



Session Initiation Protocol (SIP)

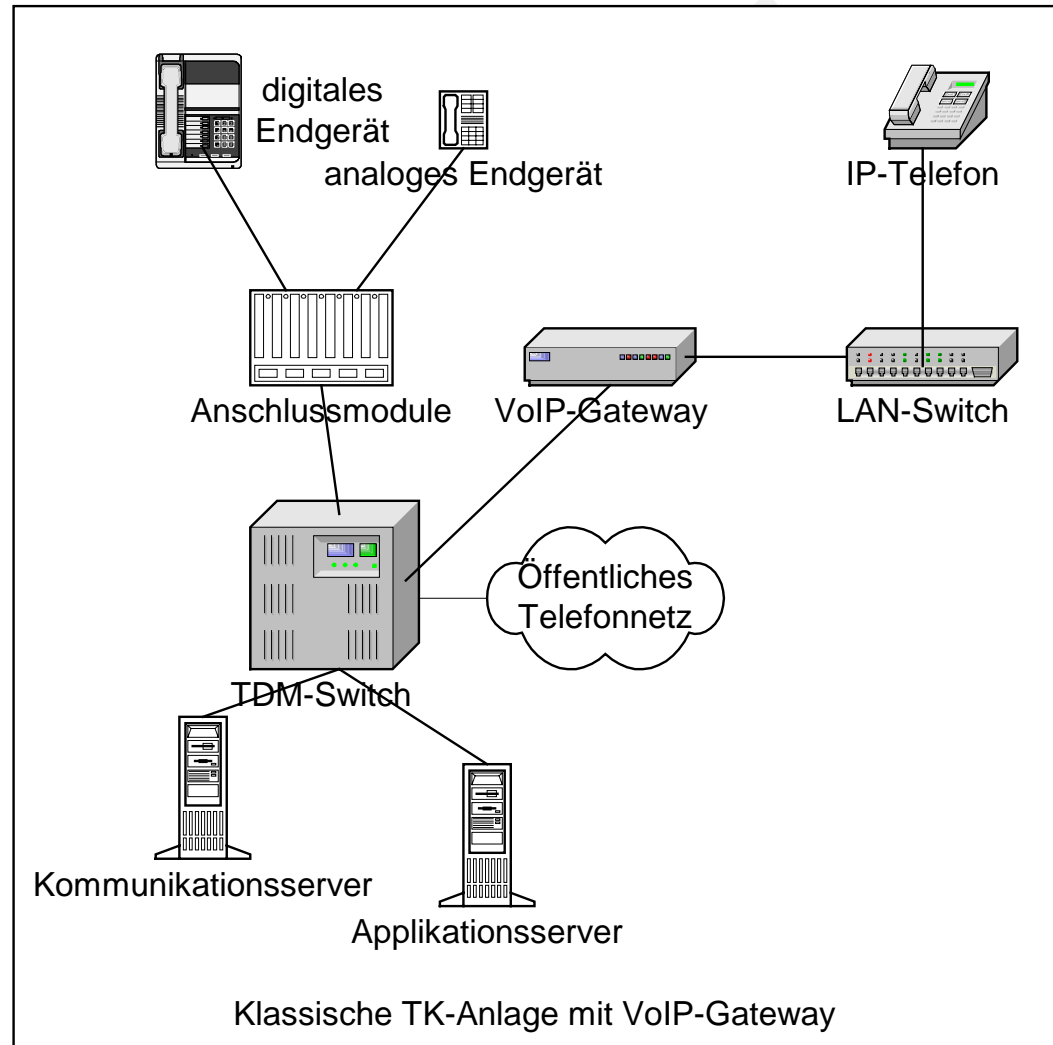
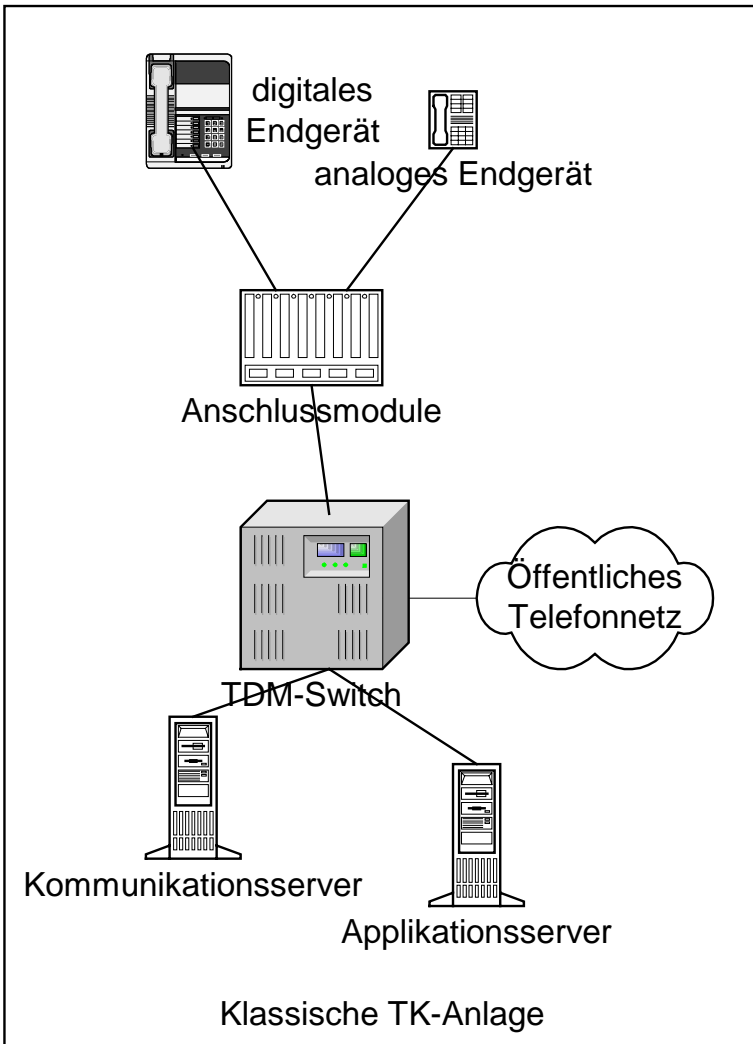
Dr.-Ing. Behrooz Moayeri

ComConsult Beratung und Planung GmbH, Pascalstraße 27,
D-52076 Aachen, Tel.: (02408) 951-09, Fax: (02408) 951-109

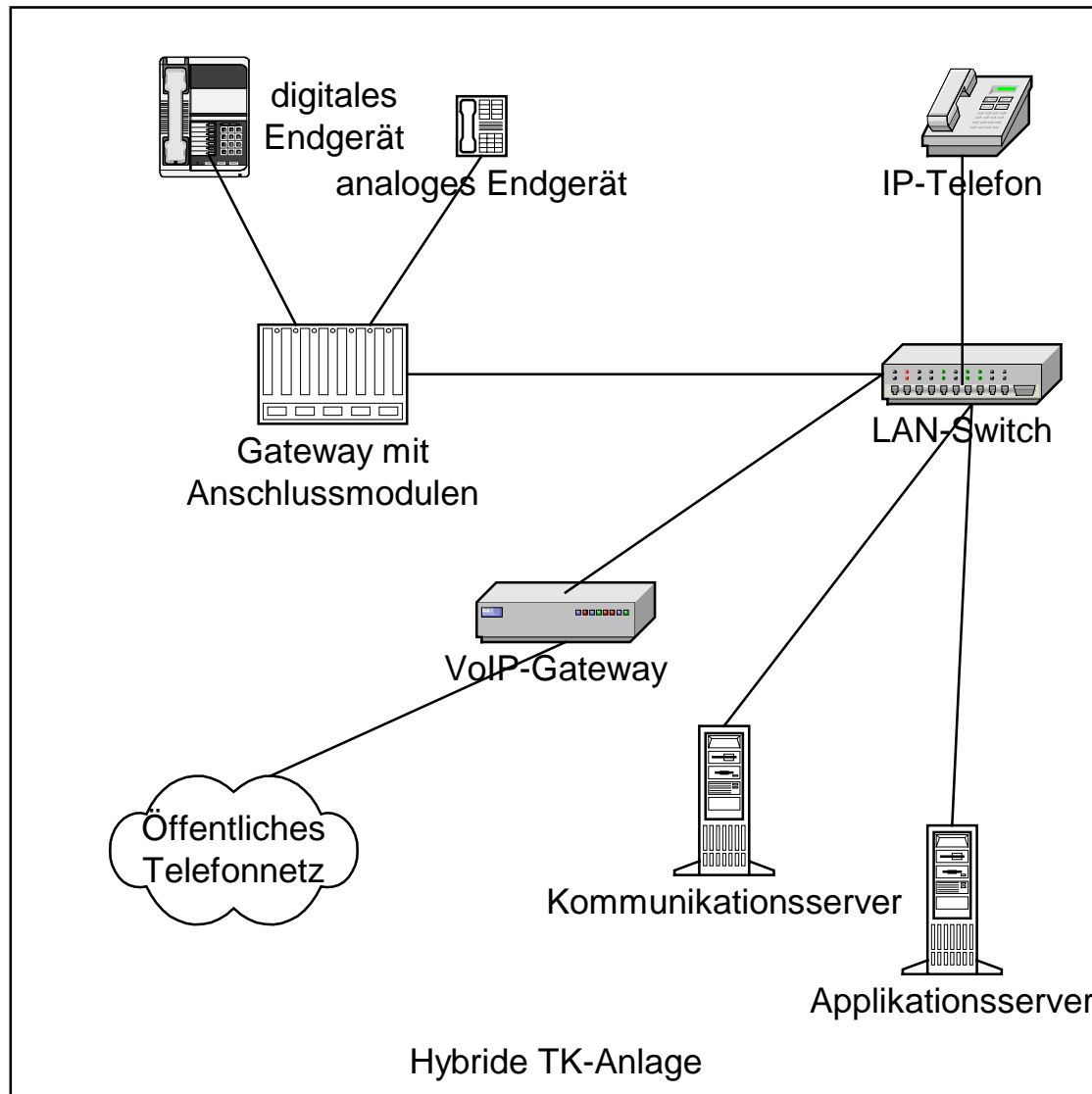
E-Mail: moayeri@comconsult.com

Web: <http://www.comconsult.com>

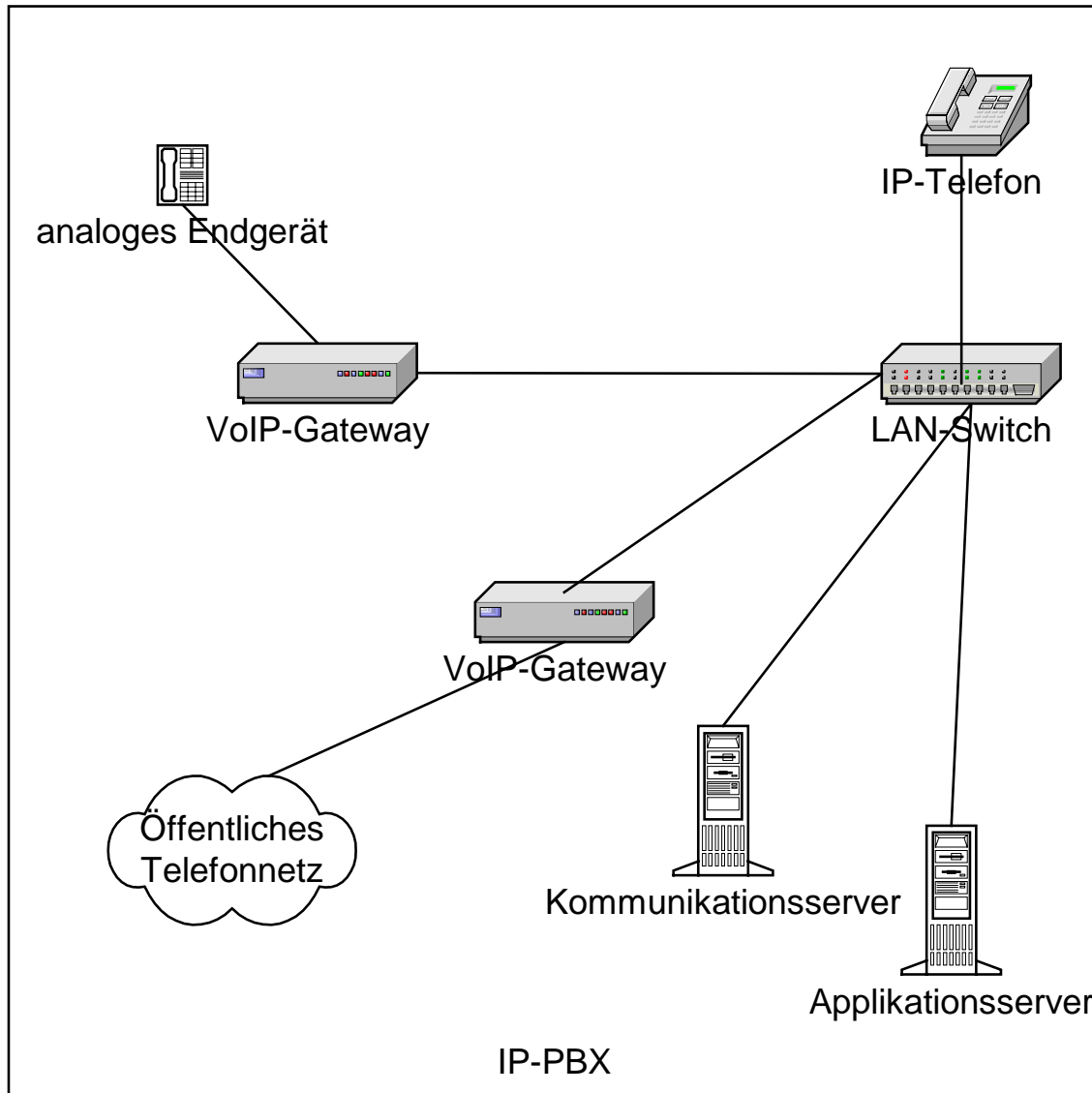
Varianten einer klassischen TK-Anlage



Hybride TK-Anlage



IP-PBX-System



Was rechtfertigt die Migration?

- **Kostensenkung**
 - kann nur punktuell die Motivation sein
 - Migration kann auch zur Kostensteigerung führen
- **Neue Applikationen**
 - Integration von Daten- und Sprachanwendungen
- **Optimierung für Netzbetreiber**
 - Trennung der Infrastruktur von den Applikationen
 - Weg von dem Einsatz „jeder Applikation ihre eigene Infrastruktur“
- **Analogie zum Internet:**
 - Content Provider
 - Infrastruktur-Provider

Zielsetzung und Vorteile

- Zielsetzung ist nicht die Restrukturierung des bestehenden Public Switched Telephone Systeme (PSTN), sondern es entsteht etwas Neues
- SIP entwickelt ein HTTP-ähnliches Modell
- Vorteile dieses Modells:
 - Provider sind global verteilt und frei wählbar
 - Das ganze System ist programmierbar, auch vom Benutzer
 - Fazit: Mehr Möglichkeiten für den Benutzer
 - Neue Applikationen
 - ✘ Verteilte Spiele
 - ✘ Virtual reality
 - ✘ Links in E-Mails
 - ✘ Interactive Voice Response (IVR) in Web-Seiten
 - ✘ Click-to-dial
 - ✘ Verzeichnisdienste
 - ✘ Videokonferenzen
 - ✘ Instant Messaging (Voice Mail, Börsenticker, Rückruf etc.)
 - ✘ Kalender (z. B. voreingestellte Konferenzen)
 - ✘ Unified Messaging (z. B. Voice Mail to E-Mail)
 - ✘ etc.



IP-Modell

- Trennung der Applikationen von der Infrastruktur
- Jeder Benutzer kann auf Applikationen jedes anderen Providers zugreifen
- Jeder mit IP Connectivity kann Provider für Applikationen werden
- Der Markt ist völlig offen
- Nutzung mehrerer Provider möglich:
 - IP-Infrastruktur bei Provider A
 - SIP Signaling bei Provider B
 - PSTN-Gateway bei Provider C
 - Least Cost PSTN Routing bei Provider D
- Es gibt bereits Sites, die nur Signaling anbieten (z. B. iptel.org)
- Proprietäre Software wird auf dem PC installiert, der Zugang zum Internet hat
- IP Phone auf dem PC wird benötigt



Weitere Eigenschaften des IP-Modells

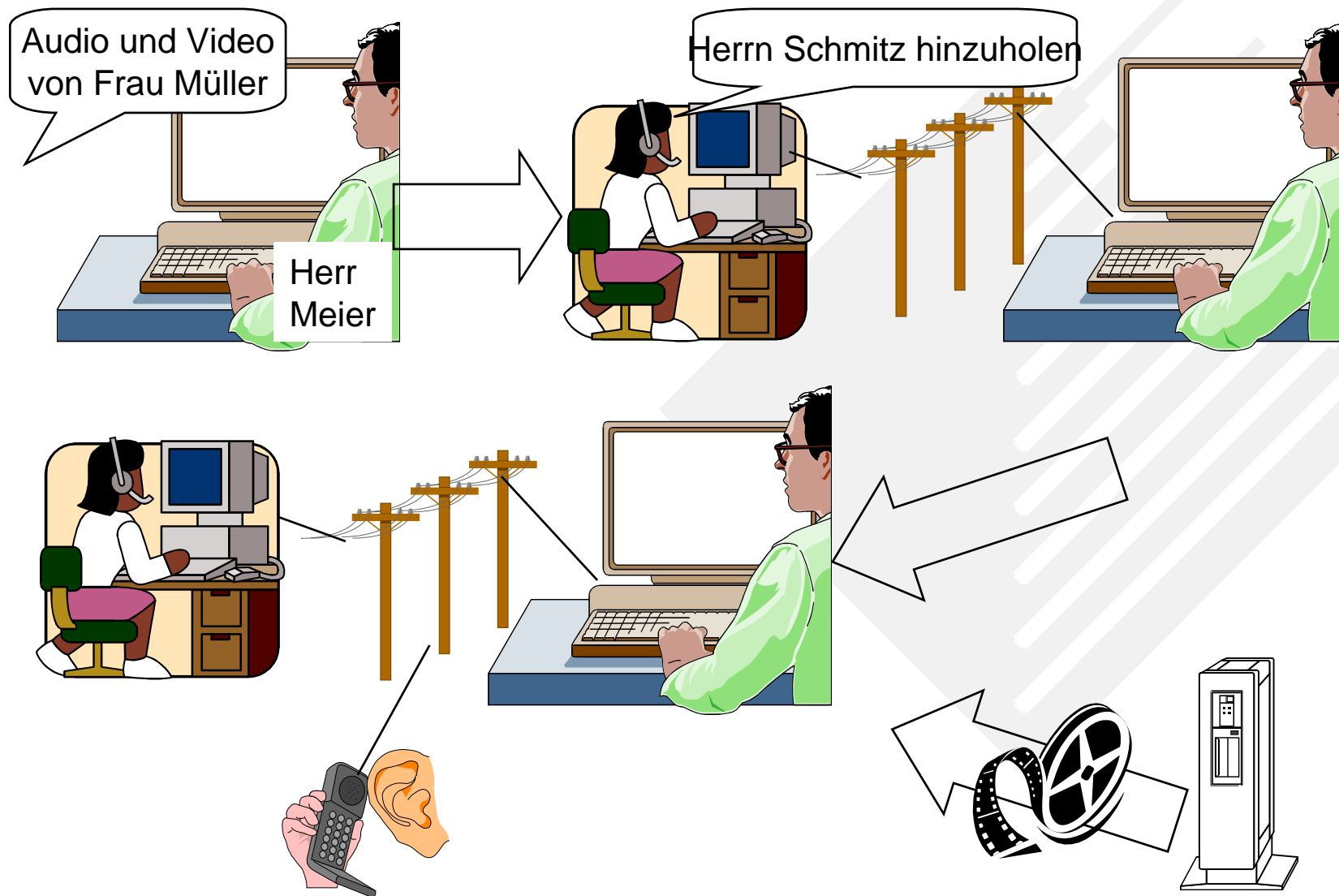
- Verteiltes Ende-zu-Ende-Design
- Intelligenz und Status der Verbindungen residiert in den Endgeräten
- Netzinfrastruktur umfasst minimale Intelligenz, bis auf Routing fast keine Intelligenz und keine Speicherung des Status von Verbindungen
- Endgeräte kommunizieren miteinander im Rahmen von beliebigen Applikationen, auf die die Infrastruktur fast keinen Einfluss hat (Ausnahmen wie Network Address Translation – NAT – bestätigen die Regel)
- Vorteile des Modells:
 - Flexibilität: Neue Applikationen können leicht eingeführt werden
 - Robustheit: Geringe Intelligenz der Infrastruktur führt zum robusteren System
 - Skalierbarkeit: Das Netz führt keine Tabellen über den Status der Verbindungen und kann durch einfache Erhöhung der Routing- und Switching-Leistung skalieren
- Kiss: Keep it simple and stupid



Warum ist die Trennung der Services von der Infrastruktur günstig?

- Neue Services können entwickelt werden, ohne die Infrastruktur zu ändern
- Fehler in der Service-Programmierung führt zu keiner Beeinträchtigung der Infrastruktur
- Services können auf der Basis von herkömmlichen Rechnern programmiert werden
- Erfahrungen aus dem Betrieb der IN-Dienste (Intelligent Network Services) bestätigen:
 - Sprachapplikationen müssen von der Infrastruktur getrennt werden
 - Bei Circuit Switching ist dies nicht vollständig gelungen
- Absehbar: auch Hersteller werden sich spezialisieren:
 - einige auf Infrastruktur
 - einige andere auf Services

Neue Applikationswelt: Beispielszenario



Kommunikation ist mehr als Signalübertragung

- Herr Meier arbeitet an seinem PC
- Der PC meldet einen Anruf von Frau Müller
- Herr Meier akzeptiert den Anruf, und die beiden kommunizieren
- Frau Müller fällt ein, dass auch Herr Schmitz einzuschalten ist
- Sie sagt: „Schmitz anrufen“
- Spracherkennung am PC setzt den Befehl um
- Client-Applikation greift auf Internet-Verzeichnis zu
- Schmitz@comconsult.com wird angerufen
- Der Verbindungsaufbau-Request erreicht den persönlichen Agenten von Herrn Schmitz
- Der Agent ist so eingestellt, dass Mobiltelefon, Heimtelefon und PC am Arbeitsplatz gleichzeitig klingeln



Mehrpunkt-Kommunikation

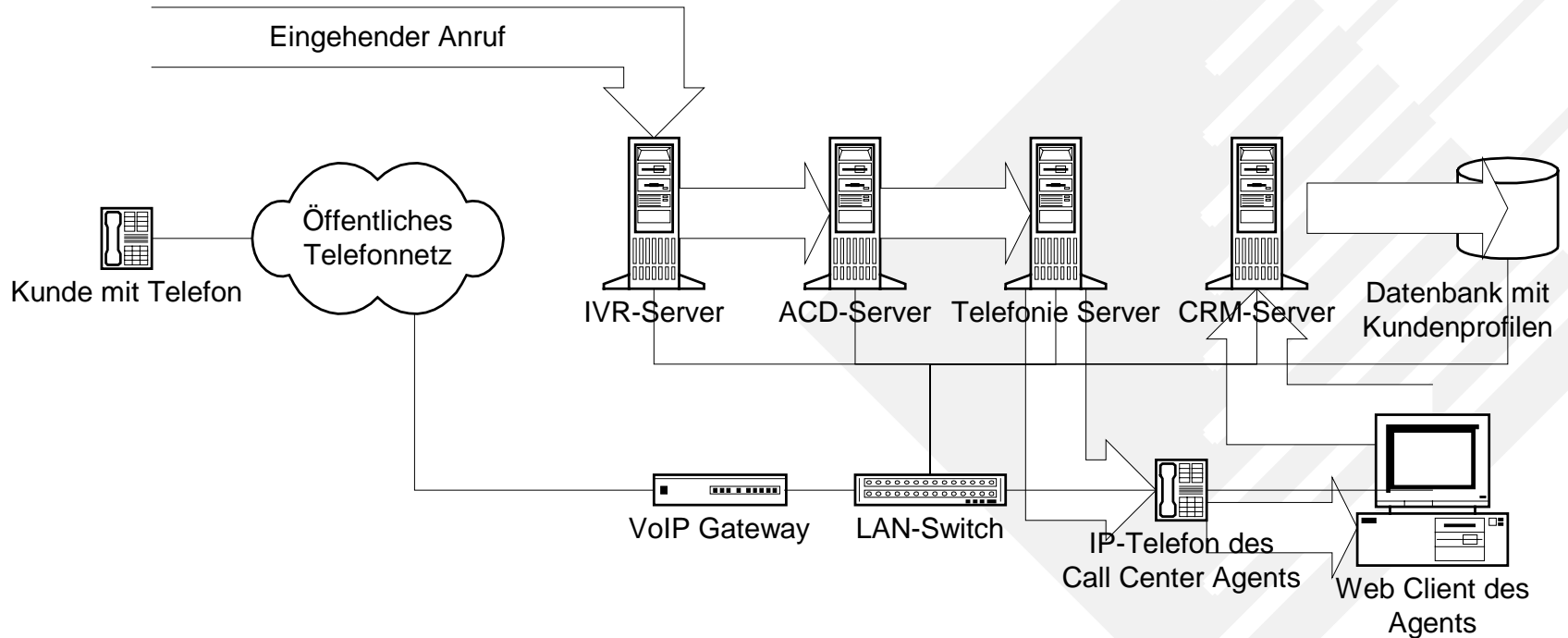
- Herr Schmitz hat den Agenten so eingestellt, dass der billigste Gateway mit Kreditkartenabrechnung benutzt wird, um das Mobiltelefon zu erreichen
- Agent findet den Gateway
- Der Anruf erreicht Herrn Schmitz im Auto
- Herr Schmitz schließt sich der Konferenz an, allerdings nur mit Sprache
- Herrn Meier fällt ein, dass eine Videodatei von der letzten Besprechung zu laden ist
- Vom Videosever wird der Inhalt abgespielt
- Frau Müller greift auf eine Web-Seite mit wichtigen Informationen zu; Textversion erscheint auf dem Telefon-Display von Herrn Schmitz
- Herr Schulze ist nicht erreichbar; Web-Seite mit seinem Terminkalender und Link zur Voice Mail wird von seinem Agenten angezeigt



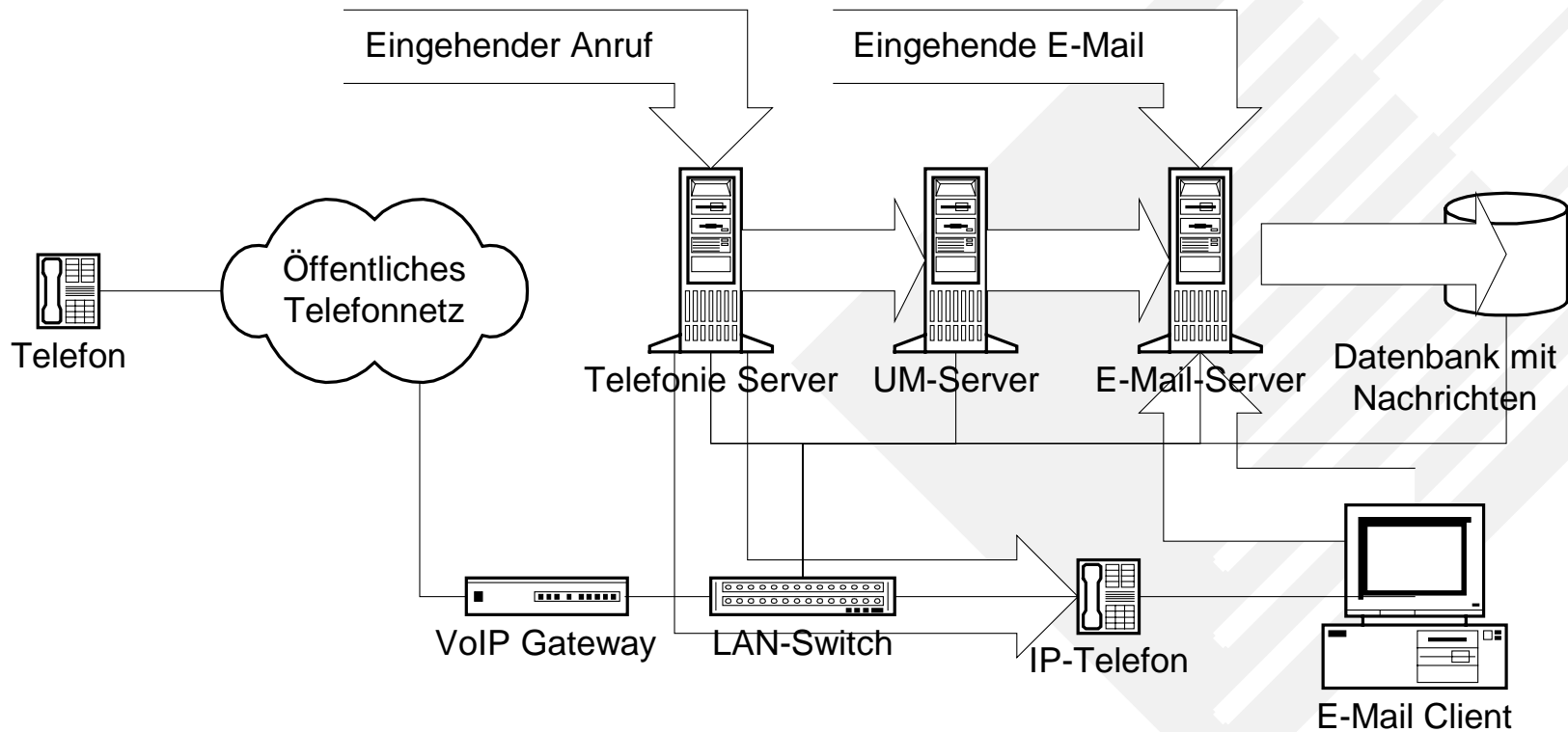
- Moayeri@comconsult.com wird angerufen
- Er befindet sich in einer Besprechung und hat seinen PDA dort an das Internet-Telefon angeschlossen
- Im PDA ist die Priorität von Müller, Meier und Schmitz höher als die aktuelle Besprechung
- Internet-Telefon klingelt
- Wäre die Priorität der aktuellen Besprechung höher, würde der Anruf zur Voice Mail umgeleitet werden
- Neue Applikationswelt: Der Benutzer bestimmt weitgehend das Verhalten des Anwendungen



Denkbares Call-Center-Szenario



Denkbares Unified-Messaging-Szenario



Was alles erforderlich ist

- Signalisierungsprotokoll für Verbindungsauf- und abbau
 - Jahrzehntelange Erfahrungen mündeten in Protokolle wie SS7 und Q.931
- Transportprotokoll für Voice- und Videokommunikation
- Protokoll zum Zugriff auf ein Verzeichnis
- Streaming-Protokoll für Video-Server
- Intelligente Dienste des Agents durch Zusammenspiel mit dem Signalisierungsprotokoll über eine Call Processing Language
- Protokoll zur Lokalisierung des Gateways
- Protokoll zur Kommunikation zwischen Gateways



Einordnung von Protokollen

- Signalisierung: SIP/SDP (Session Description Protocol), H.323
- Transport: RTP (Real-time Transport Protocol), SCTP (Stream Control Transmission Protocol, RFC 2960)
- Zuordnung von Namen zu IP-Adressen: Domain Name System (DNS)
- TRIP: Telephony Routing over IP (Finden und Austausch von Gateway-Routing-Informationen in einem IP-Netz)
- RSVP: Reservierung von Ressourcen
- COPS: Common Open Policy Service (COPS), QoS-Steuerung über Policy
- Diameter: AAA (Authentication, Accounting, Authorization)

Signalisierung				Codec	QoS	
H.323	SIP	RTSP	SIP	RTP	RTCP	RSVP
TCP			UDP			
IPv4, IPv6						
PPP	AAL 3/4	AAL 5	Ethernet	PPP		
SDH	ATM			V.34 etc.		

Zwei Modelle für die Verteilung der Intelligenz

- Peer-to-Peer-Protokolle wie
 - H.323 von der International Telecommunications Union (ITU)
 - SIP (Session Initiation Protocol) von der Internet Engineering Task Force (IETF)
- Master-slave-Protokolle wie
 - MGCP (Media Gateway Control Protocol) von der IETF
 - Megaco/H.248 von der IETF und ITU
- Es ist nicht sinnvoll, z. B. SIP und MGCP als Alternativen gegenüberzustellen
- Es wäre jedoch denkbar zu entscheiden, eine Integrated Access Device (IAD), der ein analoges Telefon mit einem IP-Netz verbindet, entweder mit SIP oder mit MGCP anzusteuern
- Der Unterschied würde in diesem Fall darin liegen, wie viel Intelligenz in der IAD residiert
 - SIP- oder H.323-Modell: intelligente IAD
 - MGCP- oder Megaco/H.248-Modell: relativ „dumme“ IAD

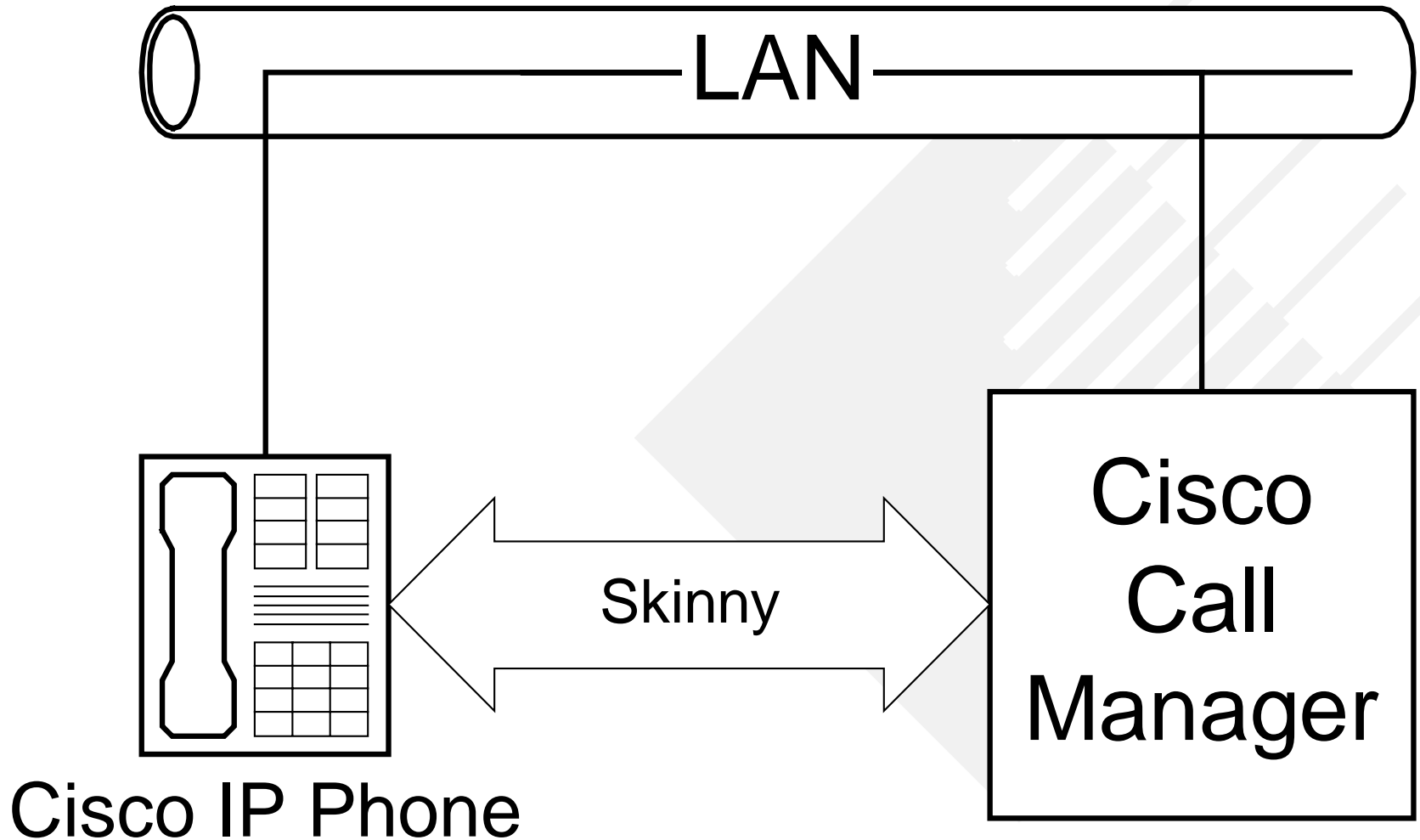


Aufgaben von Signalisierungsprotokollen

- Lokalisierung des Benutzers, da ein Benutzer eventuell über veränderliche oder mehrere IP-Adressen erreichbar ist
- Aufbau der Session
 - Akzeptieren des Anrufs
 - Ablehnen des Anrufs
 - Umleitung des Anrufs zu einer anderen Person, zur Voice Mail, Web Page etc.
- Aushandeln der Session-Merkmale
 - Audio und Video: Kompressionsalgorithmus
 - Festlegung der Ports
- Hinzufügen neuer Teilnehmer; Verlassen der Konferenz
- Im Wesentlichen beschrieben in: H.323 (ITU) bzw. SIP/SDP (IETF)
- Drei Entwicklungsstadien: Vorkommerziell (bis 1995), PC-zentrisch (1995 bis 1998) und Carrier-tauglich (seit 1998)



Beispiel für Master-Slave-Protokolle: Cisco Skinny



SIP ist ein IETF-Standard

- Entwickelt von Internet Engineering Task Force (IETF), einige Arbeitsgruppen der IETF:
 - SIP: Session Initiation Protocol
 - IPTEL: Internet Telephony
 - AVT: Audio Video Transport
 - MIDCOM: Firewall/NAT (Network Address Translation)
 - SIMPLE: SIP for Instant Messaging and Presence Leveraging
 - MMUSIC: Multiparty Multimedia Session Control
 - QoS (Quality of Service): DiffServ, IntServ, RSVP (Resource Reservation Protocol)
 - PSTN legacy: SigTran, Megaco
 - PSTN-IP-Interaktion: PINT, SPIRITS
- Request for Comment (RFC) 2543 beschreibt SIP
- 3gpp (3rd generation partnership project) nutzt SIP für Call Signaling in IP-Netzen
- Man beachte: ITU-T SG 16 beschäftigt sich mit solchen Standards wie H.323/H.248, ETSI Tiphon mit europäischen Belangen

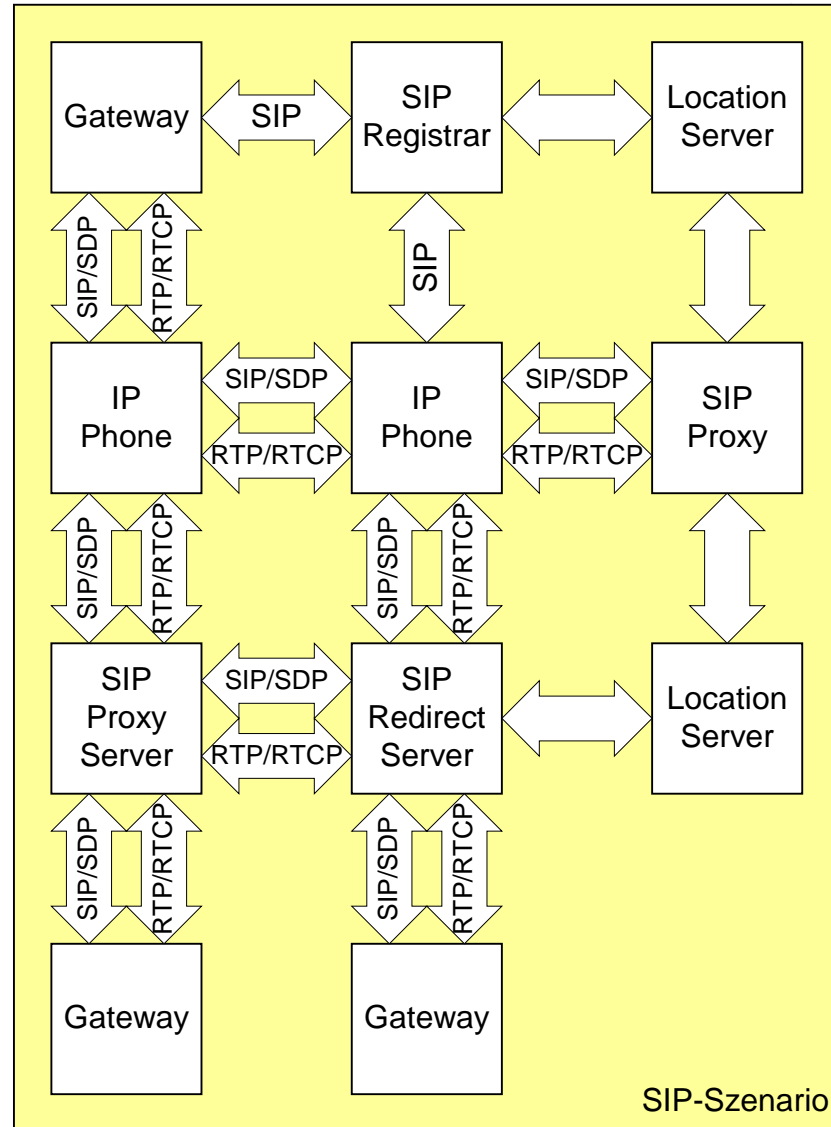
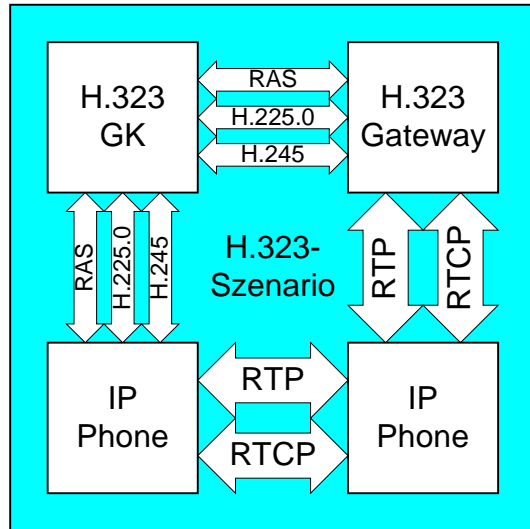


Was ist SIP?

- SIP ist ein Ende-zu-Ende-Client-Server-Signalisierungsprotokoll einschließlich Verbindungsauf- und -abbau und Änderungen zwecks Unterstützung der Lokalisierung von mobilen Benutzern
- Denkbare Einsatzgebiete:
 - Umleitung der Anrufe unbekannter Teilnehmer an das Sekretariat
 - Antwort mit einer Web-Seite, falls nicht erreichbar
 - Senden eines JPEG-Bildes bei Einladungen
- SIP verwendet Textkodierung (wie Telnet)
- Programmierbarkeit als SIP-Ziel
- Nicht auf IP-Telefonie beschränkt
- SIP-Nachricht kann enthalten: Session-Beschreibung, Instant Message, JPEG, MIME
- Applikationen können SIP-Dienste nutzen (Call Processing, User Location, Authentication)



SIP im Vergleich zu H.323



SIP-Komponenten

- UA: User Agent, eingebettet als Software oder Hardware in die Endgeräte, zuständig für
 - UA Client (Initiierung von Calls)
 - UA Server (wartet auf eingehende Anrufe)
- SIP Proxy Server
 - Signaling-Relay (agiert als Client und Server)
 - Nimmt keine Session-Status-Informationen auf, sondern arbeitet im Transaktionsmodus
- SIP Redirect Server: leitet Anrufer zu anderen Servern um
 - Im Gegensatz zum Proxy Server agiert der Redirect Server selbst nicht als Client
- SIP Registrar
 - Akzeptiert Registrierungsanfragen der Benutzer
 - Aktualisiert die Informationen eines Location Servers über die Position der Benutzer (analog zum HLR bei GSM)



SIP-Adressen

- Global erreichbare Adresse für Benutzer (wie E-Mail-Adresse)
- UA-Server melden diese Adresse beim Registrar an (SIP REGISTER)
- UA-Clients verwenden diese Adresse, um Sessions aufzubauen
- Format: URL (Unified Resource Locator) wie z.B.:
 - sip:moayeri@comconsult.com
 - sip:voicemail@comconsult.com?subject=callme
 - sip:sales@hotel.xy;geo.position=48.54_-123.84_120
- Zwingender Bestandteil der Adresse: Hostname
- Optionale Bestandteile: Benutzername, Portnummer, Parameter etc.
- Nicht-SIP-URLs können auch verwendet werden (z.B. mailto: oder http:)
- SIP-Methoden: INVITE, ACK, BYE, CANCEL, OPTIONS, REGISTER
- SIP Response Codes sind HTTP-ähnlich: Nummer, gefolgt von Erklärung

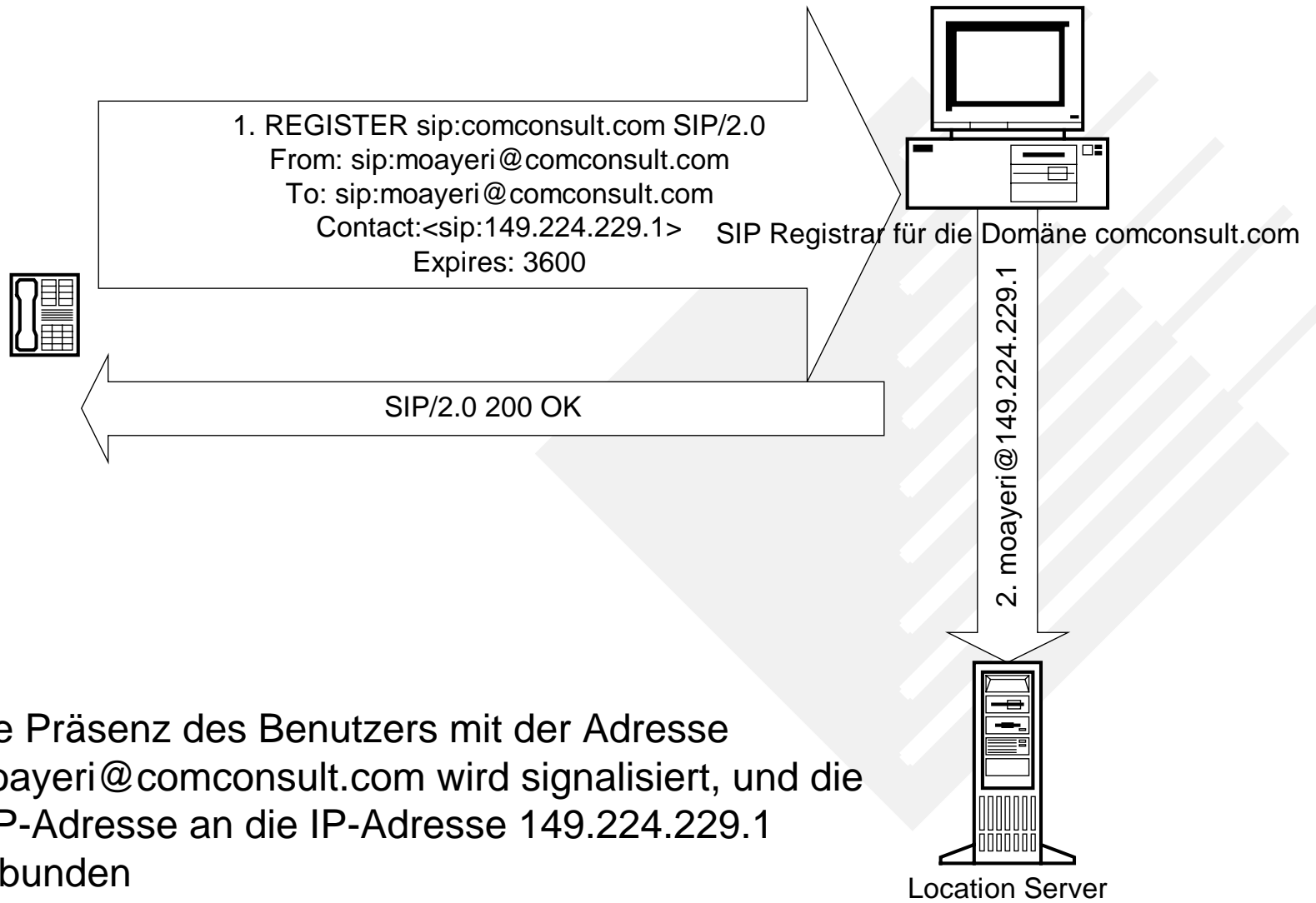


Analogie zu HTTP

- Wenn im Request URI keine Portnummer angegeben ist, wird Port 5060 verwendet
- Wenn im Request URI ein Protokoll (TCP oder UDP) vorgegeben ist, verwendet der Client dieses Protokoll
- Ansonsten versucht der Client, den Request über UDP zu senden
- Wenn die Transaktion über UDP nicht gelingt, versucht der Client eine TCP-basierte Transaktion
- Statt Timeouts sollten ICMP-Meldungen berücksichtigt werden
- Der Host-Teil des URI kann IP-Adresse oder DNS-Name sein



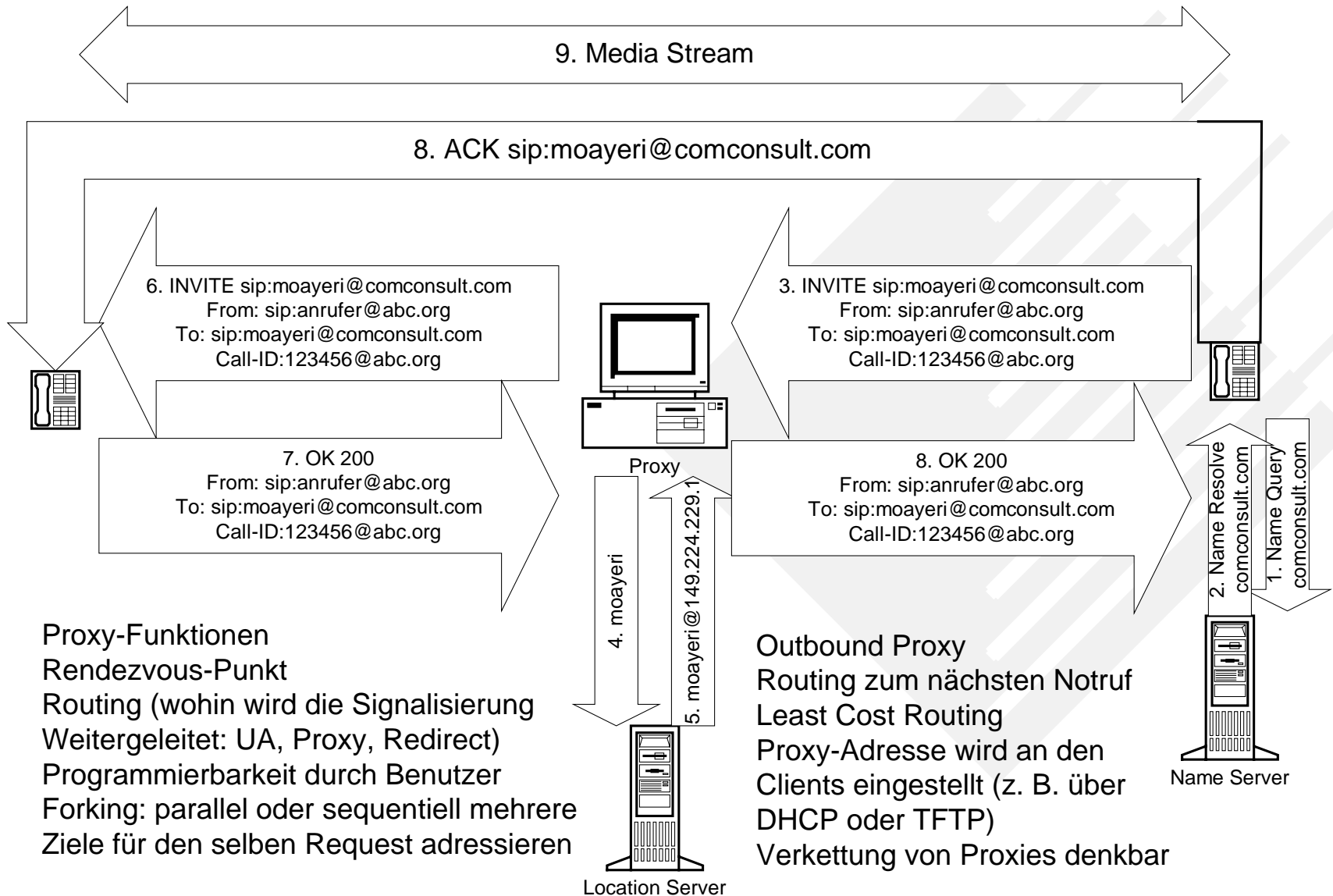
SIP-Registrierung



- Die Präsenz des Benutzers mit der Adresse moayeri@comconsult.com wird signalisiert, und die SIP-Adresse an die IP-Adresse 149.224.229.1 gebunden



SIP Proxy

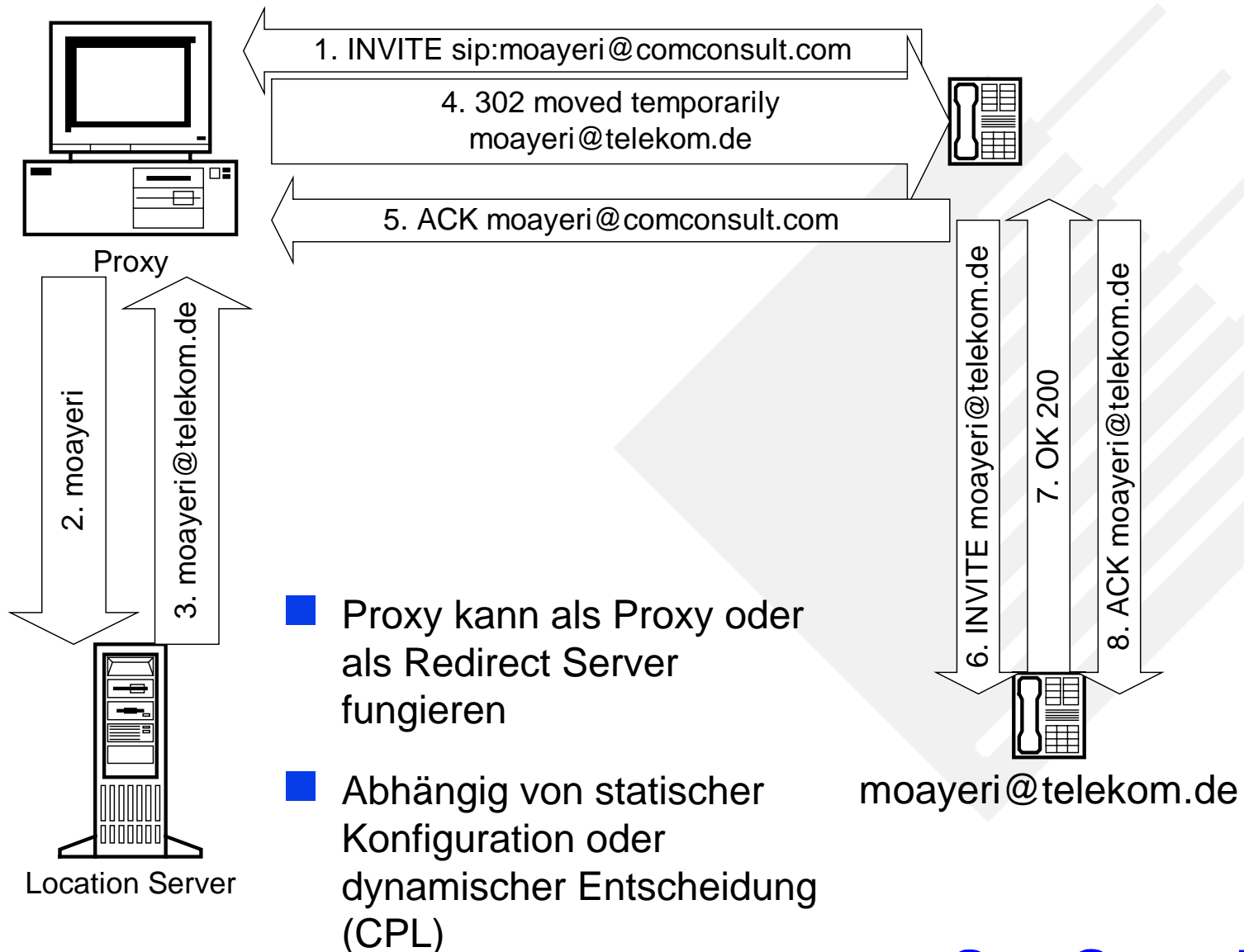


Proxy-Funktionen
 Rendezvous-Punkt
 Routing (wohin wird die Signalisierung Weitergeleitet: UA, Proxy, Redirect)
 Programmierbarkeit durch Benutzer
 Forking: parallel oder sequentiell mehrere Ziele für den selben Request adressieren

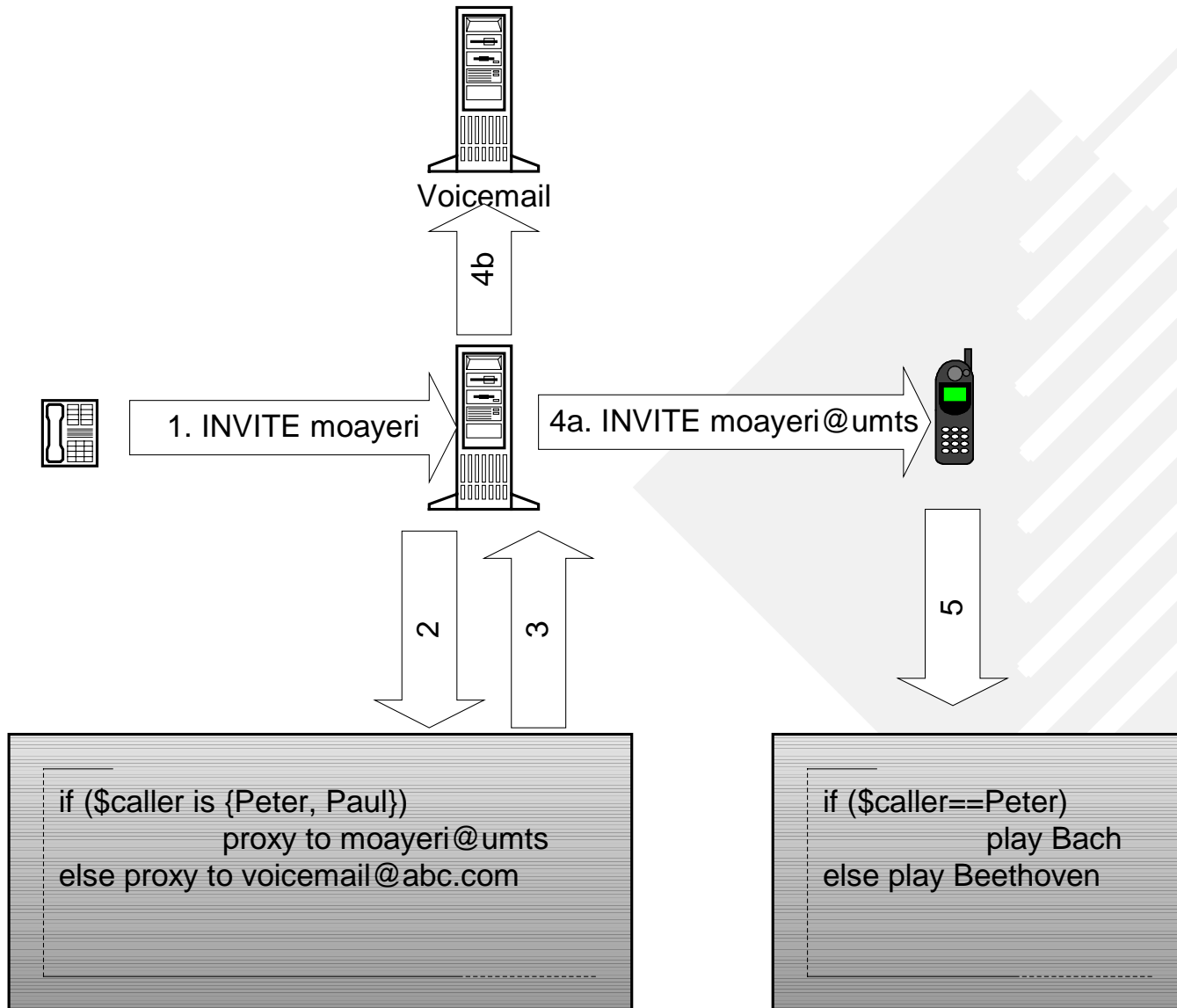
Outbound Proxy
 Routing zum nächsten Notruf
 Least Cost Routing
 Proxy-Adresse wird an den Clients eingestellt (z. B. über DHCP oder TFTP)
 Verkettung von Proxies denkbar



SIP Redirect

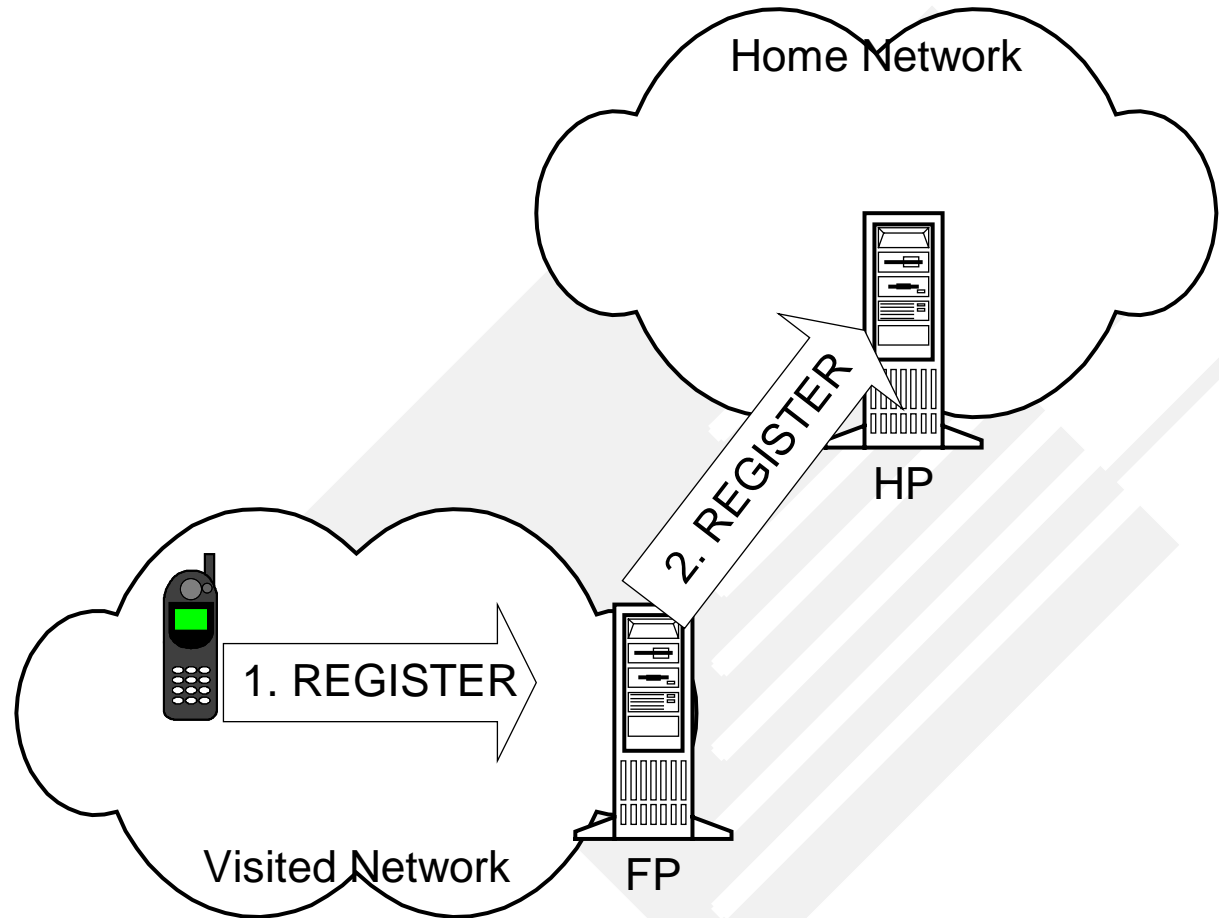


Call Processing Logic (CPL)

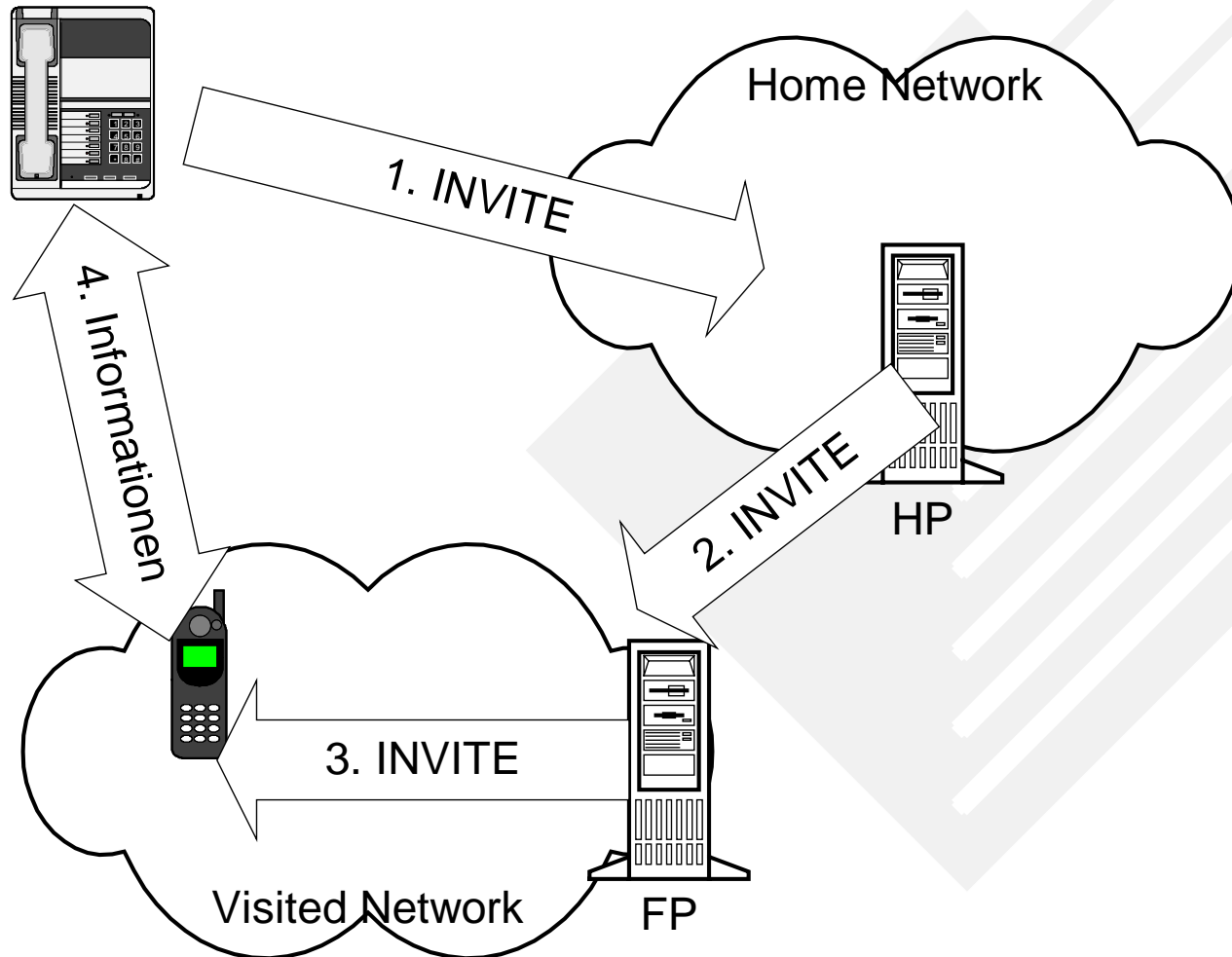


SIP und Mobilität des Endgerätes

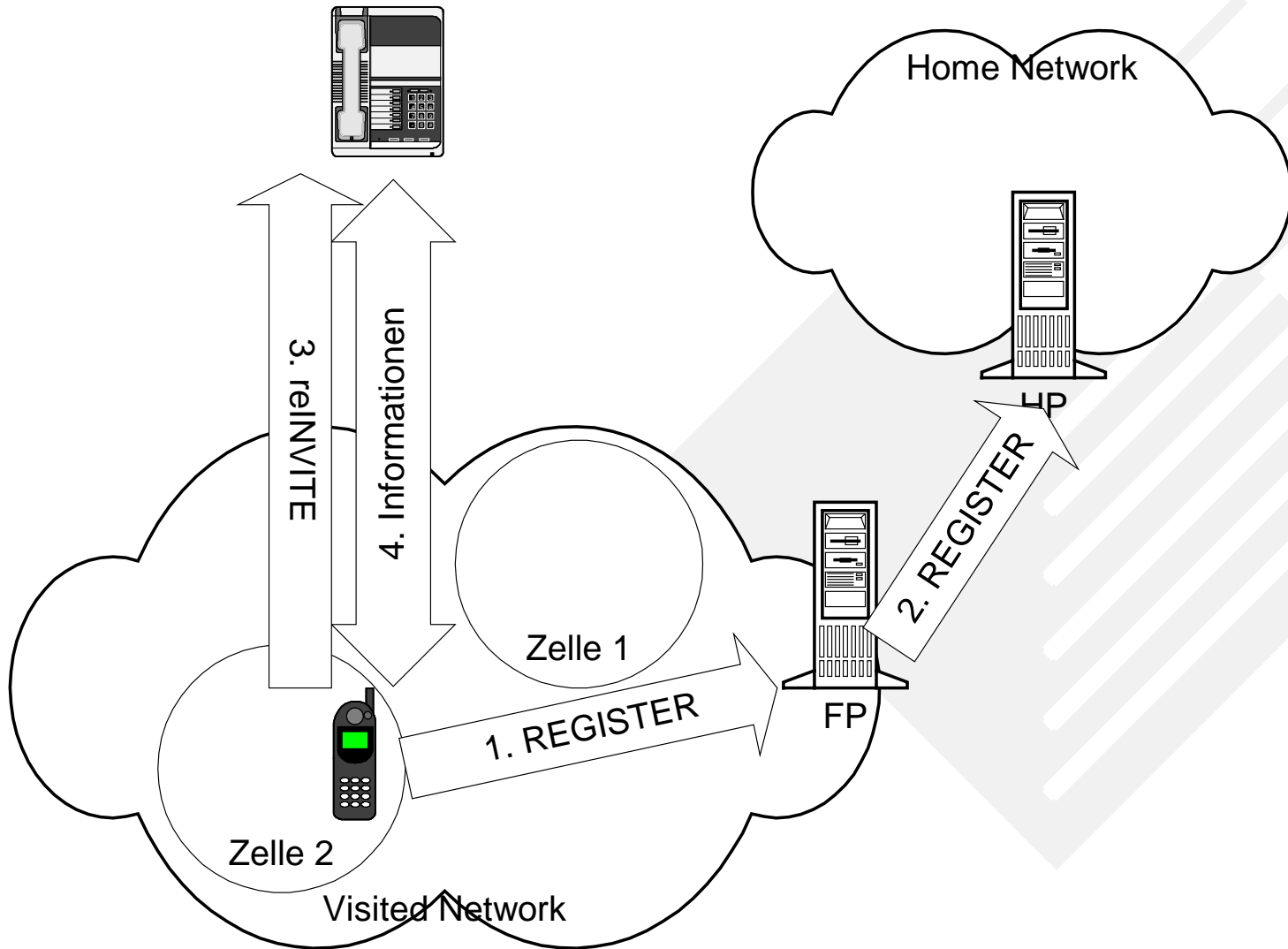
- Mobile Endgeräte informieren ihren Home Proxy durch REGISTER über ihre neue Lokation
- Mobilität inmitten der Session („session mobility“) wird durch reINVITE erreicht



Signalisierung & Informationen: verschiedene Wege

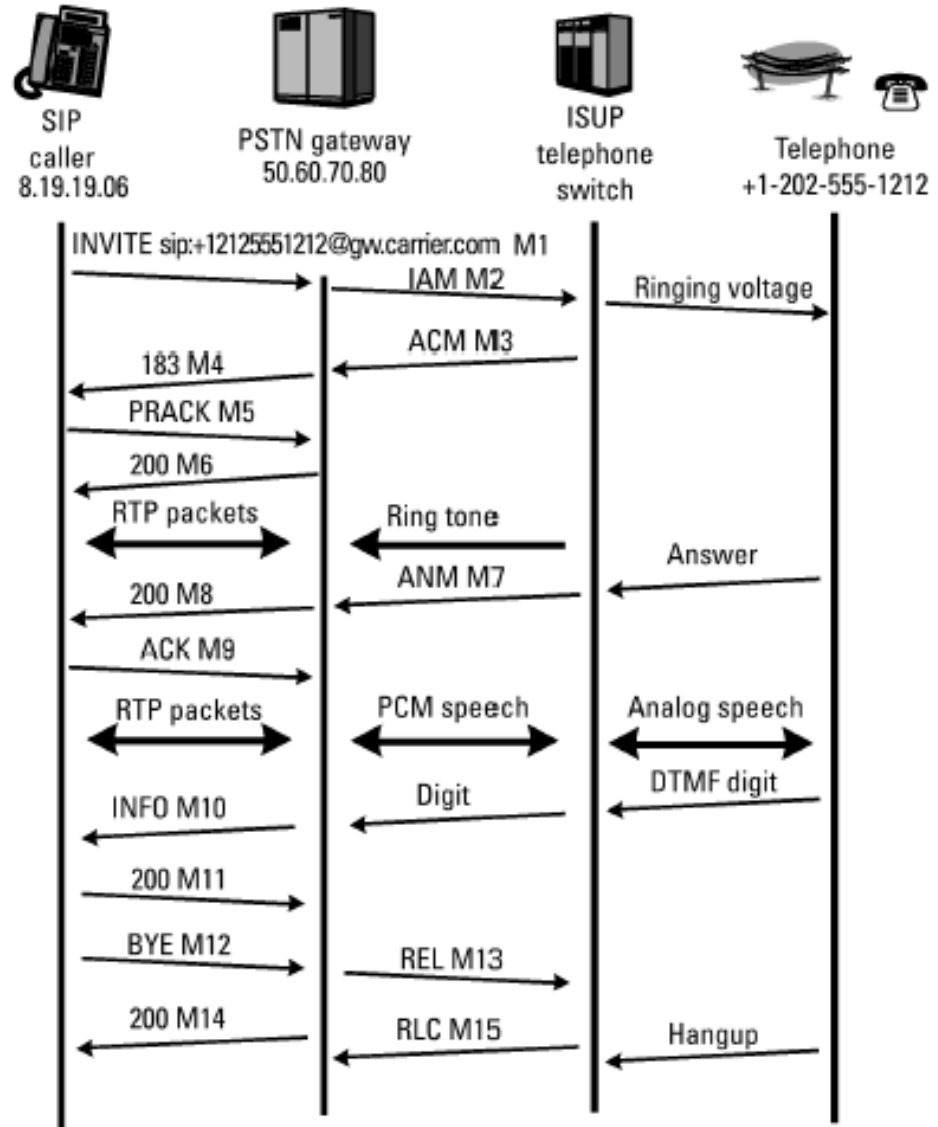


Session Mobility



SIP-zu-PSTN (Quelle: A. Johnston, SIP-Buch)

- In der SIP-INVITE-Nachricht wird die E.164-Telefonnummer des Ziels angegeben und zum Gateway geschickt
- Gateway setzt diesen Befehl in den SS7-Befehl ISUP IAM (Initial Address Message) um
- 183 Session Progress: Damit wird eine Session aufgebaut, damit der Anrufende den Ruf ton hört
- Beidseitige Kommunikation wird mit ANM (Answer Message) und dem SIP-Code 200 OK aufgebaut



H.323 vs. Session Initiation Protocol (SIP)

- SIP gewinnt immer mehr an Bedeutung, auch als Alternative zu H.323
- Eigenschaften von SIP: Einfachheit und Eignung für die schnelle Implementierung neuer Leistungsmerkmale
 - H.323-Spezifikation: mehrere Hundert Seiten
 - SIP-Standard: etwas mehr als 100 Seiten
- SIP erfordert keine Unterstützung von Q.931 und H.245 und ist daher wesentlich einfacher als H.323
- SIP-Endgeräte können preiswerter als H.323-Endgeräte gebaut werden
- Gemeinsamkeit zwischen H.323 und SIP: Intelligenz ist auf den Endgeräten
- Vorteile von H.323: installierte Basis und getätigte Investitionen
- Auf absehbare Zeit werden die beiden Protokolle koexistieren
- Interworking zwischen den beiden Protokollen?
- Produkte, die zwischen SIP-, H.248- und H.323-Signalisierung umsetzen, sind bereits verfügbar (Call Agents bzw. Soft Switches)
- Der Markt wird entscheiden



H.323 vs. SIP: Grundsätzliche Eigenschaften

	H.323	SIP
Architektur	hierarchisch	modular
Standardisierung durch	ITU	IETF
Transport	Überwiegend TCP	Überwiegend UDP
Kodierung	ASN.1	Wie HTTP
Schwerpunkt	Telefonie	Multimedia, Multicast
Adressen	Aliase	SIP URLs



Sicherheit beim Session Initiation Protocol (SIP)

- Im SIP-Modell gibt es auf Grund des Peer-to-Peer-Modells unter Umständen keine „Trusted Third Party“ (analog zum Netzbetreiber in der konventionellen TK)
- daher: Authentifizierung von entscheidender Bedeutung
- Integrität und Zugriffskontrolle nach dem HTTP-Schema
- Bei den Produkten bisher in der Regel nicht implementiert



Denkbare Angriffe bei SIP

- Registration Hijacking: Ein Angreifer kann eine Registrierung unter falschem Namen und damit die Annahme der Identität eines Benutzers vornehmen
 - Abhilfe: Client-Authentifizierung
- Server Spoofing: böswilliger Server kann SIP Requests umleiten
 - Abhilfe: Server-Authentifizierung
- Abhören vertraulicher Daten
 - Abhilfe: Ende-zu-Ende-Verschlüsselung
- Denial of Service durch SIP-Meldungen
 - Abhilfe: Authentifizierung



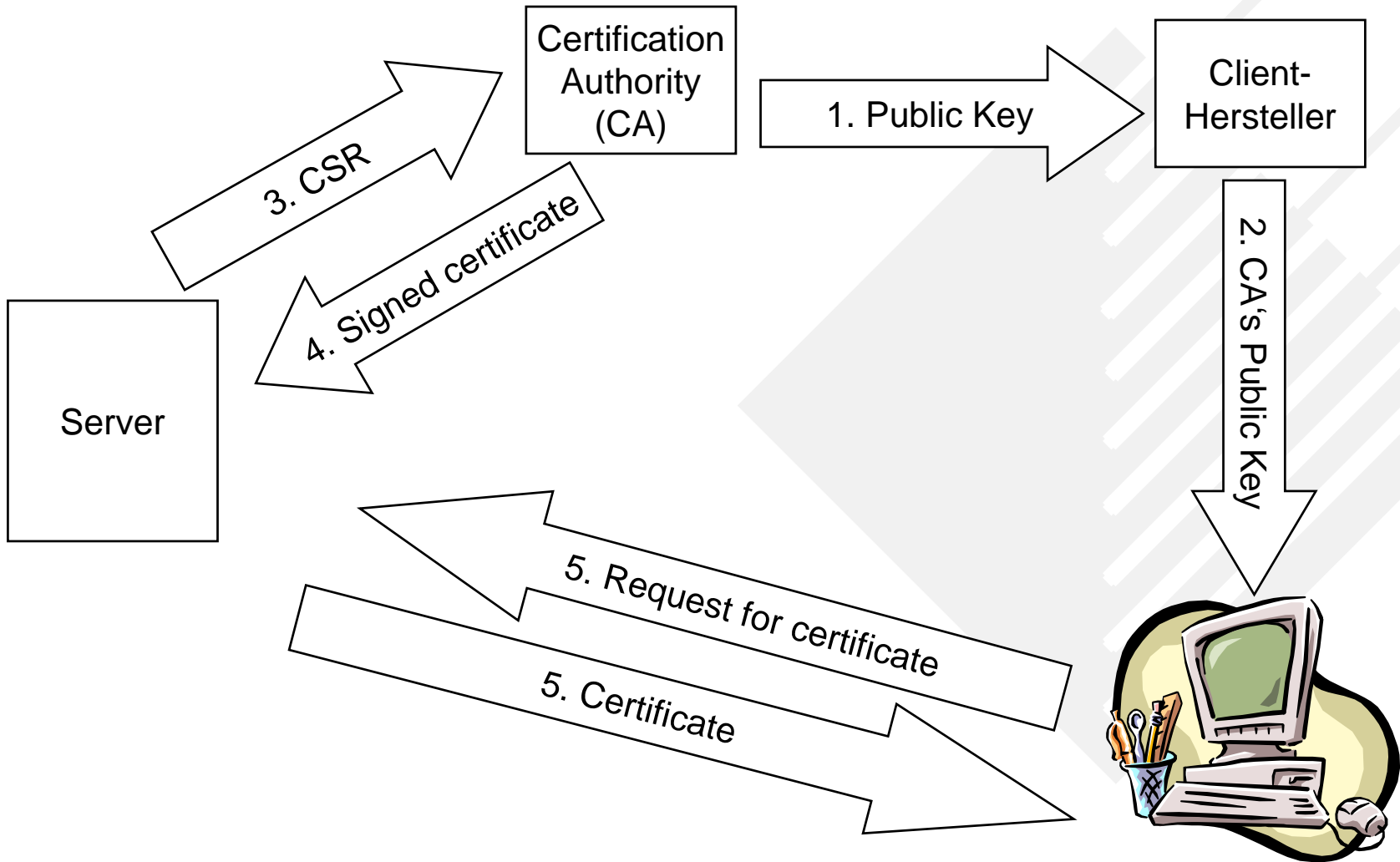
SSL-Dienste

- Statt sip:moayeri@comconsult.com sips:moayeri@comconsult.com
- Authentifizierung und Nichtbestreitbarkeit, sowohl für den Client als auch für den Server, durch den Einsatz von digitaler Signatur
- Vertraulichkeit durch Verschlüsselung
- Datenintegrität durch Authentifizierungs-codes für einzelne Nachrichten
- SSL setzt direkt auf TCP/IP auf und stellt diese Dienste den normalerweise auf TCP/IP aufsetzenden Diensten zur Verfügung
- SSL Hello: Beide Parteien prüfen, welcher das stärkste kryptografische Protokoll ist, was sie beide unterstützen
- SSL Version 1.0: nur innerhalb Netscape
- SSL Version 2.0: in Navigator 1 und 2, danach entwickelte Microsoft PCT als Konkurrenzprodukt
- SSL 3.0: Reaktion von Netscape auf PCT, nimmt die guten Eigenschaften von PCT auf
- SSL 3.0 ist die Basis von Transport Layer Security (TLS) von Internet Engineering Task Force (IETF)

Wie funktioniert SSL?

- Verschlüsselte Kommunikation
 - Statt als URL einzugeben: sip:moayeri@comconsult.com gibt man als URL ein: sips:moayeri@comconsult.com
- Public-Key-Verschlüsselung ist aufwendig, so daß SSL die Möglichkeit bietet, ein "master secret" zu cachen und bei späteren Verbindungen mit dem selben Kommunikationspartner zu nutzen
- SSL 3.0 nutzt Zertifikate nach dem Format X.509 v3
- SSL läuft nicht auf UDP
- Umleitung zu einer nicht sicheren SIP-URI ist möglich, aber der Client muss den Benutzer darüber informieren (analog zu Web)

Überprüfung des Zertifikats



Schein und Sein (Quelle: GMD Fokus, SIP Tutorial)

SIP INVITE w/JPEG

```
INVITE sip:UserB@there.com SIP/2.0
Via: SIP/2.0/UDP here.com:5060
From: BigGuy <sip:UserA@here.com>
To: LittleGuy <sip:UserB@there.com>
Call-ID: 12345600@here.com
...
```



200 OK w/JPEG

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP here.com:5060
From: BigGuy <sip:UserA@here.com>
To: LittleGuy <sip:UserB@there.com>
Call-ID: 12345601@here.com...
```



Nützliche Quellen

- <http://www.fokus.gmd.de/glone/projects/ipt>
- <http://www.cs.columbia.edu/~hgs/sip>
- <http://www.cs.columbia.edu/~hgs/internet>
- <http://www.normos.org>
- Verlag Artech House 2001, Alan B. Johnston: SIP, Understanding the Session Initiation Protocol
- RFC 2543 SIP
- draft-ietf-sip-rfc2543bis
- RFC 2327 SDP
- draft-ietf-sip-call-flows
- draft-ietf-sip-service-examples
- RFC 3050 SIP CGI
- draft-iptel-cpl
- RFC 1889 RTP

