
Praktikum Rechnernetze

Protokoll zu Versuch 10 (VoIP) von Gruppe 1

Jakob Waibel, Daniel Hiller, Elia Wüstner, Felix Pojtinger

2021-12-21

Inhaltsverzeichnis

1	Einführung	3
1.1	Mitwirken	3
1.2	Lizenz	3
2	STUN und Registrierung	4
3	Verbindungsaufbau und SDP-Protokoll	8
4	RTP/RTCP	11
5	SIP-Byte	14

1 Einführung

1.1 Mitwirken

Diese Materialien basieren auf [Professor Kiefers “Praktikum Rechnernetze”-Vorlesung der HdM Stuttgart](#).

Sie haben einen Fehler gefunden oder haben einen Verbesserungsvorschlag? Bitte eröffnen Sie ein Issue auf GitHub (github.com/pojntfx/uni-netpractice-notes):



Abbildung 1: QR-Code zum Quelltext auf GitHub

Wenn Ihnen die Materialien gefallen, würden wir uns über einen GitHub-Stern sehr freuen.

1.2 Lizenz

Dieses Dokument und der enthaltene Quelltext ist freie Kultur bzw. freie Software.



Abbildung 2: Badge der AGPL-3.0-Lizenz

Uni Network Practice Notes (c) 2021 Jakob Waibel, Daniel Hiller, Elia Wüstner, Felix Pojtinger

SPDX-License-Identifier: AGPL-3.0

2 STUN und Registrierung

Bei der Konfiguration des sipgate-Accounts sind auch Angaben zum sogenannten STUN-Server erforderlich. Beschreiben Sie mit eigenen Worten Aufgaben und die Funktion eines STUN-Servers

Die "Session Traversal Utilities for NAT" ist ein Standard, welcher dabei hilft, die öffentlichen Netzwerkadressen von Netzwerknodes herauszufinden, um eine Peer-to-peer Verbindung zwischen diesen Nodes hinter NAT herzustellen. Es kann außerdem festgestellt werden, welche Art von NAT verwendet wird (Full Cone, Restricted Cone...). Da die Belastung von STUN-Servern in der Realität vergleichsweise niedrig ist, können für viele Projekte öffentliche STUN-Server ausreichend sein.

Welche IP-Adresse hat das REGISTER-Paket nach dem NAT-Vorgang (NAT ist wegen der privaten Adresse erforderlich)?

TODO: Add interpretation

1 0.000000	10.231.172.221	217.10.79.9	SIP	710 Request: REGISTER sip:sipgate.de (1 binding)
2 0.010972	217.10.79.9	10.231.172.221	SIP	521 Status: 401 Unauthorized
3 0.011573	10.231.172.221	217.10.79.9	SIP	904 Request: REGISTER sip:sipgate.de (1 binding)
4 0.021907	217.10.79.9	10.231.172.221	SIP	585 Status: 200 OK (REGISTER) (1 binding)
5 31.298931	217.10.79.9	10.231.172.221	SIP/SDP	1359 Request: INVITE sip:2555428e0@10.231.172.221:49699


```

Request-Line: REGISTER sip:sipgate.de SIP/2.0
Message Header
  Via: SIP/2.0/UDP 194.49.221.7:22556;branch=z9hG4bK8041d10841bbe8118a33a1d115dda7c5;rport
  From: "PhonerLite" <sip:2555428e0@sipgate.de>;tag=3247336616
    SIP from display info: "PhonerLite"
    SIP from address: sip:2555428e0@sipgate.de
    SIP from tag: 3247336616
  To: "PhonerLite" <sip:2555428e0@sipgate.de>
    SIP to display info: "PhonerLite"
    SIP to address: sip:2555428e0@sipgate.de
  Call-ID: 8041D108-41BB-E811-8A30-A1D115DDA7C5@194.49.221.7
  [Generated Call-ID: 8041D108-41BB-E811-8A30-A1D115DDA7C5@194.49.221.7]
  CSeq: 1 REGISTER
  Contact: <sip:2555428e0@194.49.221.7:22556>;+sip.instance="urn:uuid:006D68F3-4421-E811-8759-B7021FA9EAB5"
    Contact URI: sip:2555428e0@194.49.221.7:22556
      Contact URI User Part: 2555428e0
      Contact URI Host Part: 194.49.221.7
      Contact URI Host Port: 22556
    Contact parameter: +sip.instance="urn:uuid:006D68F3-4421-E811-8759-B7021FA9EAB5"
  Allow: INVITE, ACK, BYE, CANCEL, INFO, MESSAGE, NOTIFY, OPTIONS, REFER, UPDATE, PRACK
  Max-Forwards: 70
  Allow-Events: org.3gpp.nwinitdereg
  User-Agent: SIPPER for PhonerLite
  Supported: replaces, from-change, gruu
  Expires: 900
  Content-Length: 0

```

Abbildung 3: Capture des Register-Pakets vor NAT

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.231.172.221	217.10.79.9	SIP	710	Request: REGISTER sip:sipgate.de (1 binding)
2	0.010972	217.10.79.9	10.231.172.221	SIP	521	Status: 401 Unauthorized
3	0.011573	10.231.172.221	217.10.79.9	SIP	904	Request: REGISTER sip:sipgate.de (1 binding)
4	0.021907	217.10.79.9	10.231.172.221	SIP	585	Status: 200 OK (REGISTER) (1 binding)
5	31.298931	217.10.79.9	10.231.172.221	SIP/SDP	1359	Request: INVITE sip:2555428e0@10.231.172.221:49699

▶ Frame 3: 904 bytes on wire (7232 bits), 904 bytes captured (7232 bits) on interface \Device\NPF_{60B079C4-4A54-4F24-9289-5222073BB27F}, in
 ▶ Ethernet II, Src: Mettler-_c8:d2:7f (00:e0:7c:c8:d2:7f), Dst: Tp-LinkT_5e:ff:c6 (60:e3:27:5e:ff:c6)
 ▶ Internet Protocol Version 4, Src: 10.231.172.221, Dst: 217.10.79.9
 ▶ User Datagram Protocol, Src Port: 49699, Dst Port: 5060
 ▶ Session Initiation Protocol (REGISTER)

▶ Request-Line: REGISTER sip:sipgate.de SIP/2.0
 ▶ Message Header

▶ Via: SIP/2.0/UDP 10.231.172.221:49699;branch=z9hG4bK8041d10841bbe8118a34a1d115dda7c5;rport
 ▶ From: "PhonerLite" <sip:2555428e0@sipgate.de>;tag=3247336616
 ▶ To: "PhonerLite" <sip:2555428e0@sipgate.de>
 ▶ Call-ID: 8041D108-41BB-E811-8A30-A1D115DDA7C5@10.231.172.221
 ▶ [Generated Call-ID: 8041D108-41BB-E811-8A30-A1D115DDA7C5@10.231.172.221]
 ▶ CSeq: 2 REGISTER
 ▶ Contact: <sip:2555428e0@10.231.172.221:49699>;+sip.instance="urn:uuid:006D68F3-4421-E811-8759-B7021FA9EAB5">
 ▶ Contact URI: sip:2555428e0@10.231.172.221:49699
 ▶ Contact URI User Part: 2555428e0
 ▶ Contact URI Host Part: 10.231.172.221
 ▶ Contact URI Host Port: 49699
 ▶ Contact parameter: +sip.instance="urn:uuid:006D68F3-4421-E811-8759-B7021FA9EAB5">\r\n
 ▶ Authorization: Digest username="2555428e0", realm="sipgate.de", nonce="W60YGlujlu4RRkLKBpUQTDfDxgDCaUq", uri="sip:sipgate.de", respo
 ▶ Allow: INVITE, ACK, BYE, CANCEL, INFO, MESSAGE, NOTIFY, OPTIONS, REFER, UPDATE, PRACK
 ▶ Max-Forwards: 70
 ▶ Allow-Events: org.3gpp.nwinitdereg
 ▶ User-Agent: SIPPER for PhonerLite
 ▶ Supported: replaces, from-change, gruu
 ▶ Expires: 900
 ▶ Content-Length: 0

Abbildung 4: Capture des Register-Pakets nach NAT

Erstellen und dokumentieren Sie den „FlowGraph“ des vorliegenden Pakets und erläutern Sie kurz den prinzipiellen Ablauf.

TODO: Add interpretation



Abbildung 5: Verbindungsaufbau mit SIP



Abbildung 6: Kommunikation mit RTP



Abbildung 7: Verbindungsabbau mit SIP

Nach diesem typischen Ablauf ist der UAC beim Provider registriert. Warum wird die Anfrage zur Registrierung zunächst abgewiesen?

TODO: Die Credentials des UAC werden mithilfe der in der Rejection (401 Unauthorized) vorhandenen Daten verschlüsselt. Sobald die Credentials verschlüsselt wurden können sie an das SIP-Gateway geschickt werden.

Worin unterscheiden sich die beiden REGISTER-Pakete?

TODO: Add interpretation



Abbildung 8: Vergleich beider SIP-Pakete (Contact & Authorization)

Warum wird für die so wichtige Registrierung nicht TCP (garantiert die bitgetreue Zustellung) verwendet, sondern UDP?

Für die Registrierung wird UDP statt TCP verwendet, da das Session Initiation Protocol (SIP) selbst eine spezifizierte Nachrichtenabfolge hat und verbindungsorientiert ist. Das ermöglicht, dass das SIP fehlerhafte Protokollabläufe selbst feststellt und nicht zwingend TCP zur Fehlerkorrektur benötigt, um Fehler festzustellen.

Wie lange ist die Registrierung gültig?

Wie im folgenden Bild zu sehen ist beträgt der "Expires" Wert 900 Sekunden. Dies entspricht 15 Minuten.

```
Session Initiation Protocol (REGISTER)
  Request-Line: REGISTER sip:sipgate.de SIP/2.0
  Message Header
    Via: SIP/2.0/UDP 10.231.172.221:49699;branch=z9hG4bK8041d10841bbe8118a34a1d115dda7c5;rport
    From: "PhonerLite" <sip:2555428e0@sipgate.de>;tag=3247336616
    To: "PhonerLite" <sip:2555428e0@sipgate.de>
    Call-ID: 8041D108-41BB-E811-8A30-A1D115D0A7C5@10.231.172.221
    [Generated Call-ID: 8041D108-41BB-E811-8A30-A1D115D0A7C5@10.231.172.221]
    CSeq: 2 REGISTER
    Contact: <sip:2555428e0@10.231.172.221:49699>;+sip.instance="urn:uuid:006D68F3-4421-E811-8759-B7021FA9EAB5"
    Authorization: Digest username="2555428e0", realm="sipgate.de", nonce="W60Y6luJlu4RRKLKBpUQTDAFdxgDCaUq", uri="sip:sipgate.de", response="29f298f70f57c059885a5e29765bed4"
    Allow: INVITE, ACK, BYE, CANCEL, INFO, MESSAGE, NOTIFY, OPTIONS, REFER, UPDATE, PRACK
    Max-Forwards: 70
    Allow-Events: org.3gpp.nwinitdereg
    User-Agent: SIPPER for PhonerLite
    Supported: replaces, from-change, gruu
    Expires: 900
    Content-Length: 0
```

Abbildung 9: Gültigkeitsdauer der Registrierung (900s)**Die interne IP-Adresse des UA wird durch NAT in eine offizielle externe IP umgesetzt. Wie lautet die externe IP und zu welchem Unternehmen gehört diese IP?**

Die externe IP des UA lautet 194.49.221.0 und gehört zur "DFS Deutsche Flugsicherung GmbH".

The screenshot shows the IPinfo.io website interface. At the top, there is a navigation bar with links for Products, Solutions, Why IPinfo?, Pricing, Resources, Docs, Login, and a Sign up button. The main content area displays 'IP range details' for the IP range **194.49.221.0/24**, which is associated with AS62434 - DFS Deutsche Flugsicherung GmbH. On the left, there is a sidebar with a search bar and three menu items: WHOIS Details (highlighted with a blue bar and a right arrow), IP Addresses, and Hosted Domains. The main content area features a 'Summary' table with the following data:

Summary	
Country	Germany
Domain	dfs.de
ASN	AS62434
Registry	ripe
Hosted IPs	256
ID	DFS-NET

Abbildung 10: Lookup-Ergebnisse zur IP (Deutsche Flugsicherung)

3 Verbindungsaufbau und SDP-Protokoll

Welche SIP_Methods unterstützt der Anrufer?

Wie im Screenshot zu sehen unterstützt der Anrufer die SIP-Methoden [INVITE](#), [ACK](#), [CANCEL](#), [OPTIONS](#), [BYE](#), [REFER](#), [SUBSCRIBE](#), [NOTIFY](#), [INFO](#), [PUBLISH](#) und [MESSAGE](#).


```

▼ Session Initiation Protocol (INVITE)
  ▶ Request-Line: INVITE sip:2555428e0@10.231.172.221:49699 SIP/2.0
  ▼ Message Header
    ▶ Record-Route: <sip:217.10.79.9;lr;ftag=as1da87d54>
    ▶ Record-Route: <sip:172.20.40.6;lr>
    ▶ Record-Route: <sip:217.10.68.137;lr;ftag=as1da87d54>
    ▶ Via: SIP/2.0/UDP 217.10.79.9;branch=z9hG4bK620d.70720930871bcf1d63f6077496ee77cd.0
    ▶ Via: SIP/2.0/UDP 172.20.40.6;branch=z9hG4bK620d.458c80f8dc48e38afdc31b1c423a13c0.0
    ▶ Via: SIP/2.0/UDP 217.10.68.137;branch=z9hG4bK620d.e61e620768ab8026e3b97ca6f225b04f.0
    ▶ Via: SIP/2.0/UDP 217.10.77.115:5060;branch=z9hG4bK1f25f9bd
    Max-Forwards: 67
    ▶ From: "anonymous" <sip:anonymous@sipgate.de>;tag=as1da87d54
    ▶ To: <sip:2555428e0@sipgate.de>
    ▶ Contact: <sip:anonymous@217.10.77.115:5060>
    Call-ID: 5d0eca60468d2182243ab84b059ee901@sipgate.de
    [Generated Call-ID: 5d0eca60468d2182243ab84b059ee901@sipgate.de]
    ▶ CSeq: 103 INVITE
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
    Supported: replaces
    Content-Type: application/sdp
    Content-Length: 415
  ▶ Message Body

```

Abbildung 11: Erlaubte SIP-Methoden

Welche Bedeutung haben Trying und Ringing?

Die Response 100 **Trying** bedeutet, dass der next-hop Server die Anfrage erhalten hat und eine un-spezifizierte Handlung vorgenommen wird, um diesen Anruf zu ermöglichen. Nach **Trying** werden die **INVITE** Nachrichten gestoppt.

Die Response 180 **Ringing** bedeutet, dass der UA den **INVITE** erhalten hat und den Nutzer benachrichtigt.

Welche Angabe bzgl. der Absender-Rufnummer erscheint auf dem Display des Empfängers?

In unserem Fall ist die Absender-Rufnummer "anonymous", was auf eine versteckte Rufnummer hin-deutet.

```

▼ Session Initiation Protocol (INVITE)
  ▶ Request-Line: INVITE sip:2555428e0@10.231.172.221:49699 SIP/2.0
  ▼ Message Header
    ▶ Record-Route: <sip:217.10.79.9;lr;ftag=as1da87d54>
    ▶ Record-Route: <sip:172.20.40.6;lr>
    ▶ Record-Route: <sip:217.10.68.137;lr;ftag=as1da87d54>
    ▶ Via: SIP/2.0/UDP 217.10.79.9;branch=z9hG4bK620d.70720930871bcf1d63f6077496ee77cd.0
    ▶ Via: SIP/2.0/UDP 172.20.40.6;branch=z9hG4bK620d.458c80f8dc48e38afdc31b1c423a13c0.0
    ▶ Via: SIP/2.0/UDP 217.10.68.137;branch=z9hG4bK620d.e61e620768ab8026e3b97ca6f225b04f.0
    ▶ Via: SIP/2.0/UDP 217.10.77.115:5060;branch=z9hG4bK1f25f9bd
    Max-Forwards: 67
  ▼ From: "anonymous" <sip:anonymous@sipgate.de>;tag=as1da87d54
    SIP from display info: "anonymous"
    ▶ SIP from address: sip:anonymous@sipgate.de
    SIP from tag: as1da87d54
  ▼ To: <sip:2555428e0@sipgate.de>
    ▶ SIP to address: sip:2555428e0@sipgate.de
  ▶ Contact: <sip:anonymous@217.10.77.115:5060>
    Call-ID: 5d0eca60468d2182243ab84b059ee901@sipgate.de
    [Generated Call-ID: 5d0eca60468d2182243ab84b059ee901@sipgate.de]
  ▶ CSeq: 103 INVITE
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
    Supported: replaces
    Content-Type: application/sdp
    Content-Length: 415
  ▶ Message Body

```

Abbildung 12: Display-Info des SIP-Headers ("anonymous")

Der sehr lange "branch"-Wert ist eine Zufallszahl und identifiziert eindeutig eine SIP-Vermittlungsinstanz. Berechnen Sie die Wahrscheinlichkeit, dass zwei SIP-Geräte einen identischen Wert erwürfeln (es zählen nur die Angaben zwischen den beiden Punkten).

Mittels folgendem JavaScript-Code wurden die Anzahl an Möglichkeiten berechnet:

```

1 Math.pow(
2   16,
3   "z9hG4bK620d.70720930871bcf1d63f6077496ee77cd.0".split(".")[1].length
4 );

```

Wir kommen zur folgenden Anzahl an Möglichkeiten:

```

1 3.402823669209385e38;

```

Die Wahrscheinlichkeit, dass zweimal diesselbe Zahl berechnet wird, lässt sich also wie folgt berechnen:

```

1 1 /
2   Math.pow(
3     16,
4     "z9hG4bK620d.70720930871bcf1d63f6077496ee77cd.0".split(".")[1].length
5   );

```

Wir kommen zur folgenden Wahrscheinlichkeit:

```
1 2.938735877055719e-39;
```

Die Wahrscheinlichkeit für eine Kollision ist, wie zu erwarten sehr klein.

Beschreiben Sie Aufbau und Inhalt des Session Description Protokoll (SDP), insbesondere die verwendeten Portnummern und das Audio-Video-Profil AVP, das die erlaubten Codecs in einer priorisierten Reihenfolge angibt.

TODO: In SDP werden Eigenschaften von Multimediadatenströmen aufgezeigt. SDP beinhaltet die Sitzungsbeschreibungen (Protokollversion (v), Session-ID (o)), die Zeitbeschreibung und die Medienbeschreibung (Medientyp, Port und Protokoll (m))

Welcher Sprach-Codec wird hier eingesetzt? Wie hoch ist die Bitrate dieses Codes?

Wie im folgenden zu sehen wird der Codec G.711 verwendet. Dieser Codec weist eine Bitrate von 64 kbit/s. Diese Bitrate resultiert aus den 8000 samples pro Sekunde mit jeweils 8 Bit.

10	39.362092	212.9.44.249	212.9.44.249	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=11383, Time=989
16	39.323881	212.9.44.249	16.231.172.221	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=58597, Time=582584289
17	39.339798	16.231.172.221	212.9.44.249	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=11384, Time=890
19	39.346934	212.9.44.249	16.231.172.221	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=58598, Time=582584440
19	39.360726	16.231.172.221	212.9.44.249	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=11385, Time=960
20	39.367082	212.9.44.249	16.231.172.221	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=58599, Time=582584600
21	39.389667	16.231.172.221	212.9.44.249	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=11386, Time=1120
22	39.386769	212.9.44.249	16.231.172.221	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=58600, Time=582584760
23	39.400150	16.231.172.221	212.9.44.249	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=11387, Time=1280
24	39.406876	212.9.44.249	16.231.172.221	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=58601, Time=582584920
25	39.420606	16.231.172.221	212.9.44.249	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=11388, Time=1440
26	39.426763	212.9.44.249	16.231.172.221	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=58602, Time=582585080
27	39.440138	16.231.172.221	212.9.44.249	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x81C1E8A8, Seq=11389, Time=1600

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

▶

Abbildung 13: Auszug des RTP-Captures (Codec G.711)

4 RTP/RTCP

Dokumentieren Sie den RTP-Kommunikationsfluss anhand der IP-Adressen. Wer kommuniziert mit wem?

TODO: Add interpretation



Abbildung 14: Flow-Chart des Kommunikationsflusses

Wieviel „Audio-Samples“ (Abtastproben) enthält ein Ethernet-Paket? In welchen zeitlichen Abständen werden die Pakete gesendet?

TODO: In digitaler Telephonie wird üblicherweise mit 8000Hz gearbeitet. Die Samplerate kann dann im Media-Attribute eingestellt werden.

Welche Ethernet-Paketlänge wird übertragen? Warum fasst man nicht längere oder kürzere Zeiträume zusammen?

TODO: Add interpretation

```

▼ Frame 391: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface \Device\NPF_{60B079C4-4A54-4F24-9289-5222073BB27F}, id 0
  ► Interface id: 0 (\Device\NPF_{60B079C4-4A54-4F24-9289-5222073BB27F})
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 20, 2018 14:48:26.957950000 CEST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1537447706.957950000 seconds
  [Time delta from previous captured frame: 0.005803000 seconds]
  [Time delta from previous displayed frame: 0.005803000 seconds]
  [Time since reference or first frame: 43.066884000 seconds]
  Frame Number: 391
  Frame Length: 214 bytes (1712 bits)
  Capture Length: 214 bytes (1712 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:rtp]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
▼ Ethernet II, Src: Tp-LinkT_5e:ff:c6 (60:e3:27:5e:ff:c6), Dst: Mettler-_c8:d2:7f (00:e0:7c:c8:d2:7f)
  ► Destination: Mettler-_c8:d2:7f (00:e0:7c:c8:d2:7f)
  ► Source: Tp-LinkT_5e:ff:c6 (60:e3:27:5e:ff:c6)
  Type: IPv4 (0x0800)

```

Abbildung 15: Länge des Ethernet-Frames (214 bytes)

Wie groß ist die Verzögerungszeit über das Verbindungsnetz?

TODO: Translate answer

In your captured trace select any RTCP packet, then right click on mouse, Select “Protocol Preferences” then select “Show relative roundtrip calculation” Secondly now apply a Display filter: `rtcp.roundtrip-delay`.

TODO: Add interpretation (is it only half the roundtrip delay?)

rtcp.roundtrip-delay				
Source	Destination	Protocol	Length	Info
212.9.44.249	10.231.172.221	RTCP	106	Sender Report (roundtrip delay <-> 212.9.44.249 = 11ms, using frame 81) Source descrip...

Abbildung 16: Roundtrip-Delay eines RTP-Pakets, wie es von RTCP dargestellt wird

Können Sie auch RTCP-Pakete erkennen? Wie häufig werden sie gesendet? Welchem Zweck dienen sie?

Es sind RTCP-Pakete in regelmäßigen Abständen zu finden. In unserem Fall beträgt das Zeitintervall zwischen von einer Node ausgehenden Nachrichten 10 Sekunden. Das ist insofern passend, da das minimale Zeitintervall zwischen RTCP-Paketen 5 Sekunden betragen sollte. RTCP dient dem Zweck Statistiken und Kontrollinformationen über RTP-Sessions bereitzustellen.

Welche Portnummern werden für die RTP-Verbindung verwendet, welche für die zugehörigen RTCP-Kontrollkanäle (Wireshark: VoipCalls – SIPFlows - FlowSequence)

RTCP verwendet den Port 49702 bei der einen Node und 21805 bei der anderen. Relativ dazu betragen die RTP Ports 49701 und 21804. Dies ist jeweils der um 1 verringerte RTCP Port.



Abbildung 17: Port-Nummern von RTP und RTCP

5 SIP-Byte

Beschreiben Sie, wie der BYE-Method-Timer arbeitet?

TODO: Translate answer

This document provides an extension to SIP that defines a session expiration mechanism. Periodic refreshes, through re-INVITEs or UPDATEs, are used to keep the session active. The extension is sufficiently backward compatible with SIP that it works as long as either one of the two participants in a dialog understands the extension. Two new header fields (Session-Expires and Min-SE) and a new response code (422) are defined. Session-Expires conveys the duration of the session, and Min-SE conveys the minimum allowed value for the session expiration. The 422 response code indicates that the session timer duration was too small.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
2	0.499997	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
3	1.500125	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
4	3.501388	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
5	7.503520	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
6	11.503866	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
7	15.504054	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
8	19.504955	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
9	23.505509	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
10	27.505805	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
11	31.506609	10.237.225.16	10.237.225.1	SIP	370	Request: BYE sip:30080@10.237.225.1:5060
12	67.993497	10.237.225.1	10.237.225.16	SIP/SDP	760	Request: INVITE sip:10.237.225.16:5060
13	68.000536	10.237.225.16	10.237.225.1	SIP	287	Status: 100 Trying
14	68.009133	10.237.225.16	10.237.225.1	SIP/SDP	806	Status: 200 OK (INVITE)
15	68.014841	10.237.225.1	10.237.225.16	SIP	403	Request: ACK sip:10.237.225.16:5060


```

▶ Frame 12: 760 bytes on wire (6080 bits), 760 bytes captured (6080 bits) on interface \Device\NPF_{60B079C4-4A54-4F24-9289-5222073BB27F}, id
▶ Ethernet II, Src: Frequent_01:17:f9 (00:01:bb:01:17:f9), Dst: Frequent_01:72:dd (00:01:bb:01:72:dd)
▶ Internet Protocol Version 4, Src: 10.237.225.1, Dst: 10.237.225.16
▶ User Datagram Protocol, Src Port: 5060, Dst Port: 5060
▼ Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:10.237.225.16:5060 SIP/2.0
    Method: INVITE
    Request-URI: sip:10.237.225.16:5060
      Request-URI Host Part: 10.237.225.16
      Request-URI Host Port: 5060
    [Resent Packet: False]
  Message Header
    ▶ Via: SIP/2.0/UDP 10.237.225.1:5060;rport;branch=z9hG4bK1118337311
    ▶ From: <sip:30080@10.237.225.1:5060>;tag=158381371
    ▶ To: <sip:10.237.225.16:5060>
    Call-ID: 1912313353
    [Generated Call-ID: 1912313353]
    ▶ CSeq: 20 INVITE
    Contact: <sip:30080@10.237.225.1:5060>
    Content-Type: application/sdp
    Allow: INVITE, ACK, BYE, CANCEL, INFO, UPDATE, REFER, NOTIFY, SUBSCRIBE, OPTIONS
    Max-Forwards: 70
    User-Agent: SipLib2-rel_1_509_0
    Subject: phone
    Supported: timer, replaces
    Session-Expires: 90
    Min-SE: 90
    Content-Length: 187
  ▶ Message Body

```

Abbildung 18: Re-INVITE mit Session Timer



Abbildung 19: Flowgraph mit Re-Tries für den BYE-Request

Berechnen Sie die Bandbreite einer bidirektionalen VoIP-Verbindung (mit dem Codec G.711) mit den angegebenen Zahlenwerten. Gehen Sie dabei davon aus, dass alle 20 ms ein Sprachpaket abgegeben wird

Teil	Größe
FCS	4 Byte
Payload	160 Byte
RTP	16 Byte
UDP	8 Byte

Teil	Größe
IP	20 Byte
Ethernet	14 Byte

- Alle 20ms ein Sprachpaket
- Pro Sekunde: $\frac{1000ms}{20ms} = 50 \text{ Sprachpakete/s}$
- Wie groß ist jedes der Pakete?
- $4 \text{ Byte} + 160 \text{ Byte} + 16 \text{ Byte} + 8 \text{ Byte} + 20 \text{ Byte} + 14 \text{ Byte} = 222 \text{ Byte}$
- $50 \text{ Sprachpakete/s} \cdot 222 \text{ Bytes} = 11100 \text{ Bytes/s} = 88800 \text{ Bit/s} = 88 \text{ kBit/s}$
- Die Bandbreite einer VoIP-Verbindung beträgt mit dem G.711-Codec 88 kBit/s.