Telefonie über das Internet

(Voice-over IP / VoIP) aus der Sicht des Fernmeldegeheimnisses (§ 85 TKG)

Peter Blauth, Sebastian Fandrich, Patrick Fröger,
Daniel Renoth, Tobias Schnetzer und Uwe Weissenbacher

FH Furtwangen

20.01.2006

Inhalt

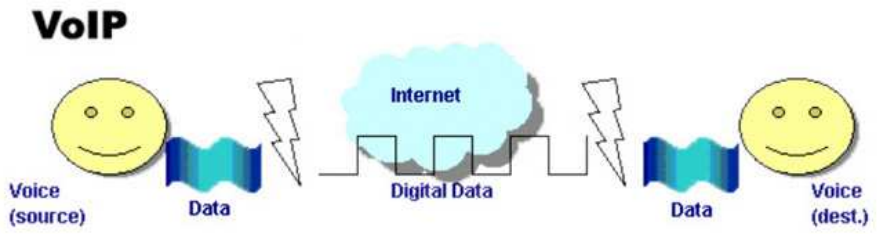
Einführung

- Was ist Voice over IP?
- Vorteile von VoIP
- VoIP Tarifübersicht

Was ist Voice over IP?

- VOIP steht für Voice over Internet Protokoll
- Telefonieren über das IP-Protokoll
- Analoge Sprachsignale in Digitale Sprachsignale

Was ist Voice over IP? Fortsetzung



- Zugang zu VoIP über:
  - PC mit DSL-Anschluss und installierter Telefonsoftware
  - spezielles IP-Telefon an einen Router
  - Analoge Telefone mittels Hilfe eines Adapters

Vorteile von VoIP

- Kosten senken durch Voice over IP:
  - Verbindungskosten Serviceprovider über Flatrate läuft
  - Verbindungskosten Vermittlungstelle - Haus nur einmal
  - Gespräche zu anderen IP-Teilnehmer teilweise kostenlos
- Erreichbarkeit erhöhen:
  - überall wo Internetanschluss besteht
- Einsatz verschiedenster Endgeräte möglich:
  - PC mit entsprechender Software
  - spezielle IP Telefone
  - Analag Telefon mit Adapter

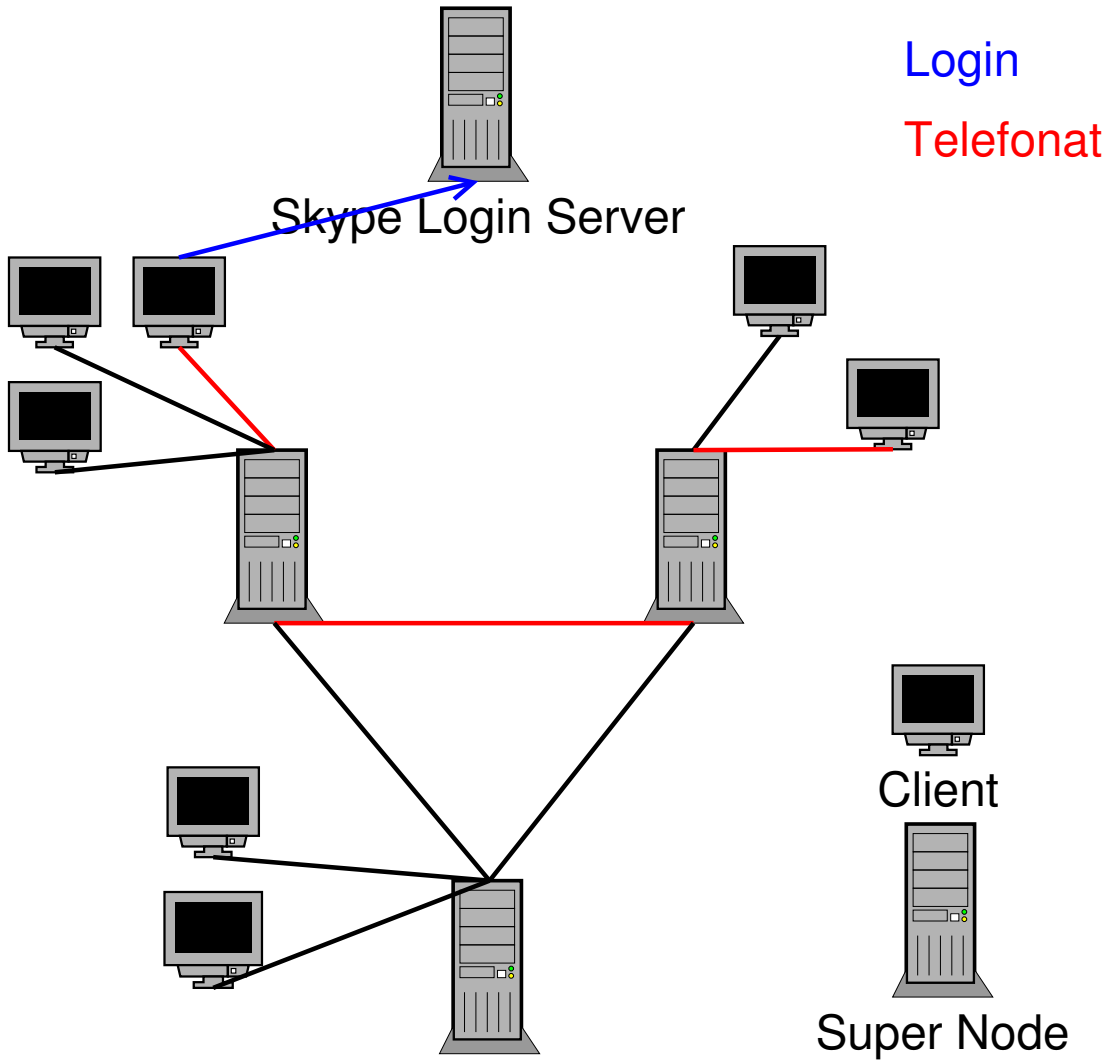
VoIP Tarifübersicht

VoiP Internettelefonie	1&1/GMX	Freenet	T-online	Stra
Minutenpreis ins deutsche Festnetz	1 Ct	1 Ct	2,9 Ct	1 C
Flatrate Preis ins deutsche Festnetz	9,99 €	9,90 €	-	9,90
Minutenpreis ins Ausland ab	1,9 Ct	2,1 Ct	4,9 Ct	2,1
Minutenpreis in Mobilfunk ab	22,9 Ct	19 Ct	22 Ct	19
Netzintern + Partner kostenlos	✔	✔	✔	✔
Abrechnungstakt	60	60	60	60
Einzelverbindungsnachweis	✔	-	-	-

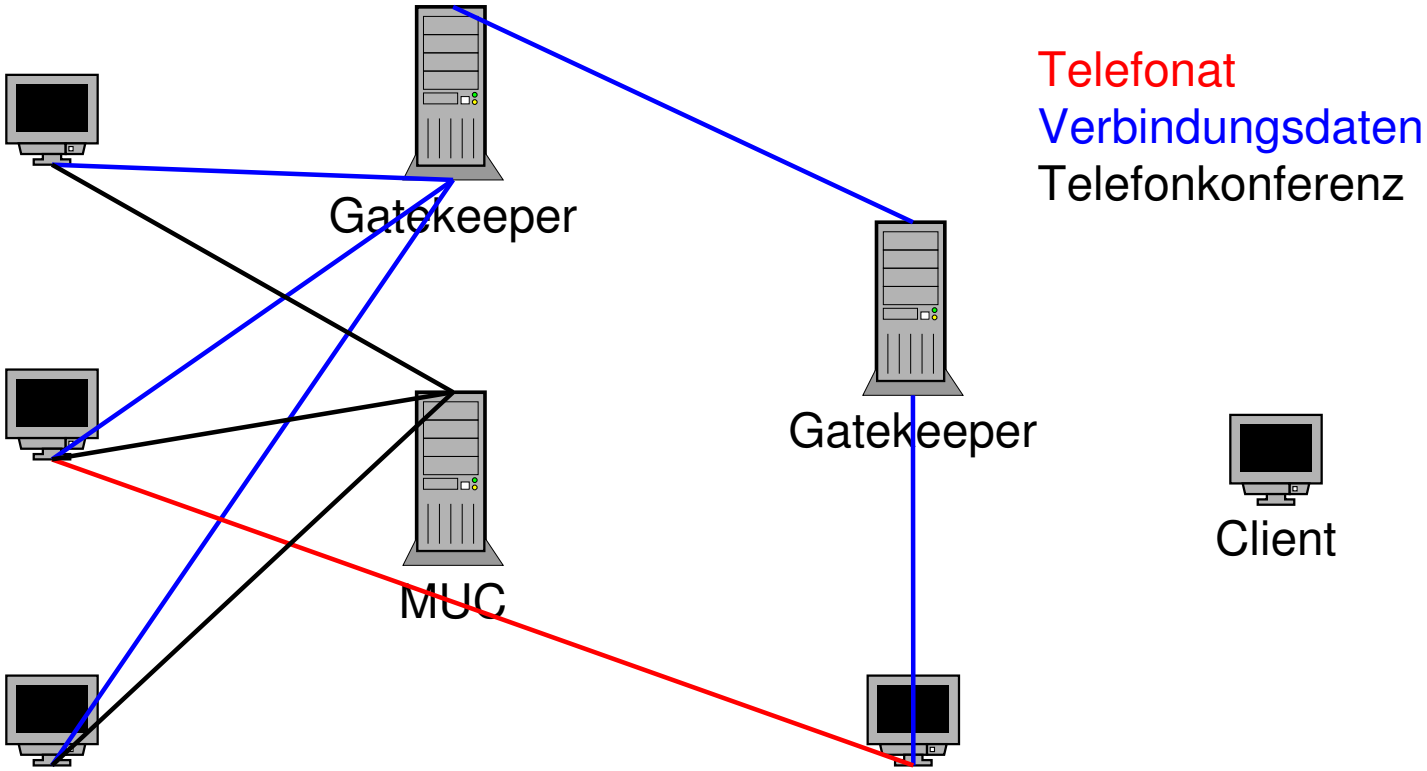
Protokollübersicht

	H.323	SIP	Skype
Standard	ITU-T	RFC 3261	propritär
Verfügbarkeit	kostenpflichtig	offen	-
Verschlüsselung	mit H.235	nein	ja
NAT-fähig	nein	nein	ja
Direkte Verbindung	ja	ja	nein

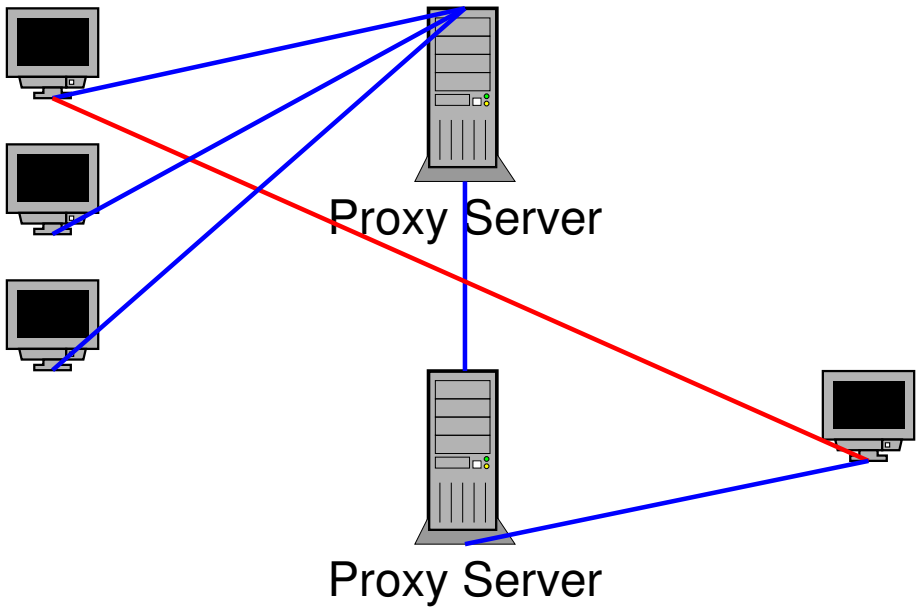
Skype Netzwerk



H.323 Netzwerk



SIP Netzwerk



Telefonat
Verbindungsdaten

Client

Übersicht der Angriffs-/Belästigungsmöglichkeiten

- Abhörbarkeit
- Bestehende Verbindungen manipulieren
- Spoofing
- Malformed messages
- Man-in-the-Middle Attacken
- Registration Hijacking
- Spit

Abhören von SIP-Verbindungen

- Alle SIP-Pakete werden im Klartext übertragen
- Mit einem Sniffer kann die komplette Kommunikation mit geschnitten und wieder gegeben werden
- Ein Angreifer kann Headerinformationen (From/To-Tags, Call-ID, Route, CSeq) sammeln, um bestehende Verbindungen zu manipulieren

Manipulieren bestehender Verbindungen

- Eine bestehende Verbindung kann mit einem BYE-Paket beendet werden
- Durch ein INVITE-Paket initiierter Verbindungsaufbau kann durch ein CANCEL-Paket beendet werden
- Können auch falsche Identitäen vorgetäuscht werden

Phising und DDoS

- SIP-Header und -Body können gespooft werden
- INVITE-Pakete mit gefälschter From-Headerzeile senden
- Kann DDoS Attacke auslösen
- Kann Anrufer ändern

Auswirkungen von Malformed Messages

- Malformed Messages: SIP-Pakete die nicht standardkonform sind
- Beispiele
  - Weglassen oder unvollständige Headern (DoS bei Grandstream BudgeTone 101)
  - Falsche Längenangaben für SIP-Body
  - Ungültige Headerinhalte
- Folgen
  - DoS
  - Instabilität des Systems
  - Systemabsturz

Man-in-the-Middle Attacken

- Angreifer hat Zugriff auf Netzwerk oder SIP-Proxy
- Kann schwache oder keine Verschlüsselung für die Sprachdaten erzwingen
- Kann Gespräche umleiten, auch dauerhaft

SIP-Benutzerdaten ändern

- Angreifer benutzt fremde Kontakte mit eigenem Gerät
- Deregistrierung bestehender Registrierungen
- Kann Gespräche umleiten, auch dauerhaft

Werbung mit VOIP

- Unaufgeforderte, automatisierte Werbeanrufe
- Vergleichbar mit Spam
- Kleinere Gefahr - Rufnummern über VoIP-Peering-Zentrale e164.info. Partnernetzen zugeordnet
- Verbundfremde oder verdächtige Nummern geblockt

Fernmeldegeheimnis § 88 TKG

- § 88 Fernmeldegeheimnis (ehemals §85):
  - (1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.
  - (2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

Fernmeldegeheimnis § 88 TKG - Fortsetzung

- § 88 Fernmeldegeheimnis (ehemals §85):
  - (3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.
  - (4) ...

Umfrage der Bundesnetzagentur zum Thema VoIP - Zusammenfassung

- Das Fernmeldegeheimnis bezieht sich auf "Telekommunikation" und damit unterliegen VoIP-Anbieter in jedem Fall auch dem Fernmeldegeheimnis. Diese Aussage geben fast alle Anbieter.
- Stehen VoIP-Dienste in Verbindung mit dem klassischen Telefonnetz ... sind die Regelungen der §§ 89-103 und § 105 TKG-E in vollem Umfang anwendbar. Quelle [BNABfD]

Abhören von VoIP, § 110ff TKG

- Erste technische (Übergangs-) Regelung im Amtsblatt der Bundesnetzagentur vom 27. Juli 2005
- Seit Anfang 2006 muss diese von den Anbietern umgesetzt sein
- Signalisierungsdaten
- Es wird bereits gelauscht, VoIP Anbieter erhalten Anfragen

Sicherheitsmechanismen - Secure RTP

Secure RTP (Real-time Transport Protocol)

- Verschlüsselung des Datenstroms (AES)
- Nachrichtenauthenisierung und Absicherung der Nachrichtenintegrität (HMAC-SHA1)
  $\Rightarrow$Spoofing der Nachricht wird unmöglich
- Weitere Details siehe RFC 3711

Sicherheitsmechanismen - SpIT

SpIT(Spam over Internet Telephony)

- "SPAM des VoIPs"
- Noch nicht weit verbreitet

Problematik:

- Filterung nicht anhand Inhalt oder Stimme möglich

Sicherheitsmechanismen - SpIT

Mögliche Lösungsansätze

- Erkennen automatisierter Anrufe bereits im Backbone
- White List-Ansatz: Jeder Anschluss muss bei einem zentralen Registrierungsstelle angemeldet werden

Gesetzliche Entwicklung in Deutschland

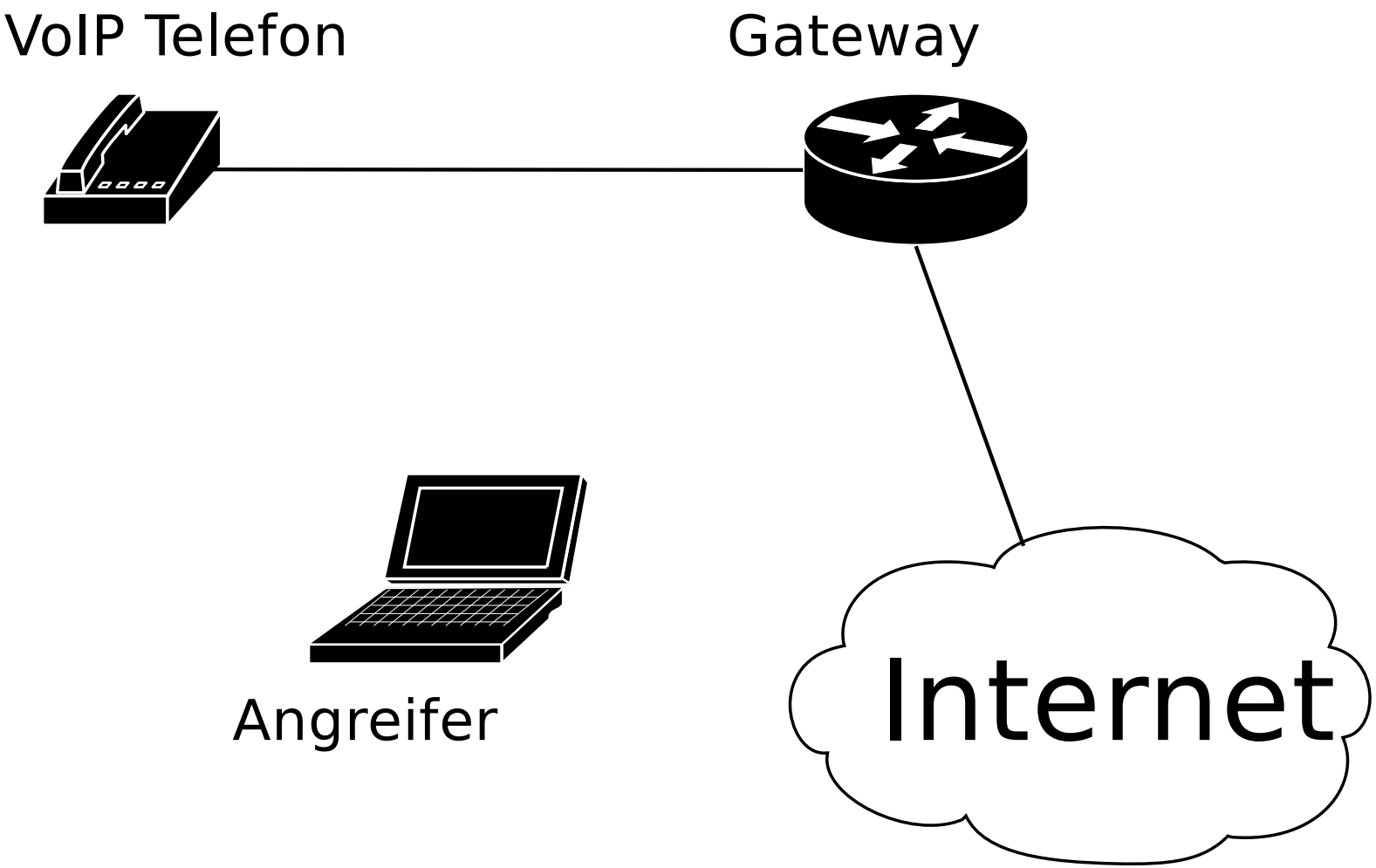
Definition einer standardisierten Überwachungsschnittstelle (ETSI - *European Telecommunications Standards Institute*)

- Bezeichnet mit ETSI TS 102 227
- Überwachung des Gesprächsinhaltes
  - Filterung
  - Ausleiten des Gespräches
- Die Benutzung dieser Schnittstellen wird durch die BNetzA zeitnah in nationalem Recht festgeschrieben

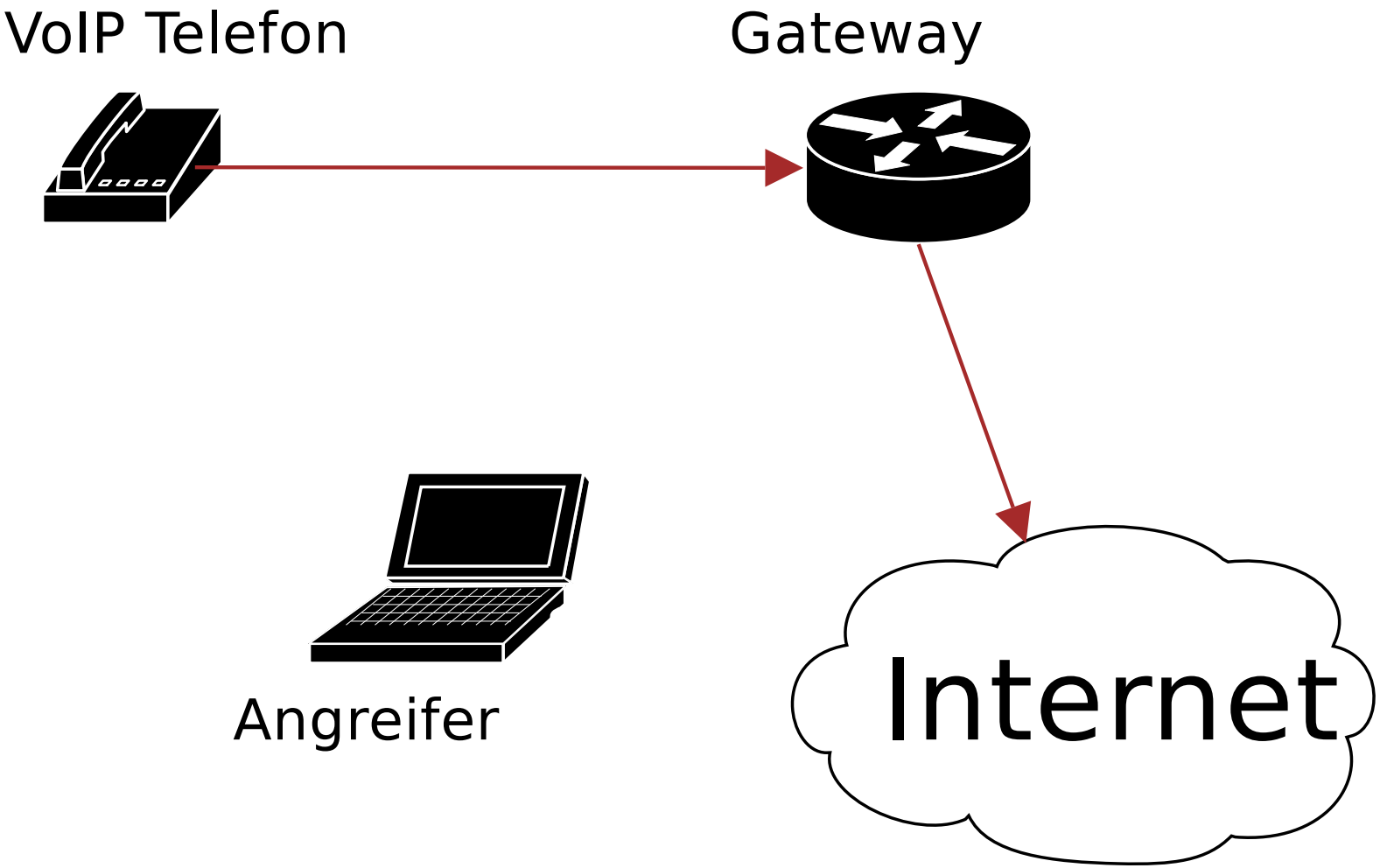
Demonstration

- VoIP Telefonat mitschneiden
- DoS Grandstream Budge Tone-100

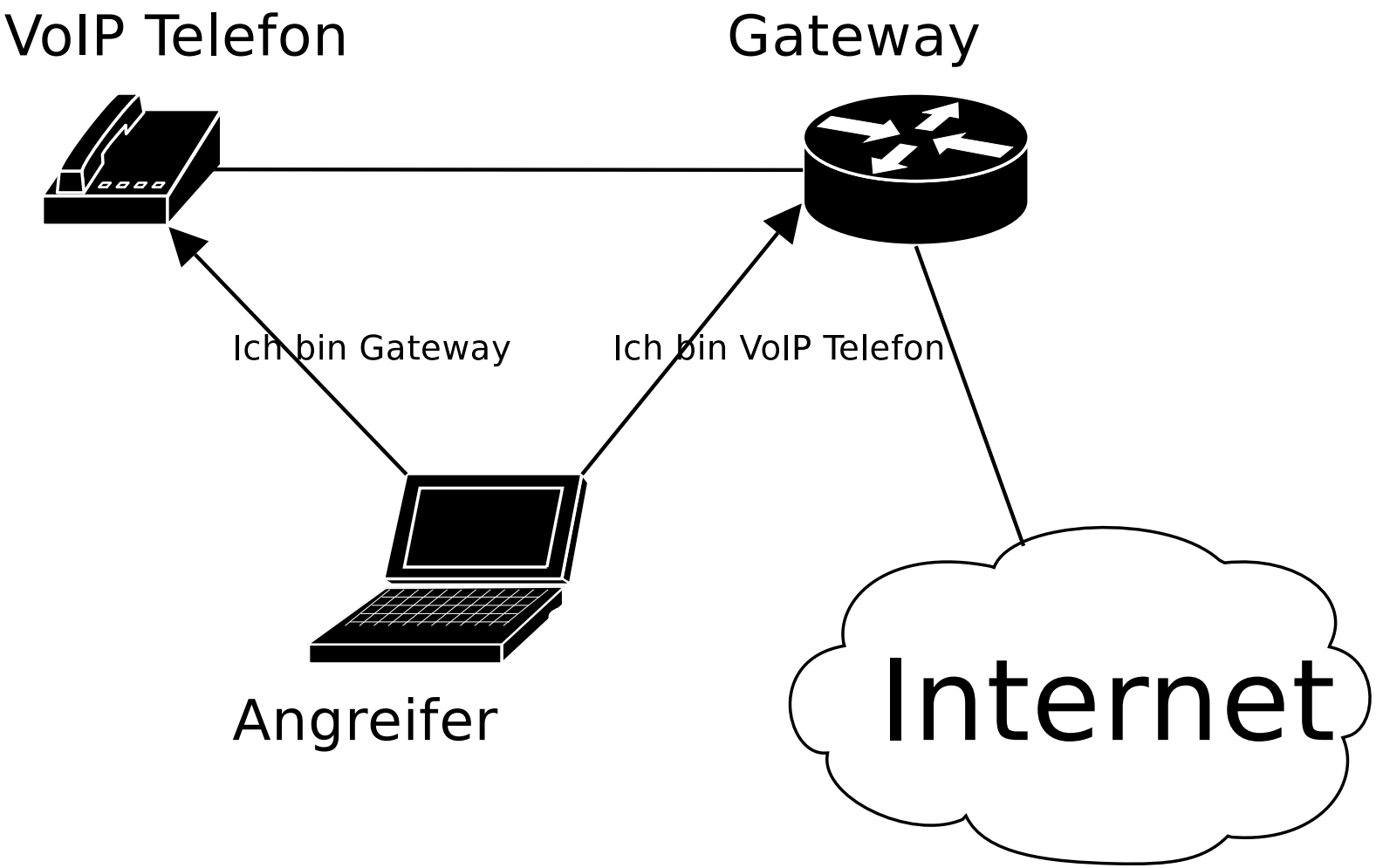
VoIP Abhören - 1



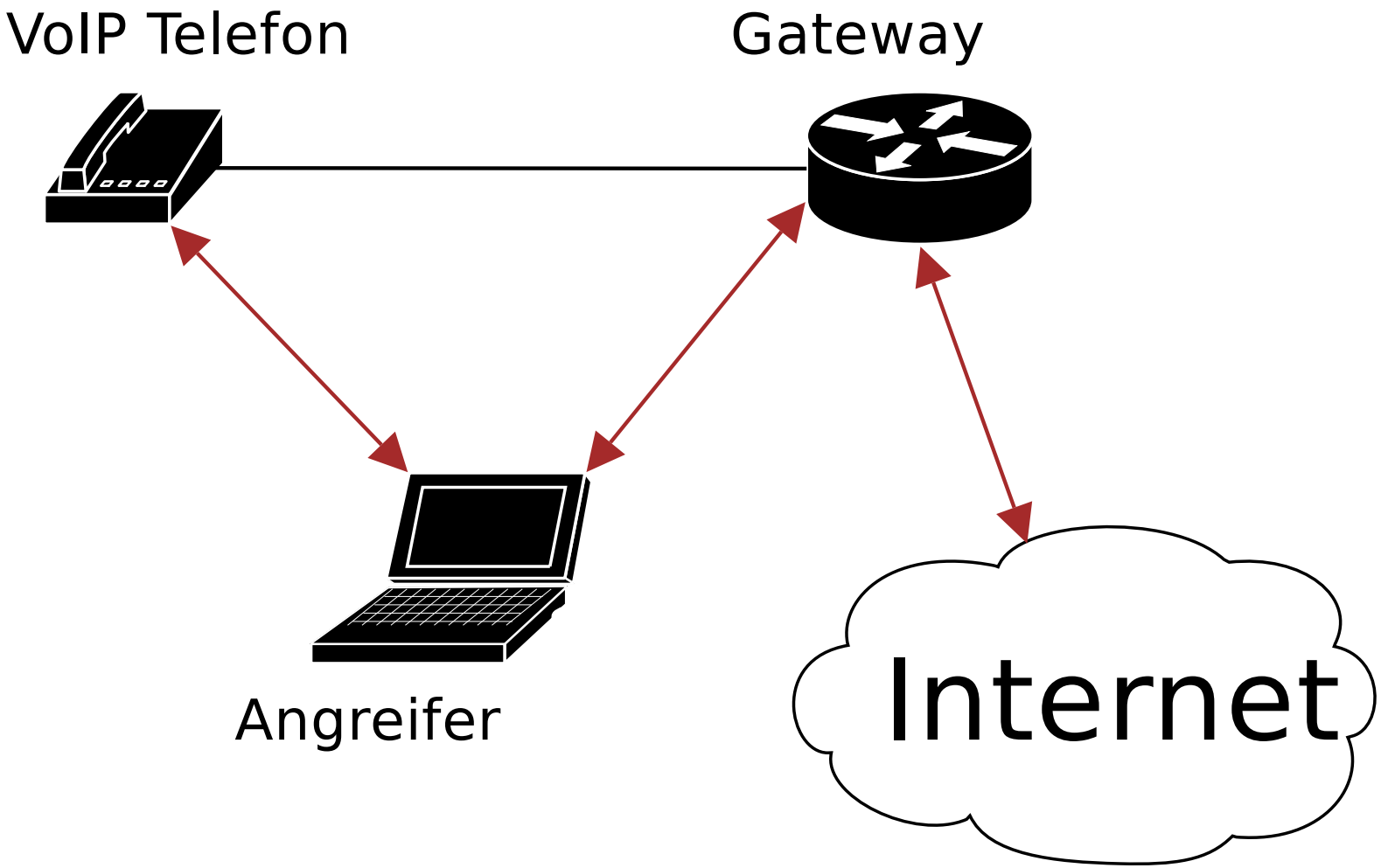
VoIP Abhören - 2



VoIP Abhören - 3



VoIP Abhören - 4



Vielen Dank für ihre Aufmerksamkeit!
Fragen?

BNABfD