

**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

<b>Inhaltsverzeichnis</b>	<b>v</b>
<b>Listings</b>	<b>1</b>
<b>1 GSM Versuch</b>	<b>1</b>
1.1 Allgemeine Beschreibung der Versuche . . . . .	1
1.1.1 Versuchsaufbau . . . . .	1
1.1.2 Die einzelnen Bauteile im Überblick . . . . .	1
1.2 Visualisieren von Frequenzen . . . . .	3
1.2.1 Frequenzen auflisten . . . . .	3
1.2.2 Frequenzen darstellen . . . . .	6
1.3 Anruf an die 2600 . . . . .	8
1.4 Datenmitschnitte . . . . .	9
1.4.1 Anruf mitschneiden . . . . .	9
1.5 Mitschnitt einer SMS . . . . .	18
1.5.1 Versuchsaufbau . . . . .	18
1.5.2 Versuchsdurchführung . . . . .	18
<b>2 BA Versuch</b>	<b>21</b>
2.1 Allgemeine Beschreibung des Versuchs . . . . .	21
2.2 Einrichten der Anlage . . . . .	21
2.2.1 Einrichten der Ports . . . . .	21
2.2.2 Einrichten der Routing Tabellen . . . . .	22
2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls . . . . .	23
2.3.1 Aufzeichnen des ISDN-D-Kanal Protokolls ?? . . . . .	23
2.3.2 Interpretieren des D-Kanal-Protokoll Mitschnitts . . . . .	23
<b>3 RSP Versuch</b>	<b>45</b>
3.1 Einleitung . . . . .	45
3.1.1 Benötigte Hardware für den Versuch . . . . .	45
3.2 Der Umgang mit Physikalischen Geräten . . . . .	47
3.2.1 Einrichtung eines Switchs . . . . .	47
3.2.2 Konfiguration eines Routers . . . . .	49
3.2.3 Fazit des Versuchs . . . . .	61
3.3 Packet Tracer . . . . .	62
3.3.1 Aufbau des Netzwerkes . . . . .	62

3.3.2	Simulieren und Analysieren eines ECHO REQUEST/ECHO REPLY	64
3.3.3	Fazit	68
<b>4</b>	<b>RSP Versuch</b>	<b>69</b>
4.1	Einleitung	69
4.2	Aufbau des Versuchs	69
4.2.1	Benötigte Geräte	69
4.3	Versuch	70
4.3.1	Konfigurieren der Router Basiseinstellungen	70
4.3.2	Konfigurieren der seriellen Interfaces	75
4.3.3	Konfigurieren der Fast Ethernet Interfaces	78
<b>5</b>	<b>SDH Versuch</b>	<b>83</b>
5.1	Einleitung	83
5.2	Downlink	83
5.3	Uplink	83
5.4	ARFCN	83
5.5	Untersuchung des Paketflusses mit Wireshark	83
<b>6</b>	<b>RN Versuch</b>	<b>85</b>
6.1	Einleitung	85
6.2	Downlink	85
6.3	Uplink	85
6.4	ARFCN	85
6.5	Untersuchung des Paketflusses mit Wireshark	85
	<b>Literatur</b>	<b>87</b>

# 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.

## 1 GSM Versuch



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 Voraussetzung.

#### 1.2.1.2 Versuchsdurchführung

Mit dem Tool lsursp wird überprüft, ob die USRP [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 O2 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

## 1 GSM Versuch

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.

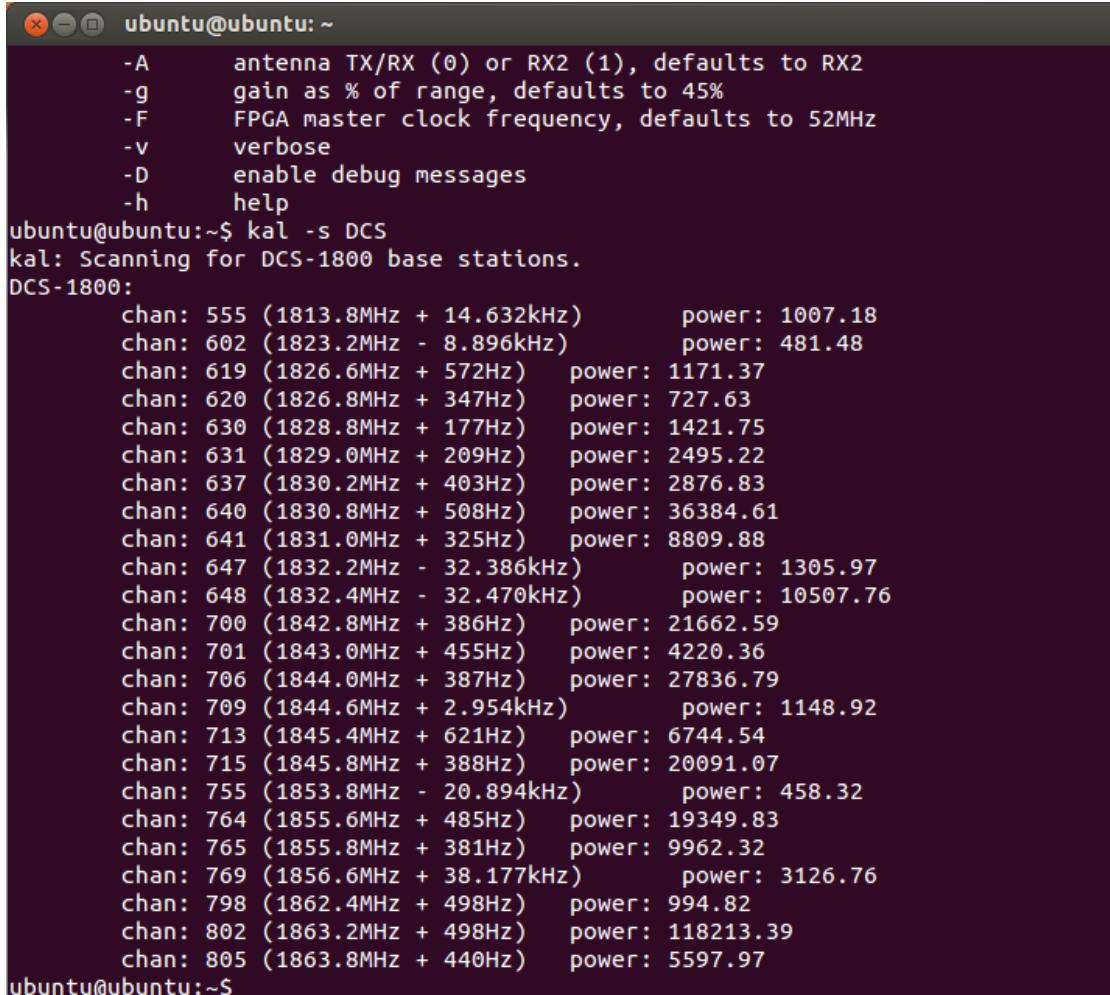
Den Scheiß habe ich mir quasi ausgedacht. Stimmt das annähernd?

Dazu was richtiges schreiben

**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.

## 1.2 Visualisieren von Frequenzen



```
ubuntu@ubuntu:~$ kal -s DCS
kal: Scanning for DCS-1800 base stations.
DCS-1800:
chan: 555 (1813.8MHz + 14.632kHz)      power: 1007.18
chan: 602 (1823.2MHz - 8.896kHz)        power: 481.48
chan: 619 (1826.6MHz + 572Hz)           power: 1171.37
chan: 620 (1826.8MHz + 347Hz)           power: 727.63
chan: 630 (1828.8MHz + 177Hz)           power: 1421.75
chan: 631 (1829.0MHz + 209Hz)           power: 2495.22
chan: 637 (1830.2MHz + 403Hz)           power: 2876.83
chan: 640 (1830.8MHz + 508Hz)           power: 36384.61
chan: 641 (1831.0MHz + 325Hz)           power: 8809.88
chan: 647 (1832.2MHz - 32.386kHz)       power: 1305.97
chan: 648 (1832.4MHz - 32.470kHz)       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 + 2.954kHz)        power: 1148.92
chan: 713 (1845.4MHz + 621Hz)            power: 6744.54
chan: 715 (1845.8MHz + 388Hz)           power: 20091.07
chan: 755 (1853.8MHz - 20.894kHz)        power: 458.32
chan: 764 (1855.6MHz + 485Hz)            power: 19349.83
chan: 765 (1855.8MHz + 381Hz)            power: 9962.32
chan: 769 (1856.6MHz + 38.177kHz)        power: 3126.76
chan: 798 (1862.4MHz + 498Hz)            power: 994.82
chan: 802 (1863.2MHz + 498Hz)            power: 118213.39
chan: 805 (1863.8MHz + 440Hz)            power: 5597.97
ubuntu@ubuntu:~$
```

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

## 1 GSM Versuch

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

	<b>von (MHz)</b>	<b>bis (MHz)</b>	<b>Kurzzeichen</b>	<b>Sendeleistung</b>	<b>Reichweite</b>	<b>Modulation</b>	<b>Gepulst</b>	<b>Betreiber</b>	<b>Sonstiges</b>	<b>Beschreibung</b>
	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)

[Black]	Militär
[Pink]	T-Mobile
[Blue]	O 2
[Red]	Vodafone
[Green]	e-plus

Abbildung 1.3: Frequenztabelle 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,

## 1.2 Visualisieren von Frequenzen

chan:	555 1813.8 MHz	Militär
chan:	602 1823.2MHz	T-Mobile
chan:	619 1826.6MHz	O <sub>2</sub>
chan:	620 1826.8 + 347Hz	O <sub>2</sub>
chan:	630 1828.8MHz	O <sub>2</sub>
chan:	631 1820.0MHz	Militär
chan:	637 1830.2MHz	O <sub>2</sub>
chan:	640 1830.8MHz	O <sub>2</sub>
chan:	641 1831.0MHz	O <sub>2</sub>
chan:	647 1832.2MHz	O <sub>2</sub>
chan:	648 1832.4MHz	O <sub>2</sub>
chan:	700 1842.8MHz	O <sub>2</sub>
chan:	701 1843.0MHz	O <sub>2</sub>
chan:	706 1844.0MHz	O <sub>2</sub>
chan:	709 1844.6MHz	O <sub>2</sub>
chan:	713 1845.4MHz	O <sub>2</sub>
chan:	715 1845.8MHz	O <sub>2</sub>
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

## 1 GSM Versuch

Wat han  
mir wei  
davon?

stark an weißes Rauschen

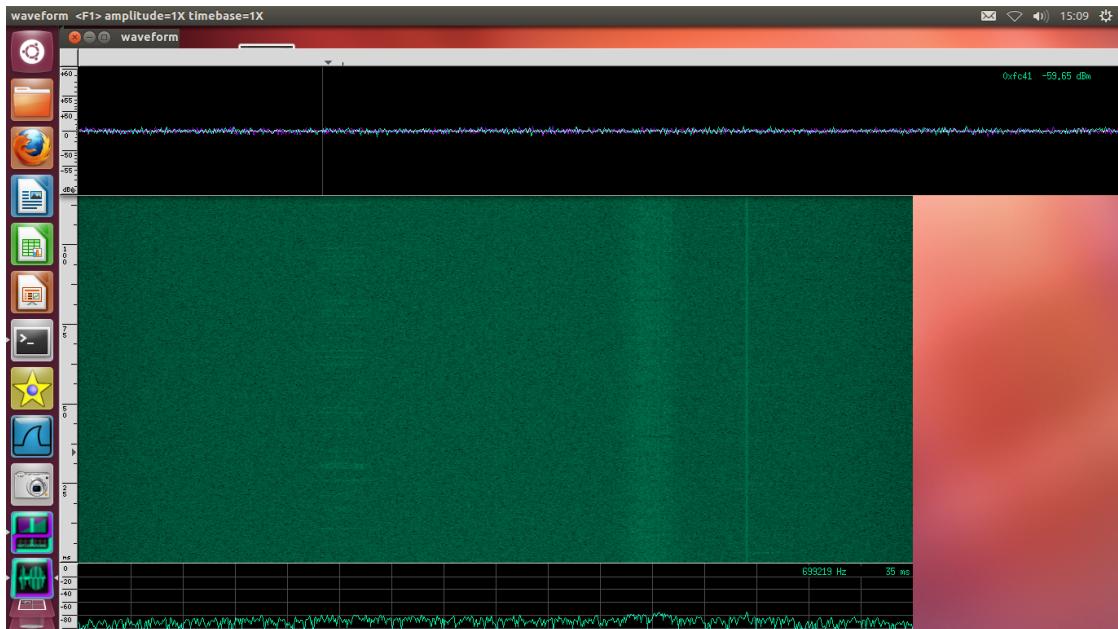


Abbildung 1.4: Eine visualisierte Frequenz

### 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 Weiterleitung 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 mitszuschneiden.

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.

Nachdem 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 unrelevanten 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.

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

## 1 GSM Versuch

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)  
umwan-  
deln 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 die Daten von der Funkschnittstelle in UDP Pakete kapselt. Der Layer 1 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 weitere 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
```

## 1.4 Datenmitschnitte

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.

```
■ GSM A-Link DTAP - Setup
Protocol discriminator: call control; call related ss messages
.... 001 = Protocol discriminator: call Control; call related ss messages (0x03)
0... .... = TI Flag: allocated by sender
000 ... = Sequence number: 1
0100 0101 = DTAP call control message type: setup (0x05)
Bearer capability 1 - (MS supports at least full rate speech version 1 and half rate speech version 1. MS has a greater preference for full rate speech version 1 than for half rate speech version 1)
Element ID: 0x00
Length: 6
Octet 3
Octets 3a - Speech Versions
Called Party BCD Number - (2600)
Element ID: 0x05
Length: 3
1... .... = Extension: No Extension
.000 .... = Type of number: unknown (0x00)
BCD digits: 2600
Calling plan identification: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
BCD digits: 2600
Call control capabilities
Element ID: 0x15
Length: 2
.... 0... = Maximum number of supported bearers: 1
.... 0... = MCAT: The mobile station does not support Multimedia CAT
.... 0... = ENCM: The mobile station does not support the Enhanced Network-Initiated In-call Modification procedure
.... 0... = DMF: The mobile station does not support the Prolonged clearing procedure
.... 1 = Other: The mobile station supports DMF as specified in subclause 5.3.7 of TS 24.008
0000 .... = Spare bit(s): 0
.... 0001 = Maximum number of speech bearers: 1
```

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.

## 1 GSM Versuch

```
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=ekvzvzbvifvluhd
      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: ekvzvzbvifvluhd
    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

Vorausgesetzt 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.

## 1.4 Datenmitschnitte

```
Frame 452: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: sip (5060), Dst Port: na-localise (5062)
Session Initiation Protocol (100)
  Status-Line: SIP/2.0 100 Trying
    Status-Code: 100
    [Resent Packet: False]
    [Request Frame: 451]
    [Response Time (ms): 0]
  Message Header
    Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hg4bkobts286aec235c0a789c46;received=127.0.0.1;rport=5062
      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=ekvzvzbbyilfvluhd
      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: ekvzvzbbyilfvluhd
    To: <sip:2600@127.0.0.1>
      SIP to address: sip:2600@127.0.0.1
        SIP to address User Part: 2600
        SIP to address Host Part: 127.0.0.1
      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-Length: 0
```

Abbildung 1.8: trying Nachricht im SIP Protokoll

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

## 1 GSM Versuch

```
□ 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;rport
      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=ekvzvzbylefvluhd
      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: ekvzvzbylefvluhd
    □ 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.

## 1.4 Datenmitschnitte

```

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=ekvzvzbvifvluhd
      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: ekvzvzbvifvluhd
    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

```

## 1 GSM Versuch

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=ekvzvzbvifvluhd
      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: ekvzvzbvifvluhd
    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

#### 1.4 Datenmitschnitte

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.

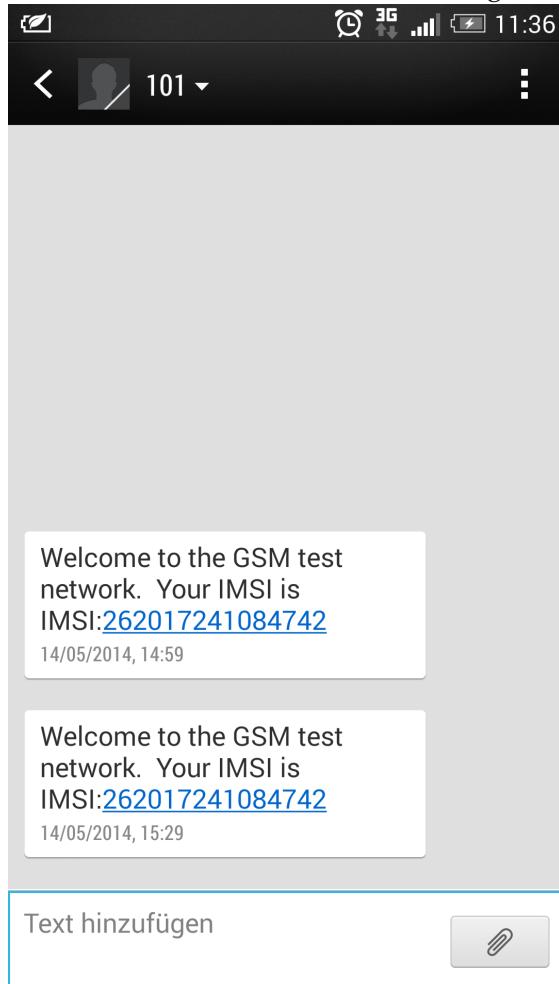


Abbildung 1.14: Quittierung der Einwahl in das GSM Netz

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

## 1 GSM Versuch

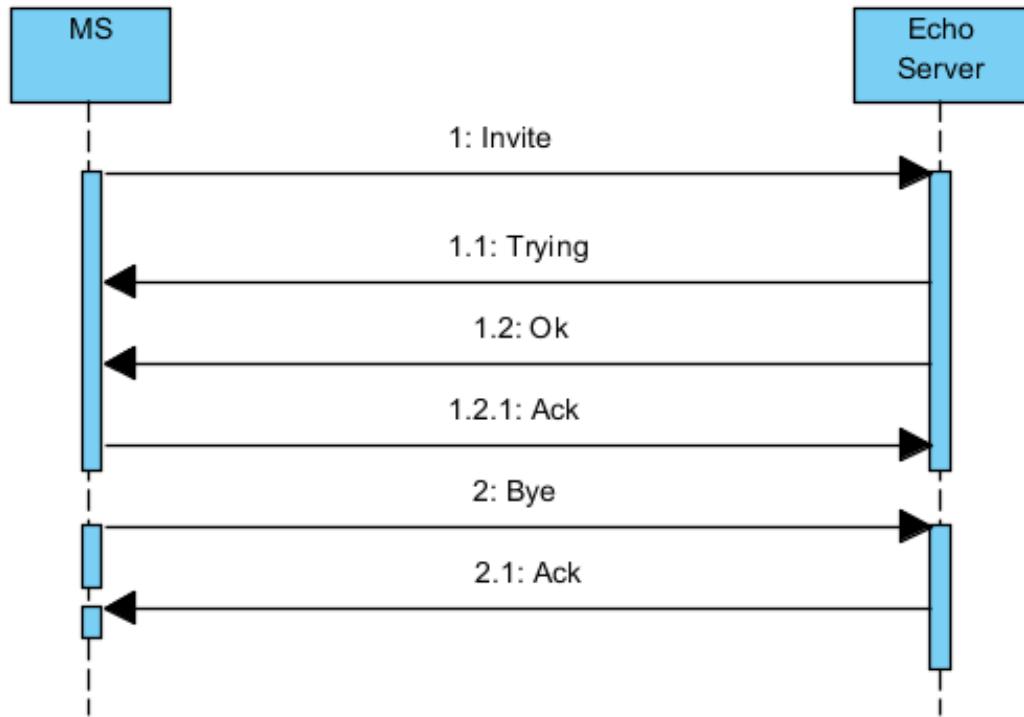


Abbildung 1.15: Ablauf SIP

## 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 Inhalt „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

## 1.5 Mitschnitt einer SMS

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

Wie man sehr gut in der 1.16 sehen kann ist der gesendete 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 handelt.

Abbildung 1.16: Gegenüberstellung Gesendet und Empfangen

Wie man in 1.17 sehen kann wird das Senden der SMS wieder von SIP initialisiert. Der Vorgang entspricht 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
566	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.

##### 2.2.1.2 Versuchsdurchführung

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

War da  
nicht  
noch  
was zur  
Stromver-  
sorgung?

## 2 BA Versuch

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 Voraussetzung.

### 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.

## *2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls*

### **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 Versuchsdurchführung**

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**

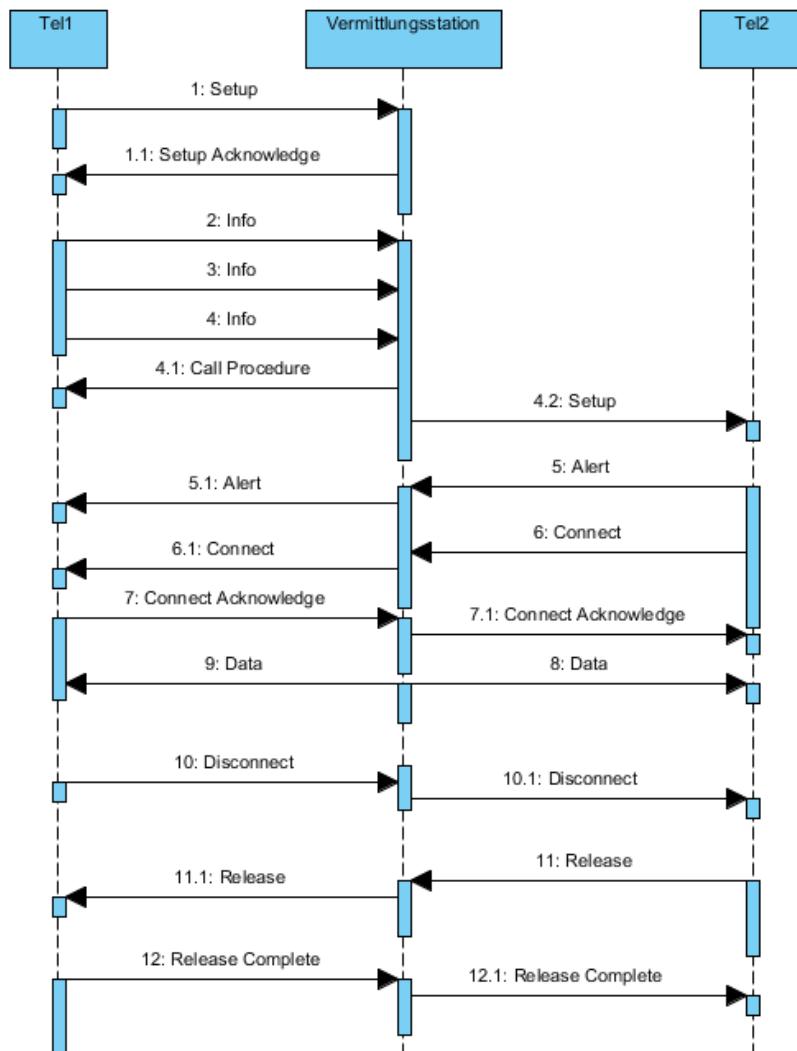
Der Versuch ?? muss durchgeführt sein und die Ergebnisse müssen vorliegen. Für die Auswertung muss ein Computer mit der Software Wireshark bereit stehen.

#### **2.3.2.2 Versuchsdurchführung**

Die aufgezeichneten Protokolldaten werden mit Wireshark geöffnet.

## 2 BA Versuch

### 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 Identity Request behandelt. Diese fordert einen TEI Wert zur Identifizierung des Endgerätes an.

### 2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

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 Identity Assigned bestätigt und ein TEI Wert wird dem Endgerät zugewiesen. In diesem Fall wird der Wert 64 zugewiesen.

## 2 BA Versuch

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: 0xeff  
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

### 2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

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.

## 2 BA Versuch

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)  
.00 0000 = Information transfer capability: Speech (0x00)  
1... .... = Extension indicator: last octet  
.00. .... = Transfer mode: Circuit mode (0x00)  
.00 0000 = Information transfer rate: 64 kbit/s (0x10)  
1... .... = Extension indicator: last octet  
.01. .... = Layer identification: Layer 1 identifier (0x01)  
.00 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?

Wie man auf dem nachfolgenden Bild in Grau hinterlegt erkennen kann wird der

### *2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls*

TU-T Standardized-Coding verwendet. Diese Richtlinie gilt für das digitalisieren analoger Audiosignale mittels Puls-Code-Modulation. Der Einsatzbereich für dieses Codecs ist wie zu erwarten in der klassischen sowie in der IP-Telefonie.

## 2 BA Versuch

No.	Time	Source	Destination	Protocol	Info
11	5294.732552	User	Network	Q.931	SETUP

Frame 11 (24 bytes on wire, 24 bytes captured)  
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)  
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 I  
    Calling party number: '100'  
        Information element: Calling party number  
        Length: 5  
        .... 0000 = Numbering plan: Unknown (0x00)  
        .000 .... = Number type: Unknown (0x00)  
        0... .... = Extension indicator: information continues through the n  
        .... .00 = Screening indicator: User-provided, not screened (0x00)  
        .00. .... = Presentation indicator: Presentation allowed (0x00)  
        1... .... = Extension indicator: last octet  
    Calling party number digits: 100  
    High-layer compatibility  
        Information element: High-layer compatibility  
        Length: 2  
        .00. .... = Coding standard: ITU-T standardized coding (0x00)  
        High layer characteristics identification: Telephony

### *2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls*

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

Im Setup Frame das man in der vorherigen Frage bereits betrachteten konnte wird die MSN des anrufenden Teilnehmers übertragen. Zu finden ist diese unter dem Abschnitt Q.931 als Callin Party-Number. Die MSN des Teilnehmers auf der anderen Seite steht die MSN in dem Connect Rahmen. Diese ist ebenfalls im Abschnitt Q.931 unter Connected Number zu sehen.

## 2 BA Versuch

No.	Time	Source	Destination	Protocol	Info
370	5944.594584	Network	User	Q.931	CONN

Frame 370 (15 bytes on wire, 15 bytes captured)  
Arrival Time: May 21, 2014 13:43:58.015584000  
[Time delta from previous captured frame: 1.964032000 seconds]  
[Time delta from previous displayed frame: 1.964032000 seconds]  
[Time since reference or first frame: 5944.594584000 seconds]  
Frame Number: 370  
Frame Length: 15 bytes  
Capture Length: 15 bytes  
[Frame is marked: False]  
[Protocols in frame: ~~isdn:lapd:q931~~]  
Point-to-Point Direction: Received (1)

ISDN

    Channel: D (0)  
    Link Access Procedure, Channel D (LAPD)  
        [Direction: Network->User (1)]  
        Address Field: 0x0281  
            0000 00.. .... .... = SAPI: Q.931 Call control procedure (0)  
            .... ..1. .... .... = C/R: 1  
            .... ...0 .... .... = EA1: 0  
            .... .... 1000 000. = TEI: 64  
            .... .... .... ..1 = EA2: 1  
        Control field: I, N(R)=4, N(S)=3 (0x0806)  
            0000 100. .... .... = N(R): 4  
            .... .... 0000 011. = N(S): 3  
            .... .... .... ..0 = Frame type: Information frame (0x0000)

Q.931

    Protocol discriminator: Q.931  
    Call reference value length: 1  
    Call reference flag: Message sent to originating side  
    Call reference value: 01  
    Message type: CONNECT (0x07)  
    Connected number: '200'  
        Information element: Connected number  
        Length: 5  
            .... 0000 = Numbering plan: Unknown (0x00)  
            .000 .... = Number type: Unknown (0x00)  
            0... .... = Extension indicator: information continues through the next octet  
            .... ..00 = Screening indicator: User-provided, not screened (0x00)  
            ..00. .... = Presentation indicator: Presentation allowed (0x00)  
            1... .... = Extension indicator: last octet  
        Connected party number digits: 200

## 2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

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

Die Schicht 3 ist Aufgebaut sobald das Netzwerk dem User eine Seup-Acknowledgment-Nachricht übersendet. Diese bestätigt die vom User gesendete Setup-Nachricht und das alles gut gegangen ist.

Vielleicht kann man hier mehr ins Detail gehen

## 2 BA Versuch

No.	Time	Source	Destination	Protocol	Info
397	6157.998584	Network	User	Q.931	SETU
Frame 397 (11 bytes on wire, 11 bytes captured)					
Arrival Time: May 21, 2014 13:47:31.419584000					
[Time delta from previous captured frame: 0.008000000 seconds]					
[Time delta from previous displayed frame: 0.008000000 seconds]					
[Time since reference or first frame: 6157.998584000 seconds]					
Frame Number: 397					
Frame Length: 11 bytes					
Capture Length: 11 bytes					
[Frame is marked: False]					
[Protocols in frame: <del>isdn:lapp:q931</del> ]					
Point-to-Point Direction: Received (1)					
ISDN					
Channel: D (0)					
Link Access Procedure, Channel D (LAPD)					
[Direction: Network->User (1)]					
Address Field: 0x0281					
0000 00... .... .... = SAPI: Q.931 Call control procedure (0)					
.... ..1. .... .... = C/R: 1					
.... ...0 .... .... = EA1: 0					
.... .... 1000 000. = TEI: 64					
.... .... .... .1 = EA2: 1					
Control field: I, N(R)=5, N(S)=2 (0xA04)					
0000 101. .... .... = N(R): 5					
.... .... 0000 010. = N(S): 2					
.... .... .... .0 = Frame type: Information frame (0x0000)					
Q.931					
Protocol discriminator: Q.931					
Call reference value length: 1					
Call reference flag: Message sent to originating side					
Call reference value: 01					
Message type: SETUP ACKNOWLEDGE (0xd)					
Channel identification					
Information element: Channel identification					
Length: 1					
1.... .... = Extension indicator: last octet					
.0... .... = Interface identifier present: False					
..0. .... = Interface type: Basic rate interface					
.... 1... = Indicated channel is exclusive: Exclusive; only the indicated channel is active					
.... .0.. = D-channel indicator: False					
.... ..01 = Information channel selection: B1 channel (0x01)					

### *2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls*

#### **7. Welchen B-Kanal weist die Vermittlung der Verbindung zu?**

In dem Call Proceeding-Frame findet man die Angabe zu dem genutzten Channel. In unserem Fall wäre das unter Q.931, Information channel selection: B1 channel (0x01. Dies gibt an das der genutzte Channel hier der B1 ist.

## 2 BA Versuch

No.	Time	Source	Destination	Protocol	Info
181	5609.390552	Network	User	Q.931	CALL
Frame 181 (11 bytes on wire, 11 bytes captured)					
Arrival Time: May 21, 2014 13:38:22.811552000					
[Time delta from previous captured frame: 0.142016000 seconds]					
[Time delta from previous displayed frame: 0.142016000 seconds]					
[Time since reference or first frame: 5609.390552000 seconds]					
Frame Number: 181					
Frame Length: 11 bytes					
Capture Length: 11 bytes					
[Frame is marked: False]					
[Protocols in frame: <del>isdn</del> :lapd:q931]					
Point-to-Point Direction: Received (1)					
ISDN					
Channel: D (0)					
Link Access Procedure, Channel D (LAPD)					
[Direction: Network->User (1)]					
Address Field: 0x0281					
0000 00.. .... .... = SAPI: Q.931 Call control procedure (0)					
.... ..1. .... .... = C/R: 1					
.... ...0 .... .... = EA1: 0					
.... .... 1000 000. = TEI: 64					
.... .... .... .1 = EA2: 1					
Control field: I, N(R)=30, N(S)=13 (0x3C1A)					
0011 110. .... .... = N(R): 30					
.... .... 0001 101. = N(S): 13					
.... .... .... .0 = Frame type: Information frame (0x0000)					
Q.931					
Protocol discriminator: Q.931					
Call reference value length: 1					
Call reference flag: Message sent to originating side					
Call reference value: 01					
Message type: CALL PROCEEDING (0x02)					
Channel identification					
Information element: Channel identification					
Length: 1					
1... .... = Extension indicator: last octet					
.0... .... = Interface identifier present: False					
..0. .... = Interface type: Basic rate interface					
.... 1... = Indicated channel is exclusive: Exclusive; only the indicated channel is active					
.... .0.. = D-channel indicator: False					
.... ..01 = Information channel selection: B1 channel (0x01)					

## *2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls*

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

Die Information-Frames senden bereits Teile der Rufnummer bevor die eigentliche Vermittlung anfängt. In unserem Fall werden hier insgesamt drei Frames gesendet die jeweils einer Nummer enthalten. Aufgrund der Übersichtlichkeit sind die Frames stark gekürzt und direkt hintereinander gesetzt.

## 2 BA Versuch

No.	Time	Source	Destination	Protocol	Info
247	5803.908536	User	Network	Q.931	INFO
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: INFORMATION (0x7b)				
	Called party number: '2'				
	Information element: Called party number				
	Length: 2				
	.... 0001 = Numbering plan: E.164 ISDN/telephony numbering (0x01)				
	.000 .... = Number type: Unknown (0x00)				
	1... .... = Extension indicator: last octet				
	Called party number digits: 2				
	E.164 Called party number digits: 2				
No.	Time	Source	Destination	Protocol	Info
249	5804.910552	User	Network	Q.931	INFO
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: INFORMATION (0x7b)				
	Called party number: '0'				
	Information element: Called party number				
	Length: 2				
	.... 0001 = Numbering plan: E.164 ISDN/telephony numbering (0x01)				
	.000 .... = Number type: Unknown (0x00)				
	1... .... = Extension indicator: last octet				
	Called party number digits: 0				
	E.164 Called party number digits: 0				
No.	Time	Source	Destination	Protocol	Info
251	5805.124584	User	Network	Q.931	INFO
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: INFORMATION (0x7b)				
	Called party number: '0'				
	Information element: Called party number				
	Length: 2				
	.... 0001 = Numbering plan: E.164 ISDN/telephony numbering (0x01)				
	.000 .... = Number type: Unknown (0x00)				
	1... .... = Extension indicator: last octet				
	Called party number digits: 0				
	E.164 Called party number digits: 0				

### *2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls*

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

Nachdem alle Ziffern gesendet worden sind und die Vermittlungstelle diese als gültige Rufnummer erkannt hat sendet Sie einen Call Proceeding-Frame an das Telefon und es wird keine weitere Ziffer mehr angenommen. Nun beginnt die Anwahl des anderen Teilnehmers. Der Call-Proceeding-Frame ist bereits zwei Fragen vorher gezeigt worden und wird deshalb hier nicht noch einmal aufgeführt.

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

Jedes Endgerät das den Anruf annehmen kann sendet eine Alerting Nachricht und beginnt darauf hin zu Klingeln.

## 2 BA Versuch

No.	Time	Source	Destination	Protocol	Info
255	5805.294552	Network	User	Q.931	ALEP
Frame 255 (8 bytes on wire, 8 bytes captured)					
Arrival Time: May 21, 2014 13:41:38.715552000					
[Time delta from previous captured frame: 0.007968000 seconds]					
[Time delta from previous displayed frame: 0.007968000 seconds]					
[Time since reference or first frame: 5805.294552000 seconds]					
Frame Number: 255					
Frame Length: 8 bytes					
Capture Length: 8 bytes					
[Frame is marked: False]					
[Protocols in frame: <del>isdn:lapp:q931</del> ]					
Point-to-Point Direction: Received (1)					
ISDN					
Channel: D (0)					
Link Access Procedure, Channel D (LAPD)					
[Direction: Network->User (1)]					
Address Field: 0x0281					
0000 00... .... .... = SAPI: Q.931 Call control procedure (0)					
.... ..1. .... .... = C/R: 1					
.... ...0 .... .... = EA1: 0					
.... .... 1000 000. = TEI: 64					
.... .... .... ..1 = EA2: 1					
Control field: I, N(R)=4, N(S)=2 (0x0804)					
0000 100. .... .... = N(R): 4					
.... .... 0000 010. = N(S): 2					
.... .... .... ..0 = Frame type: Information frame (0x0000)					
Q.931					
Protocol discriminator: Q.931					
Call reference value length: 1					
Call reference flag: Message sent to originating side					
Call reference value: 01					
Message type: ALERTING (0x01)					

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

Nachdem das Netzwerk eine Release Complete Nachricht gesendet hat sind alle vorher belegten Kanäle wieder frei und Schicht 3, sowie Schicht 2 wieder abgebaut.

### 2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

No.	Time	Source	Destination	Protocol	Info
261	5808.828536	User	Network	Q.931	RELEASE C

```

Frame 261 (8 bytes on wire, 8 bytes captured)
    Arrival Time: May 21, 2014 13:41:42.249536000
        [Time delta from previous captured frame: 0.013984000 seconds]
        [Time delta from previous displayed frame: 0.013984000 seconds]
        [Time since reference or first frame: 5808.828536000 seconds]
    Frame Number: 261
    Frame Length: 8 bytes
    Capture Length: 8 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)=4, N(S)=5 (0x080A)
            0000 100. .... .... = N(R): 4
            .... .... 0000 101. = N(S): 5
            .... .... ....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: RELEASE COMPLETE (0x5a)

```

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?

Durch Abnehmen des Hörers wird für gewöhnlich eine Setup Nachricht gesendet wodurch bereits eine Verbindung zur Vermittlungsstelle aufgebaut wird. Nimmt der Teilnehmer also erst den Hörer ab können bereits die ersten Ziffern überliefert werden. Dieser Vorgang ist durch den Versuch gut nachvollziehbar. Im Gegensatz

## 2 BA Versuch

dazu kann der Nutzer ebenfalls die Ziffern erst tippen und dann den Hörer abnehmen. Dies hat zur Folge das die benötigten Ziffern bereits vorhanden sind bevor die Setup-Nachricht gesendet wird. Dadurch können die Ziffern direkt in der Setup-Nachricht mit gesendet werden. Der folgende Frame zeigt das bereits die Called-Party-Number eingetragen ist. Hier wird das Endgerät mit der Nummer 100 von dem Endgerät mir der Nummer 200 angerufen. Der Frame wurde aufgrund der Größe etwas zugeschnitten, er enthält jedoch alle wichtigen Informationen.

### 2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

No.	Time	Source	Destination	Protocol	Info
337	5879.564536	Network	User	Q.931	SETUP
Q.931					
		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 (0x01)			
		Channel identification			
		.... ..01 = Information channel selection: B1 channel (0x01)			
		Calling party number: '200'			
		Information element: Calling party number			
		Length: 5			
		.... 0000 = Numbering plan: Unknown (0x00)			
		.000 .... = Number type: Unknown (0x00)			
		0.... .... = Extension indicator: information continues through the next octet			
		.... ..00 = Screening indicator: User-provided, not screened (0x00)			
		.00. .... = Presentation indicator: Presentation allowed (0x00)			
		1.... .... = Extension indicator: last octet			
		Calling party number digits: 200			
		Called party number: '100'			
		Information element: Called party number			
		Length: 4			
		.... 0001 = Numbering plan: E.164 ISDN/telephony numbering (0x01)			
		.000 .... = Number type: Unknown (0x00)			
		1.... .... = Extension indicator: last octet			
		Called party number digits: 100			
		E.164 Called party number digits: 100			
		High-layer compatibility			
		Information element: High-layer compatibility			
		Length: 2			
		.00. .... = Coding standard: ITU-T standardized coding (0x00)			
		High layer characteristics identification: Telephony			

## 2 BA Versuch

Nachricht	Alert	Nachrichtenelement	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 zum 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 schrei-  
ben?

### 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 Referenzmodell 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 RSP Versuch

#### 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 2960 Switch [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. Router 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 Netzwerk-adresse 172.36.0.0 ein

### 3.2 Der Umgang mit Physikalischen Geräten

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 Router, verliert der Administrator die Kontrolle über den Router. Da sich mit einer geänderten Adresse der Router und der Computer in verschiedenen 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 Router verloren hat speichert er die neue Konfiguration im Computer. Obwohl sich Computer und Router vermeintlich wieder in den gleichen Netzen befinden, hat er keinen Zugriff mehr auf den Router.

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.

### 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 Aufführungsmodus, 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 zurückgesetzt werden. Dadurch wird vermieden, dass bereits bestehende Konfigurationen die Ergebnisse beeinflussen. Die Ausgabe ist ähnlich der Ausgabe 3.1. 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.

### 3 RSP Versuch

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.	<i>ap&gt;</i>	Enter the logout command.
Privileged EXEC	From user EXEC mode, enter the enable command.	<i>ap#</i>	To exit to user EXEC mode, enter the disable command.
Global configuration	From privileged EXEC mode, enter the configure command.	<i>ap(config)#</i>	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.	<i>ap(config-if)#</i>	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: Die unterschiedlichen Command Modi von IOS

### 3.2 Der Umgang mit Physikalischen Geräten

**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 zurückgesetzt 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
```

### 3 RSP Versuch

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.
```

### 3.2 Der Umgang mit Physikalischen Geräten

```
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.

```
Password:  
Router#enable  
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
```

### 3 RSP Versuch

```
    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
```

### 3.2 Der Umgang mit Physikalischen Geräten

```
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
```

### 3 RSP Versuch

```
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 der Konfiguration nach dem Konfigurieren

### 3.2 Der Umgang mit Physikalischen Geräten

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.

```
R1_HTW#show startup-config
Using 1039 out of 245752 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
```

### 3 RSP Versuch

```
speed auto
!
interface Serial0/0/0
description R1 WAN
ip address 192.168.1.193 255.255.255.252
!
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 3.5: Die Ausgabe der Startup Config

Ein Unterschied zwischen *show running-config* und *show startup-config* ist der Unterschied der Hostnamen. Der Unterschied zwischen der running config und der startup config besteht darin, dass die startup config im NVRAM des Routers gespeichert ist, die running config ist im RAM gespeichert. 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 Er-

### 3.2 Der Umgang mit Physikalischen Geräten

läuterungen zu den Speichersorten stammen von Cisco [6]

- **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. Aber auch beim Starten des Switches wird ein Image vom Flash Speicher in den RAM geladen.
- **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 unversorgt wird.
- **ROM:** Der ROM speichert beispielsweise Informationen, die für den Selbsttest des Routers nötig sind. Da aus dem ROM nur gelesen werden kann, müssen für ein Software Update einige 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]
```

Betrachten wir nun die startup config, sollte die Ausgabe wie die Ausgabe 3.4 aussehen.

Listing 3.6: Die Startup Config nach dem Kopieren in den NVRAM

```
R1_HTW#show startup-config
Using 1058 out of 245752 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1_HTW
!
boot-start-marker
```

### 3 RSP Versuch

```
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
```

### 3.2 Der Umgang mit Physikalischen Geräten

```
!
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
\en{lstlisting}
```

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 \textit{reload} neu starten. Um die Aussage präziser zu machen, der Befehl reload stoppt nur das System. Wenn es als \textit{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.

```
\begin{lstlisting}
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.
```

### 3 RSP Versuch

### 3.2 Der Umgang mit Physikalischen Geräten

```
*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 FastEthernet
eth0/0, changed state to down
*May 28 11:13:54.835: %LINEPROTO-5-UPDOWN: Line protocol on
    Interface FastEthernet
eth0/1, 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, RELEASE
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
```

#### 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 Kon-

### 3 RSP Versuch

figuration, noch einen Unterschied zwischen einer flüchtigen Konfiguration und einer dauerhaften Konfiguration haben, sind die Profigeräte doch bei der Konfiguration deutlich aufwändiger. Der höhere Aufwand ermöglicht 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 das Standard Betriebssystem von Cisco Routern und Switchen gemeint. Eine Verwechslung 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.

Im folgenden wechseln die Namen der eingerichteten Computer. Dies ist der Versuchsbeschreibung geschuldet. An Passagen, an denen ein Wechsel des Namens die Ergebnisse des Versuchs unverständlich machen kann, wird aufgrund der geänderten Namen genauer erklärt.

Oder habe ich mich irgendwo verhaspelt?

### 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.

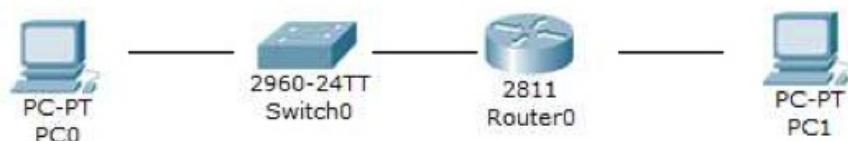


Abbildung 3.3: Der Aufbau des virtuellen Netzwerks

### 3.3 Packet Tracer

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

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

Tabelle 3.3: Ergebnisse des Ping

#### 3.3.1.2 Adressvergabe

Die in der Tabelle 4.1 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 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

### 3 RSP Versuch

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, verstkt 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 3.7: 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 3.8: 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 mglich, die einzelnen Pakete grafisch darzustellen und ihren Weg durch das Netzwerk zu verfolgen. Zur Erinnerung, der Aufbau des virtuellen Netzwerks ist in der Grafik 3.3 dargestellt.

### 3.3.2.2 Ablauf des Versuchs

Von PC1 wird ein echo request zu PC2 gesendet. Dieser request soll von PC2 durch ein echo reply beantwortet werden. Dieser Weg entspricht einem Ping. Durch die Visualisierung von Packet Tracer kann anschaulich berprft werden, wie sich die Pakete und Frames bei den bergangen zwischen den einzelnen Gerten verhalten.

### 3.3.2.3 Auswertung des Versuchs

Das Echo Paket befindet sich noch im PC1. Die Detailsicht ist in der Grafik 3.5 zu sehen. Dort sind die drei relevanten OSI Layer dargestellt. Im Layer 3 ist die IP Adresse von PC1 als Quelladresse und die IP Adresse von PC2 als Zieladresse zu sehen. Die Grafik 3.6 zeigt die gleiche ICMP Nachricht in der OSI Modell Darstellung. Da dort die relevanten Informationen zusammengefasst sind, werden wir uns im folgenden auf diese Ansicht beschrken.

Die Ansicht, wie die ICMP Nachricht im Router aussieht ist in der Grafik 3.7. Offensichtlich hat sich auf Layer 3 nichts gendert. Das war auch zu erwarten, da es sich

### 3.3 Packet Tracer

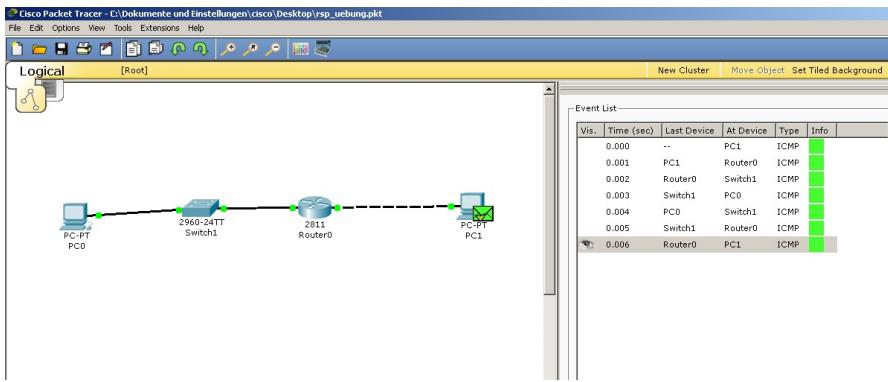


Abbildung 3.4: Der Beginn des echo request

immer noch um den gleichen echo request handelt. Die Quelle ist weiterhin PC1 und das Ziel ist PC2.

Wo eine Veränderung stattgefunden hat ist auf Layer 2. Dort ist die Quell Adresse die Zieladresse aus der Grafik 3.6. Auch diese Beobachtung deckt sich mit den Erwartungen. Die ICMP Nachricht befindet sich im Layer 3. Da der Layer 3 auf die Sicherungsschicht, bzw. Layer 2, angewiesen ist, muss die ICMP Nachricht in ein Ethernet Frame verpackt werden. Der Router packt diesen Ethernet Frame wieder aus, da er anhand des Layer 3 Routingentscheidungen treffen muss.

Der Ethernet Frame erreicht den Router am Interface FE0/1. Dieses Interface hängt im Netzwerk 10.10.10.0. Anhand des Layer 3 Headers weiß der Router, dass dieses Paket in das Netzwerk 192.168.0.0 geroutet werden muss. Dieses Netzwerk ist am Interface FE0/0 hinterlegt und somit direkt erreichbar. Er verpackt die ICMP Nachricht wieder einen Ethernet Frame. Dieses Frame wird in das andere Netzwerk, also auf den anderen Port gesendet. Dieses Senden zwischen den Ports erkennt man einfach, wenn man die In- und Out Layers in der Grafik 3.7 vergleicht. Dort ändern sich auf Layer 2 die Adressen und auf Layer 1 ist auch ausgeschrieben, dass die Ports gewechselt werden. Die Grafik 3.8 ist umspektakulär. Der Layer 3 kann im Switch nicht eingesehen werden und auf Layer 2 ändert sich nichts. Die Änderung findet auf Layer 1 statt. Dieses Ergebnis ist einfach zu erklären. Ein Switch beherrscht nur die Layer 1 und 2. Die Logik, die ein Switch auf Layer 2 leistet, ist zu entscheiden, an welchen Port ein Ethernet Frame weitergeleitet werden soll. Diese Aussage ist eigentlich unvollständig, da ein Switch auch für die Einhaltung v-Lan übernimmt und verschiedene Modi der Weiterleitung(bsp. Cut-through oder Store-and-Forward) hat. An dieser Stelle beschränken wir uns aber um das reine Weiterleiten auf einen anderen Port. Für anderen Teilnehmer ist ein Switch aber transparent, also nahezu unsichtbar. Auf Layer 1 ist zu sehen, dass der Switch den Port wechselt. Der Hintergrund ist, dass das Kabel des Routers an einem Port hängt, als das Kabel von PC0.

In der Grafik 3.9 ändert sich zwischen In Layers und Out Layers auf Layer 3 der Header. Dort werden Quell- und Zieladresse vertauscht und der ICMP Message Type ändert sich von 8 auf 0. Diese Änderung ergibt sich daraus, dass ein echo request empfangen

### 3 RSP Versuch

wurde. Die Quelle dieses Pakets ist PC 1, das Ziel ist PC 0. Der Message Type ist 8, dieser Message Type bedeutet echo request. Die Antwort hat die Quelle PC 0, da dieser antwortet und das Ziel PC 1, da dieser angefragt hat und nun die Antwort erhält. Der Message Type ist 0, dieser hat die Bedeutung echo reply. Die Änderung auf Layer 2 ist, dass die Ziel- und Quelladressen vertauscht werden. Der Hintergrund ist, dass der Ethernet Frame vom Router (über den Switch) zu PC 0 geschickt wurde. Die Antwort wird von PC 0 (über den Switch) zum Router geschickt.

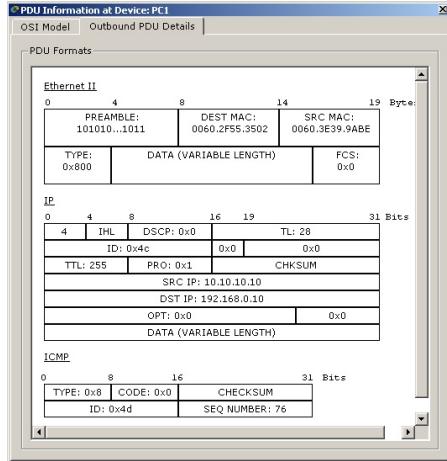


Abbildung 3.5: Detailansicht der ICMP Nachricht in PC1

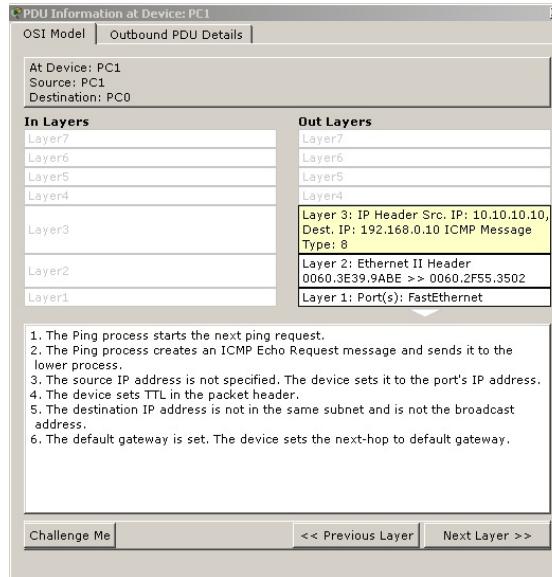


Abbildung 3.6: Ansicht der ICMP Nachricht in PC1

Der Weg des echo reply verläuft analog zu dem Weg des echo request. Deswegen wird

### 3.3 Packet Tracer

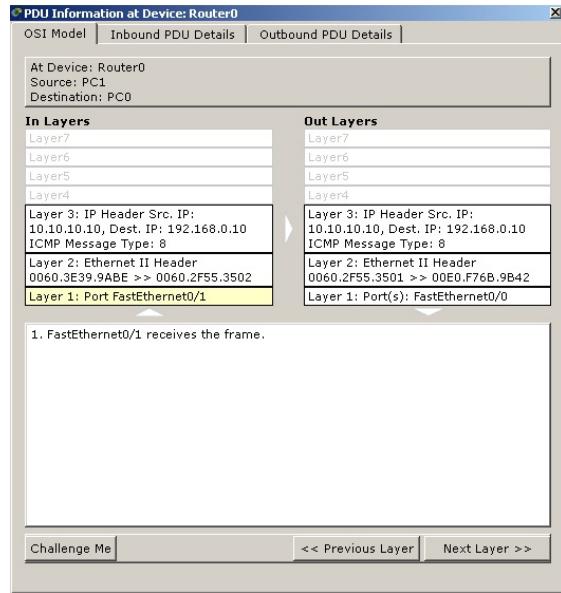


Abbildung 3.7: Ansicht der ICMP Nachricht im Router

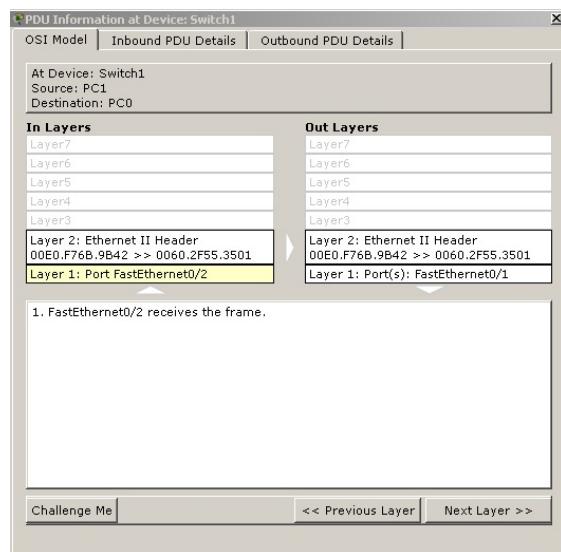


Abbildung 3.8: Ansicht der ICMP Nachricht im Switch

### 3 RSP Versuch

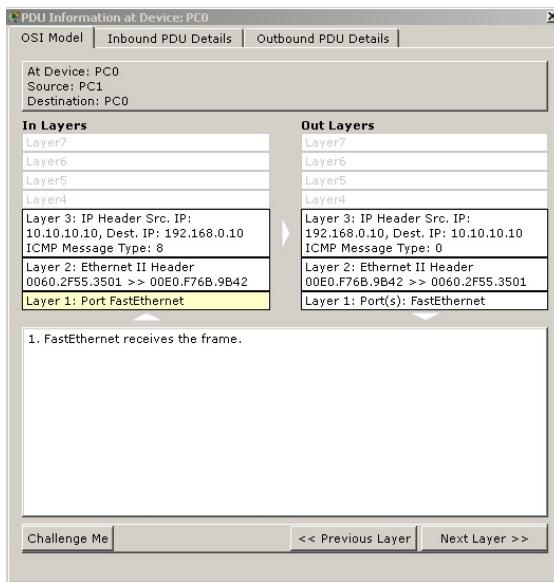


Abbildung 3.9: Ansicht der ICMP Nachricht im PC0

er nicht weiter beschrieben.

#### 3.3.3 Fazit

Der Versuch mit Packet Tracer hat eine klare Verbindung zu früheren Vorlesungen hergestellt. Die Sachverhalte wurden bereits theoretisch vermittelt. Die Theorie wurde aber während des Versuchs sehr anschaulich dargestellt und letzte Unklarheiten wurden ausgeräumt.

# 4 RSP Versuch

## 4.1 Einleitung

Im Versuch 3 haben wir die grundsätzliche Funktionsweise der Cisco Prompt kennen gelernt. In diesem Versuch wurde der Hostname konfiguriert und über Packet Tracer ein Netzwerk aufgebaut.

Da die Konfiguration im letzten Versuch noch nicht einmal die Oberfläche der Möglichkeiten angekratzt hat, möchten wir in diesem Versuch tiefer in die Konfiguration von Cisco Geräten einsteigen.

## 4.2 Aufbau des Versuchs

### 4.2.1 Benötigte Geräte

- Zwei Router
- Ein Switch
- Zwei PC mit Hyper Terminal
- Zwei Patchabel
- Ein Crossover Kabel
- Ein Serielles Kabel mit je einem DCE und einem DTE Anschluss

Der erste PC wird über ein serielles Kabel und über ein Patchkabel mit einem Switch verbunden. Der Zweite PC wird mit einem seriellen Kabel und einem Crossover Kabel mit dem Router 2 verbunden. Die seriellen Kabel dienen der Konfiguration der Geräte. Das Patchkabel und das Crossoverkabel sind für den Transport von Payload. Der Switch wird mit einem Patchkabel mit dem Router verbunden.

Die Router werden untereinander mit dem seriellen Kabel verbunden. Zu beachten ist hierbei, dass der Bustakt vom DCE (female) Port kommt. Der DTE (male) Port benötigt diesen Bustakt, damit eine Kommunikation möglich ist.

Die Router bekommen für ihre einzelnen Ports unterschiedliche IP Adressen:

Nachdem die Geräte verkabelt und gestartet sind, müssen noch die NVRAM der Geräte gelöscht werden. Dadurch kann sichergestellt werden, dass keine alten Konfigurationen mehr gespeichert sind. Diese könnten sonst im Laufe des Versuchs Fehler produzieren. Eine Ausgabe der Geräte wurde bereits im Versuch 3 dargestellt.

#### 4 RSP Versuch

Device	Hostname	Interface	IP-Address	Subnet Mask
R1	R1	Serial 0/0/0 (DCE)	172.17.0.1	255.255.0.0
		FE0/1 u. FE0/0	172.16.0.1	255.255.0.0
R2	R2	Serial 0/0/0 (DTE)	172.17.0.2	255.255.0.0
		FE0/0	172.18.0.1	255.255.0.0

Tabelle 4.1: Adresstabelle des Netzwerks

Device	IP-Address	Subnet Mask	Default Gateway
H1	????	255.255.0.0	172.17.0.1
H2	???	255.255.0.0	172.18.0.1

Tabelle 4.2: Einstellungen der Hosts

Bevor eine Kommunikation stattfinden kann, müssen erst noch die Hosts konfiguriert werden. Da im Netz kein DHCP Server läuft, müssen die Netzwerkeinstellungen der Hosts manuell vergeben werden.

### 4.3 Versuch

Im folgenden wird nicht mehr beschrieben, dass zum Ändern von Konfigurationen in einen Konfigurationsmodus, wie beispielsweise den „Global configuration“ Modus gewechselt werden muss.

#### 4.3.1 Konfigurieren der Router Basiseinstellungen

Der erste Schritt der Konfiguration ist das konfigurieren der Hostnamen. Diese können mit dem Befehl `hostname <Name>` konfiguriert werden. Der Router 1 bekommt den Hostname R1, der Router 2 den Hostname R2.

Nach dem Konfigurieren folgt das Setzen der Passwörter. Typische Zugriffspunkte für ein Cisco Gerät sind die Terminal Leitungen (auch Virtual Terminal Lines oder VTYs genannt), der Konsolen Port sowie der Hilfs Port (AUX). Die Terminal Leitungen sind über telnet oder ssh erreichbar und haben den Vorteil, dass kein Serielles Kabel benötigt wird. Die Nachteile einer solchen Konfiguration wurden im Versuch 3 erläutert. Die Zugänge müssen separat konfiguriert werden. Das Passwort des Konsolen Ports wird mit folgender Sequenz gesetzt:

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

Listing 4.1: Die Eingabe zum Setzen des Konsolen Port Passworts

### 4.3 Versuch

Nach dieser Sequenz wird für die Konfiguration über die Konsole ein Passwort benötigt. Dieses ist in dem Fall cisco. Der Router kann aber trotzdem ohne Passwort über eine Terminal Leitung konfiguriert werden. Um hierfür ein Passwort zu setzen ist folgende Sequenz nötig.

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

Listing 4.2: Die Eingabe zum Setzen des Terminal Passworts

Nach dieser Sequenz wird auch für das Konfigurieren über eine Terminal Leitung ein Passwort benötigt.

In IOS werden die Passwörter per default im Klartext gespeichert. Daraus ergibt sich ein Sicherheitsrisiko. Die Passwörter können von jedem, der Zugang zum Router hat, im Klartext ausgelesen werden. Aktuell sind auch nur die Zugänge passwortgeschützt. Sobald man eine Verbindung (VTY oder Konsole) zum Router hat, ist man automatisch berechtigt, den Router zu konfigurieren. Mit dem Befehl *enable password <Passwort>* wird sichergestellt, dass man auch ein Passwort braucht, wenn man in einen der Konfigurationsmodi will. Mit dem Befehl *enable secret <Passwort>* wird das Passwort verschlüsselt gespeichert.

```
R1(config)#enable password cisco
R1(config)#enable secret class
R1(config)#exit
```

Listing 4.3: Die Eingabe zum Aktivieren und Verschlüsseln des Passworts

Nach dieser Befehlssequenz ist ein Passwort zum Wechsel in den Konfigurationsmodus gesetzt, dieses ist auch verschlüsselt gespeichert.

Da jetzt Passwörter gesetzt sind macht es Sinn, dass Benutzer aufgefordert werden, diese einzugeben. Diese Aufforderung kann mit dem Befehl *banner motd <delimiter> message <delimiter>* konfiguriert werden. Die delimiter zeigen den Start und das Ende der Nachricht an. Sie dürfen nicht in der Nachricht genutzt werden und die Zeichen “ und % dürfen nicht genutzt werden. Ein Blank wird nicht funktionieren.

```
R1(config)#banner motd #Unauthorized Use Prohibited#
```

Listing 4.4: Setzen der Passwort Aufforderung

Router mit IOS sind standardmäßig so konfiguriert, dass sie versuchen, jedes Wort, das sie nicht kennen, in einem DNS Server mit der Broadcastadresse 255.255.255.255 aufzulösen. Eine Folge ist, dass bei einer falschen Befehlseingabe sehr lange Wartezeiten und eine unnötige Netzwerklast auftreten, weil der Router versucht die Zeichenfolge in eine IP Adresse aufzulösen. Durch

#### 4 RSP Versuch

```
R1(config)#no ip domain lookup
```

Listing 4.5: Deaktivieren des DNS im Terminal

wird dieses Verhalten abgestellt.

Der letzte Schritt der Basiseinstellung verhindert, dass Fehlermeldungen die aktuelle Eingabe in die Prompt unterbrechen.

```
R1(config)#line console 0
R1(config-line)#logging synchronous
```

Ob die Einstellungen korrekt waren, kann mit dem *show running-config* Befehl überprüft werden.

```
R1#show running-config
Building configuration...

Current configuration : 931 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$HQCF$50Cteo3yxGrpQwwSNdUIz.
enable password cisco
!
no aaa new-model
!
!
ip cef
!
!
no ip domain lookup
multilink bundle-name authenticated
!
!
!
archive
  log config
    hidekeys
!
!
!
```

### 4.3 Versuch

```
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 172.17.0.1 255.255.0.0
no fair-queue
clock rate 125000
!
interface Serial0/0/1
no ip address
shutdown
clock rate 125000
!
ip forward-protocol nd
!
!
ip http server
!
!
!
control-plane
!
banner motd #Unauthorized Use Prohibited#
!
line con 0
password cisco
logging synchronous
login
line aux 0
line vty 0 4
password cisco
login
!
scheduler allocate 20000 1000
!
end
```

Listing 4.6: Ausgabe der Config nach dem Konfigurieren der Basiseinstellungen

#### 4 RSP Versuch

An den Zeilen

```
hostname R1

enable secret 5 $1$HQCF$50Cteo3yxGrpQwwSNdUIz.
enable password cisco

no ip domain lookup

banner motd #Unauthorized Use Prohibited#

line con 0
password cisco
logging synchronous
login

line aux 0

line vty 0 4
password cisco
login
```

kann man erkennen, dass das Konfigurieren erfolgreich war. Und dass der Router weiterhin ohne Passwort über den Hilfs Port (AUX) erreicht werden kann. Eine Konfiguration wird aber über diesen Port nicht möglich sein.

Auffällig ist auch, dass sowohl das verschlüsselte, als auch das unverschlüsselte Passwort in der Ausgabe stehen. Diese Tasche wirft Fragen auf. Welches Passwort ist nun gültig? Und warum kann man überhaupt ein unverschlüsseltes Passwort eingeben? Die Antwort auf diese Fragen bringt die Homepage des Herstellers. Die erste Frage ist leicht beantwortet, das verschlüsselte Passwort wird bevorzugt, das heißt, dass man sich nur mit diesem anmelden kann. Die zweite Frage hat einen geschichtlichen Hintergrund. Wenn man eine alte Version von IOS bootet, oder veraltete boot ROM nutzt, kann es Probleme mit verschlüsselten Passwörtern geben. In diesem Fall sind unverschlüsselte Passwörter zu nutzen.

Um die Fragen der Versuchsbeschreibung zu beantworten:

- **s there an encrypted password?** Yes, the password to enter the config mode ist encrypted. The passphrase „class“ became „5 \$1\$HQCF\$50Cteo3yxGrpQwwSNdUIz.“. According to the cisco homepage ist the „5“ an indicator for an encrypted password.
- **Are there any other passwords?** Yes, there are the passwords for the configuration ports. And the decrypted password „cisco“.
- **Are any of the other passwords encrypted?** No, the other passwords are not encrypted. If you want to encrypt all of the passwords, you have to enter the command *service password-encryption*. If this service ist activated, all of the passwords will become encrypted.

### 4.3.2 Konfigurieren der seriellen Interfaces

Nachdem der Router für die Benutzung konfiguriert wurde und grundlegende Sicherheitsmaßnahmen ergriffen wurden, muss nun der Betrieb ermöglicht werden. Damit die Hosts mit den Routern und die Router untereinander kommunizieren können, müssen die Interfaces konfiguriert werden. Die Befehle

```
R1(config)#interface serial 0/0/0
R1(config-if)#description WAN link to R2
R1(config-if)#ip address 172.17.0.1 255.255.0.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
```

Listing 4.7: Konfigurieren des seriellen Interface

konfigurieren das serielle Interface.

Die ersten 3 Zeilen sind leicht verständlich. Dort wird bestimmt, welches Interface mit welcher IP und welchem Kommentar konfiguriert werden soll.

Der Befehl *no shutdown* aktiviert das Interface.

Nachdem diese Befehlssequenz eingegeben wurde, kann man sich mit dem Befehl *show interfaces serial 0/0/0* anzeigen lassen, ob die Konfiguration erfolgreich war:

```
R1#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
Hardware is GT96K Serial
Description: WAN link to R2
Internet address is 172.17.0.1/16
MTU 1500 bytes, BW 128 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:04, output 00:00:07, output hang never
Last clearing of "show interface" counters 00:24:04
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops
: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
167 packets input, 11406 bytes, 0 no buffer
Received 161 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
197 packets output, 13012 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 output buffer failures, 0 output buffers swapped out
1 carrier transitions
DCD=up  DSR=up  RTS=up  CTS=up
```

was zum  
Teufel  
ist die  
Clockrate?

## 4 RSP Versuch

Listing 4.8: Konfiguration des seriellen Interface

Um die eigenen Änderungen zu kontrollieren sind die Zeilen

```
Serial0/0/0 is up, line protocol is up
Hardware is GT96K Serial
Description: WAN link to R2
Internet address is 172.17.0.1/16

DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Fragen aus der Versuchsanleitung:

- **What did you discover by issuing the show interfaces command?**
  - Serial 0/0/0 status is up
  - Line protocol up
  - Internet address is 172.17.0.1/16
  - Encapsulation HDLC
- **To which OSI layer is the encapsulation referring?** HDLC is a bit-oriented synchronous data link layer protocol. So the encapsulation is referring to OSI Layer 2.
- **If the serial interface was configured, why did the show interfaces serial 0/0/0 indicate that the interface is down?**

Das ist  
doch  
konfi-  
guriert.  
Wat will  
der von  
Mir?

Da der Router 2 eine andere Ip Adresse vorgegeben hat, sieht hier die Konfiguration ein wenig anders:

```
R2(config)#interface serial 0/0/0
R2(config-if)#description WAN link to R1
R2(config-if)#ip address 172.17.0.2 255.255.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#exit
```

Listing 4.9: Die Einstellungen für das serielle Interface von R2

Nach dem Konfigurieren werden die Einstellungen überprüft:

```
Serial0/0/0 is up, line protocol is up
Hardware is GT96K Serial
Description: WAN link to R1
Internet address is 172.17.0.2/16
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

```

Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:02, output 00:00:09, output hang never
Last clearing of "show interface" counters 00:19:00
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops
: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
30 packets input, 1462 bytes, 0 no buffer
Received 30 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
19 packets output, 1607 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
3 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
10 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

```

Listing 4.10: show interfaces bei an R2

Analog zum Router 1 gibt es in der Versuchsbeschreibung auch Fragen zum Router 2:

- **What did you discover by issuing the show interfaces command?**
  - Serial 0/0/0 status is up
  - Line protocol is up
  - Internet address is 172.17.0.2/16
  - Encapsulation HDLC
- **To which OSI layer is the encapsulation referring?** See above
- **Why did the show interfaces serial 0/0/0 indicate that the interface is up?** The interface is physically connected to another device (R1). Additionally is is configured an with the command *no shutdown* enabled. If we started this test with R2, there was no connection, because R2 needs the clock of R1.

Laut den Einstellungen sind die Interfaces konfiguriert und arbeiten. Ob, alles korrekt funktioniert, kann einfach durch einen Ping getestet werden.

```

R1#ping 172.17.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.0.2, timeout is 2 seconds
:
!!!!!

```

#### 4 RSP Versuch

```
Success rate is 100 percent (5/5), round-trip min/avg/max =  
28/28/32 ms
```

Listing 4.11: Ping von R1 an das serielle Interface von R2

```
R2>ping 172.17.0.1  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.17.0.1, timeout is 2 seconds  
:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max =  
28/28/32 ms
```

Listing 4.12: Ping von R2 an das serielle Interface von R1

Beide Ping haben funktioniert, das bedeutet, dass die Interfaces korrekt konfiguriert wurden. Damit ist das Konfigurieren der seriellen Interfaces erfolgreich abgeschlossen.

#### 4.3.3 Konfigurieren der Fast Ethernet Interfaces

Das FE Interface 0/0 wird laut der Versuchsbeschreibung konfiguriert. Die folgende Befehlssequenz konfiguriert das Interface.

```
R1(config)#interface FastEthernet 0/0  
R1(config-if)#description R1 LAN Default Gateway  
R1(config-if)#ip address 172.16.0.1 255.255.0.0  
R1(config-if)#no shutdown  
R1(config-if)#exit  
R1(config)#exit
```

Listing 4.13: Die Befehle zum Konfigurieren des FE 0/0 Interface von R1

Die Befehle sind analog der mit denen die seriellen Interfaces konfiguriert werden. Der Unterschied ist, dass hier keine clock rate eingestellt werden muss. Die Einstellungen können wieder mit dem Befehl *show interfaces FastEthernet 0/0* überprüft werden:

```
R1#show interfaces FastEthernet 0/0  
FastEthernet0/0 is up, line protocol is up  
Hardware is MV96340 Ethernet, address is 0025.456d.c780 (bia  
0025.456d.c780)  
Description: R1 LAN Default Gateway  
Internet address is 172.16.0.1/16  
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Encapsulation ARPA, loopback not set  
Keepalive set (10 sec)  
Full-duplex, 100Mb/s, 100BaseTX/FX
```

### 4.3 Versuch

```
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:02, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops
    : 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
50 packets input, 29595 bytes
Received 50 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
93 packets output, 33415 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Listing 4.14: Anzeige der FE 0/0 Einstellungen von R1

In der Versuchsbeschreibung werden folgende Fragen gestellt:

- **What did you discover by issuing the show interfaces command?**
  - Fast Ethernet 0/0 status is up
  - Line protocol is up
  - Internet address is 172.16.0.1/16
  - Encapsulation ARPA
- **To which OSI layer is the encapsulation referring?** ARPA is the short form of „Advanced Research Projects Agency“, also called Ethernet 2 or DIX Ethernet. Ethernet 2 is a protocol of the Data Link Layer, or Layer 2.
- **Why did the show interfaces FastEthernet 0/0 command show that the interface is up?** The explanation is the same, like the serial Interfaces. Think of the physical to H1 an the configuration some lines before.

Laut den Einstellungen ist das FE 0/0 Interface von R1 nun korrekt konfiguriert. Im nächsten Schritt wird das FA 0/0 Interface von R2 konfiguriert. Hierfür sind diese Befehle nötig:

```
R2(config)#interface FastEthernet 0/0
R2(config-if)#description R2 LAN Default Gateway
R2(config-if)#ip address 172.18.0.1 255.255.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

#### 4 RSP Versuch

```
R2(config)#exit
```

Listing 4.15: Die Befehle zum Konfigurieren des FE 0/0 Interface von R2

Das Ergebnis dieser Befehle wird wieder kontrolliert:

```
R2#show interfaces
FastEthernet0/0 is up, line protocol is up
Hardware is MV96340 Ethernet, address is 58bc.2738.7c50 (bia 58bc
.2738.7c50)
Description: R2 LAN Default Gateway
Internet address is 172.18.0.1/16
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:02, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops
: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
50 packets input, 29595 bytes
Received 50 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
93 packets output, 33415 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
...
R2#
```

Listing 4.16: Anzeige der FE 0/0 Einstellungen von R2

Entweder  
Ausga-  
be fäken,  
oder tro-  
bleshoo-  
ting be-  
schreiben

In der Versuchsbeschreibung werden folgende Fragen gestellt:

- **What did you discover by issuing the show interfaces command?**
  - FastEthernet0/0 is up
  - Line protocol is up
  - Internet address is 172.18.0.1/16

### 4.3 Versuch

- Encapsulation ARPA
- To which OSI layer is the encapsulation referring? see above
- Why did the show interfaces FastEthernet 0/0 command show that the interface is up? see above

Um zu testen, ob die Konfiguration wirklich erfolgreich war, pingen wir wieder. Das Pingen auf die FA Interfaces ist am sinnvollsten, wenn es von den Hosts ausgeführt wird.

```
//Keine Ping Datei  
R2>
```

Listing 4.17: Ping von R1 an das serielle Interface von R2

```
//Keine Ping Datei
```

Listing 4.18: Ping von R2 an das serielle Interface von R1

Die Pings finde ich nicht.  
Evtl. müssen die mit nem Windows Rechner gefaket oder sonst wo abgeschrieben werden



## **5 SDH Versuch**

**5.1 Einleitung**

**5.2 Downlink**

**5.3 Uplink**

**5.4 ARFCN**

**5.5 Untersuchung des Paketflusses mit Wireshark**



# **6 RN Versuch**

**6.1 Einleitung**

**6.2 Downlink**

**6.3 Uplink**

**6.4 ARFCN**

**6.5 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](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](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](http://www.cisco.com/en/US/products-/ps5881/prod_view_selector.html).
- [6] Cisco Systems. *Introduction to Routers in WAN*. [http://www.cisco.com/web/learning/netacad/demos/CCNA2v3Demo/ch1/1\\_1\\_2/index.html](http://www.cisco.com/web/learning/netacad/demos/CCNA2v3Demo/ch1/1_1_2/index.html).



## **Kolophon**

Dieses Dokument wurde mit der L<sup>A</sup>T<sub>E</sub>X-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).