



DIGICOMP

Drive your life.



Voice over IP

(Un-) Sicherheit

Referent

- Michael A. Birrer
- Head of Voice Solutions bei green.ch
- Beratung & Projektmanagement für VoIP Lösungen beim VBS

Definition

■ BEKANNTE BEGRIFFE

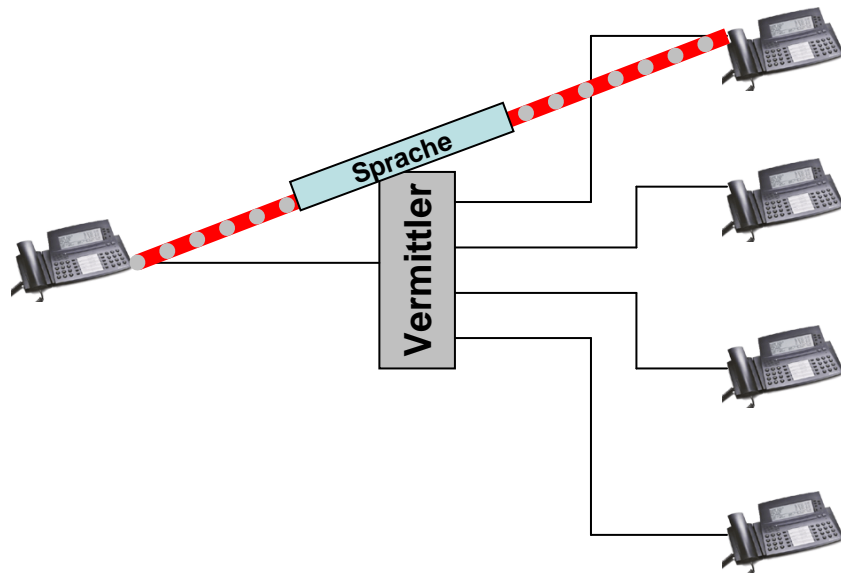
- Skype
- gratis!
- Sip
- MSN
- H.323
- T.38
- Computer
- Asterisk
- Internet-Telefonie
- ...

VoIP ist
Übertragung von Sprache über
paketvermittelte Datennetze

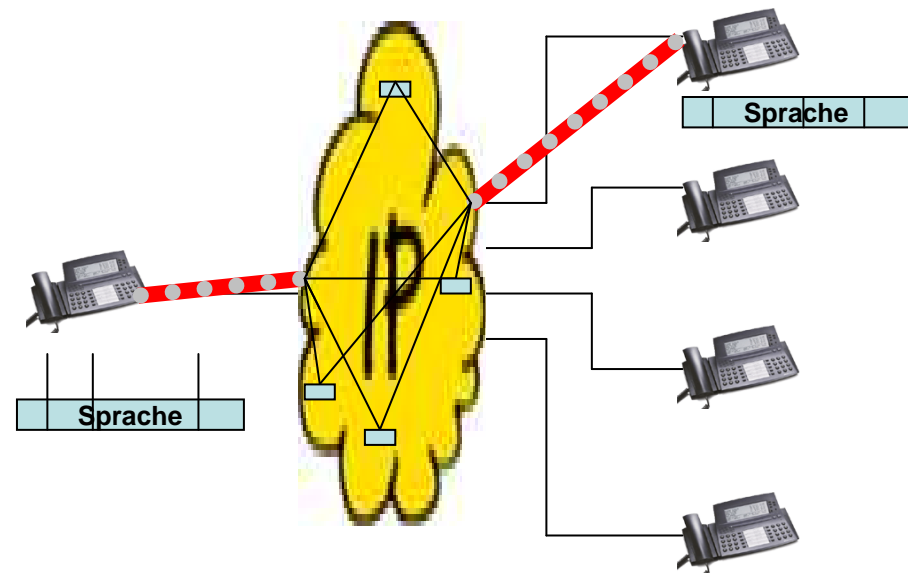
Quelle: Bakom

Vermittlung

„Leitungs-vermittelt“



„Paket-vermittelt“



Protokolle I

Signalisierungs-Protokoll *(Steuerungsprotokoll)*



- Authentication
- Codec
- Actions (Ring, Hangup, ...)

(Sprach)Transport-Protokoll



- Transport of Data

Protokolle II

Signalisierungs-Protokoll *(Steuerprotokoll)*

SIP [Session Initiation Protocol]
(plaintext) TCP

H.323
(based on ISDN, binary) TCP

(Sprach)Transport-Protokoll

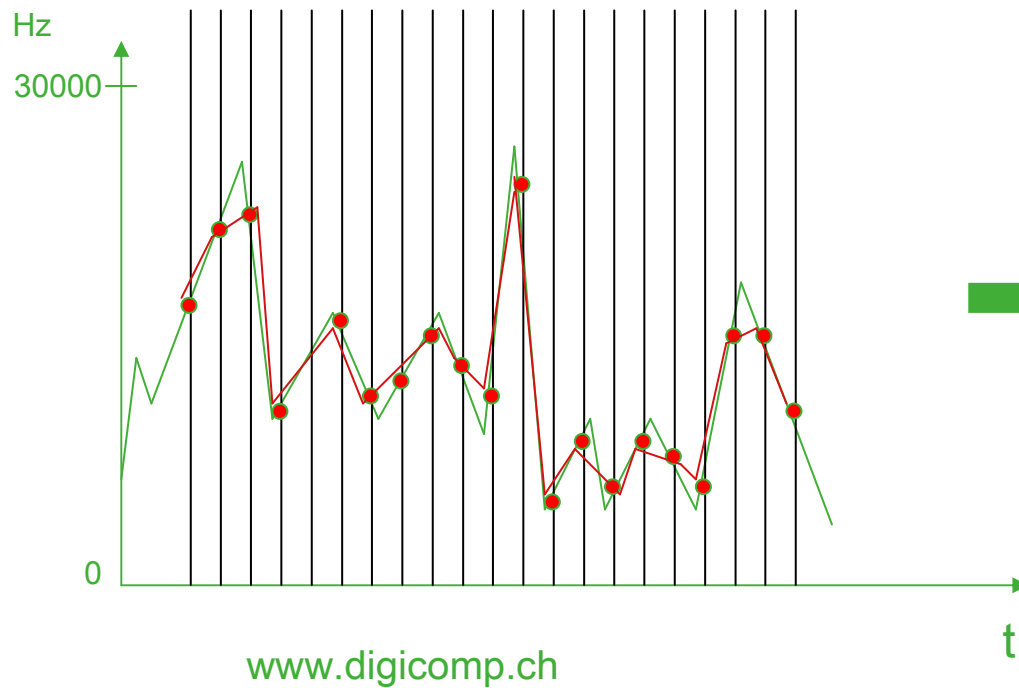
RTP [Realtime Transport Protocol] UDP

IAX [Inter Asterisk eXchange]
TCP & UDP

Codec

G.711 64 Kbits/s
G.726 32 Kbits/s
G.729 8 Kbits/s

gsm 13 Kbits/s



Paketierung

Gespräch I - Grundsatz

1. Einladung



2. Akzeptiert



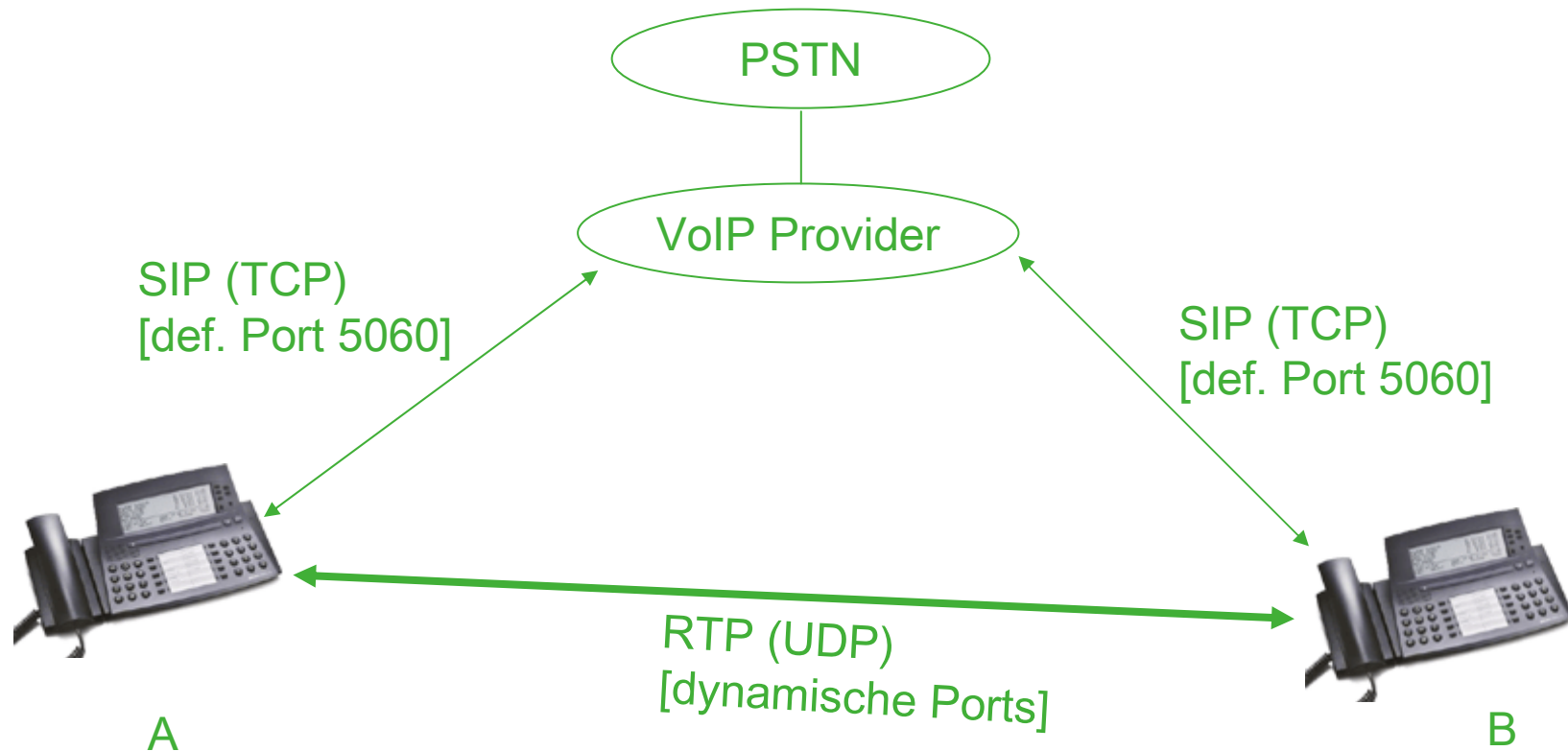
3. Gespräch



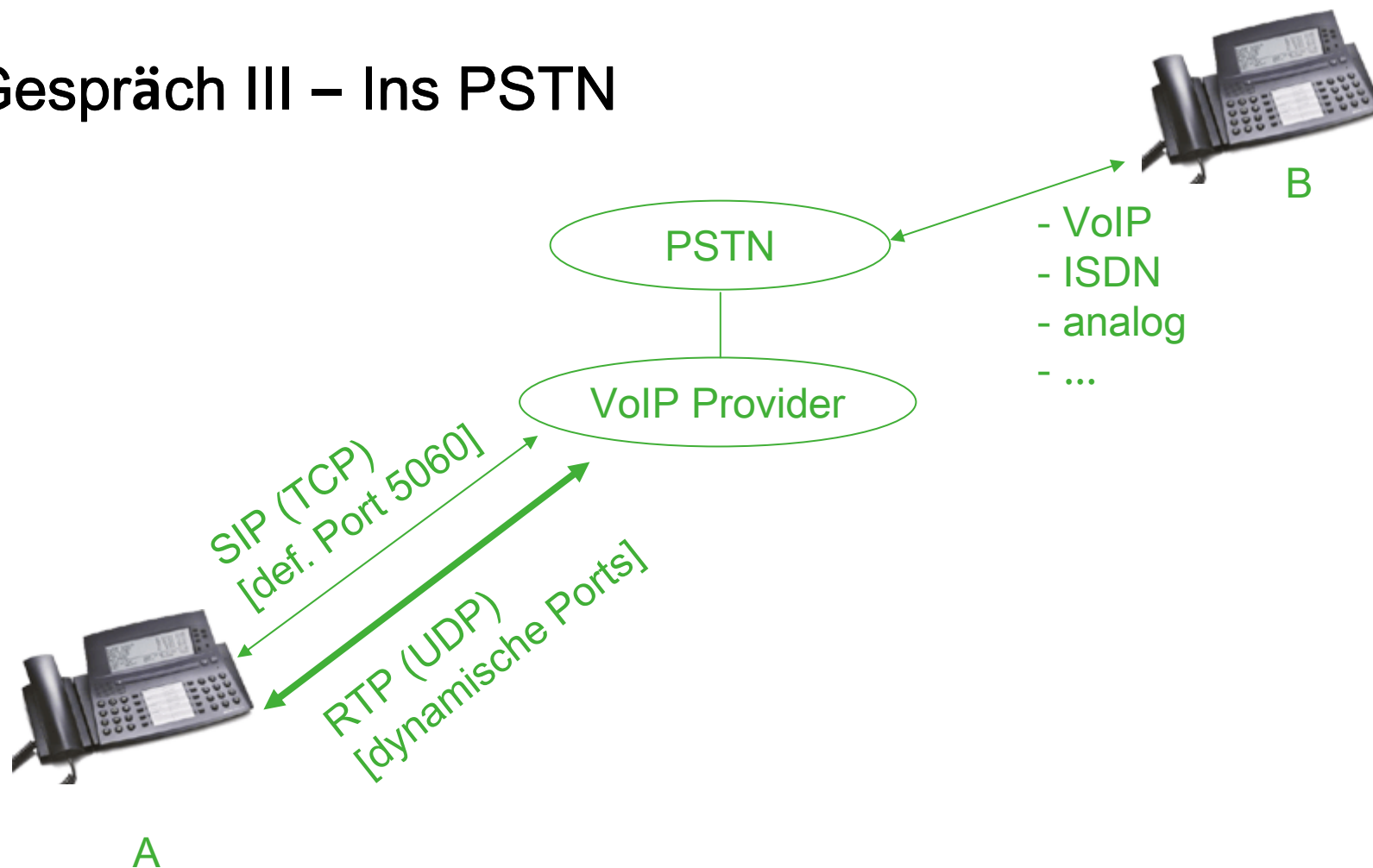
4. Bye



Gespräch II – Innerhalb des selben VoIP-Netzes



Gespräch III – Ins PSTN



MOS

- 5 excellent
- 4 gut
- 3 akzeptabel
- 2 dürftig
- 1 unbrauchbar

MOS > 3.5 =>

minimum für business
taugliche VoIP Lösung

QoS – Quality of Services, oder eben nicht... I

Delay (Latenz, Verzögerung)

Latenzzeit = Codierungszeit + Übertragungszeit + Decodierungszeit

- Traditionelles Festnetz P-P maximal 25ms
- Delay über 120ms für VoIP schwierig, ab 200ms unbrauchbar

Jitter

Unterschiede des Delays innerhalb eines Streams

- Auf Kosten des Delays wird oft ein JitterBuffer verwendet

QoS – Quality of Services, oder eben nicht... II

Paket Loss

- Bereits ab 1% Paketverlust kann das Gespräch unbrauchbar sein

Echo

Seine eigenen Worte nach geringer Zeit wieder hören
- Meistens durch „qualitativ schlechte“ Endgeräte verursacht.

Angriffsziele eines „VoIP-Systems“ I

Verfügbarkeit

Netzwerk, Endgeräte, VoIP Provider, ...

Integrität

Fälschung der Absender Tel Nummer

Änderung von „Header Informationen“ des Signalisierungsprotokolls

Vertraulichkeit

Abhören von Gesprächen

Rausholen der Login Daten

Angriffsziele eines „VoIP-Systems“ II

Aktive oder Passive Angreifer!

Software der Endgeräte

Ascotel AIMS, Aastra Endgeräte
Skype, MSN, X-Lite, SnomPhones

Netzwerkkommunikation

Kabel, Switch, Router, Firewalls,

Beispiele:

- DoS Attacken
- Man in the Middle
- ...

Bedrohung / Schutzmassnahmen Layer 1

Schutz der Hardware

Verkabelungen, Server, PBX, Serverraum,
=> Zutrittskontrollen? Raumsicherheit? -> Kafiraum = Serverraum

Der Benutzer!

Stimme, Wanzen, ...
=> Eigenverantwortung?

Bedrohung / Schutzmassnahmen Layer 2

MAC Spoofing

=> Senden von gefälschter ZielMAC an Switch. Alle Pakete kommen nun zu Spoofer

MAC Flooding

=> Gernerieren von sovielen MAC-Einträgen, dass Speicher des Switchs überläuft und alle Frames an alle gesendet werden.

Bedrohung / Schutzmassnahmen Layer 2

MAC Spoofing

=> Senden von gefälschter ZielMAC an Switch. Alle Pakete kommen nun zu Spoofer

MAC Flooding

=> Generieren von sovielen MAC-Einträgen, dass Speicher des Switchs überläuft und alle Frames an alle gesendet werden.

ARP Spoofing

=> Wie MAC Spoofing, jedoch zwischen MAC <> IP Adresse

Bedrohung / Schutzmassnahmen Layer 3

IP Spoofing

=> Vorgaukeln einer „falschen“ IP Adresse und somit den Traffic erhalten zum Missbrauch

DHCP Server

=> Parameter werden an Clients vergeben und entsprechend kann ein Endclient eine bestimmter Konfig runterladen!

Ping Flood

=> CPU, Memory etc eines Routers in die Knie zwingen!

Bedrohung / Schutzmassnahmen Layer 4

SYN Flood

=> Auslasten des Endsystems mit vielen Verbindungs-Anfragen

LAND Flood

=> Ziel und Quell IP sind gleich, somit sendet jedes Received Paket eine Antwort an sich selbst...

Auswirkungen von Angriffen auf das VoIP System

Umleiten / Man in the middle bei Gesprächen:

- Abhören der Gespräche (Vertraulichkeit)
- Missbrauch der Gebühreninfos (Integrität)

Killen der physikalischen Medien

- Betriebsprozess-Störungen

Beeinflussung der Systeme

- Schlechte Gesprächsqualität (Verfügbarkeit)
- Teilausfälle der Systeme

Auswirkungen von Angriffen auf das VoIP System

Umleiten / Man in the middle bei Gesprächen:

- Abhören der Gespräche (Vertraulichkeit)
- Missbrauch der Gebühreninfos (Integrität)

Killen der physikalischen Medien

- Betriebsprozess-Störungen

Beeinflussung der Systeme

- Schlechte Gesprächsqualität (Verfügbarkeit)
- Teilausfälle der Systeme

DEMO

X-Lite

SIP Gespräch

Skype

Skype Gespräch

ZIELE:

- Zugangsdaten rausholen
- Gespräch abhören und speichern