ingenieur
wissenschaften
htw saar

Hochschule für
Technik und Wirtschaft
des Saarlandes
University of
Applied Sciences

Zusammenfassung des TK-Praktikum des sechsten Semesters Kommunikationsinformatik

Praktikum

Deniz Kadiogullari und Christoph Drost

Erstgutachter: Harald Krauss

Zusammenfassung

Kurze Zusammenfassung des Inhaltes in deutscher Sprache, der Umfang beträgt zwischen einer halben und einer ganzen DIN A4-Seite.

Orientieren Sie sich bei der Aufteilung bzw. dem Inhalt Ihrer Zusammenfassung an Kent Becks Artikel: http://plg.uwaterloo.ca/~migod/research/beckOOPSLA.html.

Inhaltsverzeichnis

1 GSM Versuch

1.1 Allgemeine Beschreibung der Versuche

Im folgenden handelt es sich um ein Test-Versuch GSM. GSM ist die Abkürzung für Global System for Mobile Communications und ein Standard für die volldigitale Mobilfunknetze. Wir haben ihn bereits kennen gelernt, da alle unsere Handys darauf beruhen. GSM ermöglicht die eigentliche Telefonie, eine Datenübertragung und das Versenden und Empfangen von SMS, Short Message Services. Mittlerweile wurden für die Datenübertragung leistungsfähigere Standards, wie UMTS und LTE entwickelt, jedoch ist GSM noch nicht wegzudenken.

Der Versuch soll das Verständnis für die Technik vertiefen, die den reibungslosen Ablauf unserer Handygespräche ermöglicht. Zu diesem Zweck steht uns ein System zur Verfügung, das aus einer Antenne, der Technik zur Signalverarbeitung und einem Computer mit entsprechender Software besteht.

1.1.1 Versuchsaufbau

Der Aufbau des Versuchs ist auf den ersten Blick leicht beschrieben: Unser System besteht aus einer Antenne 1.1.2.1, einem USPR 1.1.2.2 und einem Computer 1.1.2.3.

1.1.2 Die einzelnen Bauteile im Überblick

1.1.2.1 Antenne

Dieses Bauteil wandelt die elektromagnetischen Signale in elektrische Signale um. Antennen sind in prinzipiell in allen Geräten enthalten, die etwas mit Funktechnik zu tun haben. Dazu zählen beispielsweise Radios oder auch Handys. Die Umwandlung hat den Hintergrund, dass die elektromagnetischen Single aus der Luft nicht direkt weiterverarbeitet werden können.

1.1.2.2 USPR

Das USPR, Universal Radio Peripheral, ist eine geschlossene Einheit, die das Verarbeiten der Empfangenen Signale ermöglicht. Es ist modular aufgebaut, sodass ein breites Frequenzspektrum abgedeckt werden kann. Für unseren Versuch interessieren aber nur die Frequenzen des GSM. Das USPR wird im folgenden nicht weiter betrachtet, da es nicht der Gegenstand des Versuchs war, sondern diesen nur ermöglicht hat.

Abbildung 1.1: USPR mit Antenne

1.1.2.3 Computer

Der Computer mit seiner entsprechenden Software ist die für den Versuch am interessanteste Komponente. Er ermöglicht es, die empfangenen Funksignale grafisch darzustellen und auszuwerten. Weiterhin stellt der Computer die Protokolle für den reibungslosen Ablauf und eine vollwertige U_m Schnittstelle zur Verfügung.

Zur Bereitstellung dieser Schnittstelle und der Protokolle wird das Softwarepaket OpenBTS genutzt.

Das Ziel des Versuchs ist es, die Paketdaten mitzuschneiden, die in einem GSM Netz auftreten. Vor dem Mitschnitt soll ein Grundverständnis über die Physik hinter dem GSM Netz geschaffen werden.

1.2 Visualisieren von Frequenzen

1.2.1 Frequenzen auflisten

1.2.1.1 Aufbau des Versuchs

Für die Visualisierung der Frequenzen werden die in 1.1.2 beschriebenen Komponenten benötigt. Aus der Softwarepaket OpenBTS werden die Tools lsursp, baudline und kal benötigt.

Neben der vorhandenen Hardware werden keine weiteren Geräte benötigt. Das Vorhandensein von Sendern in der Reichweite des Systems ist dennoch eine Vorraussetzung.

1.2.1.2 Versuchsdurchführung

Mit dem Tool lsursp wird überprüft, ob die USPR 1.1.2.2 vom System erkannt wird.

Nachdem festgestellt wurde, dass die USRP angeschlossen und vom System erkannt wurde, kann der eigentliche Versuch beginnen. Hierzu wird das Tool kal mit dem Kommando „kal -s -DCS“aufgerufen. Kal führt einen Umgebungsscan durch, das bedeutet, dass alle Frequenzen, die im DCS 1800 Band liegen und empfangen werden können, aufgelistet werden können.

1.2.1.3 Auswertung des Versuchs

Zur Erklärung, das DCS 1800 Band ist ein Frequenzband, das den Frequenzbereich um 1800 MHz nutzt. In Deutschland wurde dieser Bereich ursprünglich von den E-Netzen, also dien Anbietern E-Plus und O_2 genutzt. Aus Kapazitätsmangel haben 1999 auch die großen D-Netz Betreiber DCS 1800 Frequenzen erworben. Der Umgebungsscan gibt also die Frequenzen aus, die mit GSM zu tun haben, auf einen Anbieter ist der Scan aber nicht beschränkt. Das Ergebnis der Umgebungsscans ist in Tabelle 1.1 aufgelistet. Jede Zeile dieser Auflistung besteht aus chan mit Frequenzen und power mit einem Wert.

Quellen finden

chan Chan steht in diesem Fall für channel oder channel number. Dieser Wert wird auch als ARFCN, Absolute Radio Frequency Channel Number, bezeichnet. Der Hintergrund ist, dass ein Teilnehmer des GSM Netzes nicht das gesamte Frequenzband benötigt. Bzw. auch, dass andere Kommunikationsteilnehmer einer Base Station ausgeschlossen werden, wenn ein Teilnehmer exklusiv das gesamte Frequenzband nutzt. Deswegen werden die Frequenzbänder in Kanäle (channels), bzw. Kanalpaare, unterteilt. Das Kanalpaar hat den Hintergrund, dass GSM für den Down- und des Uplink unterschiedliche Frequenzen nutzt. Anhand der ARFCN kann die absolute Frequenz berechnet werden, die für die tatsächliche Kommunikation genutzt wird. Die Formel

chan:	555 (1813.8 MHz + 14.632kHz)	power: 1007.18
chan:	602 (1823.2MHz - 8.896kHz)	power 481.48
chan:	619 (1826.6MHz + 572Hz)	power: 1171.37
chan:	620 (1826.8 + 347Hz)	power: 727.63
chan:	630 (1828.8MHz + 177Hz)	power: 1421.75
chan:	631 (1820.0MHz + 209Hz)	power: 2495.22
chan:	637 (1830.2MHz + 403Hz)	power: 2876.83
chan:	640 (1830.8MHz + 508Hz)	power: 36384.61
chan:	641 (1831.0MHz + 508Hz)	power: 8809.88
chan:	647 (1832.2MHz - 32.386Hz)	power: 1305.97
chan:	648 (1832.4MHz - 32470Hz)	power: 10507.76
chan:	700 (1842.8MHz + 386Hz)	power: 21662.59
chan:	701 (1843.0MHz + 455Hz)	power: 4220.36
chan:	706 (1844.0MHz + 387Hz)	power: 27836.79
chan:	709 (1844.6MHz + 2.954Hz)	power: 1148.92
chan:	713 (1845.4MHz + 621Hz)	power: 6744.54
chan:	715 (1845.8MHz + 388Hz)	power: 20091.07
chan:	755 (1853.8MHz - 20.894Hz)	power: 458.32
chan:	764 (1855.6MHz + 485Hz)	power: 19349.83
chan:	765 (1855.8MHz + 381Hz)	power: 9962.32
chan:	769 (1856.6MHz + 38.177Hz)	power: 3226.76
chan:	798 (1862.4MHz + 498Hz)	power: 994.82
chan:	802 (1863.2MHz + 498Hz)	power: 118213.39
chan:	805 (1863.8MHz + 440Hz)	power: 5598.97

Tabelle 1.1: Auflistung der empfangenen Frequenzen

dazu ist in der Abbildung 1.2 beschrieben. Auf diese Thematik wird aber im weiteren Verlauf des Versuchs weiter eingegangen.

Den Scheiß habe ich mir quasi ausgedacht. Stimmt das annähernd?

power Power ist die Stärke, mit der das Signal empfangen wurde. Keine Ahnung welche Einheit.

Berechnung der Frequenzen Wie schon erwähnt, anhand dieser Auflistung ist es möglich, den Frequenzbereichs von DCS 1800 zu errechnen. Zur Berechnung eines Frequenzbereichs gibt es einige Formeln. Welche genutzt wird, hängt davon ab, welche Werte bereits bekannt sind.

Dazu was richtiges schreiben

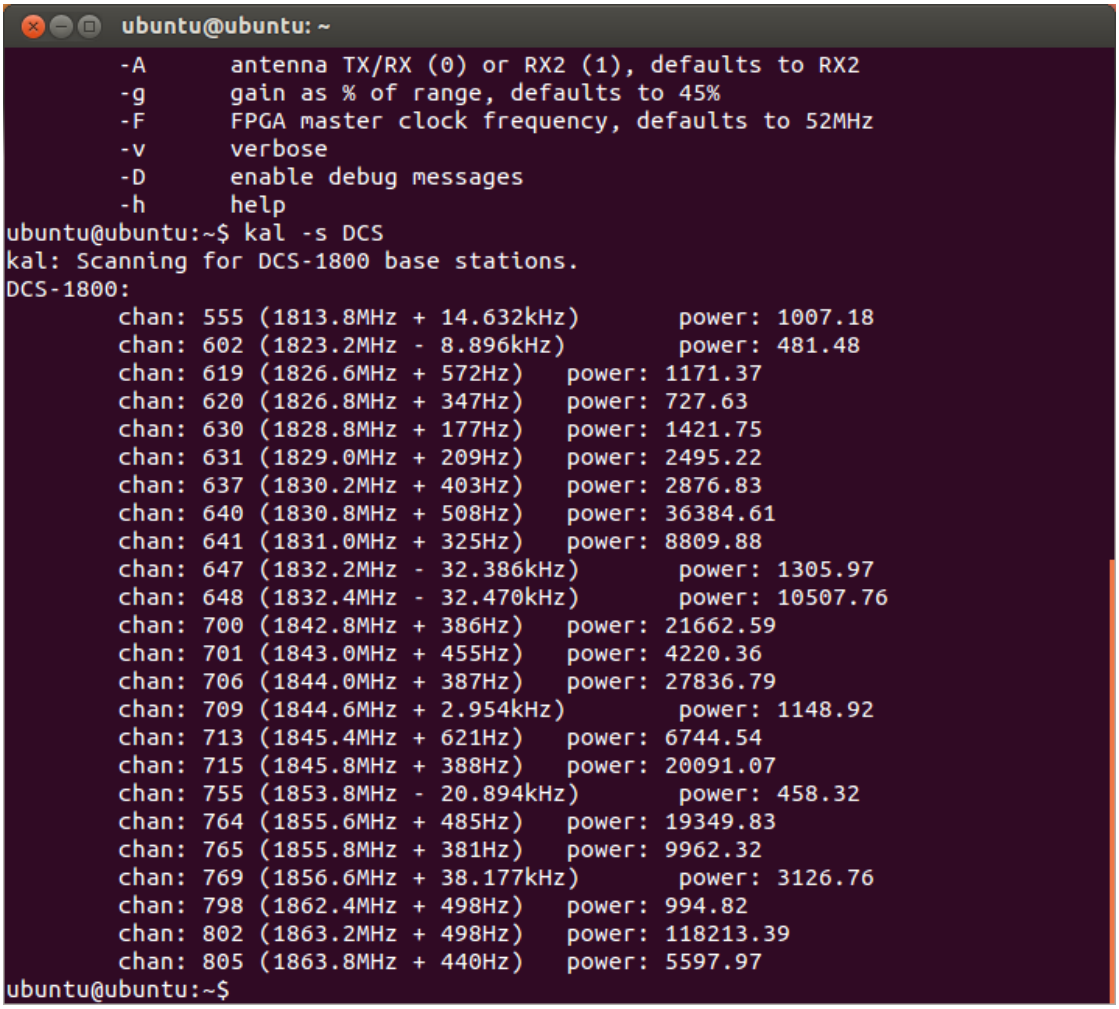


Abbildung 1.2: Screenshot des Umgebungsscans

fuplink = Startfrequenz + (ARFCN -Offset) * 0,2MHz
fdownlink = fuplink + Abstand
fuplink = fdownlink - Abstand
ARFCN = (fuplink - Startfrequenz/0,2 MHZ) + Offset

Tabelle 1.2: Formel zur Berechnung des Frequenzbereichs

Da in unserem Versuch die Antenne als reiner Empfänger gearbeitet hat, haben wir nur Frequenzen empfangen, die von den Sendern als Uplink Frequenzen genutzt werden.

Die empfangenen Frequenzen lassen sich auch einzelnen Providern zuordnen. Für diese Zuordnungen gibt es Pläne, welche Frequenzen an wen vergeben wurden. Auf

Was zur Berechnung schreiben

der folgenden Abbildung ist zu sehen welche Frequenzen in Deutschland von welchem Providern benutzt werden.

	von (MHz)	bis (MHz)	Kurzzeichen	Sendeleistung	Reichweite	Modulation	Gepulst	Betreiber	Sonstiges	Beschreibung
	1.710,0	1.725,0	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	Militär	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.725,2	1.730,0	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	T-Mobile	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.730,2	1.752,4	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	O 2	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.752,8	1.758,0	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	Vodafone	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.758,2	1.780,4	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	E Plus	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.805,0	1.820,0	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	Militär	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)
	1.820,2	1.825,0	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	T-Mobile	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)
	1.825,0	1.847,4	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	O 2	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)
	1.847,8	1.853,0	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	Vodafone	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)
	1.853,2	1.875,4	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	E Plus	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)

Militär
T-Mobile
O2
Vodafone
e-plus

Abbildung 1.3: Frequenzentabelle der Provider [1]

Wenn man die Tabelle 1.1 und die Grafik 1.3 vergleicht, ergibt sich Tabelle **??**. Auffällig ist, dass keine Signale des Anbieters Vodafone empfangen werden, dafür aber mehrere militärische Kanäle.

1.2.2 Frequenzen darstellen

Der Versuch 1.2.1 hat ergeben, dass im GSM Standard verschiedene Frequenzen genutzt werden. Die Tatsache, dass Kanäle mit einer Breite genutzt werden, wirft die Frage auf, was es mit diesen Breiten auf sich hat und wie Informationen übertragen werden.

1.2.2.1 Aufbau des Versuchs

Der Aufbau des Versuchs entspricht grob dem Aufbau des Versuchs 1.2.1. Anstelle des Tools kal wird DSP-Buttler-Tool dsusrp genutzt.

1.2.2.2 Versuchsdurchführung

Vor Beginn des Versuchs muss der Umgebungsscan aus 1.2.1 wiederholt werden. Dadurch kann sicher gestellt werden, dass die Messung mit einer aktiven, bzw. gerade gesendeten Frequenz durchgeführt wird. Nachdem eine Frequenz gefunden wurde,

chan:	555 1813.8 MHz	Militär
chan:	602 1823.2MHz	T-Mobile
chan:	619 1826.6MHz	O_2
chan:	620 1826.8 + 347Hz	O_2
chan:	630 1828.8MHz	O_2
chan:	631 1820.0MHz	Militär
chan:	637 1830.2MHz	O_2
chan:	640 1830.8MHz	O_2
chan:	641 1831.0MHz	O_2
chan:	647 1832.2MHz	O_2
chan:	648 1832.4MHz	O_2
chan:	700 1842.8MHz	O_2
chan:	701 1843.0MHz	O_2
chan:	706 1844.0MHz	O_2
chan:	709 1844.6MHz	O_2
chan:	713 1845.4MHz	O_2
chan:	715 1845.8MHz	O_2
chan:	755 1853.8MHz	E-Plus
chan:	764 1855.6MHz	E-Plus
chan:	765 1855.8MHz	E-Plus
chan:	769 1856.6MHz	E-Plus
chan:	798 1862.4MHz	E-Plus
chan:	802 1863.2MHz	E-Plus
chan:	805 1863.8MHz	E-Plus

Tabelle 1.3: Auflistung der empfangenen Frequenzen

beginnt der eigentliche Versuch mit dem Kommando *dbusrp-f 699219*. Dieses Kommando startet ein Analysetool, das sowohl den Frequenz- als auch den Amplitudenbereich ausgibt.

1.2.2.3 Auswertung des Versuchs

Das Ergebnis dieses Versuchs kann in der Grafik 1.4 betrachtet werden. Die Wellen im oberen Bereich der Darstellung sind die Darstellung im Zeitbereich, die unteren Wellen sind die Darstellung im Frequenzbereich. In der Mitte wird das Signal im Wasserfallmodell darstellt. Das Wasserfallmodell zeigt wie sich die Grundfrequenz durch abziehen oder hinzufügen von Frequenzen verändert wird. Die Darstellung des Signal erinnert

Wat han mir wei davon?

stark an weißes Rauschen

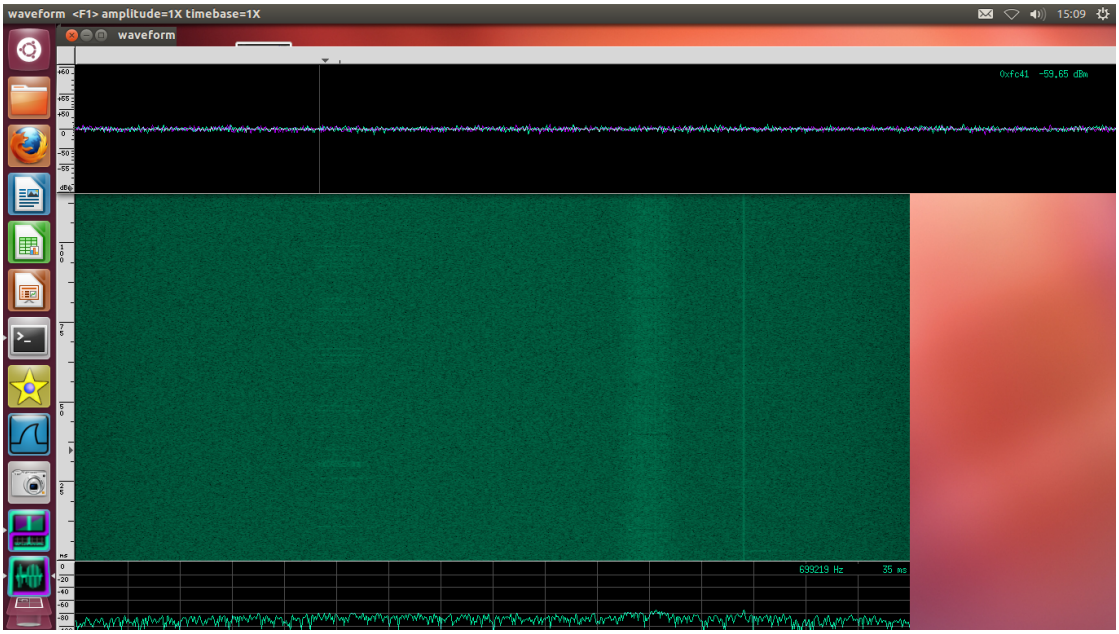


Abbildung 1.4: Eine visualisierte Frequenz

1.3 Anruf an die 2600

Es soll ein Anruf auf die 2600 was dem echo-Dienst entspricht durchgeführt werden. Dazu benötigen wir den am Anfang beschriebenen Versusaufbau sowie ein GSM-Fähiges Mobiltelefon das in dem Netz registriert ist. Als erstes muss das OpenBTS system gestartet werden dies erfolgt über mehrere Konsolen Befehle, da OpenBTS aus mehreren Komponenten besteht. Zuerst muss der Authentication-Service gestartet werden dies erfolgt durch den Befehl sipauthserve. Dannach muss die SMqueue gestartet werden die für die Weiterlietung der SMS verantwortlich ist, mit dem Befehl smqueue wird der Service gestartet. Der eigentliche OpenBTS Service muss ebenfalls gestartet werden. Dieser Dienst stellt den Kern des Systems dar, alle anderen Prozesse agieren mit diesem Prozess. Ausserdem brauchen wir noch den Asterisk Service der bereits in diesem Dokument erklärt worden ist. Diesen starten wir in einer neuen Konsole mit dem Befehl asterisk -r. Alle Befehle müssen als Superuser ausgeführt werden, sonst würden die Berechtigungen dazu fehlen. Um sich in dem Netz mit seinem eigenen Mobiltelefon registrieren zu können wählen wir das entsprechende Netz aus und erhalten unsere IMSI. Nun kann die 2600 angerufen werden und der Versuch durchgeführt werden.

1.4 Datenmitschnitte

Der vorangegangene Versuch sollte die physikalischen Eigenschaften des GSM Standards vermitteln. Der folgende Versuch beschäftigt sich mit den Protokolleigenschaften des GSM. Daher werden Situationen simuliert, die täglich millionenfach in den deutschen GSM Netzen stattfinden. Den Datenverkehr, den diese Situationen verursachen werden wir mitschneiden und analysieren.

1.4.1 Anruf mitschneiden

1.4.1.1 Versuchsaufbau

Die Hardware entspricht der des Versuchs 1.2.1. Der Unterschied liegt in der Software. Diese simuliert ein eigenes GSM Netz. Als Softwarepaket wird Open BTS genutzt, was wieder mit mehreren Softwarekomponenten interagiert. Die für uns relevanten Teile des Open BTS sind im wesentlichen:

- Sipauthserve - Ist für die Authentifizierung verantwortlich
- Smqueue - Ein store-and-forward SIP Server, dient der Weiterleitung von SMS
- Asterisk - Stellt die Telefonanlage zur Verfügung

Diese Software erlaubt in Verbindung mit der Hardware den Betrieb eines eigenen GSM Netzes. Zum Mittschnitt der Daten steht das Tool Wireshark zur Verfügung. Wireshark ist ein Protocol Analyzer, damit ist es möglich einzelne Datenpakete mitzuschneiden.

Die Hardware wird um ein Mobiltelefon erweitert. Dieses ist bereits konfiguriert und registriert. Dieses Mobiltelefon ermöglicht die Kommunikation und Interaktion mit dem GSM Netz.

1.4.1.2 Versuchsdurchführung

Zu Beginn des Versuchs muss die Software gestartet werden. Da die einzelnen Programme untereinander Abhängigkeiten haben, müssen sie in einem Befehl gestartet werden. Der Befehl *sudo sipauthserve & sudo smqueue & sudo OpenBTS & sudo OpenBTSCLI* startet die grundsätzliche Funktionalität des GSM Netzes. Mit dem Befehl *sudo asterisk -r* startet die Vermittlungenlage.

Stimmt das denn auch? Das mit den Abhängigkeiten und gleichzeitigg starten

Nachdem die die Vorbereitungen abgeschlossen sind, steht ein GSM Netz zur Verfügung. Für den Mitschnitt der Daten muss noch Wireshark konfiguriert werden. Hierzu wird das Filter *!(udp port 5700 || udp port 5702 || icmp)* gesetzt. Ein Filter in Wireshark hat den Vorteil, dass beim Datenmitschnitt die umrelevanten Daten herausgefiltert werden können und damit die doch sehr umfangreiche Datenmenge reduziert werden kann.

Der Anruf wird auf die Telefonnummer 2600 getätigt. Diese Telefonnummer ist als echo Kanal konfiguriert, das heißt, dass das Gespräch vom Netz wieder zurück zum Teilnehmer geschickt wird.

Nachdem der Versuch vorbereitet ist, wird über das Mobiltelefon die Nummer 2600 angerufen.

1.4.1.3 Auswertung des Versuchs

Der Echo Kanal funktioniert, wie beschrieben. Die Sprachdaten, die ans Netz gesendet werden, werden wieder vom Netz zurück geschickt.

Um in U(m) umwandeln so das das m klein wird

Mit geschnitten werden die Daten die über das Um Interface gesendet werden. Das Um Interface ist eine Funkschnittstelle die für die Übertragung zwischen der Mobile-Station und dem Base Transceiver Station zuständig ist. Das Um Interface arbeitet auf den Untersten drei Layer des ISO-OSI-Referenzmodell.

Durch Wireshark ist es möglich einen Einblick in die gesendeten Daten der verschiedenen Layern zu erhalten. Die Pakete die auf den verschiedenen Layern gesendet werden sind die folgenden:

- Auf Layer1 - GSMTAP
- Auf Layer2 - LAPDm
- Auf Layer3 - Resource Management Protocol (RR)

Da OpenBTS alle höheren Protokolle terminiert, erscheinen in Wireshark nicht nur die RR Nachrichten sondern auch Mobility Management und Call Management Nachrichten als Layer 3 Nachrichten welche in Wireshark als LAPDm gekennzeichnet sind. Im folgenden werden die für den Versuch wichtigen Pakete untersucht.

GSMTAP ist ein Pseudoheader für das Um Interface der in UDP Pakete gekapselt wird. Dieser Übernimmt die Aufgabe der fehlerfreien Übertragung, sowie die Verteilung der Kanäle. Im Header werden Informationen zu der verwendeten Version, der länge des Headers, der Type der übertragenden Daten, sowie die ARFCN und nähere Informationen zur Signalstärke angegeben.

```
⊟ GSM TAP Header, ARFCN: 840 (Downlink), TS: 0, Channel: CCCH (0)
    Version: 2
    Header length: 16 bytes
    Payload Type: GSM Um (MS<->BTS) (1)
    Time Slot: 0
    ..00 0011 0100 1000 = ARFCN: 840
    .0.. .... .... .... = Uplink: 0
    Signal/Noise Ratio (dB): 0
    Signal Level (dBm): 0
    GSM Frame Number: 1335747
    Channel Type: CCCH (2)
    Antenna Number: 0
    Sub-Slot: 0
⊞ GSM CCCH - Paging Request Type 1
```

Abbildung 1.5: GSMTAP-Header

Unser Hauptaugenmerk legen wir auf die Pakete die als SIP gekennzeichnet sind. Hier kann man am besten nachverfolgen was gerade für eine Aktion durchgeführt wird. Da als erstes eine Verbindung aufgebaut werden muss damit man mit dem Echo-Server interagieren kann wird zuerst eine Invite Nachricht gesendet.
Bevor das jedoch passiert wird vorher auf dem Layer 2 eine Setup Nachricht gesendet. Wie man in **??** sehen kann wird hier ebenfalls die Bearer Capability angefordert. Die Bearer Capability bedeutet das ein Gerät in unserem Fall die MS eine bestimmte Transportleistung vom Netz anfordert.

in bin einzu- binden http://www.itwiss capability- BC.html

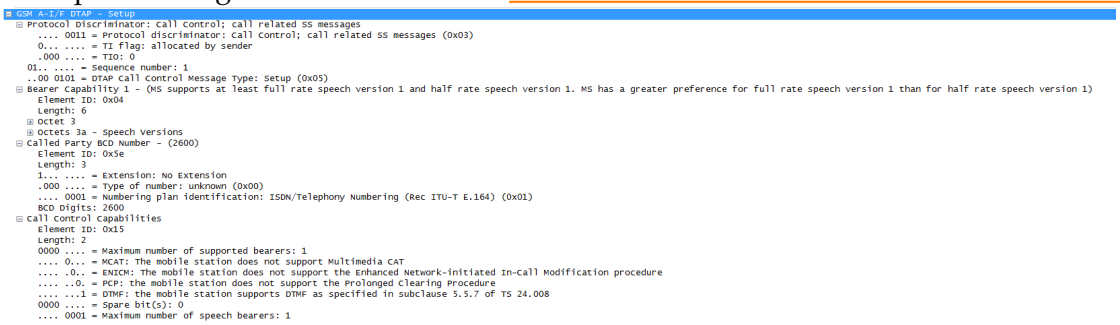


Abbildung 1.6: Setup Nachricht auf dem Layer 2

Ist dieser Vorgang abgeschlossen kann der Teilnehmer durch die Invite Nachricht den Echo-Server Anfragen und ihm für den Sprach-Aufbau relevante Daten übermitteln. Diese sind, wie man im Header sehen kann, von wem die Nachricht gestellt wird, an wen sie gesendet wird, sowie die Call-ID.

```
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:2600@127.0.0.1 SIP/2.0
    Method: INVITE
    Request-URI: sip:2600@127.0.0.1
      Request-URI User Part: 2600
      Request-URI Host Part: 127.0.0.1
    [Resent Packet: False]
  Message Header
    Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKobts286aec235c0a789c46
      Transport: UDP
      Sent-by Address: 127.0.0.1
      Sent-by port: 5062
      Branch: z9hG4bKobts286aec235c0a789c46
    From: IMSI001011832121286 <sip:IMSI001011832121286@127.0.0.1>;tag=ekvzvzbyilfvluhd
      SIP Display info: IMSI001011832121286
      SIP from address: sip:IMSI001011832121286@127.0.0.1
        SIP from address User Part: IMSI001011832121286
        SIP from address Host Part: 127.0.0.1
      SIP from tag: ekvzvzbyilfvluhd
    To:  <sip:2600@127.0.0.1>
      SIP to address: sip:2600@127.0.0.1
    Call-ID: 1246277822@127.0.0.1
    CSeq: 119 INVITE
      Sequence Number: 119
      Method: INVITE
    Contact: <sip:IMSI001011832121286@127.0.0.1:5062>;expires=3600
      Contact URI: sip:IMSI001011832121286@127.0.0.1:5062
        Contact URI User Part: IMSI001011832121286
        Contact URI Host Part: 127.0.0.1
        Contact URI Host Port: 5062
      Contact parameter: expires=3600\r\n
    Content-Type: application/sdp
    User-Agent: OpenBTS P2.8TRUNK Build Date Jun 26 2012
    Max-Forwards: 5
    P-Access-Network-Info: 3GPP-GERAN; cgi-3gpp=0010103e8000a
    Content-Length:   135
```

Abbildung 1.7: Invite Nachricht im SIP Protokoll

Vorrausgesetzt das diese Daten nicht fehlerhaft sind wird versucht eine Verbindung zu dem Server herzustellen. Diese kann man in **??** sehen. Dort wird mit dem Status-Code 100 gekennzeichnet.

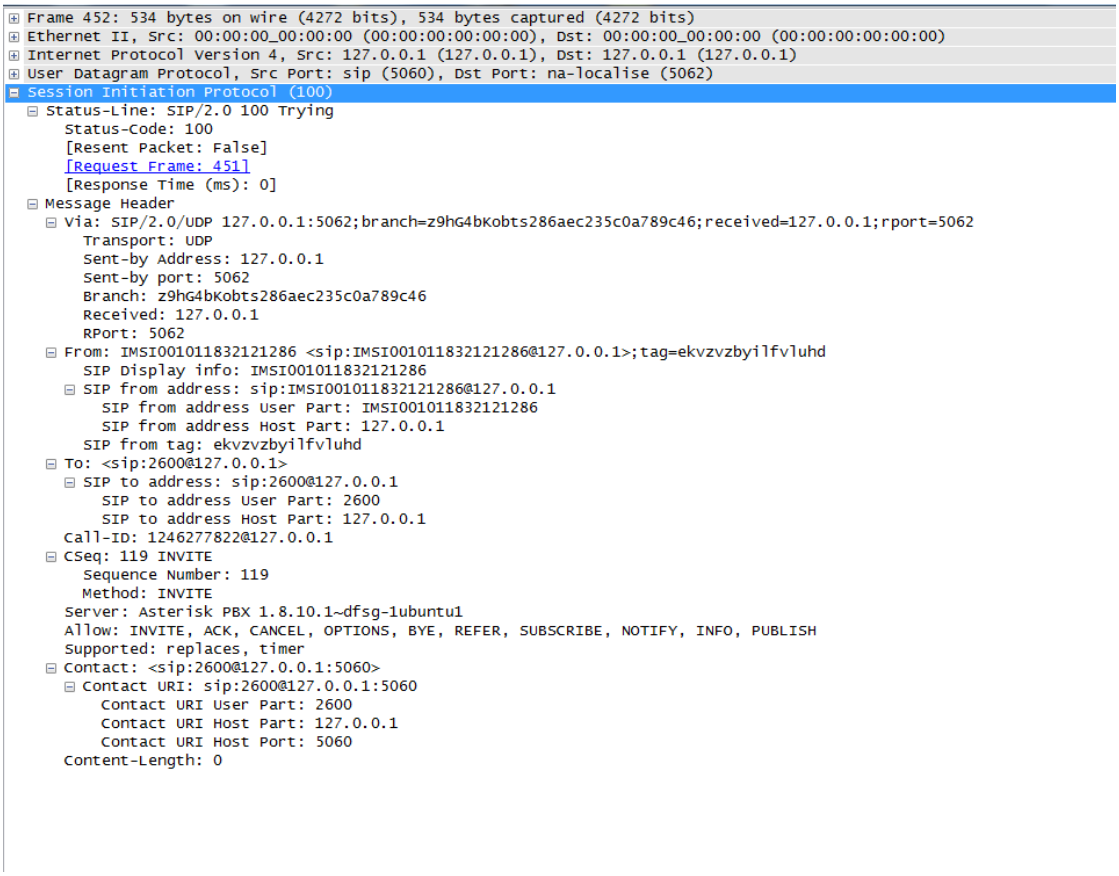


Abbildung 1.8: trying Nachricht im SIP Protokoll

Wenn die Anfrage der Verbindung erfolgreich war wird dies durch eine Ok-Nachricht bestätigt.

```
Session Initiation Protocol (200)
  Status-Line: SIP/2.0 200 OK
      Status-Code: 200
      [Resent Packet: False]
      [Request Frame: 451]
      [Response Time (ms): 1]
  Message Header
    Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKobts286aec235c0a789c46;received=127.0.0.1;rpor
      Transport: UDP
      Sent-by Address: 127.0.0.1
      Sent-by port: 5062
      Branch: z9hG4bKobts286aec235c0a789c46
      Received: 127.0.0.1
      RPort: 5062
    From: IMSI001011832121286 <sip:IMSI001011832121286@127.0.0.1>;tag=ekvzvzbyilfvluhd
      SIP Display info: IMSI001011832121286
      SIP from address: sip:IMSI001011832121286@127.0.0.1
        SIP from address User Part: IMSI001011832121286
        SIP from address Host Part: 127.0.0.1
      SIP from tag: ekvzvzbyilfvluhd
    To: <sip:2600@127.0.0.1>;tag=as6b64f7c0
      SIP to address: sip:2600@127.0.0.1
        SIP to address User Part: 2600
        SIP to address Host Part: 127.0.0.1
      SIP to tag: as6b64f7c0
    Call-ID: 1246277822@127.0.0.1
    CSeq: 119 INVITE
      Sequence Number: 119
      Method: INVITE
    Server: Asterisk PBX 1.8.10.1~dfsg-1ubuntu1
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
    Supported: replaces, timer
    Contact: <sip:2600@127.0.0.1:5060>
      Contact URI: sip:2600@127.0.0.1:5060
        Contact URI User Part: 2600
        Contact URI Host Part: 127.0.0.1
        Contact URI Host Port: 5060
    Content-Type: application/sdp
    Content-Length: 188
  Message Body
    Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): root 1953701507 1953701507 IN IP4 127.0.0.1
        Owner Username: root
        Session ID: 1953701507
        Session Version: 1953701507
        Owner Network Type: IN
        Owner Address Type: IP4
        Owner Address: 127.0.0.1
      Session Name (s): Asterisk PBX 1.8.10.1~dfsg-1ubuntu1
      Connection Information (c): IN IP4 127.0.0.1
      Time Description, active time (t): 0 0
        Session Start Time: 0
        Session Stop Time: 0
```

Abbildung 1.9: Antwort auf die Einladung im SIP Protokoll

Daraufhin erfolgt die Bestätigung und die Verbindung ist somit aufgebaut und bereit.

```
Session Initiation Protocol (ACK)
  Request-Line: ACK sip:2600@127.0.0.1 SIP/2.0
      Method: ACK
    Request-URI: sip:2600@127.0.0.1
        Request-URI User Part: 2600
        Request-URI Host Part: 127.0.0.1
    [Resent Packet: False]
    [Request Frame: 451]
    [Response Time (ms): 478]
  Message Header
    Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKobts286aec235c0a789c46
        Transport: UDP
        Sent-by Address: 127.0.0.1
        Sent-by port: 5062
        Branch: z9hG4bKobts286aec235c0a789c46
    From: IMSI001011832121286 <sip:IMSI001011832121286@127.0.0.1>;tag=ekvzvzbyilfvluhd
        SIP Display info: IMSI001011832121286
      SIP from address: sip:IMSI001011832121286@127.0.0.1
          SIP from address User Part: IMSI001011832121286
          SIP from address Host Part: 127.0.0.1
        SIP from tag: ekvzvzbyilfvluhd
    To: <sip:2600@127.0.0.1>;tag=as6b64f7c0
      SIP to address: sip:2600@127.0.0.1
          SIP to address User Part: 2600
          SIP to address Host Part: 127.0.0.1
        SIP to tag: as6b64f7c0
      Call-ID: 1246277822@127.0.0.1
    CSeq: 119 ACK
        Sequence Number: 119
        Method: ACK
      User-Agent: OpenBTS P2.8TRUNK Build Date Jun 26 2012
      Max-Forwards: 5
      Content-Length: 0
```

Abbildung 1.10: Bestätigungs Nachricht im SIP Protokoll

Nun werden die Daten via RTP zwischen Server und User ausgetauscht. RTP is das Real-Time-Transport Protocol das dazu dient audiovisuelle Daten über IP-basierte Netzwerke zu versenden. Wir legen nun auf das bedeutet wir möchten die Verbindung trennen. Das erfolgt durch einen Bye-nachricht (**??**. In dieser meldet der User dem Server das er die Verbindung nun trennt um dem Server bescheid zu geben. da ebenfalls die Layer 2 Verbindung wieder getrennt werden muss erfolgt hier eine Disconnect Nachricht wie in **??**.

```
GSM A-I/F DTAP - Disconnect
  Protocol Discriminator: Call Control; call related SS messages
      .... 0011 = Protocol discriminator: Call Control; call related SS messages (0x03)
      0... .... = TI flag: allocated by sender
      .000 .... = TIO: 0
    01.. .... = Sequence number: 1
    ..10 0101 = DTAP Call Control Message Type: Disconnect (0x25)
  Cause - (16) Normal call clearing
      Length: 2
      1... .... = Extension: No Extension
      .11. .... = Coding standard: Standard defined for the GSM PLMNS
      ...0 .... = Spare bit(s): 0
      .... 0000 = Location: User
      1... .... = Extension: No Extension
      .001 0000 = Cause: (16) Normal call clearing
```

Abbildung 1.11: Aufforderung zum Beenden der Layer 2 verbindung

```
Session Initiation Protocol (BYE)
  Request-Line: BYE sip:2600@127.0.0.1 SIP/2.0
    Method: BYE
    Request-URI: sip:2600@127.0.0.1
      Request-URI User Part: 2600
      Request-URI Host Part: 127.0.0.1
    [Resent Packet: False]
  Message Header
    Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKobts2830e292470ff33267
      Transport: UDP
      Sent-by Address: 127.0.0.1
      Sent-by port: 5062
      Branch: z9hG4bKobts2830e292470ff33267
    From: IMSI001011832121286 <sip:IMSI001011832121286@127.0.0.1>;tag=ekvzvzbyilfvluhd
      SIP Display info: IMSI001011832121286
      SIP from address: sip:IMSI001011832121286@127.0.0.1
        SIP from address User Part: IMSI001011832121286
        SIP from address Host Part: 127.0.0.1
      SIP from tag: ekvzvzbyilfvluhd
    To: <sip:2600@127.0.0.1>;tag=as6b64f7c0
      SIP to address: sip:2600@127.0.0.1
        SIP to address User Part: 2600
        SIP to address Host Part: 127.0.0.1
      SIP to tag: as6b64f7c0
    Call-ID: 1246277822@127.0.0.1
    CSeq: 120 BYE
      Sequence Number: 120
      Method: BYE
    Contact: IMSI001011832121286 <sip:IMSI001011832121286@127.0.0.1:5062>
      SIP Display info: IMSI001011832121286
      Contact URI: sip:IMSI001011832121286@127.0.0.1:5062
        Contact URI User Part: IMSI001011832121286
        Contact URI Host Part: 127.0.0.1
        Contact URI Host Port: 5062
    User-Agent: OpenBTS P2.8TRUNK Build Date Jun 26 2012
    Max-Forwards: 5
    Content-Length: 0
```

Abbildung 1.12: Aufforderung zum Beenden des Calls

Die Bye-Nachricht wird durch eine weitere OK-Nachricht bestätigt und somit ist die Verbindung vollständig abgebaut.

```
Session Initiation Protocol (200)
  Status-Line: SIP/2.0 200 OK
    Status-Code: 200
    [Resent Packet: False]
    [Request Frame: 16246]
    [Response Time (ms): 0]
    [Release Time (ms): 0]
```

Abbildung 1.13: Antwort auf die Aufforderung

Wird der Versuch mit einem eigenen Mobiltelefon ausgeführt, muss sich dieses erst an am Netz anmelden. Diese Anmeldung wird vom Netz mit einer SMS bestätigt.

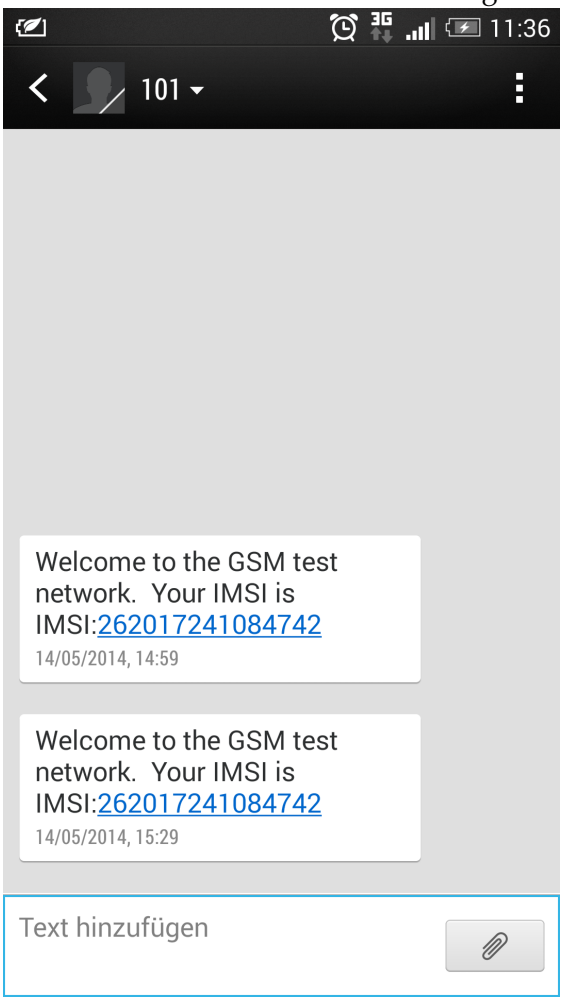


Abbildung 1.14: Quittierung der Einwahl in das GSM Netz

Der Ablauf des SIP Protokolls ist hier noch einmal in einem Diagramm genauer zusammengefasst.

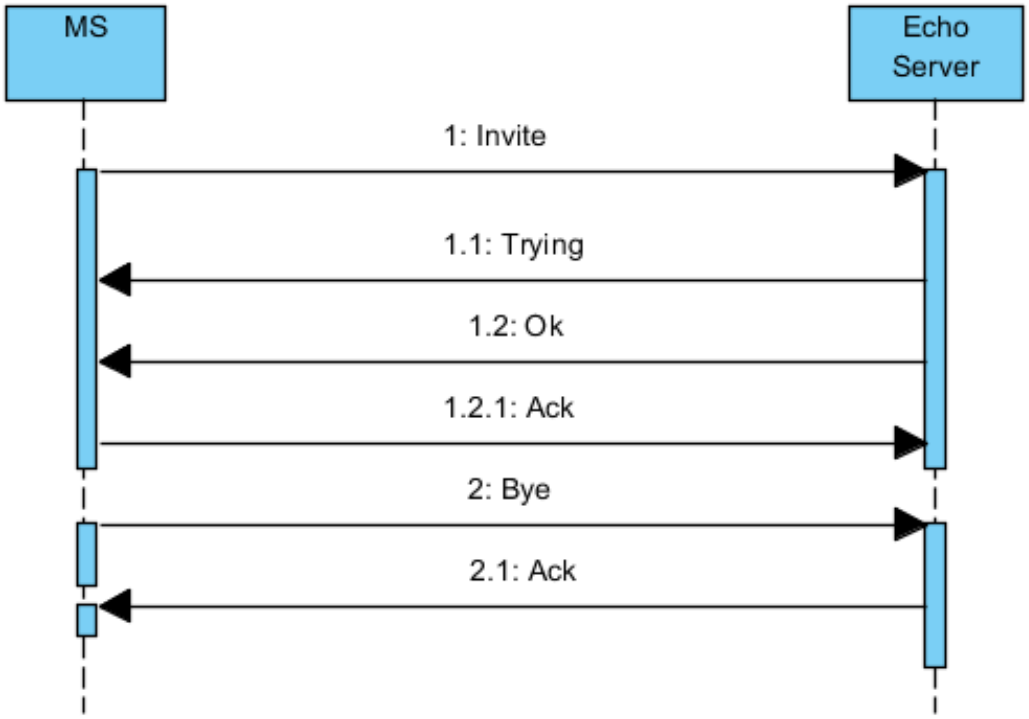


Abbildung 1.15: Ablauf SIP

1.5 Mitschnitt einer SMS

1.5.1 Versuchsaufbau

Der Aufbau des Versuchs entspricht dem Aufbau 1.4.1.1.

1.5.2 Versuchsdurchführung

Die Durchführung entspricht der Durchführung 1.4.1.2. Anstatt des Anrufs an die Nummer 2600 wird eine SMS mit dem Inhaltt „High “an die Telefonnummer 411 geschickt.

1.5.2.1 Auswertung des Versuchs

Die Protokolle LAPDm und GSMTAP unterschieden sich in ihrer Aufgabe nicht zu den vorher besprochenen.
Die Protokolle zu versenden der SMS sind jedoch wieder interessant. Dafür benötigten Protokolle sind

- Direct Transfer Application Part (DTAP)- dient zur Verbindungssteuerung
- Relay Protokoll (RP) - für das Routing verantwortlich
- Transport Protocol Data Unit (TPDU) - Übertragung der Nuzerdaten

Wie man sehr gut in der 1.16 sehen kann ist der gesenedete Text unten in der GSM SMS TPDU ebenfalls teil der ankommenden Nachricht. Dieser beinhaltet neben dem gesendeten Text auch die Zeit in der die SMS gesendet wurde sowie die IMSI Adresse und Telefonnummer. Die Inhalte können von dem von uns gemachten Versuch abweichen da die Daten von einem älteren Versuch stammen.
In dem RP Abschnitt kann man sehen in welche RIchtung die SMS gesendet wurde. Hier einmal von Netzwerk (NW) zur Mobilestation (MS) und umgekehrt. Durch das DTAP wird gekennzeichnet das es sich um eine SMS hadelt.

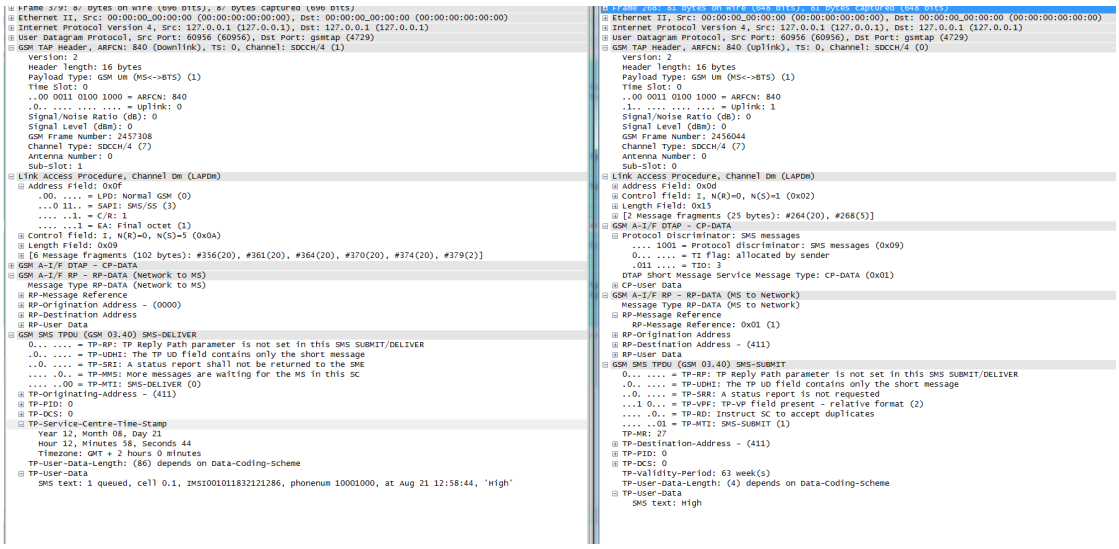


Abbildung 1.16: Gegenüberstellung Gesendet und Empfangen

Wie man in 1.17 sehen kann wird das Senden der SMS wieder von SIP initalisiert. Der Vorgang entsprich der bereits in dem Vorherigen Kapitel besprochenen Abfolge.

272	54.949984	127.0.0.1	127.0.0.1	SIP	493 Request: MESSAGE sip:smsc@127.0.0.1 | (RP)
279	55.425348	127.0.0.1	127.0.0.1	SIP	317 Status: 202 Queued |
285	55.597169	127.0.0.1	127.0.0.1	SIP	534 Request: MESSAGE sip:IMSI001011832121286@127.0.0.1:5062 | (RP)
287	55.602021	127.0.0.1	127.0.0.1	SIP	378 Status: 100 Trying |
381	60.613022	127.0.0.1	127.0.0.1	SIP	534 Request: MESSAGE sip:IMSI001011832121286@127.0.0.1:5062 | (RP)
382	60.616438	127.0.0.1	127.0.0.1	SIP	378 Status: 100 Trying |
418	62.029016	127.0.0.1	127.0.0.1	SIP	328 Status: 200 OK |
560	71.656441	127.0.0.1	127.0.0.1	SIP	328 Status: 200 OK |

Abbildung 1.17: SIP Abfolge des Sendens

2 BA Versuch

2.1 Allgemeine Beschreibung des Versuchs

BA, Basic Access, ist der Standardanschluss an das ISDN Netz. Er wird von den Anbietern an Privatkunden und kleine Betriebe vergeben. Basic Access bietet zwei Nutzkanäle (B-Kanäle) und einen Signalisierungskanal (D-Kanal). Obwohl die Netzbetreiber nach und nach auf reine IP Netze umstellen, hat ISDN in öffentlichen Telefonnetzen einen hohen Stellenwert. Mit der Entscheidung, dass die Ortsvermittlungsanlagen digitalisiert werden sollte, wurde 1979 ein wichtiger Grundstein für ISDN gelegt. 1987 wurde ISDN in Pilotprojekten erfolgreich getestet und schließlich 1989 flächendeckend eingeführt. ISDN bietet im Vergleich zu den analogen Übertragungstechniken den Vorteil, dass zwei Nutzkanäle gleichzeitig übertragen werden können. Zusätzliche Vorteile resultieren aus der verbesserten Sprachqualität und der schnelleren Datenübertragung. Der folgende Versuch soll das grundlegende Verständnis für ISDN vertiefen und gleichzeitig Einblicke in die Konfiguration gewähren. Der Einblick in die Konfiguration wird dadurch vermittelt, dass es zu dem Versuch gehört, die Anlage für den Versuch herzurichten. Durch Protokollmitschnitte und die bereitgestellten Unterlagen soll das grundlegende Verständnis für ISDN vermittelt werden.

2.2 Einrichten der Anlage

2.2.1 Einrichten der Ports

2.2.1.1 Aufbau des Versuchs

Als Switch steht ein Patapsco Liberator S zur Verfügung. Der Switch übernimmt die Funktionen des Netzes. Dazu gehören die TEI Vergabe, das Routing von Gesprächen und die Vergabe von Telefonnummern. Auf der Hardwareebene verbindet der Liberator die Telefone.
Zusätzlich steht ein EyeSDN Gerät. Dieses ermöglicht die Verbindung des Computers mit dem ISDN Netz und damit den Mittschnitt der Daten.
Zur Telefonie stehen zwei Telefone zur Verfügung und zum Konfigurieren des Systems ein Computer.

War da nicht noch was zur Stromversorgung?

2.2.1.2 Versuchsdurchführung

Die Hardware ist zu Beginn des Versuchs bereits verkabelt. Nachdem die SoftwareEyeSDN gestartet wurde, beginnt das Konfigurieren des Switches. Die Konfigura-

tion des Switches geschieht in der Anwendung Switchmanager. Dort werden die Ports eingerichtet, an denen die Telefone hängen und die Freizeichen eingestellt. Nach dem Upload wird die Konfiguration auf den Switch übertragen.
Die Einstellungen können direkt an den Telefonen getestet werden. Wenn der Hörer abgehoben wird, muss ein Freizeichen zu hören sein.

2.2.1.3

Abbildung 2.1: Der Loberator S [4]

2.2.1.4 Auswertung des Versuchs

Nachdem die Ports konfiguriert sind, und die Konfiguration auf den Liberator S übertragen sind, sind die Telefone grundsätzlich aktiv. Beide Telefone geben nach dem Abheben des Hörers ein Freizeichen.

2.2.2 Einrichten der Routing Tabellen

Nach dem Versuch 2.2.1 haben die Telefone bereits Grundfunktionalitäten. Zum Telefonieren und für die weiteren Versuche fehlt aber noch die Einrichtung der Routinginformationen. Ohne die Routinginformationen ist es nicht möglich, ein Gespräch von einem Telefon zum Anderen zu leiten, als zu telefonieren.

2.2.2.1 Aufbau des Versuchs

Der Aufbau des Versuchs entspricht dem vom Versuch 2.2.1. Dieser ist für den aktuellen Versuch aber eine Vorraussetzung.

2.2.2.2 Beschreibung des Versuchs

Das Routing wird im Interface Term des Liberator Fensters eingerichtet. Für das Einrichten von Routen können Profile angelegt werden, dadurch bleibt das System flexibler. Wir richten ein neues Profil ein, und konfigurieren die Routen von Telefon 1 zu Telefon 2 und umgekehrt. Wie bereits im letzten Versuch werden die Einstellungen nach dem Hochladen wirksam.

2.2.2.3 Auswertung des Versuchs

Nachdem die Routen konfiguriert sind, ist es möglich das Telefon 2 vom Telefon 1 an anzurufen. Bzw. ein Anruf in die Umgekehrte Richtung ist auch möglich.

2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

2.3.1 Aufzeichnen des ISDN-D-Kanal Protokolls ??

2.3.1.1 Versuchsaufbau

Der Versuchsaufbau entspricht dem Versuch 2.2.1. Die beiden vorangegangen Versuche sind für diesen voraus gesetzt.

2.3.1.2 Versuchdurchführung

Die spätere Auswertung wird erleichtert, wenn der, eventuell schon laufende, Mitschnittsdienst erst gestoppt wird und alle vorhandenen Ergebnisse verworfen werden. Nachdem das geschehen ist, wird der Mitschnittdienst wieder gestartet und das Telefon 1 vom Telefon 2 angerufen. Wenn das Telefon 2 klingelt wird der Hörer abgehoben und nach einem kurzen Moment wieder aufgelegt. Dadurch wird ein Gespräch aufgebaut und wieder abgebaut. Direkt nach dem Beenden des Gesprächs wird der Mitschnittdienst wieder gestoppt. Die Auswertung des Gesprächs beginnt, wenn der Mitschnitt im Fenster mit einem Doppelklick ausgewählt wird.

2.3.2 Interpretieren des D-Kanal-Protokoll Mitschnitts

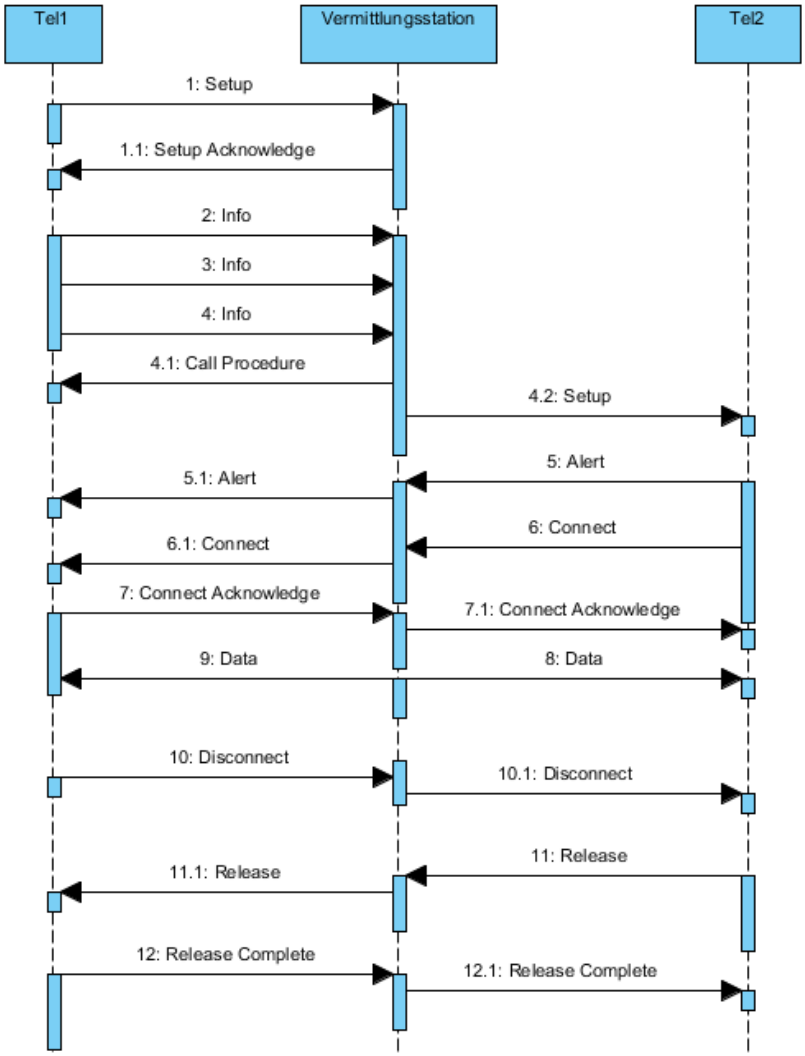
2.3.2.1 Versuchsaufbau

Der Versuch **??** muss durchgeführt sein und die Ergebnisse müssen vorliegen. Für die Auswertung muss ein Computer mit der Software Wireshark bereit stehen.

2.3.2.2 Versuchsdurchführung

Die aufgezeichneten Protokolldaten werden mit Wireshark geöffnet.

2.3.2.3 Auswertung des Versuchs



Zur einfacheren und genaueren Auswertung des Versuchs sind in der Aufgabenbeschreibung 12 Fragen beschrieben.

1. **Welche Rahmen dienen der TEI-Vergabe, und welcher TEI-Wert wird dem Telefon von der Vermittlung zugewiesen?**
   Die Tei vergabe wird über das Protocol TEI mit der info Itenty Request behandelt. Diese fordert einen TEi Wert zur indentifizierung des Endgerätes an.

```
No.   Time       Source          Destination     Protocol Info
   13 3601.022936 User            Network         TEI      Identity Request

Frame 13 (8 bytes on wire, 8 bytes captured)
  Arrival Time: May 19, 2014 14:40:01.115936000
  [Time delta from previous captured frame: 1.999952000 seconds]
  [Time delta from previous displayed frame: 1.999952000 seconds]
  [Time since reference or first frame: 3601.022936000 seconds]
  Frame Number: 13
  Frame Length: 8 bytes
  Capture Length: 8 bytes
  [Frame is marked: False]
  [Protocols in frame: isdn:lapd:tei_management]
  Point-to-Point Direction: Sent (0)
ISDN
  Channel: D (0)
Link Access Procedure, Channel D (LAPD)
  [Direction: User->Network (0)]
  Address Field: 0xfcff
    1111 11.. .... .... = SAPI: Layer 2 management procedures (63)
    .... ..0. .... .... = C/R: 0
    .... ...0 .... .... = EA1: 0
    .... .... 1111 111. = TEI: 127
    .... .... .... ...1 = EA2: 1
  Control field: U, func=UI (0x03)
    000. 00.. = Command: Unnumbered Information (0x00)
    .... ..11 = Frame type: Unnumbered frame (0x03)
TEI Management Procedure, Channel D (LAPD)
  Entity: 0x0f
  Reference: 30453
  Msg: Identity Request (1)
  1111 111. = Action: 127
  .... ...1 = Extend: 1
```

Die Anfrage wird durch einen Identy Assigned bestätigt und ein TEI Wert wird dem Endgerät zugewiesen. In diesem Fall wird der Wert 64 zugewiesen.

```
No.     Time        Source                Destination         Protocol Info
     14 3601.028984 Network               User                TEI      Identity Assigned

Frame 14 (8 bytes on wire, 8 bytes captured)
    Arrival Time: May 19, 2014 14:40:01.121984000
    [Time delta from previous captured frame: 0.006048000 seconds]
    [Time delta from previous displayed frame: 0.006048000 seconds]
    [Time since reference or first frame: 3601.028984000 seconds]
    Frame Number: 14
    Frame Length: 8 bytes
    Capture Length: 8 bytes
    [Frame is marked: False]
    [Protocols in frame: isdn:lapd:tei_management]
    Point-to-Point Direction: Received (1)
ISDN
    Channel: D (0)
Link Access Procedure, Channel D (LAPD)
    [Direction: Network->User (1)]
    Address Field: 0xfeff
        1111 11.. .... .... = SAPI: Layer 2 management procedures (63)
        .... ..1. .... .... = C/R: 1
        .... ...0 .... .... = EA1: 0
        .... .... 1111 111. = TEI: 127
        .... .... .... ...1 = EA2: 1
    Control field: U, func=UI (0x03)
        000. 00.. = Command: Unnumbered Information (0x00)
        .... ..11 = Frame type: Unnumbered frame (0x03)
TEI Management Procedure, Channel D (LAPD)
    Entity: 0x0f
    Reference: 30453
    Msg: Identity Assigned (2)
    1000 000. = Action: 64
    .... ...1 = Extend: 1
```

2. **Wann ist der Aufbau der Schicht 2 abgeschlossen?**
   Der Aufbau ist nach dem senden eines unnumbered Acknowledge Frame der zur Bestätigung des Set Asynchronous Balance Mode Extended Frame benutzt wird

```
No. Time Source Destination Protocol Info
15 3601.038936 User Network LAPD U P, func=SABME

Frame 15 (3 bytes on wire, 3 bytes captured)
Arrival Time: May 19, 2014 14:40:01.131936000
[Time delta from previous captured frame: 0.009952000 seconds]
[Time delta from previous displayed frame: 0.009952000 seconds]
[Time since reference or first frame: 3601.038936000 seconds]
Frame Number: 15
Frame Length: 3 bytes
Capture Length: 3 bytes
[Frame is marked: False]
[Protocols in frame: isdn:lapd:data]
Point-to-Point Direction: Sent (0)
ISDN
Channel: D (0)
Link Access Procedure, Channel D (LAPD)
[Direction: User->Network (0)]
Address Field: 0x0081
0000 00.. .... .... = SAPI: Q.931 Call control procedure (0)
.... ..0. .... .... = C/R: 0
.... ...0 .... .... = EA1: 0
.... .... 1000 000. = TEI: 64
.... .... .... ...1 = EA2: 1
Control field: U P, func=SABME (0x7F)
...1 .... = Poll: Set
011. 11.. = Command: Set Asynchronous Balanced Mode Extended (0x1b)
.... ..11 = Frame type: Unnumbered frame (0x03)
No. Time Source Destination Protocol Info
16 3601.042952 Network User LAPD U F, func=UA
Frame 16 (3 bytes on wire, 3 bytes captured)
Arrival Time: May 19, 2014 14:40:01.135952000
[Time delta from previous captured frame: 0.004016000 seconds]
[Time delta from previous displayed frame: 0.004016000 seconds]
[Time since reference or first frame: 3601.042952000 seconds]
Frame Number: 16
Frame Length: 3 bytes
Capture Length: 3 bytes
[Frame is marked: False]
[Protocols in frame: isdn:lapd:data]
Point-to-Point Direction: Received (1)
ISDN
Channel: D (0)
Link Access Procedure, Channel D (LAPD)
[Direction: Network->User (1)]
Address Field: 0x0081
0000 00.. .... .... = SAPI: Q.931 Call control procedure (0)
.... ..0. .... .... = C/R: 0
.... ...0 .... .... = EA1: 0
.... .... 1000 000. = TEI: 64
.... .... .... ...1 = EA2: 1
Control field: U F, func=UA (0x73)
...1 .... = Final: Set
011. 00.. = Response: Unnumbered Acknowledge (0x18)
.... ..11 = Frame type: Unnumbered frame (0x03)
```

beendet.

3. **Welchen ISDN-Dienst fordert das Telefon von der Vermittlungsstelle an, welche Übertragungskapazität benötigt dieser Dienst?**
   Das Telefon fordert den Dienst zum übertragen von Sprache an. Dies ist ein Kanal mit 64 kbit/s übertragungskapazität. Im folgenden Frame kann man dies herauslesen. Es handelt sich hierbei um eine Setup Nachricht.

```
No.   Time        Source          Destination     Protocol Info
  192 4097.270936 User            Network         Q.931    SETUP

Frame 192 (24 bytes on wire, 24 bytes captured)
  Arrival Time: May 19, 2014 14:48:17.363936000
  [Time delta from previous captured frame: 0.022000000 seconds]
  [Time delta from previous displayed frame: 0.022000000 seconds]
  [Time since reference or first frame: 4097.270936000 seconds]
  Frame Number: 192
  Frame Length: 24 bytes
  Capture Length: 24 bytes
  [Frame is marked: False]
  [Protocols in frame: isdn:lapd:q931]
  Point-to-Point Direction: Sent (0)
ISDN
  Channel: D (0)
Link Access Procedure, Channel D (LAPD)
  [Direction: User->Network (0)]
  Address Field: 0x0081
    0000 00.. .... .... = SAPI: Q.931 Call control procedure (0)
    .... ..0. .... .... = C/R: 0
    .... ...0 .... .... = EA1: 0
    .... .... 1000 000. = TEI: 64
    .... .... .... ...1 = EA2: 1
  Control field: I, N(R)=0, N(S)=0 (0x0000)
    0000 000. .... .... = N(R): 0
    .... .... 0000 000. = N(S): 0
    .... .... .... ...0 = Frame type: Information frame (0x0000)
Q.931
  Protocol discriminator: Q.931
  Call reference value length: 1
  Call reference flag: Message sent from originating side
  Call reference value: 01
  Message type: SETUP (0x05)
  Bearer capability
    Information element: Bearer capability
    Length: 3
    1... .... = Extension indicator: last octet
    .00. .... = Coding standard: ITU-T standardized coding (0x00)
    ...0 0000 = Information transfer capability: Speech (0x00)
    1... .... = Extension indicator: last octet
    .00. .... = Transfer mode: Circuit mode (0x00)
    ...1 0000 = Information transfer rate: 64 kbit/s (0x10)
    1... .... = Extension indicator: last octet
    .01. .... = Layer identification: Layer 1 identifier (0x01)
    ...0 0011 = User information layer 1 protocol: Recommendation G.711 A-law (0x03)
  Calling party number: '100'
    Information element: Calling party number
    Length: 5
    .... 0000 = Numbering plan: Unknown (0x00)
    .000 .... = Number type: Unknown (0x00)
```

4. **Welche Kodierung des Sprachkanals wird gewählt?**
   ITU-T standardized coding hab ich hier aufm block stehen.

5. **Welche MSN-Nummer wird in welchem Rahmen übertragen?**

6. **Wann ist der gesicherte Aufbau der Schicht 3 abgeschlossen?**

7. **Welchen B-Kanal weist die Vermittlung der Verbindung zu?**
   B1 Channel (0x01)

8. **Wo wird die gerufene Telefonnummer übermittelt?**

9. **Mit welchem Rahmen bestätigt die Vermittlung die Vollständigkeit der Rufnummer und beginn den angeforderten Teilnehmer anzuwählen?**
   Alerting

10. **Mit welchem Rahmen signalisiert die Vermittlung, dass der gerufene Teilnehmeranschluss ein Endgerät besitzt, das den Sprachdienst erfüllen kann und ein Rufsignal aussendet?**

11. **Wann sind die Schichten 3 und 2 jeweils wieder vollständig abgebaut?**

12. **Bei ISDN gibt es die Möglichkeit, bei einem abgehenden Ruf die Zielrufnummer vor oder nach dem Abheben des Hörers einzugeben. Wodurch unterscheidet sich die Signalisierung auf Schicht 3 (SETUP- und INFO Nachricht) der Teilnehmerschnittstelle in diesen beiden Fällen?**

Nur dass das TODO die Tabelle nicht kaputt macht

Haben wir den Versuch mit dem aufgelegten Hörer gemacht?

Nachricht \ Nachrichtenelement	Alert	Call Proc	Conn	DISC	Info	Rel	Rel. Comp	Setup	Setup Ack
Bearer Capability									
Cause									
Channel Identification									
Process Indicator									
Display									
Date / Time									
Calling Party Number									
Called Party Number									
Sending Complete									
Facility									
User to User Information									

Tabelle 2.1: Genutzte Nachrichten

3 RSP Versuch

3.1 Einleitung

Router und Switche begleiten uns im täglichen Leben. Auch wenn sie oft nicht wahrgenommen werden, sind sie doch allgegenwärtig. Ob mobiles Surfen, das Surfen am Computer oder auch telefonieren, diese Tätigkeiten sind ohne Router und Switche nicht möglich. Der Netzwerkausrüster Cisco Systems rechnet bis zu Jahr 2018 mit einem weltweiten Internettraffic von 1,6 Zettabyte [3]. Die Netzwerke, die diesen Traffic behandeln und abwickeln sollen wachsen stetig mit ihren Aufgaben. Deswegen ist eine fundierte Ausbildung in der Netzwerktechnik und ein Verständnis der Komponenten für den Informatiker der Zukunft unausweichlich.
Der folgende Versuch soll einen grundlegenden Einblick in den Aufbau eines Netzwerkes und die Konfiguration der Komponenten vermitteln.

Kann man das so schreiben?

3.1.1 Benötigte Hardware für den Versuch

Für den Versuch werden ein Cisco 2811 Router und ein Cisco 2960 Switch benötigt. Zusätzlich werden ein Windows Computer mit einem Terminal Emulationsprogramm und diverse Kabel benötigt.

3.1.1.1 Router

Die Aufgabe eines Routers, manchmal auch als Layer 3 Switch bezeichnet, ist es, zwischen mehreren Netzwerken der ISO/OSI Referenzmodells Schicht 3 zu vermitteln. Dazu besitzt ein Router mehrere (virtuelle) Ports, an denen die entsprechenden Netzwerke angeschlossen sind. Der Router, der für unseren Versuch zur Verfügung stand ist vom Netzwerkausrüster Cisco Systems und ist aus der Modellreihe 2811.

Abbildung 3.1: Ein Cisco 2800 Router [5]

3.1.1.2 Switch

Die Aufgabe eines Switches ist es, Netzwerksegmente miteinander zu verbinden. Das bedeutet, dass mehrere Kabel physikalisch miteinander verbunden werden können und die Datenpakete von einem Kabel in ein anderes weitergeleitet werden können. Logisch gesehen, werden die Datenpakete nur an die Kabel oder Ports weitergeleitet, die die Empfängeradresse dieses Pakets haben. Im Versuch stand uns ein Switch aus der Serie 2960 vom Netzwerkausrüster Cisco Systems zur Verfügung.

Abbildung 3.2: Ein Cisco 2800 Router [2]

3.1.1.3 Kabel

Bei den Kabeln gibt es verschiedene Typen. Bei den Kabeln zur Energieversorgung der Geräte handelt es sich um normale Kaltgerätekabel, diese brauchen an dieser Stelle nicht weiter beschrieben zu werden. Weiterhin waren RJ 45 Twisted Pair Kabel verwendet. Diese dienen der Verbindung zwischen den Routen, bzw, Switchen und den Computern. Diese Verbindung dient dem Austausch von Nutzdaten. Die Konfiguration wurde über eine serielle Schnittstelle vorgenommen. Das dazugehörige Kabel hat auf der einen Seite einen female COM Port, auf der anderen Seite einen male RJ 45 Stecker.

War da auch ein Crossover Kabel dabei?

3.1.1.4 Hintergrund der seriellen Übertragung

Im Abschnitt 3.1.1.3 wurde erwähnt, dass für die Konfiguration die serielle Schnittstelle genutzt wird. Dabei stellt sich die Frage, warum dieser Aufwand betrieben werden muss, obwohl ein Switch doch mit ausreichend Ethernet Ports ausgestattet sein sollte. Den Hintergrund möchten wir an dieser Stelle durch ein Beispiel beleuchten:

1. Switch und Computer befinden sich im Netzwerk 192.168.0.0/16
2. Der Administrator will das Netzwerk in das Netzwerk 172.16.0.0/12 umbenennen
3. Der Administrator vertippt sich bei der Vergabe der Ip und gibt die Netzwerkadresse 172.36.0.0 ein

Was wird nun passieren? Wir setzen voraus, dass im Netzwerk kein DHCP Server aktiviert ist und alle Ip Adressen statisch vergeben werden. Im ersten Schritt ist die Welt noch in Ordnung. Im zweiten Schritt ändert der Administrator die NW Adressen seines Computers und die des Routers. Im dritten Schritt bricht das Chaos aus. Mit dem Abspeichern der ersten Adresse, sei es Computer oder Switch, verliert der Administrator die Kontrolle über den Switch. Da sich mit einer geänderten Adresse der Switch und der Computer in verschieden Netzwerken befinden, ist dieser „Fehler“ vorhersehbar und leicht nachzuvollziehen. Der Administrator berücksichtigt diese Tatsache und speichert zuerst die Konfiguration des Switches. Nachdem er die Verbindung zum Switch verloren hat speichert er die neue Konfiguration im Computer. Obwohl sich Computer und Switch vermeintlich wieder in den gleichen Netzen befinden, hat er keinen Zugriff mehr auf den Switch.
Ohne einen logischen Zugriff auf den Switch gestaltet sich die Suche nach dem Fehler sehr schwierig. Diese Problematik kann durch die Konfiguration über die serielle Schnittstelle vermieden werden. Ein weiterer Vorteil ist, dass die Konfigurationsschnittstelle des Switches vom Rest des Netzwerkes getrennt ist. Dadurch kann alleine schon durch die Trennung ein Angriff auf den Switch erschwert werden.

3.2 Der Umgang mit Physikalischen Geräten

Die physische Einrichtung des Systems ist in der Aufgabenstellung genau beschrieben. So viel sei zu sagen, jeder der beiden Computer ist per LAN Schnittstelle mit dem Switch verbunden. Je ein Computer ist über den COM Port (seriell) mit Router und Switch verbunden. Router und Switch sind über Gigabit Ethernet miteinander verbunden.
Die logische Einrichtung des Systems geschieht über Hyper Terminal. Hyperterminal ist eine Terminal Emulationssoftware. Diese ermöglicht eine Verbindung zu anderen Computern oder Großrechnern über die serielle Schnittstelle. Diese Verbindung ist rein ASCII textbasiert.

Command Mode	Access Method	Prompt	Exit
User EXEC	This is the first level of access. Change terminal settings, perform basic tasks, and list system information.	*ap>*	Enter the logout command.
Privileged EXEC	From user EXEC mode, enter the enable command.	*ap#*	To exit to user EXEC mode, enter the disable command.
Global configuration	From privileged EXEC mode, enter the configure command.	*ap(config)#*	To exit to privileged EXEC mode, enter the exit or end command, or press Ctrl-Z.
Interface configuration	From global configuration mode, specify terminal then specify an interface by entering the interface command followed by the interface type and number.	*ap(config-if)#*	To exit to privileged EXEC mode, enter the end command, or press Ctrl-Z. To exit to global configuration mode, enter the exit command.

Tabelle 3.1: Genutzte Nachrichten

3.2.1 Einrichtung eines Switchs

Die Einrichtung des Switches beginnt mit dem Hochfahren des Geräts. Dabei kann im Hyperterminal überwacht werden, ob der Switch ordnungsgemäß startet. Nachdem die Selbstdiagnose durchgelaufen ist, kann in den Auführungsmodus, bzw. in den „privileged EXEC mode“ gewechselt werden.
Die unterschiedlichen Kommando Modi sind in Tabelle 3.1 aufgeführt.
Im privileged EXEC mode müssen erst die Einstellungen des Switches zurück gesetzt werden. Dadurch wird vermieden, dass bereits bestehende Konfigurationen die Ergebnisse beeinflussen. Die Ausgabe ist ähnlich der Ausgabe 3.4. Durch die Befehle *delete flash : vlan.dat* und **erase startup-config** werden erst die Einstellungen zu den V-Lan gelöscht und anschließend wird die gesamte Konfiguration gelöscht.

Der Unterschied zwischen *erase startup-config* und *erase running-config*: Auf den ersten Blick haben beide Befehle die gleiche Wirkung. Der Unterschied ist, dass die Konfiguration nach einem Neustart des Geräts wieder hergestellt wird, wenn *erase running-config* genutzt wurde. Wurde *erase startup-config* genutzt, ist die Konfiguration dauerhaft gelöscht. Der genaue Unterschied wird nach dem Lesen der Erklärung von Speicherunterschieden 3.2.2 deutlicher.

Nachdem die Konfiguration des Switches zurück gesetzt wurde, kommt die Aufforderung, den Switch zu konfigurieren. Diese Aufforderung wird mit einem *n* quittiert. Dadurch wird die Konfiguration nicht durchgeführt und der Switch läuft mit seinen Default Konfigurationen. Der Switch ist jetzt bereit für den weiteren Versuch.

3.2.2 Konfiguration eines Routers

Das Zurücksetzen des Routers geschieht analog zu dem Zurücksetzen des Switches.

```
        Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
   Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
*Jun  4 10:44:29.415: %SYS-7-NV_BLOCK_INIT: Initialized the
   geometry of nvram
Router#re
*Jun  4 10:45:30.887: %LINK-3-UPDOWN: Interface Serial0/0/0,
   changed state to do
wn
*Jun  4 10:45:31.887: %LINEPROTO-5-UPDOWN: Line protocol on
   Interface Serial0/0/
0, changed state to do
Router#reload
Proceed with reload? [confirm]

*Jun  4 10:45:44.707: %SYS-5-RELOAD: Reload requested  by console.
    Reload Reason
: Reload Command.

System Bootstrap, Version 12.4(13r)T11, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2009 by cisco Systems, Inc.

Initializing memory for ECC
.
c2811 platform with 262144 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled


Upgrade ROMMON initialized
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0x1859ee4
Self decompressing the image :
   ################################################
########################################
```

```
####################################
########### [OK]

Smart Init is enabled
smart init is sizing iomem
  ID            MEMORY_REQ                  TYPE
0003E7          0X00473800 C2811 Mainboard
                0X000021B8 Onboard USB
                0X002C29F0 public buffer pools
                0X00211000 public particle pools
TOTAL:          0X009493A8

If any of the above Memory Requirements are
"UNKNOWN", you may be using an unsupported
configuration or there is a software problem and
system operation may be compromised.
Rounded IOMEM up to: 10Mb.
Using 3 percent iomem. [10Mb/256Mb]

[...]

Cisco 2811 (revision 49.46) with 251904K/10240K bytes of memory.
Processor board ID FCZ131871SX
2 FastEthernet interfaces
2 Low-speed serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---
```

Listing 3.1: Die Ausgabe des Zurücksetzens

Nachdem der Router auf die Grundeinstellungen zurück gesetzt wurde, muss er neu konfiguriert werden. Der folgende Dialog startet die Konfiguration:

```
Would you like to enter the initial configuration dialog? [yes/no
   ]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
```

```
Configuring global parameters:
```

Listing 3.2: Die Aufforderung zum neukonfigurieren des Routers

Im Gegensatz zum Switch wird der Router konfiguriert. Dies geschieht über den Befehl *yes* oder einfach *y*. Die Konfiguration wird nach den Vorgaben der Versuchsbeschreibung durchgeführt. Sowohl vor, als auch nach dem Konfigurieren wird das Kommando *show running-config* aufgerufen.

```
Router#show running-config
Building configuration...

Current configuration : 1058 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$WPnk$wNZGar7F/KHiw5VcuCMtE.
enable password cisco
!
no aaa new-model
!
!
ip cef
!
!
no ip domain lookup
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
interface FastEthernet0/0
 description R1 LAN Default Gateway
 ip address 192.168.1.1 255.255.255.128
```

```
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 description R1 WAN
 ip address 192.168.1.193 255.255.255.252
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
router rip
 version 2
 network 192.168.1.0
!
ip forward-protocol nd
!
!
ip http server
!
!
!
control-plane
!
banner motd ^CUnauthorized Use Prohibited^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
scheduler allocate 20000 1000
!
end
```

Listing 3.3: Die Ausgabe der Konfiguration vor dem Konfigurieren

Nach dem Konfigurieren sieht die Ausgabe folgendermaßen aus:

```
R1_HTW#show running-config
Building configuration...

Current configuration : 1058 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1_HTW
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$WPnk$wNZGar7F/KHiw5VcuCMtE.
enable password cisco
!
no aaa new-model
!
!
ip cef
!
!
no ip domain lookup
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
interface FastEthernet0/0
 description R1 LAN Default Gateway
 ip address 192.168.1.1 255.255.255.128
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
```

```
 speed auto
!
interface Serial0/0/0
 description R1 WAN
 ip address 192.168.1.193 255.255.255.252
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
router rip
 version 2
 network 192.168.1.0
!
ip forward-protocol nd
!
!
ip http server
!
!
!
control-plane
!
banner motd ^CUnauthorized Use Prohibited^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
scheduler allocate 20000 1000
!
end
```

Listing 3.4: Die Ausgabe des Zurücksetzens

Zwischen den beiden Ausgaben gibt es augenscheinliche Merkmale:
Der Unterschied zeigt sich im Hostname. Dieser Unterschied deckt sich mit den Erwartungen, da bis auf den Hostname nichts konfiguriert wurde.

Keine Ahnung, was der in Step 2 will

Da die Änderungen sich nur auf den flüchtigen Speicher beschränken, gehen sie bei einem Neustart des Routers verloren.

Um die Auswirkungen des nächsten Schritts zu verstehen, ist es sinnvoll sich die verschiedenen Sorten von Speicher in einem Cisco Router vor Augen zu führen. Die Erläuterungen zu den Speichersorten stammen von Cisco **??**

- **RAM:** Random Access Memory ist der flüchtige Arbeitsspeicher, von Cisco auch als Dynamic RAM bezeichnet. Flüchtig bedeutet, dass die gespeicherten Informationen nach einem Spannungsverlust verloren gehen. Im RAM werden ARP Tabellen, Routing Tabellen, eine temporäre Konfiguration, Packet Queues, usw. gespeichert. Vor allem wird aber im RAM auch das entpackte Betriebssystem der Geräte vorgehalten. Der Vorteil von RAM ist, dass er sehr schnell ist und für viele Schreib- und Lesevorgänge ausgelegt ist.
- **Flash:** Der Flash Speicher beinhaltet bei Cisco Produkten ein Image oder mehrere Images des Betriebssystems. Der Flash Speicher beispielsweise genutzt, wenn das Betriebssystem des Routers neu aufgesetzt werden muss. Dies geschieht aus dem komprimierten Image vom Flash.
- **NVRAM:** Im NVRAM sind die Boot Konfigurationen gespeichert. Der Inhalt des NVRAMs geht nicht verloren, wenn der Router neu gestartet wird, oder durch einen Stromausfall unterversorgt wird.
- **ROM:** Der ROM speichert beispielsweise Informationen, die für den Selbsttest des Routers nötig sind. Für ein Software Update müssen die ROM Speichersteine ausgetauscht werden.

Die Konfiguration ist im aktuellen Stadium des Versuchs lediglich im RAM. Der Befehl *copy running-config startup-config* kopiert die Konfiguration aus dem RAM in den NVRAM.

```
R1_HTW#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Noch die config Files vergleichen

Um zu testen, ob das Kopieren der Konfig Datei vom RAM in den NVRAM bietet sich ein Neustart des Routers an. Da der RAM flüchtig ist, sollte ja die Konfiguration verworfen werden, wenn sie nur im RAM gespeichert ist. Den Router kann man mit dem Befehl *reload* neu starten. Um die Aussage präziser zu machen, der Befehl reload stoppt nur das System. Wenn es als *restart on error* konfiguriert ist, bzw. nicht anders konfiguriert wurde, startet es automatisch neu.
Vor dem Test, ob die Konfiguration immer noch gültig ist, betrachten wir das Terminal beim Hochfahren des Routers.

```
R1_HTW#reload
Proceed with reload? [confirm]
```

```
*May 28 11:12:44.035: %SYS-5-RELOAD: Reload requested  by console.
    Reload Reason
: Reload Command.

System Bootstrap, Version 12.4(13r)T11, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2009 by cisco Systems, Inc.

Initializing memory for ECC
.
c2811 platform with 262144 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled


Upgrade ROMMON initialized
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0x1859ee4
Self decompressing the image : ######################
############################
##############################
################################################
########### [OK]

Smart Init is enabled
smart init is sizing iomem
  ID            MEMORY_REQ                  TYPE
0003E7          0X00473800 C2811 Mainboard
                0X000021B8 Onboard USB
                0X002C29F0 public buffer pools
                0X00211000 public particle pools
TOTAL:          0X009493A8

If any of the above Memory Requirements are
"UNKNOWN", you may be using an unsupported
configuration or there is a software problem and
system operation may be compromised.
Rounded IOMEM up to: 10Mb.
Using 3 percent iomem. [10Mb/256Mb]

[...]



Press RETURN to get started!
```

```
*May 28 11:13:53.831: %LINK-3-UPDOWN: Interface FastEthernet0/0,
    changed state t
o up
*May 28 11:13:53.835: %LINK-3-UPDOWN: Interface FastEthernet0/1,
    changed state t
o up
*May 28 11:13:53.835: %LINK-3-UPDOWN: Interface Serial0/0/0,
    changed state to do
wn
*May 28 11:13:53.835: %LINK-3-UPDOWN: Interface Serial0/0/1,
    changed state to do
wn
*May 28 11:13:54.831: %LINEPROTO-5-UPDOWN: Line protocol on
    Interface FastEthern
et0/0, changed state to down
*May 28 11:13:54.835: %LINEPROTO-5-UPDOWN: Line protocol on
    Interface FastEthern
et0/1, changed state to down
*May 28 11:13:54.835: %LINEPROTO-5-UPDOWN: Line protocol on
    Interface Serial0/0/
0, changed state to down
*May 28 11:13:54.835: %LINEPROTO-5-UPDOWN: Line protocol on
    Interface Serial0/0/
1, changed state to down
*May 28 11:13:56.055: %SYS-5-CONFIG_I: Configured from memory by
    console
*May 28 11:13:56.455: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version
    12.4(15)T7, RELEAS
E SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Wed 13-Aug-08 17:09 by prod_rel_team
*May 28 11:13:56.463: %SNMP-5-COLDSTART: SNMP agent on host R1_HTW
     is undergoing
 a cold start
*May 28 11:13:56.759: %SYS-6-BOOTTIME: Time taken to reboot after
    reload =   73
seconds
*May 28 11:13:57.875: %LINK-5-CHANGED: Interface FastEthernet0/1,
    changed state
to administratively down
*May 28 11:13:57.939: %LINK-5-CHANGED: Interface Serial0/0/1,
    changed state to a
dministratively down
```

Running Config

3.2.3 Fazit des Versuchs

Der Versuch hat uns die grundsätzlich Einrichtung eines Cisco Routers näher gebracht. Die grundsätzliche Einrichtung umfasst sowohl die physikalische Verkabelung, als auch auch die Einrichtung der Software.
Auf der physikalischen Seite haben wir die Interfaces von Routern und Switchen kennen gelernt. Die Interfaces können sowohl für den Payload sein, aber auch für die Konfiguration. Gerade bei der Konfiguration ist uns aufgefallen, dass sich hier die Profimodelle deutlich von den Geräten für den Heimbedarf unterscheiden. Während die meisten Geräte für den Heimbedarf weder separate Interfaces für Payload und Konfiguration, noch einen Unterschied zwischen einer flüchtigen Konfiguration und einer dauerhaften Konfiguration haben, sind die Profigeräte doch bei der Konfiguration deutlich aufwändiger. Der höhere Aufwand ermöglich aber im Gegenzug eine deutlich feinere Konfiguration.
Auf der logischen Seite haben wir etwas über die interne Arbeitsweise von Routern und Switchen gelernt. Diese Aussage bezieht sich auf die Berechtigungen und auf die verschiedenen Speicher innerhalb eines Geräts. Neben dieser Erkenntnis war der Versuch aber auch eine gelungene Einführung in das Terminal von IOS. In diesem Zusammenhang ist mit IOS das Cisco Internetwork Operating System, also dem Standard Betriebssystem von Cisco Routern und Switchen gemeint. Eine Verwechselung kann mit dem gleichnamigen Apple iOS, iPhone Operating System, soll hiermit ausgeschlossen werden.

3.3 Packet Tracer

Packet Tracer ist eine Netzwerk Simulationssoftware der Firma Cisco Systems. Packet Tracer kann die Geräte der Firma simulieren und ermöglicht so einen unkomplizierten Aufbau von Netzwerken. Der Vorteil von einer Simulationssoftware gegenüber dem echten Aufbau ist, dass Fehler schnell korrigiert werden können und komplexe Zusammenhänge anschaulich visualisiert werden können.
Für den Versuch ist nur ein Computer nötig, der die entsprechende Software installiert hat.

3.3.1 Aufbau des Netzwerkes

3.3.1.1 Geräte

Das virtuelle Netzwerk setzt sich aus zwei Computern, einem Switch und einem Router zusammen. Der Begriff „virtuelles Netzwerk“steht in diesem Fall nicht mit dem Begriff „v-Lan“im Zusammenhang, sondern soll ausdrücken, dass dieses Netzwerk und die Geräte von dem Programm simuliert werden. Der Aufbau wird in der Grafik 3.3 veranschaulicht.

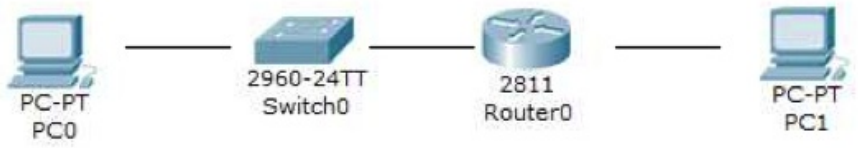


Abbildung 3.3: Der Aufbau des virtuellen Netzwerks

Device	Hostname	Interface	IP-Address	Subnet Mask	Default Gateway
PC0	Labor-PC1	Fast-Ethernet	192.168.0.10	255.255.255.128	192.168.0.1
Switch0	Labor-Switch1	FE0/1 u. FE0/2	NA	NA	NA
Router0	Labor-Router1	FE0/0	192.168.0.1	255.255.255.128	NA
		FE0/1	10.10.10.1	255.255.255.224	NA
PC1	Labor-PC2	Fast-Ethernet	10.10.10.10	255.255.255.224	10.10.10.1

Tabelle 3.2: Adresstabelle des Netzwerks

3.3.1.2 Adressvergabe

Die in der Tabelle 3.2 dargestellten Adressen stammen aus der Aufgabenbeschreibung des Versuchs. Interessant an diesem Aufbau ist, dass bis auf den Wechsel zwischen zwei v-Lan alle Standardsituationen in einem Netzwerk simuliert werden.

3.3.1.3 Überprüfung des Testaufbaus

Vertrauen ist gut, Kontrolle ist besser. Deswegen wird das soeben aufgebaute Netzwerk durch geeignete Pings getestet. Ping sendet lediglich ein ICMP echo request, wartet auf den echo reply und misst die benötigte Zeit. ICMP ist ein Bestandteil des Internet Protokolls, wird aber, je nach Literatur, als eigenständiges Protokoll betrachtet. Es ist relativ zuverlässig und eine geeignete Möglichkeit zu testen, ob ein Host erreichbar ist. Die Ergebnisse der Pings sind in der Tabelle 3.3 zusammengefasst. Diese Ergebnisse sind bei näherer Betrachtung interessant. Das Offensichtliche an den Ergebnissen ist, dass die Einrichtung des virtuellen Netzwerks scheinbar erfolgreich war. Betrachtet man die Zeiten genauer, fällt auf, dass es in jeder Zeile eine kleinere Zeit und eine größere Zeit gibt. In der Zeile PC2 fällt dieser Unterschied besonders deutlich aus. Zu

Zu / Von	PC1	PC2	Router1 (FE0/0)	Router1 (FE0/1)
PC1			78ms	62ms
PC2	82ms			35ms

Tabelle 3.3: Ergebnisse des Ping

besseren Übersicht werden noch einmal die Hostnamen aufgelöst:
10.10.10.10 → **192.168.0.10** = 82ms. Bei diesem Ping wurde das Netzwerk 10.10.10.0 verlassen und die Datenpakete mussten weiter geroutet werden. An diesem Prozess waren beide PC, der Router und der Switch beteiligt. Alleine aus der Anzahl der Geräte ergibt sich eine Latenz, darauf addiert sich die Latenz des Routings.
10.10.10.10 → **10.10.10.1** = 32ms. Dieser Ping hat das Netzwerk 10.10.10.0 nicht verlassen. Daher fällt die Latenz des Routings weg. Auch, wenn durch die anderen Geräte nur geringe Latenzen entstehen, PC1 und der Switch waren bei diesem Ping am Sendeprozess nicht beteiligt.
Die angegebenen Zeiten sind Mittelwerte, betrachtet man die Zeiten genauer, verstärkt sich der Eindruck.

```
Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 62ms, Average = 35ms
```

Listing 3.5: Die genauen Zeiten ohne Routing

```
Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 65ms, Maximum = 94ms, Average = 82ms
```

Listing 3.6: Die genauen Zeiten mit Routing

3.3.2 Simulieren und Analysieren eines ECHO REQUEST/ECHO REPLY

3.3.2.1 Aufbau

Der einzige Unterschied zum vorhergehenden Aufbau ist, dass die Software in den Simulationsmodus gewechselt wird. Dadurch ist es möglich, die einzelnen Pakete grafisch darzustellen und ihren Weg durch das Netzwerk zu verfolgen.

3.3.2.2 Ablauf des Versuchs

Von PC1 wird ein ein echo request zu PC2 gesendet. Dieser request soll von PC2 durch ein echo reply beantwortet werden. Dieser Weg entspricht einem Ping.

3.3.2.3 Auswertung des Versuchs

Auswertung schreiben

3.3.3 Fazit

Kommt auch noch

4 SDH Versuch

4.1 Einleitung

4.2 Downlink

4.3 Uplink

4.4 ARFCN

4.5 Untersuchung des Paketflusses mit Wireshark

5 RN Versuch

5.1 Einleitung

5.2 Downlink

5.3 Uplink

5.4 ARFCN

5.5 Untersuchung des Paketflusses mit Wireshark

Literatur

[1] Aaronia AG. *Frequenznutzungsplan GSM 1800*. http://www.aaronia.de/grundlagen/frequenzplaene/frequenzplan-gsm1800-de/.

[2] *Cisco 2960 Switch*. http://www.tape4backup.com/images/products/large/6047-_wsc296024ttl.jpg.

[3] Friedhelm Greis. *Cisco fordert schnelleren Videotransport in Zettabyte-Ära*. http://www.golem.de/news/traffic-prognose-cisco-fordert-schnelleren-videotransport-in-zettabyte-aera-1406-107124.html. 2014.

[4] Patapsco. *Darstellung der Liberator S*. http://www.patapsco.co.uk/-pdfs/Liberator_S_isdn_converter_isdn_conversion_pri_bri.pdf.

[5] Cisco Systems. *Cisco 2800 Router*. http://www.cisco.com/en/US/products-/ps5881/prod_view_selector.html.

Kolophon

Dieses Dokument wurde mit der LaTeX-Vorlage für Abschlussarbeiten an der htw saar im Bereich Informatik/Mechatronik-Sensortechnik erstellt (Version 1.0). Die Vorlage wurde von Yves Hary und André Miede entwickelt (mit freundlicher Unterstützung von Thomas Kretschmer und Helmut G. Folz).