message-Header und der Message Body, der gegebenenfalls das SDP beinhaltet. **Bild 3** zeigt einen Screenshot aus Wireshark und wir finden dort die drei zuvor genannten Bestandteile.

Die Request-Zeile im Screenshot enthält die verwendete Methode »INVITE« sowie die angefragte SIP-URI und die SIP-Version. Die SIP-URI wird in Kapitel 2.3.1 vorgestellt.

Es gibt unterschiedliche Header-Typen. Dies sind zunächst die General Header, wie »To« und »From«. Sie enthalten allgemeine Anforderungen und die entsprechenden

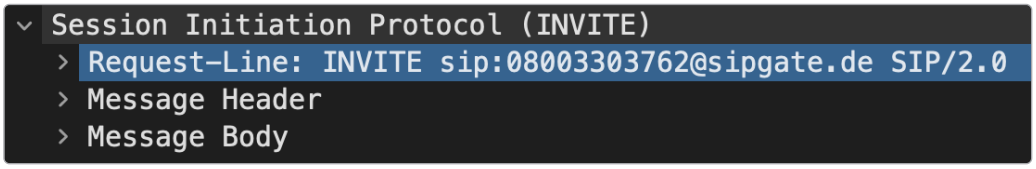

Bild 3: SIP-Nachrichtenaufbau (Screenshot aus Wireshark)

Antworten. Entity-Header stellen wiederum Informationen über den Typ, wie beispielsweise SDP oder XML für Presence und die Länge der Nachricht, dar. Request-Header beinhalten die Anforderung weiterer Informationen durch den SIP-Client. Beispiele dafür wären der Proxy-Authorization-Header zur Anforderung der Authentifizierung oder der Max-Forwards-Header, der die maximale Anzahl an Hops angibt, die die SIP-Nachricht passieren dürfen. Response-Header wie der Allow-Header liefern vonseiten des Servers Zusatzinformationen.

Nachfolgend stellen wir einige Header kurz zur Verdeutlichung ihrer Funktion vor.

2.1.2.1 To

Der To-Header dient der Angabe des Empfängers der SIP-Anfrage, also des Nutzers oder der Ressource. Dieser kann, muss aber nicht das finale Ziel der Anfrage sein. Neben der Angabe des Empfängers im SIP-URI-Schema kann auch ein Anzeigename im To-Header enthalten sein.

2.1.2.2 From

Der From-Header dient dazu, über die Identität des Initiators der SIP-Anfrage zu informieren. Wie auch beim To-Header enthält er zwingend eine SIP-URI als Adressierungsmerkmal und kann auch einen Anzeigenamen enthalten. **Bild 4** veranschaulicht dies beispielhaft.

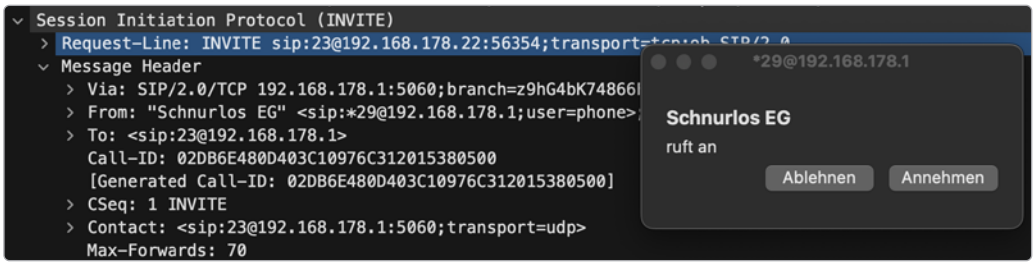

Bild 4: Screenshot einer Namensanzeige im Softphone und in Wireshark im From-Header

2.1.2.3 Call-ID

Der Call-ID-Header dient dazu, sämtliche Nachrichten innerhalb eines SIP-Dialogs zu identifizieren. Er muss für alle Anfragen und Antworten eines Dialogs gleich sein. Der Zweck eines SIP-Dialogs wird in Kapitel 3.1 dargestellt.

2.1.2.4 CSeq

Der CSeq-Header dient der Kennzeichnung der Reihenfolge von Transaktionen. Er enthält eine Sequenznummer für die Reihenfolge und die angewandte SIP-Methode.

2.1.2.5 Max-Forwards

Der Max-Forwards-Header dient der Angabe des SIP Hop Count. Dies stellt dar, wie viele SIP Hops eine Anfrage passieren darf. Bei jedem Hop verringert sich der Wert um 1, bevor der SIP-Proxy, bei dem die Anfrage mit dem Wert 0 ankommt, die Anfrage verwirft. Tritt ein solcher Fall auf, erkennen wir dies im Troubleshooting an der Antwort »483 Too Many Hops«.

2.1.2.6 Via

Der Via-Header gibt die Quelle der Anfrage an, also von welcher IP-Adresse und von welchem Port sie stammt sowie über welches Transportprotokoll die Anfrage versendet wurde.

2.1.2.7 Contact

Der Contact-Header enthält eine SIP-URI. Diese gibt die Adressierungsinformationen des Absenders an, die der Empfänger für nachfolgende Anfragen an den Absender nutzen kann.

2.1.2.8 Supported und Require

Diese Header geben unterstützte Erweiterungen des Clients an. Dadurch soll vermieden werden, dass der Server Erweiterungen an den Client übermittelt, die dieser nicht unterstützt.

2.1.2.9 Diversion und History Info

Zur Signalisierung, dass ein Anruf weitergeleitet wurde, können Diversion- und History-Info-Header dienen. Darin hinterlegt ein User Agent eine umleitende SIP-URI, um mitzuteilen, welches originäre Ziel den Anruf weitergeleitet hat. Dies kann dem Provider signalisieren, dass er einen ausgehenden Anruf von einer PBX auch annimmt, falls der User-Anteil in der SIP-URI im From-Header nicht einer Rufnummer des Rufnummernblocks des Kunden entspricht. In einem solchen SIP-INVITE können auch mehrere dieser Header enthalten sein, falls es zu einer verketteten Weiterleitung des Anrufs kam. Diese können auch den Grund für die Weiterleitung des Anrufs wie ein »486 Busy Here« enthalten. Diversion-Header stellen die ältere Implementierungsform dar, der History-Info-Header wird aber inzwischen von der IETF präferiert. Welche Variante der jeweilige Provider unterstützt, muss die Schnittstellenbeschreibung definieren. **Bild 5** zeigt ein Beispiel eines Diversion-Headers. Der Anruf von der Nebenstelle 29 an die 25 wurde in diesem Fall an die 23 weitergeleitet. Daher enthält der INVITE einen Diversion-Header mit der Information, dass die Rufnummer 25 den Anruf weitergeleitet hat.