Herzlich Willkommen zum Business Breakfast Table 2018

swizzconnexx

bintec elmeg
Teldat Group Company

Technik – Herausforderungen VoIP

swizzconnexx

Mit **All-IP** ist umgangssprachlich hauptsächlich gemeint, dass neu auch die Sprachdaten über das «IP-Netzwerk» gesendet werden, also **VoIP** (Voice over IP).

1. Datentransport

Im VoIP wurde grundsätzlich versucht die Mechanik und Logik der vermittlungsorientierten Kommunikation aus der traditionellen Telekommunikation (SDH, PDH, MPLS, ISDN, etc.) zu übernehmen.

Im IT-Netzwerk gibt es grundsätzlich 2 Transportprotokolle:

- **TCP** = verbindungsorientiert (Session), paketvermittelt
- **UDP** = verbindungslos (ohne Sicherung), sehr wenig Verzögerung

Da Sprache zeitkritische Realtimedaten sind, eignet sich aus Gründen der Latenz und Jitter nur **UDP** für **VoIP**.

Technik – Herausforderungen VoIP

swizzconnexx

2. NAT-Routing => Session Table

In IPv4 IT-Netzwerken findet aufgrund der Adressbegrenzung eine Netzwerkadressübersetzung **NAT** statt.
Bei abgehenden Datenpaketen wird vom WAN-Router (Gateway) die interne IP (z.B. 192.168.x.y) in die öffentliche IP (z.B. 178.82.50.y) umgesetzt => **Source-NAT**.

Von Extern ankommende Pakete werden nur nach Intern geleitet, wenn zuerst von Intern ein Paket gesendet wurde über dieses Port (Port-Öffnung von innen) = **NAT-Session**, oder eine spezielle Regel für die «Öffnung» von Extern definiert wurde (Destination-NAT)

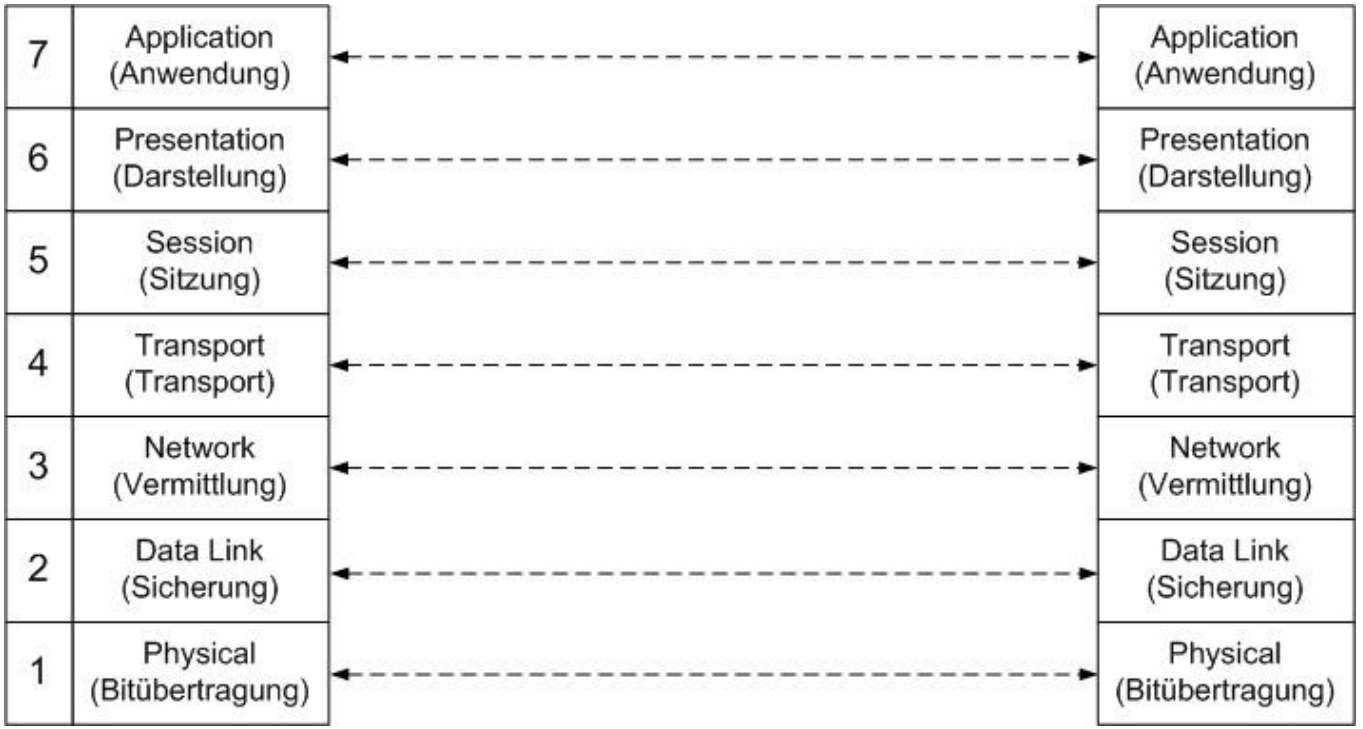
VoIP (SIP und RTP) sind UDP => UDP baut keine Session auf. Damit die Port Öffnung in UDP für eine bidirektionale Kommunkation trotzdem stattfindet werden für UDP **logische Sessions** nachgebildet mit einem **Ablauftimer**.

Technik – Herausforderungen VoIP

swizzconnexx

3. NAT-Routing => VoIP

NAT Routing (TCP und UDP) findet auf Layer 3 und 4 statt. SIP und RTP ist Layer 5.



DNS, HTTP, SMTP, POP, Telnet, FTP, **DHCP**, etc.

HTML, DOC, JPEG, MP3, etc.

SIP, RTP, Sockets, NetBIOS, SS7, etc.

TCP, **UDP**, SSL, **TLS**, etc.

IP, IPsec, ICMP, IGMP, NAT, RIP, BGP, etc.

Ethernet, VLAN (802.x), **ATM**, **PPP (PPPoE)**, **802.11**, etc.

RS-232, RJ45, **xDSL**, **802.11**, 802.x, SDH, **DOCSIS**, **ISDN**, etc.

-> **HTTPS**: HTTP über TSL -> **SIPS**: SIP über TLS

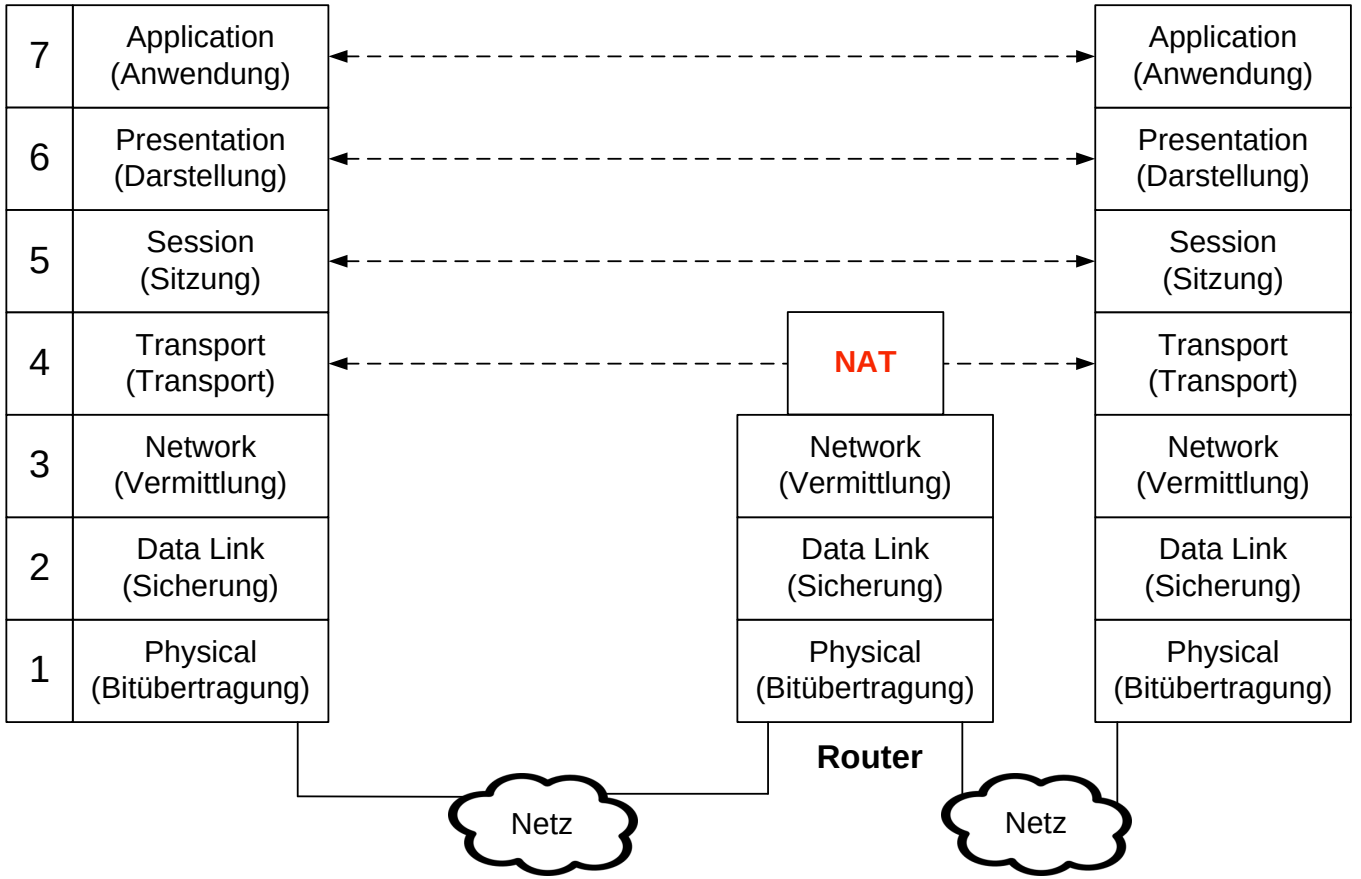
-> **«VDSL u. ADSL Übertragung»** = PPPoE / PPPoA über ATM (AAL5) über VDSL / ADSL Modulation

Technik – Herausforderungen VoIP

swizzconnexx

3. NAT-Routing => VoIP

NAT Routing (TCP und UDP) findet auf Layer 3 und 4 statt. SIP und RTP ist Layer 5.



DNS, HTTP, SMTP, POP, Telnet, FTP, **DHCP**, etc.

HTML, DOC, JPEG, MP3, etc.

SIP, RTP, Sockets, NetBIOS, SS7, etc.

TCP, **UDP**, SSL, **TLS**, etc.

IP, IPsec, ICMP, IGMP, **NAT**, RIP, BGP, etc.

Ethernet, VLAN (802.x), **ATM**, **PPP (PPPoE)**, **802.11**, etc.

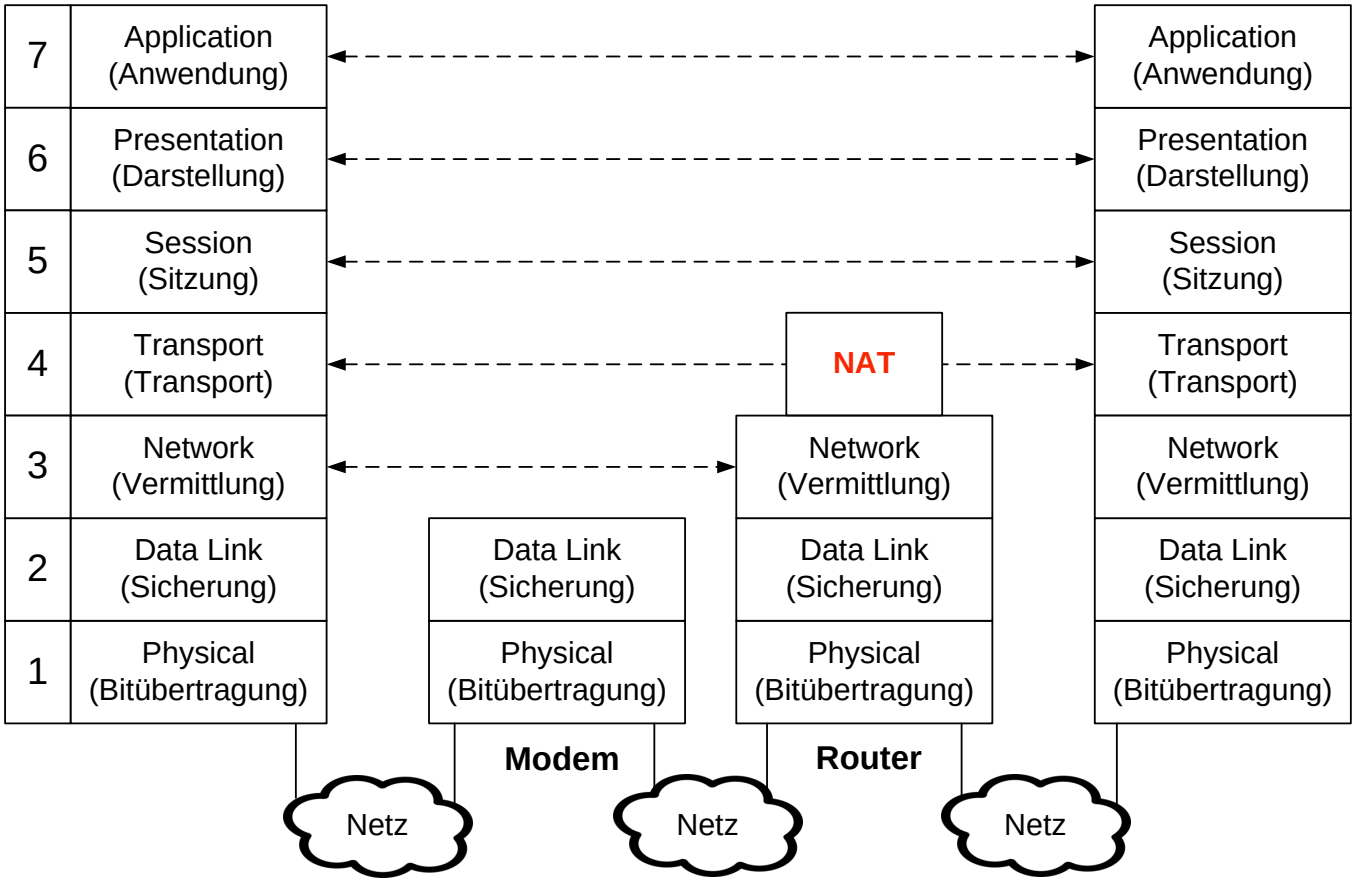
RS-232, RJ45, **xDSL**, **802.11**, 802.x, SDH, **DOCSIS**, **ISDN**, etc.

Technik – Herausforderungen VoIP

swizzconnexx

3. NAT-Routing => VoIP

NAT Routing (TCP und UDP) findet auf Layer 3 und 4 statt. SIP und RTP ist Layer 5.



DNS, HTTP, SMTP, POP, Telnet, FTP, **DHCP**, etc.

HTML, DOC, JPEG, MP3, etc.

SIP, RTP, Sockets, NetBIOS, SS7, etc.

TCP, **UDP**, SSL, **TLS**, etc.

IP, IPsec, ICMP, IGMP, **NAT**, RIP, BGP, etc.

Ethernet, VLAN (802.x), **ATM**, **PPP (PPPoE)**, **802.11**, etc.

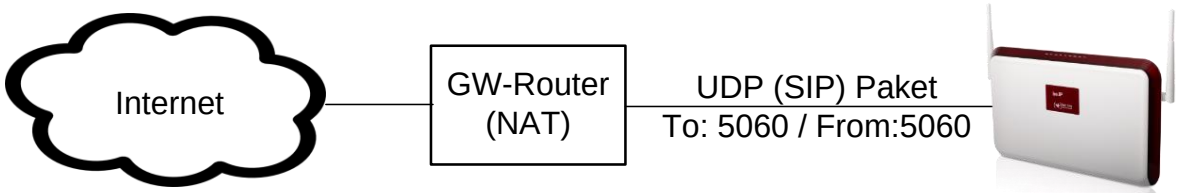
RS-232, RJ45, **xDSL**, **802.11**, 802.x, SDH, **DOCSIS**, **ISDN**, etc.

Technik – Herausforderungen VoIP

swizzconnexx

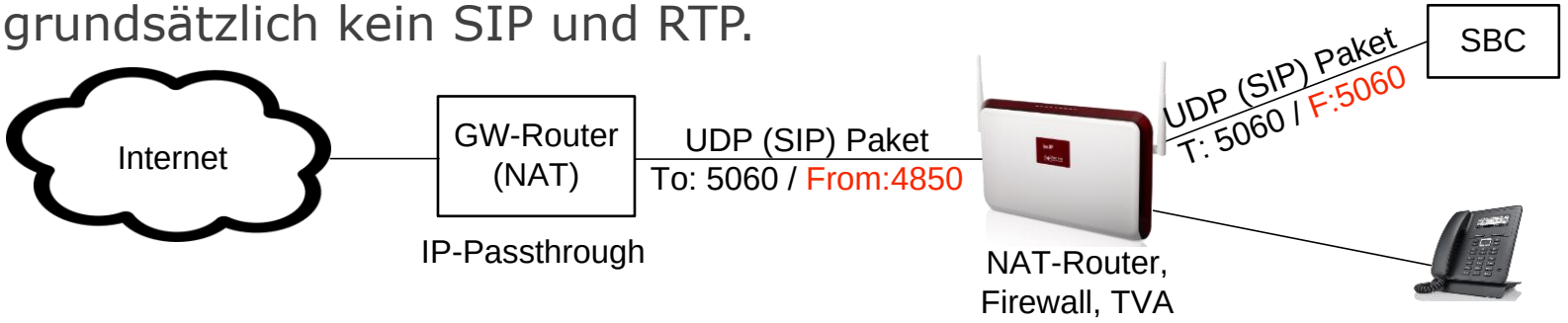
3. NAT-Routing => VoIP

Fazit: Ein normaler NAT-Router (Gateway) weiss bei UDP:5060 dass er SIP routet, hat aber keine Kenntnis über den Inhalt. RTP (UDP:Port > 10’000) erkennt er nicht.



Router mit «VoIP Intelligenz»
liest SIP und erkennt dadurch RTP

Wird eine DMZ oder Passthrough auf dem GW eingerichtet, erkennt der GW grundsätzlich kein SIP und RTP.



Mögliche Lösung: SNAT Definition mit fixem 5060 Port. VoIP Intelligenz hält SIP «offen» solange RTP gesendet wird.

Technik – Herausforderungen VoIP

swizzconnexx

SIP / RTP

SIP Invite (Datenauszug):

Internet Protocol Version 4, Src: 178.197.234.226, Dst: 84.73.156.236
User Datagram Protocol, Src Port: 35206, Dst Port: 5060
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:83@tel.swizzconnexx.ch:5060 SIP/2.0
Message Header
Via: SIP/2.0/UDP 10.128.115.223:5060;branch=z9hG4bKe973aefa818c249a6;rport
From: "71" <sip:71@tel.swizzconnexx.ch:5060>;tag=2beb427efc
To: <sip:83@tel.swizzconnexx.ch:5060>
Call-ID: 52b2cf27b7066c3b
Contact: <sip:71@10.128.115.223:5060>;audio
Session-Expires: 1800; refresher=uas
Content-Type: application/sdp
Message Body
Session Description Protocol
Owner/Creator, Session Id (o): - 305065757297 305065757297 IN IP4 10.128.115.223
Connection Information (c): IN IP4 10.128.115.223
Session Attribute (a): sendrecv
Media Description, name and address (m): audio 12100 RTP/AVP 0 8
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): sendrecv

Technik – Herausforderungen VoIP

swizzconnexx

SIP / RTP

SIP Invite (Datenauszug):

Internet Protocol Version 4, Src: 178.197.234.226, Dst: 84.73.156.236
User Datagram Protocol, Src Port: 35206, Dst Port: 5060
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:83@tel.swizzconnexx.ch:5060 SIP/2.0
Message Header
Via: SIP/2.0/UDP 10.128.115.223:5060;branch=z9hG4bKe973aefa818c249a6;rport
From: "71" <sip:71@tel.swizzconnexx.ch:5060>;tag=2beb427efc
To: <sip:83@tel.swizzconnexx.ch:5060>
Call-ID: 52b2cf27b7066c3b
Contact: <sip:71@10.128.115.223:5060>;audio
Session-Expires: 1800; refresher=uas
Content-Type: application/sdp
Message Body
Session Description Protocol
Owner/Creator, Session Id (o): - 305065757297 305065757297 IN IP4 10.128.115.223
Connection Information (c): IN IP4 10.128.115.223
Session Attribute (a): sendrecv
Media Description, name and address (m): audio 12100 RTP/AVP 0 8
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): sendrecv

SIP-Client teilt lokale IP mit, der NAT-Router ändert jedoch IP und Port

Technik – Herausforderungen VoIP

swizzconnexx

SIP / RTP

SIP Invite (Datenauszug):

Internet Protocol Version 4, Src: 178.197.234.226, Dst: 84.73.156.236
User Datagram Protocol, Src Port: 35206, Dst Port: 5060
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:83@tel.swizzconnexx.ch:5060 SIP/2.0
Message Header
Via: SIP/2.0/UDP 10.128.115.223:5060;branch=z9hG4bKe973aefa818c249a6;rport
From: "71" <sip:71@tel.swizzconnexx.ch:5060>;tag=2beb427efc
To: <sip:83@tel.swizzconnexx.ch:5060>
Call-ID: 52b2cf27b7066c3b
Contact: <sip:71@10.128.115.223:5060>;audio
Session-Expires: 1800; refresher=uas
Content-Type: application/sdp
Message Body
Session Description Protocol
Owner/Creator, Session Id (o): - 305065757297 305065757297 IN IP4 10.128.115.223
Connection Information (c): IN IP4 10.128.115.223
Session Attribute (a): sendrecv
Media Description, name and address (m): audio 12100 RTP/AVP 0 8
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): sendrecv

SIP-Client teilt lokale IP mit, der NAT-Router ändert jedoch IP und Port

Technik – Herausforderungen VoIP

swizzconnexx

SIP / RTP

SIP Invite (Datenauszug):

Internet Protocol Version 4, Src: 178.197.234.226, Dst: 84.73.156.236
User Datagram Protocol, Src Port: 35206, Dst Port: 5060
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:83@tel.swizzconnexx.ch:5060 SIP/2.0
Message Header
Via: SIP/2.0/UDP 10.128.115.223:5060;branch=z9hG4bKe973aefa818c249a6;rport
From: "71" <sip:71@tel.swizzconnexx.ch:5060>;tag=2beb427efc
To: <sip:83@tel.swizzconnexx.ch:5060>
Call-ID: 52b2cf27b7066c3b
Contact: <sip:71@10.128.115.223:5060>;audio
Session-Expires: 1800; refresher=uas
Content-Type: application/sdp
Message Body
Session Description Protocol
Owner/Creator, Session Id (o): - 305065757297 305065757297 IN IP4 10.128.115.223
Connection Information (c): IN IP4 10.128.115.223
Session Attribute (a): sendrecv
Media Description, name and address (m): audio 12100 RTP/AVP 0 8
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): sendrecv

SIP-Client teilt lokale IP mit, der NAT-Router ändert jedoch IP und Port

Nach Session Initierung soll RTP direkt an 10.128.115.223:12100 senden.

Technik – Herausforderungen VoIP

swizzconnexx

SIP / RTP

SIP Invite (Datenauszug):

Internet Protocol Version 4, Src: 178.197.234.226, Dst: 84.73.156.236
User Datagram Protocol, Src Port: 35206, Dst Port: 5060
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:83@tel.swizzconnexx.ch:5060 SIP/2.0
Message Header
Via: SIP/2.0/UDP 10.128.115.223:5060;branch=z9hG4bKe973aefa818c249a6;rport
From: "71" <sip:71@tel.swizzconnexx.ch:5060>;tag=2beb427efc
To: <sip:83@tel.swizzconnexx.ch:5060>
Call-ID: 52b2cf27b7066c3b
Contact: <sip:71@10.128.115.223:5060>;audio
Session-Expires: 1800; refresher=uas
Content-Type: application/sdp
Message Body
Session Description Protocol
Owner/Creator, Session Id (o): - 305065757297 305065757297 IN IP4 10.128.115.223
Connection Information (c): IN IP4 10.128.115.223
Session Attribute (a): sendrecv
Media Description, name and address (m): audio 12100 RTP/AVP 0 8
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): sendrecv

SIP-Client teilt lokale IP mit, der NAT-Router ändert jedoch IP und Port

Nach Session Initierung soll RTP direkt an 10.128.115.223:12100 senden.

=> Provider hat Medien-Proxy mit symmetric response routing

Technik – Herausforderungen VoIP

swizzconnexx

4. Firewall (bindings)

Ähnlich wie beim **NAT** funktioniert auch die **Firewall**.
Von Extern ankommende Pakete werden nur nach Intern geleitet, wenn zuerst von Intern ein Paket gesendet wurde über dieses Port (Öffnung von innen) = **Session**, oder eine spezielle Regel für die «Öffnung» von Extern definiert wurde.

VoIP (SIP und RTP) sind UDP => UDP baut keine Session auf. Damit die Öffnung in UDP für eine bidirektionale Kommunkation trotzdem stattfindet werden für UDP **logische Sessions** nachgebildet mit einem **Ablauftimer** (oft 180s).

Technik – Herausforderungen VoIP

swizzconnexx

Übersicht

1. **Datentransport UDP** (verbindungslos ohne Sicherung)
   - «Fire and Forget», keine Rückmeldung, keine Wiederholung
   - Wenn Latenz zu gross => gedropt
   - Wenn Jitter (Schwankungen) zu gross => unbrauchbar

   Bisher nur für Daten (TCP) benutztes LAN (auch WAN) muss nun richtig und gut funktionieren (=> evtl. VLAN, MTU, QoS, etc.)

2. **NAT-Routing:** logische Sessions UDP mit **Ablauftimer (TTL)**
   - Wenn «Port-Öffnung» von innen abläuft keine Anrufe mehr von Extern
   - Innerhalb eines SIP-Dialogs (SIP:Invite, dann RTP) muss Session nach ca. 12-14 Min. erneuert werden mit Re-Invite oder SIP:Update. Nach Ablauf der Session, nicht mehr möglich von Extern.

   SIP:Option- oder leere UDP-Pakete senden (Keep-Alive), VoIP-Intelligenz (RTP->SIP), DNAT, bestimmte ALG Features

3. **Firewall Bindings: TTL** (siehe 2. NAT-Routing)

   zusätzlich: Zugriffsregeln, VoIP-Intelligenz, bestimmte ALG Features

Technik – Herausforderungen VoIP

swizzconnexx

Übersicht

4. NAT-Routing: Erkennt SIP und RTP nicht

- kann SDP im SIP nicht lesen => RTP Port nicht offen
- SIP:Option- oder leere UDP-Pakete haben keinen Nutzen, weil jeder SIP-Dialog (z.B. SIP:Invite, dann RTP) einen neuen S-NAT Port öffnet am Router, weil symmetric NAT

VoIP-Intelligenz (RTP->SIP), auf TVA: STUN mit S-NAT z.B. Full-Cone, bestimmte ALG Features (NICHT SIP-Header Transformation), STUN-Handler im Router (von SIP auf RTP), ICE -> STUN und TURN, Provider setzt Media Gateway/Proxy ein mit symmetric response routing

5. Codec

- Provider verwenden oft teil-gehostete US-VoIP-Server, welche USA-Codec verwenden. => Transcoding im SIP Pfad, verursachen Fehler und Latenzen und Jitter.

Early Media deaktivieren, Codec Einschränken, beim Provider RTP-Proxy verlangen.

Technik – Herausforderungen VoIP

swizzconnexx

Fazit

- Bei UDP (SIP, RTP) = Telefonie, Multimedia, etc. in einem gerouteten Netzwerk hilft es sehr zu wissen was man tut.
- Bei TVA SIP- und RTP-Verbindungen über z.B. die be.IP plus als NAT-Router/Firewall werden die Probleme gelöst durch die VoIP-Intelligenz des Routers (be.IP plus).
- Bei «üblichen» TVA SIP- und RTP-Verbindungen über einen **separaten NAT-Router** zu einer VoIP-Plattform eines VoIP-Providers, löst der Provider zu 99% diese Probleme mit seiner SIP-Intelligenten Infrastruktur von SIP-Proxies, RTP-Proxies, Media-Gateway mit symmetric RTP, B2BUA (SBC) etc. - ausser Codec Probleme
  => Der Internet Provider jedoch nicht immer.
- Beim Einsatz von B2BUA (SBC) in bestimmten Netzstrukturen müssen evtl. bereits Massnahmen ergriffen werden => z.B. für ReInvite
- Bei TVA SIP- und RTP-Verbindungen zu externen Clients (z.B. App auf Mobiltelefon) über Layer 3, also nicht VPN, müssen gezielte Massnahmen umgesetzt werden.