

7 Session Initiation Protocol (SIP)

7.1 Übersicht

Das Internet arbeitet verbindungslos. Jede Kommunikation steht für sich, es gibt keine Garantie für bestimmte Verbindungseigenschaften und keine Verbindungsbeziehungen im Transportnetz. Jedes IP-Paket muss sich unabhängig von anderen Paketen seinen Weg durch das Netz suchen. Für die typischen Datenanwendungen war dieser Mechanismus optimal und garantierte eine schnelle Reaktion und optimal genutzte Verkehrskapazitäten. Zur Unterstützung von Echtzeitverbindungen, wie Sprache oder Online-Gaming, ist die Einhaltung von bestimmten Netzeigenschaften sehr wichtig. Werden bestimmte Paketlaufzeiten überschritten oder kommt es vermehrt zu Paketverlust, wird die Nutzung des Dienstes beeinträchtigt. Die übertragene Sprache bleibt dann unverständlich, oder der Bildaufbau findet verzögert statt. Der IP-Verkehr zeigt selbstähnliche Eigenschaften, die auch bei relativ geringen Auslastungen bereits große Wartezeiten verursachen. Für eine wirtschaftliche Unterstützung von Echtzeitverbindungen ist daher die Zuordnung Bandbreiten und die Überwachung der Verbindungseigenschaften (Quality of Service – QoS) notwendig. Mit einem entsprechenden QoS im Transportnetz können die Netzelemente und Leitungen deutlich höher ausgelastet werden also ohne diese Maßnahmen (vergl. Abschnitt zu QoS).

Verbindungen im
Internet

Innerhalb der IETF wurde eine Reihe von Protokollen zur Unterstützung von Multimediaverbindungen auf Basis des Internetprotokolls (IP) festgelegt. Die Protokolle betreffen alle Bereiche für die Bereitstellung von Multimedia-Mehrpunktkonfigurationen innerhalb des Internets. Dieser Ansatz geht also weit über den reinen Transport von Sprachdaten über das Internet hinaus. Das Ziel war die Definition eines umfassenden Kommunikationssystems, einschließlich traditioneller Systeme, wie dem klassischen Fernsprechnet, den Mobilnetzen sowie den klassischen Internetanwendungen wie E-Mail und World Wide Web (WWW) oder neuen Anwendungen wie beispielsweise die Aufzeichnung von Konferenzen, der Abruf und die Steuerung von Audio- oder Videodaten, die Steuerung und gemeinsame Nutzung von Whiteboards oder Projektoren. Die folgende Auflistung gibt eine Übersicht zu den wichtigsten Aktivitäten innerhalb der IETF:

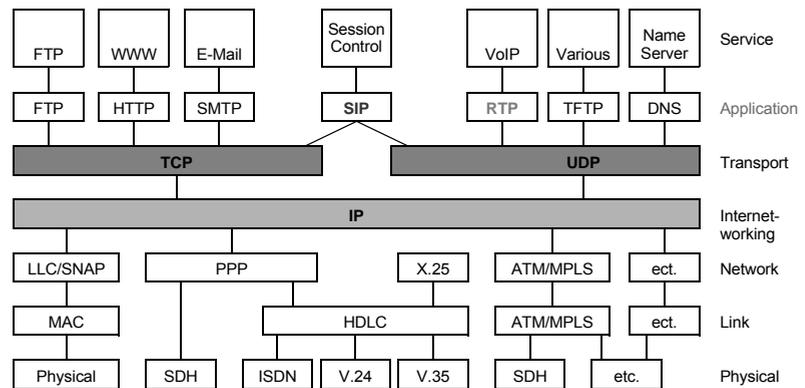


- Die Arbeitsgruppe *Multiparty Multimedia Session Control – MMUSIC* definierte eine Reihe von Protokollen zur IP-Telefonie. An erster Stelle muss hierbei das *Session Initiation Protocol (SIP, RFC 3261, früher RFC 2543)* angesprochen werden. Das Session Initiation Protocol (SIP) ist ein textbasiertes Client-Server-Anwendungsprotokoll, welches zum Aufbau, der Modifizierung oder Abbau von Multimedia Verbindungsbeziehungen zwischen ein oder mehreren Endpunkten dient. In seinem Nachrichtenaufbau und deren Ablauf ist es HTTP

sehr ähnlich, nur mit der Ausrichtung auf die Unterstützung der Steuerung von Kommunikationsverbindungen im Internet. Zur Steuerung der Media-Server wird das *Real-Time Streaming Protocol (RTSP)* verwendet. Es bietet ähnliche Funktionen wie sie beispielsweise zur Steuerung eines Videorekorders angeboten werden (Vorlauf, Rücklauf, Pause, Stopp usw.). Das *Session Description Protocol (SDP)* dient zur Beschreibung des Inhalts und Formats von Multimediaverbindungen. Das *Session Announcement Protocol (SAP)* dient zur Ankündigung von bestimmten Inhalten bei allen potenziellen Nutzern. Verwendet wird dieses Protokoll wohl nur von größeren, öffentlichen Sendungen (Verteildienste, mit Werbung gekoppelte Inhalte usw.) innerhalb des Netzes.

- Für die Zusammenarbeit mit dem klassischen Telefonnetz wurde die Arbeitsgruppe *PSTN/Internet Interworking (PINT)* eingesetzt. Das hier definierte Protokoll erlaubt den IP-Servern eine gewisse Kontrolle der im Telefonnetz angebotenen Dienste.
- Das Simple Conference Control Protocol (SCCP) wird zur Steuerung von Konferenzverbindungen angeboten.

Abb. 285:
IETF-Protokoll-
Architektur für
Multimedia-
verbindungen



Diese Protokolle stützen sich auf das bekannte Internet Protocol (IP), im Falle von Mehrpunktverbindungen auf das Internetprotokoll mit der Multicast-Erweiterung. Für den Transport von Audio- oder Videodaten sind zusätzliche Protokolle notwendig.

7.2 Architektur

Systeme der IETF werden durch Protokolle definiert

Wie bei vielen IETF-Ansätzen wird auch für die Unterstützung von Multimediaverbindungen eine Vielzahl von Protokollen festgelegt, weniger eine bestimmte Architektur. In der ITU-T-Umgebung werden immer zuerst die Architekturen und Funktionen beschrieben und danach ein Protokoll festgelegt. Im ITU-T-Ansatz sind daher die Protokolle durchaus austauschbar, in der IETF die Architekturen. SIP ist dadurch für viele Grundarchitekturen verwendbar. Übergänge zu anderen Net-

zen werden durch Gateways realisiert. SIP ist ein Teil der IETF-Multimedia-Übermittlungs- und -Steuerungsarchitektur, zu der auch das Real-Time Transport Protocol (RTP, RFC 3550 früher RFC 1889), das Real-Time Streaming Protocol (RTSP, RFC 2326), das Session Announcement Protocol (SAP), das Session Description Protocol (SDP, RFC 2327) gehören. Grundsätzlich werden im Zusammenhang mit SIP auch die folgenden Protokolle und Mechanismen angesprochen:

- ❑ Ein SIP-Terminal besteht aus einem User-Agent-Client (UAC), der Anfragen an den User-Agent-Server (UAS) richtet. Die Anfragen, Requests, Nachrichten werden in ihrem Anwendungszweck, der sog. Methode, engl. method, unterschieden. Der UAS antwortet mit Responses.
- ❑ SIP-Proxy-Server zur Weiterleitung der Steuernachrichten im Netz.
- ❑ SIP-Redirect-Server zur Ermittlung der aktuellen Zieladresse des gewählten Benutzers (Unterstützung der Teilnehmermobilität).
- ❑ SIP-Location-Server zur Abbildung von Zieladressen auf konkrete Systeme (z. B. Hotline@Firma.de auf A.Maier@Firma.de).
- ❑ Gateways für den Übergang zum konventionellen Netz. Hier müssen die Formate der Nutzinformationen und der Übergang vom leitungsvermittelten zum paketvermittelten Netz angepasst werden.
- ❑ Media-Gateway-Controller (MGC) steuern Medien- und Signalisierungs-Gateways, vergleichbar den Festlegungen nach TIPHON.
- ❑ IMPP (Instant Messaging and Presence Protocol) zur Statusüberwachung (online/offline, ready/not ready, busy/free usw.) und für die Behandlung bestimmter Leistungsmerkmale.
- ❑ SOAP (Simple Object Access Protocol) beinhaltet Remote Procedure Call-(RPC)-Mechanismen unter Verwendung von XML, die in einer HTTP- oder einer SIP-Nachricht verwendet werden können. Mit SOAP können komplexe, übergreifende Dienste relativ einfach realisiert werden, beispielsweise Text-to-Speech, Web-Anwendungen, VoiceXML.
- ❑ PINT (PSTN and Internet Interworking) besteht aus Festlegungen zu IN-Diensten, die aus dem Internet heraus initiiert werden. Mit diesen Diensten können beispielsweise Telefonverbindungen durch einen Mausklick ausgelöst werden (Click-to-Dial).

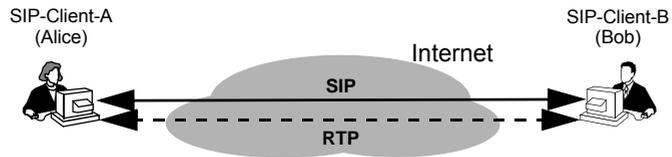
7.2.1 Direkte Kommunikation

Die einfachste Verbindung ist eine direkte Verbindung zwischen zwei User Agents. Die logische Instanz beim Initiator (Benutzer A, in dem Beispiel in der Abb. 286 Alice) für den Aufbau einer Verbindung (Session) mithilfe von SIP ist der User-Agent-Client (UAC). Der UAC richtet seine Anfragen an den User-Agent-Server. Jeder UA muss bereits einen Client und einen Server beinhalten. Dies funktioniert mit jedem SIP-Terminal, wenn dem User Agent A die Netzadresse von B bekannt ist und ihm dieses erlaubt und möglich ist (keine Restriktionen bzgl. Netz-

*Die einfachste
Verbindung*

abgrenzung, die diesen Aufbau verhindern). In größeren Konfigurationen oder Verbindungen über verschiedene Netze können keine Garantien für die Qualität der Übertragung (Quality of Service – QoS) gegeben werden, weil die User Agents meist keinen Zugriff auf die Betriebsmittel und Bandbreiten im Netz haben.

Abb. 286:
Direkte Kommunikation zwischen zwei SIP-Clients



Diese Betriebsweise wird auch für die sog. Peer-to-Peer-Netze (P2P-Netze) verwendet, in diesem Fall beinhalten die Clients aber noch weitere, unterstützende Funktionen, die auch für andere Clients nutzbar sind.

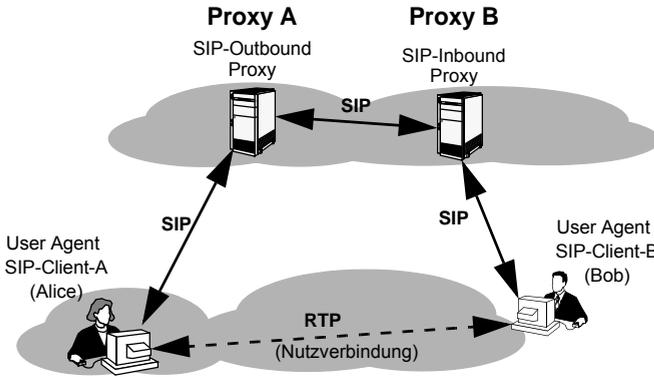
7.2.2 Proxy-Server

Proxy-Server

In Netzkonfigurationen bauen die Benutzer meist keine direkten Verbindungen untereinander auf, sondern verwenden Netzelemente, die sie beim Verbindungsaufbau unterstützen. Die Netzelemente können die Netz-Adresse des Ziels ermitteln, den Weg durch ein großes Netz festlegen und ggf. dieser Verbindung die für die Qualität der Übertragung notwendigen Betriebsmittel oder Bandbreiten zuordnen. Als Netzelement wird ein sog. Proxy-Server eingesetzt. Der SIP-Proxy-Server (Stellvertreter) handelt im Auftrag anderer User Agents und beinhaltet neben dem Server auch eine Client-Funktion. Ein Proxy-Server bearbeitet die SIP-Nachrichten (neue Header). Im Netz tritt er damit als eigenständige Quelle auf. Die Antworten auf Anforderungen von einem Proxy werden daher an den Proxy und nicht an den ursprünglichen Sender geschickt. Proxy-Server leiten (routen) SIP-Nachrichten durch das Netz.

Outbound- und Inbound-Proxy-Server

Funktional wird bei einer Verbindung zwischen zwei User Agents zwischen dem Outbound- und dem Inbound-Proxy-Server unterschieden. In dem Beispiel in der Abbildung 287 ist der Proxy A der Outbound-Server für den User Agent A (für Alice), dieser unterstützt den User Agent von Alice, um abgehende Gespräche (Outbound) aufzubauen. Auf der anderen Seite ist der Proxy B der Inbound-Proxy für den User Agent von Bob, dieser unterstützt den User Agent von Bob um kommende Sessions entgegenzunehmen (Inbound). Man spricht bei dieser Darstellung auch vom sog. SIP-Trapezoid, aufgrund der sich ergebenden Darstellungsform, dem Trapez. Nach der ursprünglichen Idee dieser Architektur sind die Proxy-Server nur für den Aufbau der Sessions notwendig. Die Nutzverbindung, auf der Basis des Real-Time Transport Protocol (RTP), zwischen A und B wird, nach dem ersten Verbindungsaufbau, direkt zwischen beiden aufgebaut. Die Proxy sind dann nicht mehr notwendig. Das hier dargestellte Trapez ist also nicht in allen Zuständen in dieser Form existent.

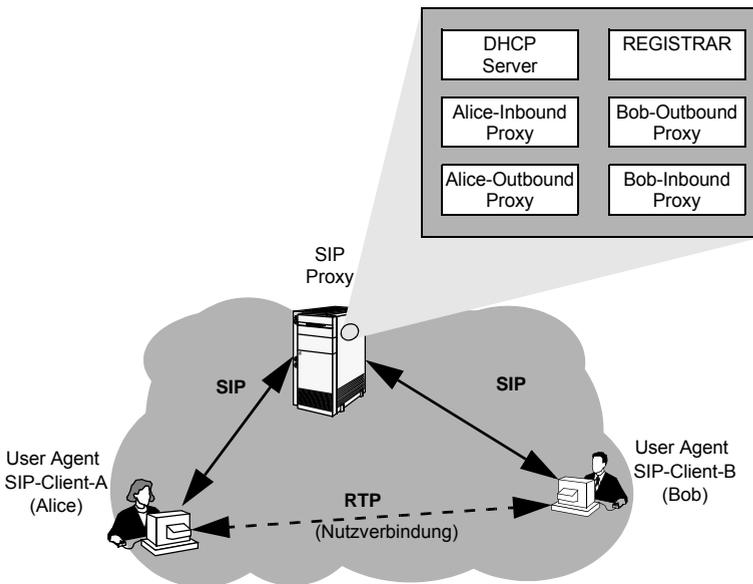


RTP: Real-Time Transport Protocol
 SIP: Session Initiation Protocol

Abb. 287:
IETF-Architektur

Die Bezeichnungen „Outbound“ und „Inbound“ hängen von der jeweiligen Betrachtungsweise und der jeweiligen Richtung des Aufbaus von Sessions ab. In der Praxis lassen sich beide nur für einen Augenblick einer bestimmten Session logisch unterscheiden. Die Realisierung umfasst immer beide Funktionen, und häufig werden noch weitere logische Einheiten im gleichen Gerät implementiert. Beispiele für solche Server wären der DHCP-Server oder der SIP-Registrierer, bei dem die SIP-Clients registriert werden.

Ansichtssache



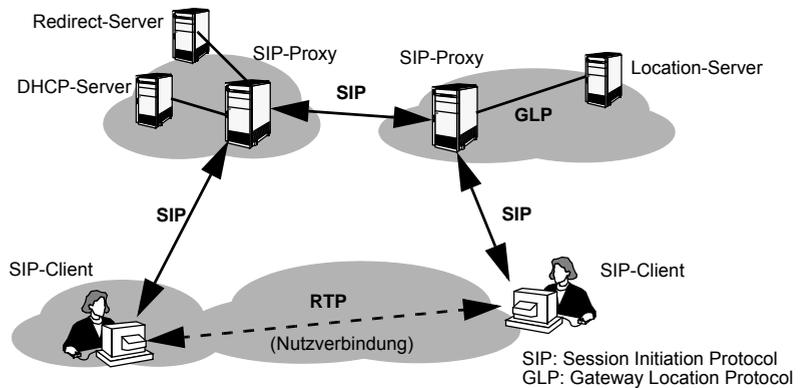
DHCP: Dynamic Host Configuration Protocol

RTP: Real-Time Transport Protocol
 SIP: Session Initiation Protocol

Abb. 288:
Inbound und Outbound-Proxy im gleichen Server

SIP-Clients Als SIP-Clients können typischerweise SIP-Terminals (Telefone oder PC-basierte Softphones) oder Gateways zu anderen Netzen/Protokollen auftreten. Neben dem Proxy-Server können noch unterstützende Server im Verlauf der Kommunikation verwendet werden. Der Redirect-Server unterstützt das Finden des gewünschten Clients und den Weg dorthin (z.B. im Falle von Rufumleitungen). Der Location-Server vermittelt das richtige, augenblicklich gültige Ziel (z.B. für lokale Call Center). Die SIP-Server können darüber hinaus mit anderen Anwendungs-Servern in Kontakt stehen und deren Dienste nutzen, z.B. für den Lightweight-Directory-Access-Protocol-Server (LDAP-Server), RADIUS-Server, DIAMETER-Server oder Server mit XML-Anwendungen.

Abb. 289:
SIP-Proxy und
Hilfs-Server



VoIP und NGN

Auf der Basis von SIP und RTP entstanden zunächst VoIP-Anwendungen im Internet und Peer-to-Peer-Anwendungen für Sprachkommunikation. Dieser Ansatz wurde dann auch von den Herstellern der VoIP-TK-Anlagen und schließlich auch von der Standardisierung für die Weiterentwicklung des Mobilfunks mit UMTS, als auch zur Steuerung von Verbindungen in den Next Generation Networks (NGN) im Festnetz übernommen. Unter diesem Begriff entwickelte die ITU-T ein architektonisches Konzept, das auf der Basis des Internetprotokolls IP die Kommunikation (Sprache, Video, E-Mail, Messaging usw.) und den Abruf von Informationen (Streaming, Video, Multicast-Dienste usw.) unabhängig von der Netzzugangstechnik ermöglicht. NGN unterscheidet sich gegenüber den VoIP-Ansätzen vor allem durch die Unterstützung von hohen Verfügbarkeiten und der Einhaltung einer gewissen Qualität in der Übertragung (Quality of Service – QoS).

QoS und Policy gehören zusammen

Die Einhaltung der geforderten Verbindungseigenschaften muss in den Netzen überwacht werden. Hierzu dient ein sogenanntes Policy-Enforcement in den Netzelementen. Diese Funktion ordnet die Ressourcen (die Bandbreite) einer Verbindung zu und überwacht, ob diese auch eingehalten und für die Nutzer der Verbindung garantiert wird. Das Policy-Enforcement kann beispielsweise durch ein Transportnetz mit diesen Eigenschaften wie MPLS (MPLS – Multi Protocol Label Switching) realisiert werden. Die Überwachung der Verbindungseigenschaften in den Transportnetzen muss von den Protokollen des Transportnetzes realisiert werden, in SIP sind diese Funktionen nicht enthalten.