

# Praktikum Rechnernetze

Protokoll zu Versuch 2 (Protokollanalyse mit Wireshark) von  
Gruppe 1

---

Jakob Waibel    Daniel Hiller    Elia Wüstner    Felix Pojtinger

2021-10-19

# Einführung

---

Diese Materialien basieren auf Professor Kiefers "Praktikum Rechnernetze"-Vorlesung der HdM Stuttgart.

**Sie haben einen Fehler gefunden oder haben einen Verbesserungsvorschlag?** Bitte eröffnen Sie ein Issue auf GitHub ([github.com/pojntfx/uni-netpractice-notes](https://github.com/pojntfx/uni-netpractice-notes)):



**Abbildung 1:** QR-Code zum Quelltext auf GitHub

# Lizenz

Dieses Dokument und der enthaltene Quelltext ist freie Kultur bzw. freie Software.



**Abbildung 2:** Badge der AGPL-3.0-Lizenz

Uni Network Practice Notes (c) 2021 Jakob Waibel, Daniel Hiller,  
Elia Wüstner, Felix Pojtinger

SPDX-License-Identifier: AGPL-3.0

# Wireshark

---

# Einführung

**An welchem Koppelement im Systemschrank sollte der Hardware-Analysator/Netzwerk-Sniffer sinnvollerweise angeschlossen werden und warum? Welche grundsätzlichen Möglichkeiten gibt es noch?**

- Switch, damit Nachrichten auf Layer 2 auch abgefangen werden können
- Grundsätzlich könnte, vor allem auch in Heimnetzwerken, der Router hierzu verwendet werden, da hier oft Router und Switch zu einem Gerät kombiniert sind.

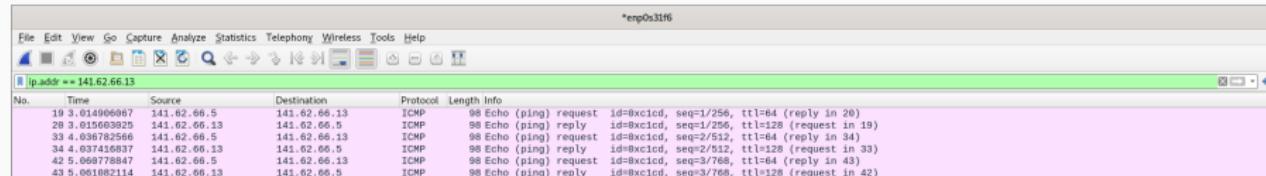
**Starten Sie Wireshark und capturern Sie den aktuellen Traffic. Dokumentieren Sie zunächst, was alles auf Wireshark einprasselt.**



# Ping

Senden Sie einen Ping zu nachfolgenden Empfängern und zeichnen Sie die entsprechenden Protokolle gezielt mit Wireshark auf. Vergleichen Sie die Protokollabläufe: wer sendet welches Protokoll warum an wen? Pingen Sie an . . . .

Einen Rechner Ihrer Wahl im Labornetz:



The screenshot shows a Wireshark interface with the title bar "eng0:31f6". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help. A search bar at the top has the filter "ip.addr == 141.62.66.13". Below the menu is a toolbar with icons for file operations, zoom, and selection. The main window displays a list of network packets. The columns are: No., Time, Source, Destination, Protocol, Length, Info. The table data is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
19	3.014906067	141.62.66.5	141.62.66.13	ICMP	98	Echo (ping) request id=0xc1cd, seq=1/256, ttl=64 (reply in 20)
29	3.015693825	141.62.66.13	141.62.66.5	ICMP	98	Echo (ping) reply id=0xc1cd, seq=1/256, ttl=128 (request in 19)
33	4.036782566	141.62.66.13	141.62.66.13	ICMP	98	Echo (ping) request id=0xc1cd, seq=2/512, ttl=64 (reply in 34)
34	4.037416837	141.62.66.13	141.62.66.5	ICMP	98	Echo (ping) reply id=0xc1cd, seq=2/512, ttl=128 (request in 33)
42	5.068778847	141.62.66.5	141.62.66.13	ICMP	98	Echo (ping) request id=0xc1cd, seq=3/768, ttl=64 (reply in 43)
43	5.061982114	141.62.66.13	141.62.66.5	ICMP	98	Echo (ping) reply id=0xc1cd, seq=3/768, ttl=128 (request in 42)

# DHCP

**Analysieren Sie die Abläufe bei DHCP (im Labor installiert).  
Ihre Teilgruppe am Nachbartisch bootet den PC am Arbeitsplatz, protokollieren Sie die DHCP-Abläufe sowie sonstigen Netzverkehr, den der PC bis zum Erhalt der IP-Adresse erzeugt.**

Während des Startens werden drei DHCP-Requests für verschiedene Komponenten abgehandelt.

No.	Time	Source	Destination	Protocol	Length	Info
47	36.248724335	0.0.0.0	255.255.255.255	DHCP	59	DHCP Discover - Transaction ID 0x620e53eb
48	36.248844227	opnsense-router.rml...	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0x620e53eb
55	49.259252520	0.0.0.0	255.255.255.255	DHCP	598	DHCP Request - Transaction ID 0x620e53eb
56	49.259252529	opnsense-router.rml...	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0x620e53eb
57	49.259797973	linux.local	Broadcast	ARP	60	Who has 141.62.66.236? Tell 141.62.66.4
58	49.278416173	linux.local	Broadcast	ARP	60	Who has 141.62.66.250? Tell 141.62.66.4
63	49.476659439	fog.rnlabor.hds-stu...	linux.local	ARP	60	Who has 141.62.66.4? Tell 141.62.66.236
65	49.52657513	fog.rnlabor.hds-stu...	linux.local	ARP	60	Who has 141.62.66.4? Tell 141.62.66.236
79	49.526653895	fog.rnlabor.hds-stu...	linux.local	ARP	60	Who has 141.62.66.4? Tell 141.62.66.236
72	49.47126304	0.0.0.0	255.255.255.255	DHCP	451	DHCP Discover - Transaction ID 0xc1470931
73	49.471263275	opnsense-router.rml...	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0xc1470931
79	49.526519769	0.0.0.0	255.255.255.255	DHCP	343	DHCP Request - Transaction ID 0xc1470931
88	50.531124982	opnsense-router.rml...	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0xc1470931
81	50.531125138	linux.local	Broadcast	ARP	60	ARP Announcement for 141.62.66.4
82	50.584564928	linux.local	Broadcast	ARP	60	Who has 141.62.66.236? Tell 141.62.66.4
85	54.826519700	linux.local	Broadcast	ARP	60	Who has 141.62.66.236? Tell 141.62.66.4
92	66.340215769	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xadc0bd5d8
93	66.342356749	0.0.0.0	255.255.255.255	DHCP	345	DHCP Request - Transaction ID 0xadc0bd5d8
95	66.629416649	linux.local	Broadcast	ARP	60	Who has 141.62.66.250? Tell 141.62.66.4

**Abbildung 9:** Gesamter Bootprozess

## Dokumentieren Sie den Ablauf bei einer DNS-Abfrage

### Fall 1: DNS-Server 141.62.66.250:

Mittels folgendem Command wurde eine DNS-Abfrage gemacht:

```
$ dig @141.62.66.250 google.com  
google.com.      163 IN  A    142.250.186.174
```

No.	Time	Source	Destination	Protocol	Length	Info
11	1.357358800	rn05.rn1abor.hdm-st... opnsense-router.rnL	DNS	93	Standard query 0xa276	A google.com OPT
12	1.371050270	opnsense-router.rnL	rn05.rn1abor.hdm-ST...	DNS	97	Standard query Response 0xa276 A google.com A 142.250.186.174 OPT

**Abbildung 12:** Ablauf der Anfrage

Hier nutzten wir den internen DNS Server und machen eine Anfrage auf google.com.

### Fall 2: DNS-Server 1.1.1.1 (Cloudflare):

Mittels folgendem Command wurde eine DNS-Abfrage gemacht:

## Lösen Sie eine ARP-Anfrage aus und protokollieren Sie die Datenpakete.

Hierzu wurde ein Rechner, welcher zuvor nicht im lokalen ARP-Cache war, neu gestartet.

Ats	Time	src	Dest	Type	Protocol	Length	Info
214	110.5158670211	linux-2.local	broadcast	ARP	00:0c:29:00:00:00	141.62.66.6 is who has 141.62.66.6? Tell 141.62.66.5	
215	110.5158672088	linux-3.local	linux-2.local	ARP	00:14:16:62:66:06	00:14:16:62:66:06 is at 4c:52:0e:54:2b	
231	115.0731647395	linux-3.local	linux-2.local	ARP	00:0c:29:00:00:00	00:0c:29:00:00:00 who has 141.62.66.5? Tell 141.62.66.6	
232	115.073180788	linux-2.local	linux-3.local	ARP	42:14:16:62:66:05	42:14:16:62:66:05 is at 4c:52:0e:54:8b	

Abbildung 15: Ablauf der Anfrage

## Wann wird eine ARP-Anfrage gestartet?

Sobald ein Paket an die Zieladresse (in unserem Fall 141.62.66.6) gesendet werden soll, wird eine ARP-Anfrage in Form eines Broadcasts gestartet, um das Zielgerät im Netzwerk zu ermitteln, sofern sich diese nicht bereits im ARP-Cache befindet. Dieser kann mit ip neigh show ausgelesen werden. Mit ip neigh flush all

## Layer-2-Protokolle

**Gelegentlich werden vom Analyzer Broadcasts erkannt. Wer sendet sie, warum und in welchen zeitlichen Abständen?**

Die Broadcasts sind ARP-Requests. Sie entstehen dadurch, da Geräte versuchen Daten an andere Geräte zu übertragen, für welche sie keinen Eintrag in ihrem ARP-Cache haben, deshalb muss eine ARP-Anfrage in Form eines Broadcasts gesendet werden, da jeder Host potenziell der gesuchte Host sein kann. Dieser besitzt gesuchte IP X und antwortet daraufhin mit seiner Mac.

No.	Time	Source	Destination	Protocol	Length Info
178	1993-07-23T06:48:00.000Z	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
178	1993-07-23T06:48:00.000Z	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
<b>175 72 .8867515887</b>	<b>Linux-3.local</b>	<b>224.0.0.251</b>	<b>MHDN</b>	<b>82 Standard query @0x8000 PTR _opkey-hkp._tcp.local. "Qn" question</b>	
178	1993-07-23T06:48:00.000Z	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
178	1993-07-23T06:48:00.000Z	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
178	1993-07-23T06:48:00.000Z	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
179	1993-07-23T06:48:00.000Z	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
181	1993-07-23T06:48:00.000Z	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
182	84.699546741	Librennes-226.rnlabor.de	Broadcast	ARP	60 Who has 141.62.66.29? Tell 141.62.66.29
183	84.731177897	Librennes-226.rnlabor.de	Broadcast	ARP	60 Who has 141.62.66.29? Tell 141.62.66.29
184	85.674657721	Librennes-226.rnlabor.de	Broadcast	ARP	60 Who has 141.62.66.29? Tell 141.62.66.29
185	85.674657721	Librennes-226.rnlabor.de	Broadcast	ARP	60 Who has 141.62.66.29? Tell 141.62.66.29
186	85.954876527	Linux-2.local	opensec_rnlabor.hds	DNS	86 Standard query @0x9e2a PTR 226.66.62.141.in-addr.arpa
187	85.956236998	opensec_rnlabor.hds	Linux-2.local	DNS	137 Standard query response 0x9e2a PTR 226.66.62.141.in-addr.arpa PTR Librennes-226.rnlabor.hdm-stuttgart.de
188	86.721457449	Librennes-226.rnlabor.de	Broadcast	ARP	60 Who has 141.62.66.29? Tell 141.62.66.29
189	86.758478381	Librennes-226.rnlabor.de	Broadcast	ARP	60 Who has 141.62.66.29? Tell 141.62.66.29
191	87.899791212	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/9/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
192	88.627049588	Linux-3.local	224.0.0.251	MHDN	81 Standard query @0x8000 PTR _newa_0183._tcp.local. "Qn" question
193	88.627049588	Linux-3.local	224.0.0.251	MHDN	81 Standard query @0x8000 PTR _newa_0183._tcp.local. "Qn" question
194	89.667590484	Linux-2.local	opensec_rnlabor.hds	DNS	42 Who has 141.62.66.29? Tell 341.62.66.5
195	91.899717208	opensec_rnlabor.hds	Linux-2.local	ARP	60 141.62.66.29 is at 00:00:09:f1:b8:14
197	93.886571335	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
198	95.899796112	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002
199	95.899796112	NewlettPc_as-80-be	Spanning-tree-(For...)	STP	119 MST Root = 32768/8/0/0.1a:c1:Se0/0:0 Cost = 228020 Port = 8x8002

# HTTP und TCP

**Initiiieren Sie eine HTTP-TCP-Sitzung (beliebige Website) und zeichnen Sie die Protokollabläufe auf**

Zuerst wird eine DNS-Request getätigt. Daraufhin folgt der 3-Way-Handshake.

**TODO:** Add valid image

**Können Sie den 3-Way-Handshake erkennen? Markieren Sie ihn in der Dokumentation. Welche TCP-Optionen sind beim Handshake aktiviert und welche Bedeutung haben sie?**

**TODO:** Add valid image

**TODO:** Add valid image

**TODO:** Add valid image

**TODO:** Add valid image

## Wie lauten die MAC-Adressen der im Labor befindlichen Ethernet-Switches? Wie haben Sie die Switches identifizieren können. Welche Möglichkeiten der Identifizierung gibt es?

Beim Spanning-Tree-Protocol lässt sich sehen, dass die Quelle der Nachrichten immer ein HP-Gerät ist. Dieses muss ein fähiges Kopplungselement des Netzwerkes sein, welches das Spanning-Tree-Protocol unterstützt. Daher wird dies mit hoher Wahrscheinlichkeit der Ethernet-Switch sein.

**MAC-Adresse:** 04:09:73:aa:8b:be

No.	Time	Source	Destination	Protocol	Length	Info
170	63. 999710934	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
171	65. 999832879	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
172	67. 999832879	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
173	70. 999817336	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
174	71. 999817336	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
178	72. 999729543	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
177	73. 999729543	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
178	74. 999729543	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
179	75. 999806699	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
178	76. 999806699	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
179	77. 999806699	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
180	78. 999806699	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
181	80. 999802388	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
182	83. 999531792	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
183	84. 999531792	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
191	87. 999710912	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
187	88. 999807785	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
198	91. 9998034042	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
199	93. 9998071526	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
197	94. 9998071526	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
206	97. 9995306051	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
201	100. 9800216873	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
203	103. 9800216873	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
204	103. 999772305	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
205	103. 999772305	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
212	108. 9800240970	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002
213	108. 999891429	HewlettPc_aa:bb:be	Spanning-tree-(For-)	STP	119	MST. Root = 32768/0/08:1a:c1:5e:eb:c0 Cost = 220020 Port = 0x8002

## Filtern Sie auf das Protokoll BPDU/STP. Wer sendet es und welchen Sinn hat dieses Protokoll?

Das STP-Protokoll ist das Spanning Tree Protocol. Das STP-Protokoll verhindert Schleifenbildung; dies ist besonders dann von Nutzen, wenn Redundanzen vorhanden sind. Beim STP-Protokoll werden durch alle am Netz beteiligten Switches eine "Root Bridge" gewählt und redundante Links werden deaktiviert. Wie anhand der OUI der MAC-Adresse erkannt werden kann wird dieses hier von einem HP-Switch verwendet.

No.	Time	Source	Destination	Protocol	Length	Info
393 102.000115680	HeuvelTP.an.Bb:be	Spanning-tree-(For-	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
394 104.000105982	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
395 106.000056817	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
397 109.000202936	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
398 110.000202937	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
406 192.000560847	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
407 194.000877110	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
408 196.000399860	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
411 200.000399861	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
412 208.000287489	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
413 292.000187163	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
417 204.000254351	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
418 206.000015959	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
420 210.000015960	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
424 218.000028987	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
425 212.000027773	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
426 214.000080847	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
427 216.000078690	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
428 218.000078691	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
430 720.000140895	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002
433 222.000177264	HeuvelTP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:cl:Se:eb:c9	Cost = 226029	Port = 0x80002

# SNMP

**Auf welchen Komponenten im Netzwerk wird das Protokoll SNMP ausgeführt?**

Es konnte kein SNMP-Traffic im Netzwerk gefunden werden. SNMP, das Simple Network Management Protocol, wird jedoch meist zur Wartung von verbundenen Geräte im Network verwendet, woraus sich schließen lässt, dass es auf Komponenten wie Switches, Routern oder Servern zum Einsatz kommen würde.

# Streaming and Downloads

**Starten Sie einen Download einer größeren Datei aus dem Internet und stoppen Sie ihn während der Übertragung. Dokumentieren Sie, wie der Stop-Befehl innerhalb der Protokolle umgesetzt wird**

**Abbildung 25:** Capture beim Canceln des eines Downloads über HTTPS

Da der Download hier via HTTPS durchgeführt wurde, kann erkannt werden, dass die darunterliegende TCP-Verbindung unterbrochen wurde, indem die RST-Flag gesetzt wurde. Auch ein TCP Segment mit der Ziel-IP 192.168.1.100 und der FIN- und ACK-Flag gesetzt.

# Telnet und SSH

Protokollieren Sie den Ablauf einer TELNET-Verbindung zur IP-Adresse 141.62.66.207 (login: praktikum; passwd: versuch). Können Sie Passwörter im Wireshark-Trace identifizieren? Wie verhält sich im Vergleich dazu eine SSH-Verbindung zum gleichen Server?

Wie zu erkennen ist, wird für eine Telnet-Verbindung eine TCP-Verbindung aufgebaut. Die Passwörter sind zu erkennen.

No.	Time	Source	Destination	Protocol	Length	Info
53	13.371899779	141.62.66.5	141.62.66.207	TELNET	69	Telnet Data ...
55	13.371964177	141.62.66.207	141.62.66.5	TELNET	69	Telnet Data ...
57	13.372108043	141.62.66.5	141.62.66.207	TELNET	69	Telnet Data ...
59	13.372108043	141.62.66.5	141.62.66.207	TELNET	69	Telnet Data ...
61	13.372108043	141.62.66.5	141.62.66.207	TELNET	69	Telnet Data ...
65	15.536484921	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
67	15.537358875	141.62.66.207	141.62.66.5	TELNET	67	Telnet Data ...
69	15.5374246784	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
71	15.5374389817	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
73	15.784452662	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
74	15.784992429	141.62.66.207	141.62.66.5	TELNET	67	Telnet Data ...
76	15.864385854	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
77	15.865698282	141.62.66.207	141.62.66.5	TELNET	67	Telnet Data ...
79	15.992584487	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
80	15.992584487	141.62.66.207	141.62.66.5	TELNET	67	Telnet Data ...
82	16.056366088	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
83	16.057270317	141.62.66.207	141.62.66.5	TELNET	67	Telnet Data ...
86	16.178463143	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
87	16.17846417	141.62.66.207	141.62.66.5	TELNET	67	Telnet Data ...
89	16.44425668	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
90	16.45301998	141.62.66.207	141.62.66.5	TELNET	67	Telnet Data ...

Frame 61: 88 bytes on wire (648 bits), 88 bytes captured (648 bits) on interface enp3s0f0, id = 0

Ethernet II, Src: rnlabor (62:39:f6:7b:b8:87) [eth0], Dst: rn6.rnlabor.hdm-stuttgart.de (4c:52:82:0e:54:8b)

Internet Protocol Version 4, Src: 141.62.66.207, Dst: 141.62.66.5

Transmission Control Protocol, Src Port: 23, Dst Port: 30234, Seq: 78, Ack: 163, Len: 14

Telnet

Data: telnet login:

# Wireshark-Filter

Entwickeln, testen und dokumentieren Sie Wireshark-Filter zur Lösung folgender Aufgaben:

Nur IP-Pakete, deren TTL größer ist als ein von Ihnen sinnvoll gewählter Referenzwert

No.	TTL	Time	Source	Destination	Protocol	Length	Info
25	255	1.444955667	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
26	255	1.444955673	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
31	255	1.451973372	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
89	255	1.498643116	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
98	255	1.3.50059800	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
112	255	1.4.35439355	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
120	255	1.4.35439357	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
1527	255	1.21.51668853	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
1567	255	1.21.65419641	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2831	255	1.25.443188947	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2844	255	1.25.456619749	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2850	255	1.25.456619750	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2849	255	1.25.509882269	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2858	255	1.25.509882265	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2851	255	1.25.509882264	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2852	255	1.25.509882265	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
11948	255	1.451373620	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QU" quest.
12818	255	75.507569660	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.
12561	255	78.567487619	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.
13269	255	87.681387937	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.
18851	255	1.134.49841999	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
18852	255	1.134.49841999	100.64.154.254	felixx-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
19848	255	340.929138747	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QU" quest.
19852	255	141.955810993	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.
23834	255	144.924217109	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.
21865	255	154.339292308	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.
21390	255	172.657443368	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.
22148	255	158.6574338164	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.
22784	255	167.657466409	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.
22852	255	168.579565631	100.64.154.245	224.0.0.251	MDNS	198	Standard query 0x0000 PTR lb_.dns-sd._udp.local. "QM" question PTR companion-link._tcp.local. "QM" quest.

Abbildung 31: Capture der TTL-Werte ab 200

Der Linux-Kernel stellt standardmäßig die TTL auf 64; hier wurde ab 200 gefiltert, damit ausschließlich „ungewöhnliche“ Pakete wie