

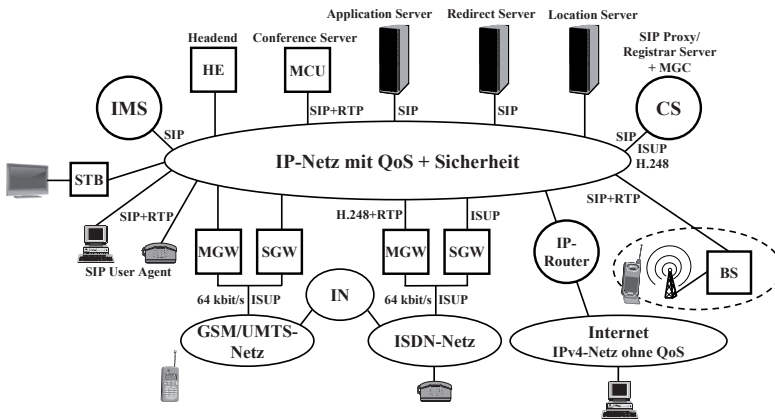


Ulrich Trick | Frank Weber

# SIP, TCP/IP und Telekommunikationsnetze

Next Generation Networks und VoIP – konkret

4. Auflage



Mit CD-ROM

Oldenbourg



---

# SIP, TCP/IP und Telekommunikations- netze

---

Next Generation Networks und VoIP – konkret

---

von  
Prof. Dr.-Ing. Ulrich Trick, Frank Weber

---

4., überarbeitete und erweiterte Auflage

---

Oldenbourg Verlag München

---

## 5.8 SIP-Basisabläufe und mögliche Anwendungen

In diesem Kapitel werden mögliche SIP-Kommunikationsabläufe anhand konkreter Anwendungen erläutert. Es ist anzumerken, dass bestimmte Basisabläufe wie z.B. der Auf- und Abbau einer Session durch die IETF einheitlich definiert sind [3261; 3665]. Allerdings gibt es bewusst Spielräume insbesondere in der Anwendung proprietärer Medienformen. Im Zweifelsfall sind die im Rahmen einer SIP-Kommunikationsinfrastruktur möglichen Anwendungsfälle also von der Unterstützung durch die SIP-Netzelemente abhängig, z.B. vom Typ der verwendeten User Agents bzw. den darin implementierten Applikationen.

### 5.8.1 VoIP (Voice over IP) – Audiokommunikation

Dies ist gewissermaßen die „Standard-Funktion“ unter den SIP-Anwendungen. Da hier lediglich der prinzipielle Ablauf verschiedener Kommunikationsweisen des SIP gezeigt werden soll, wird im folgenden Beispiel bewusst der einfachste Fall angenommen: eine „direkte Verbindung“ zwischen zwei SIP-Endsystemen ohne den Einsatz weiterer SIP-Netzelemente wie Proxy- und/oder Registrar Server. Komplexere Verbindungen unter Einbeziehung verschiedener Netzelemente werden in Kapitel 6 eingehend erläutert.

#### **Theoretische Beschreibung**

Für die direkte Kommunikation zwischen zwei SIP-User Agents ist es erforderlich, dass dem die Verbindung initiiierenden Endsystem die IP-Adresse des Zielsystems bekannt ist.

Im in Bild 5.8 dargestellten Beispiel wird – ausgehend von User Agent A – eine VoIP-Session zwischen den User Agents A und B aufgebaut und später durch User Agent B wieder beendet. Im Rahmen des SIP-Session-Aufbaus kommen die SIP-Anfragen INVITE, ACK und BYE (siehe Kapitel 5.2) sowie die Statusinformationen „100 Trying“, „180 Ringing“ sowie „200 OK“ (siehe Kapitel 5.3) zum Einsatz.

#### **Generelle Anmerkung zum Aufbau einer Session**

Die in Bild 5.8 mit unterbrochenen Pfeillinien gekennzeichneten provisorischen Statusinformationen „100 Trying“ und „180 Ringing“ sind für den Verbindungsaufbau nicht zwingend erforderlich (siehe Kapitel 5.3), auch wenn ihr Einsatz allgemein üblich ist. Obligatorisch hingegen ist der aus den drei Nachrichten „INVITE“, „200 OK“ und „ACK“ bestehende Initiierungsablauf, der als „SIP Three Way Handshake“ (siehe Kapitel 5.4) bezeichnet wird.

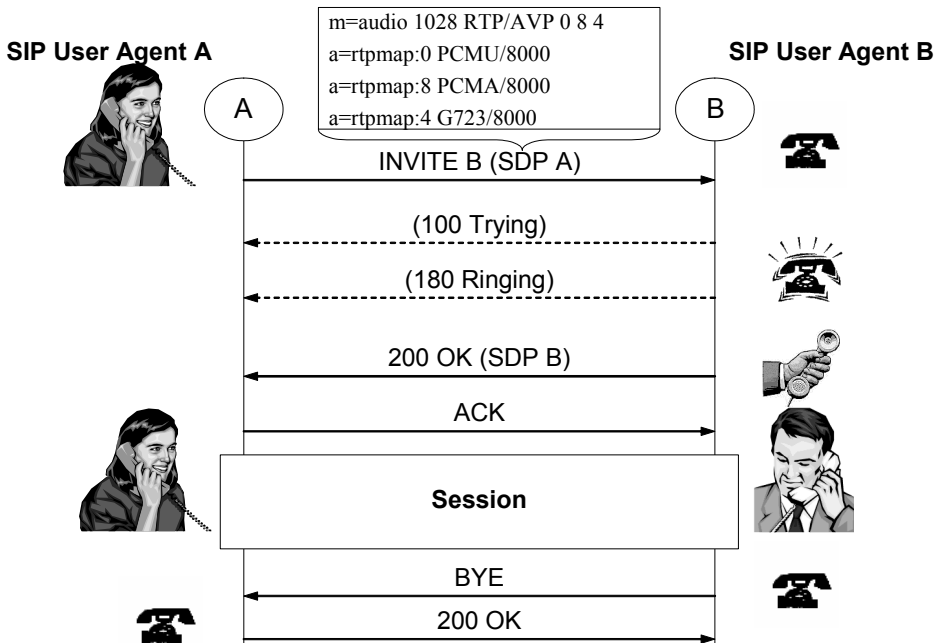


Bild 5.8: Session-Auf- und Abbau einer reinen Sprachverbindung zwischen zwei SIP-User Agents

Dass es sich bei dem in Bild 5.8 dargestellten Beispiel um eine VoIP-Session handelt, geht nur aus den im Rahmen des Three Way Handshakes ausgetauschten Elementen INVITE und „200 OK“ hervor, bzw. aus den in deren Message Bodys (siehe Kapitel 5.6) enthaltenen SDP-Anteilen (siehe Kapitel 5.7). In diesen gibt jeder Session-Teilnehmer unter Anwendung des SDP-Offer/Answer-Modells (siehe Kapitel 5.7.2) an, welches Medium (z.B. Audio, Video etc.) er empfangen kann und welche Codecs dazu verwendet werden können (siehe Kapitel 5.7.1). Ein Auszug aus dem im Message Body der INVITE-Anfrage enthaltenen SDP-Anteil ist in Bild 5.8 oberhalb der INVITE-Anfrage dargestellt.

Die Zeile „m=...“ (Media Descriptions, siehe Kapitel 5.7.1) besagt, dass der Sender dieses SDP-Inhalts ausschließlich Audio-Nutzdaten auf seinem UDP-Port 1028 empfangen kann. Er kann die im RTP-Audio-Video-Profil (RTP/AVP) [3551] festgelegten Codec-Typen 0, 8 und 4 decodieren. In den mit „a=...“ beginnenden Zeilen (Attributes, siehe Kapitel 5.7.1) werden diese Codecs rein informativ nochmals näher beschrieben: Der Codec-Typ 0 stellt eine PCM-Codierung nach dem  $\mu$ -Law-Prinzip dar, wobei eine Abtastfrequenz von 8000 Hz (8 kHz) vorgesehen ist. Der Codec-Typ 8 entspricht einer PCM-a-law-Codierung und der Codec-Typ 4 einer Codierung nach G.723, wobei auch hier jeweils eine Abtastfrequenz von 8000 Hz zu Grunde liegt.

Weitere Details über SDP und seine Parameter werden in Kapitel 5.7 eingehend erläutert.

### Praktisches Beispiel

Zur Veranschaulichung der obigen theoretischen Ausführungen soll nun eine SIP-Voice over IP-Session praktisch analysiert werden. Bild 5.9 zeigt den hierfür benötigten Versuchsaufbau.

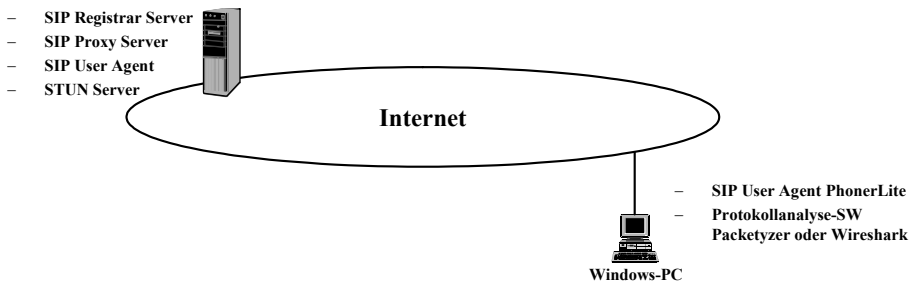


Bild 5.9: Testaufbau für praktische Beispiele zu SIP

Für die Durchführung des Versuchs wird ein am Internet betriebener PC mit Windows benötigt, auf dem die SIP User Agent-Software PhonerLite sowie eine Protokollanalyse-Software wie Packetyzer oder Wireshark installiert sind. Mittels PhonerLite kann eine SIP-Kommunikation mit einer öffentlichen SIP-Infrastruktur an der FH Frankfurt etabliert werden. Ein dort stationierter SIP Proxy/Registrar Server sorgt für die Weiterleitung der SIP-Nachrichten zu bzw. von einem automatisiert arbeitenden SIP User Agent.

Alle nötigen Informationen zur Installation, Konfiguration und Bedienung des SIP User Agents PhonerLite und von Packetyzer bzw. Wireshark können Kapitel 15 entnommen werden.

Um eine SIP-Voice over IP-Session aufzuzeichnen bzw. zu analysieren, sollte wie folgt vorgegangen werden.

1. Erforderlichenfalls Internet-Zugang des PCs aktivieren.
2. Protokollaufzeichnungsvorgang mit Packetyzer oder Wireshark starten.
3. SIP User Agent-Software PhonerLite starten.
4. Initiieren einer SIP-VoIP-Session mit dem automatisierten SIP User Agent an der FH Frankfurt. Geben Sie hierfür den Benutzernamen auto in das mit „Zielfrufnummer“ überschriebene Eingabefeld im rechten oberen Teil des PhonerLite-Hauptfensters ein. Klicken Sie dann auf die Schaltfläche mit dem diagonal angewinkelt dargestellten Hörersymbol (abgehobener (grüner) Hörer) unmittelbar unterhalb des Eingabefeldes. PhonerLite baut nun eine SIP-Session zum automatisierten SIP User Agent an der FH Frankfurt auf. Zum Beenden der Session klicken Sie auf die Schaltfläche mit dem waagrecht liegenden Hörersymbol (aufgelegter (roter) Hörer) unterhalb der Schaltfläche zum Initiieren einer Session.
5. Stoppen der Protokollaufzeichnung in Packetyzer bzw. Wireshark.

6. Speichern Sie die Aufzeichnungs-Session bei Bedarf ab.
7. Vergleichen Sie den SIP-Session-Ablauf (siehe Bild 5.10) mit der Theorie. Decodieren Sie bei Bedarf RTP und RTCP (siehe hierfür die praktischen Beispiele in Kapitel 4.2.6 (RTP) bzw. 4.2.7 (RTCP)). Vergleichen Sie des Weiteren die in den einzelnen SIP-Nachrichten enthaltenen SIP-Header-Felder und SDP-Anteile. Die Bilder 5.11 bis 5.14 zeigen Beispiele für die zwischen den beiden SIP User Agents ausgetauschten SIP-Nachrichten des SIP-Session-Aufbaus, jeweils mit detaillierter Auflösung der enthaltenen SIP-Header-Felder sowie der ggf. im Message Body enthaltenen SDP-Anteile. Die für den Session-Abbau relevanten Nachrichten sind beispielhaft in den Bildern 5.15 und 5.16 dargestellt.

Num	Source Address	Dest Address	Summary	Length
6612	192.109.234.123	192.109.234.124	SIP/SDP: Request: INVITE sip:auto@sip.fb2.fh-frankfurt.de,...	921
6613	192.109.234.124	192.109.234.123	SIP: Status: 100 trying -- your call is important to us	442
6614	192.109.234.124	192.109.234.123	SIP: Status: 180 ringing	442
6632	192.109.234.124	192.109.234.123	SIP/SDP: Status: 200 OK, with session description	808
6634	192.109.234.123	192.109.234.124	SIP: Request: ACK sip:194.94.81.201:5060	498
6635	192.109.234.123	194.94.81.201	RTCP: Sender Report	70
6636	192.109.234.123	194.94.81.201	RTP: Payload type=ITU-T G.711 PCMA, SSRC=23486, Seq...	214
6637	194.94.81.201	192.109.234.123	RTP: Payload type=ITU-T G.711 PCMA, SSRC=48643712, ...	214
6638	192.109.234.123	194.94.81.201	RTP: Payload type=ITU-T G.711 PCMA, SSRC=23486, Seq...	214
6639	194.94.81.201	192.109.234.123	RTP: Payload type=ITU-T G.711 PCMA, SSRC=48643712, ...	214
6640	192.109.234.123	194.94.81.201	RTP: Payload type=ITU-T G.711 PCMA, SSRC=23486, Seq...	214
6641	194.94.81.201	192.109.234.123	RTP: Payload type=ITU-T G.711 PCMA, SSRC=48643712, ...	214
6642	192.109.234.123	194.94.81.201	RTP: Payload type=ITU-T G.711 PCMA, SSRC=23486, Seq...	214
6643	194.94.81.201	192.109.234.123	RTP: Payload type=ITU-T G.711 PCMA, SSRC=48643712, ...	214
6644	192.109.234.123	194.94.81.201	RTP: Payload type=ITU-T G.711 PCMA, SSRC=23486, Seq...	214
...	...	...	...	...
13913	192.109.234.123	194.94.81.201	RTP: Payload type=ITU-T G.711 PCMA, SSRC=23486, Seq...	214
13914	194.94.81.201	192.109.234.123	RTP: Payload type=ITU-T G.711 PCMA, SSRC=48643712, ...	214
13915	194.94.81.201	192.109.234.123	RTP: Payload type=ITU-T G.711 PCMA, SSRC=48643712, ...	214
13916	192.109.234.123	194.94.81.201	RTP: Payload type=ITU-T G.711 PCMA, SSRC=23486, Seq...	214
13917	192.109.234.123	192.109.234.124	SIP: Request: BYE sip:194.94.81.201:5060	493
13921	192.109.234.124	192.109.234.123	SIP: Status: 200 OK	455

Bild 5.10: Ablauf einer SIP-Voice over IP-Session mit Session-Aufbau, bidirektionalem RTP-Nutzdatentransfer und Session-Abbau

## 7.2 Peer-to-Peer SIP

Bereits seit einigen Jahren erfreuen sich Peer-to-Peer-Anwendungen (P2P) im Internet, z.B. in Form von Online-Tauschbörsen für Musik- und Videodateien (File Sharing), großer Beliebtheit. Mit Skype (siehe Kapitel 3.2) wurde eine Möglichkeit zur Nutzung des Internet für komfortable Peer-to-Peer-Telefonie geschaffen, ohne dass dafür ein Dienstanbieter eine Vermittlungsinfrastruktur bereitstellen muss.

Obwohl SIP-Nachrichten prinzipiell auch ohne den Einsatz zentraler Vermittlungselemente direkt zwischen SIP User Agents ausgetauscht werden können (siehe Kapitel 7.1.2), wird in der Praxis meist von der Nutzung einer zentralen Vermittlungsinfrastruktur (bestehend aus SIP Proxy und -Registrar Servern; siehe Kapitel 6.2 und 6.3) ausgegangen. Der hauptsächliche Grund hierfür ist, dass die SIP-Endsysteme bei fehlender Vermittlungsinfrastruktur allein anhand ihrer temporären SIP URI (und somit letztendlich durch ihre IP-Adresse) identifiziert und kontaktiert werden können. Somit ist eine komfortable Teilnehmeradressierung mittels einer ständigen, unveränderlichen Kontaktadresse nicht ohne weiteres möglich (vgl. Kapitel 5.1.4). Des Weiteren sind wichtige praxisrelevante Eigenschaften wie die generelle Erreichbarkeit eines SIP User Agents auch über NAT (siehe Kapitel 8), die gesicherte Identitätsverifizierung (siehe Kapitel 12.1.1) sowie der Aufbau von Sessions über Gateways in andere Netze (z.B. ins PSTN; siehe Kapitel 6.7) ohne eine hierarchisch übergeordnete SIP-Vermittlungsinfrastruktur nur schwer realisierbar.

Die wesentlichste Aufgabe einer zentralen SIP-Vermittlungsinfrastruktur besteht also nicht in der Vermittlung der SIP-Nachrichten, sondern vielmehr in der Fähigkeit, den Zusammenhang zwischen der ständigen Kontaktadresse eines Teilnehmers und der temporären umgebungsabhängigen SIP URI des vom entsprechenden Teilnehmer benutzten Endsystems zu speichern und bei Bedarf anderen Netzelementen zur Verfügung zu stellen. Bereits seit einiger Zeit wird an verschiedenen Stellen mit zum Teil unterschiedlichen Ansätzen an der Entwicklung und Konkretisierung von Peer-to-Peer SIP-Ansätzen mit komfortabler Adressierung geforscht [P2PS]. Im Februar 2007 wurde innerhalb der IETF eine separate Working

Group gegründet, die die Standardisierung von Peer-to-Peer SIP zum Zweck hat [P2PS2]. Auch existieren bereits einige kommerzielle SIP-Kommunikationslösungen auf Peer-to-Peer-Basis.

Um die Peer-to-Peer-Fähigkeit von SIP zu nutzen und gleichzeitig nicht auf eine komfortable Adressierung sowie auf weitere Vorteile einer zentralen SIP-Vermittlungsinfrastruktur verzichten zu müssen, muss insbesondere die Funktion des Speicherns und Wiedergebens von Adresszusammenhängen unabhängig von zentralen Servern und demzufolge im Rahmen eines sog. Peer-to-Peer Overlay-Netzwerks bereitgestellt werden. Hierbei handelt es sich um einen virtuellen Zusammenschluss beliebig vieler Peers (Gleichgestellte) mit dem Ziel, einen bestimmten Dienst (z.B. SIP-Kontaktadressenverwaltung) möglichst ohne den Einsatz zentraler Instanzen (z.B. Server) anzubieten. Ein Peer im Sinne dieser Definition wird üblicherweise durch eine Software-Funktionalität auf dem Computer eines Nutzers des entsprechenden Dienstes repräsentiert, d.h. die Software zur Dienstenutzung (Client) stellt gleichzeitig auch anderen Nutzern Dienste bzw. Teile eines verteilt arbeitenden Dienstes zur Verfügung (Server). Es handelt sich bei einem Peer also im weitesten Sinne um eine Vereinigung eines Clients und eines Servers, weshalb in diesem Zusammenhang auch von einem sog. Servent gesprochen wird. Ein modernes Peer-to-Peer-Overlay-Netzwerk basiert meist auf sog. DHT (Distributed Hash Tables), die das systematische Ablegen und Auffinden beliebiger Daten (z.B. Adressierungsinformationen) auf mehreren Peers zum Zweck der verteilten Dienstbereitstellung ermöglichen [Sing1].

## 7.2.1 Grundkonzepte für Peer-to-Peer SIP-Infrastrukturen

Für die Kombination aus SIP-basierter Signalisierung und Peer-to-Peer-Overlay-basierter Kontaktadressenverwaltung können zwei prinzipielle Konzepte unterschieden werden: „SIP-using-P2P“ und „P2P-over-SIP“ [Sing2; Sing3]. Diese werden im Folgenden erläutert.

### **SIP-using-P2P**

Beim SIP-using-P2P-Konzept wird ein herkömmliches Peer-to-Peer-Overlay-Netzwerk (basierend z.B. auf OpenDHT [ODHT], Chord [Chor] oder JXTA [JXTA; Ezzo; Webe1]) verwendet, um den Zusammenhang zwischen der ständigen Kontaktadresse eines Teilnehmers und der temporären umgebungsabhängigen SIP URI des von ihm benutzten SIP-Endsystems zu verwalten. Das Endsystem eines anderen Teilnehmers fragt bei Bedarf die im Peer-to-Peer-Overlay-Netzwerk abgelegten Informationen mittels des entsprechenden Peer-to-Peer-Protokolls ab und kann anschließend das Endsystem des gewünschten Teilnehmers per SIP direkt kontaktieren. Bild 7.9 zeigt beispielhaft das Anwendungsprinzip des SIP-using-P2P-Ansatzes. Unter Anwendung eines entsprechenden Protokolls wird der User Agent des Teilnehmers B im P2P-Netzwerk angemeldet, d.h., der Zusammenhang des Teilnehmersnamens (hier: B) und der IP-Adresse des Endsystems (hier: IP 89.89.89.89) wird innerhalb des P2P-Netzwerks abgelegt (siehe Schritt (1)). Das Endsystem des Teilnehmers A, der eine P2P SIP-Session zu Teilnehmer B aufbauen möchte, erfragt im P2P-Netzwerk mit Hilfe des entsprechenden P2P-Protokolls die benötigte Information (IP-Adresse des SIP-Endsystems von Teilnehmer B; siehe Schritt (2)). Der Zusammenhang zwischen dem Namen des Teilnehmers

(B) und der IP-Adresse des von B benutzten Endsystems wird User Agent A in Schritt (3) mitgeteilt. User Agent A verwendet die erhaltene Information in Schritt (4) zur Übermittlung einer SIP-INVITE-Anfrage direkt an die temporäre SIP URI von User Agent B, ohne Einbeziehung eines weiteren SIP-Netzelements (z.B. eines SIP Proxy Servers).

Zum Zeitpunkt der Drucklegung dieses Buches wird das SIP-using-P2P-Konzept als Basis für die Peer-to-Peer SIP-Standardisierung angesehen (siehe Kapitel 7.2.2).

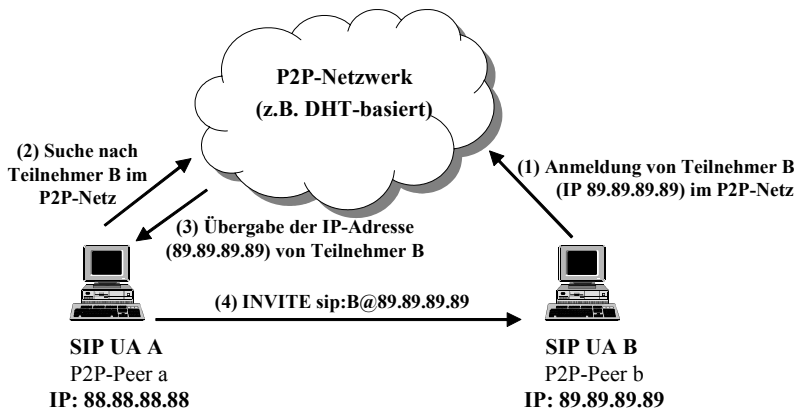


Bild 7.9: Anwendungsprinzip des SIP-using-P2P-Ansatzes für Peer-to-Peer-SIP

### P2P-over-SIP

Im Gegensatz zu „SIP-using-P2P“ wird für die Anwendung des P2P-over-SIP-Konzepts kein zusätzliches Protokoll für die Kommunikation der Peer-to-Peer SIP User Agents mit einem Peer-to-Peer-Overlay-Netzwerk benötigt. Vielmehr handelt es sich bei den das Peer-to-Peer-Overlay-Netzwerk bildenden Funktionen um Sonderformen spezialisierter SIP-Netzelemente (z.B. SIP Registrar Server, Location Server, Redirect Server), die die für das komfortable Auffinden von Nutzern benötigte Funktionalität zur Verfügung stellen. Demzufolge werden auch die für die Organisation des Peer-to-Peer-Overlay-Netzwerks nötigen Informationen in Form von SIP-Nachrichten ausgetauscht.

Bild 7.10 zeigt beispielhaft das Anwendungsprinzip des P2P-over-SIP-Ansatzes. SIP-Nachrichten der Methode ACK werden aus Gründen der Übersichtlichkeit bewusst nicht dargestellt.

Der User Agent des Teilnehmers B registriert sich per SIP-Anfrage REGISTER im SIP-basierten Peer-to-Peer-Overlay-Netzwerk (siehe Schritt (1)). Dabei wird der Zusammenhang des Teilnehmernamens (hier: B) und der IP-Adresse des Endsystems (hier: IP 89.89.89.89) innerhalb des Peer-to-Peer-Overlay-Netzwerks abgelegt. Das Endsystem des Teilnehmers A, der eine P2P SIP-Session zu Teilnehmer B aufbauen möchte, sendet in Schritt (2) die an

User Agent B gerichtete SIP-INVITE-Anfrage an einen Peer innerhalb des SIP-basierten Peer-to-Peer-Overlay-Netzwerks und erhält in Schritt (3) im Contact-Header-Feld der SIP-Statusinformation „302 Moved Temporarily“ die gesuchte temporäre SIP URI des Teilnehmers B (hier: sip:B@89.89.89.89). User Agent A richtet daraufhin in Schritt (4) eine weitere INVITE-Anfrage direkt an User Agent B.

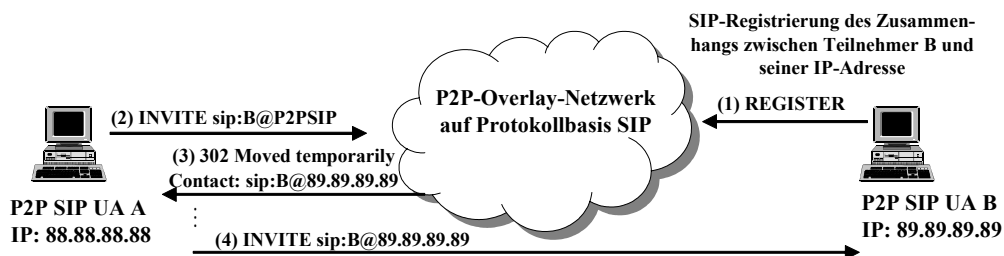


Bild 7.10: Mögliches Anwendungsprinzip des P2P-over-SIP-Ansatzes für Peer-to-Peer-SIP

## 7.2.2 Peer-to-Peer SIP-Standardisierung

Die IETF-Working Group „Peer-to-Peer Session Initiation Protocol (P2PSIP)“ [P2PS2] hat sich zum Ziel gesetzt, Konzepte, Einsatzgebiete sowie eine einheitliche Terminologie für SIP-basierte Kommunikationsinfrastrukturen auf Peer-to-Peer-Basis zu standardisieren. Hierbei wird von einem SIP-using-P2P-Konzept (siehe Kapitel 7.2.1) ausgegangen, d.h., das Management des für die SIP-Adressierungsverwaltung benötigten Peer-to-Peer Overlay-Netzwerks erfolgt unabhängig von der SIP-Signalisierung zwischen den SIP User Agents der Teilnehmer. Um beliebige Peer-to-Peer-Algorithmen (z.B. Chord [Chor] oder OpenDHT [ODHT]) zur Bildung einer verteilten Adressierungsverwaltung einsetzen zu können, wird durch die P2PSIP Working Group ein neuartiger Protokoll- und Architekturansatz namens RELOAD (REsource LOcation And Discovery) [Jenn1] entwickelt.

### RELOAD (REsource LOcation And Discovery)

RELOAD ist prinzipiell ein aus mehreren logischen Funktionskomponenten (z.B. Datenspeicherung, Datentransport etc.) bestehendes virtuelles System zur Verwaltung von Daten für Protokollanwendungen in Peer-to-Peer Overlay-Netzen. Eine solche Protokollanwendung stellt beispielsweise die Verwaltung, d.h. das Ablegen, Suchen und Weitergeben von Zusammenhängen zwischen Benutzernamen und temporären SIP URIs innerhalb einer Peer-to-Peer SIP-Infrastruktur dar. Somit ist ein RELOAD-System geeignet, die wesentlichste Aufgabe einer üblicherweise zentral angesiedelten SIP-Vermittlungsinfrastruktur auf Peer-to-Peer-Basis zu übernehmen. Das RELOAD-System wird in seiner Gesamtfunktionalität auf

alle Peers eines auf einem beliebigen Peer-to-Peer-Algorithmus basierten Overlay-Netz verteilt.

RELOAD stellt also ein universelles Bindeglied dar zwischen beliebigen Peer-to-Peer-Algorithmen einerseits und beliebigen Anwendungsprotokollen andererseits, die auf verteilt abzulegende Informationen (in Falle von SIP also Adressierungsinformationen) angewiesen sind. Neben Bildung und Management einer verteilten Infrastruktur, die das zuverlässige Ablegen sowie das schnelle Auffinden von Datenzusammenhängen in einem Peer-to-Peer Overlay-Netzwerk ermöglichen, bietet RELOAD gemäß [Jenn1] zusätzlich folgende Funktionen.

- Sicherheits-Framework: Durch einen zentralen Server werden Zertifikate für alle an der Datenhaltung und -abfrage beteiligten Peers vergeben, so dass jeder Peer, der eine Operation (z.B. eine Adressenabfrage) innerhalb des Peer-to-Peer-Netzwerks einleitet, authentifiziert werden kann.
- Anwendungsfall-Modellierung: RELOAD ist nicht auf die Anwendung mit SIP beschränkt. Durch entsprechende Dokumentationsvorgänge kann RELOAD auch für die Bildung von Peer-to-Peer-Infrastrukturen für andere Protokolle (z.B. XMPP (Extensible Message and Presence Protocol) [3920] eingesetzt werden. [Jenn2] beschreibt den entsprechenden Anwendungsfall für den Einsatz von RELOAD mit SIP.
- NAT-Überwindung: Durch integrierte NAT-Überwindungsfunktionen wie z.B. ICE (siehe Kapitel 8.3.4) kann RELOAD auch eingesetzt werden, wenn viele beteiligte Peers hinter NAT Gateways bzw. Firewalls angesiedelt sind. Die integrierten NAT-Überwindungsmechanismen unterstützen sowohl die RELOAD-interne Kommunikation beim Auffinden von gesuchten Peers als auch das mit der jeweiligen RELOAD-Umgebung assoziierte Anwendungsprotokoll (z.B. SIP).
- Ressourcenschonendes Overlay-Signalisierungsprotokoll: In einem Peer-to-Peer Overlay-Netzwerk sind Peers naturgemäß an der Weiterleitung von Informationen zwischen anderen Peers beteiligt. Das Weiterleiten von Informationen beansprucht jedoch sowohl Netzwerk- als auch Verarbeitungsressourcen des routenden Peers. Aus diesem Grund wurde das RELOAD-Signalisierungsprotokoll bezüglich seines Bandbreitenbedarfs sowie hinsichtlich des für die Verarbeitung erforderlichen Rechenaufwandes optimiert, so dass am Routing beteiligte RELOAD Peers (und somit die Rechner der am jeweiligen Peer-to-Peer-Netzwerk angemeldeten Teilnehmer) nicht unnötig belastet werden.
- Schnittstelle für Overlay-Algorithmen: Es existiert heute eine Vielzahl verschiedener Peer-to-Peer Overlay-Algorithmen. Um einen für den jeweiligen Anwendungsfall optimalen Algorithmus in das entsprechende Peer-to-Peer Overlay-Netzwerk integrieren zu können, bietet RELOAD eine entsprechende Schnittstelle zur Einbindung von unstrukturierten sowie DHT-basierten strukturierten Overlay-Algorithmen. Zur Sicherstellung der Interoperabilität zwischen verschiedenen RELOAD-basierten Peer-to-Peer-Netzwerken ist Chord [Chor] als Default-Algorithmus vorgesehen.

Da sich die Standardisierungsarbeiten zu P2PSIP und RELOAD noch in regem Fluss befinden, wird bezüglich weiterer Informationen an dieser Stelle auf die entsprechenden IETF-Drafts [Jenn1; Jenn2] bzw. deren Nachfolgeversionen verwiesen. Aktuelle Informationen

über die generelle Fortentwicklung in der Peer-to-Peer SIP-Standardisierung sind unter [P2PS2] zu finden.

## 13.2 UMTS-Mobilfunknetze

Die zellularen Mobilfunknetze der IMT-2000-Familie (International Mobile Telecommunications at 2000 MHz) und damit auch UMTS wurden und werden so spezifiziert, dass für die bestehenden Systeme ein Investitionsschutz gegeben ist. Das bedeutet im Falle von UMTS nicht nur, dass es einen direkten Migrationspfad von GSM/GPRS (General Packet Radio Service) zu UMTS gibt, sondern dass es, wie in den Tabellen 13.2 [Rel99; Rel4; Rel5], 13.3 [Rel6; Rel7; Rel8] und 13.4 [Rel9; Rel10] übersichtlich dargestellt, auch mehrere aufeinander aufbauende UMTS-Versionen gibt bzw. geben wird. Gemäß Tabelle 13.2 ist der Ausgangspunkt das Release 99. Es basiert auf dem GSM/GPRS-Kernnetz, ergänzt um ein im Vergleich zu GSM deutlich leistungsfähigeres Zugangnetz UTRAN (Universal Terrestrial Radio Access Network). Im Wesentlichen sind heute im UMTS-Wirkbetrieb Release 99-Netze im Einsatz, zunehmend aber auch schon Release 4-Netze. UMTS Release 4 zeichnet sich vor allem durch die Trennung der Verbindungssteuerung vom Nutzdatentransport aus. In der Realisierung zeigt sich das durch die Aufspaltung des bisher monolithischen MSC in einen MSC-Server für die Signalisierung und Media Gateways (MGWs) für die Nutzdaten. Wegen der hohen Bedeutung des NGN-Kennzeichens 4 „Trennung der Verbindungs- und Dienststeuerung“ vom Nutzdatentransport“ (siehe Kapitel 3.1) ist somit UMTS Release 4 durchaus ein wichtiger Schritt auf dem Weg zu einem NGN-konformen UMTS-Netz. UMTS Release 5 schließlich, das im Folgenden noch detaillierter beschrieben wird, setzt dann durch die Einführung des SIP-basierten IMS (IP Multimedia Subsystem) für die Multimediakommunikation weitgehend das NGN-Konzept um. Zudem bietet es durch die Erweiterung mit HSDPA (High Speed Downlink Packet Access) wesentliche Verbesserungen, was die Downstream-Bitraten (bis zu 14,4 Mbit/s) im Zugangnetz angeht.

Die auffälligsten neuen Funktionen bei UMTS Release 6 sind Multimedia Broadcast and Multicast Services (MBMS), die Einbindung von WLAN-Zugangnetzen und mit HSUPA (High Speed Uplink Packet Access) deutlich erhöhte Upstream-Bitraten (bis zu 5,8 Mbit/s) im UTRAN. Zudem wird hier, im Unterschied zu Release 5, davon ausgegangen, dass „normale“ Telefonate nicht grundsätzlich über MSCs bzw. MSC-Server und MGWs laufen müssen, sondern auch via IMS (Voice over IMS) realisiert werden können.

Tabelle 13.2: UMTS Releases 99, 4 und 5

Release 99 [Rel99]	Release 4 [Rel4]	Release 5 [Rel5]
<ul style="list-style-type: none"> <li>• März 2000 [3GPPr]</li> <li>• Kernnetz wie bei GSM + GPRS</li> <li>• Zugangnetz UTRAN (Universal Terrestrial Radio Access Network) + GERAN (GSM/EDGE Radio Access Network)</li> <li>• Höhere Datenraten, bis ca. 2 Mbit/s</li> <li>• USIM (UMTS Subscriber Identity Module)</li> <li>• AMR Codec (Adaptive Multi-Rate), 3,4 kHz</li> <li>• MMS (Multimedia Messaging Service)</li> <li>• Location Services</li> <li>• MExE (Mobile Station Execution Environment)</li> <li>• CAMEL (Customized Applications for Mobile network Enhanced Logic) Phase 3</li> <li>• OSA (Open Service Access)</li> <li>• Inter Network Roaming</li> </ul>	<ul style="list-style-type: none"> <li>• März 2001 [3GPPr]</li> <li>• Release 99 +</li> <li>• Trennung von Signalisierung und Nutzdaten im Kernnetz</li> <li>• Statt MSC MSC-Server + MGWs</li> <li>• ZGS Nr.7 over SIGTRAN (SIGNalling TRANsport)</li> <li>• QoS-Architektur für PS Domain (Packet Switched)</li> <li>• MMS-Erweiterungen</li> <li>• Location Services-Erweiterungen</li> <li>• MExE-Erweiterungen</li> <li>• OSA-Erweiterungen</li> <li>• Security-Erweiterungen</li> <li>• Inter Release Roaming</li> </ul>	<ul style="list-style-type: none"> <li>• Juni 2002 [3GPPr]</li> <li>• Release 4 +</li> <li>• NGN-Konzept</li> <li>• Kernnetz mit IP Multimedia Subsystem (IMS)</li> <li>• Multimedia over IP</li> <li>• SIP</li> <li>• HSDPA (High Speed Downlink Packet Access), höhere Datenraten, bis zu 14,4 Mbit/s downstream</li> <li>• Ende-zu-Ende QoS</li> <li>• UTRAN mit IP-Transport</li> <li>• 1 x RNC an N x MSC/SGSN</li> <li>• Wideband AMR, 7 kHz</li> <li>• MMS-Erweiterungen</li> <li>• Location Services-Erweiterungen</li> <li>• MExE-Erweiterungen</li> <li>• CAMEL Phase 4</li> <li>• OSA-Erweiterungen</li> <li>• Security-Erweiterungen</li> </ul>

Release 7 hat als wichtigste Aufgabe die Klammerfunktion zu den Festnetzen. Hier wurden die notwendigen IMS-Erweiterungen für ETSI TISPAN NGN Release 1 und 2 (siehe Kapitel 13.4) sowie PacketCable-basierte HFC-Netze (siehe Kapitel 10) eingebracht. Zudem werden mit HSPA+ (High Speed Packet Access Plus) die Bitraten im UTRAN nochmals bis auf max. 42 Mbit/s downstream und 22 Mbit/s upstream erhöht. Release 8 schließlich repräsentiert wie bereits Release 5 wieder einen größeren Netzentwicklungsschritt. Die Standardisierung zu LTE (Long Term Evolution) spezifiziert zukünftige UMTS-Zugangnetze E-UTRAN (Evolved-UTRAN) mit Bitraten bis zu 100 Mbit/s in Downlink- und 50 Mbit/s in Uplink-Richtung. Die Arbeiten zur SAE (System Architecture Evolution) brachten eine neue Kernnetzarchitektur hervor mit dem Ziel, unterschiedlichste Funkzugangnetze wie z.B. E-UTRAN, aber auch feste Teilnehmeranschlüsse an das UMTS-Kernnetz anbinden zu können, möglichst einfach und ohne Einbeziehung des GPRS (siehe Kapitel 13.9).

Tabelle 13.3: UMTS Releases 6, 7 und 8

Release 6 [Rel6]	Release 7 [Rel7]	Release 8 [Rel8]
<ul style="list-style-type: none"> <li>• März 2005 [3GPPr]</li> <li>• Release 5 +</li> <li>• MBMS (Multimedia Broadcast and Multicast Services)</li> <li>• WLAN/UMTS Interworking</li> <li>• IMS Phase 2</li> <li>• Voice over IMS</li> <li>• HSUPA (High Speed Uplink Packet Access), höhere Datenraten, bis zu 5,8 Mbit/s upstream</li> <li>• HSDPA-Verbesserungen</li> <li>• Presence</li> <li>• Push Services</li> <li>• Packet Switched Streaming Services</li> <li>• Dienste mit Spracherkennung</li> <li>• MMS-Erweiterungen</li> <li>• Location Services-Erweiterungen</li> <li>• MExE-Erweiterungen</li> <li>• CAMEL-Erweiterungen</li> <li>• OSA-Erweiterungen, Parlay X Web Services</li> <li>• Security-Erweiterungen</li> <li>• Digital Rights Management</li> </ul>	<ul style="list-style-type: none"> <li>• Dezember 2007 [3GPPr]</li> <li>• Release 6 +</li> <li>• IMS-Erweiterungen für TISPAN NGN Release 1 und 2 sowie PacketCable</li> <li>• Notruf via IMS</li> <li>• Voice Group Call Services (VGCS) für Polizei, Feuerwehr etc.</li> <li>• MBMS-Erweiterungen</li> <li>• WLAN/UMTS Interworking Phase 2</li> <li>• Multiple Input Multiple Output Antennas (MIMO)</li> <li>• RAN-Verbesserungen (Radio Access Network): HSPA+ (High Speed Packet Access Plus), bis zu 42/22 Mbit/s down-/upstream [Lesc2]</li> <li>• Location Services-Erweiterungen</li> <li>• OSA-Erweiterungen</li> <li>• Security-Erweiterungen</li> </ul>	<ul style="list-style-type: none"> <li>• Dezember 2008 [3GPPr]</li> <li>• Release 7 +</li> <li>• SAE (System Architecture Evolution) für Kernnetz</li> <li>• IMS-Erweiterungen, u.a. für Packet Cable und Corporate Network Access, Packet-switched Streaming Services (PSS) und Multimedia Broadcast/Multicast Services (MBMS)</li> <li>• Earthquake (Erdbeben) and Tsunami Warning System (ETWS)</li> <li>• Multimedia Priority Service</li> <li>• LTE (Long Term Evolution) für Zugangsnetz (Evolved- bzw. E-UTRAN), bis zu 100/50 Mbit/s down-/upstream</li> <li>• RAN-Verbesserungen</li> <li>• OSA-Erweiterungen</li> <li>• Security-Erweiterungen</li> </ul>

Die noch zukünftigen Releases 9 und 10 befinden sich Anfang 2009 noch mitten (Release 9) bzw. erst am Anfang (Release 10) der Standardisierung (siehe Tabelle 13.4). Release 9 wird als interessanteste Neuerungen die Unterstützung von Personal Area Networks (PAN) und vor allem als Schritt in Richtung Active Networks (siehe Kapitel 13.9) selbstoptimierende und -heilende Netze (Self-Organizing Networks (SON)) bieten. SON-unterstützende Netzknoten sollen in UMTS Release 9 auf Basis von Eigenüberwachung (Auswertung von Performance-Messwerten und Alarmen, Durchführung von Selbsttests) und Analyse bei Bedarf selbst korrigierend eingreifen, um eigenständig Probleme zu lösen [Rel9]. Während die Releases 99 bis 9 die menschliche mobile Kommunikation in den Mittelpunkt stellten, wird Release 10 u.a. einen Schwerpunkt auf die Kommunikation von und mit Maschinen/Geräten (Machine-to-Machine (M2M) communication) legen, z.B. für Autohersteller und ausgelieferte Fahrzeuge oder für die Fernsteuerung von Heizung, Alarmsystemen etc. im Haushalt [Rel10]. Zudem wird unter der Überschrift „LTE Advanced“ eine noch leistungsfähigere Zugangstechnik, die der 4. Mobilfunkgeneration, spezifiziert (siehe Kapitel 13.9) [REV0; Seid].

Tabelle 13.4: UMTS Releases 9 und 10

Release 9 [Rel9]	Release 10 [Rel10]
<ul style="list-style-type: none"> <li>• Ca. Dezember 2009 [3GPPr]</li> <li>• Release 8 +</li> <li>• Dienstebgleich und Migration bez. CS und IMS</li> <li>• IMS-Erweiterungen, u.a. für Burst-artige Registrierungen, Home Node B, Anti-SPIT</li> <li>• Öffentliches Warnsystem</li> <li>• Erweiterungen zu Multimedia Priority Service</li> <li>• Unterstützung von Personal Area Networks (PAN)</li> <li>• Selbstoptimierende und -heilende Netze (Self-Organizing Networks (SON))</li> <li>• LTE-Verbesserungen</li> <li>• RAN-Verbesserungen</li> <li>• Location Services-Erweiterungen</li> <li>• Security-Erweiterungen</li> </ul>	<ul style="list-style-type: none"> <li>• Release 9 +</li> <li>• Netzoptimierung für die Kommunikation von und mit Maschinen/Geräten (Machine-to-Machine (M2M) communication), z.B. für Autohersteller, Haushalt</li> <li>• LTE Advanced [REV0], bis zu 1000/500 Mbit/s down-/upstream</li> </ul>

Wie bereits in Tabelle 13.2 angedeutet bietet UMTS Release 9 im Wesentlichen nur eine neue, leistungsfähigere Zugangstechnik, das UTRAN (Universal Terrestrial Radio Access Network) [25401]; im Kernnetz wird weiter die GSM- und GPRS-Technik genutzt [100522], die Sprachkommunikation erfolgt nach wie vor leitungsvermittelt. Erst Release 10 stellt im Sinne der Netztechnik eine echte Innovation dar. Hier wurden die Ideen des NGN-Konzepts mit seinen Vorteilen bei den Kosten und der Zukunftsfähigkeit eines Telekommunikationsnetzes weitgehend berücksichtigt. Entstanden ist eine komplette QoS-IPv6-basierte [23221], mit Hilfe von SIP [4083] Echtzeitmultimediatelekommunikation unterstützende Kommunikationsinfrastruktur mit umfassender Mobilitätsunterstützung. Die Bilder 13.15 und 13.16 zeigen den prinzipiellen Aufbau eines solchen Netzes. Ein Vergleich mit den Bildern 3.1 und 3.3 (siehe Kapitel 3) verdeutlicht die Zusammenhänge mit dem NGN-Konzept.

## 13.7 Dienstentwicklung und -bereitstellung

Wie bereits im Zusammenhang mit der Erläuterung des SIP-Netzelements Application Server in Kapitel 6.12 angesprochen, besteht in der Zukunft bei den Netzbetreibern und Diensteanbietern ein großer Bedarf, schnell, einfach und kostenoptimiert neue Dienste, sog. Mehrwertdienste anbieten zu können. Hauptgrund hierfür ist, dass mit normalen Telefongesprächen kaum noch Einnahmen erzielt werden können und daher auf Basis der durch NGN (Next Generation Networks) gegebenen neuen Dienstmöglichkeiten neue Einnahmequellen erschlossen werden müssen. Zudem entstehen bei den Kunden durch die zukünftig in diesem Bereich prinzipiell unbegrenzten technischen Möglichkeiten auch neue Kommunikationsbedürfnisse. Daher ist es für Netzbetreiber und Dienste-Provider außerordentlich wichtig, leistungsfähige Dienstplattformen, sog. Service Delivery-Plattformen, zur Verfügung zu haben, mit denen in kürzester Zeit und mit geringstem Aufwand neue Anwendungen entwickelt und im Markt eingeführt werden können.

Obwohl der Begriff „Service Delivery Platform (SDP)“ in der Literatur häufig verwendet wird, sind die zu findenden Definitionen in vielen Punkten unklar bzw. unzureichend. Daher wird im Folgenden eine in [Lehm2] erarbeitete Konkretisierung wiedergegeben:

Eine „Service Delivery Platform“ ist eine einheitliche, standardisierte und skalierbare Software-Architektur zur Entwicklung, Bereitstellung und Integration von Mehrwertdiensten. Sie ist Teil des Application Layer. Über Abstraktionsschnittstellen ist sie mit den darunter liegenden Call Control- und Transport-Schichten verbunden. Dadurch wird die Komplexität dieser Layer verborgen und ein einfacher Zugriff auf Netzfunktionen wie z.B. Basisdienste (vgl. IMS) ermöglicht. Die angebotenen Mehrwertdienste können selbst bereitgestellt oder von Drittanbietern bezogen werden, zudem ermöglicht die SDP eine Dienstekomposition. Darüber hinaus stellt sie Standardschnittstellen zu SCE (Service Creation Environment), AAA-Server, OSS (Operations Support System, Netz- bzw. Service Management) und BSS (Business Support System, Management von Geschäftsprozessen) bereit.

Zur Veranschaulichung dieser Definition dient Bild 13.58. Hieraus geht auch die besondere Bedeutung des die SDP ergänzenden Service Creation Environment (SCE) hervor. Eine SCE stellt eine Entwicklungsumgebung zur Verfügung, mit deren Hilfe von Grund auf oder aus vorgefertigten Modulen (z.B. bereits existierenden Diensten) Mehrwertdienste entwickelt und konfiguriert werden können. Dabei werden die Entwickler üblicherweise durch grafische

Werkzeuge unterstützt. Infolge der Anbindung des SCE an die SDP können neue Mehrwertdienste im Netz unmittelbar bereitgestellt werden. Diesen Vorgang nennt man Deployment [Lehm3].

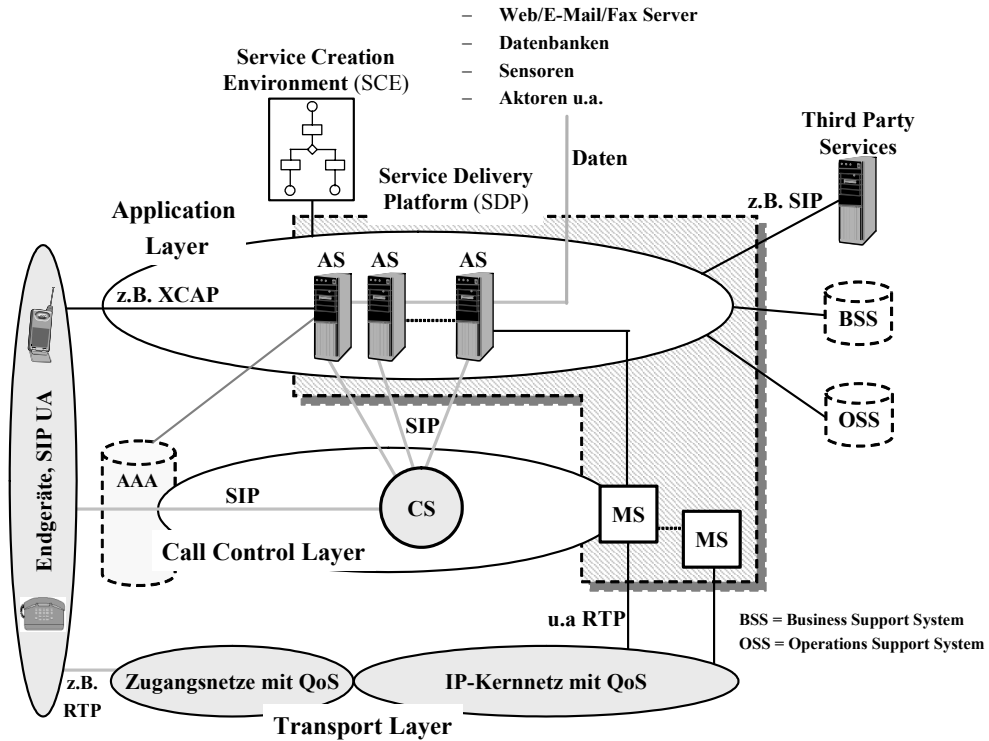


Bild 13.58: Service Delivery Platform (SDP)

Bild 13.58 verdeutlicht darüber hinaus, dass Media Server (MS) für die Nutzdatenverarbeitung ebenfalls zur SDP gehören, was zur Folge hat, dass Teile der SDP auch im Call Control und Transport Layer angesiedelt sind. Die eigentlichen SDP-Kernelemente für die Dienstebereitstellung sind aber die bereits in Kapitel 6.12 erläuterten Application Server. Daher sind zur Vertiefung in Bild 13.59 die Funktionen eines SIP Application Servers inkl. möglicher Funktionalitäten der Media Server herausgearbeitet. Hieran wird auch nochmals deutlich, welche ungeheuren Möglichkeiten bez. der Dienstentwicklung und -bereitstellung eine SIP/IP-basierte Service Delivery Platform bietet.

Für die Dienstentwicklung und -bereitstellung mittels SCE und SDP existieren verschiedene Lösungen, die anhand der vorhandenen Programmierschnittstellen in zwei Gruppen unterteilt werden können. Mit „Low Level API“ (Application Programming Interface) werden jene Techniken gekennzeichnet, die direkt auf Servern ausgeführt werden. Dagegen setzt das

„High Level API“ auf Middleware auf, d. h. auf einer die Eigenheiten und Komplexität des darunter liegenden Netzes vor den Anwendungen verbergenden zusätzlichen Software-Schicht.

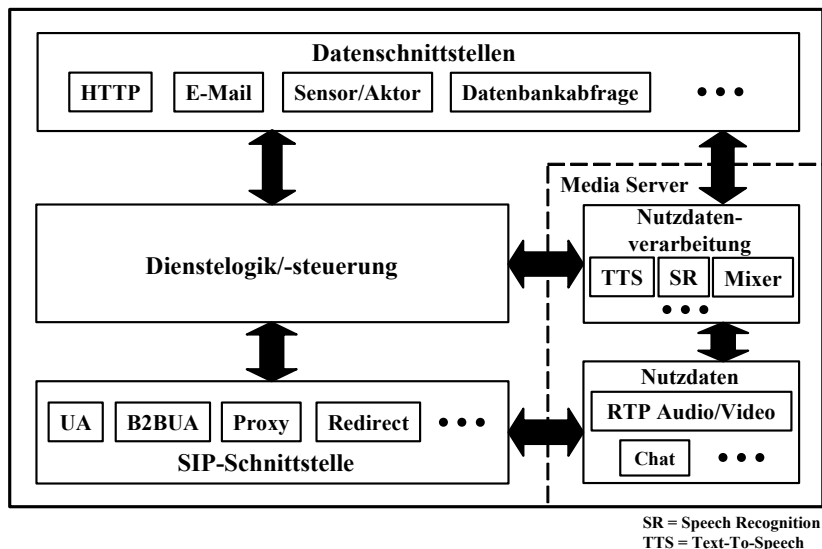


Bild 13.59: Funktionen eines SIP Application Servers

Zu den Lösungen mit Low Level API gehören

- SIP Servlets,
- CPL (Call Processing Language),
- SIP-CGI (Common Gateway Interface),
- JAIN (Java API for Integrated Networks),
- Scripting oder Software in C, C++, .NET oder Java,
- proprietäre APIs, beispielsweise Skype-API.

Lösungen mit High Level API sind

- JAIN SLEE (Service Logic Execution Environment),
- Parlay/OSA (Open Service Access) und Parlay X,
- CSE (CAMEL Service Environment),
- Web Services und SOA (Service Oriented Architecture)
- OSE (OMA Service Environment).

Auf die oben genannten proprietären APIs soll im Folgenden nicht näher eingegangen werden, da sie nicht auf offenen Standards basieren. Reine Scripting- bzw. Software-Lösungen

sind zu unflexibel, nicht plattformunabhängig bzw. nicht standardisiert und werden daher hier auch nicht näher beleuchtet [Lehm3].