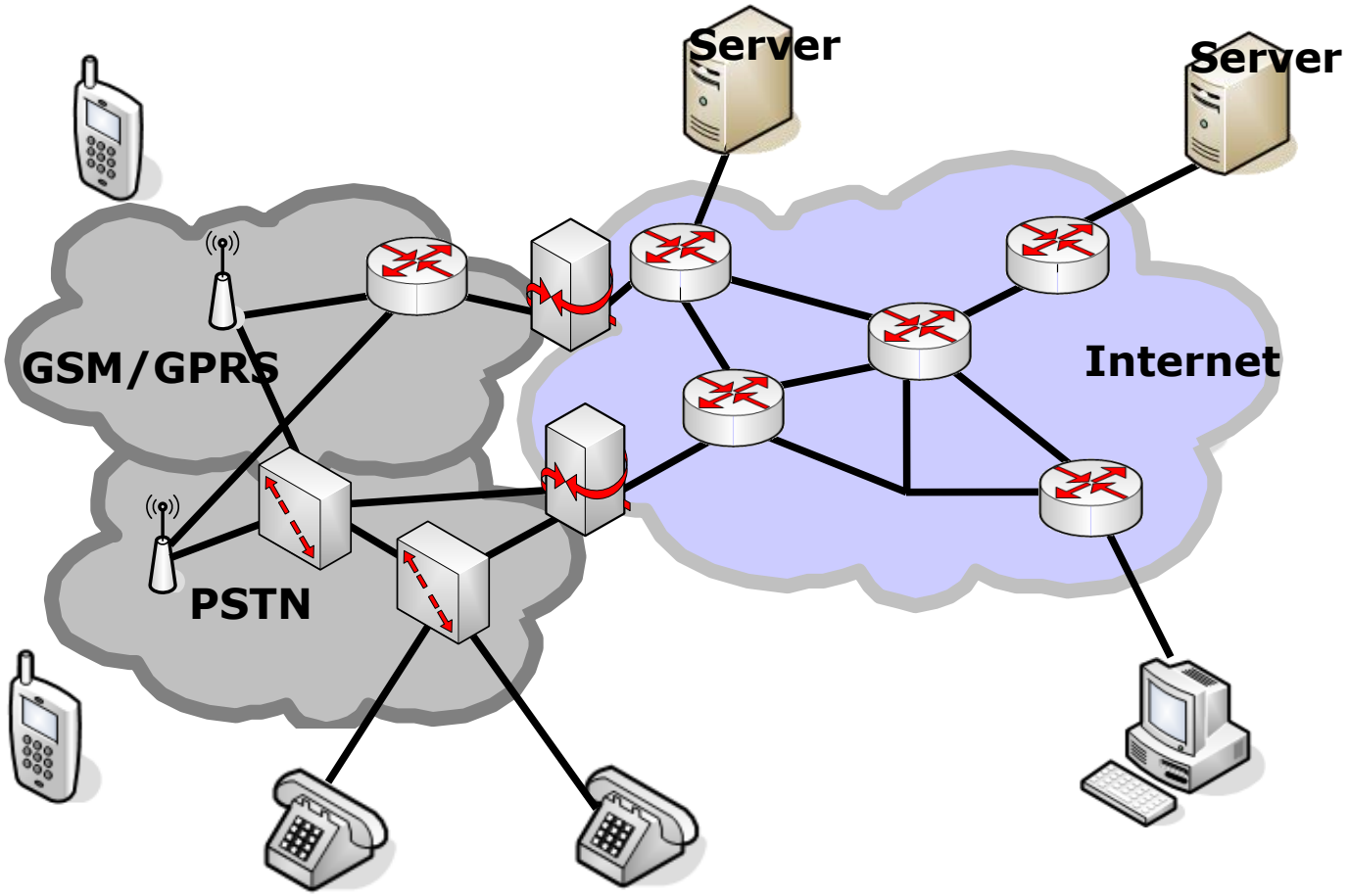
Rechnernetze und Telekommunikation

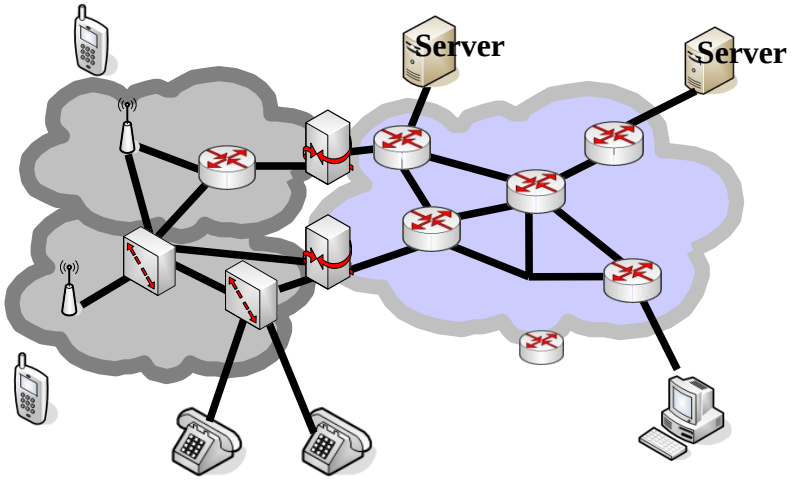
NGNs und VoIP

Previous Generation Networks (1)



Previous Generation Networks (2)

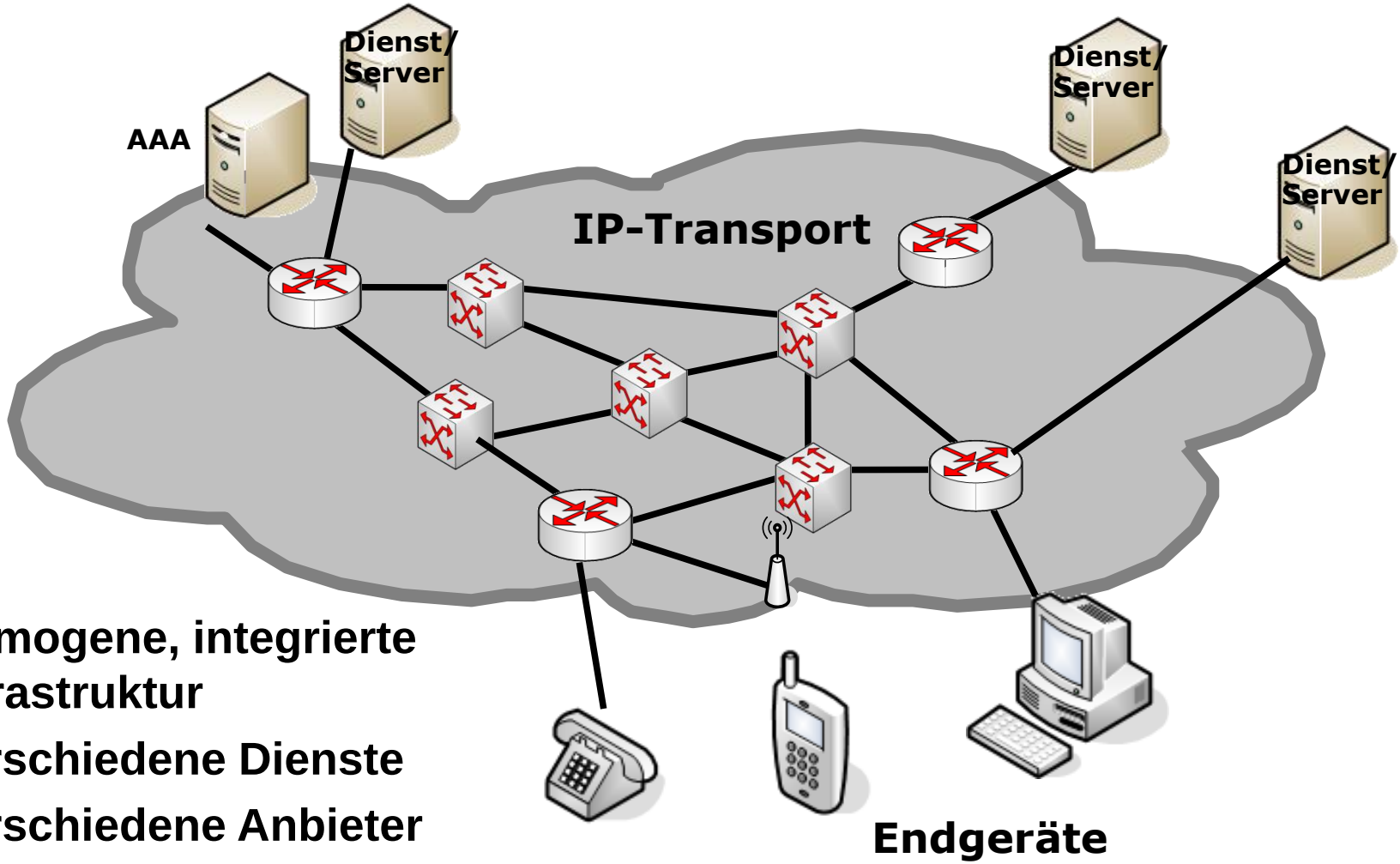
- Dienste und Infrastrukturen sind eins und sind in einer Hand
- Infrastrukturen sind heterogen
  - Verschiedene Technologien
  - Leitungs- und paketvermittelt
  - Verbunden über Gateways



NGNs

- **Ein Netz der nächsten Generation (NGN) nach ITU-Def.**
  - ist ein paketvermittelndes Telekommunikationsnetz
    - das Telekommunikationsdienste bereitstellt
    - viele breitbandige, dienstgüteklassenfähige Transporttechnologien nutzt
    - bei dem dienstbezogene Funktionen unabhängig von der genutzten Transporttechnologien sind
  - bietet den Nutzern uneingeschränkten Zugang zu Netzen, zu konkurrierenden Dienstanbietern und/oder Diensten ihrer Wahl
    - "Netzneutralität"
  - unterstützt die allgemeine Mobilität, durch allgegenwärtige Bereitstellung von Diensten
    - Geräte und Nutzermobilität
  - erfüllt alle regulatorischen Anforderungen
    - z. B. Notfallkommunikation, Sicherheit, Lawful Interception usw.

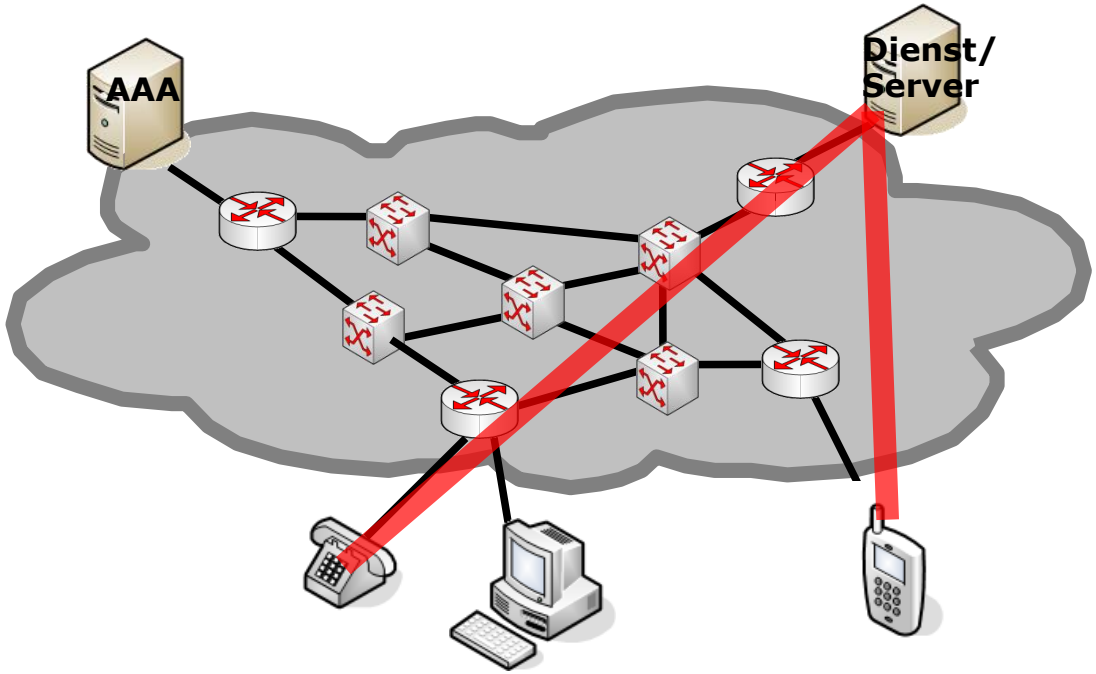
Next Generation Networks



- Homogene, integrierte Infrastruktur
- Verschiedene Dienste
- Verschiedene Anbieter

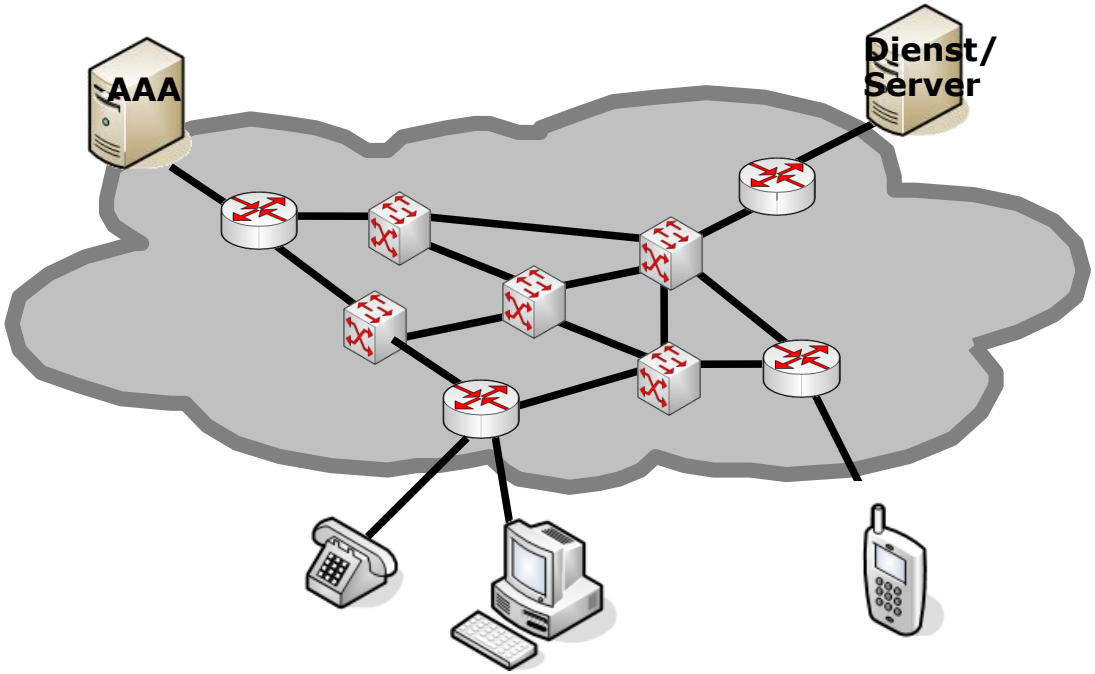
Prinzipien und Architektur des NGN

- Dienstunabhängiges Core-Network
  - Paketvermittelt
  - Mit durchgängiger QoS
  - Multicast-fähig
- Dienste in den Endpunkten realisiert
  - Services sind nur Software auf Terminals und Servern
- AAA-Server
  - zur zentralen Authentifizierung



NGN – Wozu eigentlich?

- **Netzneutralität bringt**
  - Konkurrenz der Dienstanbieter und
  - Innovationsfähigkeit
- **Mobilität der**
  - Nutzer und
  - Endgeräte
- **Konvergenz der**
  - Dienste und
  - Endgeräte



Was ist VoIP ?

- **VoIP ist die Übertragung von Sprache über IP (oder generell: Paket-vermittelte Netze wie z.B. das Internet).**
- **VoIP hat alle Features, die es zuvor im POTS (Plain Old telephone service) gab**

- **Spezielle Anforderungen:**
  - **Security**
    - Abhörsicherheit
    - Authentifizierung
    - Kein SPIT (spam over internet telephony)!
  - **Kompatibilität**
    - Notrufe
  - **Verfügbarkeit**
    - Endgeräte und Server (wie im POTS!)
    - Mobile Clients

Vorteile von VoIP

- Geringere Kosten (insb. für Ferngespräche)
- Einfachere Integration von Software-Anwendungen (z.B. Voice-Mail, Call-Center, etc.)
- Unified Messaging
- Virtuelle Konferenzräume (Teleconferencing)
- Hosted PBX

- Alles implementierbar durch Software
  - Z.B. Asterisk (http://www.asterisk.org/)

MOS - Mean Opinion Score

- **Verfahren zur subjektiven Beurteilung der Qualität von Sprach- und Bildübertragungen**
  - **5-Stufige Skala**
  - **POTS: 4,2, GSM: 3,7, schlechtes GSM: 3**
  - **Anforderung VoIP (ideal): 4,5**

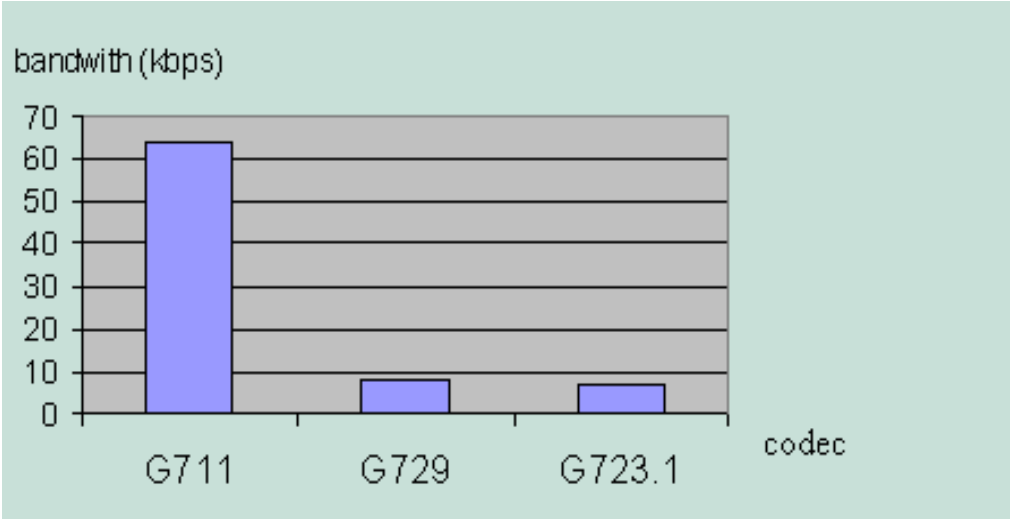
Wert	Quality	Bedeutung
5	excellent	Es ist keine Anstrengung nötig, um die Sprache zu verstehen.
4	good	Durch aufmerksames Hören kann die Sprache ohne Anstrengung wahrgenommen werden.
3	fair	Die Sprache kann mit leichter Anstrengung wahrgenommen werden.
2	poor	Es bedarf großer Konzentration und Anstrengung, um die übermittelte Sprache zu verstehen.
1	bad	Trotz großer Anstrengung kann man sich nicht verständigen.

VoIP Codecs

- Wandeln die analoge Sprache in digitale Signale um und umgekehrt
- VoIP meistbenutzten Codecs für Sprache (inkl. Kompression)

G711 -> 64 kbps
G729 -> 8 kbps
G723.1 -> 6.4 kbps

- Alle beinhalten Echo-Unterdrückung

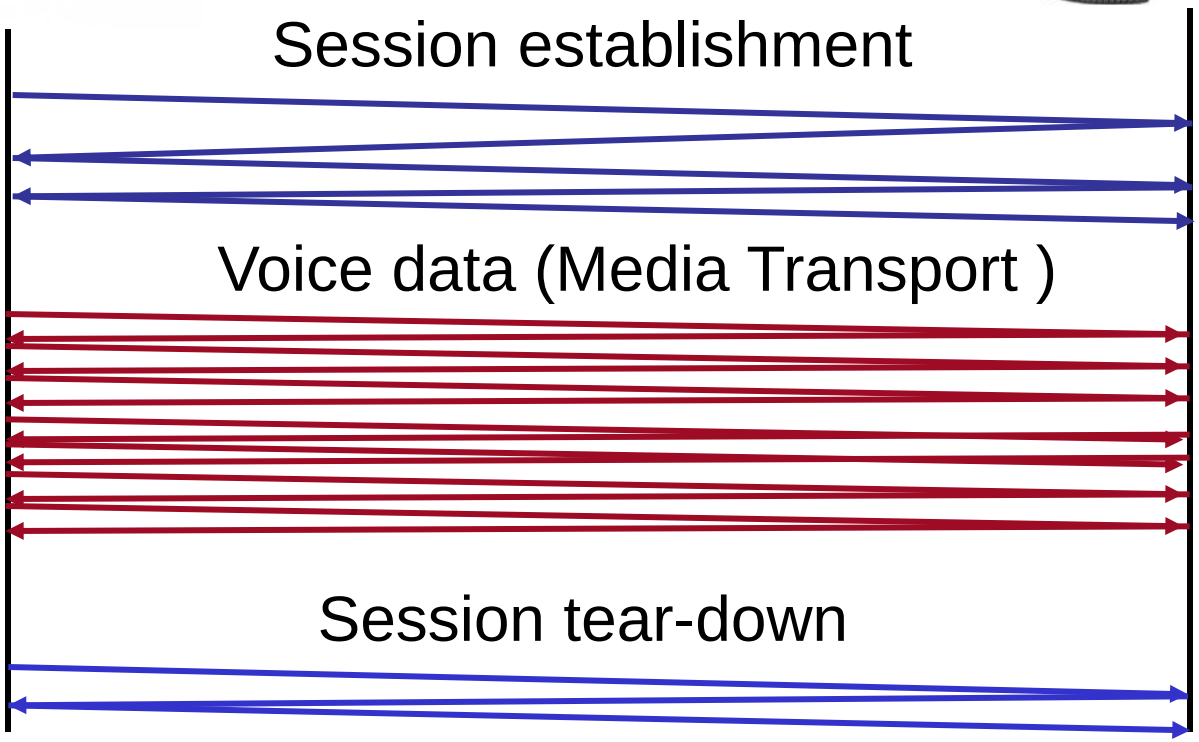


Benötigte Protokolle

- **Signalisierungs-Protokolle um Anwesenheit von Nutzer zu erkennen, sie zufinden, Anrufe auf-, um- und abzubauen**
  - **ITU-T H.323 umbrella standard**
  - **IETF SIP**
    - Angelehnt and HTTP and SMTP
- **Media Transport Protokolle und die Audio/Video-Ströme in Paketform zu übertragen**
  - **RTP (Real Time Protocol) wird von allen offenen Standards genutzt**
- **Weitere Protokolle für**
  - **Gateway Location**
  - **QoS**
  - **Interdomain AAA (Authentication, Authorization and Accounting)**
  - **etc.**

Signalisierungsprotokolle
Prinzipiell: Anrufen mit VoIP

Endpunkte müssen die die IP-Adresse des Gegenübers finden

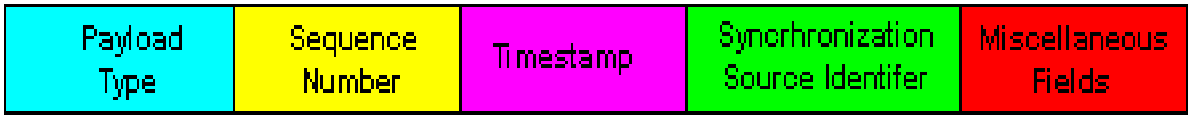


Media Transport Protokolle - RTP

- **Definiert in RFC 1889**
- **Für Video und Audio-Streaming**
- **RTP kann als Sublayer des Transport Layers gesehen werden**
- **Üblicherweise auf UDP**
  - **8-Byte Header**
    - klein = schnell
  - **Kein Setup-Overhead wie z.B. in TCP**
  - **Kein Verbindungsaufbau**
    - Aufgabe z.B. des Signalisierungs-Protokolls

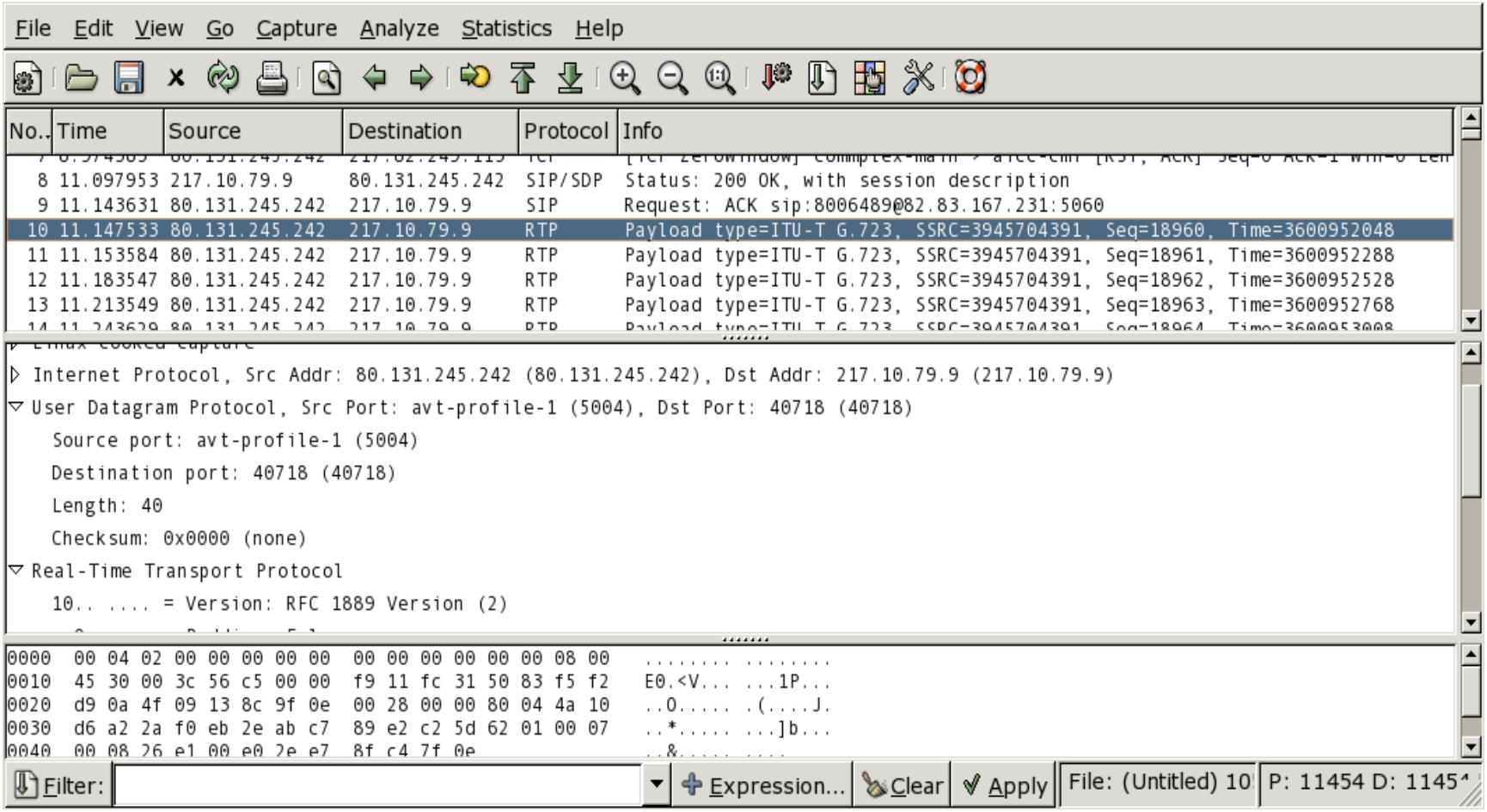
RTP Paket Header

- **Payload type (7 bits)**
  - the type of audio/video encoding
- **Sequence number (16 bits)**
- **Time stamp (32 bits)**
  - Zur Jitter Entfernung
  - abgeleitet von der Sampling Clock des Senders
- **Synchronization Source Identifier (SSRC) (32 bits): Quelle des RTP Stroms**
  - Random Stream-Number
  - Nicht IP-Adress des Senders



RTP Header

RTP: Beispiel im Wireshark



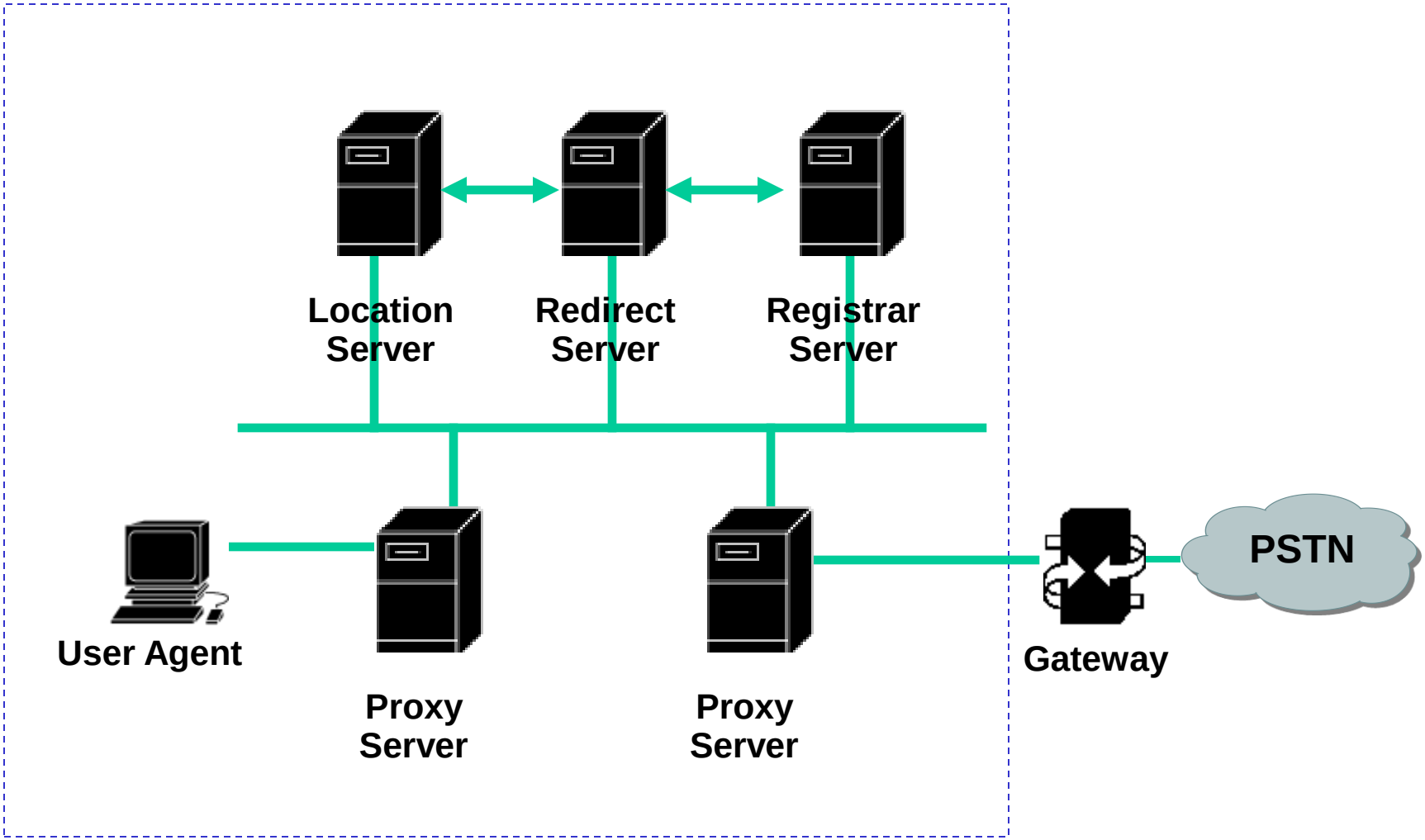
RTCP (RTP Control Protocol)

- RTCP Pakete werden periodisch zwischen Sender and Empfänger ausgetauscht
- Zur Ermittlung der Statistik:
  - Anzahl der gesendeten Pakete
  - Anzahl der verlorenen Pakete
  - Jitter
- RTP und RTCP Pakete laufen über unterschiedliche Ports

QoS-Anforderungen an VoIP

- **Bandbreite**
  - **Anhängig vom Codec**
  - **Vergleich**
    - PSTN: 1.5 Mbps mit 64kpbs pro Kanal: 24 simultane Anrufe
    - VoIP: 1 Mbps mit G.729 codec (8kpbs) 128 simultane Anrufe
- **Latenz**
  - **RTT von 150-250 ms möglich, besser kleiner**
- **Jitter**
  - **Akzeptabel: 75 msec, besser kleiner**
- **Paketverlustrate**
  - **Laut Anbieter: max. 2-3%**

Signalisierungs-Protokolle:
SIP – Architektur und Komponenten



User Agents

- **Eine Einheit, die Anrufe initiiert, empfängt und beendet**
  - **User Agent Clients (UAC)**
    - initiiert Anrufe
  - **User Agent Server (UAS)**
    - empfängt Anrufe
- **UAC und UAS können Anrufe beenden**

Proxy Server

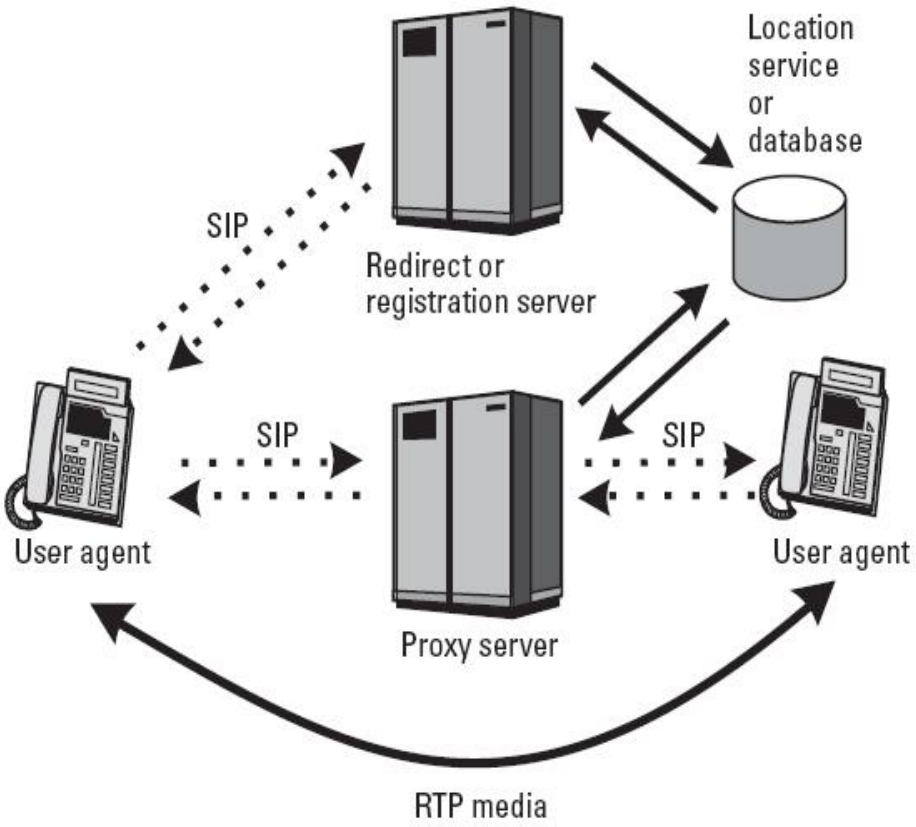
- Ein zwischengelagerter Server, der sowohl als Server als auch als Client Anfragen im Auftrage anderer bearbeiten kann.
- Anfragen werden intern bearbeitet oder indem sie – möglicherweise nach einer änderung der Adresse an andere Server weitergeleitet werden.
- Kann SIP-Nachrichten interpretieren, umschreiben oder übersetzten bevor er sie weiterleitet

Redirect Server

- Ein Server, der eine SIP Anfrage annimt und die Adresse auf keine, eine oder mehrere neue Adressen abbildet und diese an den Clinet zurücksendet
- Anders als ein Proxy Server, initiiert der Redirect Server keine eigenen Requests
- Anders als ein User Agent Server, kann der Redirect Server keine Anrufe annehmen oder beenden.

Registrar Server

- Ein Server, der REGISTER Anforderungen empfängt
- Ein Registrar Server kann eine Authentifizierung verlangen
- Ein Registrar Server ist typischerweise co-located mit einem Proxy oder einem Redirect Server



SIP Nachrichen – Methoden und Antworten

- **SIP Methods:**
  - INVITE – Initiates a call by inviting user to participate in session.
  - ACK - Confirms that the client has received a final response to an INVITE request.
  - BYE - Indicates termination of the call.
  - CANCEL - Cancels a pending request.
  - REGISTER – Registers the user agent.
  - OPTIONS – Used to query the capabilities of a server.
  - INFO – Used to carry out-of-bound information, such as DTMF digits.

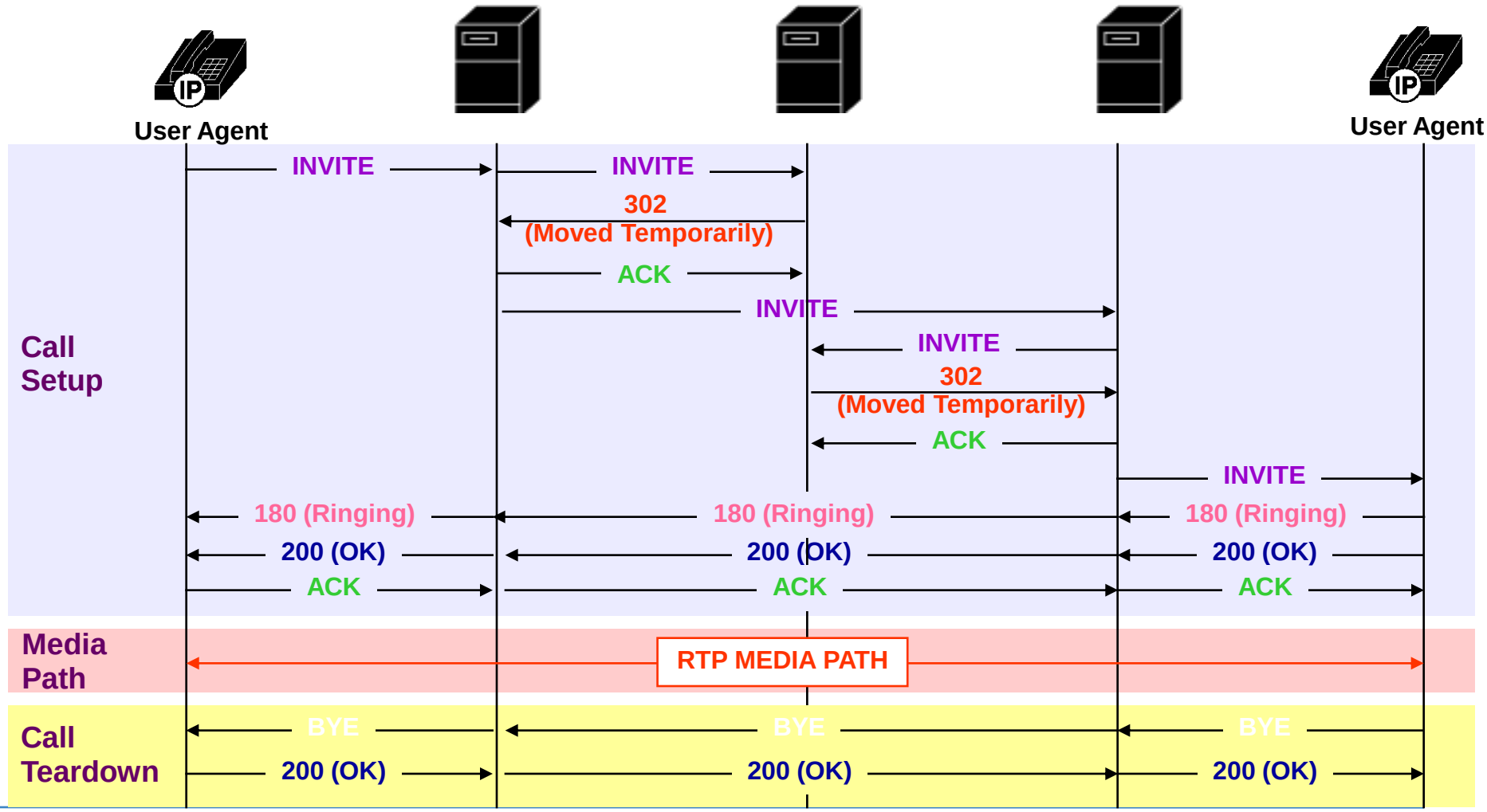
- **SIP Responses:**
  - 1xx - Informational Messages.
  - 2xx - Successful Responses.
  - 3xx - Redirection Responses.
  - 4xx - Request Failure Responses.
  - 5xx - Server Failure Responses.
  - 6xx - Global Failures Responses.

SIP Headers

- Ähnliche Syntax und Semantik zu HTTP
- Beispiel

```
-----------------------------------------------------------------
                        SIP Header
-----------------------------------------------------------------
INVITE sip:5120@192.168.36.180 SIP/2.0
Via: SIP/2.0/UDP 192.168.6.21:5060
From: sip:5121@192.168.6.21
To: <sip:5120@192.168.36.180>
Call-ID: c2943000-e0563-2a1ce-2e323931@192.168.6.21
CSeq: 100 INVITE
Expires: 180
User-Agent: Cisco IP Phone/ Rev. 1/ SIP enabled
Accept: application/sdp
Contact: sip:5121@192.168.6.21:5060
Content-Type: application/sdp
```

SIP: Auf- und Abbbau einer Verbindung



Typisches Problem bei der SIP/VoIP-Telefonie (zu Hause)

- **NAT und Firewalls**
  - **SIP Nachrichten enthalten IP-Adressen im Datenteil**
  - **Interne Adressen sind von außen nicht sichtbar**
  - **RTP benutzt keine festen Layer 4 Portnummern**
    - Variabel im Bereich von 1024 – 65534
  - → **A ruft B an, B bekommt SIP-Nachrichten von A, aber nicht umgekehrt**
  - → **RTP wird gar nicht zugestellt ☹**

- **Das Problem kann mittels SIP/RTP-Proxy auf dem NAT-Router behoben werden**
  - **Der Proxy korrigiert die SIP-Packete, und leitet die RTP-Packete über sich selbst zum jeweiligen Gesprächspartner**

Warum ist VoIP-Security ein Thema?

- Durch den Einsatz von IP-Netzwerken sinken die Angriffshürden
  - Offenes Netzwerk
  - Erreichbare Server und Endgeräte
  - Gängige Multi-Purpose-Betriebssysteme
  - Verfügbare Tools

- VoIP hat anderen Schutzbedarf
  - als herkömmliche Telefonie
  - als die restlichen Netzwerkanwendungen

Vergleich mit klassischer Telefonie

- **VoIP-Sicherheitsmechanismen theoretisch besser als bei klassischerTelefonie**
- **Aber:**
  - **Mangelnde Umsetzung**
  - **Offene Infrastruktur**
    - Werkzeuge, Wissen und Zugänge verfügbar
  - **Integrierte Sprach-, Signalisierungs-, und Management-Ebene**
  - **Konvergenz**
    - bei Endgeräten, Infrastruktur-Komponenten, Betriebssystemen, Anwendungen
  - **Minimale Verbindungskosten**

Technische Sicherheitsmaßnahmen für VoIP

- **Maßnahmen in der Netzwerkschicht**
  - Trennung von Sprach- und Datennetz
  - Schutz vor unbefugtem Netzwerkzugang
  - Schutz vor Umleitung von Nachrichten
  - Multi-Port-Switch auf VoIP-Phones deaktivieren
  - Schutz gegen DoS-Attacken

- **Maßnahmen in der Anwendungsschicht**
  - Authentifikation und Verschlüsselung der Signalisierung
  - Verschlüsselung der Sprachdaten
  - Authentifizierte und verschlüsselte Management-Zugänge
  - Überwachte Registrierung der Endgeräte
  - Eingeschränkte Nutzung von Soft-Phones

Maßnahmen in der Anwendungsschicht (1)
Signalisierungsebene

- **Authentifizierung und Verschlüsselung der SIP-Signalisierung**
  - **Schutz gegen z.B. Caller-ID Spoofing, unautorisierte Nutzung, MitM-Attacks**
  - **Signalisierungssicherheit ohne Sprachdatensicherheit weitestgehend überflüssig**

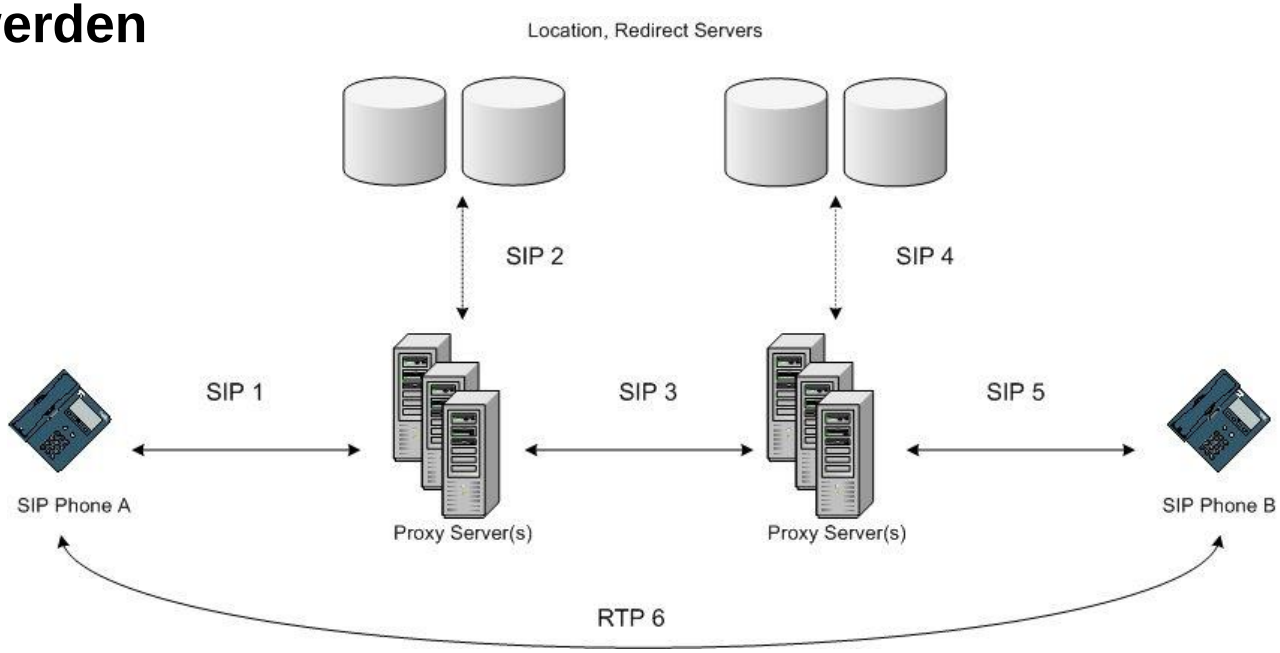
- **Maßnahmen**
  - **Mittels TLS-gesicherten Verbindungen oder S/MIME (nicht verbreitet)**
    - „SIPS“: Sip over TLS, Problem: Sicherheit nur für 1. Hop
    - S/MIME: Sicherung durch PKI, Zertifikatsverteilung aufwändig, Probleme: Proxies können SIP-Nachrichten nicht umschreiben
  - **Verzicht im vollständig geschlossenen Netz akzeptabel (siehe PSTN)**
    - Gesichert durch Maßnahmen auf der Netzwerkschicht (s.o.)

Maßnahmen in der Anwendungsschicht (2)
Datenebene

- **Verschlüsselung der Sprachdaten**
  - **Schutz gegen Abhören, Mitschneiden, Manipulation**
  - **Standard ist SRTP**
  - **Verzicht im vollständig geschlossenen Netz akzeptabel (siehe PSTN)**
    - Gesichert durch Maßnahmen auf der Netzwerkschicht (s.o.)
  - **Mandatorisch, falls die VoIP-Telefonie auf unsichere Netze ausgeweitet werden sollte**
  - **Sicherheit des Schlüsselaustausches (meistens Signalisierungs-ebene) erforderlich**

Verschlüsselung der Sprachdaten

- **SRTP**
  - **RTP Profil, sehr geringer Overhead**
  - **AES-128 Verschlüsselung**
  - **Schlüssel muss in den verschlüsselten SIP-Nachrichten übertragen werden**



Alternative:
Verschlüsselung NUR der Sprachdaten

- **ZRTP (Phil Zimmermann‘s RTP)**
  - **Diffie-Hellman Schlüsselaustausch für SRTP**
    - siehe auch: http://www.youtube.com/watch?v=YEBfamv-_do
    - gemeinsamer sym. Schlüssel
    - Aber: Man in the Middle?
  - **Schlüssel-Hash wird via Spache in der Session geprüft und autentifiziert**
    - Nachfolgende Sessions mit dem gleichen Partner nutzen den vorherigen Schlüssel
  - **Implementiert in “Zfone”**
    - Implementiert direkt in der RTP-Verbindung
    - Keine Änderung an SIP