Sicherheitsrisiko Voice over IP

Uwe Sauerbrey, VP Product Management

Swyx Solutions GmbH, Joseph-von-Fraunhofer-Str. 13 a, 44227 Dortmund, Germany

uwe.sauerbrey@swyx.com



www.swyx.com

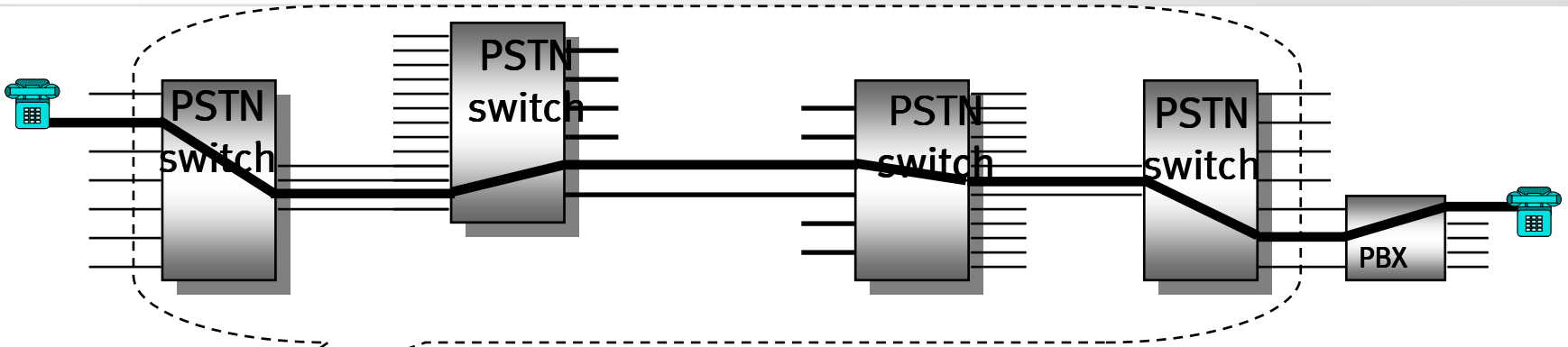
- VoIP allgemein und IP-PBX Grundlagen
- H.323 vs. SIP - Mit SIP wird alles besser! Wirklich?
- Swyx und SwyxWare – ein kurzer Überblick
- Wo liegen die potenziellen Angriffspunkte?
- Verschlüsselung von Call Control und/oder der Sprachdaten
- VoIP – SPAM – SPIT
- Was müssen die Hersteller, die Provider und die Anwender tun?
- Demonstration – Abhören eines SIP-Call

VoIP allgemein und IP-PBX Grundlagen

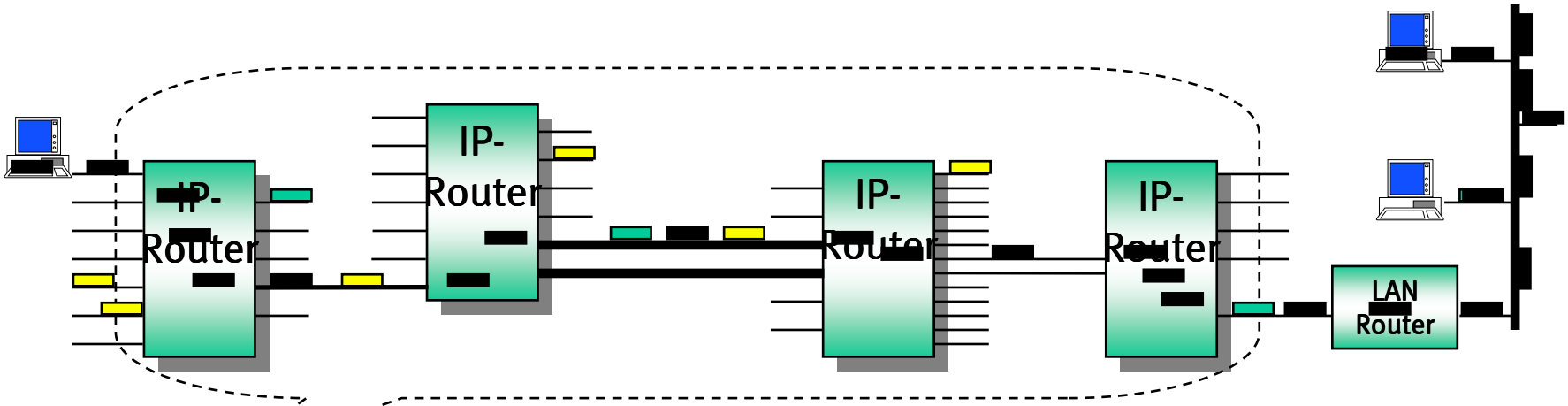
Voice over IP - Allgemein

- Übertragung der Sprache mit Hilfe von Datenpaketen
- Nutzung der Internet Protokolle (IP)
- Sowohl in öffentlichen Telefonnetzen als auch im Bereich der Telefon-Anlagen
- Ein Netz für Sprache und Daten

Transportverfahren in öffentlichen Netze

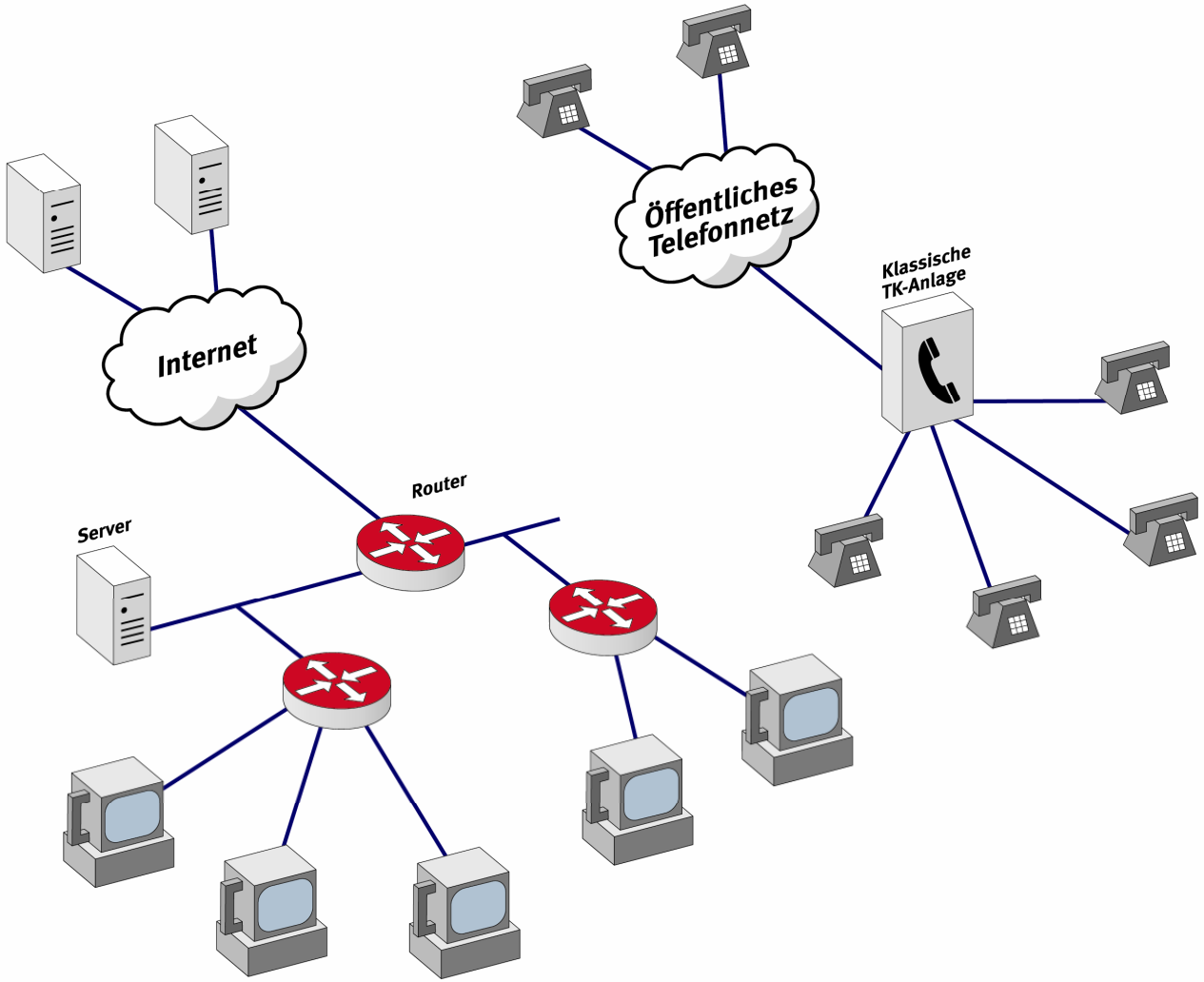


Public Switched Telephone Network (line switching)

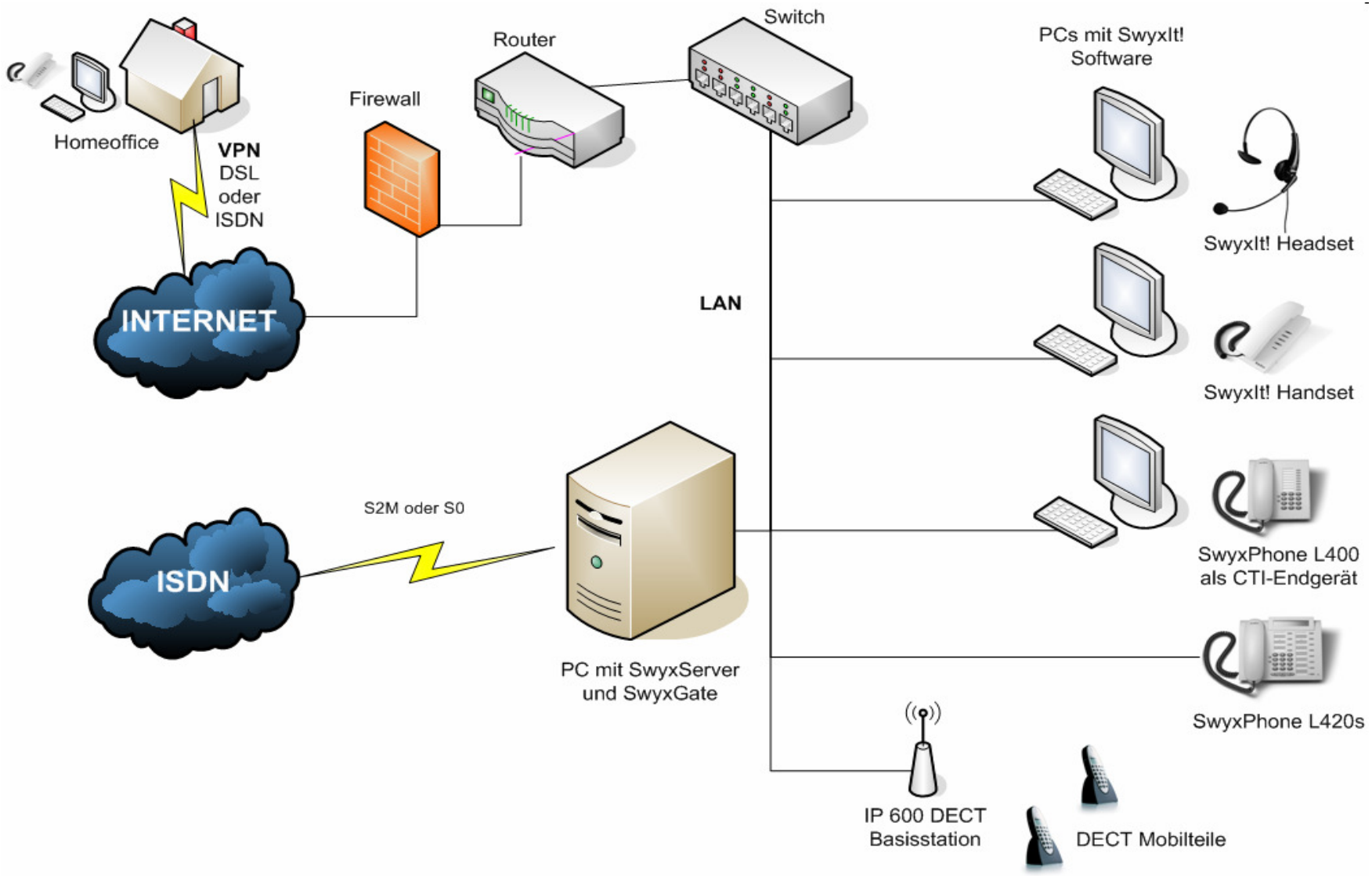


IP-based routed Internet (packet switching)

Im Unternehmen: Zwei getrennte Welten ...

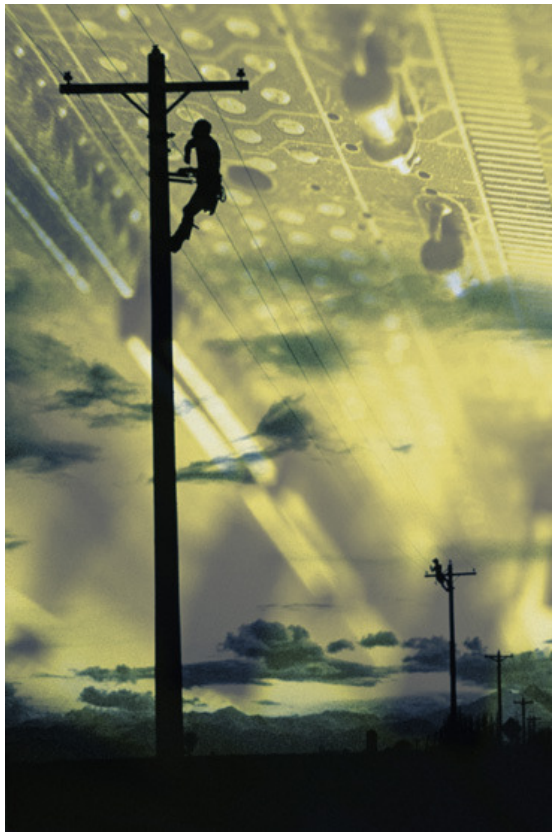


... wachsen zusammen



VoIP auf dem Weg *Pro und Contra*

- **VoIP hat Vorteile...**
  - Einheitliche Kommunikations-Infrastruktur auf IP-Basis
  - Geringere Kosten für Wartung und Administration
  - Einfachere, schnellere Erweiterung neuer Anwendungen
  - Effizienzsteigerung an Telefon-Arbeitsplätzen



- **...aber auch Nachteile**
  - höhere Bandbreite /QoS notwendig
  - Zuverlässigkeit wird gegenüber der klassischen wird TK-Technik angezweifelt
  - Lösungen fehlen oft noch offene Schnittstellen
  - Weniger Komfortmerkmale bei Standard-konformen Plattformen, d.h. oft werden proprietäre Lösungen genutzt
  - Standardisierung nicht abgeschlossen

Gründe für den Einsatz von VoIP



- Das Telefonsystem ist am Ende des technischen Lebenszyklus und muss ersetzt werden.

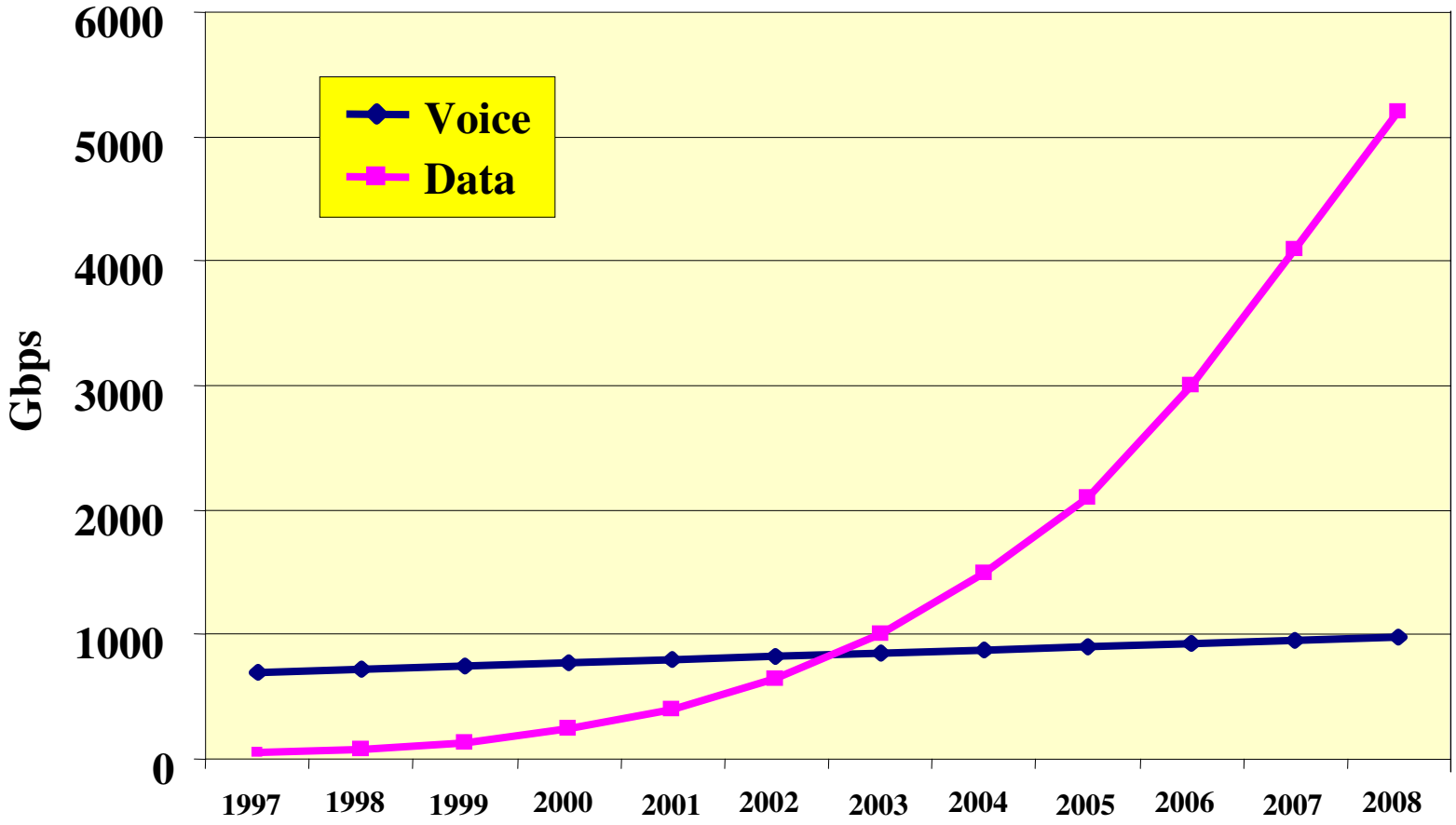
- Das Unternehmen zieht in ein neues Gebäude oder an einen anderen Ort und benötigt ein neues Telefonsystem.





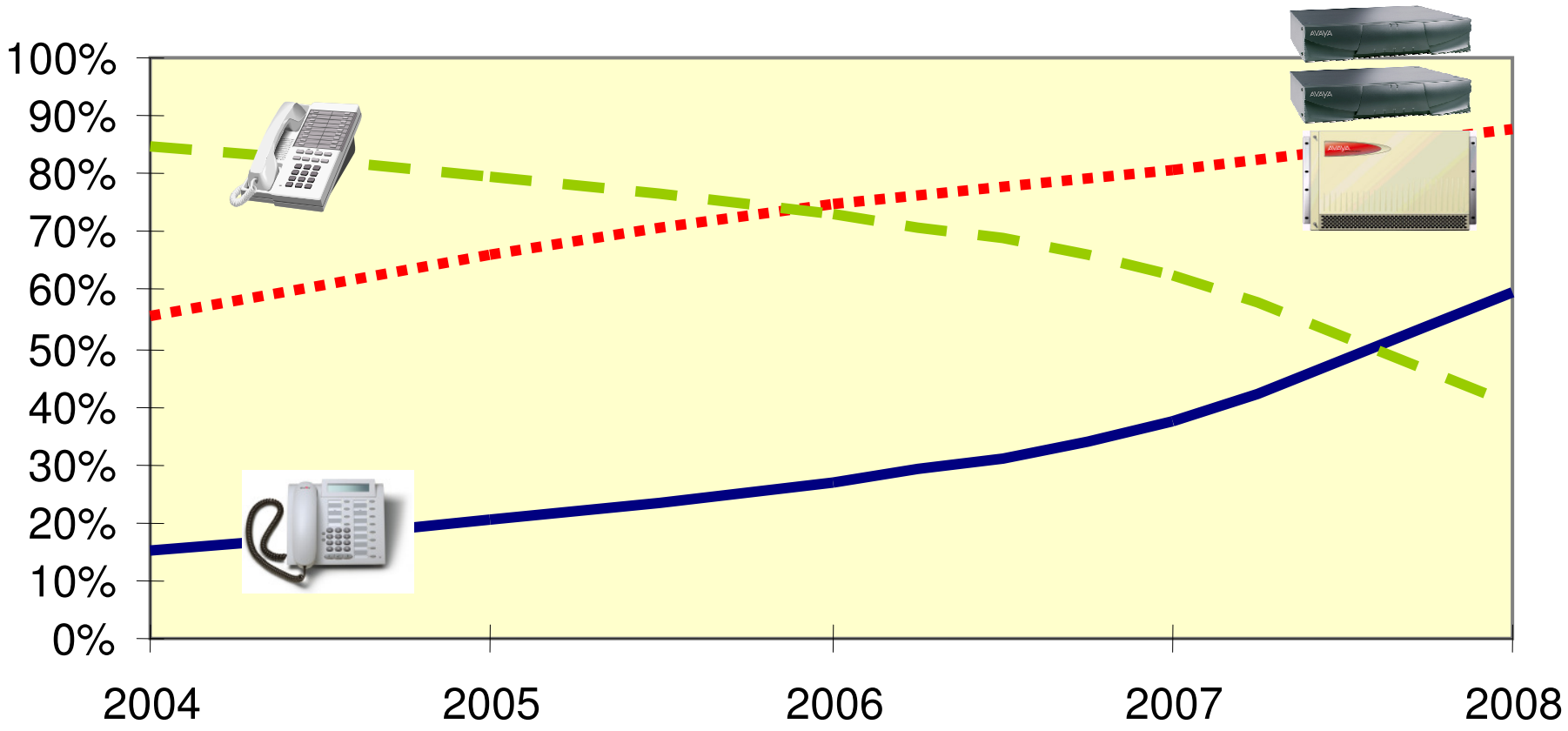
- Es werden neue Funktionen benötigt oder es gibt Kostenvorteile, welche einen direkten finanziellen Nutzen darstellen.

Verkehrsaufkommen für Sprache und Daten (weltweit)



Source: A.D. Little

Entwicklung von IP-Verbindungen



Source: Market Forecasts:
Premise Switching Equipment Western Europe, 2003

H.323 vs. SIP - Mit SIP wird alles besser! Wirklich?

SIP

- SIP - Session Initiation Protocol
- Signalisierungsprotokoll für Sprach- bzw. (allgemeiner) Multimediadaten über paketvermittelnde Netze
- Standardisiert von der IETF
- Wird auf Dauer das „alte“ H.323 ablösen (H.323 stammt von der ITU)
- Geprägt durch
  - Einfachheit
  - Erweiterbarkeit
  - Ähnlichkeit zu weit verbreiteten Protokollen wie HTTP oder SMTP
- Aber unnötige Möglichkeit der Nutzung von UDP und TCP

H.323 vs. SIP

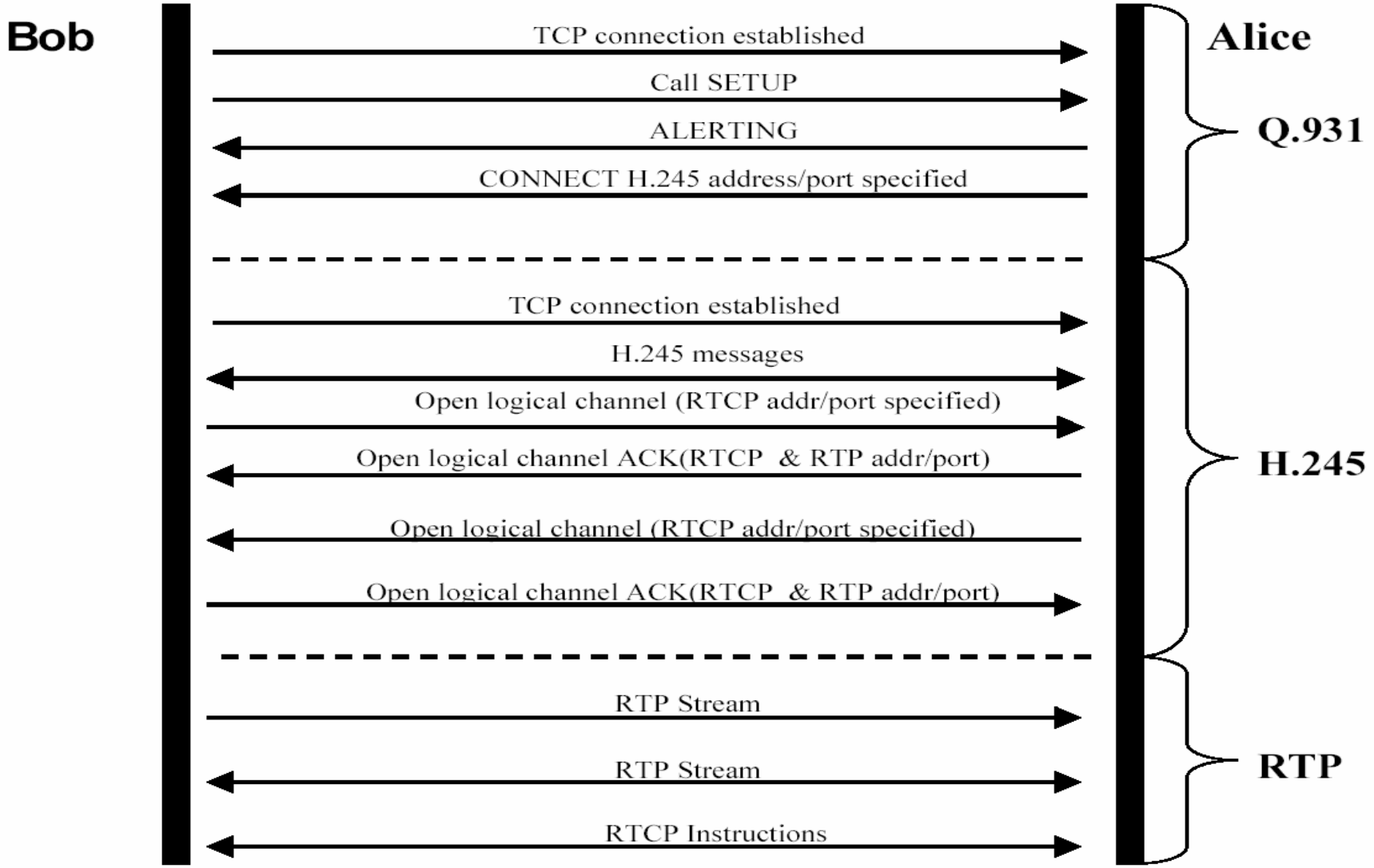
H.323

- H.323 definiert ein komplettes und komplexes Multimedia-System für Audio und Video
- H.323 definiert alle Einzelheiten von der Signalisierung, Paketierung bis zur Kodierung
- H.323 unterstützt ein Bandbreitenmanagement
- H.323 ist ein ist sehr komplexes Protokoll, binär kodiert

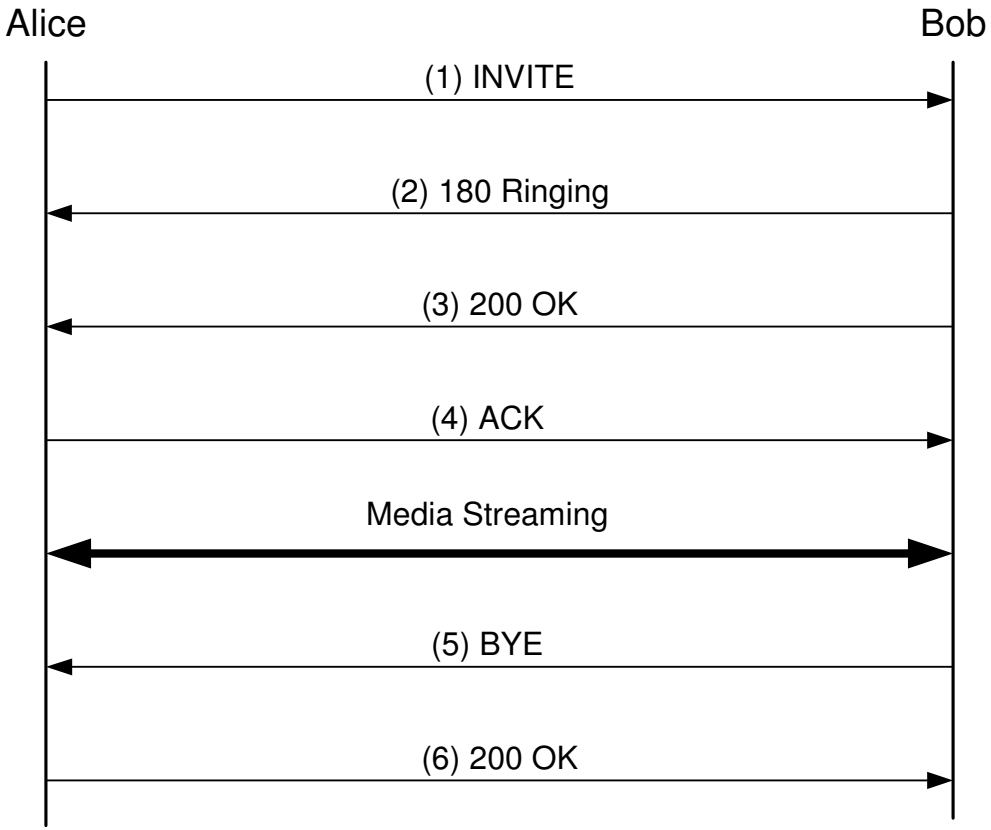
SIP

- SIP wird nur für die Signalisierung eingesetzt
- SIP wird benutzt um Sessions zwischen den Endteilnehmern auf- bzw. abzubauen
- SIP kann in einer Session beliebige Daten austauschen
- Der Transport der Nutzdatem liegt außerhalb des Definitionsbereichs des eigentlichen Standards
- Text basiert

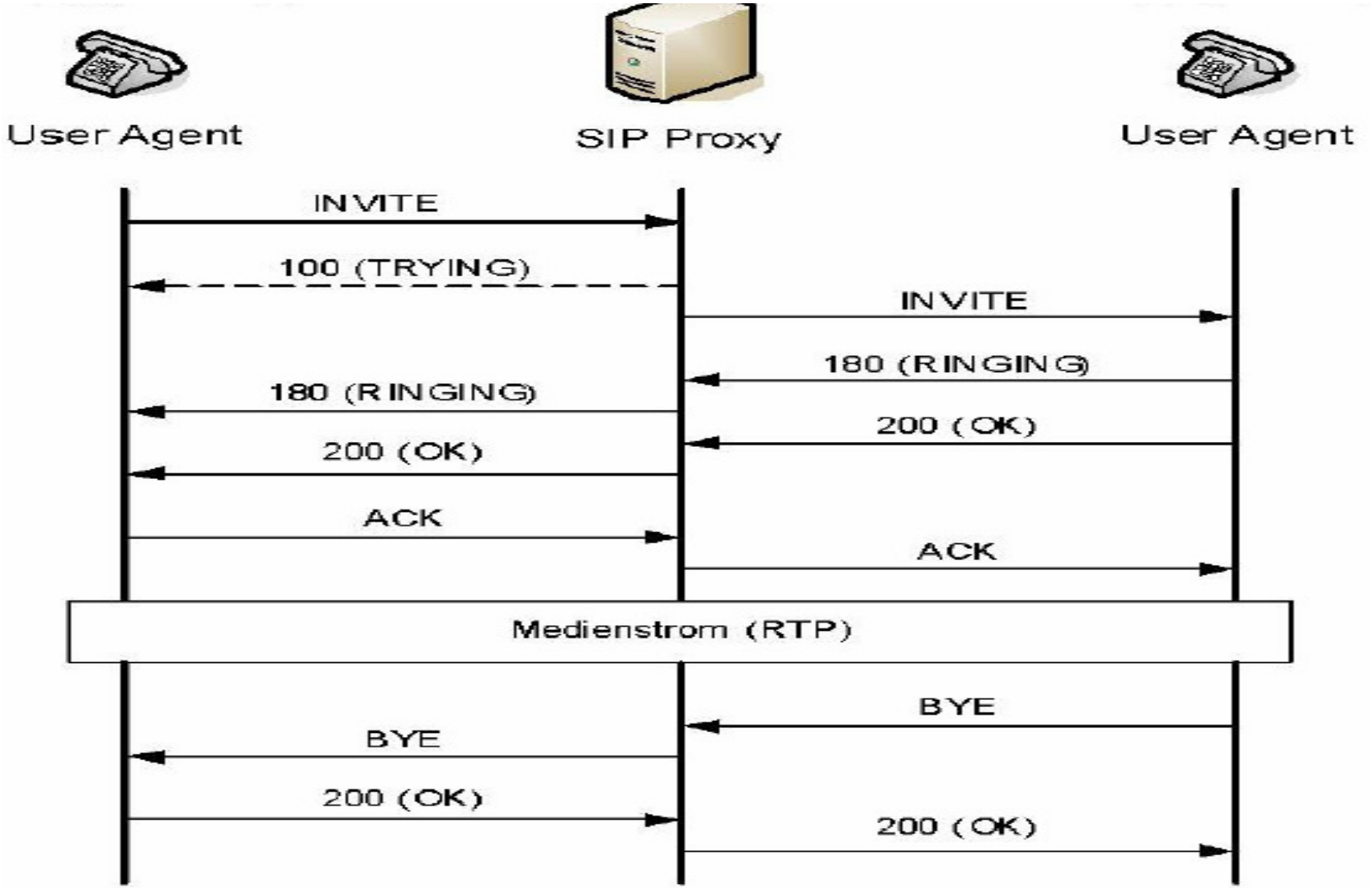
VoIP mittels H.323



SIP Messages - Verbindungsauf- und abbau



SIP Messages - Verbindungsauf- und abbau

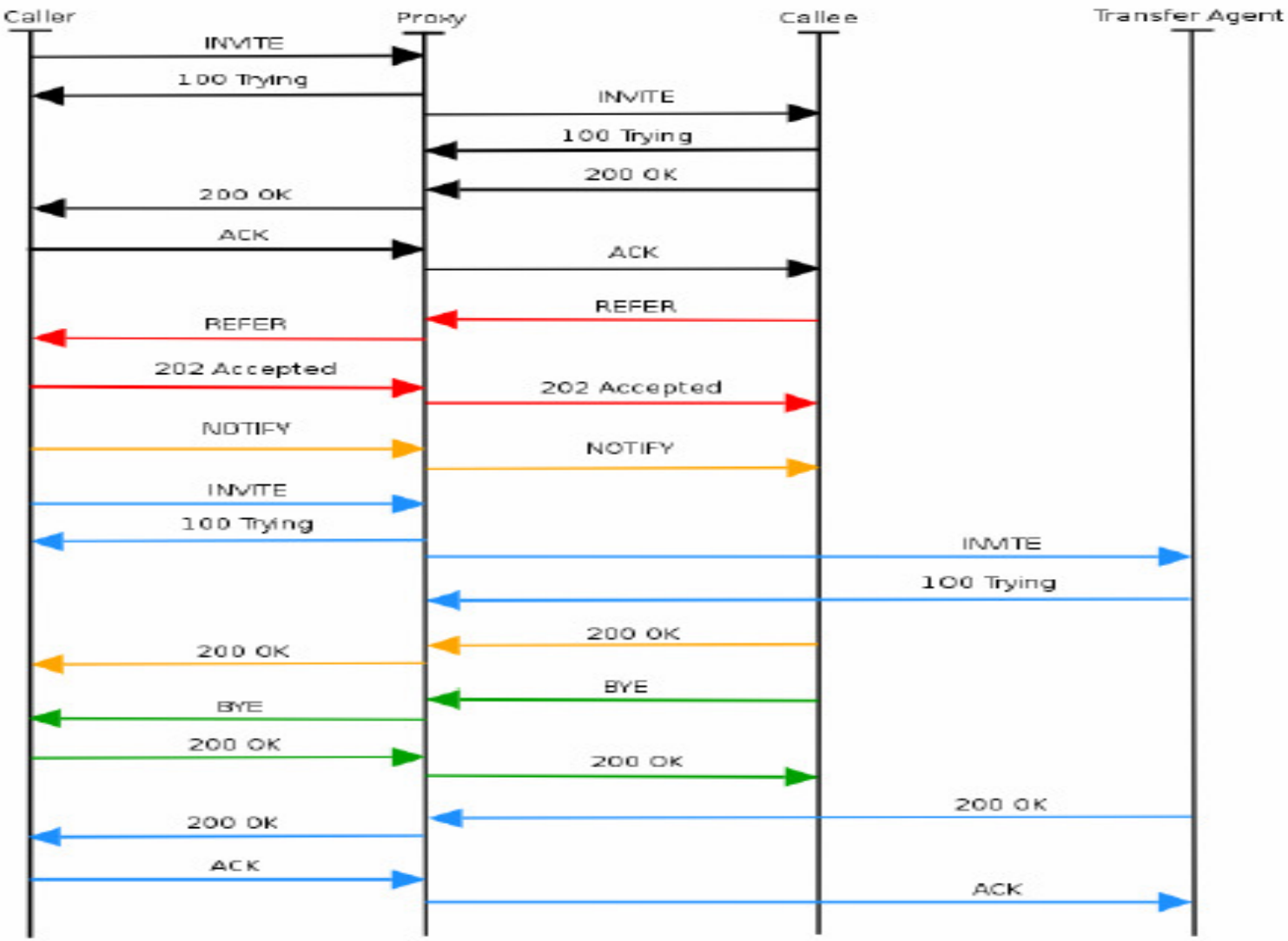


SIP Invite Message

```
INVITE sip:123@217.194.238.187;user=phone SIP/2.0
Via: SIP/2.0/UDP 217.194.238.37:5060
From: sip:ata1@217.194.238.37;tag=1765866978
To:  <sip:123@217.194.238.187;user=phone>
Call-ID: 4008732121@217.194.238.37
CSeq: 1 INVITE
Contact:  <sip:ata1@217.194.238.37:5060;transport=udp>
User-Agent: Cisco ATA  v2.15 ata186 (020723a)
Content-Type: application/sdp                    (SDP=Session Description Protocol)
Content-Length: 251
Content-Type: application/sdp
Content-Length: 251

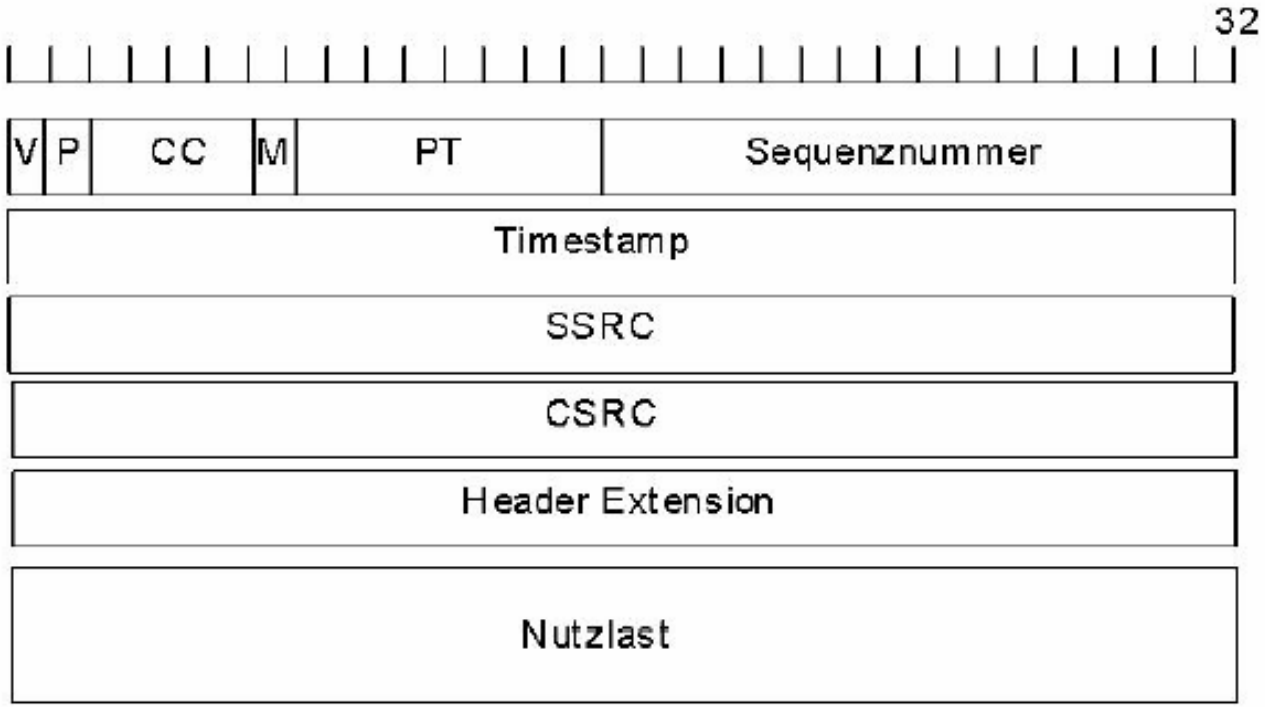
v=0
o=ata1 17803 17803 IN IP4 217.194.238.37
s=ATA186 Call
c=IN IP4 217.194.238.37
t=0 0
m=audio 16384 RTP/AVP 0 4
a=rtpmap:0 PCMU/8000/1
a=ptime:20
a=rtpmap:4 G723/8000/1
a=rtcp:53020
```

SIP Supplementary Services (Call Forwarding)



Sprachdaten - RTP Real Time Protocol

- UDP
- PT Payload Type Identification (e.g. G.711, G.729A, ...)
- Timestamp
- Sequence Number
- SSRC Synchronisation Source Identifier
- CSRC Contributing Source Identifiers



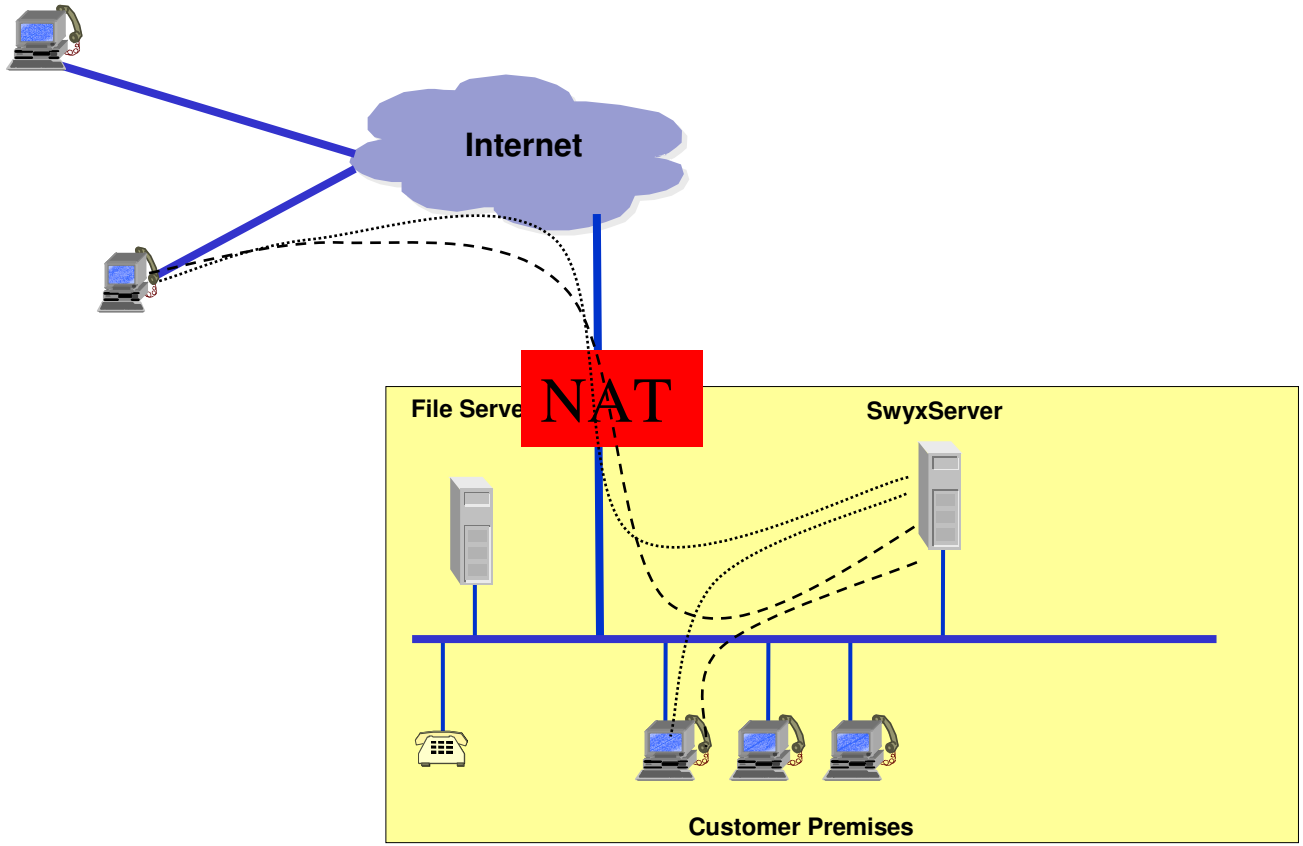
Codecs

Name	Bitrate (netto) in kbit/s	Bitrate (brutto) in kbit/s	Standardisiert	Kodierungsverfahren
G.711	64	88	ITU-T	PCM
G.723.1	5,3/6,3	21/22	ITU-T	ACELP/MP-MLQ
G.726	32	55	ITU-T	ADPCM
G.728	16	32	ITU-T	LD-CELP
G.729A	8	17	ITU-T	CS-ACELP
GSM	13	35	ETSI	RPE-LTP
iLBC	13,3/15,2	27	IETF	LPC
Speex	2 - 44	variable	IETF	

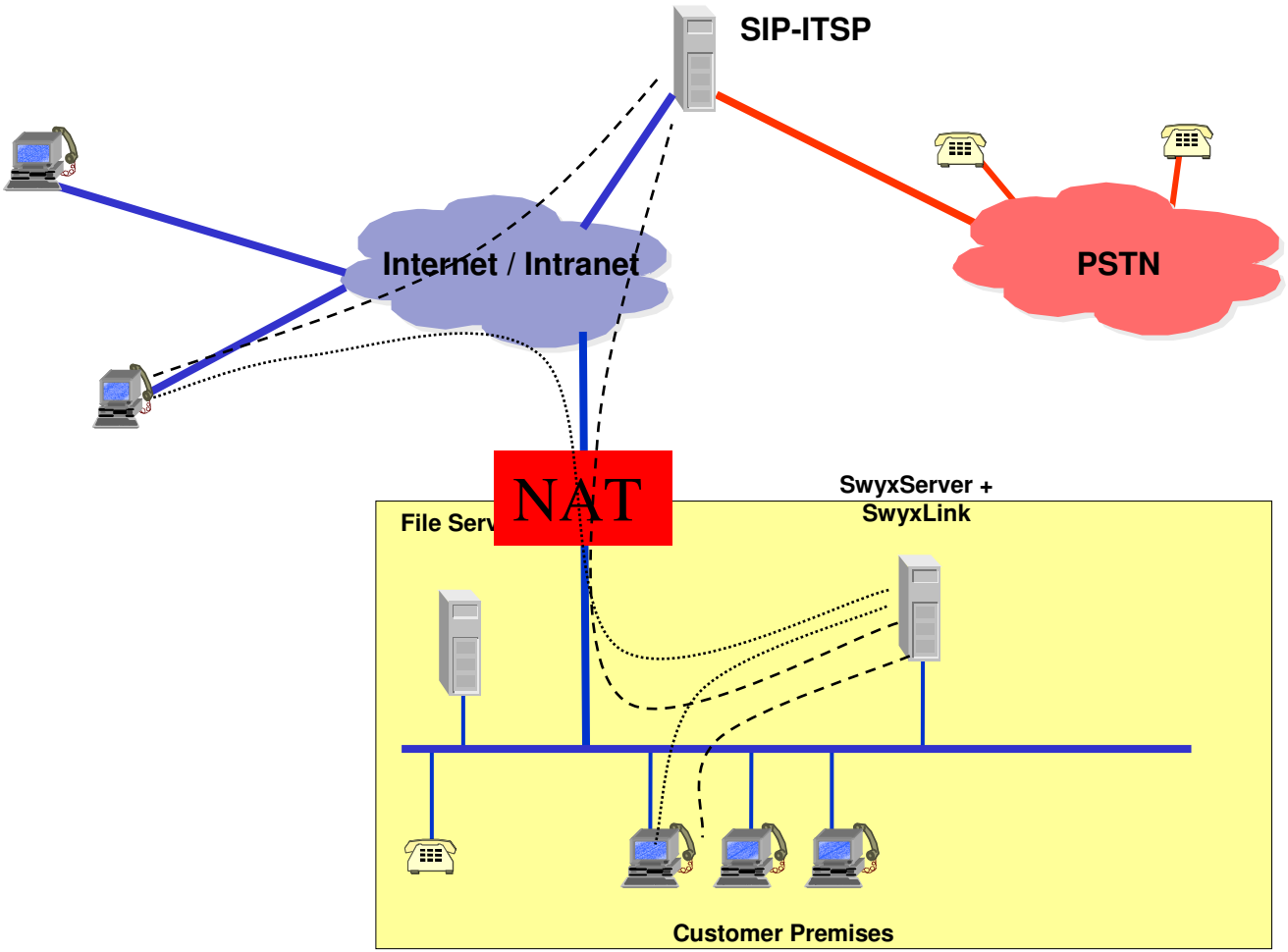
Codierungsverfahren	Delay in ms	CPU-Last in MIPS	MOS (no packetloss)
G.711	0,75	<1	4,1
G.723.1	30	16	3,65 / 3,9
G.729	10	50	3,92
G.729A	10	10,5	4,7
GSM	20		1,8-3,5
iLBC			3,9

SIP calls directly to a SIP client

SIP-Phone



SIP-Link to SIP-ITSP



Different types of NAT policies

Full Cone NAT

All requests from the same internal IP address and port are mapped to the same external IP address and port.

Restricted Cone NAT

All requests from the same internal IP address and port are mapped to the same external IP address and port.

Unlike a full cone NAT, an external host (with IP address *X*) can send a packet to the internal host only if the internal host had previously sent a packet to IP address *X*.

Port Restricted Cone NAT

Like a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address *X* and source port *P*, to the internal host only if the internal host had previously sent a packet to IP address *X* and port *P*.

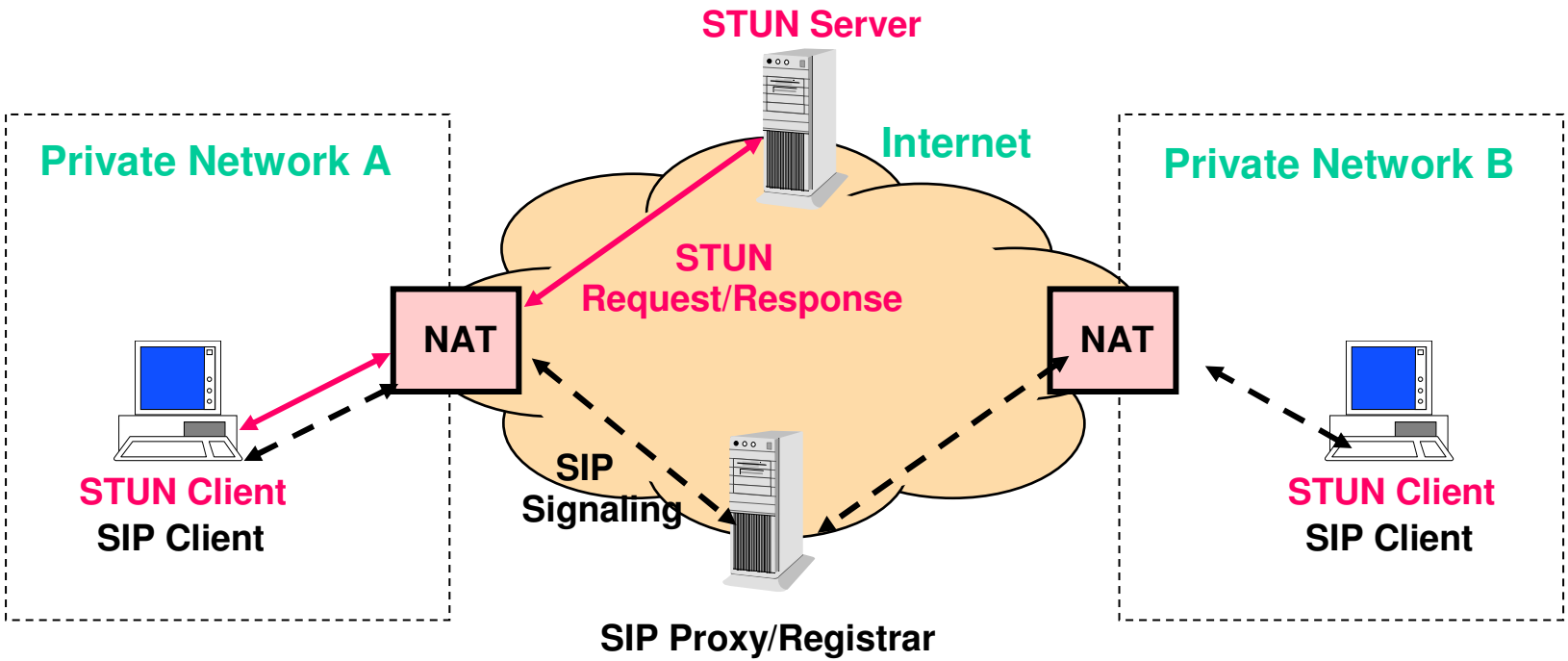
Symmetric NAT

All requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port.

If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used.

Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

STUN – Simple Traversal of UDP Through NATs



Source: P. Thermos, Telcordia

- STUN client contacts STUN server, discovers NAT, address translation
- SIP client uses “external” address in signaling for setup of media streams
- STUN does not work with symmetric NAT
  because the IP address port mapping is dependent on the destination, i.e. The STUN server would deliver the IP address port mapping for the connection to the STUN server itself, which is different from the mapping for the destination client

VoIP Routing - Wie wird ein SIP Server gefunden

- sip:uwe.sauerbrey@swyx.com (SIP URI)

- Unter swyx.com gibt es erstmal nicht direkt einen SIP-fähigen Host

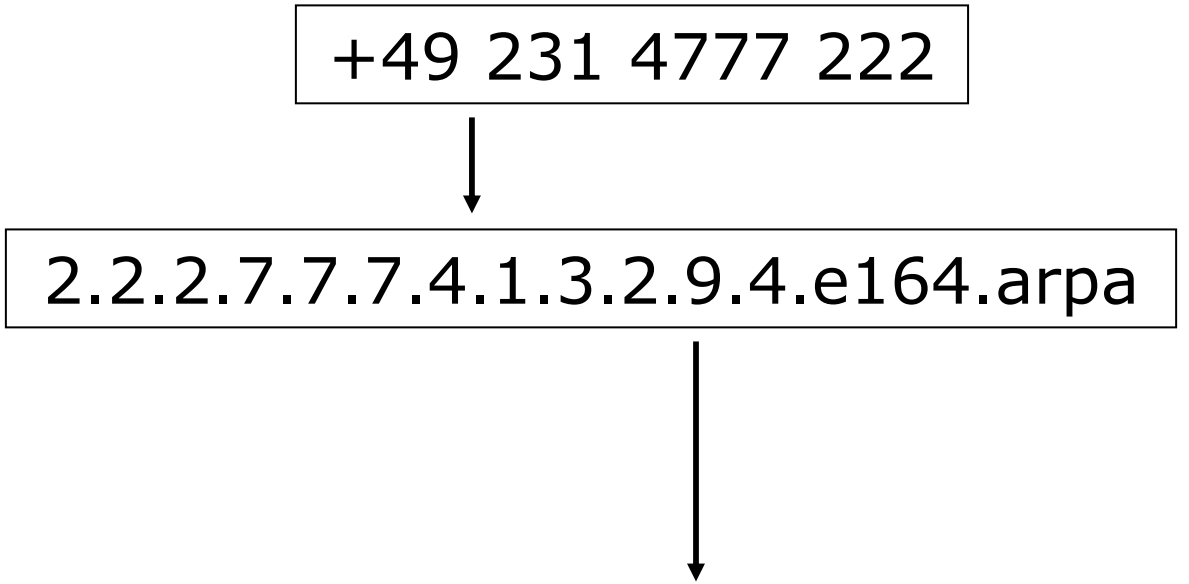
- SRV Records (RFC 2782), die zum Auffinden von VoIP–Systemen dienen.
- Ähnlich den MX Records, die das Auffinden von E-Mail-Server ermöglichen

- Ein SRV Record zeigt auf den SIP-Server, der für die Domain zuständig ist
- Werden mehrerer SIP-Proxys für eine Domain angegeben, entscheidet die Priorität zu welchem Server geroutet wird
- Format:

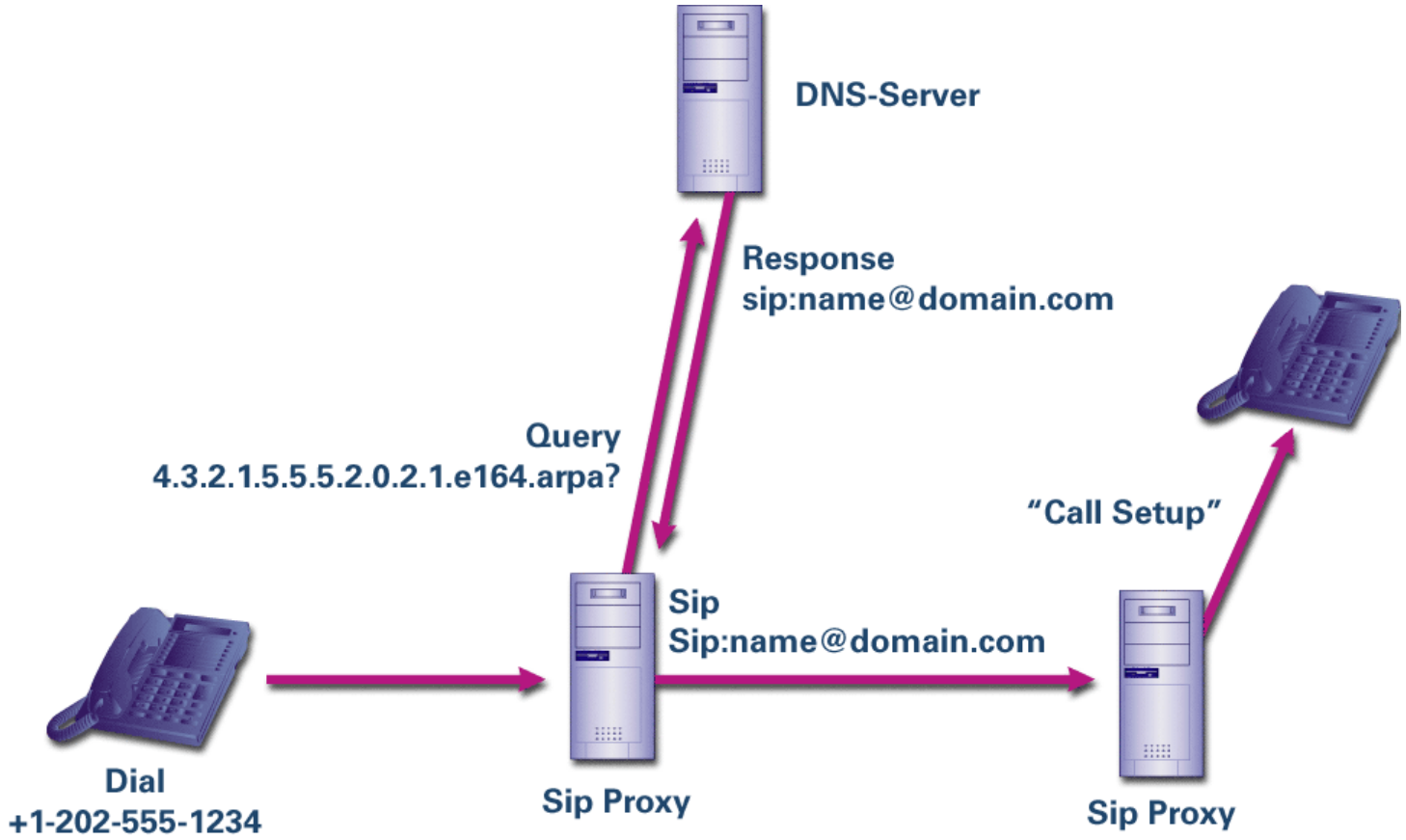
```
_sip._udp.swyx.com      1000 IN SRV 20 0 5060 sip.swyx.com
_sip._tcp.swyx.com      1000 IN SRV 20 0 5060 sip.swyx.com
```

ENUM - tElephone NUmber Mapping (RFC3761)

- take phone number
- turn it into a Domain Name
- ask the DNS
- returns URI Uniform Resource Identifier



Simple ENUM/SIP Call Flow



ENUM details

Die DNS-Anfrage liefert nicht direkt eine SIP URI sondern

- einen oder mehrere NAPTR (Naming Authority Pointer) records

- IN NAPTR 100 10 "u" "sip+E2U" "!^.*$!sip:uwe.sauerbrey@swyx.com!i“ .
- IN NAPTR 102 10 "u" "smtp+E2U" "!^.*$!mailto:uwe.sauerbrey@swyx.com!i" .

Nebenorganisationen, nicht nur e164.arpa sondern auch

- e164.org
- e164.info
- enum.org

Swyx und SwyxWare – ein kurzer Überblick

Unternehmen: **Zahlen und Fakten**

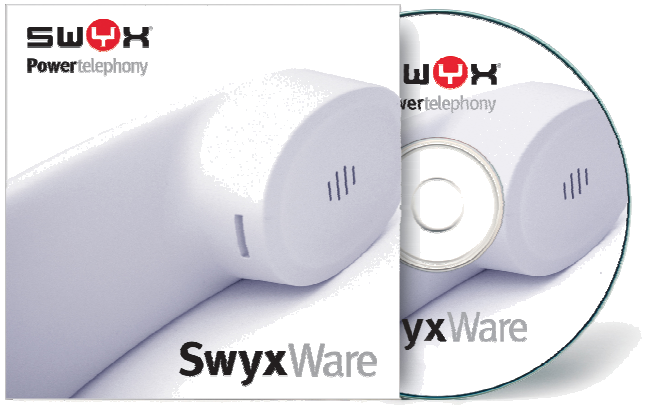
- Swyx ist Hersteller von Software-Telefonanlagen (IP-PBX) für Microsoft Windows Server
- Gegründet 1999 als StartUp-Unternehmen, derzeit 45 Mitarbeiter, stark steigend
- **Mehr als 3.000 Unternehmen** mit 90.000+ SwyxWare Benutzer setzen bereits auf Swyx-Produkte
- Umsatz in 2004: 4,1 Mio €, geplant für 2005: 10 Mio €, Profitabel seit 9/2004
- **Internationales Vertriebsnetz** mit mehr als 1.000 autorisierten Fachhandels-Partnern
- OEM-Partner, wie die Deutsche Telekom AG, haben sich für Swyx-Produkte entschieden

Swyx Zentrale in Dortmund



Unternehmen: **Swyx-Produkte**

- **SwyxWare**: Softwarebasierte IP-Telefonanlage (IP-PBX)
- **100% Microsoft Plattform**
- **Offene, skalierbare PC-Architektur** – keine proprietäre Hardware
- **Herausragende Leistungsmerkmale** – alle klassischen TK-Anlagen Feature verfügbar
- **Einzigartiger Mehrwert** für Fachhändler und Systemintegratoren
- **Komplettlösung** für kleine und mittelständische Unternehmen (ab 5 Teilnehmer)



Microsoft Windows Server

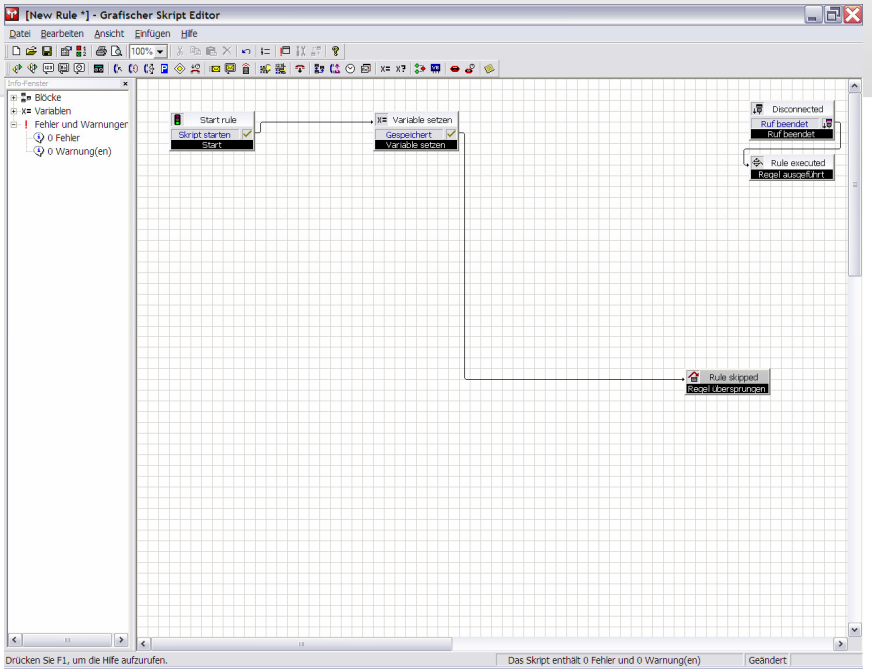
+ Voicemail und Fax an jedem Arbeitsplatz
+ Integration in Microsoft Outlook und IBM Lotus Notes
+ Intelligentes Anruf-Management (Call Routing)
+ Interactive Voice Response (IVR)
+ Konferenz-Manager
+ One Click Application Sharing

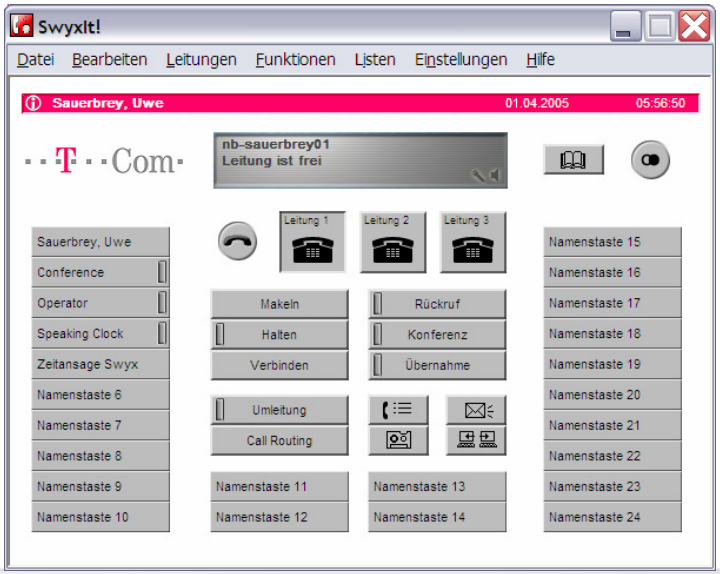
Mehr als 500 weitere **Power**telephony features...

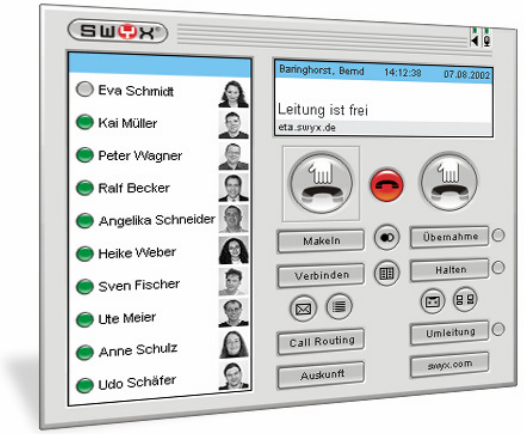


SwyxIt! **Highlights**

- **Individuelle Bedienoberflächen (Skins)** mit integriertem Skin-Editor
- **Telefonie-Integration in Microsoft Outlook und IBM Lotus Notes**
- **Individuelle Rufumleitung** mit dem Call Routing Manager
- **Integrierter Applikationsgenerator** mit dem Graphischen Skript Editor







SwyxPhone: **Modellübersicht**

- Mit den SwyxPhone bietet Swyx für jeden Mitarbeiter im Unternehmen das passende Telefon

SwyxPhone L400: Das kostengünstige Einsteigermodell, ideal für den CTI-Einsatz in Kombination mit dem PC, Warum Geld für ein Display ausgeben, der PC-Monitor ist doch groß genug?

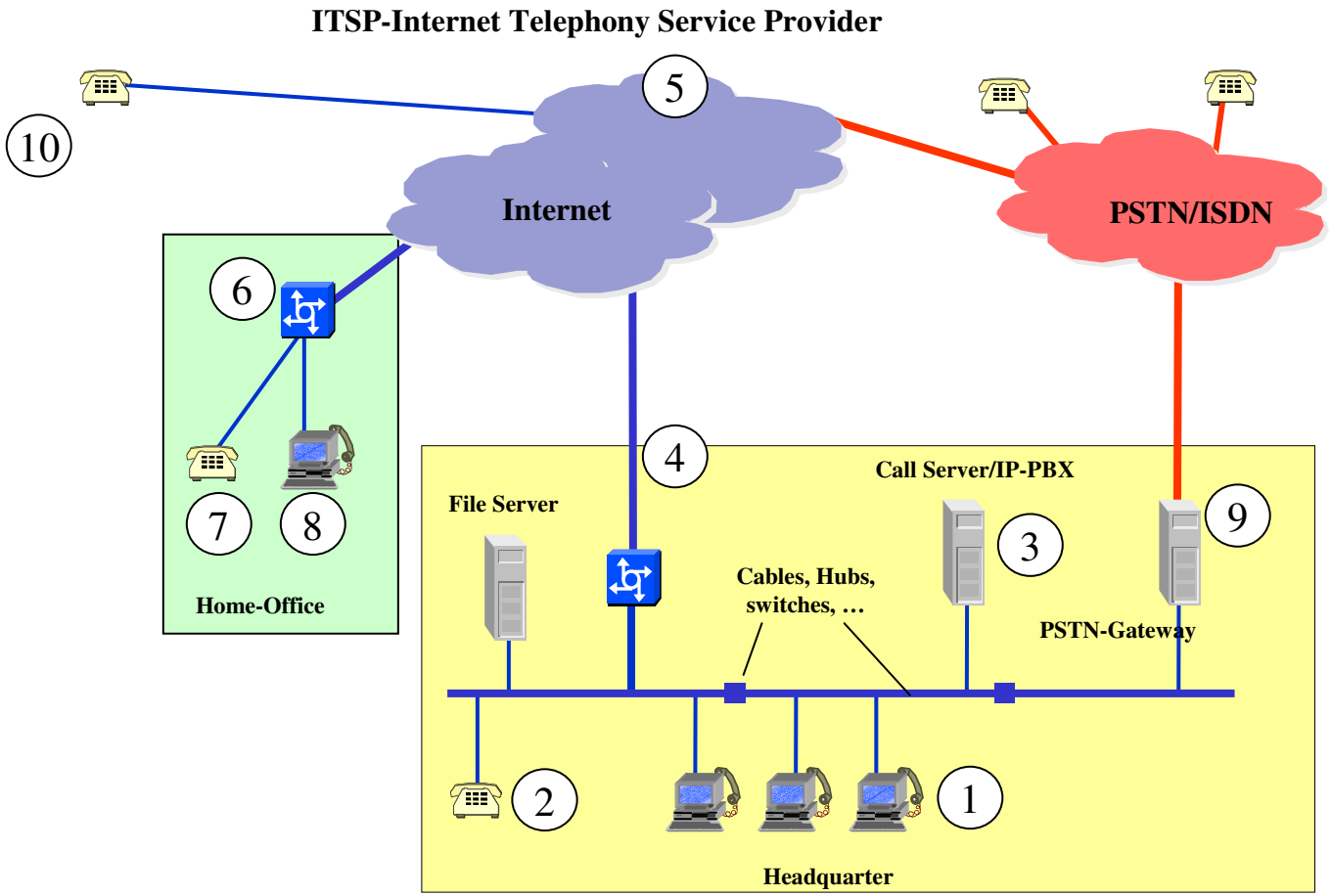
SwyxPhone L440: Das Komforttelefon mit integriertem Switch und 4-zeiligem Display



SwyxPhone L420: Das Standard-Modell, ob als CTI-Telefon mit integriertem Switch (L420s) oder als Standalone-Gerät in Konferenzräumen ohne Switch (L420e)

SwyxPhone Erweiterungsmodul: Erweitert L420s und L440 um weitere Funktionstasten

Wo liegen die potenziellen Angriffspunkte?


ITSP-Internet Telephony Service Provider
10
5
Internet
PSTN/ISDN
6
7
8
Home-Office
4
File Server
Call Server/IP-PBX
3
9
Cables, Hubs,
switches, …
PSTN-Gateway
2
1
Headquarter

Angriffe von Innen

- Verbotenes Mithören
  - HUB
  - WLAN – WEP, WPA, WPA-2
  - ARP-Spoofing, Man-in-the-Middle-Attack -› Switched Ethernet hilft nicht
  - TFTP-Angriffe auf IP-Telefone, Veränderung der Konfiguration
- Ausspähen von Verbindungsdaten (Call Detail Records)
  - Zugriff/Veränderungen auf die Datenbank der IP-PBX
- Gebührenmissbrauch
  - Weiterleitung zu externen Zielen
- Unberechtigtes Nutzen von Diensten
  - Wahl von 0900-Nummern
- Vortäuschung falscher Identitäten
  - Roaming Users - Hot-Desking
  - Verschleierung von unberechtigter Nutzung

Angriffe von Außen

- Caller-ID Spoofing, Vortäuschung fremder Rufnummern
  - Rufnummernidentifizierung nicht sicher (Gilt auch im ISDN!!)
  - Unzulässige Abfrage von Voicemail (Remote Inquiry)

- Allgemeine Angriffe auf die Daten Infrastruktur
  - Ausspähen von Verbindungsdaten (Call Detail Records)
  - Zugriff auf die Datenbank der IP-PBX

Denial of Service - allgemein

- Unterbrechung der Betriebsfähigkeit durch Denial-of-service (DOS) attacks
  - Angriffspunkte: IP-PBX (=Telefonserver)
  - Dienste wie HTTP, SNMP und Telnet sind anfällig
  - TCP/IP Stack ganz allgemein
  - Fluten mit SYN- oder mit ICMP-Paketen
  - Die Angriffe sind identisch zu allen herkömmlichen DoS Angriffen gegen Server und Arbeitsplatz PC
  - Auch die Tools und die Angriffstechniken sind die Gleichen

Denial of Service – VoIP spezifisch

- Neu und VoIP spezifisch sind die DOS Angriffe gegen IP Telefone
- Cisco dokumentiert dies in: „Cisco Security Advisory, Multiple Vulnerabilities in Cisco IP Telephones“

- Fluten des Call Contol (Port 1720 oder 5060) mit Verbindungsaufbaupaketen

- DoS gegen den Medienstrom ist ein VoIP spezifisches Problem
  Die Sprachübertragung wird von jedem Angriff beeinträchtigt, der das Netzwerk verstopft oder die QoS Parameter beeinflusst

VoIP Gefahrenpotential

- Sprachpakete werden unverschlüsselt übertragen
- Über frei verfügbare Tools können Pakete mitgeschnitten und in Audioformat umgewandelt werden
- Pakete zur Steuerung der Verbindung sind auch unverschlüsselt
- SPAM/SPIT
- Spoofing, vortäuschen falscher Identitäten für mögliche Phishing- Zwecke
- Malformed Messages können Dos-Attacken auslösen
- Registration Hijacking -- wo starke Authentifizierung fehlt, massenweise Umleitung von Rufnummern oder DoS-Attacken
- Session Initiation Protocol (SIP) Angriffe auf Protokollebene

- Fazit:
- Sicherheit und Verfügbarkeit hängen eng zusammmen
- Sicherheit und Bandbreite sind gleichwertig zu sehen um Telefonie in Echtzeit zu führen
- Generell gilt: je stabiler und sicherer das Datennetz desto besser funktioniert die zusätzliche Anforderung für VoIP

Verschlüsselung
Call Control und/oder Sprachdaten

Security of H.323 versus SIP

- Aus Sicherheitsaspekten sind beide Protokolle gleichwertig
- Sowohl H.323 als auch SIP bieten Authentifikation als auch Verschlüsselung
- Sie sind beide gleich anfällig gegen DoS Angriffe
  Angriffe auf Call Control Kommunikation (Port 1720 bzw. 5060)
- beide Protokolle nutzen RTP zur Übertragung der Sprachdaten
  RTP steht für Real Time Protocol und nutzt UDP/IP

H.235: Security and encryption for H.323 multimedia terminals

- H.235 spezifiziert die Sicherheitsmchanismen in H.323 Systemen

TLS: Transport-Layer Security

- Genutzt zur Sicherung von SIP Call Control Nachrichten

RTP: Real-Time Transport Protocol

- RTP spezifiziert die Übertragung von Echtzeitdaten via UDP
- Genutzt in allen VoIP Systemen, unabhängig vom Signalisierungsprotokoll

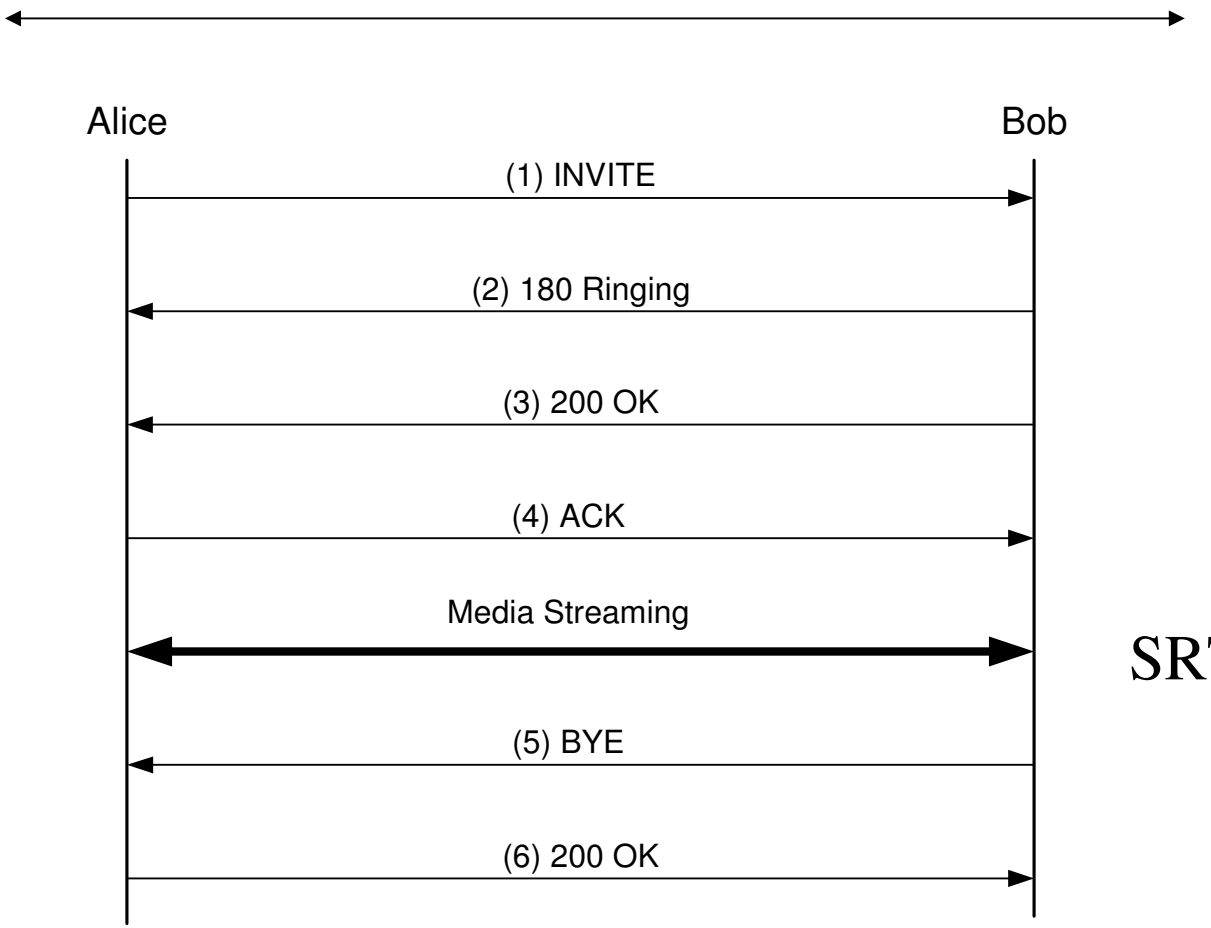
RTCP: Real-Time Control Protocol

- Erweitert RTP um Monitoring Funktionen
- QoS quality of service
- Überprüfung der Übertragungsqualität

SRTP: Secure Real-Time Protocol

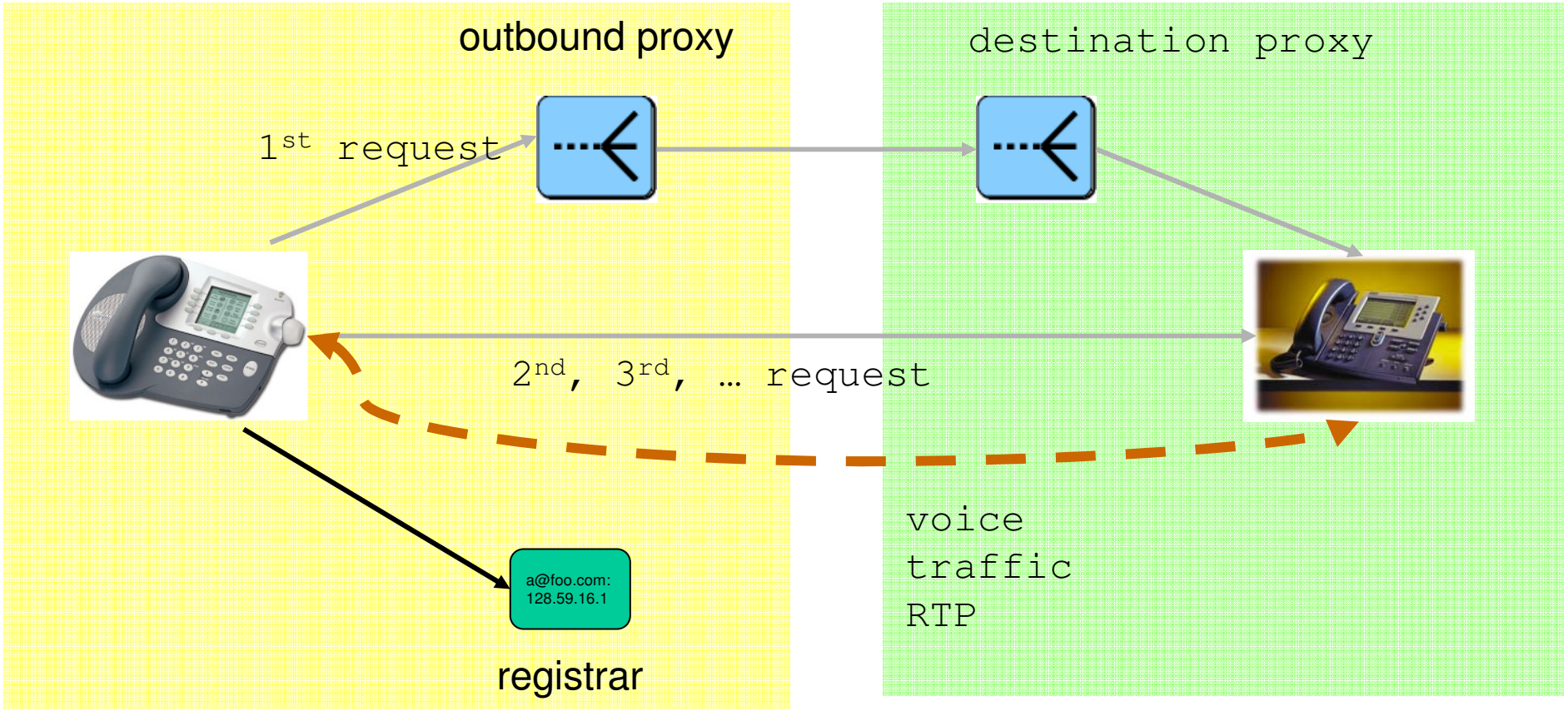
- Erweitert RTP um Verschlüsselungseigenschaften
- Gibt es auch als SRTCP

TLS-Session



SRTP

SIP trapezoid



TLS

- TLS 1.0 gilt als sicheres, etabliertes Protokoll
- Viele, teilweise freie Implementierungen verfügbar
- Basiert auf Zertifikaten
- Nur Sicherheit zwischen je 2 benachbarten Hops
- Keine echte Ende-zu-Ende Sicherheit erreichbar
- Kein sicheres „Feedback“, der den beteiligten Endgeräten bestätigt, dass alle Hops gesichert sind
- Der rufende Client kann nicht sicher sein, dass zwischen allen Hops TLS verwendet wird, obwohl er SIPS verwendet
- Der gerufene Client, der einen SIPS Request empfängt kann nicht sicher sein, dass alle Hops gesichert sind, weil ein Angreifer einen SIP Request zu einem SIPS Request umwandeln kann, um der gerufenen UA eine „sichere Verbindung“ vorzutäuschen

SRTP - Secure Real-Time-Transport Protocol

SRTP stellt folgende Sicherheitsfunktionen zur Verfügung um eine vertrauliche Übertragung zu realisieren:

- Die Verschlüsselung der Sprachübertragung schützt vor unbefugtem Abhören
- Die Authentifizierung des Absenders unterbindet Identitäts-Spoofing
- Mit der Überprüfung der Integrität werden unberechtigte Änderungen ausgeschlossen
- Mit dem Anti-Replay-Schutz wird ein unbefugter Zugriff auf Ziel-End-Einrichtungen verhindert
- symmetrischen Verschlüsselung nach AES (Advanced Encryption Standard) verschlüsselt
- Problem Schlüsselaustausch

VoIP – SPAM
SPIT

Welche Typen gibt es?

- SPIT = SPAM in Internet Telephony

- Call Spam
  - Unerwünschte Anrufe, Abspielen von Werbebotschaften
  - Klassisches Vorgehen der Telemarketer, jetzt via VoIP

- Instant Message Spam
  - Vergleichbar mit klassischer SPAM via Email
  - Nutzung von Instant Messages zur Lieferung von unerwünschten Nachrichten

- Presence Spam
  - Hierbei wird versucht durch entsprechene Anfragen auf die Buddy List zu kommen
  - Danach kann IM Spam erfolgreich eingesetzt werden

Wird es SPIT geben ?

- Wird es SPIT geben – klares JA
  - Eigentlich nichts Neues – verbotene Kalt-Aquise der Telemarketers
  - Nur eine Frage des Preises
  - Die Kosten pro Anruf werden dramatisch sinken, speziell aus dem Ausland
  - Der Effekt ist besser als SPAM, da Filter versagen

	PSTN	VoIP
Anschluss	S2m 300€/Monat	ADSL 1500/384 kBit/s 30€/flat rate
Kanäle	30	4 (unkomprimiert) 18 (komprimiert)
Anrufversuche pro Minute	180	›1000, da kein Kanalreservierung nötig
Kosten pro erfolgreichen Anruf	1-6 ct	0 ct !!!

Was müssen die Hersteller, die Provider und die Anwender tun?

Maßnahmen (1)

1. Immer nur geswitchte LAN-Infrastruktur nutzen
   - Hubs vermeiden
   - WLAN immer verschlüsseln, WPA, WPA-2 nutzen
2. VLANs können Sprach- und Datenströme und Endgeräte trennen
   - Nicht möglich bei Softphones
3. Hersteller müssen Geräte mit standardkonformer Verschlüsselung bieten
   - Call Control via TLS oder SIPS oder H.235 verschlüsseln
   - Sprachstrom via SRTP verschlüsseln
   - Speziell bei Verbindungen über das Internet – Alternative IPSec VPN
4. Kunden müssen ihre Kaufentscheidungen nach Sicherheitsaspekten ausrichten
   - Derzeit spielen hauptsächlich Funktion und Preis eine Rolle
   - Die Kunden wollen alle Leistungsmerkmale der klassischen TK-Anlagen

Maßnahmen (2)

5. Jeder VoIP Server (SIP-Proxy, etc.) muss sorgfältig gesichert werden
   - Die umfangreichen Möglichkeiten Nutzer- und Verbindungsdaten zu speichern, müssen angemessen und verantwortungsbewusst genutzt werden
   - Speicherung der Daten in Encrypted File System (EFS)
6. VoIP brauchen Redundanz
   - In Datennetzen sind die Nutzer an Unterbrechungen gewöhnt
   - Im Telefoniebereich ist dies nicht akzeptabel
   - Besonders die Notruffähigkeit (110/112) muss sichergestellt werden
7. Die (eigentlich) selbstverständlichen Sicherheitsmaßnahmen treffen
   - Aktuelle Security Patches nutzen
   - Ungenutzte Ports schließen
   - Dezidierte Server nutzen
   - Verschiedene Administrationsebenen nutzen
   - Passwörter sicher speichern und komplexe Passwörter erzwingen

Maßnahmen (3)

8. Default login Accounts sperren
   - Dabei nicht die IP-Telefone vergessen
   - Reset auf Factory-Einstellungen nur mit Passwort
9. Management Traffic (z.B. Billing Information) kann zusätzlich noch verschlüsselt werden
10. Kritische Bedrohungen müssen regelmäßig identifiziert werden
    - Security Audits von externen Dienstleistern durchführen lassen
11. Im WAN Bereich (Internet) immer verschlüsseln, z.B. per IPSec VPN
12. Die VoIP Provider (ITSP) müssen Business Angebote machen
    - Verschlüsselung der Verbindungsdaten und der Sprache anbieten

Demonstration eines SIP Calls
Mithören leicht möglich

Fragen?