

# Rechnernetze Dokumentation

Sheraz Azad und Sven Marquardt

Wintersemester 2015/16

## Inhaltsverzeichnis

<b>1 Versuch 1 Schichtenmodell</b>	<b>3</b>
1.1 Aufgabe 2 Überlegungen für das Spiel Vier gewinnt . . . . .	3
1.2 Aufgabe 4 Vor- und Nachteile der Realisierung . . . . .	4
1.3 Aufgabe 5 Verbesserte Kommunikation durch Stifte . . . . .	4
1.4 Aufgabe 6 Kommunikation durch Klatschen . . . . .	5
1.5 Aufgabe 7 Kommunikation mit beliebigen Teilnehmern . . . . .	6
1.6 Aufgabe 8 Kommunikation mit bestimmten Teilnehmern . . . . .	6
1.7 Aufgabe 9 Datenfluss Problem . . . . .	7
<b>2 Versuch 2 Zuverlässige Datenübertragung</b>	<b>8</b>
2.1 Aufgabe 2 Messung der Häufigkeit von Rahmenverlusten . . . . .	8
2.2 Aufgabe 3 Messung der Bitfehlerrate . . . . .	8
2.3 Aufgabe 4 Vorüberlegungen zum sicheren Protokoll . . . . .	8
2.4 Aufgabe 6 Verhinderung von Rahmenverlusten . . . . .	9
<b>3 Versuch 3 Anwendungsschicht und Tools</b>	<b>10</b>
3.1 Aufgabe 4 nslookup tool . . . . .	10
3.2 Aufgabe 6 Aufbau von Websites . . . . .	12
3.3 Aufgabe 7 Laden von Websites . . . . .	13
3.4 Aufgabe 8 SSL/TLS im Browser . . . . .	14
3.5 Aufgabe 9 SSL/TLS beim Server . . . . .	15
3.6 Aufgabe 10 Auswertung von Cookies . . . . .	15
3.7 Aufgabe 11 Diskussion AddOns . . . . .	16
3.8 Aufgabe 12 Steganographie . . . . .	17

<b>4 Versuch 4 Switch</b>	<b>18</b>
4.1 Aufgabe 3 MAC-Adresse . . . . .	18
4.2 Aufgabe 4 Beobachtungen im Netz . . . . .	19
4.3 Aufgabe 5 Spanning Tree Protocol . . . . .	19
4.4 Aufgabe 6 Lernen von Adressen für die MAC-Adresstabelle . . .	22
4.5 Aufgabe 7 Erstellen eines VLANs mit der Nummer 100 . . . . .	24
4.6 Aufgabe 8 VLAN-Trunk-Konfiguration . . . . .	24
<b>5 Versuch 5 Router</b>	<b>26</b>
<b>6 Versuch 6 Transportschicht</b>	<b>27</b>

**ALLE BILDER UND TABELLEN MÜSSEN IN DEN TEXTFLUSS  
EINGEBUNDEN WERDEN**

# 1 Schichtenmodell

## 1.1 Überlegungen für das Spiel "Vier gewinnt"

Die Kommunikation untereinander findet mittels einer Münze statt, welche hochgehalten wird, wobei wir den Binärcode verwenden. Zeigt die Münze Kopf stellt diese die 0 dar und zeigt die Münze Zahl stellt sie die 1 dar. Damit die beiden Positionen unterscheidbar sind, wird die Münze pro Position, also entweder Kopf (0) oder Zahl (1), jeweils für 2 Sekunden hochgehalten erst danach findet ein Positionswechsel statt.

Damit eine geregelte und sinnvolle Kommunikation zwischen den Kommunikationspartnern stattfinden kann, wurden Kommunikationsregeln festgelegt. Das Spiel "Vier gewinnt" hat 7 Reihen mit jeweils 6 Feldern, da wir bei diesem Spiel nur die Spaltenangabe brauchen um unseren Spielzug zu machen, wurden 3 Bits verwendet von 001 (1) bis 111 (7) welche die einzelnen Spalten darstellen.

**HIER EIN BILD VON EINEM VIER GEWINNT SPIELFELD  
HIER FEHLT NOCH WIE MAN ENTSCHEIDET WER ALS ERSTES DRAN IST**

Weitere Bitcodierungen für die Kommunikation sind:

Bitfolge	Bedeutung
001	Reihe voll
110	Gewonnen
101	Unentschieden
011	Weiter
100	Fertig
111	Nochmal bei Fehlübertragung

**HIER EIN BEISPIEL FÜR DEN SPIELFLUSS DEN ENTWEDER ICH IN LÜBECK HABE**

Tabelle 1: Hybrides Modell

5. Anwendungschicht	Das Spiel "Vier gewinnt"
4. Transportschicht	Wird nicht verwendet
3. Vermittlungsschicht	Wird nicht verwendet
2. Sicherungsschicht	Übersetzen der Kommunikation in Bits und Fehlererkennung
1. Bitübertragungsschicht	Übertragung von 0 und 1 durch Medium Münze

## 1.2 Vor- und Nachteile der Realisierung

Zweierteam mit dem die Analyse der Spielrealisierung gemacht wurde bestand aus Malte Grebe und Niklas Klatt.

### Vorteile:

Aufgrund der Kommunikationsregeln ist das Spiel leicht zu verstehen und zu bedienen. Durch die ständige Überprüfung wird dafür gesorgt, dass keine Fehler bei der Übertragung auftreten. Dadurch das ein Weiter (011) erwartet wird, gibt es Spielpausen und man kann in Ruhe sein Spielfeld aktualisieren.

### Nachteile:

Ein Zug dauert ca. eine Minute, da jede Position zwei Sekunden gehalten wird. Spieler 1 oder 2 fängt zu früh mit der Übertragung vom nächsten Spielzug an, dadurch gibt es eine Fehlerübertragung die wiederholt werden muss.

### Verbesserte Spielrealisierung:

Einführung einer Spielfeldsynchroneisierung um sicherzustellen, dass keine Fehler beim Eintragen der Positionen eingetreten sind.

## 1.3 Verbesserte Kommunikation durch Stifte

Es gibt zwei Varianten die Kommunikation druch Stifte zu verbessern.

Die **erste Variante** ist, das man einen waagerechten Stift als 0 und einen senkrechten Stift als 1 interpretiert. Dadurch lassen sich die drei Kommunikationsbit leicht, schnell und eindeutig darstellen.

**HIER EINE ZEICHNUNG MIT HALBWINKEL UND DIE BITS**

## ZU DEN WINKELN

Die **zweite Variante** ist, dass man die Stifte in bestimmten Winkel hinlegt. Hier können wir zum Beispiel sagen das wenn der Stift in einem 90 Grad Winkel liegt, dieser die Bitfolge 001 für Reihe voll darstellt. So können wir die verschiedenen Bitfolgen angeben und bräuchten mit dieser Variante sogar nur einen Stift statt drei.

Diese Fragestellung bezieht sich auf die Bitübertragungsschicht, da sie für die Übertragung von Informationen (Bits 0 und 1) zuständig ist.

## 1.4 Kommunikation durch Klatschen

### Problem

Dadurch das alle Teams zeitgleich angefangen haben zu klatschen, konnte man nicht unterscheiden ob das Klatschgeräusch vom gegenüber sitzenden Kommunikationspartner kam, oder von einem Kommilitonen aus einer anderen Gruppe. Aufgrund dieser Tatsache sind bei allen Teams Fehler bei der Kommunikation entstanden.

### Lösung

Auch hier gibt es zwei Lösungsansätze, die sich auf die Medienzugriffskontrolle aufbauen, in der dann nur eine Gruppe zur Zeit kommunizieren darf. Diese Möglichkeiten sind.

**1. Ohne Koordinator:** Jeder Gruppe im Raum wird eine zufällige Wartezeit in Sekunden zugeteilt, die sie abwarten müssen um kommunizieren zu können. Tritt der Fall auf das zwei oder mehrere Gruppen zur selben Zeit kommunizieren wollen, wird eine Wartezeit aus einem größeren Zeitintervall genommen um diesen Fall zu umgehen. Je nach Wichtigkeit könnte man hier den jeweiligen Gruppen eine Wartezeit aus einem kleinen Zeitintervall zu weisen, als dem Rest der Gruppen.

**2. Mit Koordinator:** Bei diesem Lösungsansatz gibt es einen Koordinator im Raum, der die Anfragen der Gruppen, die kommunizieren wollen, an sich nimmt und stellt dann eine nach seinen Kriterien faire Reihenfolge fest, in der die Gruppen dann untereinander kommunizieren dürfen. Die Reihenfolge

hängt natürlich je nach Wichtigkeit der Gruppen ab und wird vom Koordinator behandelt.

Diese Fragestellung bezieht sich auf die Sicherungsschicht, da sie für die zuverlässige Übertragung von Informationen von einem Teilnehmer zum anderen Teilnehmer zuständig ist.

## **1.5 Kommunikation mit beliebigen Teilnehmern**

Wenn man davon ausgeht das jeder Teilnehmer dieselben Kommunikationsregeln hat, vergibt man jedem Teilnehmer eine eindeutige Adresse. Möchte man nun einen anderen Teilnehmer kontaktieren, muss man die zu übermittelnde Nachricht adressieren. Die beinhaltenden Informationen der Nachricht bestehen aus Sender, Empfänger und Nachricht. Hierbei muss beachtet werden, das bevor man den Kontakt zu einem Teilnehmer aufnehmen möchte, vor Beginn des Spiels eine Kontaktaufnahme erfolgen muss die vom Empfänger bestätigt wird und erst dann kann das Spiel beginnen.

Diese Fragestellung bezieht sich ebenfalls auf die Sicherungsschicht, da sie für die zuverlässige Übertragung von Informationen von einem Teilnehmer zum anderen Teilnehmer zuständig ist.

## **1.6 Kommunikation mit bestimmten Teilnehmern**

Auch hier bekommt jeder Teilnehmer eine **eindeutige** Adresse, wobei diese jedoch noch die Informationen Gebäude-, Raum-, Reihen- und Sitznummer beinhalten. Die Nachricht wird somit anhand dieser ausführlichen Informationen an den jeweiligen Teilnehmer gesendet.

Diese Fragestellung bezieht sich auf die Vermittlungsschicht, da jeder Teilnehmer aufgrund der eindeutigen Adresse mit jedem anderenen (bestimmten) Teilnehmer kommunizieren kann.

## 1.7 Datenfluss Problem

### Problem

Bei einem worst-case-scenario erhält ein spezieller Teilnehmer soviele Informationen von anderen Teilnehmern, das er keinen Platz bzw keine Zeit mehr hat sich die Informationen zu notieren. Folglich gehen dadurch Informationen verloren und diese werden ein weiteres mal an denselben Teilnehmer gesendet, welches das Problem in die Länge zieht.

### Lösung

Um den Informationsfluss zu stoppen oder zu kontrollieren schickt der spezielle Teilnehmer bei Bedarf eine Nachricht an die Teilnehmer das diese entweder langsamer senden sollen oder nur eine bestimmte Anzahl an Informationen senden dürfen. Bleibt das Problem weiterhin bestehen, schickt der spezielle diese Nachricht solange bis der Informationsfluss für ihn verarbeitbar ist. Außerdem können weitere spezielle Teilnehmer eingeteilt werden um den Informationsfluss an mehrere spezielle Teilnehmer zu verteilen und dadurch den Arbeitsaufwand eines speziellen Teilnehmers zu senken.

Diese Fragestellung bezieht sich auf die Transportsschicht, da es sich hierbei um eine Staukontrolle handelt, damit ein Teilnehmer seine Informationsrate zu schicken mindert, wenn das Netz überlastet ist.

## 2 Zuverlässige Datenübertragung

### 2.1 Messung der Häufigkeit von Rahmenverlusten

Jedes mal wenn der Client einen Rahmen sendet erhöht der Server einen Counter für einen empfangenen Rahmen um eins. Nachdem die Übertragung statt gefunden hat, kann der Server nun überprüfen ob es einen Rahmenverlust gab, indem er die Datei aufruft und die Differenz zwischen der Länge der Datei und dem Counter berechnet.

Rahmen insgesamt - Empfangene Rahmen = Verlorene Rahmen.

Wenn die Differenz null beträgt, dann ist kein Rahmenverlust aufgetreten.

### 2.2 Messung der Bitfehlerrate

### 2.3 Vorüberlegungen zum sicheren Protokoll

Um Rahmenverluse und Bitfehler zu kompensieren, gibt es viele Möglichkeiten, wobei folgende Maßnahmen in der zu diesem Parikum zugehörigen Vorlesung und in anderen Vorlesungen wie Verteile Systeme vorgestellt wurden.

1. Die einfachste Möglichkeit ist einen **Timer** bei senden von Daten zu starten, welcher auf der Serverseite implementiert wird. Wenn nach einer bestimmten keine Rückmeldung vom Client empfangen wird, dann schickt der Server dieses Datenpaket noch einmal. Die Rückmeldung ist das Prinzip der Quittungen (Acknowledgements), welche entweder positiv (Datenpaket angekommen) oder negativ (Datenpaket nicht angekommen) sein können.
2. Passend zu dem Prinzip der oben genannten Quittungen, könnte man auch das dazu passende **Stop-and-Wait Protokoll** implementieren. Hierbei darf der Sender nur dann ein Datenpaket senden, wenn er von dem zuvor gesendeten Datenpaket eine Quittung vom Empfänger erhält. Falls die Quittung negativ ist wird das Datenpaket erneut gesendet, ansonsten das nächste Datenpaket welches an der Reihe ist, wie oben schon erwähnt wurde.

3. Um Duplikate zu verhindern kann man **Sequenznummern** verwenden. Wenn z.B. die Quittung vom Empfänger an den Sender verloren geht und dieser nach dem Timeout das Datenpaket erneut sendet, hat der Empfänger redundante Datenpakete. Dieser kann dann anhand der Sequenznummern das er dieses Datenpaket schon empfangen hat, verwirft das zweite redundante Datenpaket und verschickt erneut eine positive Quittung an den Sender.
4. Eine weitere Methode ist es ein **Paritätsbit** (Parity byte) zu verwenden. Dieses Paritätsbit wird an die Bits des Datenpakets angehängt und berechnet sich aus der Summe aller Bits. Wenn die Summe der Bits gerade ist, ist das Paritätsbit "0", ist die Summe jedoch ungerade, ist das Paritätsbit "1". Das Problem mit dem Paritätsbit jedoch ist das Fehler eventuell nicht entdeckt werden. Haben wir zum Beispiel Bytefolge "01000001" ergibt sich das Paritätsbit "0" dafür. Entstehen hier jedoch zum Beispiel zwei Bitfehler wird aus der Bytefolge "10000010", die Bytefolge "10101010" aus dem sich ebenfalls das Paritätsbit "0" berechnen lässt. Allgemein bedeutet das, dass sich eine gerade Anzahl von Fehlern aufhebt und nur eine ungerade Anzahl von Fehlern das Paritätsbit ändert.

## 2.4 Verhinderung von Rahmenverlusten

```

Last login: Sat Dec 26 14:09:49 on ttys000
[Sherazs-MBP:~ Sheraz$ nslookup -q=any fh-luebeck.de
;; Truncated, retrying in TCP mode.
Server:      192.168.178.1          Webserver & IP-Adresse
Address:     192.168.178.1#53

Non-authoritative answer:
fh-luebeck.de
    origin = dns.fh-luebeck.de
    mail addr = herrmann.fh-luebeck.de
    serial = 2015122301
    refresh = 41600
    retry = 1800
    expire = 172800
    minimum = 86400
Name:   fh-luebeck.de
Address: 193.175.120.222
fh-luebeck.de  nameserver = ws-kar1.win-ip.dfn.de.
fh-luebeck.de  mail exchanger = 10 mailin2.fh-luebeck.de.
fh-luebeck.de  mail exchanger = 20 mailin1.fh-luebeck.de. Mailserver zweimal
fh-luebeck.de  text = "v=spf1 ip4:193.175.120.16/28 ip4:193.175.120.87/32 ip4:193.175.120.88/32 ?all"
fh-luebeck.de  nameserver = deneb.dfn.de.
fh-luebeck.de  nameserver = dns.fh-luebeck.de.

```

## 3 Anwendungsschicht und Tools

### 3.1 nslookup tool

(Verwendet wurde das Terminal von einem MacBook Pro mid 2014 mit dem OS El Captian)

Bei dem Befehl **nslookup -q = any fh-luebeck.de** erhält man die IP-Adresse **192.168.178.1** für den Server und ***fh-luebeck.de mail exchanger = 20 mailin1.fh-luebeck.de. und fh-luebeck.de mail exchanger = 10 mailin2.fh-luebeck.de.*** für die Mail Server.

Aufgrund einer Aktualisierung konnte mit dem Befehl **nslookup -q = any fh-luebeck.de 8.8.8.8 / 8.8.4.4** konnte keine Unterschied weder am Macbook noch an den Laborrechnern festgestellt werden. Aus Neugier wurden Informationen bezüglich des Unterschiedes der beiden Anfragen, von Kommilitonen aus dem höheren Semester nachgefragt. Der offensichtliche Unterschied der beiden Anfragen ist, dass beim zweiten Befehl nicht nur der Hostname-Parameter sondern auch der Server-Parameter eingegeben wurde. 8.8.8.8/8.8.4.4 ist ein öffentlich zugänglicher DNS Server von Google, der auch Informationen über die FH-Lübeck gespeichert hat, welche wir dann über diesen öffentlichen DNS Server bekommen.

Wi-Fi: en0 [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
53	13.169.194.000	192.168.178.20	192.168.178.1	DNS	73	Standard query 0x1ae4 ANY fh.luebeck.de
54	13.352034000	192.168.178.1	192.168.178.20	DNS	73	Standard query response 0x1ae4
58	13.354473000	192.168.178.20	192.168.178.1	DNS	99	Standard query 0x1da3 ANY fh.luebeck.de
60	13.650028000	192.168.178.1	192.168.178.20	DNS	369	Standard query response 0x1a3 NS ws-karl.win-ip.dfn.de MX 20 mailin1.fh-luebeck.
65	14.540794000	192.168.178.29	224.0.0.251	MDNS	76	Standard query 0x0000 PTR_difi_tcp.local. "QM" question
167	44.544150000	192.168.178.29	224.0.0.251	MDNS	76	Standard query 0x0000 PTR_difi_tcp.local. "QM" question
243	53.066203000	192.168.178.20	192.168.178.1	DNS	87	Standard query 0xe361 A api-glb-drf.smoot.apple.com
244	53.078001000	192.168.178.20	192.168.178.1	DNS	96	Standard query 0xcbcf7 A plav-cdn.itunes.apple.com.akadns.net

Frame 53: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface ...  
Ethernet II, Src: Apple\_e7/db:bc (3c:15:c2:e7:db:bc), Dst: AvnGmbh\_ce:a4:a3 (34:31:c4:ce:a4:a3)  
Internet Protocol Version 4, Src: 192.168.178.20 (192.168.178.20), Dst: 192.168.178.1 (192.168.178.1)  
Version: 4  
Header Length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))  
Total Length: 59  
Identification: 0xa2e3 (41699)  
Flags: 0x00  
Fragment offset: 0  
Time to live: 64  
Protocol: UDP (17) Protocol: UDP (17)  
Header checksum: 0xf267 [validation disabled]  
Source: 192.168.178.20 (192.168.178.20)  
Destination: 192.168.178.1 (192.168.178.1)  
[Source GeoIP: Unknown]  
[Destination GeoIP: Unknown]  
User Datagram Protocol, Src Port: 54741 (54741), Dst Port: 53 (53)  
Domain Name System (query)

Frame (frame), 73 bytes | Packets: 336 · Displayed: 10 (3.0%) · Dropped: 0 (0.0%) | Profile: Default

Capturing from Wi-Fi: en0 [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply Save

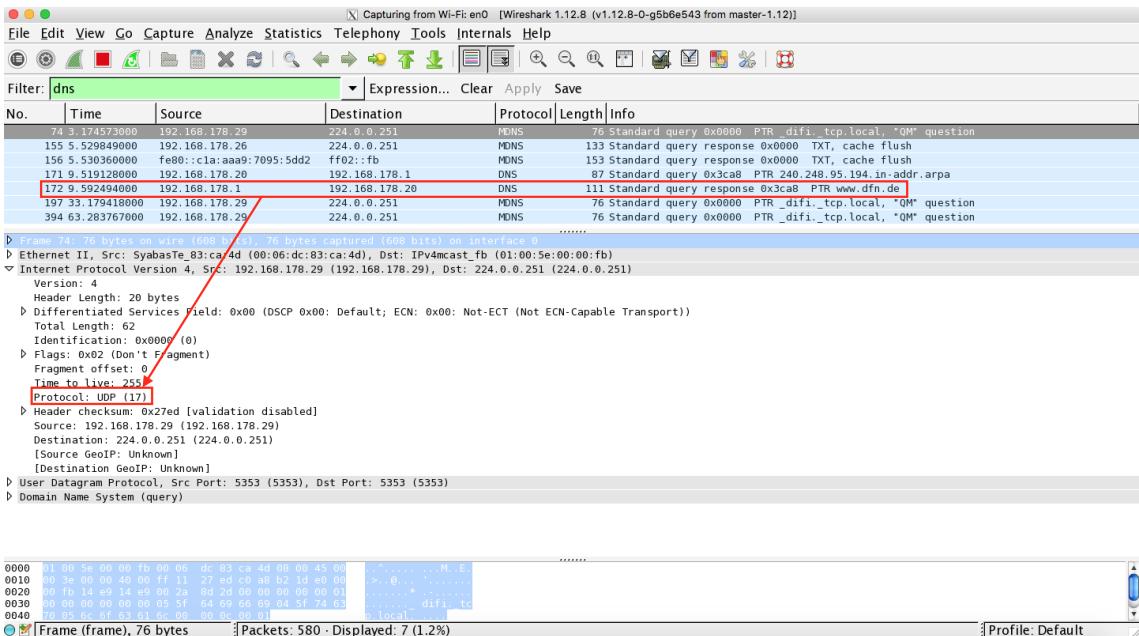
No.	Time	Source	Destination	Protocol	Length	Info
15	9.540733000	192.168.178.29	224.0.0.251	MDNS	76	Standard query 0x0000 PTR_difi_tcp.local. "QM" question
34	15.085930000	192.168.178.20	8.8.8.8	DNS	73	Standard query 0xc3e4 ANY fh.luebeck.de
40	15.630725000	8.8.8.8	192.168.178.20	DNS	343	Standard query response 0xc3e4 SOA dns.fh-luebeck.de TXT MX 20 mailin1.fh-luebeck.d

Frame 15: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface ...  
Ethernet II, Src: Syabaste\_83:ca:4d (00:06:dc:83:ca:4d), Dst: IPv4mcast\_fb (01:00:5e:00:00:fb)  
Internet Protocol Version 4, Src: 192.168.178.29 (192.168.178.29), Dst: 224.0.0.251 (224.0.0.251)  
Version: 4  
Header Length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))  
Total Length: 62  
Identification: 0x0000 (0)  
Flags: 0x02 (Don't Fragment)  
Fragment offset: 0  
Time to live: 255  
Protocol: UDP (17) Protocol: UDP (17)  
Header checksum: 0x27e [validation disabled]  
Source: 192.168.178.29 (192.168.178.29)  
Destination: 224.0.0.251 (224.0.0.251)  
[Source GeoIP: Unknown]  
[Destination GeoIP: Unknown]  
User Datagram Protocol, Src Port: 5353 (5353), Dst Port: 5353 (5353)  
Domain Name System (query)

Frame (frame), 76 bytes | Packets: 162 · Displayed: 3 (1.9%) | Profile: Default

```
[Sheraz-MBP:~ Sheraz$ nslookup -q=any 194.95.248.240
Server:      192.168.178.1
Address:     192.168.178.1#53

Non-authoritative answer:
240.248.95.194.in-addr.arpa      name = www.dfn.de.
```



Hinter der DNS `194.95.248.240` verbirgt sich die Website vom "Deutschen Forschungsnetz" (`www.dfn.de`).

### 3.2 Aufbau von Websites

Beim Aufruf der beiden Webseiten `www.fh-luebeck.de` und `www.t-online.de` mit aktivierten AddOns, wurden bei beiden mittels "IPvFox" Hosts angezeigt die beim Aufruf der Webseiten als Ressourcen mit geladen wurden. Die Liste der Hosts von t-online.de war um ein dreifaches größer als der von fh-luebeck.

Nach und nach werden weitere Skripte mit "NoScript" erlaubt/zugelassen, wobei auf beiden Webseiten nun einige Hosts mehr geladen werden. Außerdem

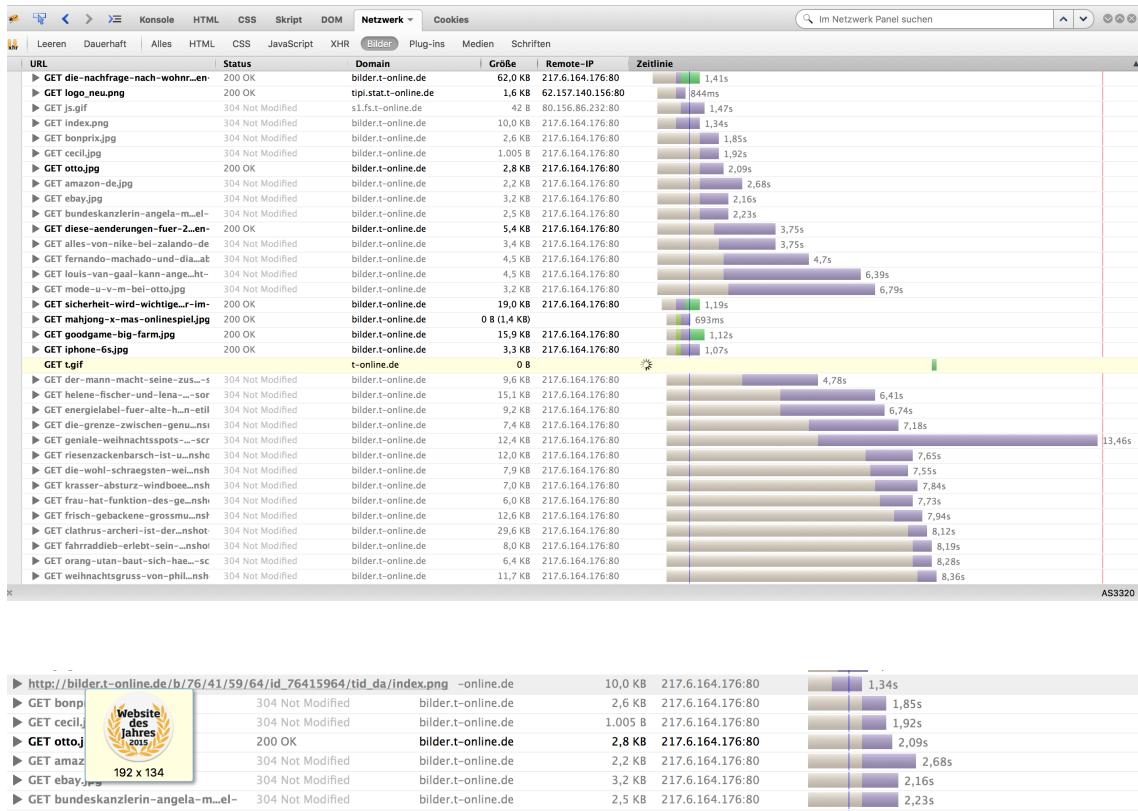


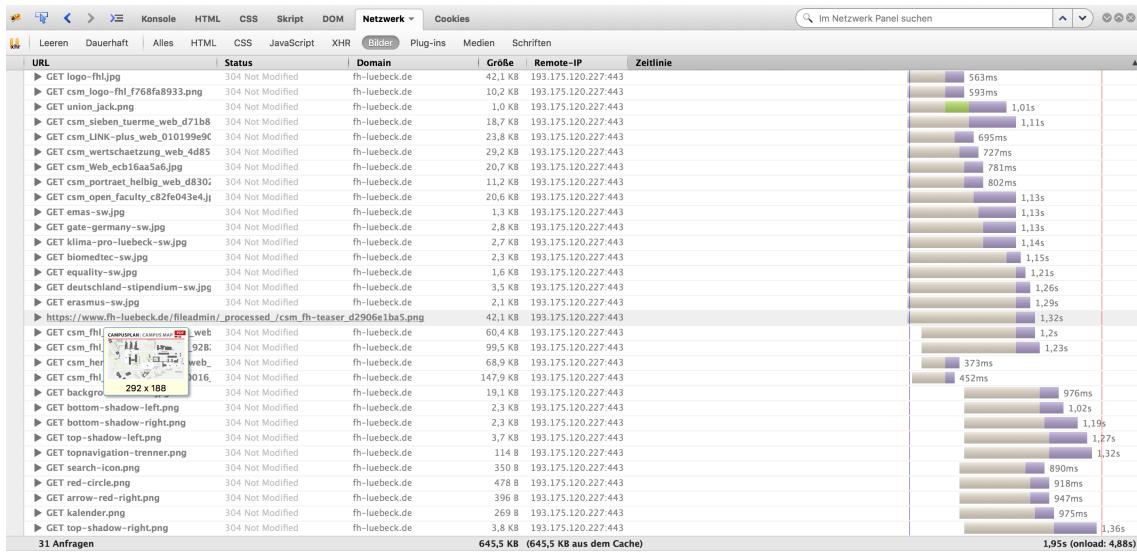
Abbildung 1: T-Online Website des Jahres 2015

haben wir mit *"Ghostery"* beide Websites auf Tracker (Tracker dienen zur Analyse des Surfverhaltens eines Nutzers) untersucht. Auf t-online wurden vierzehn Tracker gefunden, wobei auf fh-luebeck erstaunlicherweise nur ein Tracker gefunden wurde.

### 3.3 Laden von Websites

Bei erneutem Laden der beiden Website, dieses mal mit gestartetem AddOn *"Firebug"*, konnte festgestellt werden, dass es einige Inhalte oder Bilder gibt die t-online oder die fh-luebeck möglichst schnell bzw als erstes geladen haben möchte.

Wie man in der Abbildung 1 sehen kann, möchte T-Online natürlich dieses Bild



vorher laden als, ein Icon auf der unteren Hälfte der Website. Außerdem fällt auf das nachdem die für t-online "wichtigen" Inhalte/Bilder geladen wurden, die Website anfängt Inhalte/Bilder der Werbeagenturen wie (Otto, Bonprix, Ebay, Amazon, etc) zu laden.

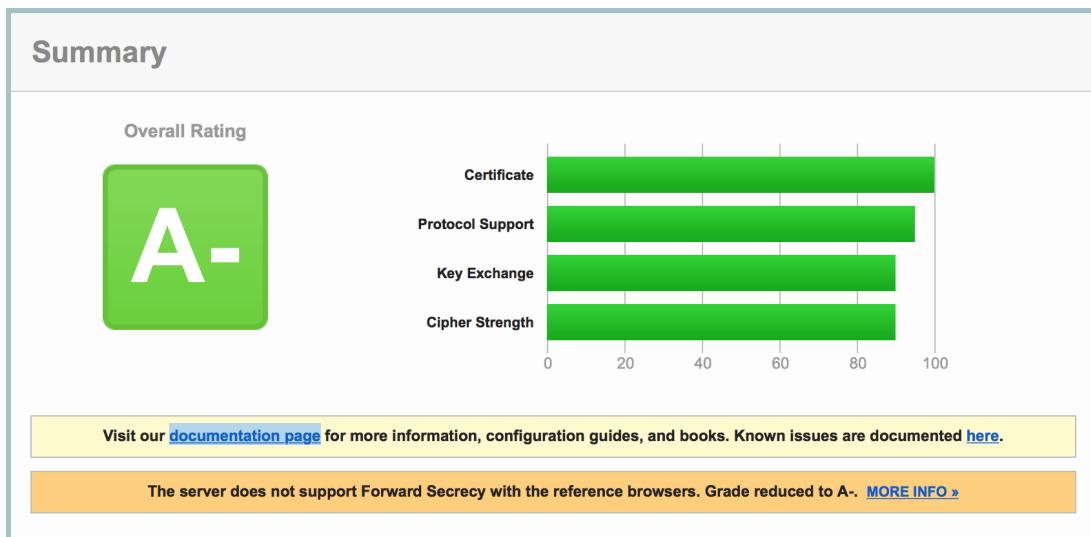
Ähnliches Prinzip finden wir bei der Website [www.fh-luebeck.de](http://www.fh-luebeck.de), hier werden auch erst das Logo und dann die Bilder für die Kategorie "Aktuelles der Fachhochschule Lübeck" geladen. Angesichts dieser Fakten kann man davon ausgehen das beide Websites beim laden Ihrer Inhalte/Bilder Prioritäten setzen, in welcher Reihenfolge was geladen werden soll.

### 3.4 SSL/TLS im Browser

#### HIER DIE ANTWORT VON SVEN NOCH ABWARTEN WAS ER ZU DEM VERGLEICH DER BILDER SAGT

Mit der Website von <https://cc.dcsec.uni-hannover.de/> wurden die Browser Firefox und Safari getestet. Dabei konnte man eindeutig feststellen Außerdem können wir in die Suchleiste von Firefox `about:config` eingeben und so manuell SSL/TLS Einstellungen vornehmen.

## SSL Report: [signin.ebay.de](#) (66.211.181.105)



## 3.5 SSL/TLS beim Server

Mit Hilfe der SSL Tools wurden die Seiten [www.signin.ebay.de](http://www.signin.ebay.de) und [www.banking.haspa.de](http://www.banking.haspa.de) untersucht. Hierbei lieferten beide das Ergebnis "A-", welches ein sehr unerwartetes und entäuschendes Ergebnis ist. Man hatte bei beiden Websites ein Ergebnis von "A++" erwartet, da beide eine Möglichkeit für Online Transaktionen sind. Die Protokolle auf solchen Seiten sollten immer aktuell und im Schnitt "A+" haben.

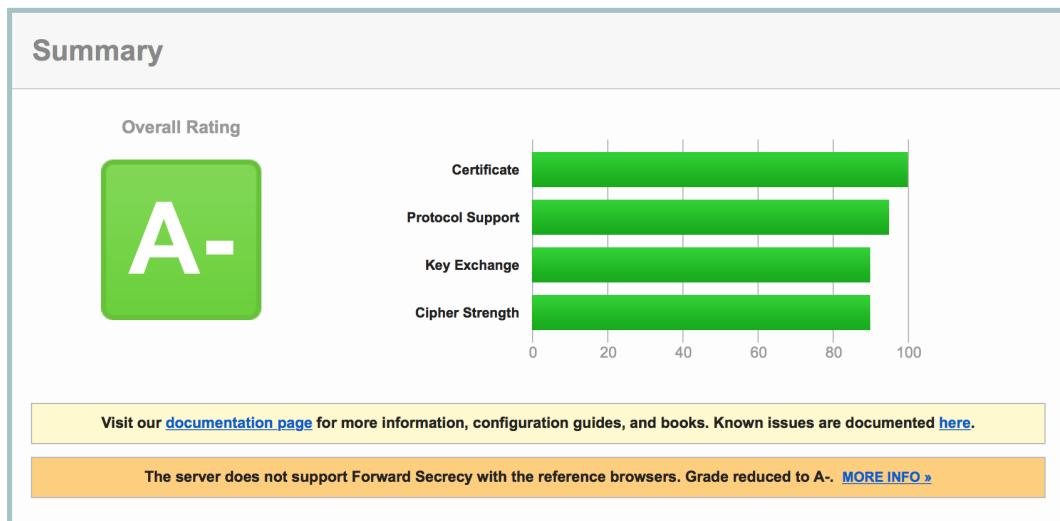
## 3.6 Auswertung von Cookies

Im Laufe des Praktikums haben sich sehr viele Cookies angesammelt, viele davon sind von Drittanbietern die man, wenn man sich davor mit Cookies nie befasst hat, nicht kennt. Es haben sich ca. 80 Cookies angesammelt. Mit "Cookie Monster" kann Einstellungen vornehmen wie einzelne Cookies zu erlauben oder alle/keine Cookies erlauben. Außerdem kann man noch sehen welcher Cookie von welcher Website ist.

## SSL Report: banking.haspa.de (94.126.73.55)

Assessed on: Sat, 26 Dec 2015 18:05:12 UTC | [Clear cache](#)

[Scan Another »](#)



### 3.7 Diskussion AddOns

**Firebug** ist kein gutes AddOn für Netzwerkspezialisten oder Entwickler, aber für einen "normalen" Anwender hat dieses AddOn wenig Sinn.

Fazit: Wir werden dieses AddOn weiterhin **nicht benutzen**.

**No Script** ist ein sehr sinnvolles Tool, da es nicht nur Sicherheit mit sich bringt sondern auch noch die Leistung steigert. Da man durch dieses Tool sinnlose Werbungen und Scripte deaktivieren kann, lädt die Website viel schneller. Jedoch kommt es ab und zu vor das man eine Website besucht und ein bestimmtes Skript verwenden will welches aber von dem Tool blockiert wird, dies ist jedoch kein großes Problem, da man manuell Skripte temporär oder für immer für die Webiste erlauben kann.

Fazit: Da wir vor dem Praktikum schon dieses AddOn kannten und verwendet haben, werden wir es auch in der Zukunft weiterhin **benutzen**.

**Ghostery** dient zum blockieren der Tracker und man hat immer den Überblick über die Tracker, da sie oben rechts auf dem Bildschirm beim laden der Website angezeigt werden.

Fazit: Wir kannten das AddOn vorher nicht und waren sehr beeindruckt und

werden es in der Zukunft **benutzen**.

**CookieMonster** lässt sich sehr einfach bedienen und man kann leicht Cookies ganz oder einzelnd erlauben und verbieten.

Fazit: Auch dieses AddOn war uns zuvor bekannt und wir werden es weiterhin **benutzen**.

**DNSSec Validator** prüft ob eine Website mit DNSSec geschützt ist. Man muss einige Einstellungen vornehmen, bevor man dieses AddOn zum laufen bekommt.

Fazit: Da wir keinen sinnvollen Anwendungsfall im Alltag dafür finden, werden wir dieses AddOn **nicht benutzen**.

### 3.8 Steganographie

Im Bild war die Datei ... enthalten und man konnte mit dem bloßen keinen einzigen Unterschied zwischen den beiden Bildern finden.

**SVEN NOCHMAL FRAGEN WELCHE DATEI DA RAUS KAM  
UND WAS MAN MIT DER HISTOGRAMM FUNKTION GESEHEN HAT**

```

Administrator: Command Prompt - ectpping -server
> ipconfig /release *Con*           name starting with EL
                                         ... release all matching connections
                                         eg. "Wired Ethernet Connection 1" or
                                         "Wired Ethernet Connection 2"
> ipconfig /allcompartments        ... Show information about all
                                         compartments
> ipconfig /allcompartments /all  ... Show detailed information about all
                                         compartments

C:\Users\stud>ipconfig /all
Windows IP Configuration

Host Name . . . . . : adminpc1
Primary Dns Suffix . . . . . :
Netw Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : rnlab.local

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : rnlab.local
Description . . . . . : Intel(R) 82567LF Gigabit Network Connecti
on
Physical Address . . . . . : 00-14-0B-61-61-D2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address . . . . . : 172.16.101.100<Preferred>
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : Monday, November 23, 2015 10:43:53 AM
Lease Expires . . . . . : Thursday, December 30, 2015 9:10:45 PM
Default Gateway . . . . . :
DHCP Server . . . . . : 172.16.100.1
DNS Servers . . . . . : 172.16.100.1
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : fh-luebeck.de
Description . . . . . : Intel(R) WiFi Link 5100 AGN
Physical Address . . . . . : 00-21-5D-31-2F-9C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter isatap.rnlab.local:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : rnlab.local
Description . . . . . : Microsoft ISATAP Adapter #3
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes

C:\Users\stud>ectpping
Usage: ectpping [-?|-h] [-t] [-n count] [-l size] [[-j host-list] | [-k host-lis
t]] [-w timeout] [-S srcaddr] [target-mac] [-server]

Options:
-?|-h      Display this information and exit.
-d          Display all interfaces and exit.
-t          Ping the specified host until stopped.
           To see statistics and continue - type Control-Break;
           To stop - type Control-C.
-i if       Number of interface.
-n count   Number of echo requests to send.
-l size    Send buffer size.
-j host-list Loose source route along host-list <not yet implemented>.
-k host-list Strict source route along host-list <not yet implemented>.
-w timeout Timeout in milliseconds to wait for each reply.

```

## 4 Switch

### 4.1 MAC-Adresse

Die MAC-Adresse wurde mit dem Befehl *ipconfig/all* unter dem Punkt "Physische Adresse" gefunden 4.1. Mittels der Website

<http://standards.ieee.org/regauth/oui/index.shtml> wurde der in Abbildung 2 abgebildete Hersteller gefunden.

00-14-0B (hex)	MA-L	FIRST INTERNATIONAL COMPUTER, INC.	FIC BUILDING, NO.300, YANG GUANG ST., TAIPEI COUNTY 114 TW
00140B			

Abbildung 2: Hersteller

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\stud>ectpping -server
Using [0] Intel(R) 82567LF Gigabit Network Connection <00:14:0b:61:61:d2>
Waiting for ECTP Requests: (Press Ctr-l C to stop)
Request from 04:7d:7b:e7:2b:90: bytes=64
Control-C
```

## 4.2 Beobachtungen im Netz

- a) Die folgenden Befehle wurden auf dem Admin-PC und dem Lab-PC, wie man in der Abbildung sehen kann erfolgreich durchgeführt und mit Wireshark aufgezeichnet.  
**ectpping - mac destination** (Admin-PC)  
**ectpping - server** (Lab-PC)
- b) Um nur die Rahmen der Kommunikation von ectpping herauszufinden, kann man nach dem Protokoll "LOOP" filtern. In diesem Beispiel wird der Ethernet II Rahmentyp verwendet, welches man anhand der Abbildung 2 ablesen kann.
- c) Durch das umstecken der Netzwerkkabel entsteht eine Endschlossschleife. Eine Netzwerküberlastung wird sofort sichtbar, da es keine Regelungen für redundante Pakete gibt. Als Lösung könnte man wie in Versuch 2 schon besprochen Sequenznummern einführen.
- d) **KEINE NOTIZEN DAZU SVEN ODER ANDERE GRUPPE FRAGEN**

## 4.3 Spanning Tree Protocol

- a) Erst wurde die Nachricht *No spanning tree Instance exists* zurückgegeben. Nachdem das Spanning Tree Protocol mit den gegebenen Befehl-

The screenshot shows the Wireshark interface with the following details:

- Panels:** Top bar includes LAN-Verbindung, Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10), File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help.
- Filter Bar:** Filter: loop, Expression..., Clear, Apply, Save.
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info, ...
- Table Data:** 65 rows of network traffic, mostly loopback frames (Frame 50 to Frame 64) between Quantaco and Firstint\_4f:72:07, with various protocols like Ethernet II, ARP, and Configuration Test Protocol.
- Details Panel:** Shows frame 65: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0. It details the Ethernet II frame structure: Src: Quantaco\_e7:28:d7 (00:14:0b:4f:72:07), Dst: Firstint\_4f:72:07 (00:14:0b:4f:72:07), Type: Loopback (0x9000).
- Configuration Test Protocol (Loopback) Section:**
  - Type: Loopback (0x9000)
  - skipCount: 8
  - Function: Forward Data (2)
  - Forwarding address: Firstint\_4f:72:07 (00:14:0b:4f:72:07)
  - Relevant function:
  - Function: Reply (1)
  - Receipt number: 94
- Data (36 bytes) Section:**
  - Data: 00...
  - [Length: 36]
- Bytes Panel:** Hex dump of the data bytes.

```
sw1#show spanning-tree  
No spanning tree instance exists.
```

len eingeschaltet wurde, wurde eine Tabelle zurückgeliefert, welche alle Schnittstellen mit Informationen über ihre Kosten und andere enthielt.

- b) Um Schleifzustände zu vermeiden versetzt der STP die Ports, die zusammen den Spanning Tree bilden, in fünf verschiedene Portzustände. Diese Portzustände werden mittels Timer für jeden Portzustand berechnet. In der Tabelle unten sieht man die fünf Zustände die Ports annehmen können.<sup>1</sup>

Das STP findet redundante Kommunikationswege heraus und ändert die ganze Netzwerktopologie in eine Baumtopologie, die keine Schleifen besitzt. Die Kosten zur Root Bridge sind vier welche man aus der Abbildung 1 entnehmen kann.

- c) Das Team, welches das Kabel zum zentralen Switch entfernt, erhält hö-

<sup>1</sup>[www.airnet.de](http://www.airnet.de)

```

sw1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
              Address     ccef.48d5.d800
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
              Address     ccef.48d5.d800
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi0/1          Desg FWD 4        128.1      P2p
Gi0/2          Desg FWD 4        128.2      P2p
Gi0/3          Desg FWD 4        128.3      P2p

sw1#

```

Portzustand	Beschreibung
Disabled	Administrativer shutdown
Listening	Horchen auf BPDU-Pakete oder versenden von BPDU-Paketen
Learning	Listening-Funktions und lernen von Quell-MAC-Adressen
Forwarding	Listening- und Learning-Funktion und weiterleiten von Datenframes
Blockeing	Horchen auf BPDU-Pakete

Tabelle 2: Prozesstabelle (BPDU-Pakete sind spezielle Pakete die Switches senden können)

```

sw1#show mac address-table aging-time
Global Aging Time: 300
Vlan   Aging Time
----  -----

```

here Kosten. Der Grund dafür ist, das dieser sich nun erst über einen anderen Switch verbinden muss um eine Verbindung zum Switch 0 herzustellen.

- d) **IST BEI UNS HIER EINE SCHLEIFE ENTSTANDEN ODER KAM HIER DASSELBE RAUS WIE ICH ES SCHON IN AUFGABE 5 b ERWÄHNT HABE ?**
- e) Typische Informationen vom STP sind:

- MAX Age
- Hello Time
- Forward Delay

Wobei die STP-Rahmen folgende Schichten beinhalten:

**ICH HABE KEINE NOTIZEN ZU DEN RAHMEN** (war damit gemeint das mit längen und typ feld ? oder ist damit gemeint welche Tabs angezeigt werden ? das kann man aus den Bildern von Wireshark entnehmen) SONST WIEDER JEMANDEN FRAGEN

#### 4.4 Lernen von Adressen für die MAC-Adresstabelle

- a) In einem Intervall von 300 s sind erneuerungen der Adressen notwendig, wie man in der Abbildung unten sehen kann.
- b) Die Einträge waren in sehr kurzer Zeit wieder in der Tabelle eingetragen. Da wir in einem vorhandenem Netzwerk sind und die Switch (wie

The screenshot shows two terminal windows and one Wireshark capture window. The left terminal window is titled 'COM1-PUTTY' and displays the configuration of interface GigabitEthernet0/9, changing its state from down to up. The right terminal window is titled '(v10.8 from master-1.10)' and shows the configuration of interface GigabitEthernet0/1, also changing its state from down to up. The bottom terminal window shows the MAC address table for both interfaces, listing various dynamically learned MAC addresses and their associated ports.

```

COM1-PUTTY
Nov 30 14:24:16 336: %LINK-3-UPDOWN: Line protocol on interface GigabitEthernet0/9, changed state to up
sw1
Nov 30 14:27:16 338: %LINK-3-UPDOWN: Line protocol on interface GigabitEthernet0/1, changed state to down
sw1
Nov 30 14:27:16 345: %LINK-3-UPDOWN: Interface GigabitEthernet0/9, changed state to down
sw1
Nov 30 14:27:19 224: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
sw1
show mac address-table dynamic
Mac Address Table
Vlan Mac Address Type Ports
---+---+---+---+
1 0001.0512.eb84 DYNAMIC G10/24
1 047d.7be7.2998 DYNAMIC G10/24
1 5475.40e2.9f81 DYNAMIC G10/24
1 5473.4443.4f81 DYNAMIC G10/24
1 f866.7288.4192 DYNAMIC G10/24
Total Mac Addresses for this criterion: 5
sw1
show mac address-table dynamic
Mac Address Table
Vlan Mac Address Type Ports
---+---+---+---+
1 047d.7be7.2998 DYNAMIC G10/24
1 4443.4f81.5c00 DYNAMIC G10/24
1 5475.40e2.9f81 DYNAMIC G10/24
1 5473.4443.4f81 DYNAMIC G10/24
1 f866.7288.4192 DYNAMIC G10/24
Total Mac Addresses for this criterion: 5
sw1
show mac address-table dynamic
Mac Address Table
Vlan Mac Address Type Ports
---+---+---+---+
1 0001.0512.eb84 DYNAMIC G10/24
1 047d.7be7.2998 DYNAMIC G10/24
1 5475.40e2.9f81 DYNAMIC G10/24
1 5473.4443.4f81 DYNAMIC G10/24
1 f866.7288.4192 DYNAMIC G10/24
Total Mac Addresses for this criterion: 5
sw1

```

wir in der Vorlesung gelernt haben) selbstlernend (self-learning) ist, speichert diese Einträge selbstständig in die Tabelle. Die Einträge beinhalten folgende Informationen, die MAC-Adresse, die aktuelle Zeit und die Schnittstelle über die der Rahmen eingetroffen ist.

- c) Durch den Broadcast an andere unbekannte Ziele, hat die Adresstabell weitere "DYNAMIC" Einträge dazu bekommen, weil der Switch diese Adressen schnell dazu gelernt hat.
- d) Während beim fortlaufenden ectrapping der Port abgezogen wurde, kam die Meldung "*Request Timed out*" für ca. 10 s, danach jedoch ging es "normal" weiter. Wie schon in den Aufgaben davor besprochen lässt sich dieses Verhalten durch das selbstlernen des Switches erklären. Beim Umstecken der Ports hat Wireshark angezeigt das, dass STP aktiviert wurde.
- e) Die Quelladresse lässt sich sehr leicht manipulieren ist jedoch zwiespältig zu beurteilen. Aus Sicht des Senders ist eine gute Möglichkeit sich als jemand anderes auszugeben, doch aus Sicht des Empfängers ist es sehr gefährlich, da wenn als Sicherheitsmaßnahme nur die Gültigkeit der MAC-Adresse überprüft wird, jede Anfrage von einem x beliebigen System angenommen werden könnte. Ein Beispiel dazu wäre wenn Gruppe 1 Ihre Quelladresse auf die von Gruppe 3 ändern würde, würde Gruppe 1 Daten von Gruppe 4 erhalten ohne das diese bemerkt das die Daten an uns gesendet wurden.

## **4.5 Erstellen eines VLANs mit der Nummer 100.**

- a) Der Bereich zwischen den Ports 13-18 ist nun unabhängig von den anderen.
- b) Die Kommunikation zwischen dem VLAN 100 und dem Default Bereich ist möglich, wenn die Kabelenden an den jeweiligen Bereichen eingesteckt sind.
- c) Es sind nun weitere Einträge in der Tabelle verzeichnet worden. Das VLAN und der Verbindungspunkt sind in der Tabelle eingetragen, außerdem wird angezeigt dass dieser Switch die Root Bridge im VLAN 100 ist. Dieser VLAN hat nun seinen eigenen Spanning-Tree und die Ports von 13-18 sind nun für die anderen nicht mehr erreichbar.
- d) **KEINE NOTIZEN DAZU JEMAND ANDEREN FRAGEN ODER SVEN**

## **4.6 VLAN-Trunk-Konfiguration**

- a) Einstellungen vorgenommen.
- b) Das "Trunking" auf dem Interface *gigabitEthernet 0/15* ist aktiviert und erlaubt.
- c) Die VLAN Tags die gefundenen enthielten folgende Informationen:
  - Priority
  - CFI
  - ID
  - Ethernet Type/Length
- d) Die Erreichbarkeit bleibt weiterhin behalten, jedoch haben sich die Portzustände bei einigen anderen Gruppen geändert.

```

sw1(config-if-range)#switchport access vlan 100
% Access VLAN does not exist. Creating VLAN 100
sw1(config-if-range)#enfd
          ^
% Invalid input detected at '^' marker.

sw1(config-if-range)#end
sw1#sh
Nov 30 14:40:42.813: %SYS-5-CONFIG_I: Configured from console by console
sw1#show vlan

VLAN Name                               Status    Ports
---- -----
1   default                             active    Gi0/1, Gi0/2, Gi0/3, Gi0/
4
8
0/12
i0/22
100 VLAN0100                           active    Gi0/23, Gi0/24
i0/16
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Transl T
rans2
---- -----
1   enet    100001   1500   -     -     -     -     -     0     0
100  enet    100100   1500   -     -     -     -     -     0     0
1002 fddi    101002   1500   -     -     -     -     -     0     0
1003 tr     101003   1500   -     -     -     -     -     0     0
1004 fdnet   101004   1500   -     -     -     ieee  -     0     0
1005 trnet   101005   1500   -     -     -     ibm  -     0     0

--More-- 

```

```
sw1#enable
sw1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
sw1(config)#interface gigabitEthernet 0/15
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
sw1(config-if)#end
sw1#
Nov 30 14:56:31.747: %SYS-5-CONFIG_I: Configured from console by console
sw1#show interfaces gigabitEthernet 0/15 switchport
Name: Gi0/15
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 100 (VLAN0100)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

- e) Um ein VLAN 200 zu konstruieren welches nur die LABPCs aller Teams vertritt, muss man nichts am "Trunking" verändern, weil diese automatisch generiert werden.

## **5 Router**

## **6 Transportschicht**