

**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

| | |
|---|-----------|
| Inhaltsverzeichnis | v |
| Listings | 1 |
| 1 GSM Versuch | 1 |
| 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 | 20 |
| 1.5.1 Versuchsaufbau | 20 |
| 1.5.2 Versuchsdurchführung | 20 |
| 2 BA Versuch | 23 |
| 2.1 Allgemeine Beschreibung des Versuchs | 23 |
| 2.2 Einrichten der Anlage | 23 |
| 2.2.1 Einrichten der Ports | 23 |
| 2.2.2 Einrichten der Routing Tabellen | 24 |
| 2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls | 25 |
| 2.3.1 Aufzeichnen des ISDN-D-Kanal Protokolls ?? | 25 |
| 2.3.2 Interpretieren des D-Kanal-Protokoll Mitschnitts | 25 |
| 3 RSP Versuch | 39 |
| 3.1 Einleitung | 39 |
| 3.1.1 Benötigte Hardware für den Versuch | 39 |
| 3.2 Der Umgang mit Physikalischen Geräten | 41 |
| 3.2.1 Einrichtung eines Switchs | 41 |
| 3.2.2 Konfiguration eines Routers | 43 |
| 3.2.3 Fazit des Versuchs | 55 |
| 3.3 Packet Tracer | 56 |
| 3.3.1 Aufbau des Netzwerkes | 56 |

| | | |
|----------|--|------------|
| 3.3.2 | Simulieren und Analysieren eines ECHO REQUEST/ECHO REPLY | 58 |
| 3.3.3 | Fazit | 62 |
| 4 | RSC Versuch | 63 |
| 4.1 | Einleitung | 63 |
| 4.2 | Aufbau des Versuchs | 63 |
| 4.2.1 | Benötigte Geräte | 63 |
| 4.3 | Versuch - Teil 1 | 64 |
| 4.3.1 | Konfigurieren der Router Basiseinstellungen | 64 |
| 4.3.2 | Konfigurieren der seriellen Interfaces | 69 |
| 4.3.3 | Konfigurieren der Fast Ethernet Interfaces | 72 |
| 4.4 | Versuch Teil 2 | 75 |
| 4.4.1 | Konfigurieren der Switch Ports | 80 |
| 4.4.2 | Port Security | 82 |
| 4.4.3 | Geschwindigkeits- und Duplexeinstellungen des Switchs | 85 |
| 4.4.4 | Reflection | 87 |
| 5 | SDH Versuch | 89 |
| 5.1 | Allgemeine Beschreibung der Versuche | 89 |
| 5.2 | Versuchsgegenstände im Detail | 90 |
| 5.2.1 | GN Elmi EST 2100 | 90 |
| 5.2.2 | TMNS | 94 |
| 5.3 | Fehlereinspeisung | 100 |
| 5.3.1 | Pointer | 102 |
| 5.4 | Fazit | 104 |
| 6 | RN Versuch | 107 |
| 6.1 | Einleitung | 107 |
| 6.2 | Downlink | 107 |
| 6.3 | Uplink | 107 |
| 6.4 | ARFCN | 107 |
| 6.5 | Untersuchung des Paketflusses mit Wireshark | 107 |
| | Literatur | 109 |

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.

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 |

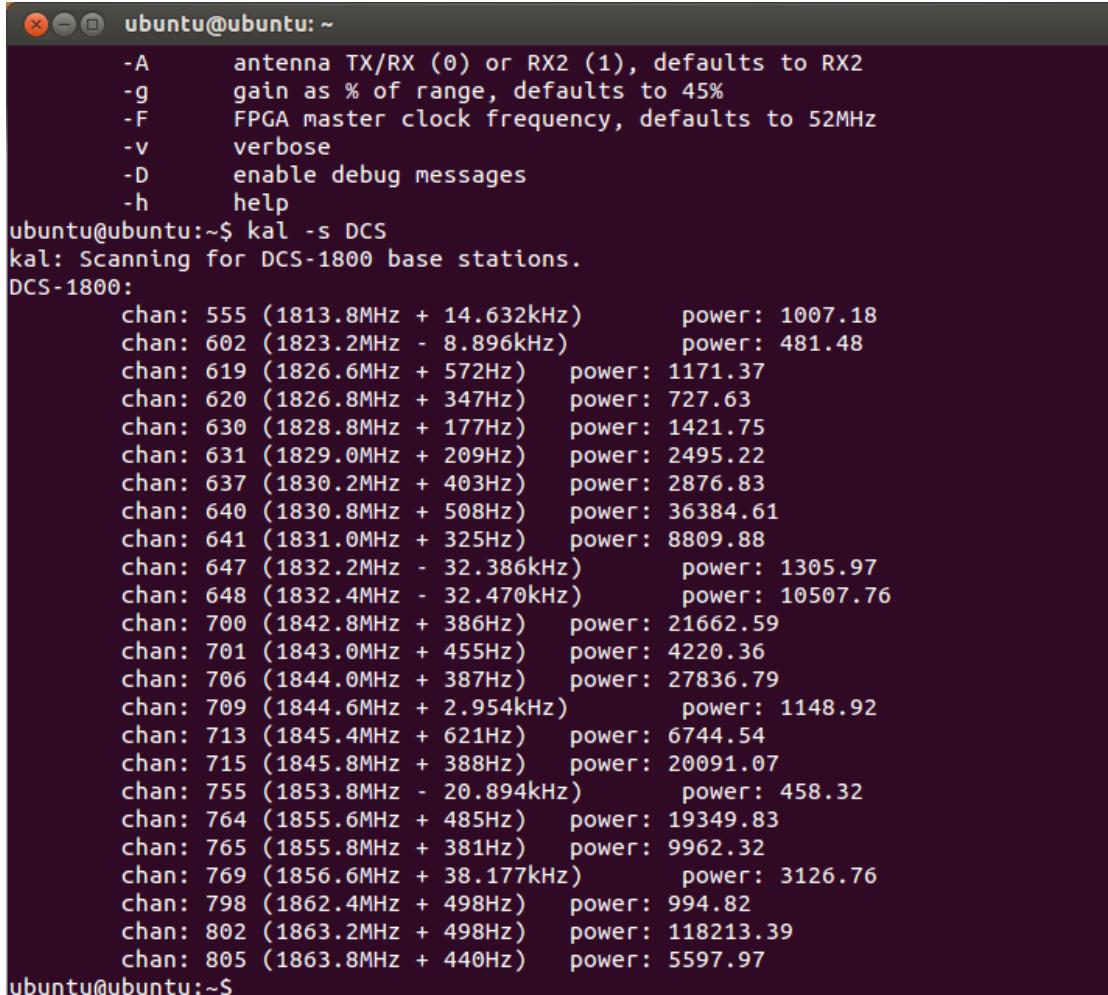
Tabelle 1.1: Auflistung der empfangenen Frequenzen

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

power Power ist die Stärke, mit der das Signal empfangen wurde. Für unseren Versuch nehmen wir die stärkeren Signale da siech diese besser Visualisieren lassen. Leider ist die Dokumentation zu *kal* sehr spärlich ausgefallen und es bleibt im verborgenen was für eine Einheit diese Spalte ausdrückt. Fest steht, das Werte jenseits der 900er Marke ein starkes Signal darstellen.

Berechnung der Frequenzen Wie schon erwähnt, anhand dieser Auflistung ist es möglich, den Frequenzbereichs von DCS 1800 zu errechnen. Zur Berechnung eines Fre-

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

quenzbereichs gibt es einige Formeln. Welche genutzt wird, hängt davon ab, welche Werte bereits bekannt sind.

| |
|---|
| 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 wer-

1 GSM Versuch

den. In der Tabelle 1.2 werden die Zusammenhänge von Up- und Downlink klar. Die Startfrequenz ist ein festdefinierter Wert von 1710,2 Mhz. Die zu GSM 1800 gehörenden Channels sind von 512 bis 885 definiert, daher auch der feste Offset von 512. Der Abstand ist wie bereits erwähnt, zwischen der Up- und der Downlinkfrequenz gemeint. Dieser hat den Wert 95Mhz. Mit Hilfe dieser Werte lassen sich also ganz leicht der ARF-CN von einer Frequenz berechnen bzw auch die Down- oder Uplinkfrequenz zu einem passenden Channel.

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

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

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

- Militär
- T-Mobile
- O2
- Vodafone
- e-plus

Abbildung 1.3: Frequenztabelle der Provider [1]

Wenn man die Tabelle 1.1 und die Grafik 1.3 vergleicht, ergibt sich Tabelle 1.3. Aufällig 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

1.2 Visualisieren von Frequenzen

| | | |
|-------|--------------------|----------------|
| chan: | 555 1813.8 MHz | Militär |
| chan: | 602 1823.2MHz | T-Mobile |
| chan: | 619 1826.6MHz | O ₂ |
| chan: | 620 1826.8 + 347Hz | O ₂ |
| chan: | 630 1828.8MHz | O ₂ |
| chan: | 631 1820.0MHz | Militär |
| chan: | 637 1830.2MHz | O ₂ |
| chan: | 640 1830.8MHz | O ₂ |
| chan: | 641 1831.0MHz | O ₂ |
| chan: | 647 1832.2MHz | O ₂ |
| chan: | 648 1832.4MHz | O ₂ |
| chan: | 700 1842.8MHz | O ₂ |
| chan: | 701 1843.0MHz | O ₂ |
| chan: | 706 1844.0MHz | O ₂ |
| chan: | 709 1844.6MHz | O ₂ |
| chan: | 713 1845.4MHz | O ₂ |
| chan: | 715 1845.8MHz | O ₂ |
| chan: | 755 1853.8MHz | E-Plus |
| chan: | 764 1855.6MHz | E-Plus |
| chan: | 765 1855.8MHz | E-Plus |
| chan: | 769 1856.6MHz | E-Plus |
| chan: | 798 1862.4MHz | E-Plus |
| chan: | 802 1863.2MHz | E-Plus |
| chan: | 805 1863.8MHz | E-Plus |

Tabelle 1.3: Auflistung der empfangenen Frequenzen

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

1 GSM Versuch

gesendeten Frequenz durchgeführt wird. Nachdem eine Frequenz gefunden wurde, beginnt der eigentliche Versuch mit dem Kommando `dbusrp-f 699219`. Dieses Kommando startet ein Analysetool, das sowohl den Frequenz- als auch den Amplitudenhochreichtum 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 Signals erinnert stark an weißes Rauschen

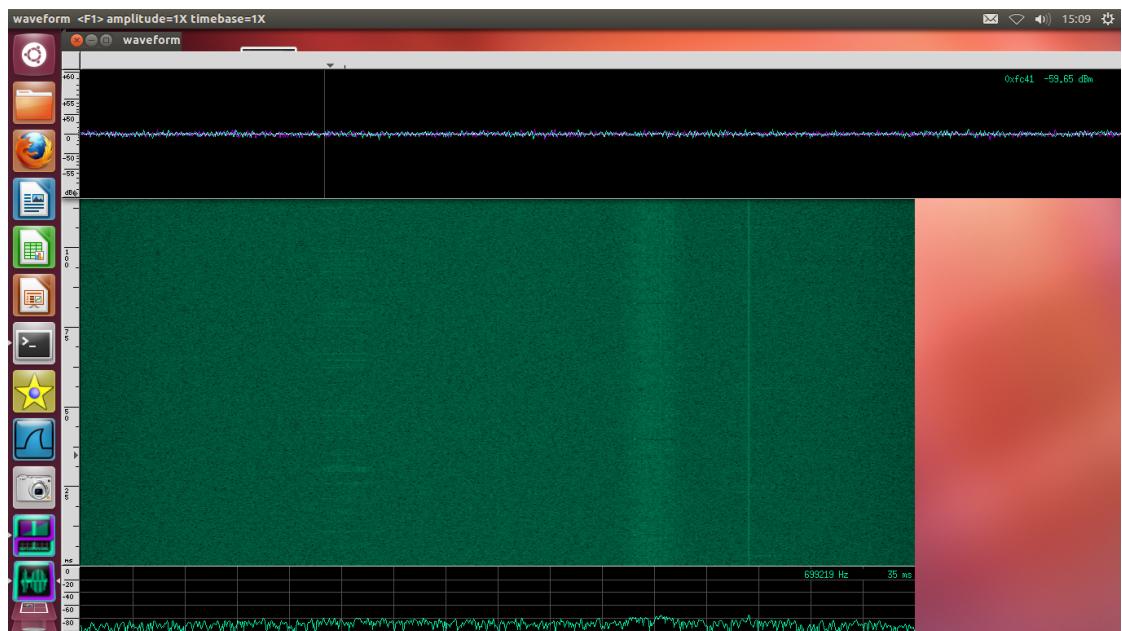


Abbildung 1.4: Eine visualisierte Frequenz

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

1.4 Datenmitschnitte

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

1 GSM Versuch

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 umrelevanten Daten herausgefiltert werden können und damit die doch sehr umfangreiche Datenmenge reduziert werden kann.

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

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

1.4.1.3 Auswertung des Versuchs

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

Mit geschnittenen werden die Daten die über das U_m Interface gesendet werden. Das U_m Interface ist eine Funkschnittstelle die für die Übertragung zwischen der Mobile-Station und dem Base Transceiver Station zuständig ist. Das U_m 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 U_m 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 nähere Informationen zur Signalstärke angegeben.

1.4 Datenmitschnitte

```

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

```

Abbildung 1.5: GSMTAP-Header

Unser Hauptaugenmerk legen wir auf die Pakete die als SIP gekennzeichnet sind. Hier kann man am besten nachverfolgen was gerade für eine Aktion durchgeführt wird. Da als erstes eine Verbindung aufgebaut werden muss damit man mit dem Echo-Server interagieren kann wird zuerst eine Invite Nachricht gesendet.

Bevor das jedoch passiert wird vorher auf dem Layer 2 eine Setup Nachricht gesendet. Wie man in 1.6 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-T/F DTAP - Setup
  Protocol Discriminator: call control; call related ss messages
  .... 0011 = Protocol discriminator: call control; call related ss messages (0x03)
  0... .... = TI Flag: allocated by sender
  ... .... = Sequence number: 1
  ..00 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: 0x04
  Length: 6
  Octet 3
  Octets 3a - Speech Versions
  Call Party BCD Number - (2600)
  Element ID: 0x98
  Length: 3
  1... .... = extension: no Extension
  ...0000 = Type of number: unknown (0x00)
  ...0001 = Home/roaming plan identification: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
  BCD digits: 2600
  Call control Capabilities
  Element ID: 0x15
  Length: 2
  0000 .... = 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 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 1.8 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=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
        SIP to address User Part: 2600
        SIP to address Host Part: 127.0.0.1
      Call-ID: 1246277820@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=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>;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 ist 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 ([1.12](#). 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 [1.11](#).

1 GSM Versuch

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

Abbildung 1.11: Aufforderung zum Beenden der Layer 2 verbindung

1.4 Datenmitschnitte

```
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.

1 GSM Versuch

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

Abbildung 1.13: Antwort auf die Aufforderung

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

1.4 Datenmitschnitte

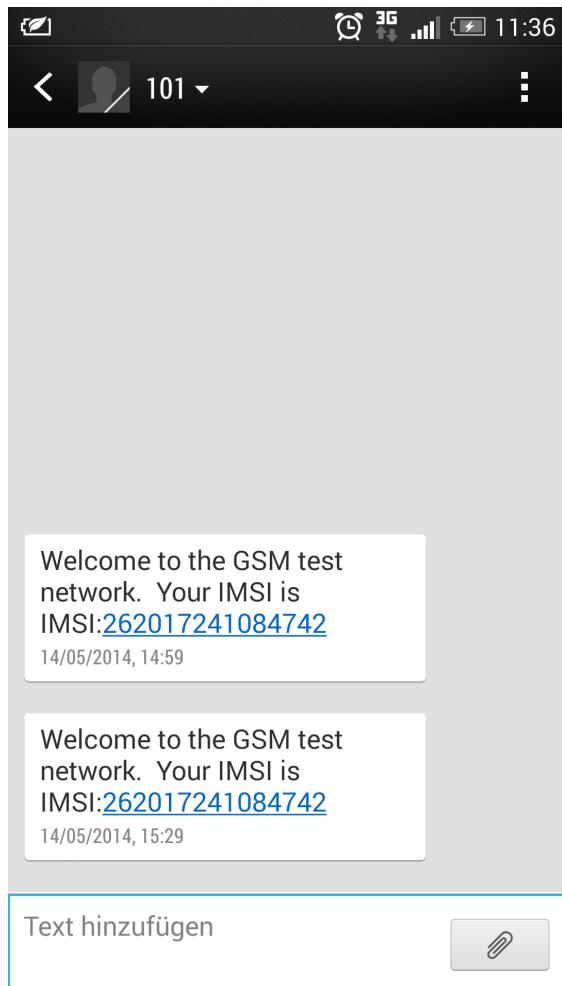


Abbildung 1.14: Quittierung der Einwahl in das GSM Netz

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

1 GSM Versuch

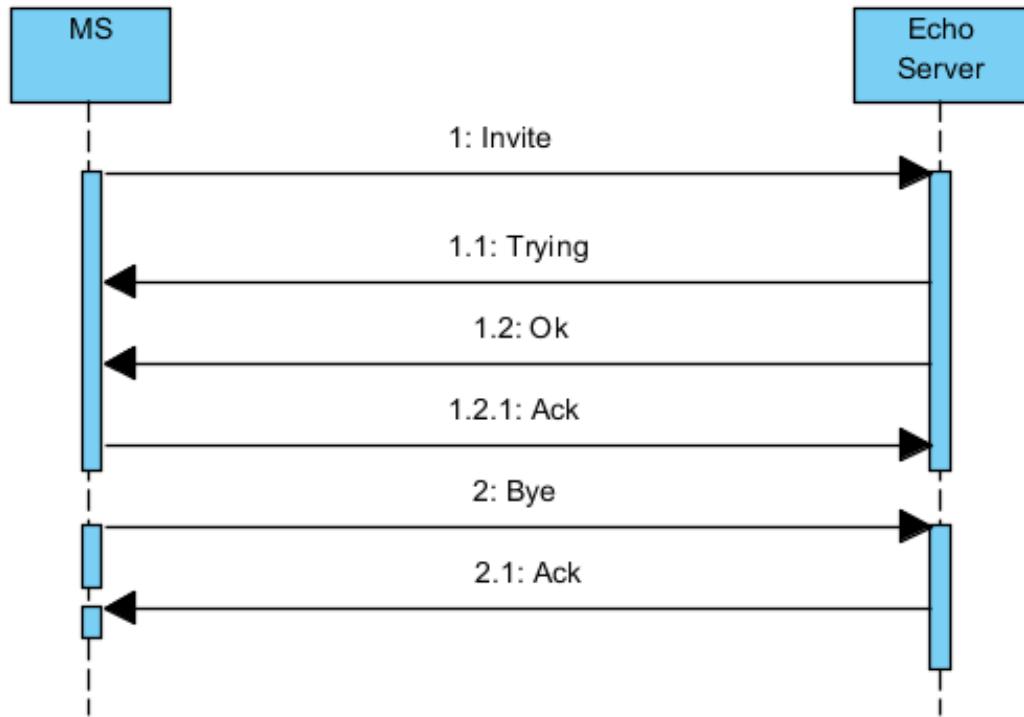


Abbildung 1.15: Ablauf SIP

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.

```

# interface eth0:0 up on wire (64 bits), 0 bytes captured (0 bytes)
# 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)
# ICMPv4 Destination Unreachable, Src Port: 60956 (60956), Dst Port: gsmmap (4729)
# GSM TAP Header, ARFCN: 840 (Downlink), TS: 0, Channel: S0CH/4 (1)

Version: 2
Header length: 16 bytes
Payload length: GSM UM (MS->BTS) (1)
Time Slot: 0
.. .000 001 0100 1000 = ARFCN: 840
.. ..000 0000 0000 0001 = Uplink: 0
Signal/Noise Ratio: 0
Signal Level (dBm): 0
GSM Frame Number: 2457308
Channel Type: S0CH/4 (7)
Antenna Number: 0
Sub-Slot: 0

# L1/H Access Procedure, channel DM (LAPDR)
# Address Field: Ox00
# ..0000... = LBD: Normal GSM (0)
# ..0011... = SAP1: SMS/SS (3)
# ...11... = EAI: Final octet (1)
# Control field: I, (N(R)=0, N(S)=5 (0x0A)
# Length Field: Ox15
# [4] Message Contents (102 bytes): #356(20), #361(20), #364(20), #370(20), #374(20), #379(2)
# GSM A-1/T DTAP - CP-DATA
# GSM A-1/F RP-DATA (Network to MS)
# RP-Message Reference
# RP-Originination Address - (0000)
# RP-Destination Address
# RP-User Data
# GSM SMS-TRU (GSM 03.40) SMS-DELIVER
0..... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
0..... = TP-UDHI: TP UDHI field contains only the short message
0...0 = TP-PID: A short message shall not be returned to the SME
0...0 = TP-PMS: More messages are waiting for the MS in this SC
0...0 = TP-WMTI: SMS-DELIVER (0)
# RP-Destination-Address - (411)
# TP-PID: 0
# TP-DSCS: 0
# TP-Service-Center-Name: ScS-Scmp
# TP-User-Data: Month 08, Day 21
# Hour 12, Minutes 58, Seconds 44
# Timezone: GMT + 2 hours 0 minutes
TP-User-Data-Length: (86) depends on Data-Coding-Scheme
# TP-User-Data
#MS text: I queued, cell 0.1.1MS1001011832121286, phonenum 10001000, at Aug 21 12:58:44, 'High'

# interface eth0:0 up on wire (64 bits), 0 bytes captured (0 bytes)
# 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)
# ICMPv4 Destination Unreachable, Src Port: 60956 (60956), Dst Port: gsmmap (4729)
# GSM TAP Header, ARFCN: 840 (Uplink), TS: 0, Channel: S0CH/4 (0)

Version: 2
Header length: 16 bytes
Payload length: GSM UM (MS->BTS) (1)
Time Slot: 0
.. .000 001 0100 1000 = ARFCN: 840
.. ..000 0000 0000 0001 = Uplink: 1
Signal/Noise Ratio (dB): 0
Signal Level (dBm): 0
GSM Frame Number: 2456044
Channel Type: S0CH/4 (7)
Antenna Number: 0
Sub-Slot: 0

# L1/H Access Procedure, channel DM (LAPDR)
# Address Field: Ox0d
# Control Field: I, N(R)=0, N(S)=5 (0x02)
# Length Field: Ox15
# [4] Message Contents (35 bytes): #264(20), #268(5)
# GSM A-1/T DTAP - CP-DATA
# Protocol Discriminator: SMS messages
....1001... = protocol discriminator: SMS messages (0x009)
....0000... = TP-PI: TP message allocated by sender
....011... = TOT: 3
DTAP SMS-TRU Message Service Message Type: CP-DATA (0x01)
# GSM A-1/F RP-DATA (MS to Network)
# Message Type RP-DATA (MS to Network)
# RP-Message Reference
# RP-Originating Address: (0000)
# RP-Destination Address
# RP-User Data
# GSM SMS-TRU (GSM 03.40) SMS-SUBMIT
0..... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
0..... = TP-UDHI: The TP UDHI field contains only the short message
0...0 = TP-PID: The TP PID field is not required
0...0 = TP-VPI: TP-VPI field present - relative format (2)
0...0 = TP-RD: Instruct SC to accept duplicates
....01 = TP-MTDL: SMS-SUBMIT (1)
# TP-User-Data
# TP-Destination-Address - (411)
# TP-PID: 0
# TP-DSCS: 0
# TP-Service-Center-Period: 63 week(s)
# TP-User-Data-Length: (4) depends on Data-Coding-Scheme
# TP-User-Data
#MS text: high

```

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 |
| 560 | 71.656441 | 127.0.0.1 | 127.0.0.1 | SIP | 328 Status: 200 OK |

Abbildung 1.17: SIP Abfolge des Sendens

2 BA Versuch

2.1 Allgemeine Beschreibung des Versuchs

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

2.2 Einrichten der Anlage

2.2.1 Einrichten der Ports

2.2.1.1 Aufbau des Versuchs

Als Switch steht ein Patapsco Liberator S zur Verfügung. Der Switch übernimmt die Funktionen des Netzes. Dazu gehören die TEI Vergabe, das Routing von Gesprächen und die Vergabe von Telefonnummern. Auf der Hardwareebene verbindet der Liberator die Telefone.

Zusätzlich steht ein EyeSDN Gerät. Dieses ermöglicht die Verbindung des Computers mit dem ISDN Netz und damit den Mittschnitt der Daten.

Zur Telefonie stehen zwei Telefone zur Verfügung und zum Konfigurieren des Systems ein Computer. Die Stromversorgung der Telefone wird vom Liberator eingespeist.

2.2.1.2 Versuchsdurchführung

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

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

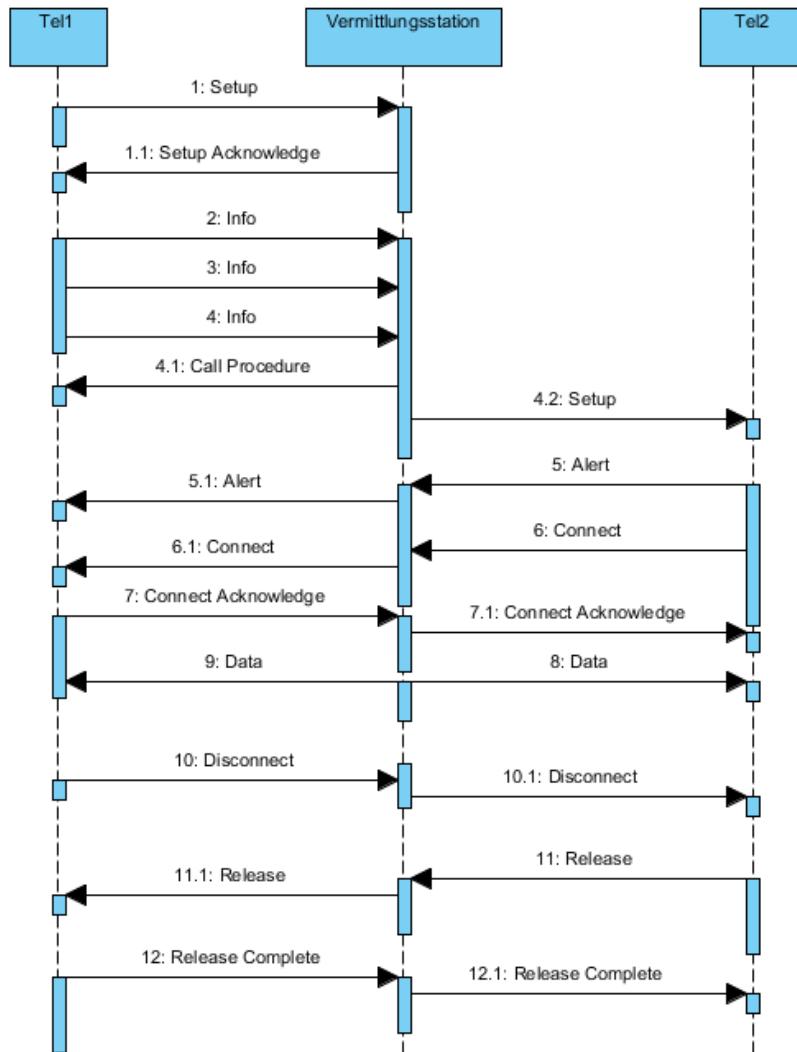


Abbildung 2.2: Aufbau und Abbau einer ISDN Verbindung

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

1. Welche Rahmen dienen der TEI-Vergabe, und welcher TEI-Wert wird dem Telefon von der Vermittlung zugewiesen?

Die Tei vergabe wird über das Protocol TEI mit der info Itenty Request behandelt. Diese fordert einen TEI Wert zur indentifizierung des Endgerätes an.

2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

| No. | Time | Source | Destination | Protocol Info |
|-----|-------------|--------|-------------|------------------|
| | | | Network | TEI |
| 13 | 3601.022936 | User | | 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

Abbildung 2.3: Identity Request Frame

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 | | | | |

Abbildung 2.4: Identity Assigned Frame

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

Abbildung 2.5: SABME Nachricht

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)
        .01 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)

```

Abbildung 2.6: Setup Nachricht

2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

4. Welche Kodierung des Sprachkanals wird gewählt?

Wie man auf dem nachfolgenden Bild in Grau hinterlegt erkennen kann wird der TU-T Standardized-Coding verwendet. Diese Richtlinie gilt für das digitalisierten analoger Audiosignale mittels Puls-Code-Modulation. Der Einsatzbereich für dieses Codecs ist wie zu erwarten in der klassischen sowie in der IP-Telefonie.

```
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 A-law (0x03)
    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 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: 100
    High-layer compatibility
        Information element: High-layer compatibility
        Length: 2
        .00. .... = Coding standard: ITU-T standardized coding (0x00)
    High layer characteristics identification: Telephony
```

Abbildung 2.7: Verwendete Codecs

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   CONNECT

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
```

Abbildung 2.8: Connect Nachricht

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

Die Schicht 3 ist Aufgebaut sobald das Netzwerk dem User eine Setup-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

2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

```
No.    Time        Source          Destination       Protocol Info
 397 6157.998584 Network        User            Q.931   SETUP ACKNOWLEDGE

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: 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)=5, N(S)=2 (0x0A04)
    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 (0x0d)
  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 acceptable
    .... 0... = D-channel indicator: False
    .... .01 = Information channel selection: B1 channel (0x01)
```

Abbildung 2.9: Setup Acknowledge

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 PROCEEDING |
| 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: <code>isdn:lapd:q931</code>] | | | | |
| 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 acceptable | | | | |
| 0.. = D-channel indicator: False | | | | |
|01 = Information channel selection: B1 channel (0x01) | | | | |

Abbildung 2.10: Call Proceeding Nachricht

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.

2.3 Aufzeichnungen und Interpretationen des ISDN-D-Kanal Protokolls

| No. | Time | Source | Destination | Protocol Info |
|---|-------------|--------|-------------|-------------------|
| 247 | 5803.908536 | User | Network | Q.931 INFORMATION |
| 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 INFORMATION |
| 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 INFORMATION |
| 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 | | | | |

Abbildung 2.11: Informations Rahmen

9. **Mit welchem Rahmen bestätigt die Vermittlung die Vollständigkeit der Rufnummer und beginnt 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?**

2 BA Versuch

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

```
No.      Time          Source           Destination        Protocol Info
255 5805.294552 Network          User              Q.931    ALERTING

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: 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)=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)
```

Abbildung 2.12: Alert Frame

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 COMPLETE |

```

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)

```

Abbildung 2.13: Realease Complete Frame

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 Signialisierung 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 überliefer werden. Dieser Vorgang ist durch den Versuch gut nachvollziehbar. Im Gegensatz 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 mit der Nummer 200 angerufen. Der Frame wurde aufgrund der Größe etwas zugeschnitten, er enthält jedoch alle wichtigen Informationen.

2 BA Versuch

| 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 (0x03) | | | | |
| 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 | | | | |

Abbildung 2.14: Setup Nachricht mit vollständiger Rufnummer

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.

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.

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></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.

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.

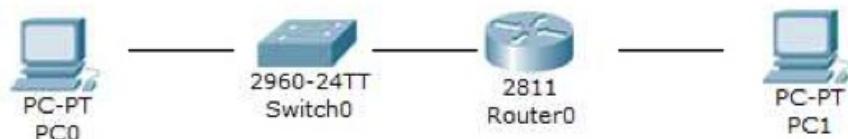


Abbildung 3.3: Der Aufbau des virtuellen Netzwerks

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

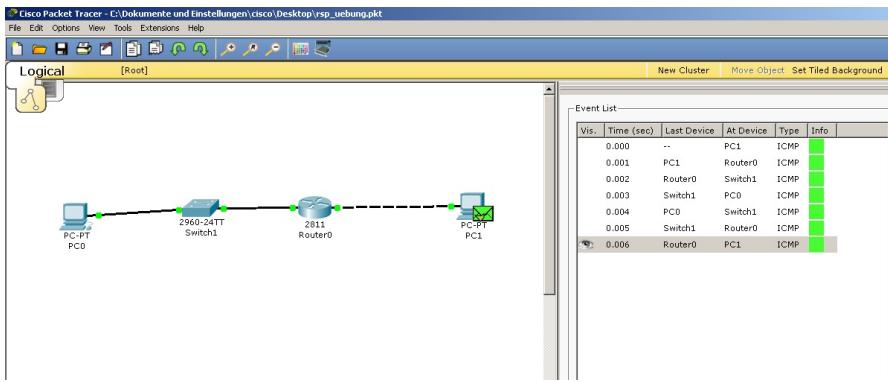


Abbildung 3.4: Der Beginn des echo request

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.

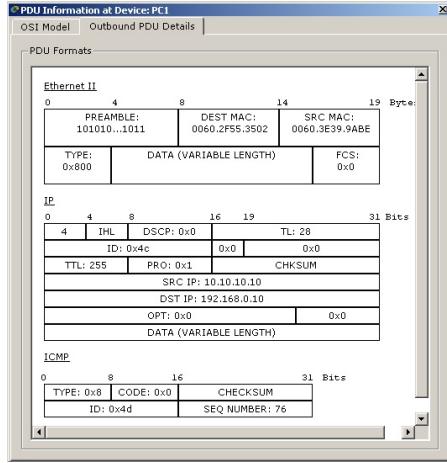


Abbildung 3.5: Detailansicht der ICMP Nachricht in PC1

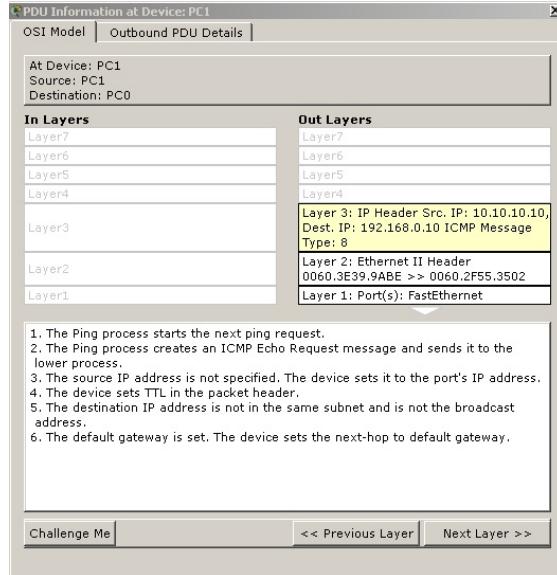


Abbildung 3.6: Ansicht der ICMP Nachricht in PC1

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

3.3 Packet Tracer

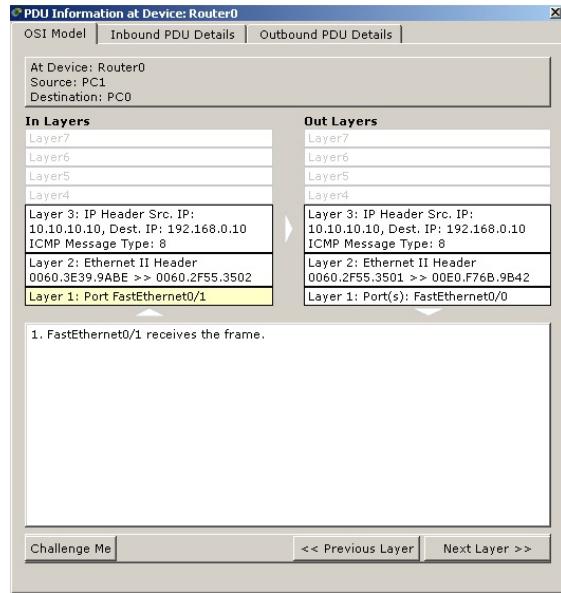


Abbildung 3.7: Ansicht der ICMP Nachricht im Router

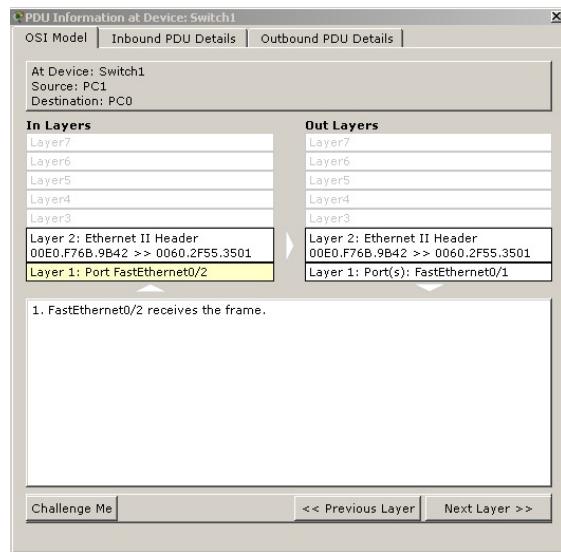


Abbildung 3.8: Ansicht der ICMP Nachricht im Switch

3 RSP Versuch

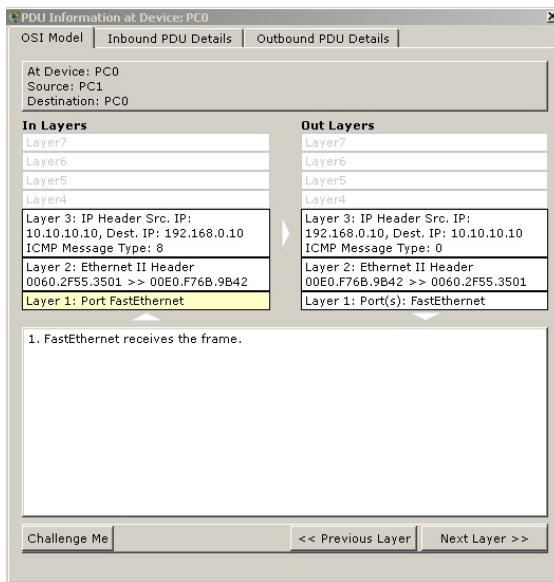


Abbildung 3.9: Ansicht der ICMP Nachricht im PC0

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 RSC 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 RSC 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 - Teil 1

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 - Teil 1

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 RSC 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
!
!
!
```

```

!
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 RSC 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
Clockra-
te?

4 RSC 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 RSC 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 - Teil 1

```
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 RSC 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

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
 - 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

4.4 Versuch Teil 2

Für den zweiten Teil des Versuchs muss der Aufbau geändert. Die Geräte entsprechen grundsätzlich Teil 1 des Versuchs, es wird lediglich nur noch ein Router benötigt. Die beiden Hosts werden mit dem Switch verbunden, der Host H1 hat eine serielle Verbindung zum Switch. Vor Beginn des Versuchs wird sichergestellt, dass die Konfigurationen von Router und Switch zurückgesetzt sind. Ist das nicht der Fall können unerwartete Ergebnisse auftreten.

| Dev | Hostname | IF | IP-Address | SN Mask | Def GW | Switch IP |
|-----|----------------|--------|-------------|---------------|-------------|-----------|
| S1 | CustomerSwitch | VLAN 1 | 192.168.1.5 | 255.255.255.0 | 192.168.1.1 | N/A |
| R1 | CustomerRouter | Fa0/1 | 192.168.1.1 | 255.255.255.0 | N/A | Fa0/5 |
| H1 | H1 | NIC | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | Fa0/11 |
| H2 | H2 | NIC | 192.168.1.4 | 255.255.255.0 | 192.168.1.1 | Fa0/18 |
| H3 | H3 | NIC | 192.168.1.6 | 255.255.255.0 | 192.168.1.1 | None |

Tabelle 4.3: Übersicht der Netzwerkadressen

Die Hosts werden nach der Adresstabelle konfiguriert. Im Router werden die Grund-einstellungen konfiguriert, das Interface Fa0/1 wird nach der Tabelle konfiguriert. Nachdem die Vorbereitungen abgeschlossen sind, wird der Switch konfiguriert. Die grundsätzliche Konfiguration entspricht der Konfiguration von Routern.

```
Switch(config)#hostname CustomerSwitch
```

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

Wie soll ein Router ohne serielle Kabel zurück gesetzt werden?
Evtl. anmerken, dass da doch ein serielle Kabel dran hängt

4 RSC Versuch

```
CustomerSwitch(config)#enable password cisco
CustomerSwitch(config)#enable secret cisco123
CustomerSwitch(config)#line console 0
CustomerSwitch(config-line)#password cisco123
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#line vty 0 15
CustomerSwitch(config-line)#password cisco123
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#end
```

Listing 4.19: Die Befehle zum Konfigurieren des Switches

Die Auswirkungen dieser Befehle sind im Teil 1 des Versuchs beschrieben. Jetzt folgen die Einstellungen zum Interface. Bei diesen Einstellungen wird ein v-Lan konfiguriert. Ein v-Lan ist ein logisches Teilnetz innerhalb eines Netzwerks. Bei Cisco Geräten ist das VLAN1 auf allen Ports per default konfiguriert. Der Befehl

```
CustomerSwitch(config)#interface vlan 1
```

Stimmt
das so?

konfiguriert dieses Interface. Damit werden alle Ports konfiguriert. Dieses Interface wird mit den Befehlen

```
CustomerSwitch(config-if)#ip address 192.168.1.5 255.255.255.0
CustomerSwitch(config-if)#no shutdown
CustomerSwitch(config-if)#exit
CustomerSwitch(config)#ip default-gateway 192.168.1.1
CustomerSwitch(config)#end
```

Listing 4.20: Die Befehle zum Konfigurieren des VLAN1 Interfaces

konfiguriert. Um zu überprüfen, ob die Konfiguration erfolgreich war, bietet sich der Befehl *show running-configuration* an. An der Ausgabe

```
CustomSwitch#show run
Building configuration...

Current configuration : 1418 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname CustomSwitch
!
enable secret 5 $1$BRz6$AhGrgo3ovcz9Px5pGe75p.
enable password cisco
!
no aaa new-model
```

```
system mtu routing 1500
ip subnet-zero
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
```

4 RSC Versuch

```
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
    ip address 192.168.1.5 255.255.255.0
    no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
!
control-plane
!
!
line con 0
    password cisco123
    login
line vty 0 4
    password cisco123
    login
line vty 5 15
    password cisco123
    login
!
end
```

Listing 4.21: Die Ausgabe der running configuration nach dem Konfigurieren des VLAN1 Interfaces

sieht man, dass die Konfiguration erfolgreich war. Die IP der Hosts und die IP des Interface befinden sich im gleichen Netzwerk. Um die Konfiguration dauerhaft im NVRAM zu sichern, muss noch die running-config in die startup-config kopiert werden.

```
CustomerSwitch#copy running-config startup-config
```

Laut der Ausgabe der Konfiguration scheint alles korrekt konfiguriert zu sein. Um zu testen, ob alles wirklich korrekt konfiguriert und angeschlossen ist, bieten sich einige Pings und eine Verbindung via Telnet an.

4.4 Versuch Teil 2

```
CustomSwitch#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/202/1007 ms
CustomSwitch#
```

Listing 4.22: Das Ergebnis des Pings von Switch zu Router

```
//Dafür noch ne Ausgabe "suchen"
```

Listing 4.23: Das Ergebnis des Pings von H1 zu Switch

Wird eine telnet Sitzung auf das Switch Management VLAN1 gestartet, ergibt sich folgendes Ergebnis:

```
CustomSwitch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(35)SE5, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 19-Jul-07 20:06 by nachen
Image text-base: 0x00003000, data-base: 0x00D40000

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE6,
RELEASE SOFTWARE
RE (fc1)

CustomSwitch uptime is 2 hours, 49 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-35.SE5/c2960-
lanbase-mz.122-35.
SE5.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision F0) with
61440K/4088K bytes of memory.
Processor board ID FOC1310W4F8
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
```

Keine Ahnung, welches Ergebnis

4 RSC Versuch

```

Base ethernet MAC Address      : 00:24:F9:8A:E7:00
Motherboard assembly number   : 73-11473-05
Power supply part number     : 341-0097-02
Motherboard serial number    : FOC131016QE
Power supply serial number   : AZS130807AL
Model revision number        : F0
Motherboard revision number  : A0
Model number                 : WS-C2960-24TT-L
System serial number         : FOC1310W4F8
Top Assembly Part Number    : 800-29859-02
Top Assembly Revision Number: A0
Version ID                  : V05
CLEI Code Number             : COM3L00BRD
Hardware Board Revision Number: 0x01

Switch  Ports  Model           SW Version      SW
Image
-----
*      1      26    WS-C2960-24TT-L    12.2(35)SE5  C2960-
          LANBASE -M

Configuration register is 0xF

```

Listing 4.24: Die Ausgabe von show version über Telnet

Dieser Switch nutzt das IOS Release „Version 12.2(35)SE5, RELEA“.

4.4.1 Konfigurieren der Switch Ports

Die Mac
Adresse
für Host
3 muss
noch "ge-
sucht"werden

In der Versuchsbeschreibung wird gefragt, welche Mac Adressen die Hosts haben.

| Device | Layer 2 Address |
|--------|-----------------|
| H1 | 1cc1.de5f.b7b3 |
| H2 | 1cc1.de5f.b9fa |
| H3 | |

Tabelle 4.4: Übersicht der Netzwerkadressen

Diese Mac Adressen können mit der mac address table des Switches verglichen werden.
Diese Tabelle kann man sich mit dem Befehl *show mac-address-table* ausgeben lassen.

```

CustomSwitch#sh mac-address-table
      Mac Address Table
-----
```

4.4 Versuch Teil 2

| Vlan | Mac Address | Type | Ports |
|--|----------------|---------|--------|
| All | 0100.0ccc.cccc | STATIC | CPU |
| All | 0100.0ccc.cccd | STATIC | CPU |
| All | 0180.c200.0000 | STATIC | CPU |
| All | 0180.c200.0001 | STATIC | CPU |
| All | 0180.c200.0002 | STATIC | CPU |
| All | 0180.c200.0003 | STATIC | CPU |
| All | 0180.c200.0004 | STATIC | CPU |
| All | 0180.c200.0005 | STATIC | CPU |
| All | 0180.c200.0006 | STATIC | CPU |
| All | 0180.c200.0007 | STATIC | CPU |
| All | 0180.c200.0008 | STATIC | CPU |
| All | 0180.c200.0009 | STATIC | CPU |
| All | 0180.c200.000a | STATIC | CPU |
| All | 0180.c200.000b | STATIC | CPU |
| All | 0180.c200.000c | STATIC | CPU |
| All | 0180.c200.000d | STATIC | CPU |
| All | 0180.c200.000e | STATIC | CPU |
| All | 0180.c200.000f | STATIC | CPU |
| All | 0180.c200.0010 | STATIC | CPU |
| All | ffff.ffff.ffff | STATIC | CPU |
| 1 | 0025.456d.c781 | DYNAMIC | Fa0/5 |
| 1 | 1cc1.de5f.b7b3 | DYNAMIC | Fa0/11 |
| 1 | 1cc1.de5f.b9fa | DYNAMIC | Fa0/18 |
| Total Mac Addresses for this criterion: 23 | | | |

Listing 4.25: Die Mac Adress Tabelle des Switches

Diese Liste enthält drei dynamische Mac Adressen. Diese Mac Adressen können H1, H2 und dem Router zugeordnet werden. Mit dem Befehl

```
mac address-table static 1cc1.de5f.b9fa interface fastethernet  
0/18 vlan 1
```

kann die Adresse von H2 fest an diesen Port vergeben werden. Dieser Eintrag kann mit dem Befehl *sh mac-address-table* überprüft werden.

| CustomSwitch#show mac-address-table | | | |
|-------------------------------------|----------------|---------|--------|
| Mac Address Table | | | |
| Vlan | Mac Address | Type | Ports |
| [...] | | | |
| All | ffff.ffff.ffff | STATIC | CPU |
| 1 | 0025.456d.c781 | DYNAMIC | Fa0/5 |
| 1 | 1cc1.de5f.b7b3 | DYNAMIC | Fa0/11 |
| 1 | 1cc1.de5f.b9fa | STATIC | Fa0/18 |

Das mit H1 und H2 ist frei erfunden, weil ich die ip-config dieser Dinger von hier übernommen habe

4 RSC Versuch

```
Total Mac Addresses for this criterion: 23
```

Listing 4.26: Die Mac Adress Tabelle des Switches nach dem Vergeben eines statischen Ports

Es sind immer noch 23 Mac Adressen eingetragen. Der Unterschied ist, dass die Adresse 1cc1.de5f.b9fa nun statisch eingetragen ist. Da jetzt der Switch grundsätzlich konfiguriert ist, kommen jetzt die Sicherheitseinstellungen. Im Folgenden soll die Port Security eingerichtet werden. Port Security bedeutet, dass für einen Port berechtigte Mac Adressen eingetragen werden. Nur noch Devices mit berechtigten Mac Adressen dürfen dann noch über diesen Port kommunizieren. Die Befehle

```
CustomerSwitch(config)#interface fastEthernet 0/18  
CustomerSwitch(config-if)#switchport port-security ?
```

listen die verfügbaren Möglichkeiten zum Thema port security auf. Bevor die port security aktiviert wird, wird der statische Port Fa0/18 wieder dynamisch gemacht. Dies geschieht mit dem Befehl:

```
no mac address-table static 1cc1.de5f.b9fa interface fastethernet  
0/18 vlan 1
```

4.4.2 Port Security

Anschließend wir die port security für den Port Fa0/18 eingerichtet. Dies geschieht mit den Befehlen:

```
CustomerSwitch(config-if)#switchport mode access  
CustomerSwitch(config-if)#switchport port-security  
CustomerSwitch(config-if)#switchport port-security mac-address  
sticky  
CustomerSwitch(config-if)#end
```

Listing 4.27: Aktivieren der Port Security für den Port Fa0/18

Der erste Befehl bringt das Interface in den access mode. Im access mode ist das trunking permanent deaktiviert. Im trunked mode ist keine port security möglich. Der Befehl *switchport port-security* aktiviert aktiviert die port security auf diesem Interface. Mit *switchport port-security mac-address sticky* wird das automatische Lernen von Mac Adressen aktiviert. Im Lern Modus werden alle erkannten Mac Adressen als erlaubt gespeichert.

Den Erfolg dieser Befehle kann man mit den Befehlen *show port-security* oder *show port-security interface fa0/18 address* sofort kontrollieren.

Aus dieser Ausgabe lässt sich ableiten, dass die security action „Shutdown“ ist und dass die Anzahl der secure addresses ist 1. Der maximum secure address count gibt an, wie viele Mac Adressen gelernt werden dürfen. Bei einer falschen Mac Adresse wird der Port deaktiviert

Die neuen Einstellungen sind auch in der running config einzusehen:

Fuck,
hierfür
gibt es
keine Da-
tei. Die
sollten
wir auf-
treiben
oder aus
der Ver-
suchsbe-
schrei-
bung ko-
pieren

das mit
dem ma-

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

Current configuration : 1573 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname CustomSwitch
!
enable secret 5 $1$BRz6$AhGrgo3ovcz9Px5pGe75p.
enable password cisco
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
[...]
interface FastEthernet0/18
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 1cc1.de5f.b9fa
!
[...]
interface Vlan1
  ip address 192.168.1.5 255.255.255.0
  no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
!
control-plane
!
!
line con 0
  password cisco123
  login
line vty 0 4
```

4 RSC Versuch

```
password cisco123
login
line vty 5 15
password cisco123
login
!
end
```

Listing 4.28: Ansicht der running config nach dem Aktivieren der port security

In dieser Ansicht sind direkt einige Sicherheitsvorkehrungen erkennbar.

```
enable secret 5 $1$BRz6$AhGrgo3ovcz9Px5pGe75p .
```

Diese Zeile zeigt, dass die Konfiguration des Switches durch ein verschlüsseltes Passwort gesichert ist. Die Zeilen

```
interface FastEthernet0/18
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 1cc1.de5f.b9fa
```

zeigen an, dass das Interface FE0/18 durch eine port security gesichert ist. Diese port security ist im Lern Modus. Die Zeilen

```
line con 0
password cisco123
login
```

```
line vty 0 4
password cisco123
login
```

```
line vty 5 15
password cisco123
login
```

zeigen, dass die Zugänge zum Switch auch passwortgeschützt sind. Diese Passwörter sind aber nicht verschlüsselt.

Das Verhalten des Switch bei Verstößen gegen die port security kann durch einen einfachen Versuch getestet werden. Auf dem Port von H2 (FE0/18) wird der Host 3 angeschlossen. Die Mac Adresse dieses Hosts ist dem Switch bis jetzt unbekannt. Das Ergebnis ist, dass dieser Host trotz korrekter Einstellungen keine Verbindung zum Netzwerk aufbauen kann.

Da hätten wir was messen sollen
Step9 b)

Die Status des Interface sind:

```
FastEthernet0/18 is down, line protocol is down (err-disabled)
```

Da der Port durch die unberechtigte Mac Adresse deaktiviert wurde, muss er wieder aktiviert werden. Bevor dies passiert, wird die gelernte Mac Adresse wieder gelöscht. Dies geschieht mit dem Befehl:

```
CustomerSwitch#clear port-security sticky interface fa0/18 access
```

Anschließend wird das Interface wieder aktiviert. Dazu wird das Interface erst manuell deaktiviert und dann wieder manuell aktiviert.

```
CustomerSwitch(config)#interface fa0/18
CustomerSwitch(config-if)#shutdown
CustomerSwitch(config-if)#no shutdown
```

4.4.3 Geschwindigkeits- und Duplexeinstellungen des Switchs

Die Ports eines Switches haben per default die Einstellungen auto duplex und auto speed. Das bedeutet, dass der Switch anhand des angeschlossenen Device die Geschwindigkeit und den Übertragungsmodus.

In diesem Teil des Versuchs soll diese Eigenschaft konfiguriert werden. Vor Beginn dieser Konfiguration werden erst die Interfaces betrachtet. Dadurch ist es möglich zu überprüfen, ob die Änderungen erfolgreich waren.

```
FastEthernet0/5 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0024.f98a.e705 (bia 0024.f
98a.e705)
MTU 1500 bytes, BW 100000 Kbit, 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, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:07, output 00:00:00, 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
    284 packets input, 29831 bytes, 0 no buffer
    Received 42 broadcasts (0 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 40 multicast, 0 pause input
    0 input packets with dribble condition detected
    1465 packets output, 115081 bytes, 0 underruns
```

Was bedeutet das geht nicht in der Datei?

Die Ausgabe von FE0/18 ist gefäked(Der Port wurde in Step10 nicht freigeschaltet). Vor Abgabe checken, ob das plausibel ist

4 RSC Versuch

```
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out

FastEthernet0/11 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0024.f98a.e70b (bia 0024.f
98a.e70b)
MTU 1500 bytes, BW 100000 Kbit, 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, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, 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 1000 bits/sec, 1 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    140 packets input, 18837 bytes, 0 no buffer
    Received 71 broadcasts (0 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 4 multicast, 0 pause input
    0 input packets with dribble condition detected
    1574 packets output, 122260 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 PAUSE output
    0 output buffer failures, 0 output buffers swapped out

FastEthernet0/18 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0024.f98a.e712 (bia 0024.f
98a.e712)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto-speed, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:07:37, 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
    131 packets input, 14849 bytes, 0 no buffer
    Received 19 broadcasts (0 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    1296 packets output, 102046 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 PAUSE output
    0 output buffer failures, 0 output buffers swapped out

```

Listing 4.29: Die Interface Informationen vor der Konfiguration der Sende Modi

| Interface | Duplex Modus | Geschwindigkeit | Media Typ |
|-----------|--------------|-----------------|--------------|
| FE0/5 | Full-duplex | 100 Mb/s | 10/100BaseTX |
| FE0/11 | Full-duplex | 100 Mb/s | 10/100BaseTX |
| FE0/18 | Auto-duplex | Auto-Speed | 10/100BaseTX |

Tabelle 4.5: Die Übertragungsmodi in der Übersicht

4.4.4 Reflection

Zum Ende des Versuchs gibt es noch einige Fragen, die prüfen sollen, ob der Versuch verstanden wurde.

1. **Which password needs to be entered to switch from user mode to privilege exec mode on the Cisco switch, and why?** The password „cisco123“ is the correct password. In step 3 we set two passwords. „cisco“ and „cisco123“ The second one was set als encrypted password. IOS prefers the encrypted passwords. If a decrypted and an encrypted password is set, IOS will just use the encrypted one.
2. **Which symbol is used to show a successful ping in the Cisco IOS software?** Our successful ping commands had every time the sequence !!!!! after the prompt, that 5 pings being send. After these 5 ! was the prompt with the success rate. So the symbol to show a successful ping ist the „!“.
3. **What is the benefit of using port security?** The benefit of port security is a higher security in your network.

Die Zeile von FE0/18 kann aber auch falsch sein, weil das Interface down ist(Ich habe nur die erste Zeile manipuliert)

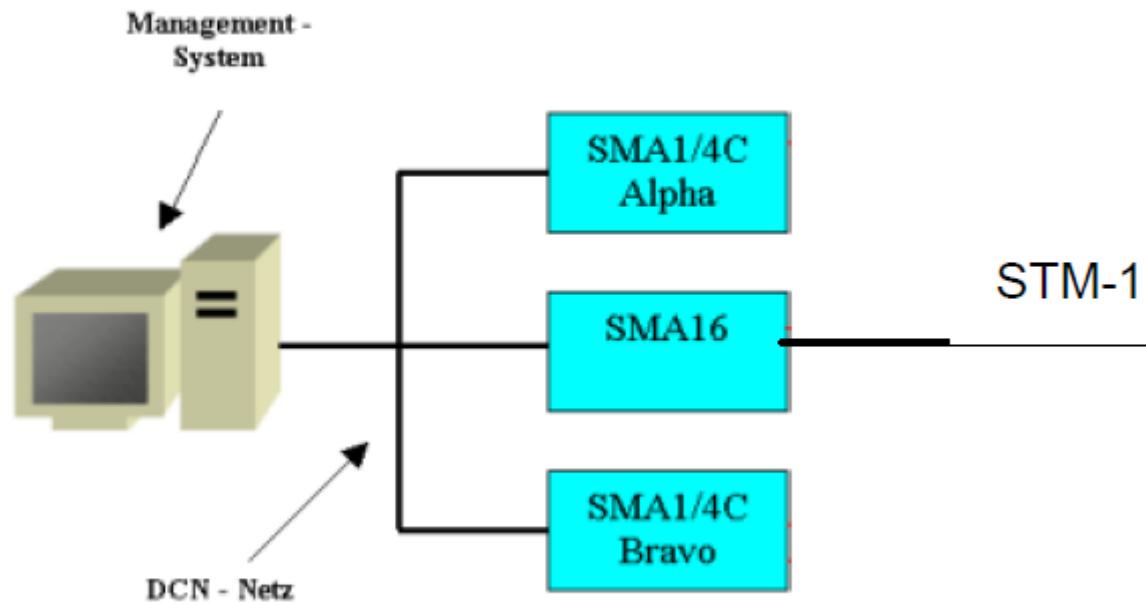
Die Teile c und d machen keinen Sinn. Warum soll ich FE0/10 konfigurieren und auf FA0/5 achten? Außerdem fehlt

5 SDH Versuch

5.1 Allgemeine Beschreibung der Versuche

Der folgende Versuch handelt von der Multiplextechnik SDH. SDH steht Synchrone Digitale Hierarchie die es möglich macht niederratige Datenströme zu einem hochratenigen Datenstrom zu multiplexen, das Netz taktet dabei vollkommen synchron. In unserem Versuchsaufbau werden wir absichtlich verschiedene Fehler einspeisen sowie uns die Pointeraktivitäten im Netz genauer ansehen. Die Möglichkeit Fehler einzuspeisen wird uns durch das Messgerät GN Elmi EST 2100 ermöglicht, der ebenfalls als Multiplexer fungiert. Das Auswerten dieser Fehler ist über die Software Telecommunications-Management-Network-Software von Siemens gegeben. Der Rechner auf dem die Software läuft ist über die QST-E3 Schnittstelle mit den SMA 16 Multiplexern verbunden und sammelt so die nötigen Daten.

Die Multiplexer unter sich sind mit Lichtwellenleiter verbunden die theoretisch eine Entfernung von gut 50Km schaffen würden. Da Elmi leider nicht von Siemens ist, ist es auch nicht möglich direkt über die Software zu sehen wie Elmi sich als Multiplexer verhält.



5.2 Versuchsgegenstände im Detail

Im folgenden betrachten wir uns die TMNS und Elmi für das Verständnis den den Umgang etwas genauer.

5.2.1 GN Elmi EST 2100

Elmi ist ein Messgerät das direkt mit den anderen Multiplexern über einen Lichtwellenleiter angeschlossen ist. Er fungiert in erster Linie zum einspeisen von Fehlern ins Netz um zu betrachten wie sich das SDH darauf verhält. Wie oben bereits erwähnt ist er selbst ebenfalls Teil des Netzes in Form von einem Multiplexer. Folgende Grafiken erläutern wie mit dem Gerät um zu gehen ist.

5.2 Versuchsgegenstände im Detail



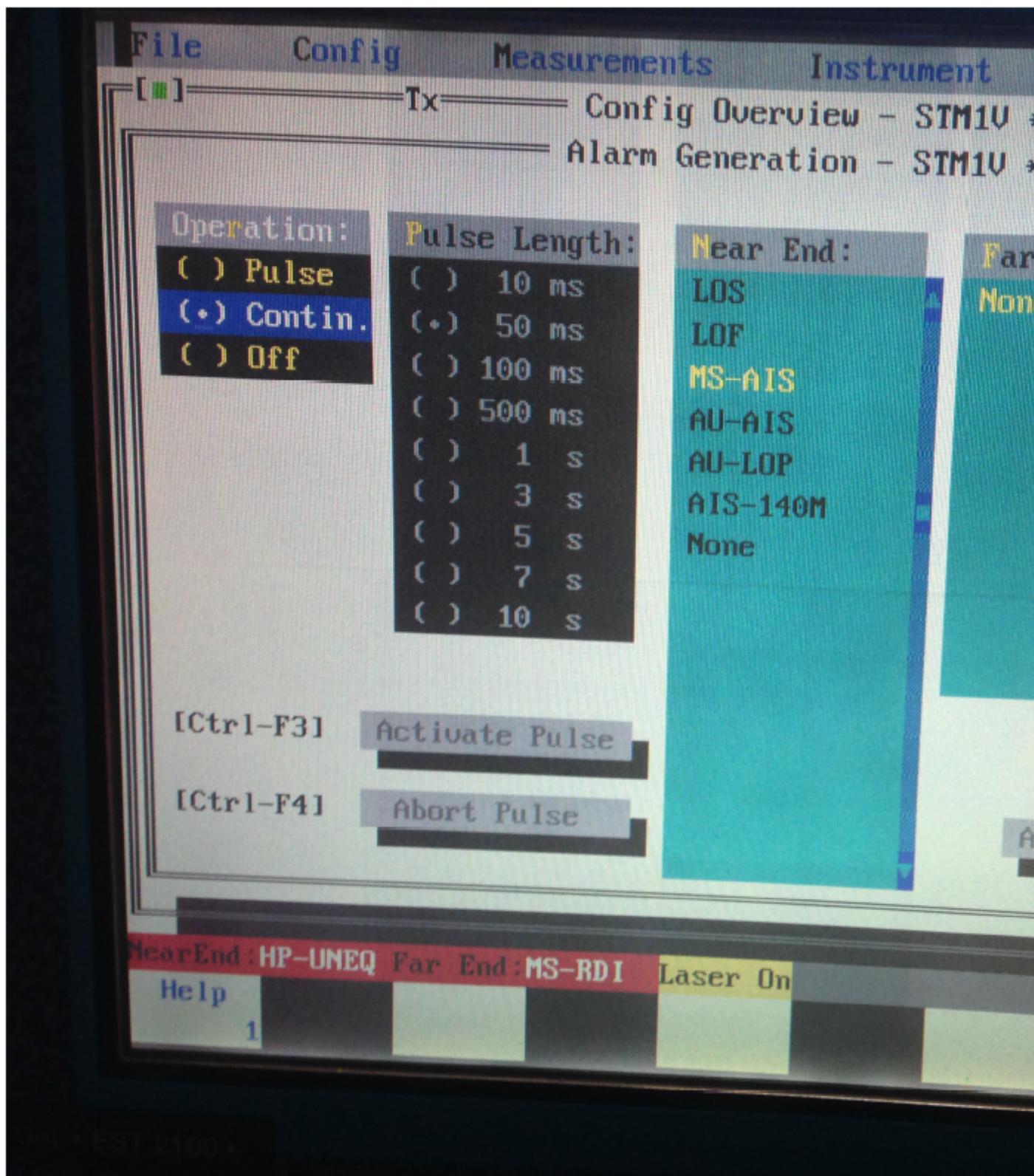
5 SDH Versuch

Es gibt es verschiedene Möglichkeiten das Netz zu beeinflussen. Da Elmi einen eigenen internen Systemtakt besitzt, kann man diesen auch verwenden um so beispielsweise zwei verschiedene Takte im Netz zu simulieren. Unter den Menüpunkt Ref. kann man diesen dann beeinflussen.

Bild von
Taktmenu

Desweiteren für unseren Versuch wichtige Funktion bietet die Sektion ALARM. Hier kann man nach belieben Fehler ins Netz einspeisen. Diese kann man entweder als Burst, das bedeutete über einen bestimmten Zeitrahmen, oder kontinuierlich setzen. Für unserem Versuch werden nur diese zwei Sektionen benötigt deswegen wird hier nicht weiter auf die Funktionalität von Elmi eingegangen.

5.2 Versuchsgegenstände im Detail



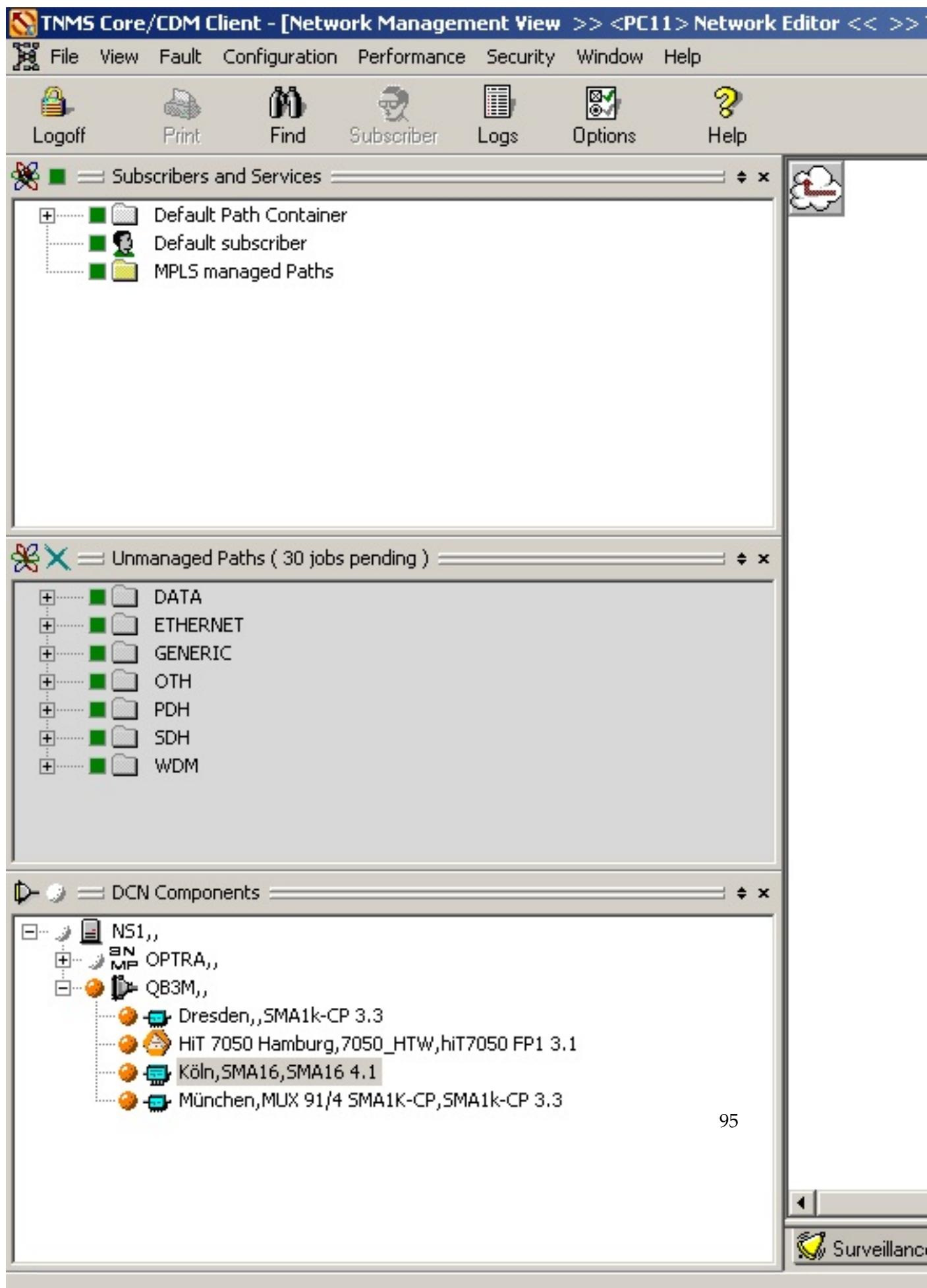
5 SDH Versuch

5.2.2 TMNS

Die TMNS ist zur Analyse und Überwachung des SDH-Netzes hilfreich. In der Hauptansicht wird das Netz abstrakt für eine gute Übersicht dargestellt. Klickt man nun auf unser Testnetz *Köln* auf die Performancemessung gelangt man in die für den Versuch interessante Performanceansicht.

stimmt
das?

5.2 Versuchsgegenstände im Detail



5 SDH Versuch

Im Hauptfenster werden sämtliche Komponenten angezeigt die zu dem Netz gehören bis auf Elmi. Hier werden bei einkommenden Fehlern, durch rotes blinken markiert welche Komponente einen Fehler aufweist. In der Folgenden Abbildung ist zu sehen wie die Komponente in dem Steckplatz 406 auf Port 3 einen einkommenden Fehler anzeigt. Port 1 und 2 sind ebenfalls rot markiert jedoch weil die Ports konfiguriert sind aber kein Kabel angeschlossen ist. Also können wir diese einfach ignorieren.

5.2 Versuchsgegenstände im Detail

SMA16 "Köln"

File View NE State Fault Performance Security Options Window Help

Module View

NE / Subrack

| | | | | | | | | | | | | | | | |
|-------------------|-------------------|------------|-----|-----------|------------------|------------|-----|-----|-----|------------------|-----------------------|-----|-----|-----|-----|
| 401 | 402 | 403 | 404 | 405 | 406 | 407 | 408 | 409 | 410 | 411 | 412 | 413 | 414 | 415 | 416 |
| T A E12-42 (W) | | | | | T A OIS1D (W) | A IPU16 | | | | T A OIS4D (W) | T A OIS4D (In MSP) | | | | |
| 501 | 502 | 503 | 504 | 505 | 506 | 507 | 508 | 509 | 510 | | | | | | |
| T A OIS16D (W) | T A OIS16D (W) | A IPU16 | | A SN64 | | A IPU16 | | | | | | | | | |

OIS1D #406

| Symbol | Card | ProvMode | Slot # | Port # | NE Conn... | Distrib... |
|--------|-------|----------|--------|-----------|--------------|------------|
| O | OIS1D | Working | 406 | 01 (155M) | 406 in: a... | ATRJL... |
| O | OIS1D | Working | 406 | 02 (155M) | 406 in: a... | ATRJL... |
| O | OIS1D | Working | 406 | 03 (155M) | 406 in: a... | ATRJL... |
| O | OIS1D | Working | 406 | 04 (155M) | 406 in: a... | ATRJL... |

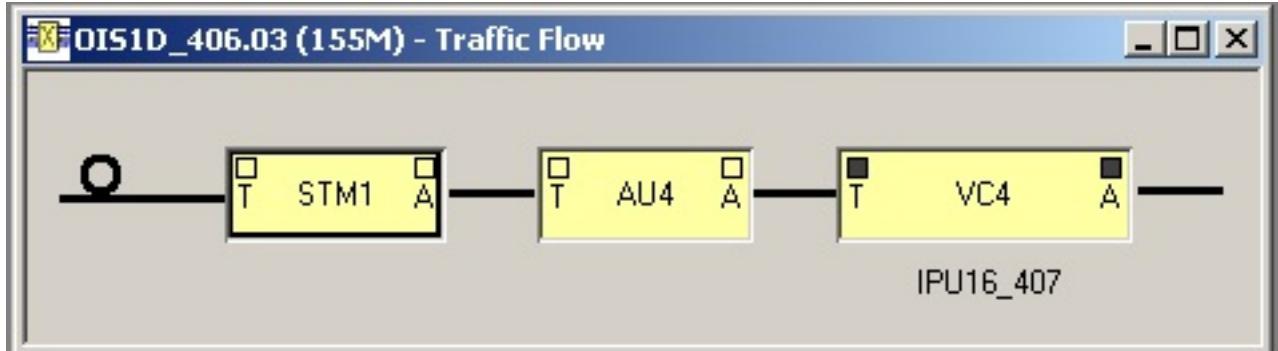
97

| Object | Location | Time (local) | Message Type | Message Content |
|-----------|---------------------|---------------------|--------------|-----------------|
| FAULT-MGR | | 06/11/2014 14:42:29 | Notification | Up... |
| MS | OIS1D_406.03 (155M) | 06/11/2014 14:39:01 | Response | thr... |
| MS | OIS1D_406.03 (155M) | 06/11/2014 14:39:01 | Response | thr... |
| MS | OIS1D_406.03 (155M) | 06/11/2014 14:39:01 | Response | thr... |

For Help, press F1

5 SDH Versuch

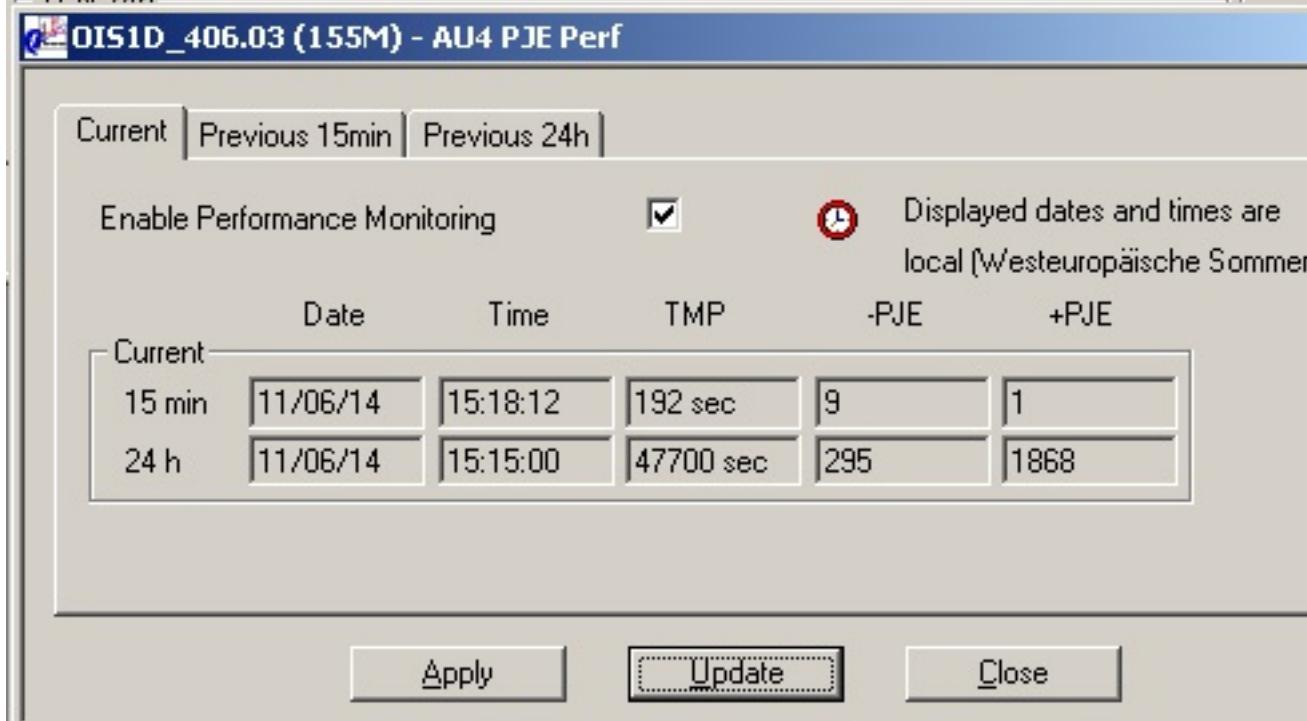
Bei einem ankommenden Fehler kann man sich nun die Komponente genauer anschauen indem man den entsprechenden Port sich unter die Lupe nimmt. Durch Auswahl der Submenu-View gelangt man in eine Ansicht in der man genauer sehen kann wo der Fehler entstanden ist.



Hier hat man nun je nach Fehler die Auswahl. Wenn es um Pointer geht wird hier im Normalfall das AU-4 Fenster anfangen zu Blinken, wenn ein Netz-Fehler auftritt das STM-1 Fenster.

Diese schauen wir uns hier noch im Detail an.

Zuerst sehen wir hier die Performance-Ansicht von dem AU4 Fenster.



Dieses beinhaltet:

- Date - Das Aktuelle Datum
- Time - Die Aktuelle Zeit

5.2 Versuchsgegenstände im Detail

- TMP - Dauer des gemessenen Intervalls
- -PJE - Die gezählten Negativ Pointer-Vorgänge
- +PJE - Die gezählten Positiv Pointer-Vorgänge

Die Aktualisierung der Daten findet nur manuell mit dem Update Knopf statt. TMP ist hier im Auge zu behalten da die Daten alle 15 Minuten in eine Log-Datei geschrieben werden. Die Log-Dateien sind in den Reitern *Previous 15min* und *Previous 24h* wieder zu finden.

Um im genau zu sehen was im STM-1 vor sich geht kann man sich ebenfalls die Performance-Ansicht anzeigen lassen.

The screenshot shows the 'OIS1D_406.03 (155M) - STM1 MS Near End Perf' dialog box. At the top, there are three tabs: 'Current' (selected), 'Previous 15min', and 'Previous 24h'. Below the tabs are two checkboxes: 'Enable Performance Monitoring' (checked) and 'Displayed dates and times are local (Westeuropäische Sommerzeit)' (unchecked). A note indicates that monitored values are in local time (Central European Summer Time).

| | Date | Time | TMP | BBE | ES | SES | UAS |
|---------|----------|----------|-----------|-----|----|-----|-------|
| Current | | | | | | | |
| 15 min | 11/06/14 | 15:19:16 | 256 sec | 0 | 4 | 4 | 14 |
| 24 h | 11/06/14 | 15:15:00 | 47700 sec | 0 | 53 | 53 | 32828 |

Below the table, there are sections for 'TCN 15min' and 'TCN 24h'. Each section has 'Monitoring enabled' checkboxes and 'upper Threshold' and 'lower Threshold' input fields. The 'TCN U' checkbox is checked in the 'TCN 15min' section.

| | Monitoring enabled | upper Threshold | lower Threshold | |
|-----------|-------------------------------------|-------------------------------------|-------------------------------------|-----|
| TCN 15min | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| | | 7200000 | 900 | 900 |
| | | 7200000 | 900 | 900 |

| | Monitoring enabled | upper Threshold | | |
|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------|
| TCN 24h | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| | | 691200000 | 86400 | 86400 |

At the bottom are three buttons: 'Apply', 'Update' (disabled), and 'Close'.

Folgende Daten werden angezeigt:

- Date - Das Aktuelle Datum

5 SDH Versuch

- Time - Die Aktuelle Zeit
- TMP - Dauer des gemessenen Intervalls
- BBE - Background Block Error
- ES - Errored Seconds
- SES - Severely Errored Seconds
- UAS - Unavailable Seconds

Was das Aktualisieren und das wegschreiben in die Log-Datei angeht ist der Vorgang wie bereits vorher beschrieben der Fall.

Die Fehlerrate wird in Error-Sekunden angegeben die unterschiedliche Aussagen über den Fehler angeben.

- ES - beinhaltet, innerhalb einer Sekunde, ein oder mehrere fehlerhafte Blöcke.
- SES - beinhaltet, innerhalb einer Sekunde, 30 Prozent fehlerhafte Blöcke.
- UAS - Nach 11 SES gilt eine Leitung als nicht mehr verfügbar. Im Gegenzug gilt sie als verfügbar, nach 11 Sekunden ohne SES.

5.3 Fehlereinspeisung

Nachdem wir alle für den Versuch erforderlichen Komponenten kennengelernt haben, können wir nun den eigentlichen Versuch weiter beschreiben. Im folgenden sollen drei verschiedene Fehlermeldungen mit Hilfe von Elmi einmal kontinuierlich und einmal als Bursts eingespeist werden. Wenn im empfangenen Signal Bitfehler enthalten sind sendet der Empfänger eine Alarm-Nachricht in Senderichtung zurück. Bei dieser Rückmeldung spricht man von REI (Remote Error Indication). Die für uns wichtigen sind:

- LOS - Lost of Singnal, Rückgang der eingehenden optischen Leistungspegel, verursacht hohe Bitfehlerrate
- MS-AIS - Multiplex Section Alarm Indication Signal, wird ausgelöst wenn K2 (bits 6, 7, 8) auf 111 gesetzt ist für mehr als 3 Frames.
- LOF - Lost of Frame tritt auf wenn das Signal für mehr als 3 ms OOF (Out of Frame) ist.
- OOF - Out of Frame tritt auf wenn die Bytes A1 und A2 länger als

Sind im empfangenen Signal Bitfehler enthalten, meldet der Sensor BIP Errors. Da das nicht gleichbedeutend mit dem Ausfall der Verbindung ist, spricht man von einer Anomalie, die in Senderichtung zurückgemeldet wird. Die Rückmeldung wird als REI (Remote Error Indication) bezeichnet.

Ich habe den Fehler auskommentiert

5.3 Fehlereinspeisung

5.3.0.1 Kontinuierliches Fehlereinspeisen

Zuerst werden wir die Fehler kontinuierlich einspeisen. Nach dem feuern der Fehler fängt die entsprechende Komponente an zu Blinken und wir klicken uns bis in das STM-1_performance-Fenster durch.

OS1D_406.03 (155M) - STM1 MS Near End Perf

| | Current | Previous 15min | Previous 24h | | | | |
|--------------------------------------|-------------------------------------|---------------------------------------|--|-----|----|-----|-------|
| Enable Performance Monitoring | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Displayed dates and times are local (Westeuropäische Sommerzeit) | | | | |
| Current | Date | Time | TMP | BBE | ES | SES | UAS |
| 15 min | 11/06/14 | 15:09:06 | 546 sec | 0 | 14 | 14 | 276 |
| 24 h | 11/06/14 | 15:00:00 | 46800 sec | 0 | 18 | 18 | 32552 |
| TCN 15min | | | | | | | |
| Monitoring enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | | | |
| upper Threshold | 7200000 | 900 | 900 | | | | |
| lower Threshold | 7200000 | 900 | 900 | | | | |
| TCN 24h | | | | | | | |
| Monitoring enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | | | |
| upper Threshold | 691200000 | 86400 | 86400 | | | | |
| <input type="button" value="Apply"/> | | <input type="button" value="Update"/> | <input type="button" value="Close"/> | | | | |

Die Ergebnisse sind alle wie zu erwarten gleich. Alle drei Fehlermeldungen lassen den UAS-Counter solange ansteigen bis man aufhört den Fehler einzuspeisen. Da alle drei Fehler kontinuierlich auftreten verursachen sie dauerhaft SES und somit nach kurzer Zeit UAS. Somit sind kontinuierliche Fehler sehr schwerwiegend und sofort zu behandeln.

Hier noch einmal ein Tabellarischer Überblick über alle gemessenen Daten:

Caption
der Table
ändern

5 SDH Versuch

| Fehlermeldung | Burst-Time | ES | SES | UAS | Fenster |
|---------------|----------------|----|-----|-----|---------|
| MS-AIS | Kontinuierlich | 0 | 0 | ++ | STM1 |
| LOS | Kontinuierlich | 0 | 0 | ++ | STM1 |
| LOF | Kontinuierlich | 0 | 0 | ++ | STM1 |

Tabelle 5.1: Irgend eine Unterschrift

5.3.0.2 Burst Fehlereinspeisung

Als zweites Verursachen wir eine MS-AIS und ein LOS jeweils innerhalb von 100ms, einer Sekunde, und sieben Sekunden.

| Fehlermeldung | Burst-Time | ES | SES | UAS | Fenster |
|---------------|------------|----|-----|-----|---------|
| MS-AIS | 100 ms | 1 | 1 | 0 | STM1 |
| MS-AIS | 1 s | 2 | 2 | 0 | STM1 |
| MS-AIS | 7 s | 8 | 8 | 0 | STM1 |
| LOS | 100 ms | 3 | 3 | 0 | STM1 |
| LOS | 1 s | 4 | 4 | 0 | STM1 |
| LOS | 7 s | 0 | 0 | 14 | STM1 |

Wie man anhand der Tabelle sehen kann löst die MS-AIS lediglich maximal 8 SES aus und somit wird die Leitung nicht als Unavailable gesetzt.

Zu Beobachten war das bei den kruzen Bursts die TMNS überhaupt gar nicht auf den Fehler reagiert. Das ist erklärbar da bevor der Fehler erkannt wird, er bereits wieder vorbei ist. Bei den LOS Alarmen sind die Error Sekunden schon betrachtlich höher. Ein sieben Sekunden langer LOS kann die Leitung bereits für einige Momente ausser gefecht setzen wie man an dem UAS Feld erkennen kann.

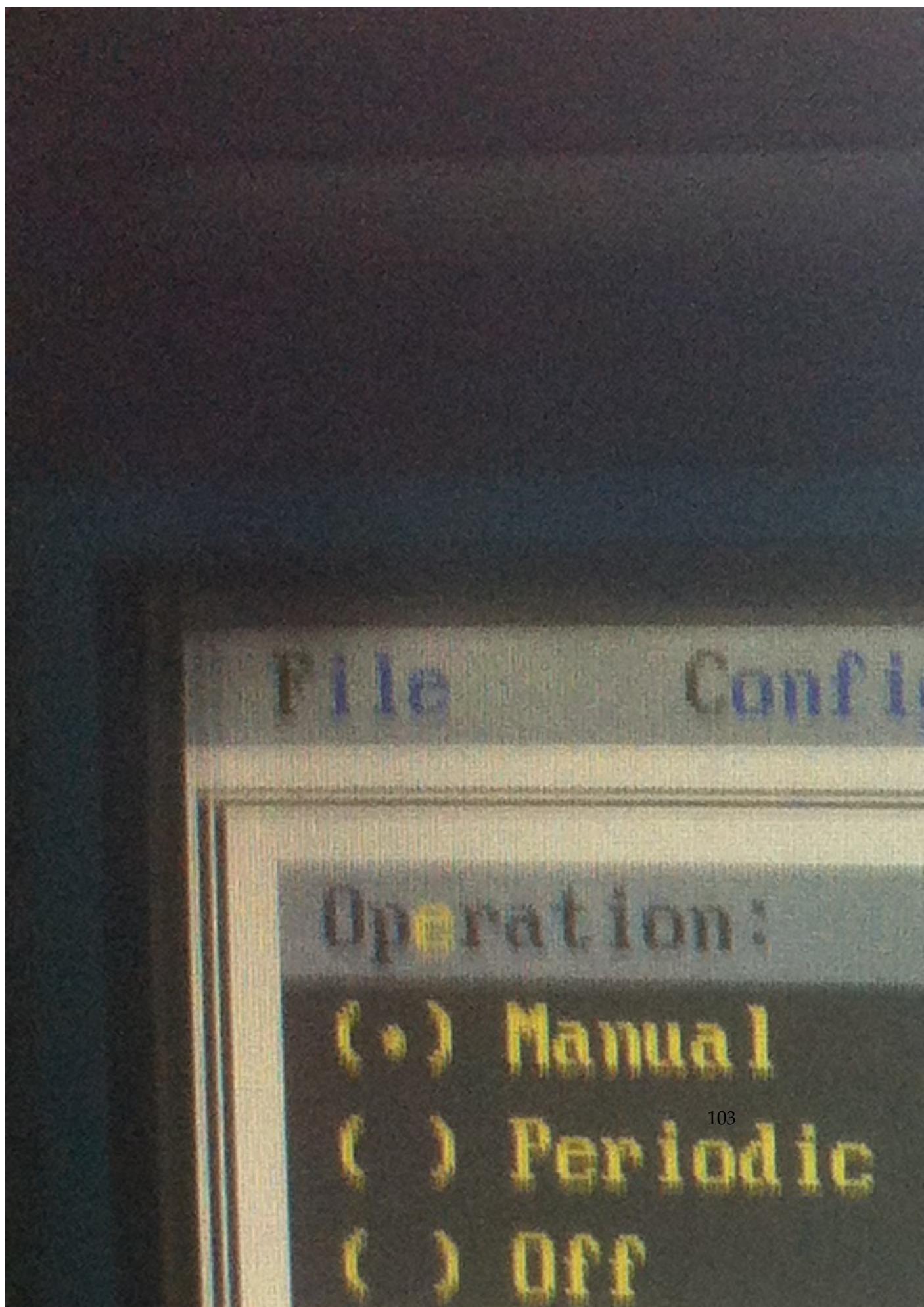
5.3.1 Pointer

Da das SDH-Netz ein voll getaktetes Netz ist und so durch Taktunterschiede es theoretisch zu einer Überlast kommen kann, gibt es Pointer. Dieser ist in der Administrative Unit zu finden und zeigt auf die Position der Nutzinfomrationen im Payload Bereich. Durch Pointer ist es möglich die Taktunterschiede, durch einfugen von Leer-Bytes oder früheres Senden von Payload, auszugleichen. Es können allerdings nur in jedem vierten Rahmen nach Ankündigung die Pointer angepasst werden.

In diesem Versuch beschäftigen wir uns mit dem dekrementieren und Inkrementieren von Pointern. Zusätzlich dazu, werden wir mit dem Systemtakt des Netzes hantieren.

5.3.1.1 Manuelles negativ und positiv Justieren

Elmi hat für die Justierung des Pointers ein eigenes Menu. Hier kann man einstellen ob man die Pointer-Justierung dauerhaft alle 1500 ms oder manuell durchführen will.



5 SDH Versuch

Zuerst Dekrementieren wir den Pointer was ein Pointer Justification Event auslöst und in TMNS im Performance Menu von AU-4 als +PJE-Erhöhung wahrzunehmen ist. Entsprechend umgekehrt verhält sich das System für die Inkrementierung des Pointers. Im Versuch war zu erkennen das die ersten drei gesendeten Werte nicht in dem Perfomance-Fenster sichtbar waren. Dies ist darauf zurück zu führen das nur bei jedem vierten Rahmen eine Pointer-Aktivität durchgeführt wird. Also wurden die ersten drei als Ankündigung verstanden das nun der Pointer geändert wird.

stimmt
das denn
auch?

5.3.1.2 Ändern des Taktes von Elmi

Ändert man den Takt von Elmi auf den Internen so kann man einen hohen Sprung des +PJE Feldes beobachten. Dies zeigt das das System die beiden Multiplexer versucht zu synchronisieren. Dannach sieht man das das +PJE Feld weiter steigt, um etwa drei pro Sekunde. Die Erklärung dafür ist, das der interne Takt von Elmi etwas langsamer ist als der des anderen Multiplexern. So muss dieser positiv Inkrementieren um den Takt auszugleichen und das Netz synchron zu halten.

5.3.1.3 kontinuierliches negatives Justieren bei Internem Takt

Als letztes möchten wir gerne noch Versuchen was passiert wenn wir zusätzlich zu dem geändertem Takt noch negativ den Pointer justieren. Bei Verwendung des internen Taktes von Elmi haben wir festgestellt das eine positive Pointerjustierung nötig ist um das Netz Synchron zu halten. Wenn wir nun aber auf der Sende Seite den langsameren Takt durch negativ Justierung ausgleichen kann man beobachten wie die benötigten Pointer-Aktivitäten sinken. Wenn man das Intervall entsprechend weit runter stellen würde könnte man den kompletten Ausgleich zwischen den unterschiedlichen Takten erreichen. In dem Versuch haben wir beobachtet wie sich die Pointerjustierung auswirkt. Dies ist hier noch einmal Tabellarsich aufgeführt.

| Justierung | PointerAktivität |
|-----------------|-----------------------|
| Inkrementierung | 5 Pointer pro Sekunde |
| Dekrementierung | 3 Pointer pro Sekunde |
| Ohne | 4 Pointer pro Sekunde |

Die Tabelle zeigt auf das mit einer Positiven Justierung des Pointers zusätzlich zu dem unterschiedlichen Takt eine noch höhere Pointer-Aktivität nötig ist um das System synchron zu halten. Wie oben beschrieben führt eine Dekrementierung zu einem annähernden Ausgleich. Diese Aussage wird unterstützt wenn man sich die Spalte Ohne Justierung anschaut. Hier ist es etwa der Mittelwert der beiden anderen.

5.4 Fazit

In den Versuchen wurde das bereits erlangte Wissen praktisch angewandt. Vor allem in dem Bereichen Pointer wurden die das Verständnis dafür sehr viel klarer und die

5.4 Fazit

Zusammenhänge eindeutiger. Allerdings waren die Versuche alle sehr klar definiert und die Erwartungen nicht überrascht.

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.
- [3] Friedhelm Greis. *Cisco fordert schnelleren Videotransport in Zettabyte-Ära*. <http://www.golem.de/news/traffic-prognose-cisco-fordert-schnelleren-videotransport-in-zettabyte-aera-1406-107124.html>. 2014.
- [4] Patapsco. *Darstellung der Liberator S*. http://www.patapsco.co.uk/-pdfs/Liberator_S_isdn_converter_isdn_conversion_pri_bri.pdf.
- [5] Cisco Systems. *Cisco 2800 Router*. http://www.cisco.com/en/US/products-/ps5881/prod_view_selector.html.
- [6] Cisco Systems. *Introduction to Routers in WAN*. http://www.cisco.com/web/learning/netacad/demos/CCNA2v3Demo/ch1/1_1_2/index.html.

Kolophon

Dieses Dokument wurde mit der L^AT_EX-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).