Voice over Internet Protocol (VoIP)

ENTWURF

63 Seiten

INHALT

1 Übersicht

VoIP ist die allgemeine Bezeichnung für die Anwendungsgebiete Internet- bzw. Intranet-Telefonie, manchmal auch als LAN-Telefonie oder DSL-Telefonie bezeichnet.

- Die **Internet-Telefonie** kennzeichnet einen Anwendungsbereich mit einer oft schlechteren Sprachqualität als in anderen Anwendungsbereichen da sich der gesamte Datenpfad einer Sprachverbindung nicht vom Sender bis zum Empfänger kontrollieren lässt wodurch netzwerkbezogene Verfahren zur Verbesserung der Sprachqualität, nicht oder nur in unzureichendem Maße eingesetzt werden können. Im Internet treten außerdem häufig sehr große Paketübertragungszeiten und hohe Paketverlustraten auf, welche die Sprachübertragung ebenfalls beeinträchtigen.
- Die **Intranet-Telefonie** kennzeichnet einen Anwendungsbereich, der Sprachtelefonie innerhalb eines geschlossenen Unternehmensnetzes. Weil in Firmennetzwerken unterschiedliche Netzwerktechnologien eingesetzt werden, enthält der Begriff Intranet-Telefonie keine eindeutige Klärung bezüglich der verwendeten Netzwerktechnik wie z.B.: Token-Ring, ATM, oder Ethernet.

In vielen Fällen wird VoIP in Kombination mit konventionellen Konfigurationen eingesetzt. So haben beispielsweise viele Firmen ihr internes Telefonnetz auf VoIP umgestellt, und die „Telefonanlage“ nicht nur an das Internet angebunden, sondern auch über einen herkömmlichen ISDN-Anschluss an das öffentliche Telefonnetz.
VoIP unterscheidet sich von einer konventionellen Sprachverbindung durch die Übertragungsweise der Sprachinformation. Im herkömmlichen Telefonnetz wird ein Sprachkanal aufgebaut, der während der gesamten Verbindungsdauer gehalten und erst am Ende des Gesprächs wieder abgebaut wird. Bei Voice over IP werden keine Sprachkanäle geschaltet, sondern die Sprachinformation wird in IP-Pakete umgewandelt die durch die Routing-Mechanismen des Internet Protocols (IP) paketindividuell auf nicht festgelegten Wegen zu ihrem Ziel übertragen werden.
Würden zwei Teilnehmer sowohl die IP-Adressen und Ports über welche sie kommunizieren wollen als auch den Zeitpunkt wann sie ihre Telefoniesoftware starten vereinbaren, könnte theoretisch ohne weitere Maßnahmen zum festgelegten Zeitpunkt eine Sprechverbindung zwischen den beiden Teilnehmern hergestellt werden.

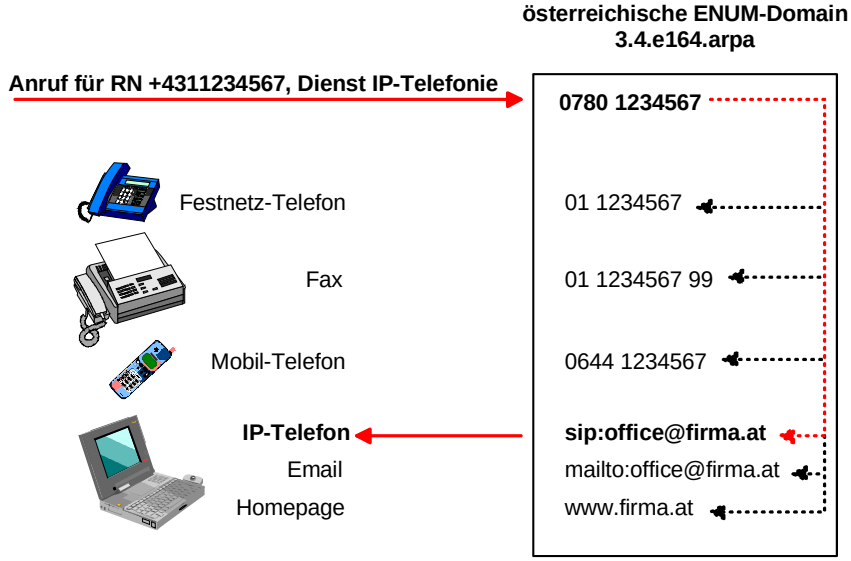

Bild 1: Prinzip von ENUM

Will man jedoch die Merkmale der konventionellen Telefonie wie z.B.: Frei- und Besetztton oder Voicebox nützen ist ein „Verbindungsaufbau“ durch den Austausch von Signalisie-

rungsnachrichten ähnlich der konventionellen Telefonie erforderlich. Zur IP basierte Signalisierung und Verbindungssteuerung werden im VoIP-Bereich derzeit zwei sehr unterschiedlichen Technologien[1] eingesetzt:

- Der **Standard H.323** mit dem Titel „Packet based multimedia communications systems" der weiteren Standards übergeordnet ist und 1996 von der ITU-T verabschiedet wurde ist. Er sehr weit verbreitet und wird auch als Dachstandard bezeichnet, weil er neben einer genauen Detaildefinition paketbasierter Multimediasysteme auch auf einige weitere Standards Bezug nimmt und diese implizit in die eigene Spezifikation integriert.
  Die wichtigsten Unterstandards von H.323 sind H.245 „Control protocol for multimedia communication" [10] und H.225.0 „Call signalling protocols and media stream packetization for packet-based multimedia communication systems" [11], wobei beispielsweise über den H.225.0-Layer sämtliche Daten zwischen Endgeräten ausgetauscht werden, so dass H.245-Nachrichten für die Übertragung auf H.225.0 angewiesen sind.
- Das **Session Initiation Protocol (SIP)** durch, welches von der IETF standardisiert wurde (RFC 3261) und im März 1999 von der IETF eingeführt wurde und sich innerhalb kurzer Zeit als direkter Konkurrent zu H.323 sehr schnell verbreitet hat, obwohl die Standardisierung zum gegenwärtigen Zeitpunkt noch nicht abgeschlossen ist. Fast alle namhaften Hersteller haben SIP-Implementierungen oder haben zumindest angekündigt, SIP zukünftig zu unterstützen, obwohl H.323 immer noch als bewährte und praxiserprobte Basis angesehen wird.
  Das SIP-Protokoll hat sich inzwischen weltweit in öffentlichen Providernetzen etabliert. H323 ist in diesem Bereich kaum noch anzutreffen. Auf dem deutschen und amerikanischen Markt sind inzwischen zahlreiche Anbieter aktiv, die fast ausnahmslos SIP einsetzen. Inzwischen können über derartige Voice over IP-Dienste über Gateways der Provider auch Festnetzanschlüsse erreicht werden, bzw. umgekehrt IP-Telefoniekunden aus dem Festnetz angerufen werden. Des Weiteren wird SIP in UMTS-Netzwerken für die Signalisierung von Multimedia-Diensten, nicht aber für die klassische Telefonie, verwendet.

Im öffentlichen Fernsprechnetz (PSTN) gibt es für die Adressierung von Teilnehmern und das Routing nur Rufnummern nach dem in der Empfehlung ITU-T E.164 spezifizierten Format (Ländercode + ONKZ + Teilnehmer).
Im Internet werden die Teilnehmer anhand von IP-Adressen angesprochen und adressiert wobei eine Auflösung von leichter zu merkenden Namen (sog. Domains) zu IP-Adressen Aufgabe des DNS ist. Diese Adressen stellen alternative Kommunikationswege zur "klassischen" Telefonie dar, ein SIP-basiertes VoIP-Telefon kann mit diesen Informationen einerseits ein Gespräch zu dieser Rufnummer direkt über das Internet zustellen, und zusätzlich (falls das Gerät dies unterstützt) die angegebene Website am Display des Geräts darstellen.
Um verschiedene Adressen wie das private Telefon zu Hause, das Telefon in der Firma, die Faxnummer, Handynummern, geschäftliche und private eMailadressen, Videokonferenzadressen, die eigene Website und alle anderen denkbaren Kommunikationsadressen unter einer einzigen Nummer verfügbar zu machen wurde ENUM – siehe „ENT ENUM.doc“ - entwickelt.
ENUM ist ein international genormter Internetstandard, der weltweit jeder Telefonnummer eine eindeutige Internetadresse (ENUM-Domain) zuordnet und in weiterer Folge zur Herstellung beliebiger Kommunikationsverbindungen herangezogen werden kann. Unter ENUM kann man sich – sehr vereinfacht gesprochen – ein Art Anrufumleitung vorstellen, bei der

[1] Für die Interoperabilität von H.323 und SIP in heterogenen Umgebungen ist von Vorteil, dass beide für den Nutzdatentransport dasselbe Echtzeit-Protokoll RTP verwenden. Auch die verfügbaren Sprachcodecs können mit beiden Signalisierungen zusammen eingesetzt werden.

man beispielsweise auch ein E-Mail an dieselbe Rufnummer senden kann. Das E-Mail wird dann auf die tatsächliche E-Mail Adresse ,umgeleitet.

ENUM ist also eine verteilte Datenbank, mit der Möglichkeit, zu jeder weltweit verwendeten Telefonnummer Kommunikationsadressen zu speichern. Sie ist eine spezielle Anwendung des bewährten Domain Name Systems (DNS), das im Internet für den Anwender unbemerkt die Umwandlung der leicht merk-und lesbaren Domain-Namen (z.B. www.enum.at oder www.rtr.at) auf die numerischen IP-Adressen (83.136.32.24 oder 192.168.2.5) durchführt.
Von der RTR-GmbH wurde dafür der speziell für den Einsatz konvergenter Dienste vorgesehene Rufnummernbereich (0)780 geschaffen.
Damit sich bei VoIP Anrufer und Gerufener per ENUM "finden" müssen zwei Bedingungen erfüllt sein:

- Der Angerufene muss die ENUM-Domain zu seiner Rufnummer registriert und seine VoIP-Adresse als ENUM-Service eingetragen haben.
- Das VoIP-Gerät (oder der Server) des Anrufers muss im Rahmen des Rufaufbaus eine ENUM-Abfrage durchführen

Verfügt eine Telefonanlage sowohl über einen Anschluss ans herkömmliche Festnetz als auch über einen IP-fähigen Anschluss der mit dem Internet verbunden ist, erreichen Gespräche die Mitarbeiter, egal ob aus dem Internet oder aus dem Festnetz, am gewohnten Tischtelefon.
Mit nur einer einzigen ENUM-Domain (nämlich die zur Kopfnummer der Anlage) können zu allen Durchwahlen die zugehörigen VoIP-Adressen eingetragen werden - die Nebenstellen sind damit für alle Geräte und Betreiber, die ENUM im Rufaufbau unterstützen, direkt per Internet erreichbar.

2 VoIP-Netzwerke

2.1 Netzwerkstrukturen

VoIP kann in zahlreichen Anwendungsbereichen eingesetzt werden wodurch Netzwerkstrukturen unterschiedlicher Ausprägung mit unterschiedlichen Verfahren für den Transport von Signalisierungsnachrichten entstehen. Die folgenden Beispiele berücksichtigen nicht nur die Endgerätethematik, welche durch die Art der Endgeräteanbindung, z.B. analog oder digital, Einfluss auf die gesamte Netztopologie hat, sondern auch den Einsatz von Gateways zwischen öffentlichen und privaten Telefonnetzen, sowie Media Gateways.

2.1.1 Kompaktlösungen

ISDN S_0

Ein zentrales Gateway verbindet ein privates IP-Netz mit dem öffentlichen Telefonnetz. In kleineren VoIP-Netze mit bis zu ca. 30 Gateway-Anschlüssen wird eine entsprechende Anzahl von ISDN-Basisanschlüssen[2], für die externe Sprachverbindung zum Telefonnetz eingesetzt. - Ein ISDN-S_0-Anschluss enthält zwei unabhängige Sprachkanäle (B-Kanäle) mit je 64 kBit/s Nutzbandbreite und einem D-Kanal mit 16 kBit/s für die Übertragung von Signalisierungsdaten.
Das Gateway enthält ferner die Kommunikationssteuerung für die angeschlossenen Endgeräte im internen IP-Netz, so dass die Signalisierung und die Umsetzung der Sprachinformationen zwischen beiden Netzen in einem Gerät durchgeführt wird.

[2] ISDN-Basisanschlüsse werden auch Basic Rate Interface (BRI) Anschlüsse genannt

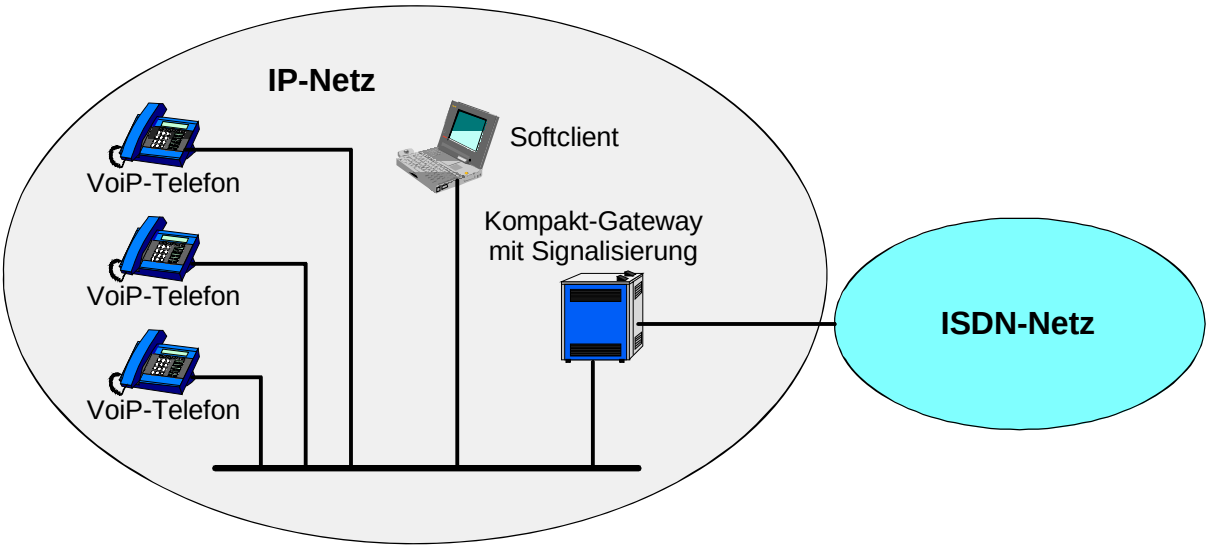

Bild 2: Konfigurationsbeispiel mit Kompakt-Gateway

ISDN S_{2M}

Bei einer höheren Anzahl von Sprachkanälen wird statt einer ISDN- S_0- Schnittstelle eine S_{2M}-Schnittstelle verwendet. Diese enthält 30 ISDN-Sprachkanäle und wird ISDN-Primärmultiplexanschluss oder Primary Rate Interface (PRI) genannt. Dieser Anschluss entspricht dem europäischen Standard E1 mit einer Nutzbandbreite von 2,048 MBit/s. S_{2M} enthält 32 Kanäle mit je 64 kBit/s, davon 30 Sprachkanäle, einen Signalisierungs- und einen Servicekanal.

In Nordamerika und Japan wird die Variante T1 verwendet die eine Nutzbandbreite von 1,544 MBit/s hat. Sie enthält lediglich 24 B-Kanäle mit je 64 kBit/s, davon 24 Sprachkanäle mit je 56 kBit/s, 24 Signalisierungskanäle mit je 8 kBit/s und einem Steuerkanal mit 8 kBit/s. Hersteller bieten meist Geräte mit kombinierten E1/T1-Anschlüssen an, die sich dem Einsatzort angepasst konfigurieren lassen.

LAN-PBX

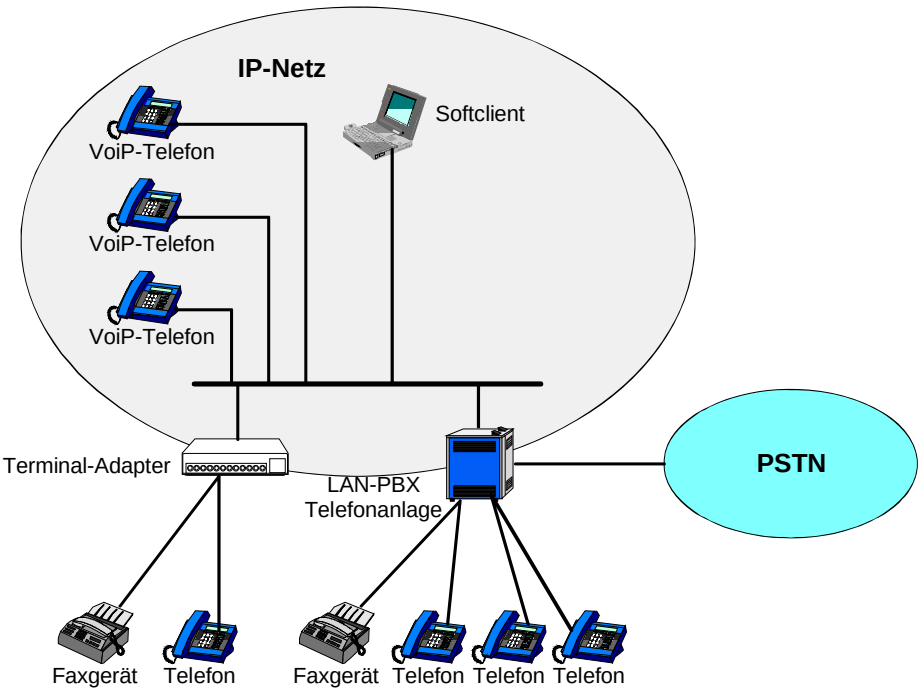

Bild 3: Konfigurationsbeispiel mit LAN-PBX

Bei Modularen LAN-PBX-Anlagen bzw. herkömmlichen, leitungsvermittelten TK-Anlagen (PBX) können, modularen Aufbau vorausgesetzt, die Telefonschnittstellen durch Gatewayschnittstellen zum lokalen Datennetz ersetzt bzw. erweitert werden. Die Anbindung an das lokale Datennetz erfolgt durch den Anschluss der Ethernet- oder Fast-Ethernet-Schnittstellen der Gateways an einen lokalen LAN-Switch.
Reine LAN-PBX-Anlagen sind nur auf VoIP-Umgebungen spezialisiert, modulare LAN-PBX-Anlagen ermöglichen den gemischten Betrieb von leitungsvermittelten Telefonen und von IP-Endgeräten. Sie werden daher vor allem in Migrationsszenarien eingesetzt, bei denen nur ein Teil der Netzwerkinfrastruktur mit VoIP ausgestattet werden kann.
IP-Telefone für LAN-PBX-Anlagen sind meist herstellerabhängig implementierte IP-Systemtelefone, bei denen die proprietären Leistungsmerkmale der TK-Anlage unterstützt werden. Aus Sicht der PBX-Anlagenadministration lassen sich diese Endgeräte wie herkömmliche Systemtelefone konfigurieren und verwalten, so dass Anwender keinen Unterschied bei der Bedienung von IP-Systemtelefonen und klassischen Systemtelefonen bemerken. Ein Aufbau standardkonformer und herstellerübergreifender Lösungen ist mit LAN-PBX-Anlagen nicht oder nur sehr eingeschränkt möglich.

Soft-PBX

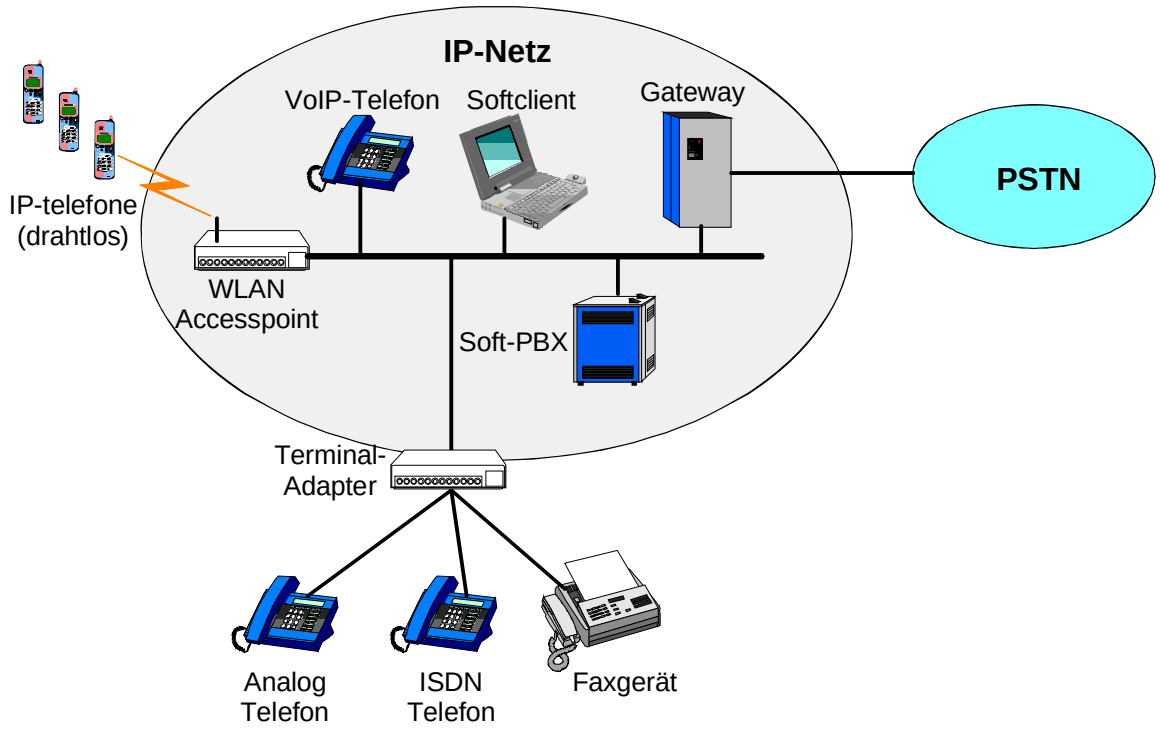

Bild 4: Konfigurationsbeispiel mit Soft-PBX

Bei einer Soft-PBX werden die Funktionen der lokalen TK-Anlage von einer Telefonanlagensoftware übernommen, die bei vielen Herstellern als Anwendung auf einem Windows-NT-Server installiert ist und die klassische „Telefonieumgebung“ vollkommen ersetzt. Der Einsatz einer Soft-PBX lohnt sich vor allem dann, wenn die bestehende IT/TK-Infrastruktur vollständig erneuert werden soll, oder bei Neuinstallationen, wo auf keine vorhandene IT/TK-Installation Rücksicht genommen werden muss. Die Soft-PBX – auch Call Server genannt – ist auf einem PC-System installiert und über eine Ethernet-Schnittstelle nach dem Standard IEEE 802.3 mit dem lokalen Datennetz verbunden. Die IP-Telefone sind als Hardwaregeräte an das Datennetz angeschlossen. Parallel dazu kommen auch Software-Telefone (Softclients) auf den Arbeitsplatz-PCs zum Einsatz. Externe Gateways im Netzwerk ermöglichen den Übergang vom lokalen Datennetz zu anderen Sprachnetzen (z.B. in öffentliche Telefonnetze).

Analoge Faxgeräte können über spezielle Schnittstellenadapter mit analoger a/b- und Ethernet-Schnittstelle einbezogen werden. Auch drahtlose IP-Telefone lassen sich über Wireless LAN (WLAN) nach dem Standard IEEE 802.11 einbinden.
Die Funktionen einer Soft-PBX können durch zusätzliche Anwendungen und Dienste die auf IT-Systemen installiert sind ergänzt werden. Speziell in Call-Centern, wo die Integration von Computer- und Telefoniefunktionen zu erheblichen Prozessoptimierungen führen kann, wird die Anwendung von Soft-PBX Systemen forciert.

2.1.2 TK-Anlagen-Kopplung (Trunking)

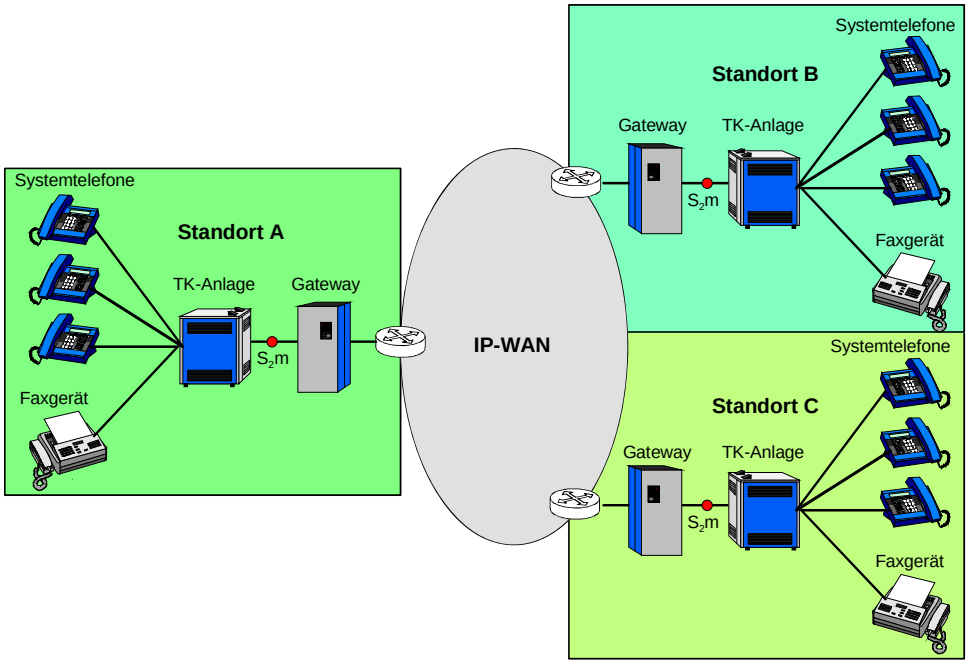

Bild 5: TK-Anlagen-Kopplung mit VoIP

Aus Gründen kürzlich getätigter Investitionen, vorhandener Leistungsmerkmale oder der Betriebssicherheit ist es nicht immer sinnvoll, bestehende Telekommunikationsanlagen (TK-Anlagen) komplett zu ersetzen, sondern sie zusätzlich zu den standortübergreifenden Mietleitungen für die Sprachkommunikation auch an ein WAN-Datennetz (Wide Area Network) anzubinden wodurch separate Netzwerke für Daten und Telefonie nicht mehr erforderlich sind.
Bei der Vernetzung von TK-Anlagen mittels VoIP wird das WAN-Datennetz genutzt, um die Sprachdaten mit Hilfe von IP-Paketen zu übertragen. Zur Wandlung der Sprachdaten werden VoIP-Gateways eingesetzt, die auf der einen Seite mit den Schnittstellen der TK-Anlage (analog, S_0, S_{2M}) und auf der anderen Seite mit dem Datennetzwerk (IP) verbunden sind.
Die Gateways führen nicht nur die Wandlung der Sprachdaten (Nutzdaten) durch, sondern setzen auch die Signalisierungsdaten um die bei digitalen Schnittstellen (z.B. S_0, S_{2M}) in einem separaten Kanal, getrennt vom Nutzsignal (Outband-Signalisierung)erfolgt. Als Protokoll werden Standards wie DSS1 (Euro ISDN), QSIG (SIGnalisierung am Q.Referenzpunkt) oder proprietäre, herstellerabhängige Protokolle — z.B.: CorNet N (Siemens), ABC-F (Alcatel) oder TNet (Bosch/Tenovis) —eingesetzt.
Die Entscheidung für die Nutzung eines speziellen Protokolls hängt von folgenden Kriterien ab:

- Welche Leistungsmerkmale soll die TK-Anlage im Netzverbund unterstützen?
- Welche Protokolle soll die Schnittstelle am VoIP-Gateway unterstützen?
- Welche Protokolle soll die TK-Anlage unterstützen?

In einem heterogenen TK-Anlagenumfeld mit Komponenten verschiedener Hersteller ist es nicht möglich, proprietäre Signalisierungsprotokolle einzusetzen, weil diese nicht untereinan-

der kompatibel sind. Deshalb wird bei der Kopplung von TK-Anlagen über VoIP häufig auf das Signalisierungsprotokoll QSIG zurückgegriffen.
Die benötigte Bandbreite pro Sprachverbindung bei der TK-Anlagen-Kopplung ist abhängig von der verwendeten Sprachkodierung und Sprachkomprimierung. Der Overhead durch die Paketheader muss zusätzlich berücksichtigt werden, zumal er bei sehr kurzen Sprachpaketen ungefähr der Nutzdatenmenge entspricht.
Moderne TK-Anlagen bieten auch die Möglichkeit, VoIP-Gateways direkt als Schnittstellenkarte zu integrieren.

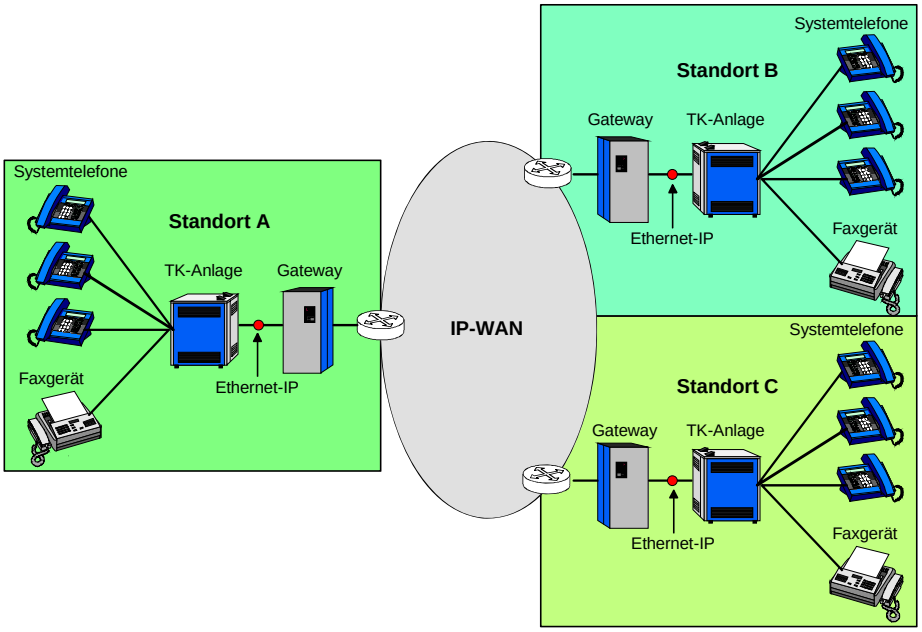

Bild 6: TK-Anlagen-Kopplung mit integrierten VoIP-Gateways

2.1.3 Endgeräteanschlussvarianten

Endgeräte können, je nach eingesetzter Technologie, auf verschiedenartige Weise eingesetzt werden. Weit verbreitete Varianten sind:

- VoIP-Endgeräte
  sie sind speziell für den Einsatz in VoIP-Netzwerken entwickelt worden und bedürfen keiner Anpassung unter der Voraussetzung, dass innerhalb eines Netzes ausschließlich miteinander kompatible Produkte eingesetzt werden.
- Mobile Endgeräte
  diese können grundsätzlich über den WLAN-Standard IEEE 802.11 in ein Netzwerk integriert werden. Die drahtlose Kommunikation findet in einem Shared Medium statt. Endgeräte, die mit einem Access-Point im WLAN kommunizieren, teilen sich die verfügbare Bandbreite, genauso wie es in der Vergangenheit in 10 MBit Ethernet-Netzen mit Koax-Verkabelung der Fall war. Das verwendete Zugangsverfahren wird als CSMA/CD (Carrier Sense Multiple Access/Collision Detection) bezeichnet. Sprachdaten werden hierbei nicht bevorzugt behandelt.

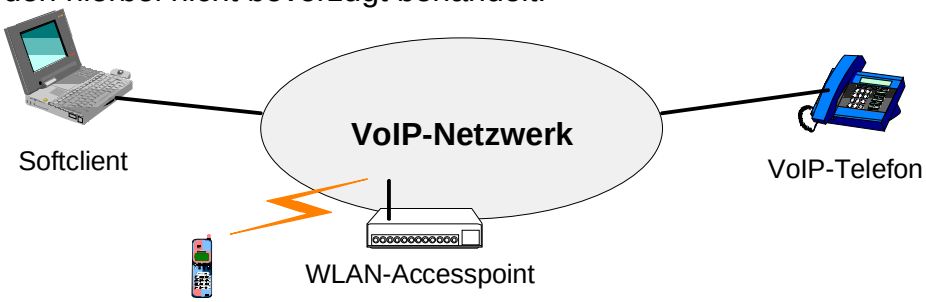

Bild 7: Anschluss stationärer und mobiler VoIP-Endgeräte

- Analogtelefone/-faxgeräte
  analoge Endgeräte werden über Terminal-Adapter an ein VoIP-Netz angeschlossen. An so genannten a/b-Anschlüssen können sowohl Telefone als auch Faxgeräte betrieben werden. Der Anschluss von Faxgeräten stellt in diesem Zusammenhang besonders hohe Anforderungen an die VoIP-Umgebung.

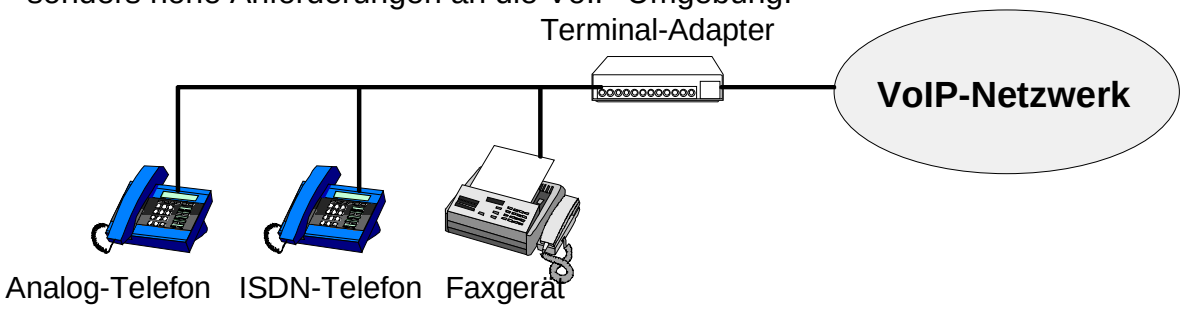

Bild 8: Anschluss von Analog- und ISDN-Endgeräten

- ISDN-Telefone
  Vorhandene ISDN-Endgeräte können, wie die analogen Endgeräte, ebenfalls mit Hilfe von Terminal-Adaptern an VoIP-Netze angeschlossen werden, sofern ein ISDN-S_0-Anschluss am Terminal-Adpater vorhanden ist.

2.2 Transportnetze für Voice over IP

2.2.1 Technische Anforderungen an Transportnetze für VoIP

Um VoIP in eine Netzwerkumgebung integrieren zu können, müssen einige Voraussetzungen geschaffen werden, damit die Telefoniedienste über Datennetze reibungslos betrieben werden können.

Netzwerke: Nicht jedes Netzwerk ist für Sprachübertragung geeignet. Je nach eingesetztem Netzwerkstandard müssen Maßnahmen ergriffen werden, um eine gleichbleibende Sprachqualität zu garantieren oder zumindest unter normalen Betriebsbedingungen zu ermöglichen. Eine Sicherheit für die Einhaltung einer gewünschten Sprachqualität kann nur mit Netzwerken erreicht werden, die garantierte Dienstgütemerkmale bieten. Diese Eigenschaft wird auch als Quality of Service (QoS) bezeichnet.
Der Einsatz von VoIP erfolgt zur Zeit hauptsächlich im Ethernet, DSL für VPN-Anbindung von Mitarbeitern in Home-Offices, ISDN für effektivere Ausnutzung von Mietleitungen durch komprimierte VoIP-Sprachübertragungen und ansatzweise im WLAN. VoIP wird auch im Carrier-Bereich zwischen Netzwerkknoten oder als Transportmedium zwischen Endgeräten auf Kundenseite (Customer Promises Equipement – CPES) eingesetzt. Dabei wird IP zusammen mit SDH oder SONET (Packet over SONET), Frame Relay und ATM eingesetzt. ATM wird für die Sprachübertragung vorwiegend über AAL-Schichten ohne Verwendung von IP-Protokollen verwendet.
ATM-Netze beispielsweise bieten garantierte Dienstgüte, während Ethernet-Netze diese Möglichkeit nicht bieten. Sie können lediglich Bandbreite bereitstellen, solange diese in ausreichendem Maße zur Verfügung steht. QoS-Verfahren werden auch in Ethernet-Netzen eingesetzt, die beispielsweise Audioübertragungen gegenüber anderen Datenströmen priorisieren. Dabei kann jedoch nicht ausgeschlossen werden, dass die Ressourcen während eines Gesprächs aufgrund einer Netzwerküberlastung derart eingeschränkt werden, dass ein Gespräch trotz verwendeter QoS-Merkmale gestört wird.
Die benötigte Bandbreite errechnet sich aus dem Datenvolumen der kodierten und ggf. komprimierten Sprachdaten und dem Overhead, den die eingesetzten Protokolle, u.a. für die Header der Sprachpakete, benötigen. Das Ergebnis wird mit der Anzahl maximal gleichzeitig

zu erwartender Gespräche, die über einen Strang des Netzwerks geführt werden, multipliziert. Neben den Sprachdaten muss jedoch auch die im Mittel benötigte Bandbreite für Signalisierungsinformationen berücksichtigt werden. Des Weiteren ist zu beachten, dass die Nenndatenrate eines Netzwerks normalerweise nicht vollständig genutzt werden kann. Üblicherweise werden gleichzeitig weitere Datenströme unabhängig von VoIP-Daten über das Netzwerk transportiert, die durch sprunghaften, kurzzeitigen Bandbreitenbedarf (Bursts) den Fluss der Sprachdatenpakete beeinträchtigen können. Ein Beispiel ist der Abruf einer Webseite, der für eine kurze Zeitdauer eine Datenübertragung zur Folge hat.

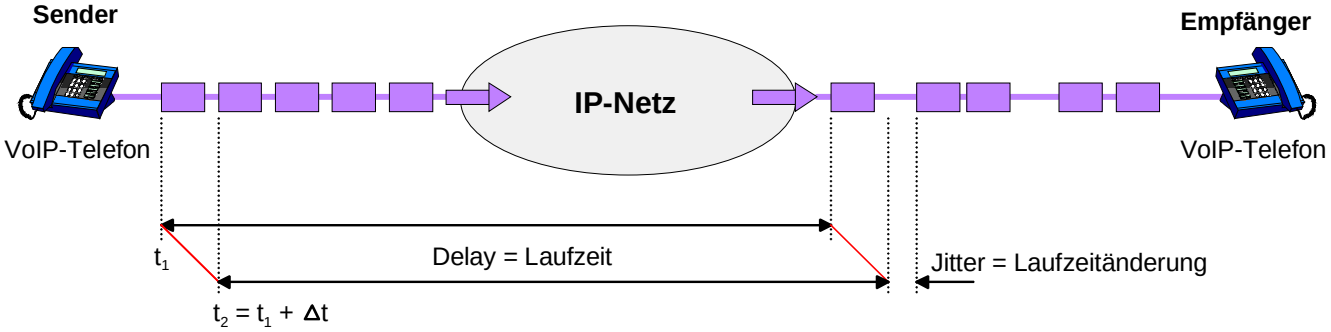

Bild 9: Delay und Jitter in einem Paketnetzwerk

Ausreichend verfügbare Bandbreite von Netzwerken sind ein notwendiges, jedoch kein hinreichendes Kriterium für eine störungsfreie Sprachkommunikation. Weitere wichtige Merkmale sind die Verzögerungszeiten (Delay), die sowohl durch Endgeräte als auch durch Netzwerke verursacht werden, sowie Verzögerungszeitschwankungen (Jitter), die zu kurzzeitigen Aussetzern der Sprachübertragung führen können. Abhilfe können Pufferspeicher schaffen. Sie speichern auf Empfangsseite für eine einstellbare Zeitdauer empfangene Daten, um Jitter auszugleichen. Dadurch wird jedoch die Verzögerungszeit zwischen Sender und Empfänger zusätzlich erhöht.

Kodierung/Kompression: Die Sprachqualität eines VoIP-Systems hängt entscheidend von den eingesetzten Sprachkodierungen (Codecs) ab, die sowohl die Kodierung auf der Sendeseite, als auch die Dekodierung auf der Empfangsseite übernehmen. Meistens wird gleichzeitig eine Kompression bzw. Dekompression der zu übertragenden Sprachdaten durchgeführt, um die Übertragungsrate zu reduzieren.
Die eingesetzte Kodierung sollte den von Anwendern erwarteten Anforderungen an die Sprachqualität genügen. Handelt es sich nicht um ein geschlossenes System, sollte ein Codec verwendet werden, der zu den weit verbreiteten Standard-Codecs der ITU-T zählt. Eine solche Maßnahme erhöht die Interoperabilität mit anderen Gegenstellen und vermeidet die Notwendigkeit einer Umkodierung der Sprachdaten in Gateways oder MCUs, bei der eine zusätzliche Zeitverzögerung und eine Verschlechterung der Sprachqualität die Folge wäre.

Transportprotokolle: Die Sprachdaten sollen ihr Ziel bei Echtzeitübertragungen wie der Sprachtelefonie mit möglichst geringer Verzögerung erreichen. Deshalb muss darauf geachtet werden, dass die Weiterleitung der Sprach-Datenpakete im Netzwerk unverzüglich erfolgt und sowohl die Datenverlustrate, als auch die Fehlerrate gering gehalten wird.
Die Übertragung von Sprachdaten in Echtzeit sollte bei Echtzeitübertragung über so genannte ungesicherte Protokolle durchgeführt werden. In diesem Fall werden die Daten ohne weitere Schutzmaßnahmen übertragen. Die Unsicherheit, ob die Daten den Empfänger tatsächlich fehlerfrei erreichen, wird in Kauf genommen, weil der Vorteil geringerer Verzögerung überwiegt: Die Verzögerungszeit wird bei der Übertragung im Vergleich zu gesicherten Protokollen gering gehalten, weil keine als verloren erkannte Datenpakete zu einem Zeitpunkt wiederholt an den Empfänger übermittelt werden, wenn diese nicht mehr aktuell sind.

2.2.2 Ethernet

Der Ethernet-Standard wurde bereits 1980 am Xerox Palo Alto Research entwickelt und veröffentlicht und in einer verbesserten Version von IEEE als Standard 802.3 genormt.
Der Standard basierte ursprünglich auf einem CSMA/CD-Zugriffsverfahren (Carrier Sense Multiple Access with Collision Detection) auf eine Busstruktur. Bei gleichzeitigem Sendeversuch von zwei oder mehr Endgeräten kommt es dabei zu einem Konkurrenzverhalten auf dem gemeinsam genutzten Datenkabel und bei zu starker Belastung zu einem Zusammenbruch des Datenverkehrs. Da die Gewährleistung von Dienstgütemerkmalen mit CSMA/CD nicht möglich ist, sind ältere Netze, die noch mit Bustechnologie auf Basis von CSMA/CD arbeiten, nicht für den Einsatz von VoIP geeignet.
Neuere Ethernet-Standards enthalten zwar auch das CSMA/CD-Verfahren, jedoch kommt es bei den heutzutage verwendeten Switched-Ethernet-LAN-Netzwerken nicht mehr zum Tragen, da zwischen Switch und Endgerät eine Twisted-Pair-Verkabelung z.B. mit 100Base-T-Anschlusstechnik im Full-Duplex-Verfahren eingesetzt wird. Für Sende- und Empfangsrichtung steht daher die volle Bandbreite kollisionsfrei zur Verfügung.
Heutzutage gebräuchliche Ethernet-Varianten sind:

- Fast Ethernet mit 100 MBit/s (IEEE 802.3n)
- Gigabit Ethernet mit 1 Gbit/s (IEEE 802.3z)
- 10 Gigabit Ethernet mit 10 Gbit/s (IEEE 802.3ae)
  10 Gigabit Ethernet ist kein LAN-Standard mehr, sondern fokussiert sich auf den Einsatz in Weitverkehrsnetzen (WANs) und ist zur Zeit ausschließlich für Glasfaserverkabelung spezifiziert.

Bild 7.4: Struktur des Ethernet-MAC-Frame

Die Übertragung von Daten über Ethernet wird in Rahmen, so genannter Frames, durchgeführt. Die Nutzdaten sind in dem Rahmen enthalten.
Der Ethernet-Frame des Standards IEEE 802.3 enthält folgende Felder:

- Präambel (PA, 7 Byte): Wiederholte Bitfolge „01" zur Bitsynchronisation.
- Start Frame Delimiter (SFD, 1 Byte): Kennzeichnung des Frame-Anfangs mit der Bitfolge „10101011".
- Destination Address (DA, 2 bzw. 6 Byte): Empfänger-MAC-Adresse.
- Source Address (SA, 2 bzw. 6 Byte): Sender-MAC-Adresse.
- Length (LEN, 2 Byte): Länge des Frames.
- Data (variable Länge): Nutzdaten
- Padding (PAD, variable Länge): Auffüllen des MAC-Frame auf Mindestgröße von 512 Byte.
- Frame Check Sequence (FCS, 4 Byte): Feld zur Fehlerüberprüfung.

Einige Erweiterungen des Ethernet-Standards sind in Bezug auf VoIP von besonderem Interesse:

- IEEE 802.3af: Supplement to CSMA/CD access method and physical layer specifications - Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI) [60]: In dieser Erweiterung wird eine Stromversorgung für Endgeräte über die Netzwerkverbindung der Endgeräte ermöglicht.
- IEEE 802.1p: Traffic Class Expediting and Dynamic Multicast Filtering [61]: Bietet Priorisierung auf Layer-2 (vgl. Kapitel 9.3).

- IEEE 802.1q: Virtual Bridged Local Area Networks (VLANs) [62]: Mit Hilfe dieser Erweiterung können Netze logisch voneinander getrennt werden, um eine gegenseitige Beeinflussung zu verhindern. IEEE 802.1q wird zwangsläufig verwendet, wenn IEEE 802.1p eingesetzt werden soll. Grund ist das VLAN-Tag, das die benötigten drei Bit für die Prioritätsklassen enthält.

Vorteile von Ethernet:
- Kostengünstig, weit verbreitet, in fast allen LAN-Netzen eingesetzt
- In mehreren Bandbreitenabstufungen (100 MBit/s, 1 GBit/s, 10 GBit/s) bei Verwendung derselben Technologie verfügbar
- Verschiedene QoS-Verfahren auf Layer 2 und 3 verfügbar
- Effektive Bandbreitennutzung durch QoS-Verfahren möglich, nicht genutzte Bandbreite für andere Anwendungen verfügbar

Nachteile von Ethernet:
- QoS nur durch zusätzliche Verfahren wie z.B. IEEE802.1p bzw. ToS oder DiffServ auf Schicht 3 möglich
- Keine absolut garantierte Dienstgüte für einzelne Verbindungen möglich

Einsatzgebiete von Ethernet:
- Firmen-LANs und private LANs
- Mit zunehmender Bandbreite (1 GBit/s bzw. 10 GBit/s) auch im MAN/ WAN

2.2.3 DSL

Digital Subscriber Line ist eine auf Kupferkabel-Übertragung basierte Modemtechnik zur Anbindung von Endkunden an ein Provider-Netzwerk. DSL arbeitet unabhängig von den Telefoniestandards parallel zu analogen oder ISDN-Anschlüssen in höheren Frequenzbereichen und verwendet auf den Kupfer-Doppeladern unter anderem ATM zum Nachrichtentransport Auf Endkundenseite ermöglichen DSL-Modems den Anschluss an ein DSL-Netzwerk, während auf Providerseite DSL-Access-Multiplexer (DSLAM) zahlreiche Endkunden bedienen. Je nach verwendeter ATM-AAL-Schicht können unterschiedliche QoS-Anforderungen erfüllt werden.
Am weitesten verbreitet ist die asynchrone Variante ADSL, weitere Varianten sind in folgender Tabelle angeführt:

DSL-Variante	Bedeutung	Datenübertragung	Übertragungsmodus	Reichweite
ADSL	Asymmetric Digital Subscriber Line	1,5 bis 9 Mbit/s (Download) 16 bis 768 kbit/s (Upload)	Down/Up	6 km
SDSL	Symmetric Digital Subscriber Line	1,544 Mbit/s-2,048 Mbit/s	Duplex	3 km
HDSL	High Bit Rate Digital Subscriber Line	1,544 Mbit/ s - 2,048 Mbit/s	Duplex	4-5 km
VDSL	Very High Bit Rate Digital Subscriber Line	13 bis 52 Mbit/s (Download) 1,5 bis 2,3 Mbit/s (Upload)	Down/Up	1,5 km

Tabelle 1: DSL-Varianten

Damit IP-Pakete über DSL übertragen werden können, wird ein serielles Punkt-zu-Punkt-Protokoll wie beispielsweise PPPoE (Point-to-Point-Protocol over Ethernet) verwendet und mit Hilfe von ATM-Zellen über die DSL-Leitung übertragen.

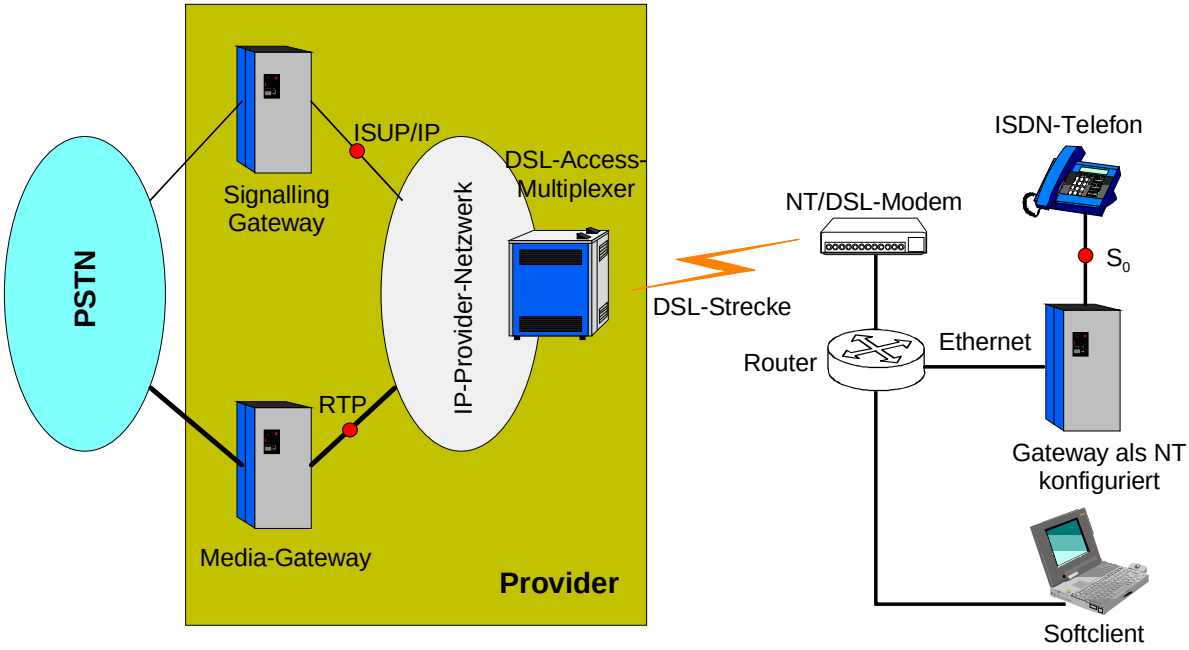

Bild 10: Endkundenanbindung mit DSL

Vorteile von DSL:

- Kostengünstig und weit verbreitet
- Einsatz von IP mit Hilfe des seriellen Protokolls PPPoE möglich

Nachteile von DSL:

- Verfügbare Dienste und QoS abhängig von Providernetzwerk
- Einsatz zusätzlicher Hardware (DSL-Splitter/Modem) notwendig

Einsatzgebiete von DSL:

- Privatkundenanbindung
- Home-Offices mit VPN-Verbindung zu Firmennetzwerken
- Vernetzung weit entfernter Standorte bis maximal 6 km bei vorhandener Kupferdoppelader

2.2.4 ISDN

Integrated Services Digital Network (ISDN) ist ein leitungsvermittelndes Netzwerk dessen Grundlagen von ITU-T in folgenden Empfehlungen der I-Serie festgelegt wurden:

- I.100 series: General, structure, terminology
- I.200 series: Services and their characteristics
- I.300 series: Global network aspects and functions
- I.400 series: Interface between user and network
- I.500 series: Internetwork interfaces

Nachdem In Europa zunächst einzelne Länder auf Basis der I-Serien-Empfehlungen eigene ISDN-Standard-Varianten entwickelten und einsetzten– in Deutschland beispielsweise 1TR6

– mündete eine europäische Einigung in dem vom European Telecommunications Standards Institute (ETSI) genormten Euro-ISDN-Standard.
Die Signalisierung wird in den folgenden ITU-T Q-Serien Empfehlungen festgelegt:

- Q.921: ISDN user-network interface - Data link layer specification
- Q.931: Digital subscriber Signalling System No. 1 (DSS 1) - ISDN user-network interface layer 3 specification for basic call control

Bei ISDN stehen zwei Teilnehmer-Anschlussvarianten bzw. deren Vielfache und Kombinationen zur Verfügung:

- der ISDN-Basisanschluss mit 2 Nutzdatenkanäle à 64 kbit/s + 1 Datenkanal für Signalisierung und Steuerung mit 16 kbit/s so wie
- der ISDN-Primärmultiplexanschluss mit 30 Nutzdatenkanälen à 64 kbit/s + 1 Datenkanal für Signalisierung und Steuerung mit 64 kbit/s + 1 Steuerkanal mit 64 kbit/s.

ISDN überträgt G.711 kodierte Daten isochron. Alternativ können VoIP-Paketdaten mit Hilfe eines seriellen Protokolls wie PPP übertragen werden. Solange die Bandbreite nicht durch zusätzliche Paketdaten gestört wird, lassen sich mit Hilfe von ISDN VoIP-Daten nahezu störungsfrei übertragen. Im Unterschied zur nativen Sprachübertragung können mit Hilfe von VoIP mehrere komprimierte Sprachkanäle über einen 64 kBit/s-ISDN-Kanal übertragen werden. Dabei entsteht ein zusätzlicher Protokolloverhead durch die IP-basierten Protokollschichten.
Vorteile von ISDN:

- Sehr weit verbreitet
- Isochrone Übertragung, die jedoch nur bei nativer Sprachübertragung bzw. ausschließlicher Nutzung durch VoIP störungsfrei ablaufen kann
- Bandbreite in 64 kBit/s-Schritten skalierbar
- Einsatz von VoIP mit Hilfe von seriellem Protokoll PPP möglich
- Kompatibilität mit H.323-Signalisierung

Nachteile von ISDN:

- Bandbreite pro ISDN-Kanal für Dauer der Verbindung belegt. Keine anderweitige Verwendung nicht genutzter Bandbreite möglich
- Anfallende Verbindungsgebühren
- Bandbreite mit 2x64 kbit/s bzw. ganzzahligen Vielfachen sehr gering

Einsatzgebiete von ISDN:

- Privat- bzw. Geschäftskundenanbindung in öffentlichen und privaten Telefonnetzen

2.2.5 Frame Relay

Bei Frame Relay handelt es sich um eine paketvermittelnde Netzwerktechnologie, die sowohl vom ANSI als auch von der ITU-T standardisiert wurde und durch folgende grundlegende Standards beschrieben wird:

- ANSI-Standards:
  - Dienstebeschreibung T1.606
  - Hauptaspekte T1.618
  - Signalisierung T1.617

ITU-Standards:

- o Dienstebeschreibung I.233
- o Hauptaspekte Q.922 Annex A
- o Signalisierung Q.933

Frame Relay wird hauptsächlich im Weitverkehrsnetzbereich beispielsweise zur LAN-LAN-Kopplung verwendet und arbeitet ohne Fehlerkorrektur die von höheren Protokollschichten durchgeführt werden muss. Frame Relay nutzt das statistische Multiplexing, um mehrere Endanwender mit unregelmäßiger Bandbreitennutzung über einen einzelnen Port an ein paketvermittelndes Netz anzuschließen. Frame Relay basiert auf dem Paketnetzstandard X.25, ist jedoch lediglich ein Softwareprotokoll ohne eigene physikalische Schicht. Frame Relay kann deshalb u.a. mit folgenden Schicht-1-Netzwerktechnologien verwendet werden:

- X.21 / X.27
- V.24 / V.35
- HSSI (bis 52 MBit/s)
- E1 (2,048 MBit/s)
- E3 (34,368 MBit/s)
- DS1 (1,544 Mbit/s)
- DS3 (44,736 Mbit/s)

Frame Relay-Netze basieren auf virtuell vermaschten oder Punkt-zu-Punkt-Verbindungen in Verbindung mit Permanent Virtual Connections (PVCs) oder Switched Virtual Connections (SVCs), die gleichermaßen auch bei ATM verwendet werden. Für die Interoperabilität zwischen Frame Relay und ATM wurde eine Implementierungsvereinbarung zwischen dem Frame Relay- und dem ATM-Forum entwickelt. Aufgrund dieser Vereinbarung kann ATM z.B. als Backbone-Netz für Frame Relay-Netze eingesetzt werden und ermöglicht eine Investitionssicherung vorhandener Netzwerkstrukturen.

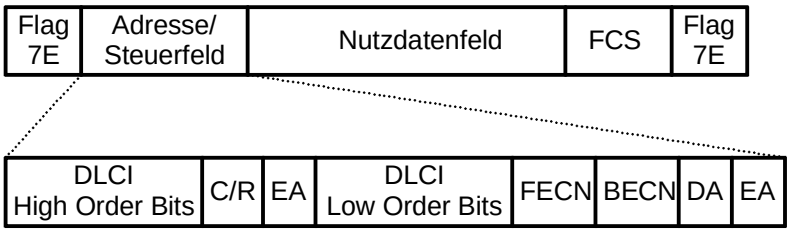

Bild 11: Aufbau des Frame Relay-Rahmens

Der Frame Relay-Rahmen enthält folgende Felder:

- DLCI (Data Link Connection Identifier, 10 Bit): Aufgeteilt in High- und Low-Order Bits, identifiziert die logische Verbindung.
- C/R (Command/Response Bit, 1 Bit): Unterscheidung von Kommando/Antwort.
- EA (Address Field Extension Bit, 1 Bit): Kennzeichnet Erweiterung des Headers auf 3 bzw. 4 Byte lange Header.
- FECN/BECN (Forward Explicit Congestion Notification/Backward Explicit Congestion Notification, jew. 1 Bit): Kennzeichnung einer Netzwerküberlastung.
- DE (Discard Eligibility Indicator, 1 Bit): Kennzeichnung von Frames, die bevorzugt verworfen werden dürfen.
- FCS (Frame Check Sequence, 16 Bit): Checksumme.

Eine garantiert verfügbare Mindestbandbreite kann als Committed Information Rate (CIR) festgelegt werden. Bei Überlast werden Pakete genauso wie bei fehlerhafter Übertragung einfach verworfen.

Vorteile von Frame Relay:

- „Soft"-Standard, gemeinsam mit unterschiedlichen Schicht-1-Technologien verwendbar
- Effektive Bandbreitennutzung durch statistisches Multiplexing zur Anbindung von Anwendern mit diskontinuierlichem Bandbreitenbedarf
- Festlegung einer Mindestbandbreite möglich
- Interoperabilität mit ATM
- Headerlänge beträgt im Normalfall lediglich zwei Byte

Nachteile von Frame Relay:

- Keine Fehlerkorrektur
- Begrenzte Bandbreite

Einsatzgebiete von Frame Reläy:

- Weitverkehrsnetzbereich z.B. zur LAN-LAN-Kopplung

2.2.6 ATM

Der Asynchronous Transfer Mode (ATM) ist ein paketorientiertes Übertragungsverfahren, für das unterschiedliche Organisationen wie z.B. ITU-T, IETF oder das ATM-Forum Standards entwickeln. Die grundlegenden Mechanismen sind in den ITU-T-Empfehlungen der I-Serie enthalten.
ATM verwendet zum Datentransport so genannte ATM-Zellen die aus genau 48 Byte Nutzdaten und einem 5 Byte langen Header bestehen. ATM unterscheidet zwei Zelltypen

- einen für die Schnittstelle zwischen Anwender und Netzwerk (User Network Interface – UNI) und
- einen zwischen Netzwerken (Network Network Interface – NNI).

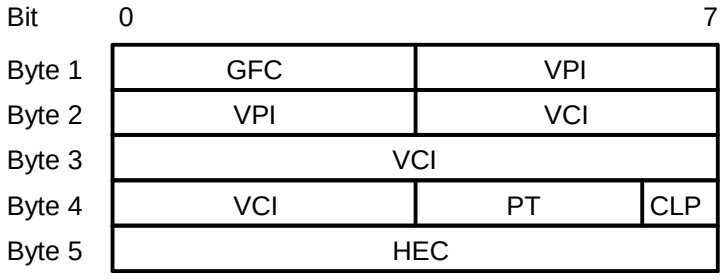

Bild 12: Aufbau des Headers für ATM-Zellen der UNI-Schnittstelle

Der UNI-Header enthält folgende Felder:

- GFC (Generic Flow Control, 4 Bit): Flusskontrolldaten, die aufgrund eines zuvor geschlossenen Verkehrsvertrages ausgetauscht werden.
- VPI Virtual Path Identifier, 8 Bit): Identifizierung von Kanalbündel
- VCI (Virtual Channel Identifier, 16 Bit): Identifizierung eines einzelnen Übertragungskanals
- PT (Payload Type, 3 Bit): Unterscheidung zwischen Nutz- und Managementdaten.
- CLP (Cell Loss Priority, 1 Bit): Markierung von verlustsensitiven Paketen, um Verwerfen bei Überlast zu vermeiden.
- HEC (Header Error Control, 8 Bit): Fehlerkorrekturbyte.

ATM-Zellen werden nach einem Zeitmultiplexverfahren übertragen, bei dem die einzelnen Zeitschlitze frei vergeben werden können. Die Zellen werden bei Bedarf eingefügt, weshalb

die Übertragungsart als asynchron bezeichnet wird. Sind keine Nutzdatenblöcke zu übertragen, werden Leerzellen eingefügt, so dass ein ununterbrochener Transport von Zellen durchgeführt wird. ATM eignet sich deshalb gut für die Übertragung von Bitströmen unterschiedlicher Datenraten.
ATM ist ein verbindungsorientiertes Verfahren, bei dem die Verbindung durch eine Kombination von virtuellem Pfad (Virtual Path Identifier - VPI) und virtuellem Kanal (Virtual Channel Identifier - VCI) repräsentiert wird. Virtuelle Pfade bündeln mehrere virtuelle Kanäle. Ein virtueller Kanal repräsentiert eine einzelne Verbindung. Bei einer Vermittlungsinstanz in einem ATM-Netz können entweder virtuelle Pfade, virtuelle Kanäle oder virtuelle Pfad-/Kanalpaare vermittelt werden. Die Vermittlung von virtuellen Pfaden ist von Bedeutung, weil Anwender damit die zugewiesenen Pfade frei mit virtuellen Verbindungen belegen können.

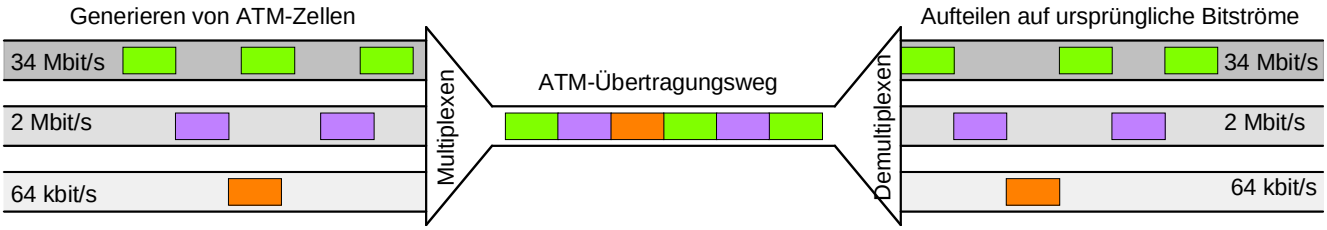

Bild 13: Asynchrones Zeitmultiplexverfahren für ATM-Zellen

ATM verwendet zum Abbilden von Nutzdatenströmen auf Zellen und umgekehrt Adaptionsschichten, so genannte ATM Adaption Layer (AAL). Folgende Adaptionsschichten werden unterschieden:

- AAL 1: Verbindungsorientierter Dienst mit konstanter Bit-Übertragungsrate (Circuit Emulation) und speziellen Timing-Anforderungen. Wird z.B. für Telefongespräche verwendet.
- AAL 2: Verbindungsorientierter Dienst mit variabler Übertragungsrate.
- AAL 3/4: Zusammenfassung zweier ursprünglich eigenständiger AAL-Varianten. Verbindungsorientierter oder verbindungsloser Dienst, der z.B. Übertragung von X15- oder IP-Paketen über ATM ermöglicht.
- AAL 5: Vereinfachte Spezifikation, ähnlich wie AAL 3/4 mit reduziertem Protokolloverhead.

Zur Übertragung verschiedener LAN-Protokolle, wie z.B. TCP, UDP und IP, über ATM wurde im ATM-Forum eine LAN-Emulation spezifiziert. Es handelt sich u.a. deshalb um eine Emulation von LAN-Netzwerken, weil damit verbindungslose IP-Dienste auf dem verbindungsorientierten ATM abgebildet werden.

Vorteile von ATM:

- Garantierte QoS für die gesamte Zeit der Verbindung möglich
- Bandbreite wird nur bei tatsächlicher Nutzung im Netzwerk belegt, flexible Anpassung an Anwendungen mit unterschiedlichen Datenraten

Nachteile von ATM:

- Hohe Anschaffungs- und Betriebskosten im Vergleich zu Ethernet
- Wenig verbreitet in LAN-Netzwerken, nicht kompatibel mit etablierter Ethernet-Technologie
- IP-Protokolle nur mit komplexer und administrativ aufwendiger LAN-Emulation nutzbar
- Eingeschränkte Übertragungsgeschwindigkeit gegenüber aktuellen Ethernet-Varianten

Einsatzgebiete von ATM:

- Backbon-Netze von Providern oder von größeren Firmen-LANs
- High-Performance-LANs für spezielle Anwendungen

2.2.7 Weitere Netzwerke

Voice over IP kann auch über folgende Netze übertragen werden:

- Token Ring-Technologie
- FDDI
- Wireless LAN
- Universal Mobile Telecommunication System (UMTS)

2.3 Faxübertragung

Fax over IP (FoIP) stellt besondere Anforderungen an die Echtzeitkommunikationsfähigkeiten von VoIP-Systemen und wird daher von den Herstellern als eigenständiges Feature angesehen und vermarktet.
Grundsätzlich sind VoIP-Systeme nicht ohne zusätzliche Maßnahmen zur Faxübertragung geeignet. Die Faxübertragung basiert auf einer Modulation, mit der die „Daten" einer zu übermittelnden Seite als Bildinformation kodiert werden. Bei Einsatz von komprimierenden Sprachcodecs in VoIP-Netzen wird die Modulation verfälscht, weil die Codecs keinen linearen Frequenzgang besitzen. Auch bei Verwendung eines G.711-Codecs, der unkomprimierte PCM-Daten übermittelt, bleibt die Faxübertragung über IP-Netze problematisch, obwohl dieses Verfahren in ISDN-Netzen bei isochroner Datenübertragung eingesetzt wird und dort reibungslos funktioniert. IP-Netze bieten, bis auf einzelne Sonderfälle, keine isochrone Übertragung. Insbesondere der Jitter in IP-Netzen verhindert eine erfolgreiche Faxkommunikation, während das Delay aufgrund ausreichend hoher Timeout-Zeiten bei der Fax-Übertragung relativ unkritisch ist.
Maßgeblich für erfolgreiche FoIP-Übertragungen sind geeignete Codecs, die mit zusätzlichen Maßnahmen zur Reduzierung von Paketlaufzeit-Änderungen eingesetzt werden. Speziell für Fax-Übertragung konfigurierte Jitter-Algorithmen reduzieren die Paketlaufzeitänderungen auf ein tolerierbares Maß.
In analogen Telefonnetzen hat sich der T.30 Standard der ITU-T für Fax-Kommunikation etabliert. Die Kodierung ist in der Empfehlung T.4 (Fax Gruppe 3) enthalten. Die Fax Gruppe 4 der ITU-Empfehlung T.6 enthält eine andere, zweidimensionale Kodierung und unterstützt mit 400 dpi die doppelte Auflösung im Vergleich zur Fax Gruppe 3, ist jedoch noch nicht weit verbreitet. Fax-Dokumente der Gruppe 4 können direkt ohne Umwandlung in digitaler Form z.B. über ISDN übertragen werden, wobei die Übertragung nicht mit Gruppe 3-Faxgeräten kompatibel ist.
Der T.30 Standard wird in IP-Netzen durch die Standards T.37 (Store-and-Forward-Fax) oder T.38 (Realtime Fax) ersetzt. T.38 der ITU-T hat sich inzwischen weltweit als Standardlösung für Fax-over-IP etabliert.
In einem IP-Netzwerk werden eingehende Fax-Anrufe, die aus dem PSTN kommen, stets vom VoIP-Gateway bzw. der TK-Anlage mit Hilfe von Auto-Sensing-Funktionen erkannt. Anschließend werden die Anrufe nicht als VoIP-, sondern als Fax-Verbindung mit entsprechenden Protokollen zwischen Gateway und Endgerät behandelt.
Einige Hersteller haben trotz des verfügbaren T.38-Standards Versuche unternommen, analoge Faxübertragungen mit T.30 über Gateways bei Verwendung von G.711-Sprachkodierungen in IP-Netze zu übertragen. Hierfür ist ein Jittermanagement notwendig, das Faxübertragungen erkennt und extrem lange Jitterbuffer für die Dauer einer T.30-Übertragung verwendet. Trotzdem funktioniert das Verfahren in der Praxis nur für eine be-

grenzte Anzahl, nach Herstellerangaben ca. 5-10 aufeinander folgende Seiten, und führt früher oder später zu einem Übertragungsabbruch.

3 Dienstgüte und Sicherheit

3.1 Dienstgüte in IP-Netzen

Die Dienstgüte wird allgemein auch als Quality of Service (QoS) bezeichnet und wird bei VoIP-Lösungen hauptsächlich an ihren Echtzeiteigenschaften gemessen wobei eine verständliche, echtzeitnahe Sprachübertragung im Mittelpunkt steht. Neben der verfügbaren Bandbreite sind die Parameter Delay, Jitter und Fehler- bzw. Verlustfreiheit der übertragenen Daten maßgeblich für eine hohe Dienstgüte bei der Sprachübertragung verantwortlich. Während ausreichend verfügbare Bandbreite eine grundlegende Voraussetzung für den Einsatz von VoIP ist, wird die auftretende Verzögerungszeit als wichtigstes Kriterium für eine optimale Übermittlung von Echtzeitdaten angesehen.
Folgende Verfahren werden in IP-Netzwerken eingesetzt, um eine Verbesserung der Dienstgüte zu erreichen:

- Ressourcenreservierung,
- Priorisierungsmechanismen,
- Fehlerkorrektur durch Redundanzmechanismen,
- Label Switching und
- Netzwerkmanagement.

3.1.1 Ressourcenreservierung

Die benötigte Bandbreite muss in Paketnetzen für die gesamte Zeit der Sprachübertragung uneingeschränkt zur Verfügung stehen. Ein Ansatz, dieses Ziel zu erreichen, ist ein Ressourcenmanagement. Die benötigte Bandbreite wird vor Aufbau einer Verbindung auf der gesamten Übertragungsstrecke zwischen den Endgeräten reserviert. Dabei wird eine feste Wegewahl (Routing) für alle Datenpakete der Verbindung durchgeführt.
Der ATM-Standard unterstützt einen Constant Bit Rate (CBR)-Modus für die Reservierung von Bandbreite während des Verbindungsaufbaus. Entsprechende Fähigkeiten müssen in Ethernet-Netzwerken durch zusätzliche Maßnahmen wie dem **RSVP-Protokoll** nachgerüstet werden das voraussetzt, dass alle Netzwerkkomponenten, die sich innerhalb der Übertragungskette zwischen den Endgeräten befinden, RSVP unterstützen. Ist dies nicht der Fall kann RSVP trotzdem eingesetzt werden, die Bandbreite jedoch nicht garantiert werden.
Das RSVP-Protokoll wird auf Layer 4-Ebene über UDP/TCP eingesetzt.

3.1.2 Priorisierungsmechanismen

Diese bewirken eine bevorzugte Weiterleitung von Datenpaketen nach dem Best Effort-Prinzip in den Netzwerkkomponenten. Eine Garantie von Dienstgütemerkmalen ist mit diesen Verfahren nicht möglich.

3.1.3 Fehlerkorrektur durch Redundanzinformationen

Mit Hilfe eines Forward Error Correction (FEC)-Verfahrens werden den VoIP-Sprachdaten Redundanzinformationen hinzugefügt. Bei Paketausfällen können die fehlenden Daten aufgrund der Redundanz nachträglich berechnet werden, ohne dass es zu Störungen in der Sprachwiedergabe kommt. Die benötigte Bandbreite erhöht sich mit dem Anteil der Redun-

danzinformationen im Datenstrom. Das Delay erhöht sich durch die benötigte Zeit, die für die Wiederherstellung der Sprachdaten benötigt wird.
FEC unterscheidet zwei unterschiedliche Verfahren:

- die Intrapacket-FEC fügt Redundanzinformationen innerhalb eines Datenpaketes ein und
- die Extrapacket-FEC versendet Redundanzinformationen in separaten Datenpaketen.

3.1.4 Label Switching

Die Multiprotocol Label Switching (MPLS)-Technologie hat das Ziel, IP-Pakete einer Verbindung mit besonders geringer Verzögerung über dieselbe Route zu leiten, ohne dass der Datenstrom von anderen Nutzern beeinflusst oder gelesen werden kann. Mit MPLS können, verbindungsorientierte Eigenschaften, die als Vorteil von ATM gelten, auch im Ethernet eingeführt werden. MPLS ist nicht auf Ethernet-Netze beschränkt, sondern ist zwischen der Schicht 2 und der Schicht 3 angesiedelt. Deshalb können unterschiedliche Netzwerkprotokolle im Zusammenhang mit MPLS verwendet werden.

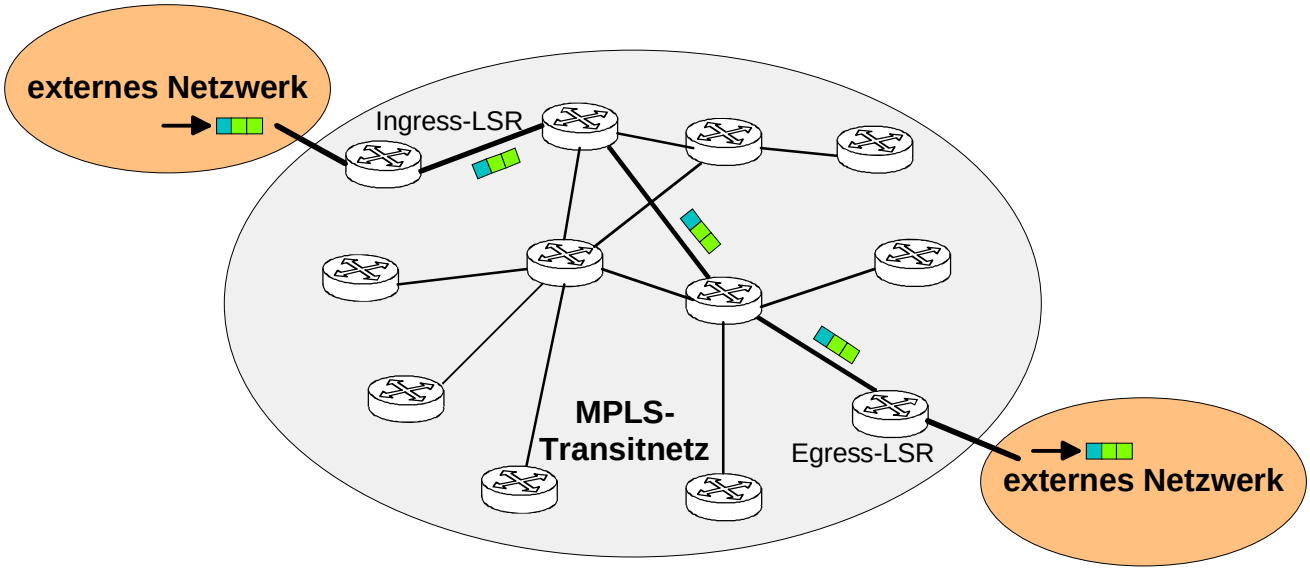

Bild 14: MPLS als Transitnetz

MPLS bietet die Möglichkeit, garantierte Dienstgüte (QoS) in IP-Netzen zu implementieren. Gleichzeitig ermöglicht es den Aufbau von Virtual Private Networks (VPN), bei denen die Teilnehmer eines VPN-Netzes nicht durch andere Netzwerkteilnehmer abgehört oder gestört werden können.
MPLS-Netze sind durchgängig mit Label Switched Routern (LSR) ausgestattet, die Wege von Datenpaketen über Label Switched Paths (LSP) festlegen können. Die Label Switched Paths (LSPs) werden in einer Konfigurationsphase mit Hilfe des Label Distribution Protocol (LDP) zwischen benachbarten LSRs vereinbart und haben nur eine lokale Gültigkeit in der Kommunikation zwischen den beteiligten Netzwerkknoten.
An einem Eingang zu einem MPLS-Netzwerk, dem so genannten Ingress-LSR, werden IP-Pakete analysiert, klassifiziert und an eine Forwarding Equivalence Class (FEC) gebunden. Anschließend werden die Pakete mit einem Label versehen und in das MPLS-Netz eingespeist. Die Pakete werden über den zuvor festgelegten Label Switched Path geleitet. Das Label beschreibt den Weg zum jeweils nächsten benachbarten MPLS-Netzwerkknoten. Für IP-Netze hat diese Vorgehensweise zur Folge, dass nicht mehr die IP-Header in den MPLS-Routern ausgewertet werden. Stattdessen werden nur noch die Label mit 32 Bit Länge für die Weiterleitung eines IP-Pakets verwendet. In jedem Netzwerkknoten innerhalb des MPLS-

Netzes wird das Label interpretiert und möglicherweise entfernt bzw. durch ein oder mehrere neue Label ersetzt. Anschließend erfolgt die Weiterleitung zum nächsten LSR. Am Ausgang des MPLS-Netzwerks, dem Egress-LSR, wird lediglich das Label entfernt.
Im MPLS-Header können mehrere Label enthalten sein, die zusammen einen Stack bilden und nach dem Prinzip Last-in-first-out (LIFO) ausgewertet werden. Dieser Stack wird in einer hierarchisch aufgebauten Netzwerkstruktur verwendet, bei der sich die Pakete in verschiedenen Stufen der Netzwerkhierarchie bewegen.

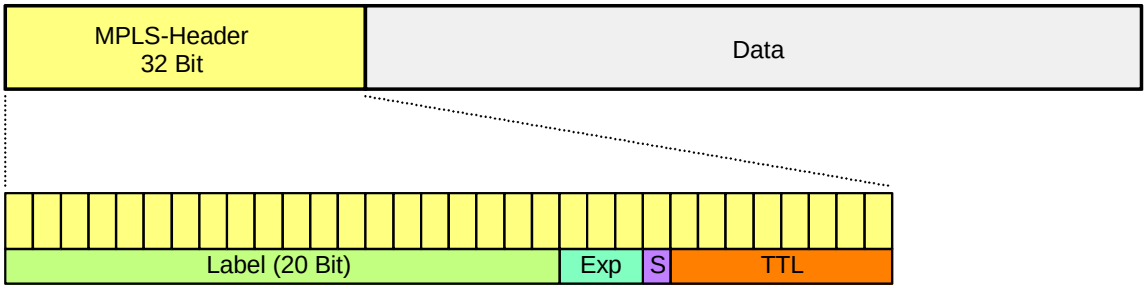

Bild 15: MPLS-Header

Der MPLS-Header enthält folgende Felder:

- Label (20 Bit): Label, das Weiterleitungsinformation enthält.
- Exp (Experimental, 3 Bit): Für experimentelle Zwecke vorgesehen, kann für Class-of-Service-Mapping verwendet werden.
- S (Stacking Bit, 1Bit): Bei mehreren Labeln, die sich zwischen dem Header des Data Link Layer (z.B. Ethernet) und dem Header des Network-Layer befinden, wird im letzten Label das Stacking Bit als Kennzeichnung gesetzt.
- TTL (Time To Live, 8Bit): „Lebensdauer" eines Telegramms. Kennzeichnet wie beim gleichnamigen IP-Header-Feld, über wie viele Netzwerkknoten hinweg ein Telegramm transportiert werden darf.

Ende-zu-Ende Quality of Service mit MPLS
MPLS (Multiprotocol Label Switching) ist eine Netzwerktechnologie, die nicht im Endgerät verfügbar ist, sondern im Netzwerk verwendet wird. Um Ende-zu-Ende-QoS zu ermöglichen, müssen zwei QoS-Arten in Verbindung stehen: Endgeräte-QoS wird zwischen Endgerät und dem Eingang (Ingress LSR) des MPLS-Netzwerkes bzw. dessen Ausgang (Egress LSR) etabliert. QoS im MPLS-Netz muss zwischen Ingress- und Egress-LSR unterstützt werden.
In IP-Netzen wird ein Austausch zwischen dem DiffServ-DSCP-Datenfeld und MPLS favorisiert. Zwei unterschiedliche Methoden können verwendet werden:

- Label-inferred LSPs (L-LSPs): Hierbei wird am Ingress-LSR das DSCP-Feld ausgelesen und einem MPLS-Label zugeordnet, das der Quality-of-Service-Definition in DiffServ entspricht. Entlang des LSPs werden die Label entsprechend der QoS-Anforderungen interpretiert.
- Experimental LSPs (E-LSPs): Sie verwenden das drei Bit lange Experimental-Feld des Labels, um maximal acht DSCP-Serviceklassen zu unterscheiden. Der Ingress-LSR bildet die DiffServ-Codepoints auf die EXP-Bits ab und leitet diese über den Pfad von LSRs, die E-LSP unterstützen. Jeder Netzwerkknoten behandelt das Paket wie ein IP-basierter DiffServ-Netzwerkknoten anhand der DiffServ-Regeln.

3.1.5 Netzwerkmanagement

In geschlossenen Netzen werden die Regeln (Policies) für Quality-of-Service (QoS) zentral definiert wodurch sichergestellt wird, dass alle Netzwerkkomponenten eine einheitliche Sicht der Parameter erhalten. Diese Informationen werden üblicherweise mit Hilfe eines Netz-

werkmanagement-Protokolls von einem zentralen Netzwerkmanagementsystem auf die einzelnen Netzwerkkomponenten (Switches, Router, VoIP-Gateways etc.) verteilt.
Das Simple Network Management Protocol (SNMP) hat sich im Netzwerkmanagement weltweit als Standard durchgesetzt. Es verwendet einzelne Management Information Base (MIB)-Datenstrukturen zur Konfiguration, die eine Liste von Variablen unterschiedlicher Datentypen und auch Tabellen enthalten können. MIB-Daten sind hierarchisch als Baumstruktur aufgebaut und verwenden pro Datenelement jeweils einen Object Identifier (OID) zur Kennzeichnung einer Variablen. Für DiffServ ist beispielsweise der Internet Draft „Management Information Base for the Differentiated Services Architecture" (RFC 3289) in Verwendung. Zusätzlich hat die Network Working Group der IETF die Empfehlung „A Framework for Policy based Admission Control" als RFC 2753 veröffentlicht. Für spezielle Anwendungsfälle werden Policy Information Base (PIB)-Datenstrukturen definiert, die über Netzwerkmanagement-Protokolle wie SNMP eine Datenbasis für regelbasierten QoS anbieten, um sie auf eine Anzahl von Netzwerkkomponenten zu verteilen.

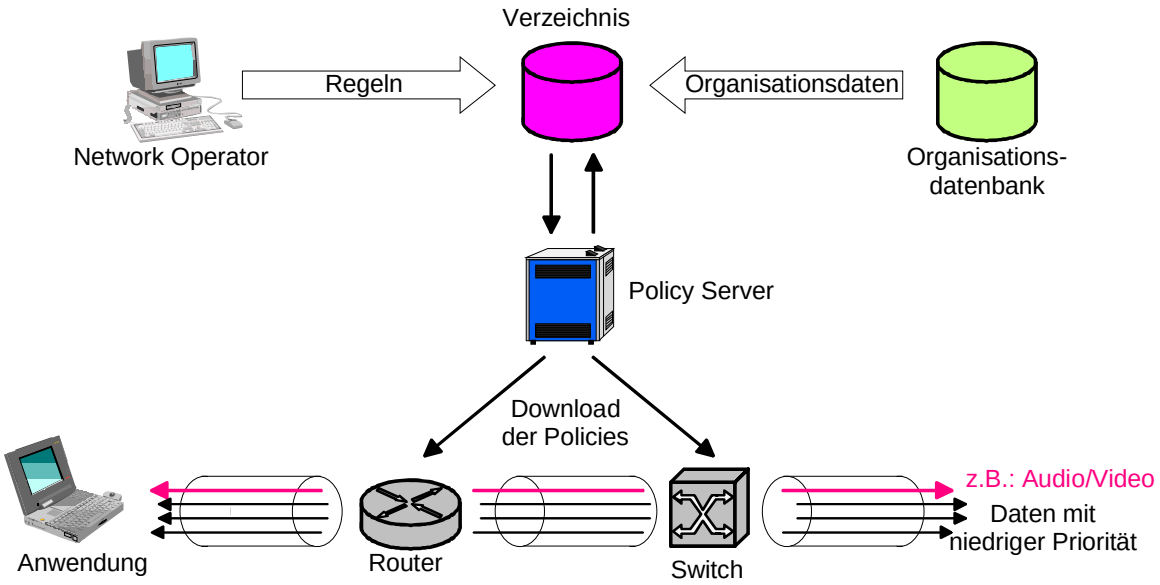

Bild 16: Regelbasierte Implementierung von QoS

3.2 Sicherheit in IP-Netzen

Um die Übertragung von Informationen über digitale Netze zu sichern, sind verschiedene Verfahren entwickelt worden. Die wichtigsten Sicherheitsverfahren dienen der

- Authentifizierung (Authentication): Authentifizierung wird eingesetzt, um die Identität des Absenders von Daten verifizieren zu können.
- Verschlüsselung (Confidentiality/Privacy): Die Nutzdaten oder vollständige Datentelegramme inklusive aller oder Teile der Headerinformationen werden verschlüsselt übertragen, um sie vor unbefugtem Zugriff zu schützen.
- Zugangsberechtigung (Authorization): Die Teilnehmeridentifikation wird überprüft, um die Zugriffsberechtigung auf Daten zu überprüfen.
- Integritätssicherung (Integrity): Sicherung der Informationen gegen Veränderung durch Unbefugte.

Authentifizierung und Verschlüsselung sind die wichtigsten Sicherheitsmaßnahmen, die in VoIP-Umgebungen notwendig sind. In Produkten für handelsübliche VoIP-Inhouse-Lösungen wird Verschlüsselung und Authentifizierung fast gar nicht eingesetzt, im WAN-Bereich ist ins-

besondere IPSec mit ESP (IP Encapsulating Security Payload) und AH (IP Authentification Header) vertreten.
In der Praxis ist zu beachtet, dass bei Einsatz von Sicherungsverfahren die Bandbreitenanforderung signifikant ansteigt. Bei Einsatz von IPSec mit ESP (IP Encapsulating Security Payload) und AH (IP Authentification Header) tritt dadurch fast eine Verdoppelung des Bandbreitenbedarfs auf.

3.2.1 Grundlegende Protokolle

- AH (IP Authentication Header) RFC 2402 [80]
- ESP (IP Encapsulating Security Payload) RFC 2406 [81].
- TLS (Transport Layer Security)

AH (IP Authentication Header)
Im Transport Mode werden für das AH-Protokoll Sicherheitsdienste auf Teile des IP-Headers, des Extension-Headers und die Optionsfelder erweitert.
Der AH-Header wird bei IPv4 zwischen dem IP-Header und dem Payload höherer Protokollschichten eingefügt. Bei IPv6 wird AH nach dem Hop-by-Hop-Feld und vor den Destination-Options eingefügt.

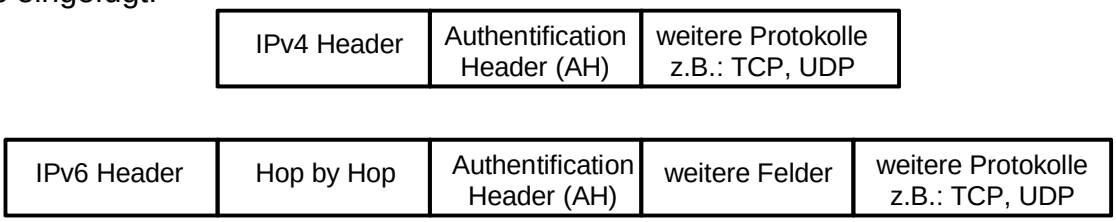

Bild 17: Authentification Header (AH) mit IPv4 und IPv6

ESP (IP Encapsulating Security Payload)
Es sind zwei Betriebsarten möglich:

- Transport-Mode:
  In dieser Betriebsart wird eine Securit Association SA zwischen den Kommunikations-Endgeräten gebildet. Für das ESP-Protokoll werden Sicherheitsdienste nur für Protokolle angeboten, die auf IP aufsetzen, nicht jedoch für die IP-Schicht selbst.
- Tunnel-Mode:
  Er wird zwischen Security-Gateways verwendet, kann aber auch zwischen Endgeräten bzw. zwischen Security-Gateway und Endgerät eingesetzt werden. In der Praxis wird diese Variante eingesetzt, um beispielsweise bei einer Standortvernetzung eines Unternehmens den unsicheren Übertragungsweg über ein Providernetz abzusichern, ohne dass die Endgeräte selbst Sicherheitsverfahren unterstützen müssen. In der Tunnel-Betriebsart werden zwei IP-Header verwendet: Der äußere Header enthält die nächste IP-Zieladresse, während der innere Header die eigentliche Zieladresse enthält.

Im Transport Mode wird der ESP-Header nach dem IPv4- bzw. IPv6-Header eingefügt. Am Ende des Pakets folgt ein ESP-Trailer und ein ESP-Authentification-Feld.

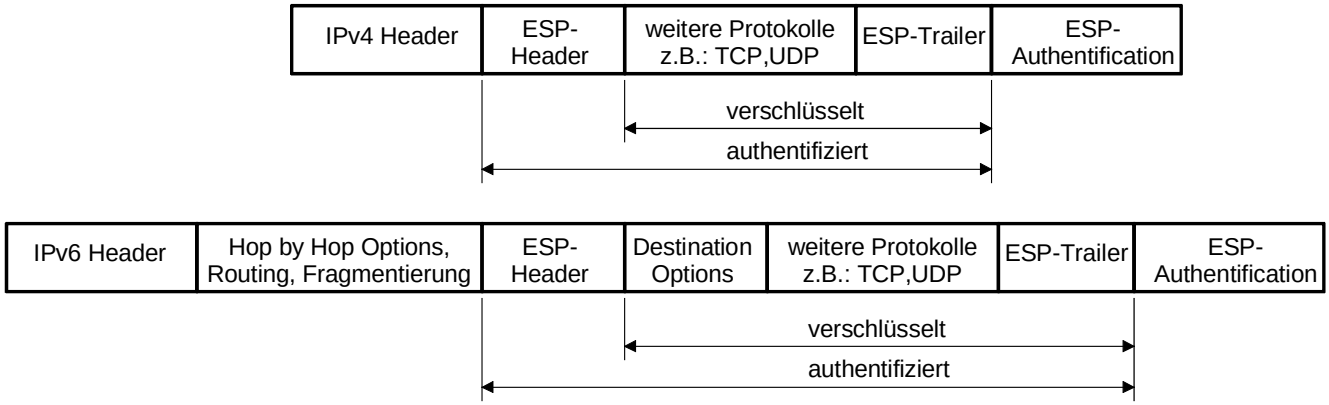

Bild 18: ESP-Header mit IPv4 und IPv6 (Transport Mode)

Im Tunnel-Mode wird ein neuer IPv4- bzw. IPv6-Header erzeugt. Anschließend wird bei IPv4 der ESP-Header eingesetzt, bei IPv6 folgen zuvor noch die Extension-Header. Am Ende des Pakets folgt ein ESP-Trailer und ESP-Authentification-Feld.

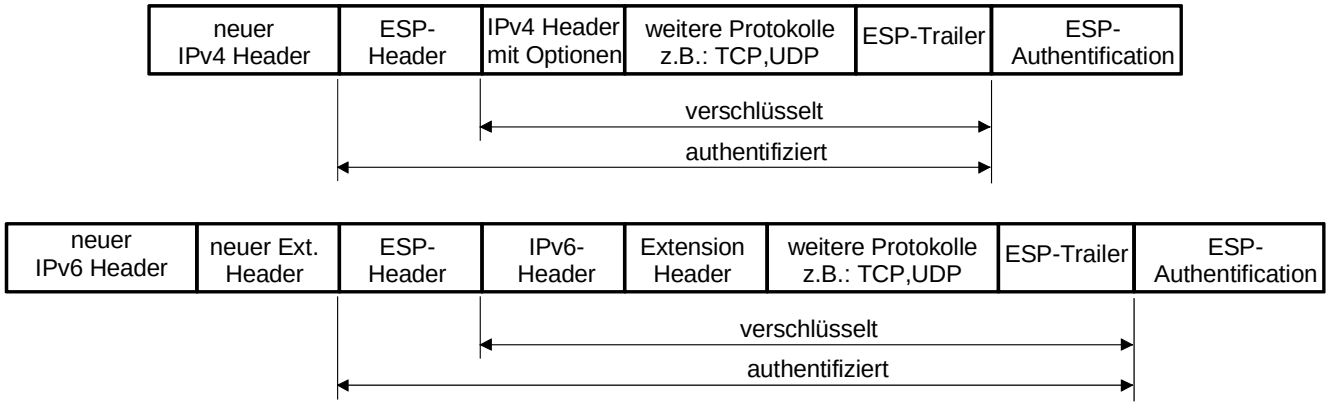

Bild 19: ESP-Header mit IPv4 und IPv6 (Tunnel Mode)

TLS (Transport Layer Security)

Transport Layer Security (TLS) ist eine neuere Version des SSL-Protokolls (Version 3) von Netscape und ist als „The TLS Protocol Version 1.0" [83] (RFC 2246) der IETF veröffentlicht worden. HTTP-Übertragungen mittels HTTPS werden üblicherweise mit Hilfe von TLS/SSL durchgeführt.

TLS setzt auf gesicherten Transportprotokollen, wie beispielsweise TCP, auf. Die grundlegenden Eigenschaften umfassen eine private und gesicherte Ende-zu-Ende-Kommunikation. Das Protokoll besteht aus dem TLS Record Protocol und dem TLS Handshake Protocol.

Die private, verschlüsselte Kommunikation wird durch Verfahren wie DES, RC4 etc. ermöglicht. Die symmetrischen Schlüssel werden speziell für eine Kommunikationsverbindung generiert und basieren auf einem ausgehandelten Shared Secret. Die Aushandlung kann durch das TLS Handshake Protocol erfolgen, bevor eine darauf aufsetzende Anwendung Daten sendet.

Der gesicherte Datentransport wird durch Integritätsprüfungen erreicht. Hash-Funktionen wie SHA oder MD5 werden zur Berechnung verwendet.

Die Identität der Gegenstellen kann mit Hilfe asymmetrischer oder Public-Key-Verfahren (z.B. RSA, DSS) sichergestellt werden.

3.2.2 H.323-Sicherheit

H.323 ermöglicht mit Hilfe der ITU-T Empfehlung H.235 „Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals" folgende Sicherheitsdienste für die Sicherung von Signalisierungs- und Mediendaten:

- Authentifizierung
- Verschlüsselung
- Integritätssicherung

Authentifizierung

Die Authentifizierung des Benutzers wird durch das H.235 Protokoll unterstützt. Der Austausch von Sicherheitszertifikaten wird im Protokoll festgelegt, nicht jedoch deren Art oder Behandlung. In H.235 sind zwei Arten der Authentifizierung vorgesehen:

- eine Methode basiert auf symmetrischer Verschlüsselung (Diffie-Hellman), so dass vor dem Verbindungsaufbau keine Informationen der Gegenstellen notwendig sind,
- die andere Methode basiert auf der Shared-Secret-Methode, die auch als subscription-based bezeichnet wird. Hierbei werden vor Verbindungsaufbau zwischen den Gegenstellen Informationen ausgetauscht, die entweder Passwort- oder Zertifikat-Informationen enthalten.
  Die Shared-Secret-Methode wird in drei Kategorien eingeteilt:
  - Password-basiert mit symmetrischer Verschlüsselung wobei User-iD und Passwort zwischen den Kommunikationspartnern ausgetauscht werden.
  - Password-basiert mit Hashing wobei der Schlüssel aus dem Passwort generiert wird und mit dem Passwort identisch ist, falls Passwortlänge und Schlüssellänge übereinstimmen. Falls das Passwort kürzer ist, wird es mit Nullwerten aufgefüllt (Padding). Längere Passwörter werden zyklisch oktettweise mit der logischen XOR-Funktion verknüpft.
  - Zertifikat-basiert mit Signaturen wobei User-ID und Zertifikat zwischen den Kommunikationspartnern ausgetauscht werden.

Sicherung des Rufaufbaus

Zur Sicherung des Rufsignalisierungskanals ist entweder der Einsatz von IPSec oder TLS (Transport Layer Security) vorgeschrieben,

Sicherung der Rufsteuerung

Um eine Verschlüsselungsmethode zwischen den Endgeräten auszuhandeln und um Sicherheitsschlüssel auszutauschen wird ein H.245-Rufsteuerungskanal (Call Control Channel) verwendet. Verschiedene Medienkanäle (RTP-Kanäle) können mit unterschiedlichen Verschlüsselungsmethoden bedient werden.

Sicherung der Medienkanäle

Um eine Sicherung der Medienkanäle zu erreichen, kann bereits ein gesicherter (verschlüsselter) H.245-Rufsteuerungskanal verwendet werden, um die ASN.1-kodierten Sicherheitsschlüssel für die Medienkanäle auszutauschen.

3.2.3 SIP-Sicherheit

SIP ist ein reines Signalisierungsprotokoll. Die Verschlüsselung und Authentifizierung der Kommunikation muss deshalb zwischen den Endgeräten unabhängig von der Signalisierung behandelt werden. Das SIP-Protokoll unterscheidet sich von anderen Protokollen dadurch, dass der Header nicht aus Bitfeldern, wie bei TCP, UDP oder IP, besteht, sondern aufgrund der Entwicklung aus HTTP heraus aus ASCII-Strings. Aus diesem Grund gibt es Ähnlichkeiten zur E-Mail-Übertragung.

Ende-zu-Ende-Verschlüsselung
Die Übertragung einer verschlüsselten SIP-Nachricht kann mit Hilfe folgender Methoden durchgeführt werden:

- S/MIME: Die Verschlüsselung zwischen den Endgeräten wird durch „Secure/Multipurpose Internet Mail Extensions" (S/MIME)-Methoden ermöglicht. Aufgrund des textbasierten Charakters von SIP-Messages können diese, ursprünglich für E-Mail und HTTP-Anwendungen entwickelten Methoden, in Zusammenhang mit SIP eingesetzt werden.
- HTTP-Basic und Digest Schema: wurde von IETF als RFC 2617 veröffentlicht und bietet Authentifizierung des Anrufers und des Angerufenen durch „HTTP Authentication: Basic and Digest Access Authentication". Während das Basic-Schema User-ID und Passwort als Klartext überträgt und somit abgehört werden kann, bietet das Digest-Schema ein verschlüsseltes Verfahren. Das Basic-Schema wird von SIP inzwischen, wie im RFC 3261 beschrieben, nicht mehr unterstützt.

Hop-by-Hop-Verschlüsselung
Hop-by-Hop-Verschlüsselung wird entweder durch das TLS-, AH- oder ESP-Protokoll ermöglicht.

4 Protokolle und Standards

Die VoIP-Technologie befindet sich in einem kontinuierlichen Entwicklungsprozess und es werden laufend bestehende Verfahren um neue Features erweitert oder es kommen neue hinzu.
Neben ITU und IETF, die maßgeblich für die Entwicklung der bei VoIP eingesetzten Standards verantwortlich sind, veröffentlichen folgende Organisationen Protokolle und Standards im Telekommunikationsbereich, die für VoIP relevant sind:

- European Computer Manufacturer's Association (ECMA)
- European Telecommunications Standards Institute (ETSI)
- International Organization for Standardization (ISO)
- Institute of Electrical and Electronics Engineers (IEEE)

4.1 IP basierte Signalisierung und Verbindungssteuerung

Um bei VoIP-Telefonie die Merkmale der konventionellen Telefonie wie z.B.: Frei- und Besetztton nützen zu können ist ein „Verbindungsaufbau“ durch den Austausch von Signalisierungsnachrichten ähnlich der konventionellen Telefonie erforderlich. Derzeit werden zur IP basierten Signalisierung und Verbindungssteuerung im VoIP-Bereich der

- Standard H.323 der ITU-T mit dem Titel „Packet based multimedia communications systems" oder das
- Session Initiation Protocol (SIP) der IETF (RFC 3261) verwendet.

Der Standard H323 der ITU-T existiert seit 1996 und ist durch die lange Historie sehr weit verbreitet. H.323 wird auch als Dachstandard bezeichnet, weil er neben einer genauen Detaildefinition paketbasierter Multimediasysteme auch auf einige weitere Standards Bezug nimmt und diese implizit in die eigene Spezifikation integriert.
Das Session Initiation Protocol (SIP) der IETF wurde 1999 eingeführt und hat sich innerhalb kurzer Zeit als direkter Konkurrent zu H.323 sehr schnell verbreitet, obwohl die Standardisierung zum gegenwärtigen Zeitpunkt noch nicht abgeschlossen ist. Fast alle namhaften Hersteller haben SIP-Implementierungen oder haben zumindest angekündigt, SIP zukünftig zu

unterstützen, obwohl H.323 immer noch als bewährte und praxiserprobte Basis angesehen wird.

4.1.1 Dachstandard H.323

Der Standard H.323 der ITU-T besitzt den Titel „Packet based multimedia communications systems", die derzeit aktuelle Version stammt vom November 2000. Der Standard definiert ein vollständiges, funktionierendes Multimedia-System für Audio und Video. Von der Signalisierung über die Paketisierung bis zur Verwendung von Kodierungen sind alle Einzelheiten festgelegt. H.323 wird auch als vertikaler Standard bezeichnet, weil er alle benötigten Protokolle für eine Audio-Videokommunikation definiert, bzw. auf untergeordnete Standards verweist. Aufgrund der vollständigen Systemdefinition ist H.323 sehr komplex.
Die wichtigsten Unterstandards sind:

- H.245 „Control protocol for multimedia communication" und
- H.225.0 „Call signalling protocols and media stream packetization for packet-based multimedia commtmication systems".
  Zwischen beiden Unterstandards besteht ein enger Zusammenhang. Beispielsweise werden über den H.225.0-Layer sämtliche Daten zwischen Endgeräten ausgetauscht, so dass H.245-Nachrichten für die Übertragung auf H.225.0 angewiesen sind.

Im Standard H.323 sind Wählverbindungen oder Punkt-zu-Punkt-Verbindungen, die auf paketbasiertem Datentransport wie z.B. PPP aufsetzen, eingeschlossen. Gateways ermöglichen die Interoperabilität mit Systemen, die auf korrespondierenden Standards wie z.B. H.310 (B-ISDN bzw. ATM) oder H.320 (ISDN) beruhen. Für den Einsatz von H.323 ist Ethernet als Netzwerkplattform am weitesten verbreitet.
Im Standard H.323 sind folgende Systemkomponenten definiert:

- Terminal
- Gateway
- Gatekeeper
- Multipoint Control Unit (MCU)
  - Multipoint Controller (MC)
  - Multipoint Processor (MP)

Terminal
Terminals können direkt mit ihrer Netzwerk-Transportadresse adressiert werden. Für diese Kommunikation ist kein Gatekeeper notwendig. Zusätzlich besteht die Möglichkeit, einzelnen Terminals so genannte Alias-Adressen zuzuordnen, die innerhalb einer Gatekeeper-Zone eindeutig sein müssen. Alias-Adressen können z.B. E.164-Adressen (Telefonnummern), alphanumerische Zeichenketten oder auch E-Mail-ähnliche Adressbezeichnungen sein. Die Alias-Adresse wird vom Gatekeeper aufgelöst und in die zugeordnete Transport-Adresse umgewandelt. Ein H.323-Terminal (Endgerät) besteht aus folgenden Funktionseinheiten:

- Video-Codec (optional): Der Video-Codec muss mindestens das H.261-Kodierverfahren im CIF-Format (352*288 Pixel) unterstützen. Die Einstellung der Bildparameter wird beim Austausch der Fähigkeiten im H.245-Protokoll festgelegt.
- Audio-Codec: Alle Terminals sollten asymmetrisch arbeiten können und Audio nach dem G.711-Standard mit A-law- und µ-law-Quantisierung in Sende- und Empfangsrichtung unterstützen können. Die Formatierung der Audio-Daten erfolgt nach dem Unterstandard H.225.0.
- Datenübertragungskanäle (optional): Sie können zusätzlich verwendet werden, um neben Audio- und Video auch beliebige Datenapplikationen wie z.B. Anwendungen für Dateitransfers oder Shared Whiteboards zum gemeinsamen Bearbeiten von Zeich-

nungen und Texten nutzen zu können.
Für die Datenübertragung können beliebige Standards genutzt werden. Der Datenübertragungsstandard T.120 muss jedoch bei Verwendung von Datenkanälen zumindest unterstützt werden.

- H.225.0 Layer: Als zentrale Schicht für den Datenaustausch ist der H.225.0 Layer für die Formatierung der Nutz- und Steuerungsdaten in Senderichtung und für die Entnahme der Daten in Empfangsrichtung zuständig. Die Aufteilung der Daten in logische Rahmen und die Sequenznummerierung wird ebenfalls in dieser Schicht durchgeführt.
- Paketbasiertes Netzwerkinterface: Die Anforderungen an das Interface sind in H.225.0 formuliert. Die Art des Netzwerkinterfaces und dessen Eigenschaften sind jedoch nicht festgelegt.

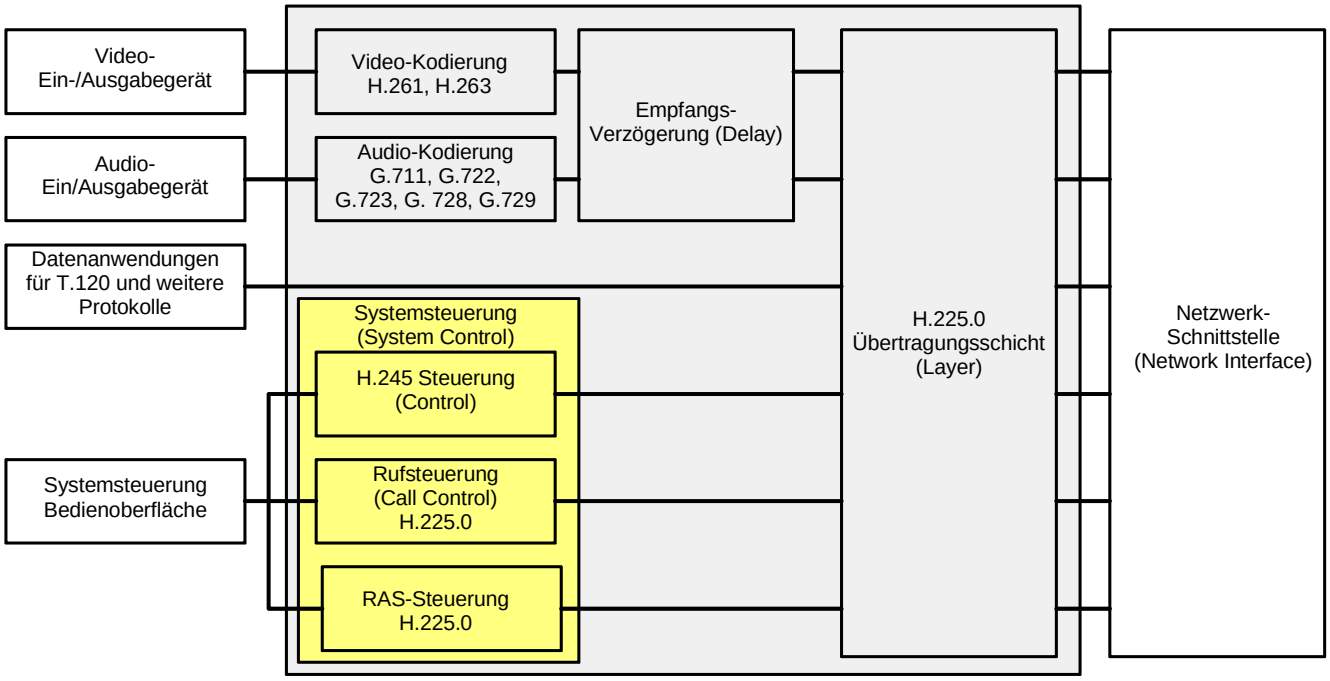

Bild 20: H.323-Terminal Blockstruktur und Definitionsbereich

Gateway

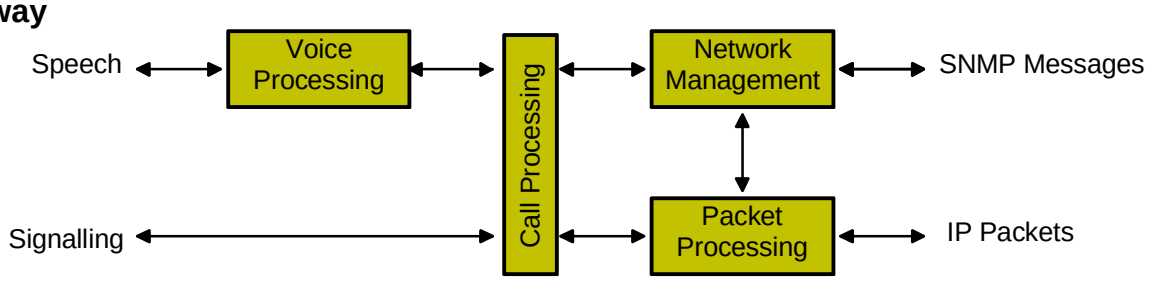

Bild 21: Voice Gateway/Terminal Functions

Ein Gateway stellt eine Schnittstelle zu anderen Netzwerken dar. Die Signalisierungs- und Nutzdaten werden durch das Gateway bidirektional übersetzt.
Prinzipiell arbeitet ein Gateway auf jeder Netzwerkseite der Schnittstelle wie ein normales Endgerät, das intern Daten zwischen den Netzwerksystemen austauscht und sie dabei konvertiert, um eine Medien-Kommunikation über Netzwerkgrenzen hinweg zu ermöglichen.
Typischer Anwendungsfall für ein Gateway ist die Kopplung zwischen einem paketbasierten Ethernet-Netzwerk mit H.323 und einem verbindungsorientierten digitalen ISDN-Telefonnetz über ein H.323-ISDN-Gateway. Bei Verwendung des H.320-Standards im ISDN-Netzwerk wird entsprechend ein H.323-H.320-Gateway eingesetzt. Es bietet die Einsatzmöglichkeit

von Bildtelefonie oder Datenkommunikation, während mit einem H.323-ISDN-Gateway lediglich Telefongespräche übertragen werden können.

Gatekeeper
Ein Gatekeeper ist eine optionale Einheit, die Signalisierungsfunktionen anbietet, um Endgeräte von Vermittlungsfunktionen zu entlasten. Ein Gatekeeper kann aus mehreren physikalischen Einheiten bestehen. Einfache Endgeräteverbindungen in einem Netzwerk können ohne Gatekeeper hergestellt werden, Gegenstellen müssen dabei vom Initiator eines Verbindungsaufbaus direkt adressiert werden. Die Verbindungsinformationen müssen deshalb zumindest dem Initiator einer Verbindung vor Beginn des Rufaufbaus bekannt sein.
Ein Gatekeeper ist eine separate logische Einheit, die sich physikalisch auch innerhalb eines Terminals oder Gateways befinden kann. Innerhalb einer Zone kann lediglich ein logischer Gatekeeper aktiv sein.
Die wichtigsten Aufgaben eines Gatekeepers umfassen:

- Adressübersetzung zwischen Alias-Adressen und Transportadressen
- Zugriffssteuerung mit Hilfe von Autorisierungsmechanismen, Bandbreiten-oder anderen Kriterien
- Bandbreitenkontrolle basierend auf einem Bandbreitenmanagement
- Zonen-Management der registrierten Endgeräte
- Rufsteuerung (bei Gatekeeper Routed Signalling)

Gatekeeper-Registrierung: Bei Verwendung eines Gatekeepers für die Verbindungssteuerung wird nach Ermittlung des zuständigen Gatekeepers eine Registrierung des Endgerätes durchgeführt.
Mit Hilfe einer Gatekeeper-Request-Nachricht (GRQ) kann ein Endgeräte-Terminal, z.B. mit Hilfe eines Multicast-Protokolls, versuchen einen oder mehrere zuständige Gatekeeper im Netzwerk zu ermitteln. Gatekeeper können den Request mit einer Gatekeeper Confirmation (GCF) bestätigen oder mit einem Gatekeeper Reject (GRJ) ablehnen.
Ein Gatekeeper kann in einer GCF- oder GRJ-Nachricht mehrere Gatekeeper angeben, mit denen ein Terminal alternativ kommunizieren kann, falls dieser Gatekeeper zu einem späteren Zeitpunkt selbst nicht erreichbar ist. Diese weiteren Gatekeeper werden als alternate Gatekeeper bezeichnet.

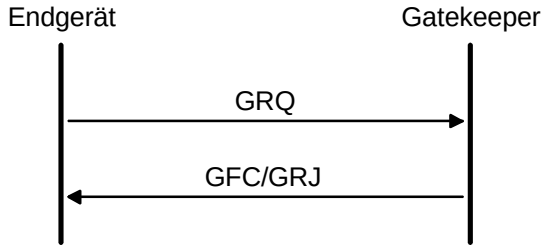

Bild 22: Gatekeeper-Ermittlung durch Gatekeeper-Requests (GRQ)

Die Registrierung wird mit Hilfe von „Registration, Admission and Status" (RAS)-Nachrichten über H.225.0 durchgeführt. Dabei wird die RAS-Signalisierung über einen eigenen Datenkanal unabhängig vorn H225.0 Call Signalling Channel und dem H245 Control Channel abgewickelt. Die Registrierung eines Endgeräts ist für die Erreichbarkeit eines Teilnehmers unter einer bestimmten Rufnummer bzw. Adresse notwendig und geschieht zeitlich vor dem ersten Ruf bzw. der ersten Rufannahme.

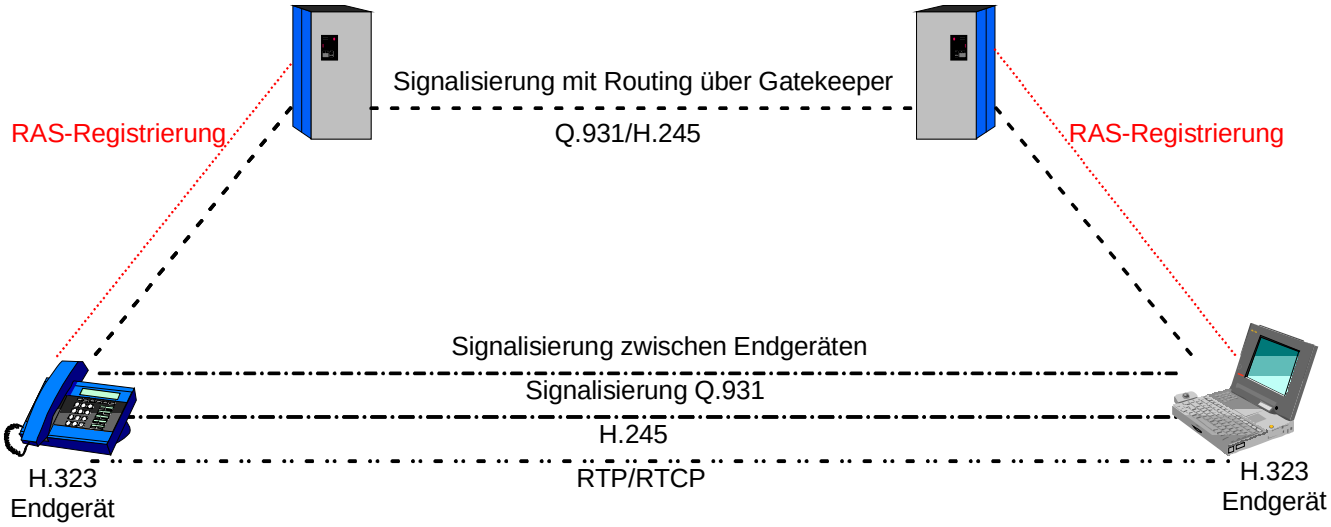

Bild 23: Signalisierungspfade mit und ohne Gatekeeper

Zu Beginn des Verbindungsaufbaus wird ein Rufsignalisierungskanal (Call Signalling Channel) geöffnet, der direkt zwischen zwei Endgeräten aufgebaut wird, falls kein Gatekeeper vorhanden ist. Ist ein Gatekeeper involviert, entscheidet dieser selbst, ob der Steuerkanal direkt zwischen den Endgeräten mit der Methode des Direct Routed Signalling, oder zwischen jeweiligem Endgerät und Gatekeeper mit der Methode des Gatekeeper Routed Signalling aufgebaut wird.

Multipoint Control Unit (MCU)

Eine Multipoint Control Unit enthält einen Multipoint Controller und entweder keinen oder eine beliebige Anzahl von Multipoint-Prozessoren. Sie kann mit Terminals Verbindung aufnehmen. Eine typische MCU für zentralisierte Mehrpunktkonferenzen besteht aus einem MC und einem Audio-, Video- und einem Daten-MP. Für dezentrale Mehrpunktkonferenzen sind typische Bestandteile der MCU ein MC und ein Daten-MP, der T.120 unterstützt, weil in diesem Fall keine Audio- oder Videodaten von der MCU verarbeitet werden.

- Ein **Multipoint Controller (MC)** steuert die Auswahl von Verbindungsparametern in einem H.323-System bei Verwendung von Mehrpunktkonferenzen. Der MC ermittelt dabei einen Kommunikations-Modus, genannt Selected Communications Mode (SCM), der für alle Endgeräte gleich ist oder für einzelne Endgeräte individuell bestimmt werden kann.
  Zwei Betriebsarten sind möglich: Bei der dezentralen Konferenz-Betriebsart senden die Endgeräte selbst die Nutzdaten an mehrere Empfänger. Bei der zentralisierten Variante nimmt der Multipoint Processor (MP) die eingehenden Datenströme entgegen und verteilt sie an die Empfänger.
- Ein **Multipoint Processor (MP)** wird in zentralisierten oder in hybriden Mehrpunktkonferenzen verwendet, um eingehende Audio- oder Videodatenströme entweder per Switching nach selbst zu bestimmenden Verfahren am Eingang umzuschalten und an die Empfänger zu verteilen oder per Mixing einen resultierenden Datenstrom durch Mischen der Daten zu erzeugen und zu verteilen.
  MC- und MP-Einheiten können in verschiedenen Varianten mit Terminals, Gatekeepern, Gateways oder MCUs kombiniert werden. Mögliche Anordnungen zeigt das folgende Bild

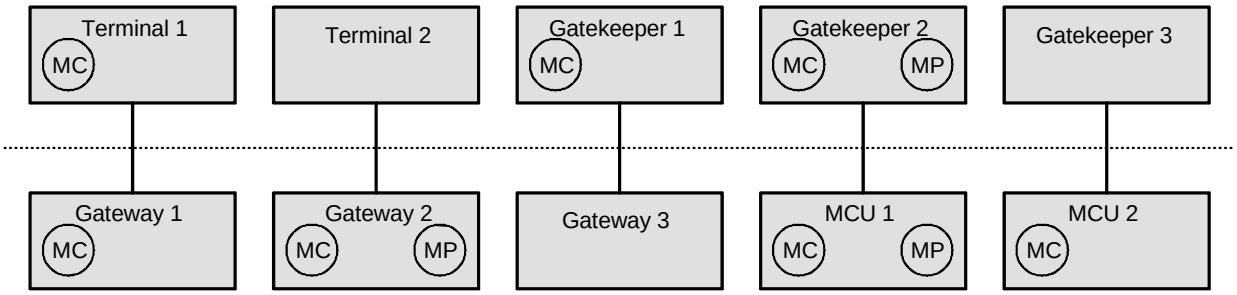

Bild 24: Mögliche Anordnungen von MC und MP

H.225.0

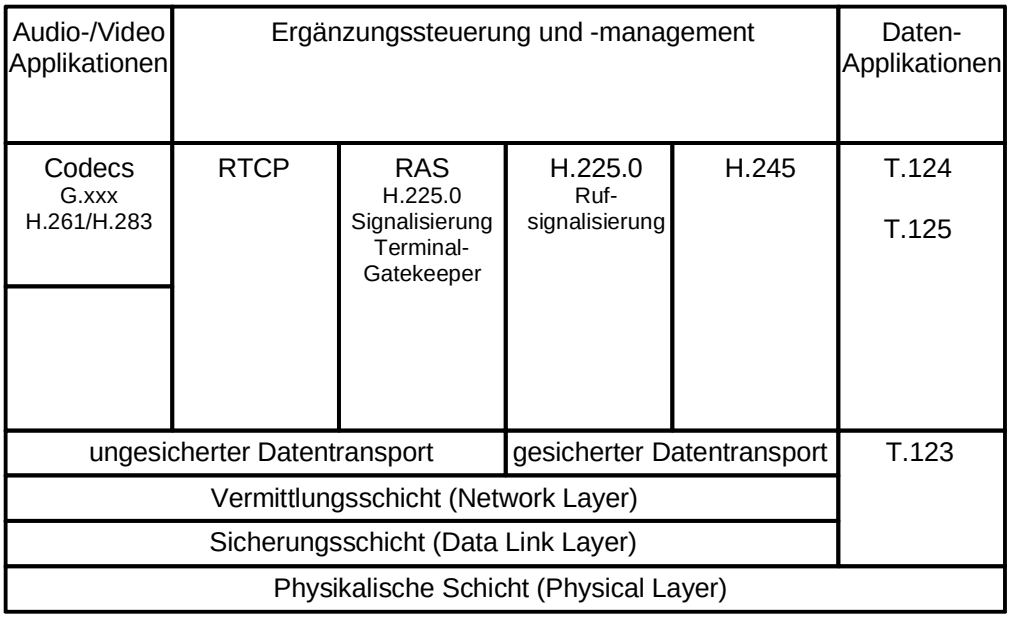

Bild 25: H.225.0-Definitionsbereich

Der H.225.0-Standard „Call signalling protocols and media stream packetization for packet-based multimedia communication systems" der ITU-T [11] spezifiziert die Verwendung von Audio, Video, Daten und Steuerungsdaten. Ferner werden Kodierung und Transport dieser Nutzdaten zwischen H.323-Gegenstellen untereinander inklusive der Verwendung von Gateways als Schnittstellen zu anderen Telefoniesystemen über den H. 225.0-Layer beschrieben. Für den Echtzeitdatentransport von Multimediadaten wird das Realtime Transport Protocol (RTP) der IETF eingesetzt, für ungesicherte Audio- oder Videokanäle z.B. UDP oder IPX. Die Kanäle können unidirektional oder bidirektional sein und entweder in Unicast- oder Multirast-Verbindungen (Punkt-zu-Punkt bzw. Punkt-zu-Mehrpunkt) eingesetzt werden.

Control Protocol for Multimedia Communication - H.245

Der H.245-Standard „Control Protocol for Multimedia Communication" der ITU-T beschreibt Nachrichten und Verfahrensweisen für die Abstimmung von Terminals während des Verbindungsaufbaus oder während der Verbindung. Die Rollenverteilung bei Entscheidungen wird über eine Master-/Slave-Festlegung durchgeführt.
Die Nachrichten enthalten Signalisierungsdaten, Informationen über die Fähigkeiten zum Senden und Empfangen von Multimediadaten, sowie Kontroll- und Informationsdaten. Bestätigte Signalisierungsverfahren ermöglichen den gesicherten Ablauf von Entscheidungen über die Audio-, Video- und Datenkommunikation.
Folgende Verfahren sind in H.245 festgelegt:

- Master-/Slave-Erkennung
- Austausch der Fähigkeiten beteiligter Endgeräte

- Unidirektionale Signalisierung logischer Kanäle
- Bidirektionale Signalisierung logischer Kanäle
- Signalisierung der Close-Anforderung zum Beenden logischer Kanäle
- H.223 Multiplex-Tabelleneintragsänderung
- Anforderung von Multiplex-Tabelleneinträgen
- Empfänger-zu-Sender-Übertragungsmodusanforderung
- Round Trip Delay-Erkennung
- Überwachungsschleife

Die Signalisierungsmeldungen werden über einen H.245-Steuerkanal, der als H.245 Control Channel bezeichnet wird, ausgetauscht. Steuerkanäle werden entweder als Kommunikationsmedium zwischen den Endgeräten verwendet oder können, bei vorhandenem Gatekeeper, zwischen Endgerät und zugeordnetem Gatekeeper in einer Gatekeeper Zone eingesetzt werden. Im letzteren Fall tauschen dann die beteiligten Gatekeeper als Stellvertreter für die Endgeräte Signalisierungsinformationen aus, wie es in Bild 23 auf Seite 29 dargestellt ist. Bei Mehrpunktkonferenzen werden die Signalisierungsdaten zwischen einem Endgerät und dem Multipoint Controller (MC) ausgetauscht.
Der Austausch der Fähigkeiten beteiligter Endgeräte erfolgt entweder symmetrisch oder asymmetrisch. Bei der symmetrischen Variante fordert eine Gegenstelle, dass gleiche Fähigkeiten für beide Übertragungsrichtungen zu vereinbaren sind. Beispielsweise kann die Forderung lauten, die Audiokodierung G.711 in beiden Übertragungsrichtungen zu verwenden. Bei asymmetrischer Übertragung können für jede Richtung individuell Fähigkeiten vereinbart werden, so dass beispielsweise von A nach B G.711 und von B nach A G.729 als Kodierung verwendet werden kann.
H.245 enthält als wichtigste Protokollelemente die Kommandos openLogicalChannel und closeLogicalChannel, um einen Nutzkanal auf- bzw. abzubauen. Hierbei werden alle Informationen über Medientyp, verwendete Kodierung und über weitere Übertragungsparameter ausgetauscht. Dieses Verfahren ist notwendig, damit Empfänger von Nutzdaten diese korrekt interpretieren und weiterverarbeiten können. Logische Kanäle sind in den meisten Fällen unidirektional. T.120-Datenkanäle können jedoch auch bidirektional sein.

H.323-Netzwerkstrukturen
Im Anhang G des H.225.0-Standards (Annex G) sind verschiedene Netzwerkstrukturen definiert, die so genannte administrative Domains miteinander verbinden. Administrative Domänen sind Netzwerkbereiche, die einer gemeinsamen Administration unterliegen. Border Elements sind logische Einheiten, die mit anderen gleichartigen Elementen in externen administrativen Domänen kommunizieren. Sie haben die Aufgabe, die eigene Domäne für verschiedene Dienste zu repräsentieren.
Folgende Strukturen sind möglich:

- Hierarchische Struktur: Bei einer hierarchischen Struktur befragt ein Border Element eine entsprechende Instanz einer höheren Hierarchie-Ebene, um eine Endgeräte-Adresse aufzulösen zu können.

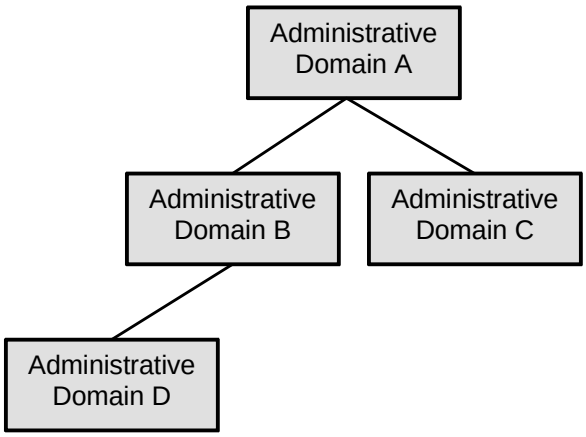

Bild 26: Hierarchische Domainstruktur

- Verteilte bzw. voll vermaschte Struktur: Bei dieser Struktur kommunizieren Border-Elemente mit gleichartigen Instanzen beliebiger anderer Domänen.

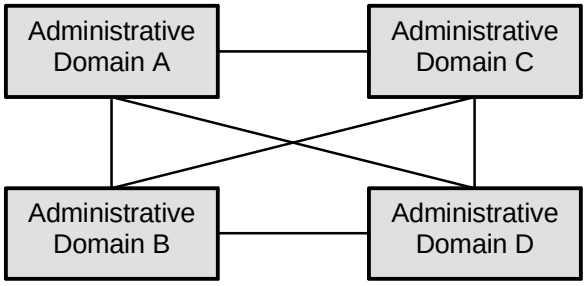

Bild 27: Verteilte bzw. voll vermaschte Domainstruktur

- Clearing House: Das Clearing House ist eine übergeordnete Instanz, die von allen Border Elementen der administrativen Domänen genutzt wird, um Adressen aufzulösen.

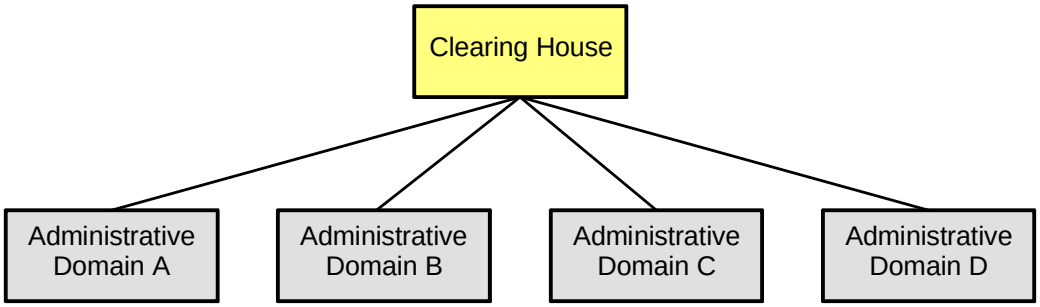

Bild 28: Clearing House-Domainstruktur

4.1.2 Session Initiation Protocol - SIP

Das Session Initiation Protocol RFC 3261 - SIP der IETF ist ein Signalisierungsprotokoll, das zusammen mit beliebigen anderen Protokollen, Medien-Kodierungen und Anwendungen verwendet werden kann. Es wird verwendet, um Sitzungen zwischen Verbindungspartnern aufzubauen und zu unterhalten. Innerhalb einer Sitzung können beliebige Medien zwischen den Beteiligten ausgetauscht werden. Dieser Medientransport geschieht außerhalb des Definitionsbereiches von SIP.
Es gibt zahlreiche weitere Protokolle und Empfehlungen der IETF, die den Anwendungsbereich von SIP erweitern bzw. SIP in ein Umfeld mit speziellen Features wie Audio, Video oder neuerdings auch Instant-Messaging einbetten.

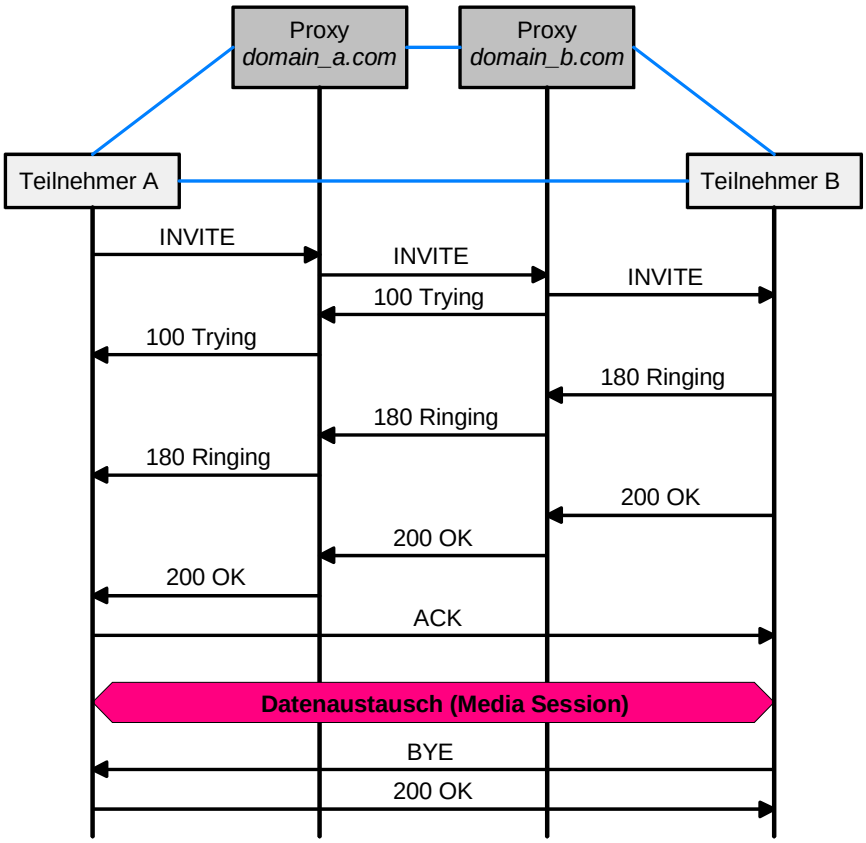

Bild 29: SIP-Verbindungsaufbau mit HTML-basierten Textnachrichten

Das SIP-Protokoll ist textbasiert und ähnlich wie die Webseiten-Beschreibungssprache HTML aufgebaut. Dies erleichtert sowohl die Entwicklung von Protokollsoftware, die sich an Internet-Browser-Technologie orientieren kann, als auch den Test von SIP-Implementierungen aufgrund der leichten Lesbarkeit von Aufzeichnungen der Protokollabläufe. SIP ist, genauso wie H.323, nicht auf ein spezielles unterliegendes Transportprotokoll festgelegt. Es kann u.a. sowohl UDP als auch TCP nutzen.
SIP enthält Protokollelemente, mit deren Hilfe Multimedia-Sitzungen auf- und abgebaut werden können. Die Festlegung von Medienarten kann zusammen mit dem SDP-Protokoll durchgeführt werden. Während einer Verbindung können weitere Teilnehmer zu einer laufenden (Konferenz-)sitzung eingeladen bzw. aus einer Sitzung entfernt werden. Weitere Funktionen umfassen die Benutzer-Lokalisation und deren aktuelle Verfügbarkeit im Netzwerk, sowie die Rufweiterleitung.
SIP bietet keine eigenen Dienste an, sondern enthält lediglich Hilfsmittel zur Realisierung von Diensten. Beispielsweise integriert es keine Konferenzsteuerung für Multimedia-Konferenzen. Es ist dennoch möglich, Konferenzen mit einer separaten Konferenzsteuerung mit SIP als Signalisierungsprotokoll zu implementieren.
SIP unterstützt die Mobilität der Nutzer durch mehrere Eigenschaften wie manuelle und automatische Rufweiterleitungen, Benutzer-IDs, mit denen ein Benutzer auf mehreren Terminals gleichzeitig eingeloggt sein darf, und so genanntes forking, einer gleichzeitigen Weiterleitung eines Anrufes an mehrere Endgeräte, um einen möglichst schnellen Verbindungsaufbau mit dem Gesprächspartner zu ermöglichen.
Das SIP-Protokoll besteht aus Nachrichten und Antworten. Die grundlegenden SIP-Nachrichten sind:

- REGISTER - für die Registrierung eigener Benutzerinformationen
- INVITE - zur Einladung von Verbindungspartnern zu einer Sitzung
- ACK - als Bestätigungsnachricht
- CANCEL - für Verbindungsabbruch

- BYE - zum Beenden einer Sitzung
- OPTIONS - für die Suche nach Fähigkeiten von erreichbaren Servern

Antworten werden mit Statuscodes wie folgt versehen:

- 1xx (Provisional) - Befehl empfangen, wird weiterverarbeitet
- 2xx (Success) - Befehl wurde empfangen, verstanden und akzeptiert
- 3xx (Redirection) - weitere Aktionen sind notwendig, um einen Befehl zu beenden
- 4xx (Client Error) - Befehl enthält Syntaxfehler oder kann vom Server nicht verarbeitet werden
- 5xx (Server Error) - Server kann einen korrekten Befehl nicht verarbeiten
- 6xx (Global Error) - Befehl kann von keinem Server ausgeführt werden

Folgende Systemkomponenten sind im SIP-Protokoll definiert:

- User Agent Client (UAC), User Agent Server (GAS)
- Proxy-Server
- Redirect-Server
- Registrar

User Agent Client (UAC), User Agent Server (UAS)
User Agents sind vergleichbar mit den H.323-Terminals. Sie stellen die Endgeräte in SIP-basierten Systemen dar.
Ein User Agent Client sendet eine Anforderung an einen User Agent Server. Die Rolle des Clients ist lediglich für die Transaktion selbst festgelegt, d.h. ein UAC kann in einem anderen Zusammenhang als User Agent Server (UAS) arbeiten. Ein User Agent Server nimmt Anforderungen eines Clients entgegen, beantwortet diese und akzeptiert die Anforderung, lehnt sie ab oder leitet sie an eine andere User Agent Server-Instanz weiter.

Proxy-Server
Ein SIP-Proxy-Server hat die primäre Aufgabe, SIP-Protokollelemente mittels Routing weiterzuleiten. Ein Proxy-Server ist in dieser Vermittlerrolle Client und Server zugleich und bewirkt die Weiterleitung von Anforderungen in Richtung des UAS bzw. Rückleitung der Antworten zum UAC. Während einer Weiterleitung können SIP-Nachrichten mehrere SIP-Proxies passieren. Innerhalb eines Proxies werden die Nachrichten gelesen, interpretiert und, beispielsweise zwecks Einfügung von Routing-Informationen, angepasst.
Proxies sind zudem für das Rechtemanagement zuständig und ermitteln beispielsweise, ob Benutzer die Berechtigung besitzen, einen Ruf durchzuführen.
Es gibt sowohl stateful Proxies, die den aktuellen Zustand einer Verbindung zwischen UAC und UAS speichern, als auch stateless Proxies. Sie sind „vergessliche" Instanzen, die lediglich Nachrichten weiterleiten. Stateful-Proxies unterscheiden sich zusätzlich durch die Eigenschaften call-stateful oder transaction-stateful. Call-statefull Proxies speichern den jeweils aktuellen Zustand für die Dauer der Verbindung und sind stets transaction-stateful. Die Umkehrung gilt jedoch nicht in jedem Fall. Transaction-stateful Proxies speichern den aktuellen Zustand lediglich für die Dauer einer einzelnen Transaktion zwischen Nachricht und Antwort.
Rufsignalisierung:
① ein UAC sendet eine INVITE-Nachricht an einen Proxy-Server
② der Proxy-Server wendet sich an einen Location-Server um die Zieladresse aufzulösen
③ der Proxy-Server erhält die Zieladresse als Rückantwort
④ die INVITE-Nachricht wird anschließend mit der aufgelösten Zieladresse an den UAS weitergeleitet
⑤ der UAS ermittelt, ob die Rufannahme möglich ist
⑥zur Bestätigung sendet der UAS eine 200 OK-Nachricht zurück an den Proxy-Server

⑦ der Proxy-Server leitet diese Bestätigung an den UAC weiter
⑧ der UAC bestätigt die Nachricht mit einer ACK-Nachricht zum Proxy-Server
⑨ der Proxy-Server leitet diese ACK-Nachricht zum UAS weiter
⑩ anschließend wird der Nutzdatenaustausch direkt zwischen den Endgeräten durchgeführt

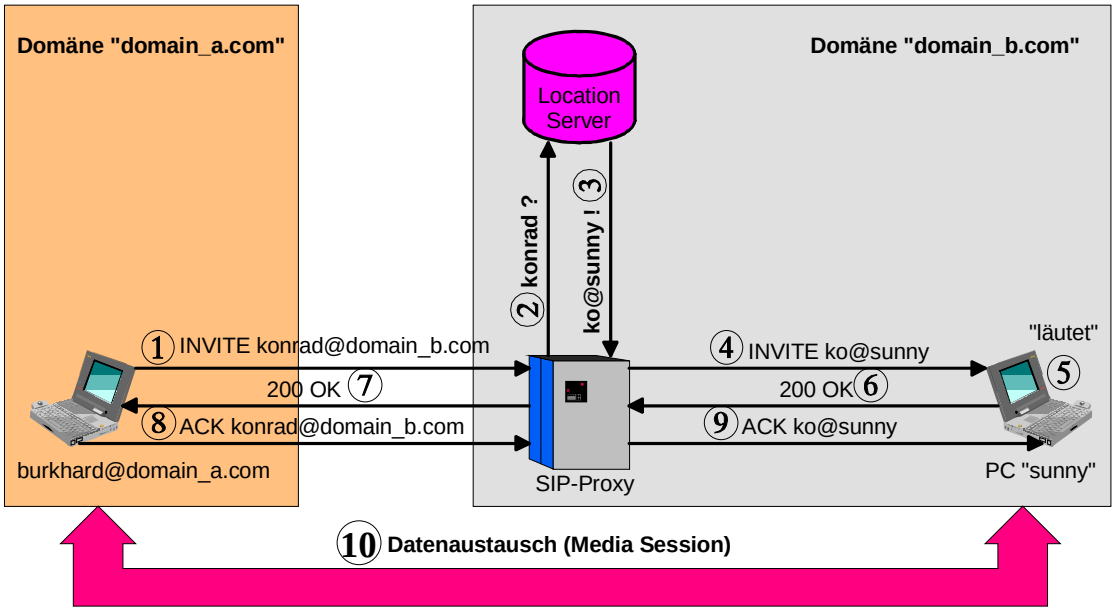

Bild 30: SIP-Verbindungsaufbau-Beispiel mit Proxy-Server

Redirect-Server

Ein Redirect-Server ist selbst ein UAS, der eine Nachricht mit einer Weiterleitungsinformation an den UAC beantwortet, damit der UAC die Nachricht an eine alternative Adresse sendet. Redirect-Server sind jedoch nicht mit Endgeräten zu verwechseln, da sie nicht die Rolle eines UAC einnehmen und selbsttätig Nachrichten senden.

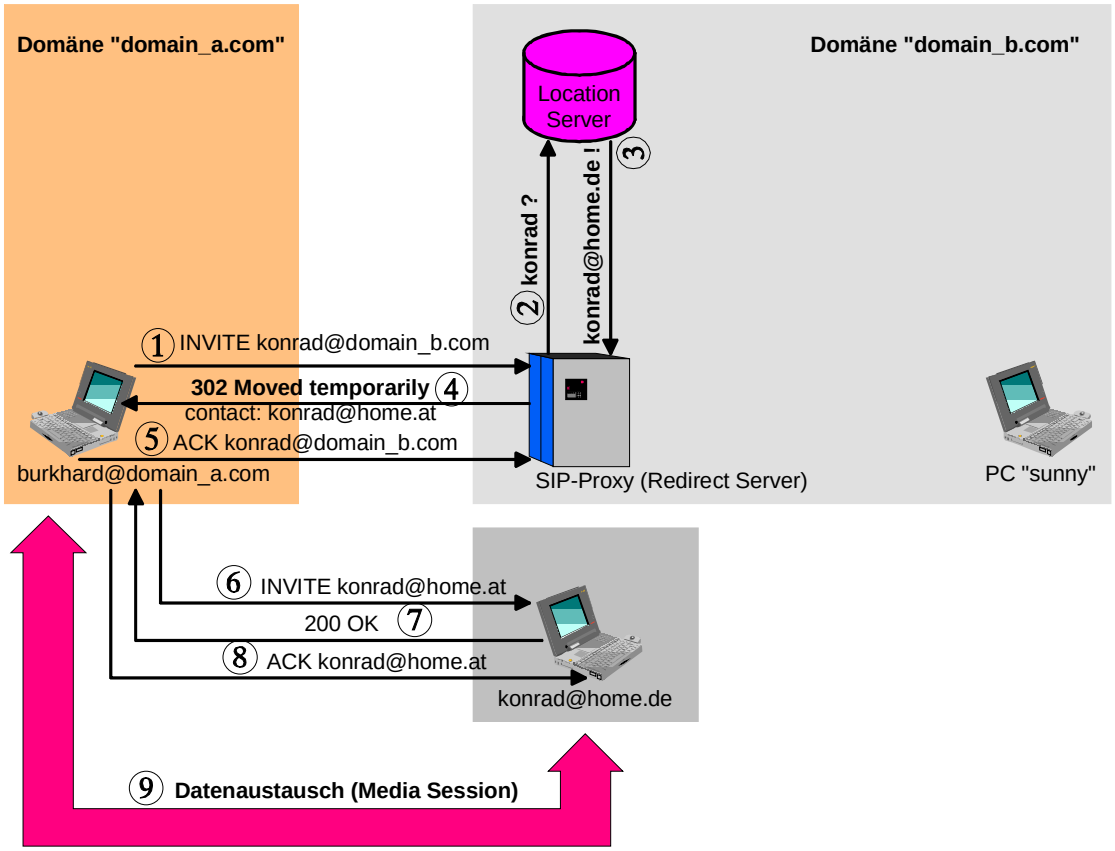

Bild 31: SIP-Verbindungsaufbau-Beispiel mit Redirect-Server

Rufsignalisierung:
① bei der Rufsignalisierung mit einem Redirect-Server sendet ein UAC eine INVITE-Nachricht an einen Redirect-Server
② der Redirect-Server wendet sich an einen Location-Server - um die Zieladresse aufzulösen
③ der Location-Server sendet die aufgelöste Zieladresse als Rückantwort an den Redirect-Server
④ anschließend sendet der Redirect-Server dem UAC die Rückantwort 302 Moved Temporarily
⑤ der UAC sendet eine ACK-Nachricht zurück an den Redirect-Server
⑥ anschließend sendet der UAC dem UAS die INVITE-Nachricht, deren Zieladresse die Adresse des UAS enthält.
⑦ der UAS bestätigt die INVITE-Nachricht mit einer OK-Rückantwort
⑧die vom UAC mit der ACK-Nachricht angenommen wird
⑨ anschließend efolgt der Nutzdatenaustausch direkt zwischen den Endgeräten

Registrar
Ein Registrar nimmt REGISTER-Nachrichten entgegen und leitet diese an einen Location Service-Dienst weiter, der die Lokalisierung von Teilnehmern ermöglicht.

4.1.3 Session Announcement Protocol - SAP

Das Session Announcement Protocol RFC 2974 der IETF unterstützt die Veröffentlichung von Multimedia-Sitzungen (z.B. Konferenzen), um Informationen über deren Inhalt mitzuteilen.
In diesem Zusammenhang wird ein Sitzungsverzeichnis verwendet, das häufig im Netzwerk verteilt vorliegt. Eine Instanz dieses Sitzungs-Verzeichnisses veröffentlicht über einen Multicast-Versand periodisch Datenpakete, die eine Beschreibung der Sitzungen beinhalten. Die Beschreibung muss alle Informationen enthalten, die notwendig sind, um eine Teilnahme an einer Sitzung zu ermöglichen. Das Protokoll legt fest, wie Veröffentlichungen mit Hilfe von Multicast durchgeführt werden. Sitzungen werden mit Hilfe des SDP-Protokolls beschrieben.

4.1.4 Session Description Protocol - SDP

Das Session Description Protokoll RFC 2327 der IETF beschreibt Inhalte von Multimedia-Sitzungen (z.B. Konferenzen). Diese Beschreibungen können für die Veröffentlichung, zur Einladung in eine Sitzung oder für andere Zwecke verwendet werden.
Obwohl SDP, wie im RFC-Dokument selbst beschrieben, ursprünglich nicht für den Austausch und die Aushandlung von Fähigkeiten beim Verbindungsaufbau gedacht ist, existiert ein weiteres Dokument „An Offer/Answer Model Session Description Protocol" (RFC 3264) das ein entsprechendes Verfahren erläutert.
Das SIP-Protokoll kann SDP-Nachrichten versenden, die Beschreibungen der Medien einer Session, wie z.B. Kodierungen und Übertragungsparameter, beinhalten. Auf der Basis dieser Informationen können SIP-Endgeräte bei Verbindungsaufbau einen Fähigkeitenaustausch durchführen, um eine Einigung auf gemeinsam unterstützte Medien zu erzielen.
Das Protokoll ist aus der Notwendigkeit entstanden, im Internet Multicast Backbone (MBone) Konferenzen bekannt machen zu wollen. Hierfür werden SDP-Nachrichten an eine Multicastadresse mit Hilfe des Session Announcement Protocols (SAP) gesendet. Nachrichten können außerdem per E-Mail oder HTTP versendet werden.
SDP- Nachrichten beinhalten:

- Sitzungsname und -inhalt
- Zeitangaben, wann die Sitzung geöffnet wird

- Medienarten, die in der Sitzung verwendet werden
- Informationen, wie die Sitzung empfangen werden kann (z.B. Kombination aus IP-Adresse und Portnummern)

4.2 PSTN Signalisierungsprotokolle und Standards

Im Bereich öffentlicher Telefonnetze hat sich ISDN (Integrated Services Digital Network) als digitales Netz konkurrenzlos im zentraleuropäischen Raum etabliert.

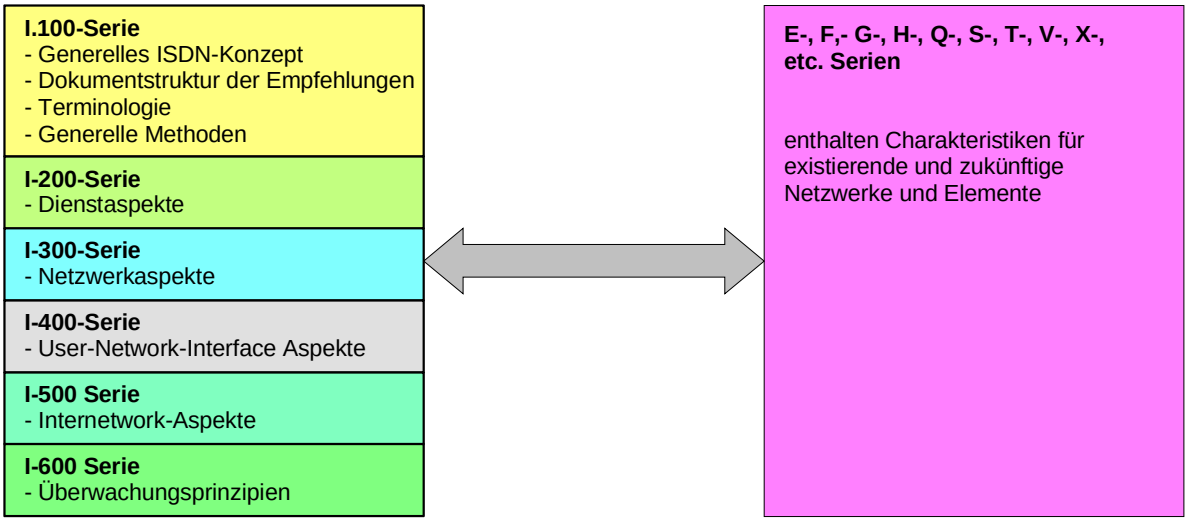

Bild 32: Übersicht der ITU-T ISDN-Empfehlungen

Die Standards für ISDN wurden ursprünglich von der ITU-T spezifiziert und in wesentlichen Teilen vom European Telecommunications Standards Institute (ETSI) übernommen. Zunächst wurde in Deutschland eine nationale ISDN-Variante mit der Bezeichnung 1TR6 eingesetzt, die jedoch nach Einigung auf den europäischen Standard durch die Variante E-DSS1 ersetzt wurde.

- Die **physikalische Schicht** (OSI-Layer 1 – Physical Layer) wurde durch die ITU-T Empfehlung
  - I.430 für den ISDN-Basisanschluss und
  - I.431 für den ISDN-Primärratenanschluss festgelegt.
- Die **zweite Schicht** (OSI-Layer 2 – Data Link Layer) wurde durch die ITU-T-Empfehlungen I.440 und I.441 festgelegt die später unter den Bezeichnungen Q.920 bzw. Q.921 veröffentlicht wurden.
  - Q.920 behandelt generelle Aspekte des Data Link Layers, während
  - Q.921 die eigentlichen Festlegungen enthält.
- Die **dritte Schicht** (OSI-Layer 3 – Network Layer) ist die höchste für ISDN festgelegte Kommunikationsschicht unterhalb der Anwendungsebene und wurde ursprünglich durch die ITU-T Empfehlungen I.450 und I.451 festgelegt die später unter den Bezeichnungen Q.930 und Q.931 veröffentlicht wurden.
  - Q.930 enthält eine Übersicht über die Layer 3-Spezifikationen mit Referenzen auf weiterführende Standards und eine kurze Interface-Übersicht für die Rufsteuerung
  - Q.931 legt das Verhalten und die Funktionsweise der Netzwerkschicht fest. Die Empfehlung enthält u.a. mögliche Layer 3-Zustände und definiert Nachrichten, wie z.B.: ALERTING; CONNECT; SETUP, etc., die eine Netzwerkschicht mit Hilfe von Q.921 austauschen kann:

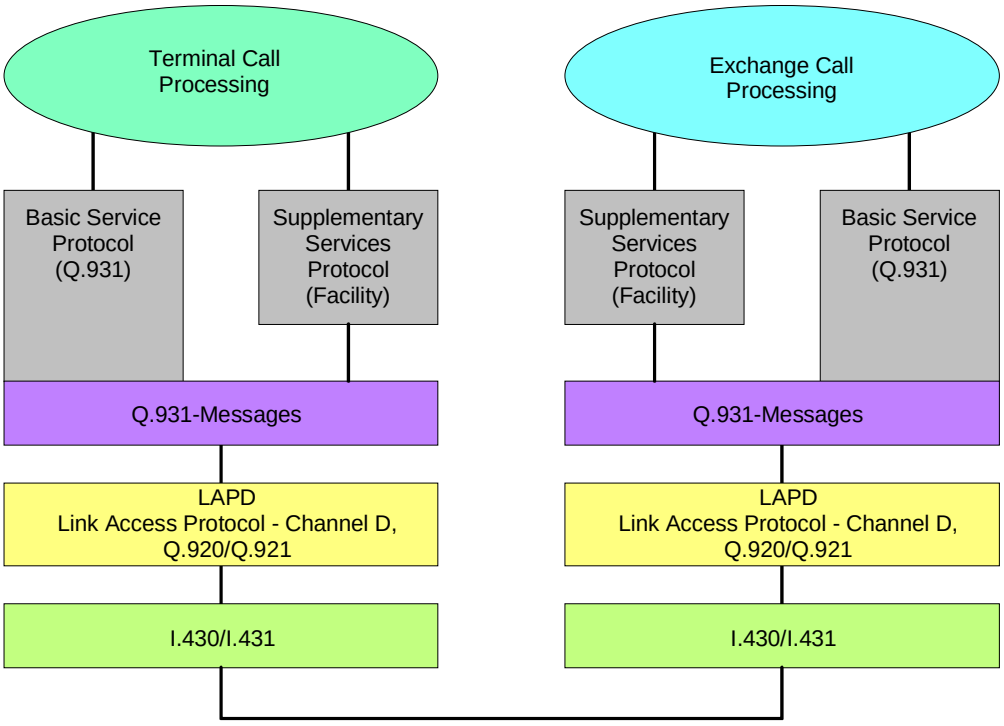

Bild 33: Q.930-Modell für Basis- und erweiterte Dienste (Basic-/Supplementary Services)

4.2.1 D-Kanal-Protokoll - QSIG/PSS1

QSIG ist vom Standard Q.931 der ITU-T abgeleitet und wird offiziell als „D-Kanal-Protokoll am Q-Referenzpunkt" bezeichnet. Die QSIG-Spezifikationen werden vom IPNS-Forum (ISDN PBX Network Specification Forum) gemeinsam mit der ECMA entwickelt. Anschließend werden sie direkt an die ISO/IEC bzw. deren JTC 1 (Joint Technical Commitee) weitergeleitet und als globale Standards definiert. Diese Standards dienen dann wiederum als Vorlage für die ETSI, die QSIG unter der Bezeichnung PSS1 standardisiert hat.

4.2.2 Signalling System No. 7 - SS7

Das „Signalling System No. 7", durch die CCITT (später ITU-T) standardisiert, wird durch eine ganze Familie von Empfehlungen beschrieben. Ausgangspunkt ist die Empfehlung Q.700 der ITU-T, die eine Einführung in die Architektur und die generellen Konzepte von SS7 enthält.
Auch in der IETF werden Empfehlungen zu SS7 von der Arbeitsgruppe Signaling Transport veröffentlicht. Sie betreffen Schnittstellen zwischen SS7-Netzwerken und IP-basierten Protokollen. Die unterschiedliche Schreibweise Signalling (ITU-T) bzw. Signaling (IETF) entspricht jeweils dem Originaltext.
Die wesentlichen SS7-Spezifikationen sind in folgenden Empfehlungen enthalten:

Funktionale Einheiten von SS7	**Empfehlungen**
Message Transfer Part (MTP)	Q.701-Q.704, Q.706, Q.707
Telephone User Part (TUP)	Q.721-Q.725
Supplementary services	Q.73x Serie
Data User Part (DUP)	Q.741
ISDN User Part (ISUP)	Q.761-Q.764, Q.766
Signalling Connection Control Part (SCCP)	Q.711-Q.714, Q.716
Transaction Capabilities (TC)	Q.771-Q.775
Operations Maintenance and Administration Part (OMAP)	Q.750-Q.755

Tabelle 2: Empfehlungen zentraler SS7-Funktionselemente

Die SS7-Architektur orientiert sich am OSI-Schichtenmodell und implementiert die Schichten eins bis drei und sieben. Die Schichten vier bis sechs sind nicht besetzt.

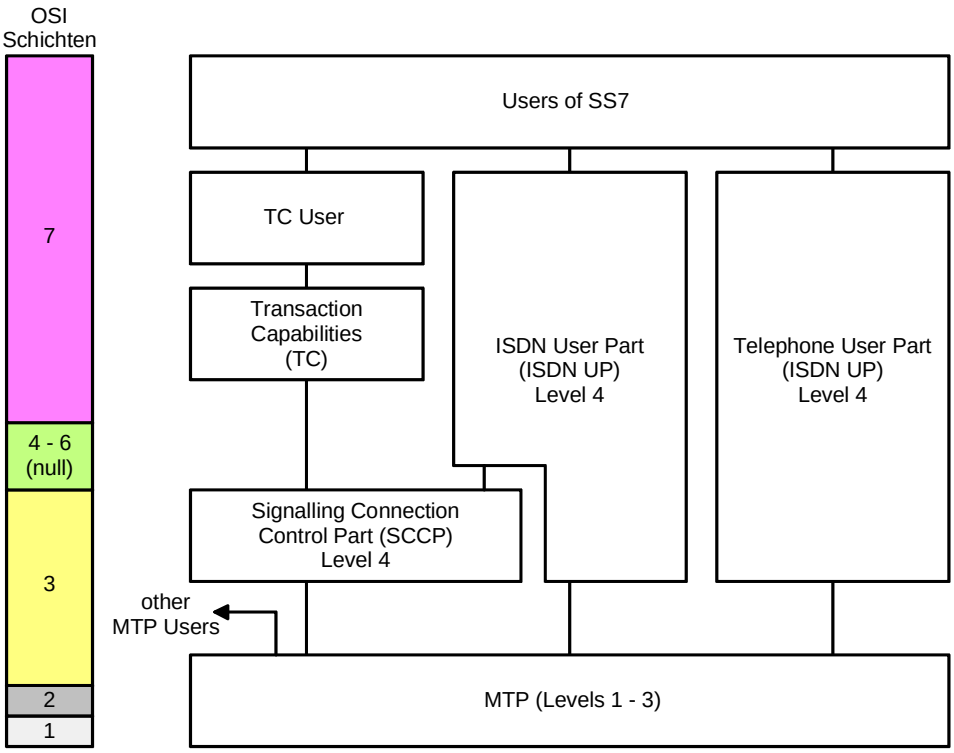

Bild 34: SS7-Architektur

SS7 enthält folgende funktionale Elemente:

- **Message Transfer Part (MTP):** Der MTP stellt den grundlegenden Transport von Signalisierungsnachrichten sicher.
  - Level 1 „Signalling data link functions" legt die physikalischen, elektrischen und funktionalen Eigenschaftenfest
  - Level 2 „Signalling link functions" stellt die Funktionen für einen gesicherten Signalisierungsdatenaustausch über einen einzelnen Level-1-Data Link zur Verfügung
  - Level 3 „Signalling network functions" definiert die Transportfunktionen der Netzwerkschicht, die unabhängig von den zu übermittelnden Daten gemeinsam von allen Signalling Links genutzt werden können.
- **Signalling Connection Control Part (SCCP):** Erweitert die MTP-Funktionen zum verbindungsorientierten oder verbindungslosen Transport von Signalisierungsnachrichten und steuert logische Signalisierungsverbindungen in SS7-Netzwerken. Signalisierungsdaten können mit oder ohne Verwendung von logischen Signalisierungsverbindungen übermittelt werden. Der SCCP definiert Routingfunktionen basierend auf Dialed Digits, d.h. auf gewählten Rufnummern, um gezielt adressierte Subsysteme anzusprechen. Des Weiteren sind Managementfunktionen enthalten, die eine Verfügbarkeit von Subsystemen ermitteln.
- **Telephone User Part (TUP):** Legt die Anrufsignalisierungsfunktionen zur internationalen Nutzung mit SS7-Netzen fest.
- **ISDN User Part (ISUP):** Enthält die Signalisierungsfunktionen, welche für Wählverbindungen für Sprach- und Daten-Applikationen in ISDN-Netzen verwendet werden. Der ISUP enthält eine Schnittstelle zum SCCP, um eine Ende-zu-Ende-Signalisierung zu ermöglichen.

- **Transaction Capabilities (TC):** Definiert Verfahren, um verbindungslosen Informationsaustausch zwischen Endpunkten in einem Signalisierungsnetzwerk zu ermöglichen.
- **Operations, Maintenance and Administration Part (OMAP):** Verfahren und Protokolle für Verwaltung, Überwachung und Administration von SS7-Netzen, die sowohl die Initiierung, als auch die Ermittlung von benötigten Daten betreffen.

Die Elemente TUP und ISUP verwenden das in der ITU-T Empfehlung E.164 festgelegte Rufnummernformat. Für den SCCP können Formate der Empfehlungen E.164 (inklusive E.163), X.121, F.69, E.210, E.211, E.212, E.213 und E.214 verwendet werden.

Management
SS7 definiert zwei Arten von einsetzbaren Managementverfahren:
- Signalisierungs-Netzwerkmanagement und
- Signalisierungs-Systemmanagement.

Das Netzwerkmanagement wird durch Funktionen realisiert, die im MTP und SCCP enthalten sind, die automatisch durch intern implementierte Prozeduren die Performance des Netzwerkes messen können.
Das Systemmanagement wird durch externe Aktionen realisiert, die im Problemfall durchgeführt werden können.

4.3 IP-Transportprotokolle

Das Internet Protocol (IP) ist die Basis, auf der weitere Protokolle direkt oder indirekt aufsetzen. Die Reihenfolge der Vorstellung, beginnend bei IP, UDP, TCP usw., entspricht der Protokollschichtung beginnend bei der unterliegenden IP-Protokollschicht.

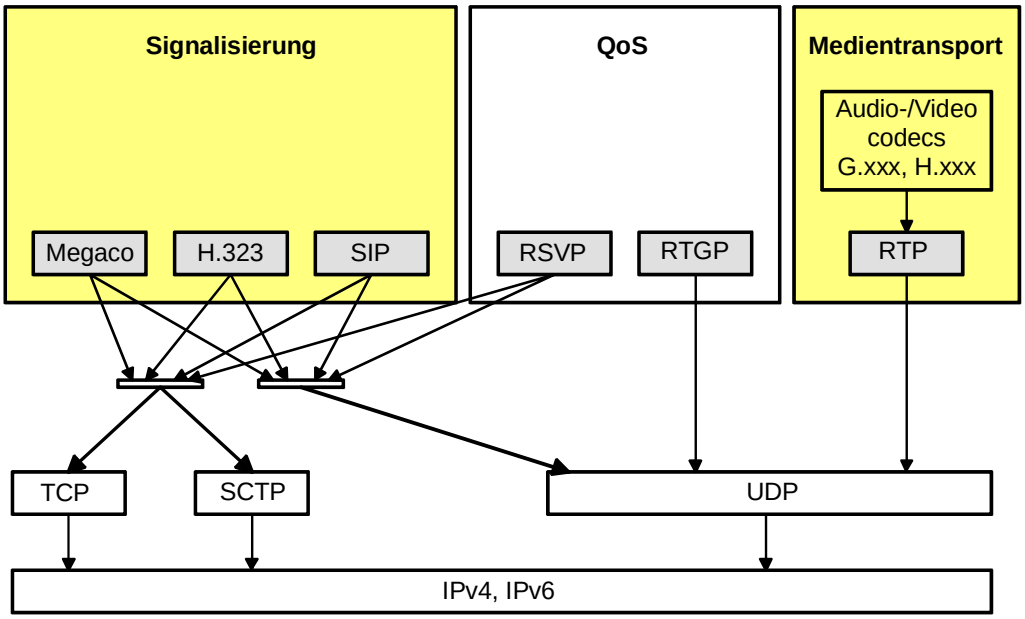

Bild 35: Protokollstack auf Basis des IP-Protokolls

Eine Übersicht über die für VoIP relevanten Protokolle im Kontext des Protokollstacks zeigt Bild 35. Es wird deutlich, dass die gängigen Signalisierungsprotokolle sowohl über gesicherte Transportprotokolle (TCP, SCTP) als auch über ungesicherte Transportprotokolle Daten austauschen können. Dasselbe gilt für RSVP. Der Medientransport für Audio- oder Videodaten erfolgt stets über RTP und UDP als ungesichertes Protokoll.

4.3.1 Internet Protocol - IP

Auf dem Internet-Protokoll (engl. Internet Protocol) der IETF, umgangssprachlich als IP-Protokoll bezeichnet, bauen nahezu alle anderen Protokolle auf. Das Protokoll ist Bestandteil der Netzwerkschicht und wird von höheren Protokollschichten verwendet. Applikationen verwenden IP nicht direkt, sondern meist in Zusammenhang mit höheren Protokollebenen wie z.B. UDP oder TCP. Die aktuelle Version 4 (IETF Standard RFC 791), auch als IPv4 bezeichnet, wird in Zukunft durch die erweiterte Version 6 (IETF Draft RFC 2460), als IPv6 bezeichnet, ersetzt.
Das Internet-Protokoll beschränkt sich auf wenige Eigenschaften und ist nicht verbindungsorientiert, d.h. so genannte IP-Telegramme werden versendet, ohne Kenntnis über den erfolgreichen Empfang zu erhalten. Deshalb gibt es keinerlei Sicherungsmechanismen bei Paketverlusten. Derartige Mechanismen werden bei Bedarf in höheren Protokollschichten implementiert.
Das Internet-Protokoll beinhaltet hauptsächlich die beiden Funktionen Adressierung und Fragmentierung: Die Adressierung beinhaltet in der Version 4 die Verwendung der 32 Bit langen Internetadressen, bestehend aus einer Netz-ID und einer Host-ID. Für die Adressvergabe werden fünf Klassen unterschieden. In den Klassen A bis C besitzen die Netz- und Host-ID unterschiedliche Längen. Die Klasse D ist für Multicast-Gruppenkennungen und Klasse E für zukünftige Verwendung reserviert. Aufgrund der Adressknappheit bei IPv4 wird zunehmend auf die starre Einteilung der Adressklassen zugunsten von Netzmasken mit variablen Längen verzichtet.
Die Fragmentierung ermöglicht den Transport von Datenpaketen, die aufgrund ihrer Länge nicht von den unterliegenden Schichten verarbeitet werden können.
Die maximale Größe wird als Maximum Transfer Unit (MTU) angegeben. IP kann in diesem Zusammenhang Pakete selbständig fragmentieren und auf Empfangsseite wieder zusammensetzen. Der Einsatz dieses Mechanismus kann mit Hilfe eines Flags (dont fragment) unterbunden werden. In IPv6 ist die Fragmentierung in eine optionale Headererweiterung ausgelagert worden. Die Version IPv6 wurde entwickelt, um den bisherigen Adressraum, der durch die 32 Bit langen Adressen nahezu ausgeschöpft ist, auf 128 Bit lange Adressen zu erweitern.
Zur Verbesserung der Sicherheit im Internet wurde in IPv6 der IP Authentification Header (AH) eingefügt. Er ist in einem eigenen RFC 2402 spezifiziert. Das IP Encapsulation Security Payload (ESP), im RFC 2406 festgelegt, schafft zusätzlich die Möglichkeit, ganze Datagramme zu verschlüsseln.
Das für VoIP relevante Type-of-Service (ToS)-Feld wurde in Version 6 durch das Traffic Class-Feld ersetzt. Beide Felder ermöglichen eine prioritätengesteuerte, bevorzugte Weiterleitung von Datentelegrammen. Durch diese Maßnahme kann eine erhebliche Verbesserung der Sprachqualität erreicht werden, weil Sprachpakete vor anderen Daten im Netzwerk zum Empfänger weitergeleitet werden können und somit Verzögerungen und Paketverluste im Netzwerk für Sprachdaten weitestgehend vermieden werden.
Der IPv4-Header enthält folgende Felder:

- Version (4 Bit): Versionsnummer.
- Header Length (4 Bit): Länge des Headers in Byte.
- Type-of-Service (8 Bit): Festlegung für die Dienstgüte. Kann verwendet werden, um eine bevorzugte Weiterleitung von wichtigen Daten, wie z.B. Sprachdatenpaketen, zu ermöglichen. Bei VoIP wird auch eine Neudefinition dieser acht Bit als DiffServ-Feld verwendet.
- Total Length (16 Bit): Gesamtlänge des Pakets inklusive Header.
- Identification (16 Bit): Fortlaufende Nummerierung fragmentierter Telegramme.
- Flags (3 Bit): Bits zur Steuerung des Fragmentierungsmechanismus.

- Fragment Offset (13 Bit): Position des aktuellen Dateninhalts (Fragments) in einem Telegramm, das aus mehreren Fragmenten besteht.
- Time to Live (8 Bit): „Lebensdauer“ eines Telegramms. Kennzeichnet, über wie viele Netzwerkknoten (Router bzw. Layer 3-Switches oder Gateways) hinweg ein Telegramm transportiert werden darf. Der Wert wird innerhalb jeder Netzwerkkomponente einer Transitstrecke dekrementiert. Bei Erreichen des Wertes Null wird das Telegramm verworfen.
- Protocol Type (8 Bit): Identifikation des übergeordneten Transportprotokolls, wie z.B. UDP oder TCP.
- Header Checksum (16 Bit): Checksumme, mit der ein Empfänger Fehler im Telegrammheader identifizieren kann.
- Source IP Address (32 Bit): Absenderadresse des Telegramms.
- Destination IP Address (32 Bit): Zieladresse des Telegramms.
- Options (Länge variabel): In IPv4 definierte Optionen, die z.B. Informationen über Routingverfahren enthalten.
- Padding (Länge variabel): Bits, die den Header auf ein Vielfaches von 32 Bit mit Nullwerten auffüllen.

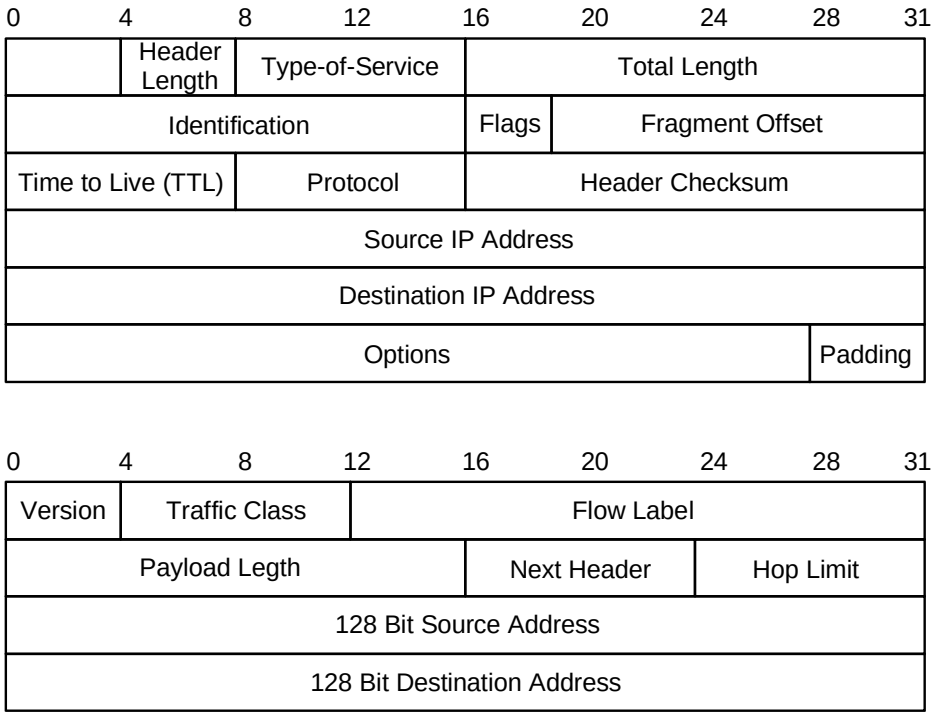

Bild 36: Paketheader IPv4 (oben) und IPv6 (unten) im Vergleich

Der IPv6-Header enthält folgende Felder:

- Version (4 Bit): Versionsnummer.
- Traffic Class (8 Bit): Prioritätenunterscheidung in den Netzwerkknoten, die z.B. vom DiffServ-Verfahren verwendet wird.
- Flow Label (20 Bit): Durch den Absender werden identische Flow-Labels für alle Daten vergeben, die einem gemeinsamen Flow zugeordnet werden. Die Kombination aus Source Address. und Flow Label ist eindeutig.
- Payload Length (16 Bit): Länge des Telegramminhalts ohne Header.
- Next Header (8 Bit): Identisch mit IPv4 Protocol-Type-Feld.
- Hop Limit (8 Bit): Identisch mit IPv4 Time-to-Live-Feld.
- Source IP Address (128 Bit): Absenderadresse des Telegramms.
- Destination IP Address (128 Bit): Zieladresse des Telegramms.

4.3.2 User Datagram Protocol - UPD

Das UDP-Protokoll (IETF Standard RFC 768) ermöglicht Anwendungsprogrammen einen einfachen Informationsaustausch auf Basis von Daten-Telegrammen. Es setzt direkt auf dem IP-Protokoll auf und stellt die einfachste Netzwerkschnittstelle für Anwendungsprogramme basierend auf dem IP-Protokoll dar.
Die Datentelegramme werden direkt zwischen zwei Endgeräten ausgetauscht, ohne dass eine Empfangsbestätigung oder Transportsicherung erfolgt. Der Empfang von UDP-Paketen wird nicht garantiert. Pakete, die den Empfänger nicht erreicht haben, werden nicht wiederholt gesendet. Diese Eigenschaft von UDP hat in Bezug auf VoIP sowohl positive als auch negative Eigenschaften. Wiederholtes Senden von Datenpaketen würde bei Sprachdaten zu einer Zeitverzögerung bei der Wiedergabe führen, weshalb UDP bessere Echtzeiteigenschaften hat als beispielsweise TCP mit Transportsicherung. Nachteilig ist ein möglicherweise hoher Paketverlustanteil in Netzen wie dem Internet, wo ein signifikanter Anteil von Datenpaketen auf der Übertragungsstrecke verloren geht. Ursache sind meist überlastete Netzwerkkomponenten, die empfangene Pakete verwerfen, wenn sie diese nicht verarbeiten können. In mobilen Netzen entstehen Paketverluste häufig auch durch Übertragungsstörungen.

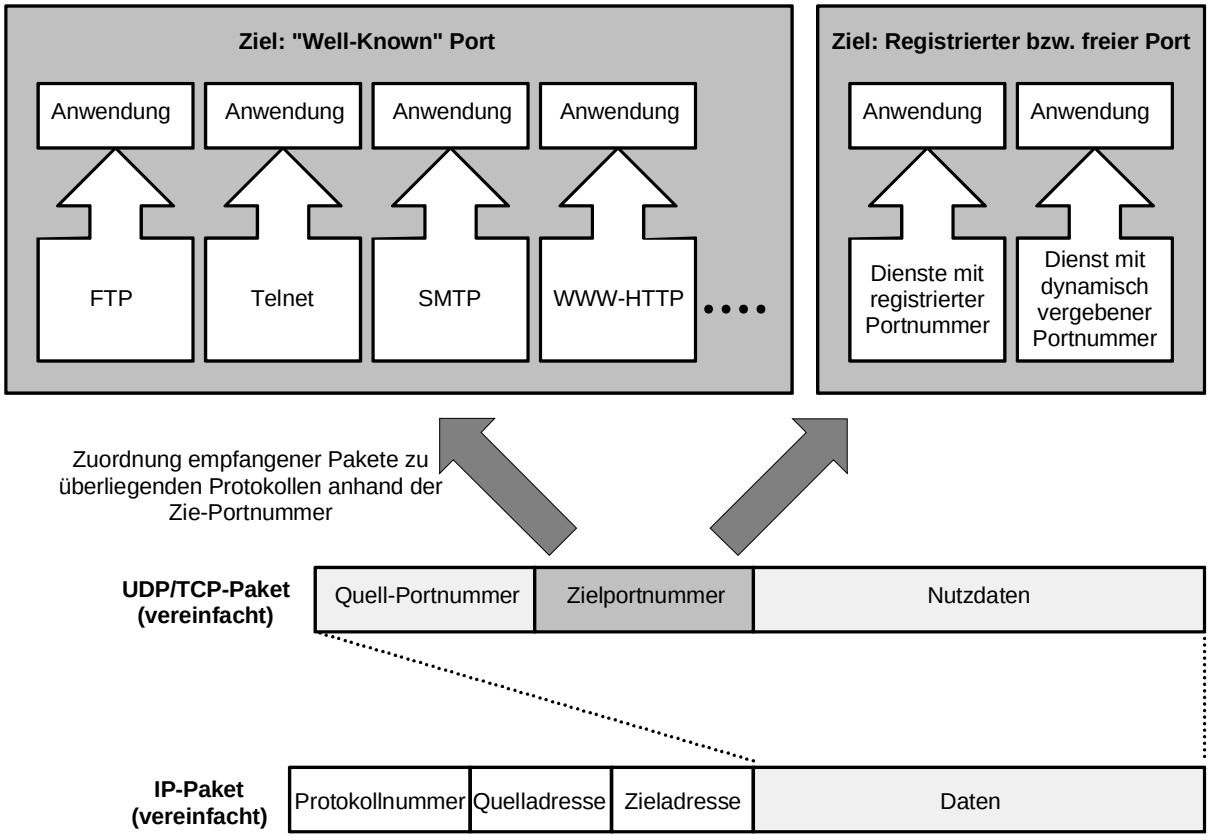

Bild 37: Portnummern als lokales Adressierungsmerkmal

UDP verwendet ein zusätzliches Datenfeld zur Adressierung, das ebenfalls beim TCP-Protokoll verwendet wird. Das unterliegende IP-Protokoll adressiert lediglich Endgeräte anhand ihrer IP-Adresse, die der Netzwerkkarte zugeordnet ist. Als Ausnahme gibt es so genannte Multihomed Hosts – Endgeräte, die mehrere Netzwerkkarten in einem Endgerät enthalten. In diesem Fall sind einem Endgerät mehrere IP-Adressen zugeordnet. Um unterschiedliche Anwendungen innerhalb eines Endgerätes adressieren zu können, verwenden UDP und auch TCP das Adresselement Port. Eine Kombination aus IP-Adresse und Port kann innerhalb eines Endgerätes zu einem beliebigen Zeitpunkt nur von einer Anwendung verwendet werden und ist somit lokal eindeutig. Diese Kombination ermöglicht die eindeutige Adressierung von Anwendungsprogrammen in einem Netzwerk.

Für Echtzeitübertragungen wie VoIP wird oberhalb von UDP das RTP-Protokoll verwendet welches keine festen Portnummern benutzt. Die Kombination aus IP-Adresse und Portnummer muss vor Beginn der Echtzeitübertragung mit Hilfe von Signalisierungsinformationen sowohl für Sender als auch Empfänger ausgetauscht werden, damit eine VoIP-Übertragung stattfinden kann.

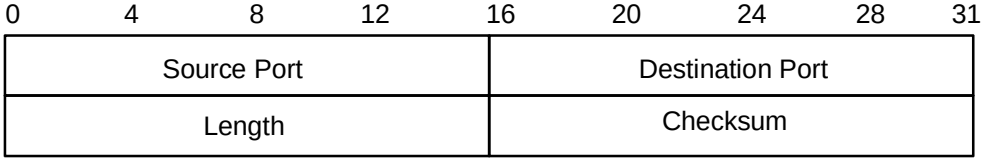

Bild 38: UDP-Paketheader

Der UDP-Header enthält folgende Felder:

- Source Port (16 Bit): Optionales Feld. Sofern ungleich Null, ist üblicherweise die Portnummer des Senders angegeben, um die Rücksendung von Telegrammen mit Hilfe von IP-Adresse und Portnummer zu ermöglichen.
- Destination Port (16 Bit): Gibt das Ziel an. Durch Kombination von IP-Adresse und Portnummer ist die Empfänger-Anwendung netzweit eindeutig bestimmt.
- Length (16 Bit): Enthält die Länge des Datentelegramms inklusive UDP-Header und nachfolgenden Daten.
- Checksum (16 Bit): Checksumme zur Erkennung von Übertragungsfehlern.

4.3.3 Transmission Control Protocol - TCP

Das TCP-Protokoll (IETF Standard RFC 793) ist ein transportsicherndes Protokoll, bei dem der Empfang von Datenpaketen sichergestellt wird. TCP basiert auf Streams, bei denen im Gegensatz zum Datagrammtransport keine logische Aufteilung des Datenstroms auf die Länge einzelner, vom Anwendungsprogramm übergebener Datenpakete erfolgt. Deshalb können der Anwendung auf Empfangsseite die Daten in abweichenden Datenblockgrößen übergeben werden, ohne dass dadurch ein Nachteil entsteht. Die Daten werden meist nicht sofort versendet, sondern werden gepuffert, bis eine gewisse Paketgröße erreicht ist oder für eine bestimmte Zeit keine Daten von der sendenden Applikation abgeliefert worden sind. TCP schützt die Verbindungspartner vor korrupten, verlorenen, duplizierten oder in falscher Reihenfolge übertragenen Datenpaketen. Prozesse, die eine TCP-Verbindung unterhalten, führen einen gesicherten Datenaustausch durch, bei dem der Stream von der empfangenden Anwendung genauso entgegengenommen wird, wie er versendet wurde.
Das streamorientierte Verhalten von TCP impliziert den Nachteil, dass häufig eine Kennzeichnung von Datensätzen notwendig ist, um sie aus einem kontinuierlichen Datenstrom entnehmen zu können.
Beim Senden von einzelnen Nachrichten muss der Push-Mechanismus der TCP-Protokollimplementierung verwendet werden, damit sie verzögerungsfrei gesendet werden. Normalerweise sammelt TCP die Daten, um größere Pakete senden zu können. Der Einsatz des Push-Mechanismus entspricht nicht der Philosophie des TCP-Protokolls, so dass durch Verwenden dieser Sonderfunktionalität ein vom üblichen Verfahren abweichendes Verhalten erzwungen wird.

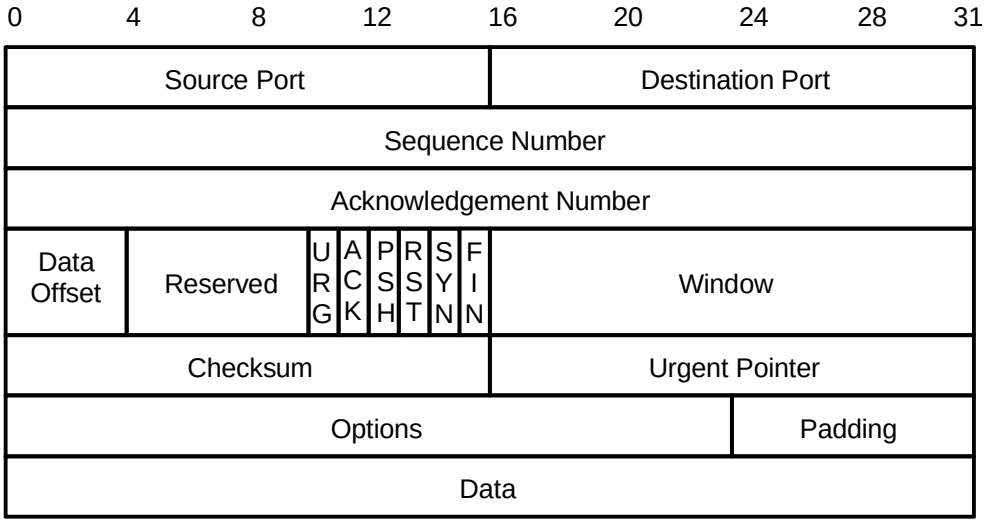

Bild 39: TCP-Paketheader

Der TCP-Header enthält folgende Felder:

- Source Port (16 Bit): Portnummer des Senders von TCP-Paketen.
- Destination Port (16 Bit): Portnummer des Empfängers von TCP-Paketen.
- Sequence Number (32 Bit): Sequenznummer des ersten Bytes zur eindeutigen Identifizierung. Wenn das SYN-Bit gesetzt ist, handelt es sich um die initiale Sequenznummer.
- Acknowledgement Number (32 Bit): Wenn ACK-Bit gesetzt ist, enthält das Feld die Sequenznummer des nächsten von der Gegenstelle erwarteten Pakets.
- Data Offset (4 Bit): Offset, der den Beginn der Daten als Vielfaches von 32-Bit-Worten kennzeichnet.
- Reserved (6 Bit): Reserviert für zukünftige Verwendung.
- Control Bits (6 Bit):
    - URG (1 Bit): Urgent Pointer Feld
    - ACK (1 Bit): Bestätigung von Paketen (Acknowledgment)
    - PSH (1 Bit): Push Funktion für sofortiges Senden
    - RST (1 Bit): Reset der Verbindung
    - SYN (1 Bit): Sequenznummer für die Synchronisation
    - FIN (1 Bit): Beenden der Kommunikation
- Window (16 Bit): Anzahl der Datenbytes, für die Empfangsbereitschaft besteht, beginnend mit dein Byte, das im Acknowledgement Number-Feld enthalten ist.
- Checksum (16 Bit): Checksumme.
- Urgent Pointer (16 Bit): Enthält die Sequenznummer des ersten Bytes, das den Urgent Data folgt. Wird nur verwendet, wenn URG-Bit gesetzt ist.
- Options (Länge variabel): Felder für Optionen.
- Padding (Länge variabel): Bits, die den Header auf ein Vielfaches von 32 Bit mit Nullwerten auffüllen.

Window-Technik

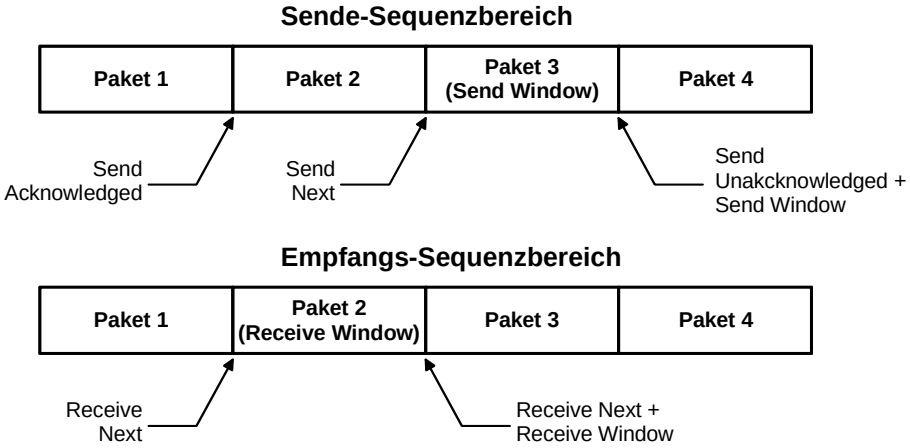

Bild 40: Flusskontrolle mit Send- bzw. Receive-Windows (Window-Technik)

Unter Window-Technik versteht man bei TCP eine Flusskontrolle, bei der ein Empfänger dem Sender mitteilt, wie viele Bytes er, beginnend mit einer bestimmten Sequenznummer, zu empfangen bereit ist. Ein Überlauf des Empfangspuffers kann mit diesem Verfahren zuverlässig verhindert werden.
Die hierfür benötigten Informationen, Sequenznummer und Offset, werden dem Sender in einem Telegramm übermittelt. Dieses Telegramm kann in einer Duplexverbindung selbst Datenblöcke enthalten.
Empfängerseitig ergibt sich das Fenster aus Receive-Next und dem Offset Receive Window. Receive-Next ist der Wert des Acknowledgement Number-Feldes im Datagramm, Receive Window das 16-Bit-lange Window-Feld.
Ein Teilnehmer muss empfangene Daten innerhalb einer festgelegten Zeitdauer bestätigen. Gehen Daten auf dem Übertragungsweg verloren, werden diese automatisch vom Sender nach Ablauf einer Timeout-Zeit wiederholt gesendet, wenn kein Acknowledge empfangen wurde.

4.3.4 Stream Control Transmission Protocol - SCTP

Das „Stream Control Transmission Protocol" (IETF Proposed Standard RFC 2960) wurde vorrangig für die Übertragung von PSTN-Signalisierungsmeldungen über IP-Netze entwickelt ist aber nicht auf diesen Anwendungszweck beschränkt. Im Mittelpunkt stehen die ISDN User Part (ISUP)-Informationen, die in öffentlichen Telefonnetzen über eigenständige SS7- Signalisierungsnetze – und somit unabhängig von den Sprachdaten – übertragen werden.
SCTP bietet gesicherten Datentransport über ungesicherte Paketnetze wie beispielsweise IP. Im Unterschied zum streamorientierten TCP ist SCTP nachrichtenorientiert, was für die Performance von Signalisierungsprotokollen von Vorteil ist. Signalisierungsdaten müssen sofort an den Empfänger weitergeleitet werden, damit keine Verzögerungen im Signalisierungsablauf auftreten.
SCTP bietet folgende Dienste:

- Bestätigter, fehlerfreier und nicht duplizierter Transport von Nutzdaten
- Fragmentierung von Datentelegrammen bei MTU-Überschreitung
- Sequentielle Übertragung von Nachrichten in multiplen Streams
- Optionaler Empfang der Daten in korrekter Reihenfolge
- Optionale Bündelung mehrerer Nutzdatenpakete (User Messages) in einem SCTP-Paket
- Fehlertolerantes Verhalten auf der Netzwerkebene durch Nutzung bei Multi-homed Hosts an einem oder beiden Enden einer Verbindung

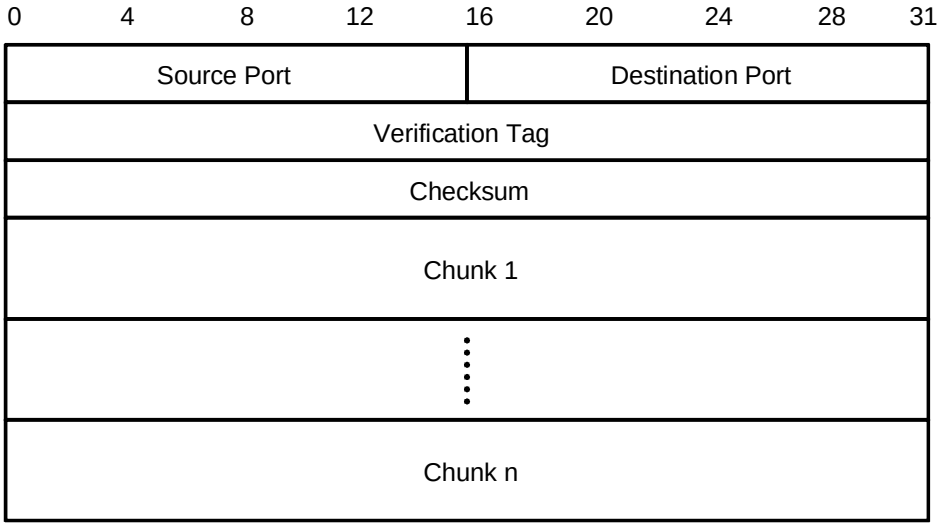

Bild 41: SCTP-Paketheader

Der SCTP-Header enthält folgende Felder:

- Source Port (16 Bit): Portnummer des Senders von SCTP-Paketen.
- Destination Port (16 Bit): Portnummer des Empfängers von SCTP-Paketen.
- Verification Tag (32 Bit): Feld zur Validierung des Senders.
- Checksum (32 Bit): Checksumme.

Dem Header folgen so genannte Chunks bei denen es sich um Datencontainer mit unterschiedlichen Inhalten handelt, die durch den Chunk-Type unterschieden werden.

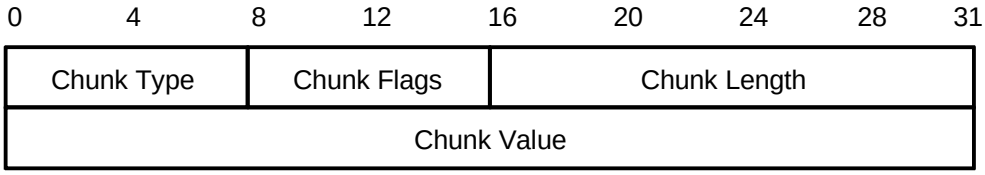

Bild 42: SCTP-Chunk-Format

Ein Chunk des Headers enthält folgende Felder:

- Chunk Type (8 Bit): Art des Chunks, z.B.:
  - 0 Payload Data DATA
  - 1 Initiation INIT
  - 2 Initiation Acknowledgement INIT ACK
  - 3 Selective Acknowledgement SACK
  - 6 Abort ABORT
- Chunk Flags (8 Bit): Flags, deren Definition abhängig vom Chunk Type sind.
- Chunk Length (16 Bit): Länge des Chunks inklusive Chunk Type, Chunk Flags, Chunk Length und Chunk Value.
- Chunk Value (variable Länge): Inhalt des Chunks; z.B.: Payload Data, Initiation, Initiation Acknowledgement, Abort; …….

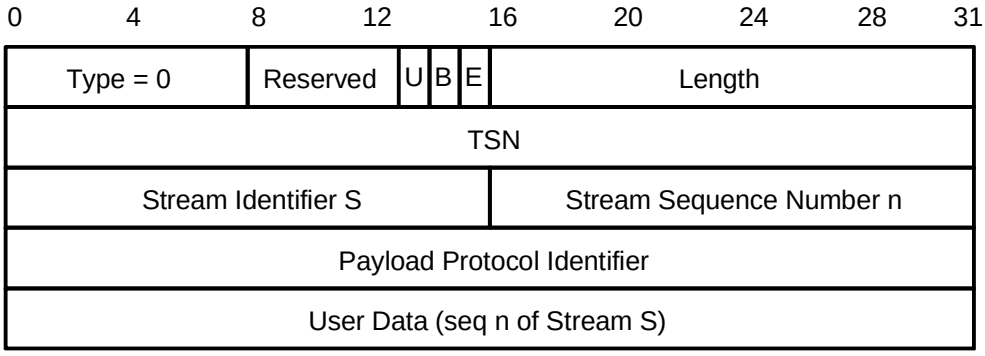

Bild 43: Payload Data Chunk

Der Chunk-Typ Payload Data enthält die folgenden Felder:

- Type (8 Bit): Wert Null.
- Reserved (5 Bit): Felder sind zu ignorieren.
- U (1 Bit): Unordered-Bit, wenn Bit gesetzt ist, handelt es sich um einen ungeordneten Stream und das Feld Stream Sequence Number n wird ignoriert.
- B (1 Bit): Beginning Fragment Bit, wenn Bit gesetzt ist, handelt es sich um den ersten Teil einer fragmentierten Nachricht.
- E (1 Bit): Ending Fragment Bit, wenn Bit gesetzt ist, handelt es sich um den letzten Teil einer fragmentierten Nachricht.
- Length (16 Bit): Länge inklusive aller Chunk-Felder und Nutzdaten.
- TSN (32 Bit): Transmission Sequence Number, die streamübergreifend bei jeder zu sendenden Nachricht inkrementiert wird.
- Stream Identifier S (16 Bit): Identifizierungsnummer eines Streams.
- Stream Sequence Number n (16 Bit): Nachrichten-Sequenznummer innerhalb eines Streams; Wert ist bei fragmentierten Nachrichten für alle Fragmente gleich.
- Payload Protocol Identifier (32 Bit): Protokollidentifizierung, die entweder von der Applikation oder von übergeordneten Protokollschichten festgelegt wird.
- User Data (seq n of Stream S, variable Länge): Die zu transportierenden Nutzdaten.

SCTP als Transportprotokoll für SIP

Für den Einsatz in Zusammenhang mit dem SIP-Protokoll existiert ein Internet-Draft „The Stream Control Transmission Protocol as a Transport for the Session Initiation Protocol" der die Verwendung von SCTP als unterliegendes Transportprotokoll beschreibt.
SCTP eignet sich besonders als Transportprotokoll für SIP-Nachrichten. Gegenüber TCP hat es den Vorteil, Nachrichten sofort versenden zu können und nicht wie bei Streams, größere Paketmengen sammeln zu müssen.
In größeren TK-Netzen, bei denen mehrere SIP-Sessions über eine SCTP-Verbindung übertragen werden kann SCTP Nachrichten unterschiedlicher Streams, die zu verschiedenen Verbindungen gehören, unabhängig voneinander senden und bei Verlusten wiederholen, ohne dass sie einander gegenseitig beeinflussen.

SCTP als Transportprotokoll für H.323

In der zukünftigen Version 5 des H.323 Standards wird ITU-T voraussichtlich SCTP als Transportprotokoll unterstützen.

SCTP in SS7-Signalisierungssystemen öffentlicher Telefonnetze

Eine der Hauptanwendungen für SCTP ist der Transport von ISDN User Part (ISUP)-Nachrichten. Diese Nachrichten werden zwischen nativen TK-Systemen und IP-basierten Systemen mit Hilfe von Signalling Gateways ausgetauscht die als Brücke zwischen den unterschiedlichen Netzwerken dienen und die Verbindungen in ihrem jeweiligen Netz als Signa-

lisierungsendpunkt terminieren. Zwei parallele Protokollstacks beider Netzwerke werden durch eine Signalisierungsanwendungsschicht miteinander verbunden, die als „Message Transfer Part 3 User Adaptation Layer (M3UA)" definiert wurde.

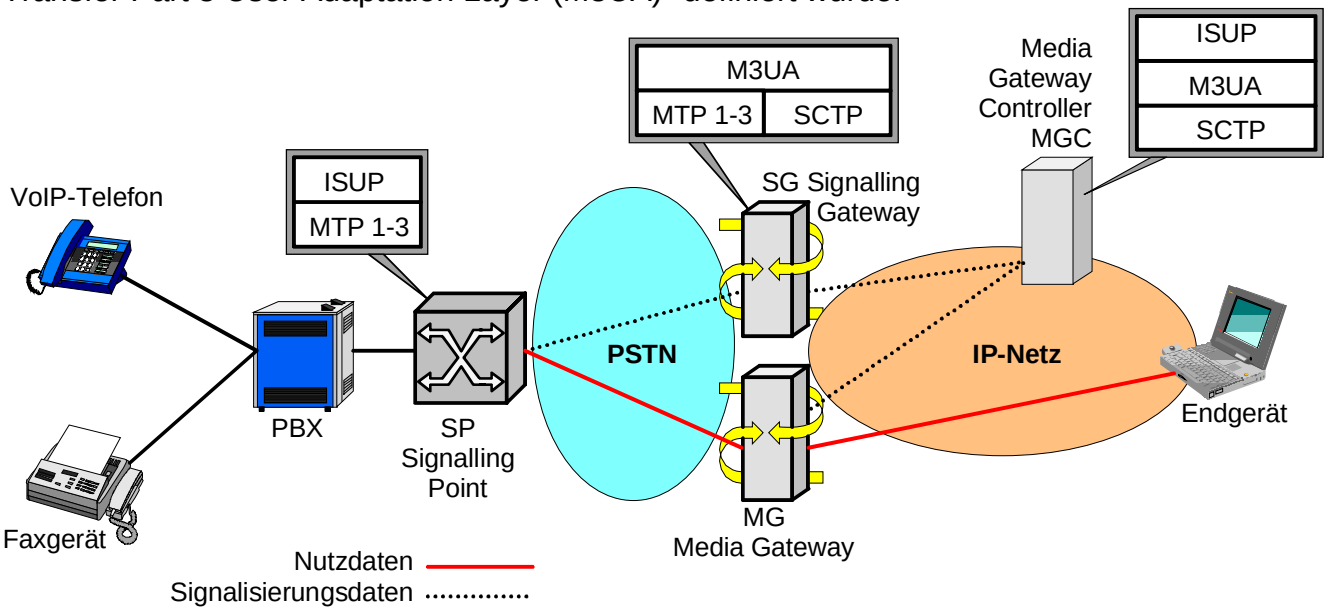

Bild 44: Datenaustausch zwischen SS7-Netz und IP-Netz

Im SS7-Signalisierungsnetz werden die ISUP-Nachrichten über die drei MTP-Protokollschichten MTP-1, -2 und -3 geleitet. Der MTP wird im Signalisierungsgateway terminiert. Über die M3UA-Anpassungsschicht wird der ISUP mit Hilfe der Protokollschichten SCTP, IP und dem MAC-Layer – im Allgemeinen Ethernet – in das IP-Netz geleitet. Die SCTP-IP-Protokollschichten sind identisch in den Media Gateway Controllern (MGC) implementiert und enthalten ebenfalls die M3UA-Anpassungsschicht, die dem MGC die unveränderten ISUP-Nachrichten zur Verfügung stellt.
Der MGC steuert aufgrund der ISUP-Signalisierungsdaten die Media-Gateways, um Sprachverbindungen zwischen Endgeräten im TK- und im IP-Netz schalten zu können. Damit eine große Anzahl von Verbindungen gleichzeitig gesteuert werden kann und um die Verfügbarkeit zu erhöhen, können MGCs zu Clustern in einer verteilten Rechnerarchitektur zusammengeschaltet werden. Mittels Trunking können Signalling Gateways eine größere Anzahl von Signalisierungsverbindunger für die Sprachtelefonie in einer SCTP-Session bündeln.

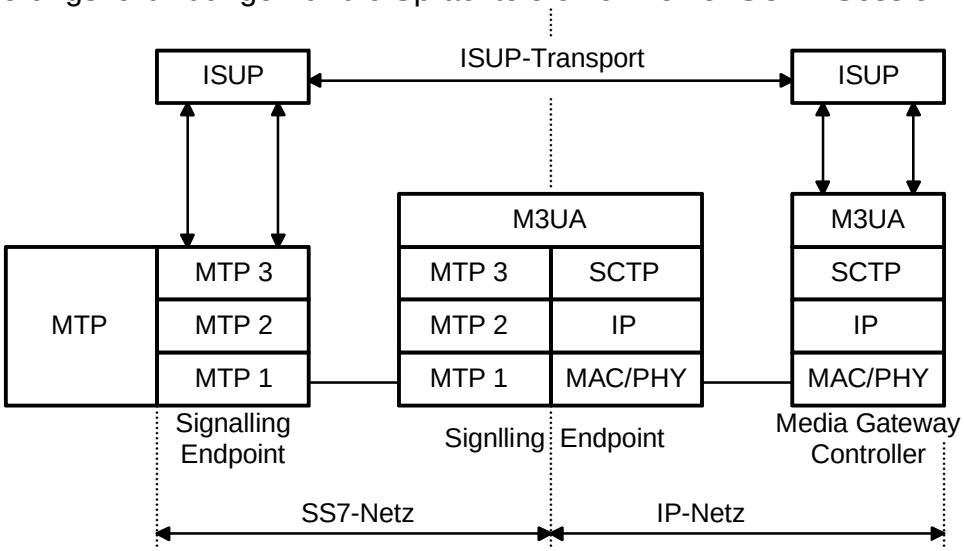

Bild 45: Austausch von ISDN-ISUP Nachrichten zwischen SS7- und IP-Netzen

4.4 Gateway- und Routingprotokolle

4.4.1 Media Gateway Control Protocol H.248/Megaco

Protokolle zur Steuerung von Gateways konzentrieren die „Intelligenz" eines Netzwerkes im Zentrum wobei Gateways am Rand des Netzwerkes als Slave-Instanzen von einem Softswitch bzw. Call Agent als Master-Instanz gesteuert werden.
In der Vergangenheit gab es mehrere getrennte Entwicklungen. Zuerst enstanden das „Simple Gateway Control Protocol" (SGCP) und das „IP Device Control" (IPDC) als Industrieentwicklungen und anschließend, aus beiden hervorgegangen, das „Media Gateway Control Protocol" (MGCP) der IETF und der ITU-T.

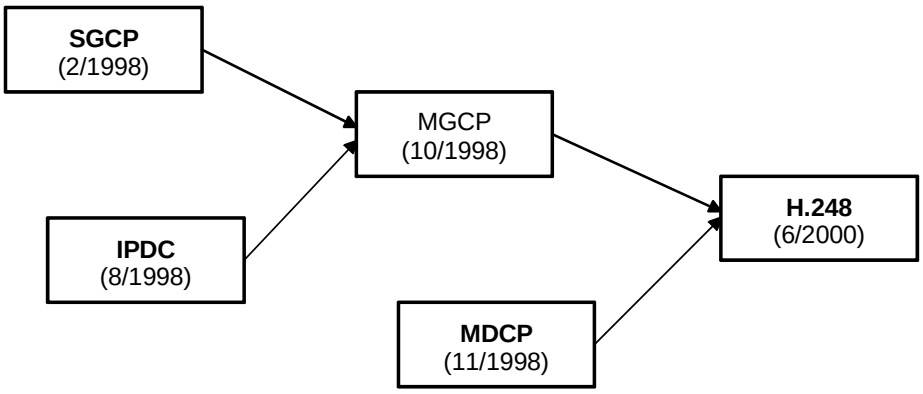

Bild 46: Evolution der Gateway-Steuerungsprotokolle

Das Protokoll zur Steuerung von Medien-Gateways H248/Megaco (nachfolgend als Megaco bezeichnet) arbeitet unabhängig von der Rufsignalisierung mit H.323 oder SIP.
Die Steuerung von Verbindungen wird zentral im Netzwerk lokalisiert. Die als Call Agents, Softswitch oder Media Gateway Controller (MGC) bezeichneten Rufsteuerungsinstanzen ersetzen den einfachen Gatekeeper oder SIP-Proxy-Server durch eine multiprotokollfähige Instanz, die H.323, SIP und weitere Signalisierungsprotokolle implementieren kann.

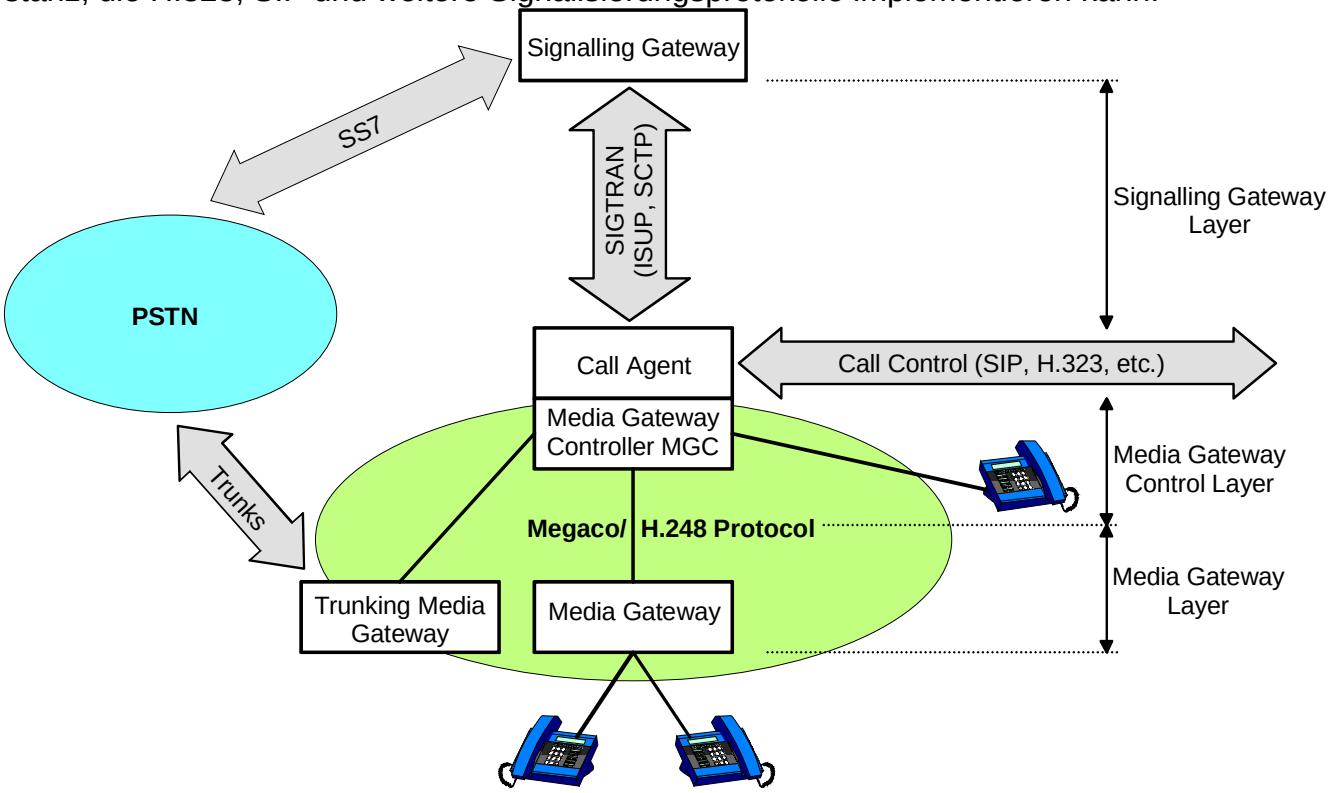

Bild 47: Einsatzbereich von H.248/Megaco

Ein MGC ist die Schnittstelle zwischen Endgerät und Signalisierungsgateway und tauscht Informationen mit Signalisierungsgateways aus, die auf der PSTN-Seite beispielsweise SS7-Netze terminieren. Es handelt sich um ISUP-Informationen, die über das SIP-ISUP-Mapping, (RFC 3398) in einem MGC umgesetzt werden.
Auf der anderen Seite steuert ein MGC mit Hilfe des Megaco-Protokolls die an den Netzwerkschnittstellen zu PSTN-Netzen installierte Mediengateways, deren Controller Sprachkanäle zwischen Endgeräten und Gateways oder, bei Transitnetzen, zwischen mehreren Gateways schalten können. So kann mit Hilfe von Megaco die Trennung von Signalisierung und Sprachdaten der digitalen PSTN-Netze nahtlos in Paketnetzen abgebildet werden.
Die Media Gateway Controller übernehmen als steuernde Instanzen in einem Master/Slave-Verhältnis die Master-Funktion. Gateways für den Medientransport (MGs) werden als Slaves von den MGCs gesteuert. Das Megaco-Protokoll wird ausschließlich zwischen Media Gateway Controller und Media Gateway eingesetzt.
Megaco unterstützt unterschiedliche paketbasierte Netze, wie beispielsweise IP oder ATM, und unterstützt auf der PSTN-Netzwerkseite Signalisierung u.a. durch Ton-Signalisierung (DTMF-Töne), ISDN, ISUP, QSIG und GSM.

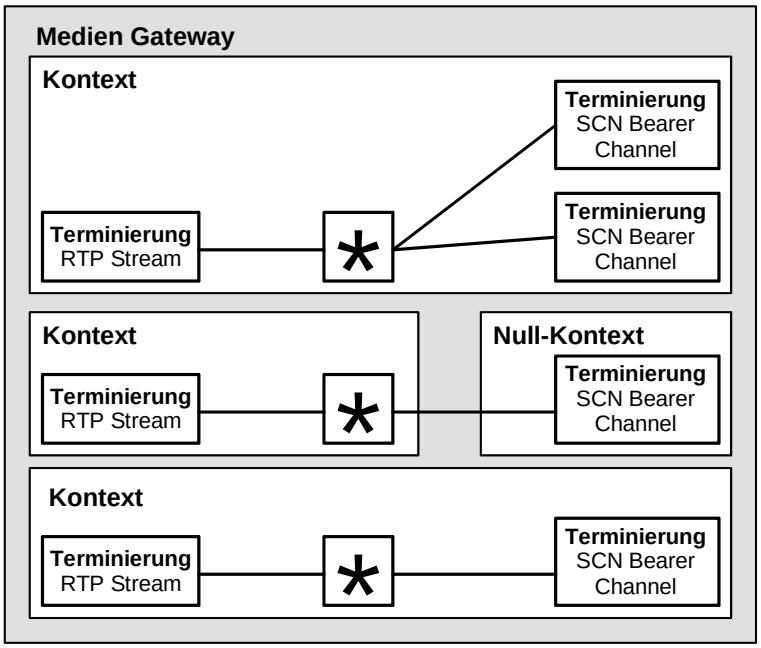

Bild 48: Verbindungsmodell von H.248/Megaco

Das Verbindungsmodell von Megaco ist kontextbasiert was bedeutet dass Terminierungen auf PSTN-Seite und auf der Paketnetz-Seite einen Medienaustausch erlauben, wenn sie einem gemeinsamen Kontext zugeordnet sind.
Beispiele von Kontexten sind in Bild 5.37 dargestellt. Der erste Kontext stellt eine Dreierkonferenz zwischen einem Teilnehmer im Paketnetz und zwei Teilnehmern im PSTN-Netz dar. Im zweiten Beispiel ist ein NULL-Kontext enthalten, der einen nicht verbundenen Teilnehmeranschluss zeigt. Der dritte Kontext zeigt eine einfache Punkt-zu-Punkt-Verbindung zweier Teilnehmer zwischen PSTN und IP-Netz.
Bild 49 zeigt ein Szenario, bei dem ein wartender Anruf angenommen wird. Zunächst ist Terminierung T1 (RTP-Stream) mit T2 (SCN-Verbindung) im Kontext 1 verbunden, während T3 (SCN-Verbindung) — allein im Kontext 2 — wartet. Im zweiten Schritt wird der wartende Ruf T3 mit T2 verbunden, wobei T2 vom Kontext 1 nach Kontext 2 übergeht. Jetzt wartet T1 allein im Kontext 1.

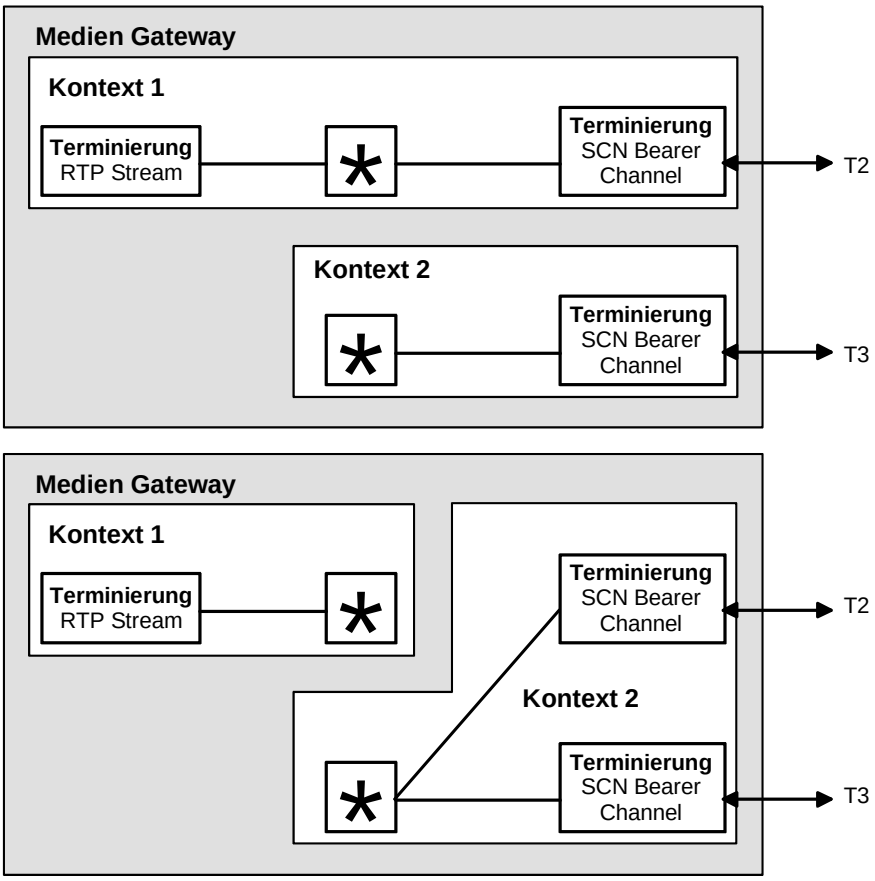

Bild 49: Szenario eines wartenden Anrufs (Call Waiting)

4.4.2 Telephony Routing over IP - TRIP

Das Telephony Routing over IP (TRIP)-Protokoll übermittelt Domain-übergreifend Informationen über die Erreichbarkeit von Teilnehmern in IP-basierten Telefonnetzen und über die Eigenschaften der zu verwendenden Routen zwischen so genannten Location-Servern. Es arbeitet unabhängig von den Signalisierungsprotokollen für Endgeräte wie H.323 oder SIP. TRIP orientiert sich an dem Border Gateway Protocol (BGP-4), das ähnliche Aufgaben für das IP-Routing erfüllt.

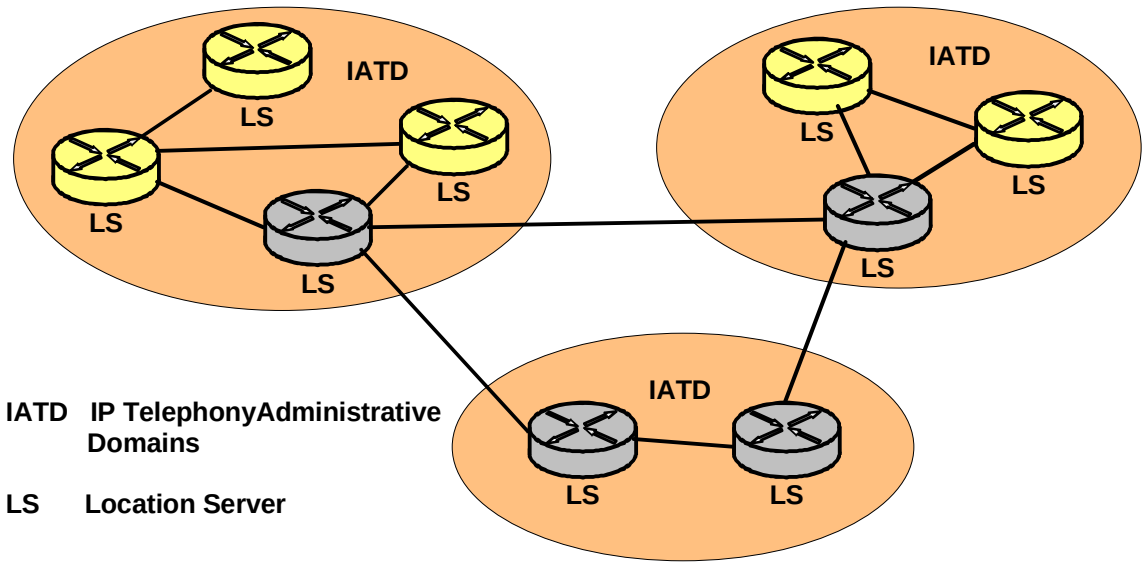

Bild 50: TRIP-Datenaustausch über Routinginformationen

Daten werden in der „Telephony Routing Information Base" (TRIB) gespeichert. Diese werden zwischen „IP Telephony Administrative Domains" (ITADs) ausgetauscht. Die Informationen über TRIP-Ziele bestehen aus Adressen, die mit der Information über das bei Anrufen zu verwendende Endgeräte-Signalisierungsprotokoll, wie z.B. H.323 oder SIP, verknüpft sind.

5 Bilder und Tabellen

6 Abkürzungen

1 TR6	Nationales ISDN-Protokoll für den ISDN D-Kanal
3GPP	3rd Generation Partnership Project
A/D	Analog/Digital
AAL	ATM Adaption Layer
ABNF	Augmented Backus Naur Form
AbS	Analysis by Synthesis
ACELP	Algebraic-Code-Excited Linear-Prediction
ADPCM	Adaptive Differential Pulse Code Modulation
ADSL	Asymmetric Digital Subseriber Line
ADSpec	Admission Specification
AH	IP Authentification Header
ALG	Application Layer Gateway
AMR-WB	Adaptive Multi-Rate-Wideband
ANF	Additional Network Feature
ASN.1	Abstract Syntax Notation 1
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BRI	Basic Rate Interface
CAR	Committed Access Rate
CAS	Channel Associated Signalling
CBR	Constant Bit Rate
CCITT	International Telegraph and Telephone Consultative Conunittee
CDR	Call Detail Records
CELP	Code Excitation Linear Predictivc Coding
CIR	Committed Information Rate
CNAME	Canonical Name
CNG	Comfort No ise Generation
CoS	Class-of-Service
CRD	Call Related Data
CRTP	Compressed RTP
CS-ACELP	Conjugate-Structure Algebraic-Code-Excited Linear-Prediction
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSRC	Contributed Source
CTI	Computer-Telefony-Integration
D/A	Digital/Analog
DBCES	Dynamic Bandwidth Circuit Emulation Service
DECT	Digital European Cordless Telephone Standard
DES	Data Encryption Standard
Diffserv	Differentiated Services
DPCM	Differential-PCM
DSCP	Differentiated Services Codepoint
DSL	Digital Subscriber Line
DSLAM	DSL-Access-Multiplexer
DSS	Digital Signature Standard
DSS1	Digital Subscriber Signalling System No. I
DTMF	Dual Tone Multi-Frequency
DUP	Data User Part

ECMA	European Computer Manufacturer's Association
E-DSS1	European Digital Subscriber Signalling System No. 1
E-LSP	Experimental LSP
EN	Egress Node
ENUM	Telephone Number Mapping
ERL	Echo Return Loss
ESP	IP Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
FDDI	Fiber Distributed Data Interface
FEC	Forward Error Correction
FEC	Forwarding Equivalence Class
FEP	Firewall Enhancement Protocol
FIFO	First-In-First-Out
FoIP	Fax over IP
FTP	File Transfer Protocol
G3	Fax Gruppe 3
G4	Fax Gruppe 4
GCF	Gatekeeper Confirmation
GF	Generic Funetional Procedures
GRQ	Gatekeeper Request
GSM	Global System for Mobile Communications
H.xxx	Nummerierte Standards der 1TU-T
HDSL	High Bitrate Digital Subscriber Line
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
I.xxx	Numerierte Standards der ITU-T
IAD	Integrated Access Device
JANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IN	Ingress Node
IN	Intelligent Network
IP	Internet Protocol
IPDC	IP Device Control
IPSec	IP Security Protocol
Iptel	IP Telephony Working Group (IETF)
IPX	Internetwork Packet Exchange Protocol
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISUP	ISDN User Part
ITAD	IP Telephony Administrative Domain
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IVR	Interactive Voice Response
LAN	Local Area Network
LDP	Label Distribution Protocol
LIFO	Last-In-First-Out
L-LSP	Label-inferred LSP
LPC	Linear Predictive Coding
LSP	Label Switched Path

LSR	Label Switched Router
LWL	Lichtwellenleiter
M2UA	Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) -User Adaptation Layer
M3UA	Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) -User Adaptation Layer
MAC	Media Access Control
MBone	Multicast Backbone
MC	Multipoint Controller
MCU	Multipoint Control Unit
MD5	(Hash-Funktion)
MDCP	Media Device Control Protocol
Megaco	Media Gateway Control Protocol
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MIDCOM	Middlebox Communications
MOS	Mean Opinion Score
MP	Multipoint Processor
MPLS	Multiprotocol Label Switching
MTP	Message Transfer Part
MTU	Maximum Transfer Unit
NAT	Network Address Translation
NetBEUI	NetBIOS Extended User Interface
NT	Network-Termintor
NTP	Network Time Protocol
OID	Object Identifier
0-MAP	Operations Maintenance and Administration Part
OSI	Open System Interconnection
PAMS	Perceptual Analysis Measurement System
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PDH	Plesiochrone Digitale Hierarchie
PDP	Policy Decision Point
PER	Packet Encoding Rules
PESQ	Perceptual Evaluation of Speech Quality
PGP	Pretty Good Privacy
PHB	Per Hop Behaviour
PIB	Policy Infonnation Base
PICS	Protocol Implementation Confonnance Statements
PINT	PSTN to Internet Interworking
P1NX	Private Integrated Network Exchange
PISN	Private Integrated Services Network
PPP	Point to Point Protocol
PPPoE	Point-to-Point-Protocol over Ethernet
PRI	Primary Rate Interface
PSQM	Perceptual Speech Quality Measurement
PSSI	Private Signalling System 1
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Connection

QSIG	Signalisierung am Q.Referenzpunkt
Q.xxx	Nummerierte Standards der ITU-T
QoS	Quality of Service
RAS	Registration, Admission and Status
RELP	Residual Excited Linear Prediction
RFC	Request For Comment
RPE-LTP	Regular Pulse Excitation Long Term Predictor
RR	Receiver-Report
RSA	Rivest-Shamir-Adleman
RSVP	Resource Reservation Protocol
RTCP	RTP Control Protocol
RTP	Realtime Transport Protocol
RTT	Round Trip Times
rt-VBR	real-time Variable Bit Rate
S/MIME	Secure/Multipurpose Internet Mail Extensions
ISDN-Basisraten-Schnittstelle	
S2M	ISDN-Primärraten-Schnittstelle
SA	Security Association
SAP	Session Announcement Protocol
SB-ADPCM	Subband Adaptive Differential Pulse Code Modulation
SCCP	Signalling Connection Control Part
SCM	Selected Communications Mode
SCN	Switched Circuit Network
SCTP	Stream Control Transmission Protocol
SCU	System Control Unit
SDH	Synchrone Digitale Hierarchie
SDP	Session Description Protocol
SDSL	Symmetric Digital Subscriber Eine
SG	Signalling-Gateway
SGCP	Simple Gateway Control Protocol
SHA	(Hash-Funktion)
SIGTRAN	Signaling Transport Working Group (IETF)
SIP	Session Initiation Protocol
SIPPING	Session Initiation Proposal Investigation Working Group (IETF)
SIP-T	SIP for Telephons
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPAN	Simple Protocol for Augmenting NATs
SPIRITS	Services in the PSTN/IN Requesting Internet Services
SPX	Sequenced Packet Exchange Protocol
SR	Sender Report
SRTP	Secure Real-time Transport Protocol
SS7	Signalling System No. 7
SSL	Secure Socket Layer Protocol
SSRC	Synehronization Source
SSTP	Services Support Transfer Protocol
ST2	Internet Stream Protocol Version 2
STP	Signalling Transfer Points
STUN	Simple Traversal of UDP Through Network Address Translators
SVC	Switched Virtual Connection
TC	Transaction Capabilities

TCA	Traffic Conditioning Aggregates
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE	Terminal Equipment TK-Anlage Telekommunikations-Anlage
TLS	Transport Layer Security
ToS	Type-of-Service
TRIB	Telephony Routing Information Base
TRIP	Telephony Routing over IP
Tspec	Traffic Specification
TTP	Time Token Protocol
TUP	Telephone User Part
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USV	Unterbrechungsfreie Stromversorgung
V5UA	V5.2-User Adaptation Layer
VAD	Voice Activity Detection
VBR	Variable Bit Rate
VCA	Voice Controlled Assistent
VCI	Virtual Channel Identifier
VDSL	Very high bit-rate Digital Subscriber Line
VLAN	Virtual Bridged Local Arca Networks
VoATM	Voice over ATM
VoDSL	Voice over DSL
VoFR	Voice over Frame Relay
VoIP	Voice over IP VoIPoMPLS Voice over IP over MPLS
VoMPLS	Voice over MPLS
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless-LAN

7 Literatur und Web-Links

[1] Jochen Nölle: Voice over IP, ISBN 3-8007-2850-8, VDE Verlag GmbH Berlin und Offenbach 2005
[2] Mathias Hein: Voice over IP, ISBN: 3772366864, Franzis Verlag 2002
[3] Anatol Badach, Voice over IP - Die Technik. Grundlagen und Protokolle für Multimedia-Kommunikation, ISBN: 3446403043, Hanser Fachbuchverlag; Auflage: 2., überarb. u. erw. Aufl. (Juni 2005)
[4] Davidson, Voice over IP - Grundlagen - Cisco Press . Konzepte, Technologie, Anwendungen, ISBN: 3827258006, Verlag Markt+Technik; Auflage: 1. Aufl. (15. Juli 2000)
[5] Andreas Tikart, Voice over IP - Das Praxisbuch, ISBN: 3826616294, Mitp-Verlag (Mai 2006)

[6] Einführung in VoIP,
http://www.florianmessner.com/support/themen/voip/
[7] ENUM-Einführung,
http://www.bakom.ch/de/telekommunikation/numad/internet/unterseite01050/index.html
[8] Sprachkodierung und Kompression
http://www.swyx.de/basics/codec.html
[9] Migrationsszenarien
http://www.swyx.de/basics/szenario-migration.html

Protokolle und Standards lassen sich über die nachfolgend aufgeführten WWW-Seiten der Standardisierungsgremien beziehen:
ECMA: Kostenlos über Web-Interface
http://www.ecma-international.org/publications/publications.htm
IEEE: Kostenlos über Web-Interface für LAN/MAN-Netzwerkstandards:
http://standards.ieee.org/getieee802
IETF: Kostenlos über Web-Interface
http://www.ietf.org/rfc.html , Eingabe der RFC-Nummer im Formular
ITU-T: Kostenpflichtig, über Web-Interface
http://www.itu.int/ITU-T/publications/recs.html
ISO: Kostenpflichtig, über Web-Interface
http://www.iso.org/iso/en/CatalogueListPage.CatalogueList