VoIP

Sicher und sorgenfrei

10.12.2009 Thomas Gelf <thomas.gelf@raiffeisen.it>

RaiffeisenOnline

Dieser Vortrag wird nicht...

- Alle VoIP-Probleme lösen können
- IPv6 einführen
- NAT abschaffen
- Die Welt so schön machen, wie die Autoren von RFC3261 sie offensichtlich sahen
- Jeden glücklich machen...
- ...aber vielleicht den ein oder anderen ;-)

Dieser Vortrag soll...

- Grundwissen vermitteln
- Häufige Stolperfallen erklären
- Mit verbreiteten Irrtümern aufräumen
- Klassische NAT-Probleme erörtern
- Tipps zur Konfiguration geben

Zwischenfragen...

...sind willkommen!

Raiffeisen OnLine?

- Klassischer ISP in Südtirol (Italien) seit 1997
- Gehört zur Bankengruppe, ist aber eigenständige Genossenschaft
- VoIP-Provider seit 2005
- Immer noch einziger Südtiroler SIP-Provider

Kurzer Rückblick

- Erste VoIP-Gespräche
  - 1973: Erste digitale Sprachübertragung im Arpanet
  - 1995: Erste Software für Windows
  - 1996: QuickTime Conferencing, RTP (RFC 1889)
- 1998: H.323 - ITU-T
- 1999: SIP - IETF
- 2002: RFC 3261
- 2004: Skype

RTP – Real-Time Transport Protocol

- RFC 1889 (1996), RFC 3550 (2003)
- Statische und dynamische Payload-Typen
  - RFC 3551
- Übermittelt Sprach- und Videodaten
- IP:Port anzurufen ist nicht sehr intuitiv
- Deshalb wurde SIP erfunden

SIP – Session Initiation Protocol

- Aufbau, Steuerung und Abbau von Kommunikations-Sitzungen (Sessions)
- Kann prinzipiell Sessions jeglicher Art signalisieren
  - Am häufigsten: Audio und Video
  - Aber auch: Multiplayer-Games
- RFC 2543 (1999)
- Abgelöst durch RFC 3261 (2002)

Welche Protokolle muss ich kennen?

- H.323, Skinny und IAX werden nicht so schnell verschwinden, aber:
- SIP hat die Schlacht für sich entschieden
- SIP zu verstehen bedeutet aber auch:
  - SDP, RTP, STUN...
  - Codecs: G.711, G.729, iLBC, GSM, G.722...
  - T.38, UDPTL
  - uvm

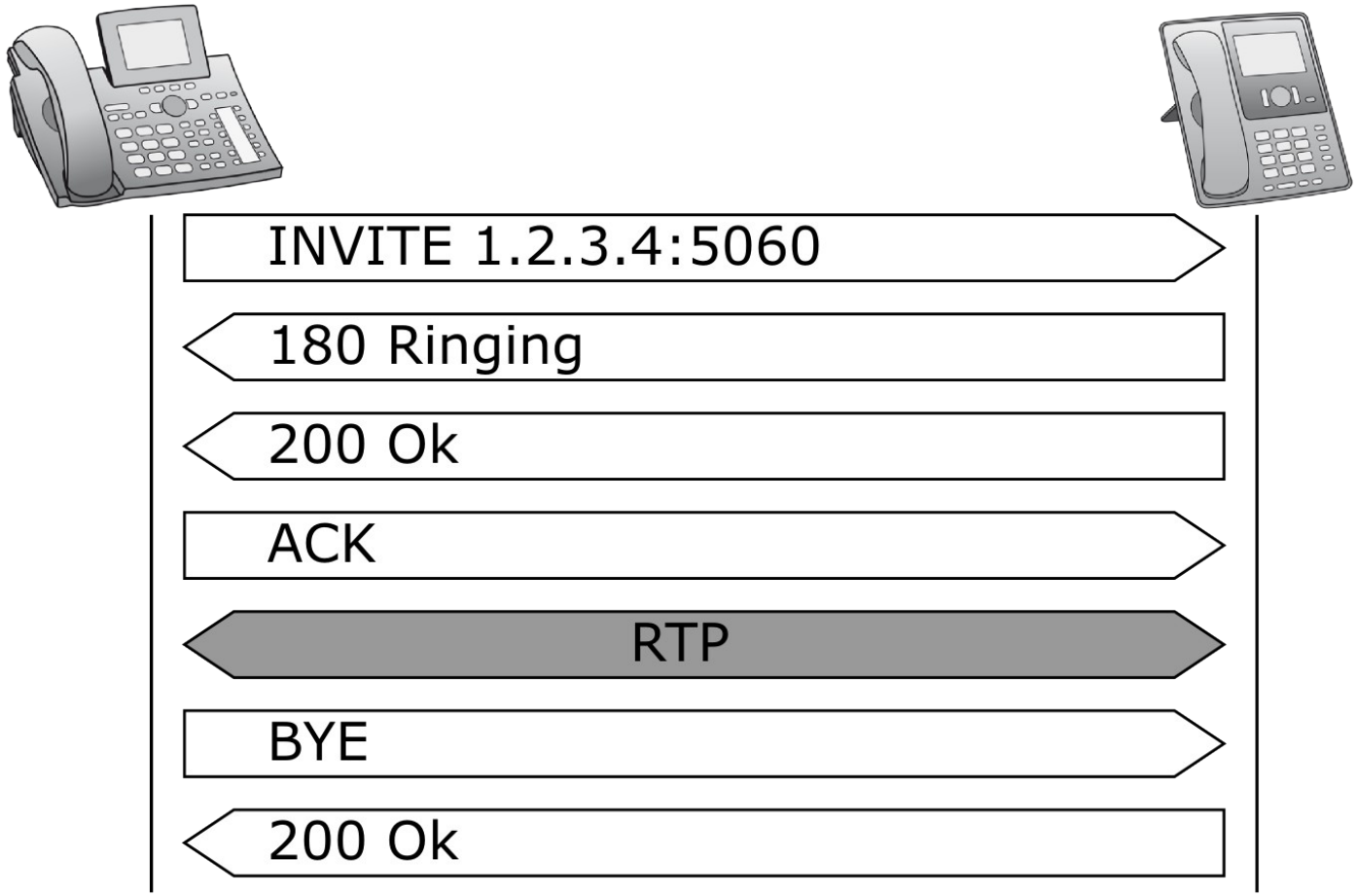
Blick nach vorne

- 3GPP, IMS?
- Bald von Realität überholt?
- P2P SIP?
- Man darf gespannt sein!
- Sicher ist bloß: SIP gehört die Zukunft ;-)

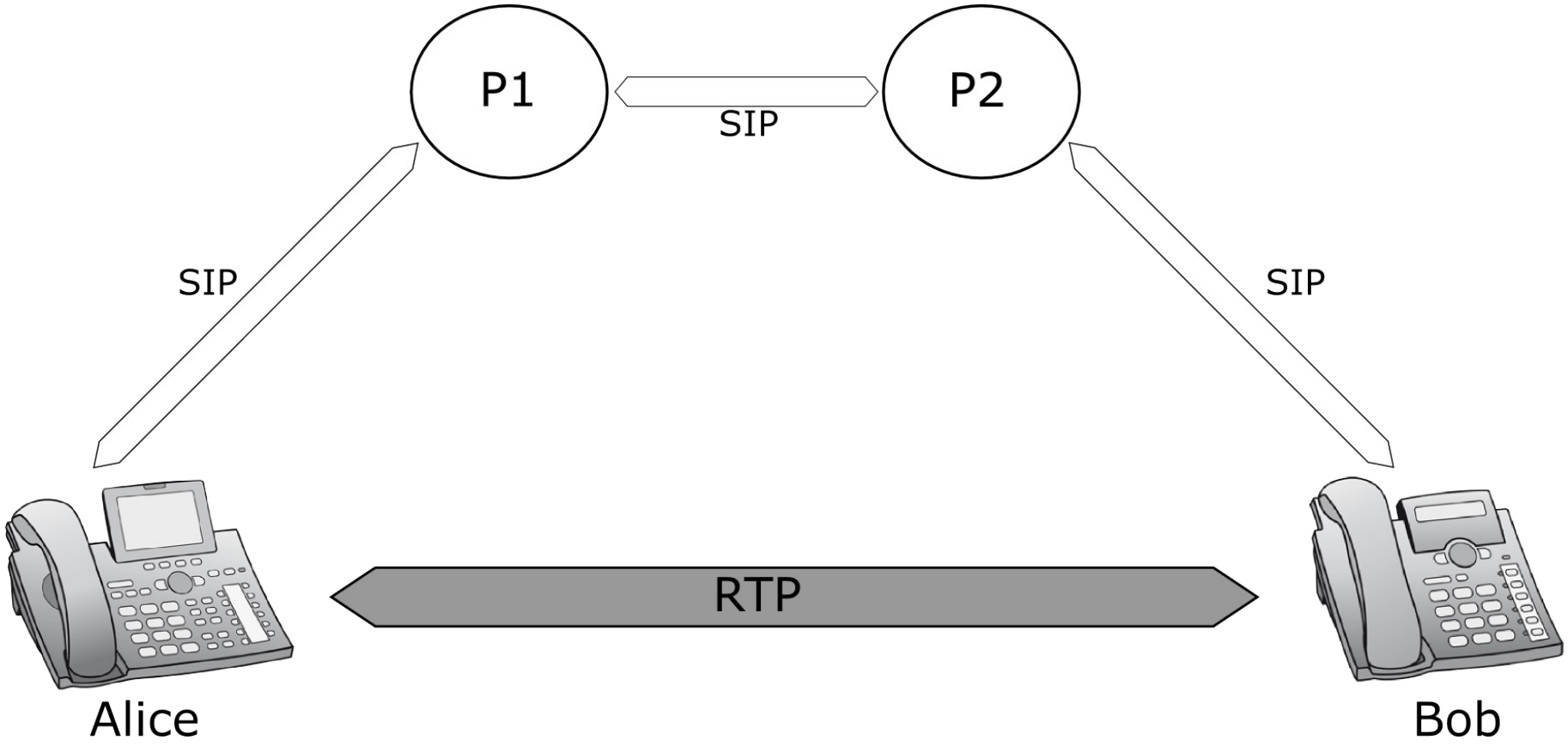
Wie sieht SIP aus?

- Wie ein Mix aus HTTP- und Mailheader
- Textform
- Nachteil:
  - Größere Pakete
  - Text-Parser erforderlich
- Vorteil:
  - Für Mensch einfach lesbar (Debugging!)
  - Erprobte Bibliotheken

SIP-Flow mal ganz einfach



SIP Trapezoid



SIP-Paket

```
Session Initiation Protocol
  Request-Line: INVITE sip:marc[illegible]co@195.2[illegible]4:62315;line=45080 SIP/2.0
  Message Header
    Record-Route: <sip:195.[illegible]219;lr;ftag=E9BA8EBC-1DC8;rdlg=072.b87843d6>
    Record-Route: <sip:83.[illegible].21;ftag=E9BA8EBC-1DC8;lr=on>
    Via: SIP/2.0/UDP 195.2[illegible].219;branch=z9hG4bK341b.2d955ff.0
    Via: SIP/2.0/UDP 83.[illegible].21;rport=5060;received=8[illegible]1;branch=z9hG4bK341b.0d98c064.0
    Via: SIP/2.0/UDP  195.[illegible]18:5060;rport=61931;x-route-tag="tgrp:Slot7";branch=z9hG4bK40E3561853
    From: <sip:047120[illegible]@195.[illegible]18>;tag=E9BA8EBC-1DC8
    To: <sip:0471[illegible]t>
    Call-ID: FFA5A399-B71811DE-93518D39-BE5F5BC8@195.[illegible]18
    CSeq: 101 INVITE
    Max-Forwards: 8
    Remote-Party-ID: <sip:047120[illegible]8>;party=calling;screen=yes;privacy=off
    Contact: <sip:0471204[illegible]@195.[illegible]8:5060>
    Expires: 180
    Allow-Events: telephone-event
    Content-Type: application/sdp
    Content-Length: 327
  Message Body
```

Wichtigste Header

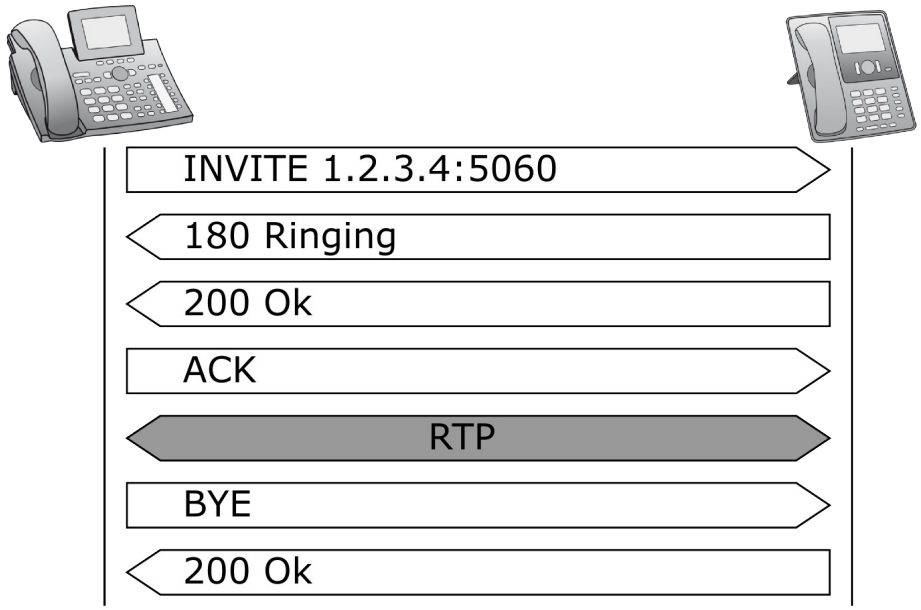
- From / To (Tags!)
- Call-ID
- Record-Route
- Via
- Contact

Durch SIP definierte Rollen

- User Agent (UAS / UAC)
- Proxy Server
- Registrar Server
- Location Server
- Redirect Server
- Gateways (B2BUA, SBCs)

Request / Response

- Unterschied zu HTTP:
  - Mehrere Responses pro Request möglich
- Ein Proxy kann sein:
  - Stateless
  - Transaction stateful
  - Dialog stateful



Die wichtigsten SIP-Methoden / -Requests

- INVITE – eine Sitzung anfragen
- ACK – finale Antwort auf eine Sitzungsanfrage
- OPTIONS – Eigenschaften abfragen
- CANCEL – aktiven Request abbrechen
- BYE – Sitzung beenden
- REGISTER – Informationen zur eigenen Erreichbarkeit hinterlegen

SIP-Responses

- 1xx - Provisional (100 Trying, 180 Ringing)
- 2xx - Success (200 Ok)
- 3xx - Redirection (302 Moved Temporarily)
- 4xx - Client Error (404 Not found)
- 5xx - Server Error (500 Internal Server Error)
- 6xx - Global Failure (603 Decline)

Authentifizierung, Beispiel REGISTER

- Client sendet REGISTER, Proxy antwortet

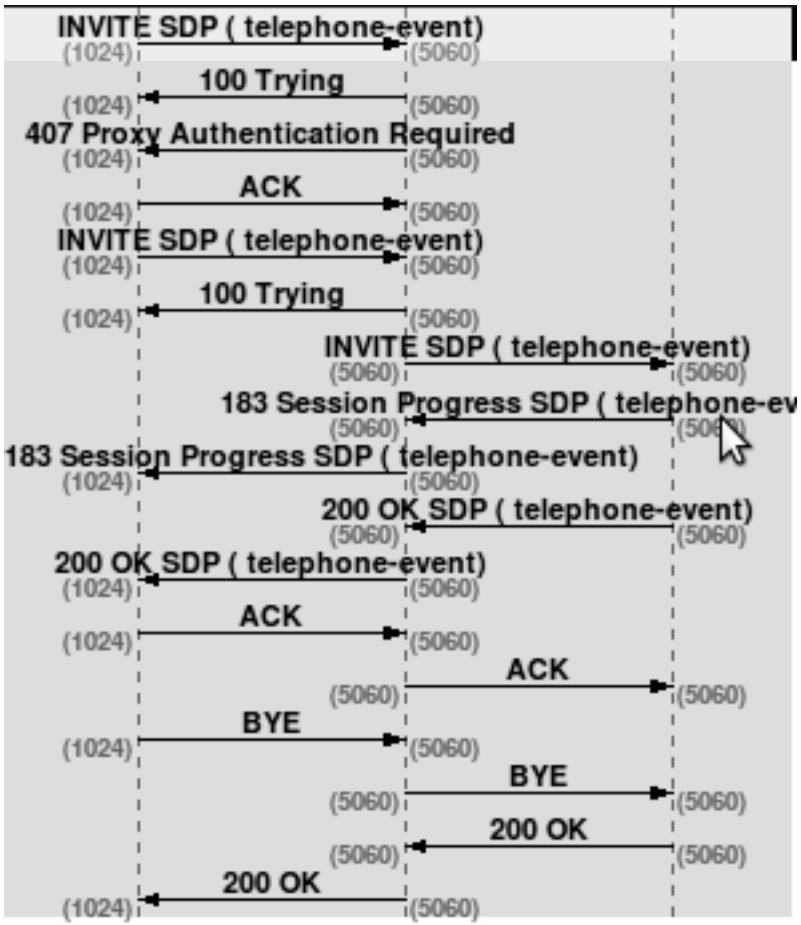
```
401 Unauthorized
WWW-Authenticate: Digest realm="domain.tld",
nonce="4ac...6bd"
```

- Client benutzt diese Challenge, antwortet

```
Authorization: Digest username="user1",
realm="domain.tld", algorithm=MD5,
uri="sip:domain.tld", nonce="4ac...6bd",
response="6df...321"
```

SIP-Flow mit einem Proxy

- Proxy zwingt Retour-Pakete, ebenfalls durch den Proxy zu wandern
- Er macht dies mit Record-Route Headern



Record-Route – INVITE (Proxy 1)

```
Session Initiation Protocol
  Request-Line: INVITE sip:047118[redacted]@195[redacted]19 SIP/2.0
  Message Header
    Record-Route: <sip:83[redacted]1;ftag=E9BA8EBC-1DC8;lr=on>
    Via: SIP/2.0/UDP 83.[redacted]21;branch=z9hG4bK341b.0d98c064.0
    Via: SIP/2.0/UDP  195.[redacted]18:5060;rport=61931;x-route-tag="tgrp:Slot7";branch=z9hG4bK40E3561853
    From: <sip:047120[redacted]@195[redacted]18>;tag=E9BA8EBC-1DC8
    To: <sip:047118[redacted]7@v[redacted]t>
    Call-ID: FFA5A399-B71811DE-93518D39-BE5F5BC8@195[redacted]18
    User-Agent: Cisco-SIPGateway/IOS-12.x
    CSeq: 101 INVITE
    Max-Forwards: 9
    Remote-Party-ID: <sip:047120[redacted]3@195[redacted]8>;party=calling;screen=yes;privacy=off
    Contact: <sip:047120[redacted]@195[redacted]18:5060>
    Expires: 180
    Allow-Events: telephone-event
    Content-Type: application/sdp
    Content-Length: 414
  Message Body
```

Record-Route – INVITE (Proxy 2)

```
Session Initiation Protocol
  Request-Line: INVITE sip:marc[...]co@195.2[...]4:62315;line=45080 SIP/2.0
  Message Header
    Record-Route: <sip:195.[...]219;lr;ftag=E9BA8EBC-1DC8;rdlg=072.b87843d6>
    Record-Route: <sip:83.[...].21;ftag=E9BA8EBC-1DC8;lr=on>
    Via: SIP/2.0/UDP 195.2[...].219;branch=z9hG4bK341b.2d955ff.0
    Via: SIP/2.0/UDP 83.[...].21;rport=5060;received=8[...]1;branch=z9hG4bK341b.0d98c064.0
    Via: SIP/2.0/UDP  195.[...]18:5060;rport=61931;x-route-tag="tgrp:Slot7";branch=z9hG4bK40E3561853
    From: <sip:047120[...]@195.[...]18>;tag=E9BA8EBC-1DC8
    To: <sip:0471180[...]t>
    Call-ID: FFA5A399-B71811DE-93518D39-BE5F5BC8@195.[...]18
    CSeq: 101 INVITE
    Max-Forwards: 8
    Remote-Party-ID: <sip:047120[...]8>;party=calling;screen=yes;privacy=off
    Contact: <sip:0471204[...]@195.[...]8:5060>
    Expires: 180
    Allow-Events: telephone-event
    Content-Type: application/sdp
    Content-Length: 327
  Message Body
```

Record-Route – Reply (200 Ok)

```
Session Initiation Protocol
  Status-Line: SIP/2.0 200 OK
  Message Header
    Via: SIP/2.0/UDP 195.[redacted].219;branch=z9hG4bK341b.2d955ff.0
    Via: SIP/2.0/UDP 83.[redacted].21;rport=5060;received=83.[redacted]21;branch=z9hG4bK341b.0d98c064.0
    Via: SIP/2.0/UDP  195.[redacted].18:5060;rport=61931;x-route-tag="tgrp:Slot7";branch=z9hG4bK40E3561853
    Max-Forwards: 70
    From: <sip:04712[redacted]@1[redacted].18>;tag=E9BA8EBC-1DC8
    To: <sip:04711[redacted]@v[redacted]t>;tag=q0a5..3
    Call-ID: FFA5A399-B71811DE-93518D39-BE5F5BC8@195.[redacted].18
    CSeq: 101 INVITE
    Contact: <sip:marc[redacted]co@195.[redacted]34:62315;line=45080>
    Accept: application/sdp
    Allow: INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, REFER, SUBSCRIBE, NOTIFY, MESSAGE, INFO, PRACK
    Content-Disposition: session
    Record-Route: <sip:195.[redacted]219;lr;ftag=E9BA8EBC-1DC8;rdlg=072.b87843d6>,<sip:83.[redacted]21;ftag=E9BA8EBC-1DC8;lr=on>
    User-Agent: snom-m3-SIP/02.02 (MAC=00041[redacted]5; HW=1)
    Content-Type: application/sdp
    Content-Length: 290
  Message Body
```

SDP – Session Description Protocol

- Ursprünglich definiert in RFC 2327
- Media-Typ: Audio, Video...
- Transport-Protokoll: RTP,UDP,IP,UDPTL,H.320...
- Medien-Format / Codec: G.711, H.264...
- Informationen, wo und wie man diese(n) Stream(s) empfangen will (Adressen, Ports...)

SDP - Beispiel

```
Session Description Protocol
  Session Description Protocol Version (v): 0
  Owner/Creator, Session Id (o): user 7928335 7928335 IN IP4 195.25[redacted]
  Session Name (s): call
  Connection Information (c): IN IP4 195.254[redacted]
  Time Description, active time (t): 1254925263 1254928863
  Media Description, name and address (m): audio 7078 RTP/AVP 8 0 2 102 100 99 97 18 101
  Media Attribute (a): sendrecv
  Media Attribute (a): rtpmap:2 G726-32/8000
  Media Attribute (a): rtpmap:102 G726-32/8000
  Media Attribute (a): rtpmap:100 G726-40/8000
  Media Attribute (a): rtpmap:99 G726-24/8000
  Media Attribute (a): rtpmap:97 iLBC/8000
  Media Attribute (a): fmtp:97 mode=30
  Media Attribute (a): rtpmap:101 telephone-event/8000
  Media Attribute (a): fmtp:101 0-11
  Media Attribute (a): rtcp:7079
```

Der NATürliche Feind

- NAT ist für einige Experten:
  - Ein Geschenk des Himmels
  - Ein Sicherheits- und/oder Privacy-Feature
- Und für andere:
  - Das Schlimmste, was dem Netz je passiert ist
- Für SIP
  - War und ist NAT eines der größten Probleme...
  - ...jedenfalls so lange man es nicht verstanden hat

Wie äußern sich NAT-Probleme?

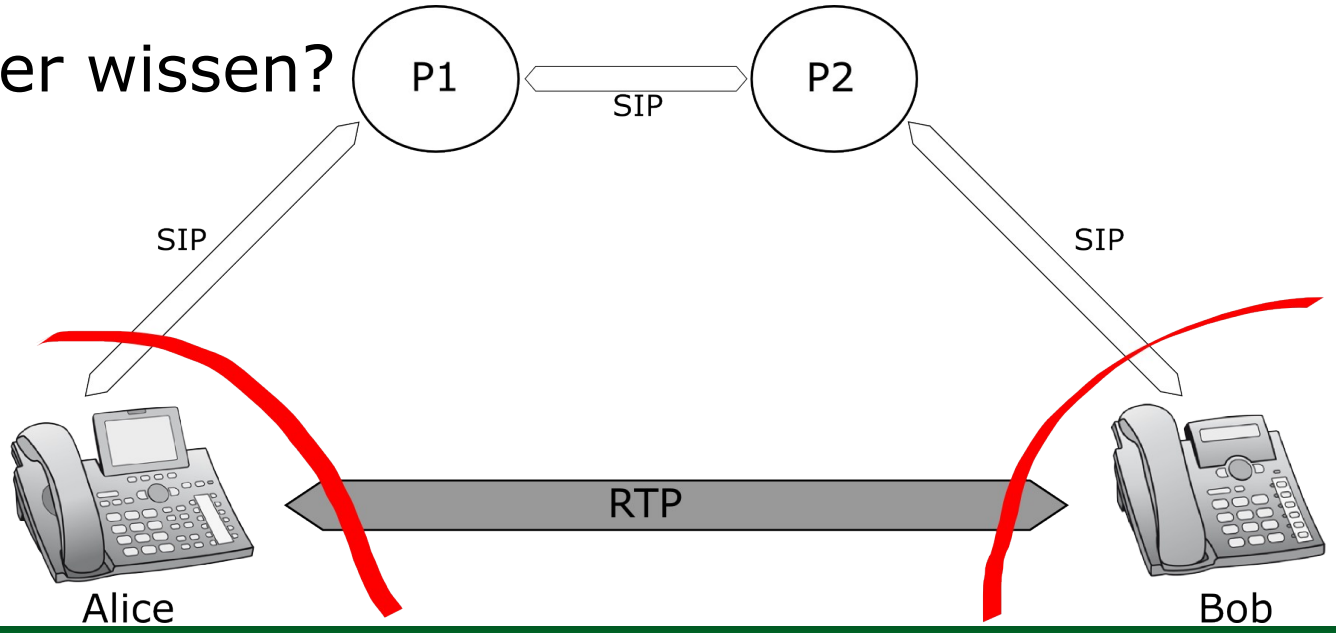
- Kein Gesprächsaufbau
- One-Way-Audio
- Gesprächspartner nimmt ab, der Anrufende hört dennoch weiterhin den RBT
- Gespräch fällt nach 30 Sekunden

Wo genau stört NAT?

- Bei SIP-Signalisierung:
  - Ein Client schreibt selbst seinen Contact-Header in den Request
  - In diesem steht, unter welchem IP/Port-Paar er erreichbar ist
  - Aber: wie soll er das wissen? Welchen unprivilegierten Port wird er auf der WAN-Seite des Routers erhalten? Wie oft wechselt dieser die NAT-Bindings?

Wo genau stört NAT?

- Bei RTP: Wie soll direktes RTP zwischen zwei Clients (SIP Trapezoid!) möglich sein, wenn beide hinter NAT-Routern sitzen, die nichts voneinander wissen?



NAT-Bindings verfallen

- Ausgehende Anrufe sind immer möglich
- Eingehende sporadisch / selten / nie
- Ursache: kein Verkehr, Port wird geschlossen
- Firewalls haben teilweise sehr niedrige Default-Timeouts für UDP

Erster Einruck

- Nur Probleme
- Kann nicht klappen
- Darum z.B. auch "IAX vs SIP":
  - War in erster Linie ein Glaubenskrieg, aber:
  - IAX kann in Spezialfällen ein Quick-Win sein
  - SIP denkt in weitaus größeren Dimensionen
- Alle genannten Probleme sind aber lösbar, ohne seine Firewall komplett durchlöchern zu müssen

STUN

- Definiert in RFC 3489, Abschnitt 5 insgesamt vier unterschiedliche NAT-Typen
- Erlaubt Endgeräten, auch hinter NAT zu funktionieren
- Hilft, Informationen über die Arbeitsweise des vorgeschalteten NAT zu erlangen
- Mittlerweile durch RFC 5389 abgelöst

Full Cone NAT

- Alle Anfragen mit
  - Derselben internen IP und
  - Demselben internen Port
- ...werden auf...
  - Dieselbe externe IP
  - Mit demselben externen Port
- ...abgebildet
- Von externen Hosts auf diese Weise erreichbar

Restricted Cone NAT

- Unterscheidet sich in einem wesentlichen Detail vom Full Cone NAT:
- Ein externer Host X kann nur dann ein Paket an einen internen senden, wenn dieser bereits zuvor ein Paket an die IP-Adresse von X gesendet hat

Port Restricted Cone NAT

- Entspricht dem Restricted Cone NAT...
- ...mit der Einschränkung, dass zusätzlich die Ports übereinstimmen müssen
- Ein externer Host mit IP X und Port P kann also nur dann an den internen Host Pakete senden, wenn dieser zuvor bereits ein Paket zu X:P gesendet hat
- Netfilter!

Symmetric NAT

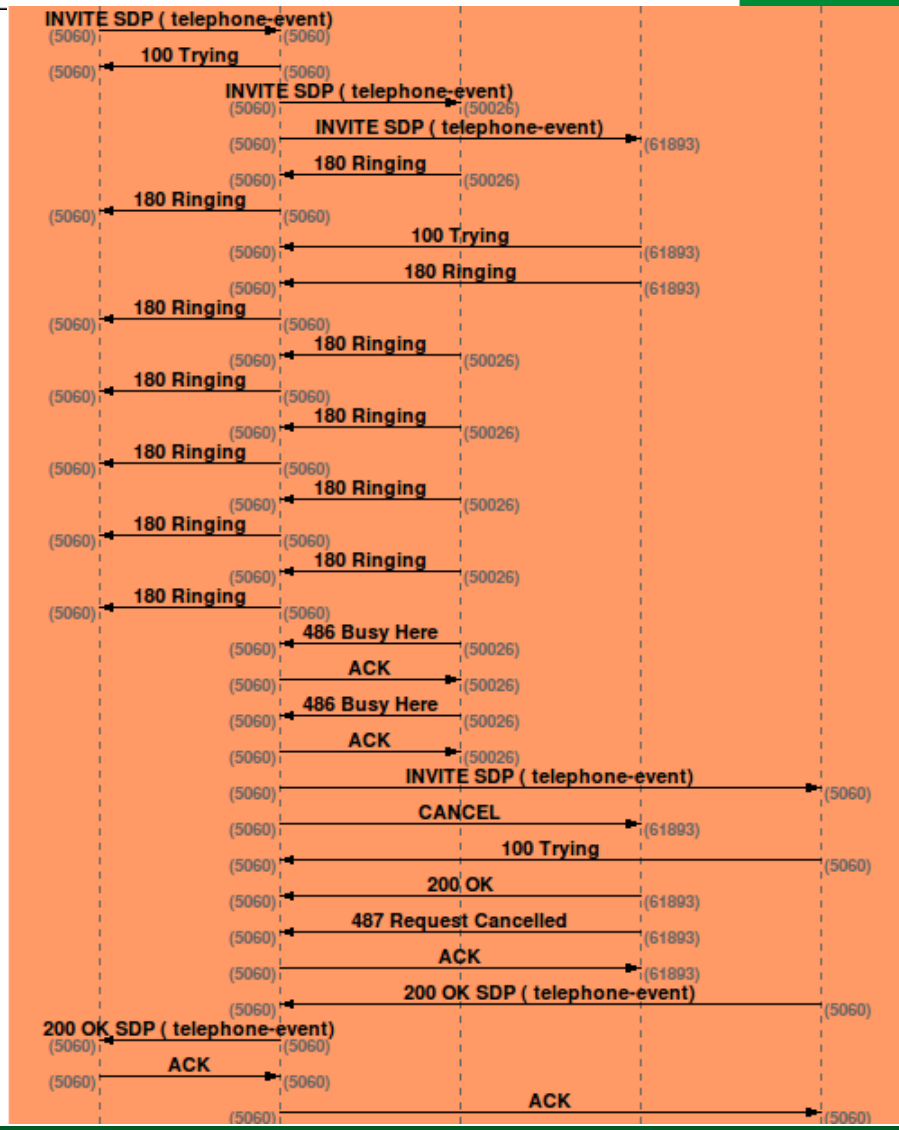
- Das restriktivste NAT
- Wechselt sogar dann das NAT-Binding, wenn...
  - Derselbe Client
  - Vom selben Source-Port
- ...ein Paket zu einem anderen Ziel sendet
- Jeder externe Host kann seine Antworten nur jeweils mit/an exakt diesen Socket senden
- Client kann keine Vorhersagen treffen

Wo / wie kann STUN helfen?

- Immer dann, wenn
  - Kein symmetrisches NAT im Einsatz ist
  - Kein SIP-ALG oder ähnliches aktiv ist
- Client kann durch STUN korrekte Informationen in SIP-Header und SDP schreiben
- Erkennt ein Client ein symmetrisches NAT, darf er KEINE Annahmen bzgl IP & Port treffen
- Symmetrisches NAT? STUN einfach abschalten!

SIP kann viel mehr!

- Einfaches Beispiel:
  - Forking, zwei Clients
  - Unterschiedliche NAT-Typen
  - Eine Client lehnt ab
  - Zweiter: Timeout
  - Rufumleitung ins Festnetz



Irrtum 1: Port-Forwarding für Port 5060

- Ist in den allerwenigsten Fällen nötig
- Öffnet das eigene SIP-Gerät für Angriffe aus aller Welt
- Wer vertraut der Firmware seines Telefons?
- Wer macht sich darüber überhaupt Gedanken?
- Wer trennt brav Telefonie- und Daten-Netz in dedizierte Broadcast-Domains / VLANs?

Irrtum 2: Port 3478/79 für STUN freischalten

- Ist völliger Quatsch
- STUN soll zuverlässig den NAT-Typ unseres Routers erkennen
- Wenn wir STUN etwas vorschwindeln, kann nichts Gescheites dabei herauskommen

SIP-ALGs - Freund oder Feind?

- Prinzipiell eine gute Idee
- NAT-Router spielt mit
- Öffnet die jeweils erforderlichen Ports
- Korrigiert SIP/SDP on-the-fly
- Immer mehr Router kommen mit per default aktiviertem SIP-ALG
- Sowohl im Enterprise- wie auch im Consumer-Bereich

Das Problem mit den SIP-ALGs...

- ...sie funktionieren nicht!
- Ich habe noch nie eine ernstzunehmende Implementierung angetroffen
- Die meisten Enterprise-Firewalls bewerben SIP-Unterstützung in deren Hochglanzprospekten...
- ...und empfehlen auf deren eigenen FAQ-Seiten und / oder Support-Foren denen, die SIP nutzen wollen, dieses Feature doch bitte auszuschalten

SIP-ALGs in Consumer-Produkten

- Auch viele Consumer- und SOHO-Router kommen heute bereits mit SIP-ALGs
- Me-Too: Mitbewerb hat's auf der Verpackung
- SIP scheint von denen aber keiner so wirklich verstanden zu haben
- ALG kommt teilweise per Auto-Upgrade
- Lässt sich manchmal gar nicht mehr abschalten

Praxisbeispiel, bekannter Hersteller

- SIP hat funktioniert
- Firmware-Upgrade, ALG aktiv
- Respektierte Record-Route Header nicht
- Ausgehendes Gespräch meistens korrekt
- Eingehendes bricht nach 30 Sekunden ab

Wie soll ein Helpdesk solche Probleme lösen?

- Brainware: Schulungen
- Support-Tiefe definieren
- ITIL: Eskalation-Mechanismen
- "Intelligente" Tools

Grandstream GXP2020 1.2.1.4
195.254[redacted]64649 - RIS-NET-6
(AS8564: Raiffeisen Online Gen. / Raiffeisen Online Gen. xDSL)
Anmeldung zuletzt aktualisiert um 15:23, gültig bis 16:23
Neue Firmware verfügbar: 1.2.2.14

snom370/7.3.26
195.254[redacted]20973 - RIS-NET
(AS8564: Raiffeisen Online Gen. / Raiffeisen OnLine Gen.)
Anmeldung zuletzt aktualisiert um 15:34, gültig bis 16:34
Neue Firmware verfügbar: 7.3.27
Dieses VoIP-Gerät befindet sich entweder hinter einem symmetrischen NAT-Router (bzw Firewall) - oder aber die STUN-Einstellungen sind nicht korrekt. Die Sprachpakete werden auf jeden Fall über die Mediaproxies umgeleitet.

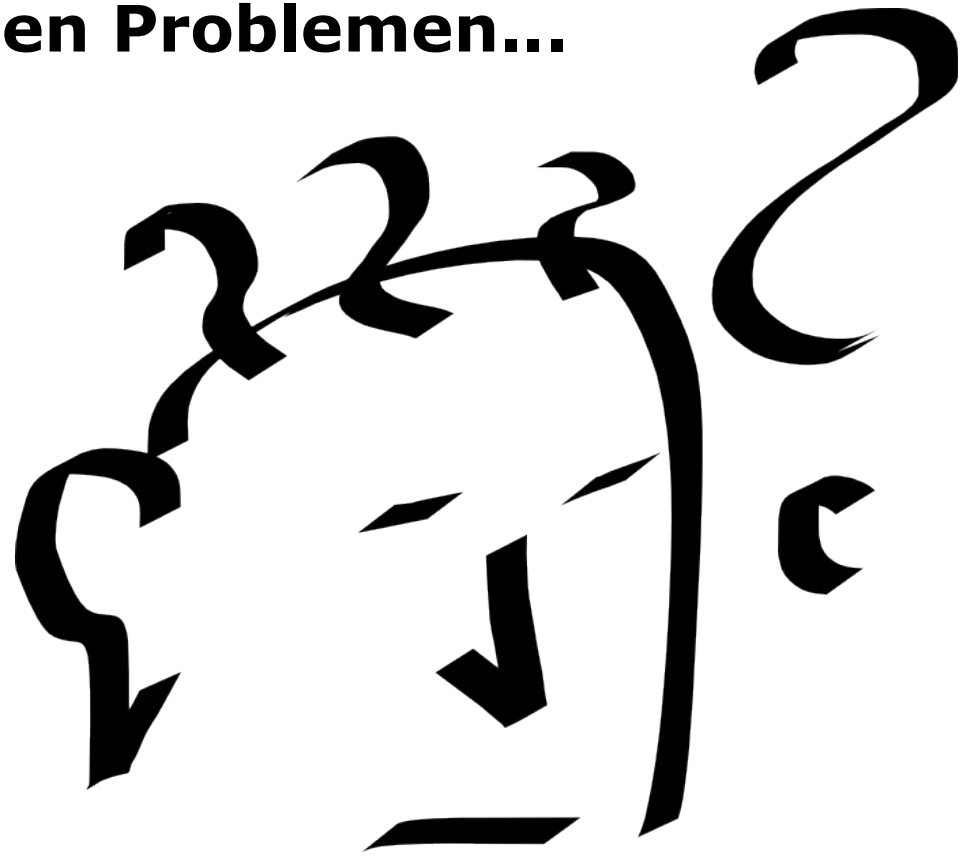
Session Border Controller

- Ein Produkt, das die Welt nicht braucht...
- ...und das sich bestens verkaufen lässt :-)
- Zwar aus Sicherheitsgründen je nach Szenario durchaus sinnvoll
- Meistens aber ziemlich überflüssig
- Egal, die Sales-Leute freuts: dank verbreiteter fachlicher Unsicherheit lässt sich's gut verkaufen

Problem: Hair-Pinning

- Telefonat zwischen zwei lokalen Telefonen, aber über gemeinsamen SIP-Provider
- RTP geht raus, Ziel: eigene offizielle IP
- RTP kommt wieder rein, Router sieht eigene IP als Absender, muss Spoofing sein, wirft's weg
- Ergo: telefonieren klappt in die ganze Welt, bloß nicht zum Nachbarbüro

Nach so vielen Problemen...



...Lust auf ein paar Lösungsansätze??

Problem Nr. 1: SIP Contact Header bei NAT

- Wird STUN nicht benutzt, ist er falsch
- Wird STUN genutzt, sollte (!) er korrekt sein (außer ein ALG oder statisches NAT pfuschen drein)
- RFC3581: Symmetric Response Routing (rport)
  - Definiert, dass Replies und auch neue Requests stets symmetrisch sein müssen
  - Dadurch klappt es dann auch mit symmetrischem NAT

Was macht rport?

- Parameter im Via-Header: ;rport
- Informiert die Gegenseite darüber, dass symmetrisches Routing unterstützt wird
- Client gibt dem Parameter keinen Wert
- Proxy hängt die Portnummer dazu (=12345)
- Gemeinsam mit dem received-Parameter erhält man so den Socket, unter welchem der Client wirklich erreichbar ist

Klappt rport immer?

- Nicht jeder Client implementiert es
- Ein Proxy kann es aber dennoch erzwingen
  - Gibt Probleme mit asymmetrischen Clients
  - Solche sind aber kaum noch im Einsatz
- Hilft für gewöhnlich nur bei UDP

Wie bleibt das NAT-Binding aktiv?

- Keepalive-Mechanismen
- Server- oder Clientseitig?
  - Wer ist zuständig? Client? Proxy?
  - Hierfür existierte kein Standard!
  - Zu viel: Last auf Proxies, Batterieverbrauch steigt
  - Zu wenig: Client nicht mehr erreichbar
- Von Provider zu Provider verschieden
- Client "sollte" Keepalives <30sec senden

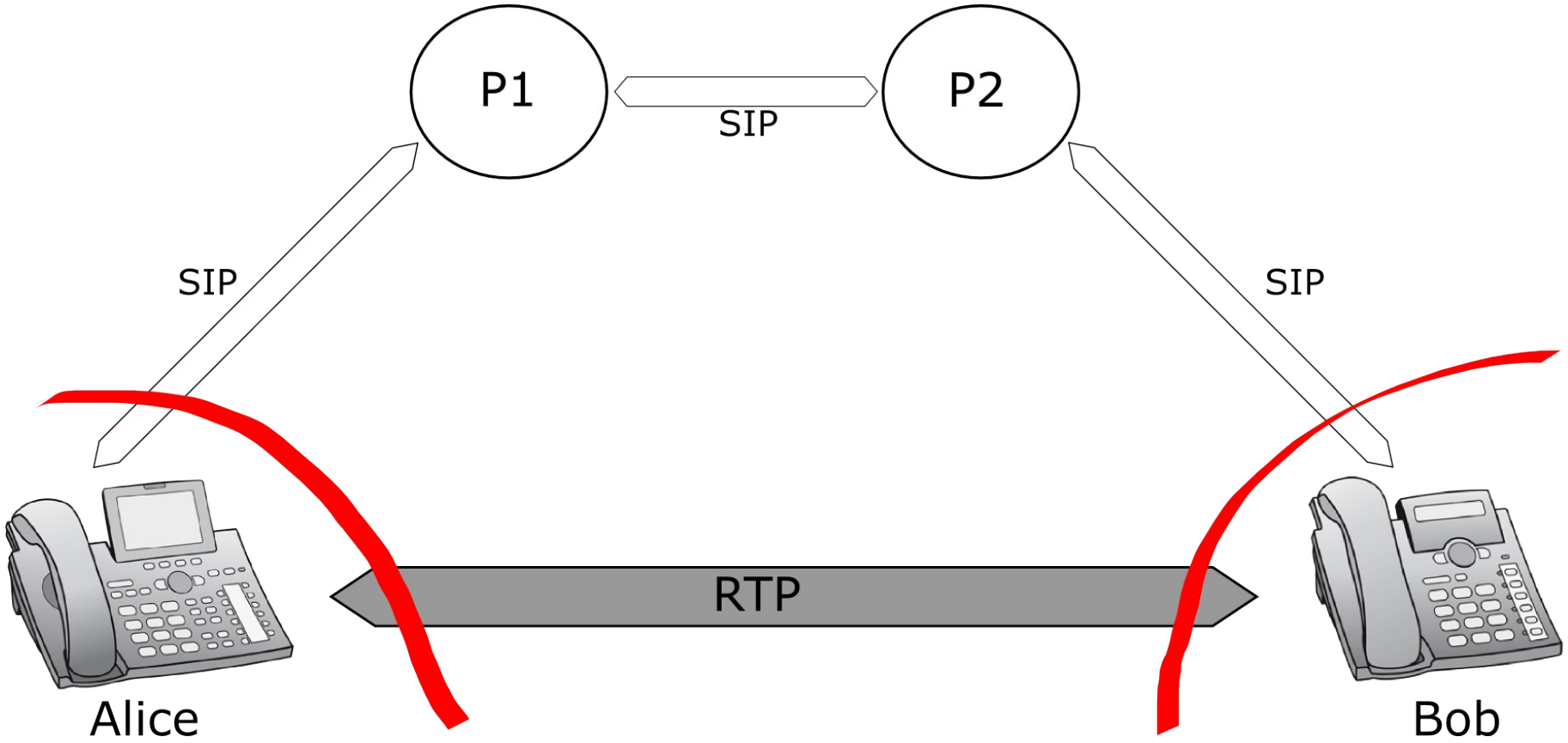
Wie bleibt das NAT-Binding aktiv?

- IETF Network Working Group hat sich des Problems angenommen
- RFC 5626 (Oktober 2009):
  - Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
- Wird den Aufwand zur Entwicklung von Clients und Proxys weiter erhöhen
- SIP wird dadurch aber stabiler werden

Voodoo: "direktes" RTP bei NAT

- Heute wird fast ausschließlich symmetrisches RTP benutzt
- Dank STUN „weiß“ der Client, welches externe IP/Port Paar benutzt wird
- Sobald von jeder Seite ein Paket gesendet worden ist, sieht es für die NAT-Router wie eine UDP-Verbindung aus, die „established“ ist

Voodoo: "direktes" RTP bei NAT



Probleme bei direktem RTP

- Effekt: man hört nichts, bevor man "Hallo" sagt
- Silence Suppression, Comfort Noise Generation
- Potentiell auch Probleme mit "early media"
- Kann bei symmetrischem NAT nicht klappen
- Ist symmetrisches NAT somit ein K.O.?
- Bei gutem Provider: nein!

Wie kann ein Proxy/Provider hier helfen?

- Er erkennt Fehler in der Signalisierung:
  - Private IP-Adressen (RFC1918) in SIP und SDP
  - UDP-Port entspricht nicht dem Contact-Header
- Was passiert dann?
  - Hinweise in SIP-Paket (Via: ;rport, ;received)
  - "Flags" im Record-Route Header
  - SDP wird on-the-fly korrigiert, RTP über entsprechende Gateways "umgeleitet"

Fax klappt nicht?

- Problem liegt vielleicht genau an vorhin genannten Media-Gateways
- Einige unterstützen bloß UDP
- T.38/UDPTL schlägt fehl

Wie konfiguriere ich Router / Firewall?

- Generell gilt: für die Telefonie mit SIP keine(!) Port-Forwardings von außen nach innen
- Was aber darf von innen nach außen?
- SIP (Port 5060, UDP und/oder TCP) und...
- ...prinzipiell "alles", denn RTP wird dynamisch ausgehandelt
- Bei restriktiver Security-Policy ein Problem

Firewall-Problem: Lösungsansätze

- Saubere Lösung:
  - Telefone in eigenes VLAN mit anderer Policy
- Kompromisse:
  - Dedizierte FW-Regeln für IPs der Telefone
  - Nur bestimmten Source-Ports "alles" erlauben
  - STUN abschalten, somit RTP über Gateways des Providers erzwingen, nur selbige freischalten

SIP und Verschlüsselung

- Geht das?
- SIPS (TLS)
- SRTP
  - Key-Exchange im SDP
  - Außerhalb (MIKEY?)
- ZRTP
- DTLS

Angriffsmöglichkeiten (generell)

- Kennwörter werden zwar nie übertragen, aber:
  - So lange man SIP im Klartext nutzt, ist jeder nur erdenkliche MITM-Angriff möglich
  - Dazu muss man aber an einer entsprechenden Position sitzen
  - Alles andere ist erst mal Panikmache
- In erster Linie ist hier der Provider in der Pflicht
- Außer mein Port 5060 ist komplett offen(!)

Angriffsmöglichkeiten

- Fragen?

Bandbreite, QoS

- QoS? NGN? Ipv6?
- So richtig helfen kann nur eins: ausreichend Bandbreite
- QoS ist machbar, wenn
  - Man selbst am Flaschenhals sitzt

    (oder diesen künstlich kreiert)
  - Man weiß, WAS man priorisieren muss

Wichtigstes Werkzeug: der Sniffer

- Wireshark
- Remote per SSH und tcpdump:

```
ssh root@host "tcpdump -s0 -n -U -w - port 5060" > file
```

- Auf SIP-Geräten existiert oft Capture-Funktion (AVM, snom...): ist häufig eine große Hilfe
- Kann lokal mit Wireshark untersucht werden
- Asterisk und andere bieten Debug-Funktionen

sipsak – das Schweizer Messer für SIP

- Nützlich z.B., um vordefinierte Pakete zu senden
- Monitoring (OPTIONS, INVITE)
- Anmeldung (REGISTER) in Spezialfällen
  - z.B. wenn ein reiner SIP-Proxy benutzt wird, und externe Accounts angemeldet werden müssen
- uvm

Vielen Dank für Ihre Aufmerksamkeit!

Noch Fragen?

mail: thomas@gelf.net

web: http://thomas.gelf.net