

Rechnernetze & Telekommunikation
SoSe 2021
LV 2142

Übungsblatt 10

Bearbeiten Sie diese Aufgaben bitte **vor** Beginn Ihrer Praktikumsgruppe und halten Sie Ihre Ergebnisse **schriftlich** in einem Protokoll Ihrer Versuche fest. Die nötigen Informationen über ACLs erhalten Sie aus den Vorlesungen (<https://video.cs.hs-rm.de/course/5/lecture/84/> und <https://video.cs.hs-rm.de/course/5/lecture/87/>, Rechnernetze und Telekommunikation > 12/13 IPv6 Teil 2 & NGNs und VoIP Teil 1 und 2).

Zu Beginn werden Einzelne vom Praktikumsleiter stichprobenartig gebeten elektronisch abzugeben. Die Bearbeitung der Fragen bildet mit eine Grundlage der Bewertung.

Die Fragen werden anschließend in der Praktikumsgruppe interaktiv besprochen und vorgeführt.

Vorbemerkungen und Hinweise

Für diesen Versuch können Sie sich einen VoIP-Client auf Ihrem Rechner installieren, z.B. „Linphone“ von <https://www.linphone.org/>. Nutzen Sie hier die folgenden Einstellungen (abweichend default: DTMFs und STUN):

The screenshot shows the 'Einstellungen' (Settings) window of the Linphone application. The window has a title bar with standard Windows controls and a menu bar with 'Netzwerkeinstellungen', 'Multimedia-Einstellungen', 'SIP-Konten verwalten', 'Codecs', and 'Benutzeroberfläche'. The 'Multimedia-Einstellungen' tab is active.

Übertragung

- ☒ Maximum Transmission Unit setzen: 1300
- ☒ DTMFs als SIP-Info senden
- ☐ IPv6 statt IPv4 verwenden

Netzwerkprotokoll und Ports

SIP/UDP Port	<input type="checkbox"/> Gesperrt	<input type="checkbox"/> Random	5060
SIP/TCP Port	<input type="checkbox"/> Gesperrt	<input type="checkbox"/> Random	5060
Audio RTP/UDP:	7078	7078	<input checked="" type="checkbox"/> Fest
Video RTP/UDP:	9078	9078	<input checked="" type="checkbox"/> Fest

Verschlüsselungstyp der Medien: Keinen

☐ Medienverschlüsselung erzwingen

DSCP-Felder: [Empty]

[Bearbeiten]

NAT und Firewall

- ☐ Direkte Verbindung ins Internet
- ☐ Hinter NAT / Firewall (Gateway IP angeben)
- ☒ Hinter NAT / Firewall (STUN verwenden)
- ☐ Hinter NAT / Firewall (ICE verwenden)

Öffentliche IP-Adresse: [Empty]

STUN-Server: stun.sipgate.net:10000

[Fertig]

Falls Sie bereits einen anderen SIP-fähigen Client haben, sollte auch das funktionieren. Fall Sie keinen Client installieren können, finden Sie unter „Trace VoIP“ auch einen bereits aufgenommenen Trace, den Sie weiter analysieren können.

Aufgabe 10.1: VoIP Analyse

Rufen Sie mit Ihrem Client die SIP-Adresse sip:301@ideasip.com an. Wen erreichen Sie dort? Schneiden Sie den Netzverkehr Ihres Rechners während des VoIP-Telefonates mit, beantworten Sie anschließend die folgenden Fragen und belegen Sie Ihre Antworten im Trace:

- a) Welche VoIP-Protokolle werden benutzt?
- b) Welche IPs hatte die Gegenstellen?
- c) Welcher PBX (Vermittlungs) Software benutzt die Gegenstelle?
- d) Welche Sprach-Codecs werden vom Client angeboten?
- e) Welcher Codec wird dann für die Sprachübertragung benutzt?
- f) Wie lange dauerte das Gespräch?
- g) Was ist „Jitter“? Wie groß war der maximale Jitter der empfangenen Pakete?
- h) Erstellen Sie eine Nachrichten-Diagramm vergleichbar zu Folie 26 der VoIP-Vorlesung für diese Kommunikation.
- i) Ist die Übertragung verschlüsselt? Können Sie rekonstruieren, was in dem Telefonat gesagt wurde?
- j) Wozu dienen die „CLASSIC-STUN“ Pakete vor dem Beginn der Verbindung?

Aufgabe 10.2: SIP-Provider

Informieren Sie sich, mit welchen Konditionen Sie einen Account bei einem SIP-Provider erhalten können:

- a) Welchen SIP-Provider haben Sie betrachtet?
- b) Wie sieht das Kostenmodell aus?
- c) Welche Vorteile gäbe es im Vergleich mit einem „normalen“ Festnetzanschluss?