

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):



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.**

TODO: Add descriptions

No.	Time	Source	Destination	Protocol	Length	Info
47	36.248724335	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x6269e53eb
48	36.248724327	openSense-router.rml...	255.255.255.255	DHCP	348	DHCP Offer - Transaction ID 0x6269e53eb
55	46.250854243	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0x6269e53eb
56	48.2598518738	openSense-router.rml...	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0x6269e53eb
57	48.259797973	linux.local	Broadcast	ARP	60	Who has 141.62.66.236? Tell 141.62.66.4
58	48.278416173	linux.local	Broadcast	ARP	60	Who has 141.62.66.250? Tell 141.62.66.4
63	45.478669439	fog.rnlabor.hds-stu...	linux.local	ARP	60	Who has 141.62.66.47 Tell 141.62.66.236
65	46.582657513	fog.rnlabor.hds-stu...	linux.local	ARP	60	Who has 141.62.66.47 Tell 141.62.66.236
79	47.526653895	fog.rnlabor.hds-stu...	linux.local	ARP	60	Who has 141.62.66.47 Tell 141.62.66.236
72	48.259851873	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover - Transaction ID 0xc1478931
73	48.498452075	openSense-router.rml...	255.255.255.255	DHCP	348	DHCP Offer - Transaction ID 0xc1478931
79	50.529353459	0.0.0.0	255.255.255.255	DHCP	463	DHCP Request - Transaction ID 0xc1478931
80	58.531124992	openSense-router.rml...	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0xc1478931
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	54.628510700	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 0xadc98d59
93	66.342356749	0.0.0.0	255.255.255.255	DHCP	345	DHCP Request - Transaction ID 0xadc98d59
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.rn1...	DNS	93	Standard query 0xa276	A google.com OPT
12	1.371052670	opnsense-router.rn1...	rn05.rn1abor.hdm-st... DNS	97	Standard query Response 0xa276	A google.com A 142.250.186.174 OPT

Abbildung 12: Ablauf der Anfrage

TODO: Add interpretation

Fall 2: DNS-Server 1.1.1.1 (Cloudflare):

Mittels folgendem Command wurde eine DNS-Abfrage gemacht:

```
$ dig @1.1.1.1 +noall +nosec google.com
```

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

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

No.	Time	Source	Destination	Protocol	Length	Info
234	110.515570213	linux-2.local	Broadcast	ARP	42	who has 141.02.66.5 Tell 141.02.66.5
235	110.515867208	linux-3.local	linux-2.local	ARP	60	141.02.66.6 is at 46:52:62:0e:54:2b
233	115.673164730	linux-3.local	linux-2.local	ARP	60	who has 141.02.66.6 Tell 141.02.66.6
232	115.673186703	linux-2.local	linux-3.local	ARP	42	141.02.66.5 is at 46:52:62:0e:54:0b

Abbildung 15: Ablauf der Anfrage

Wann wird eine ARP-Anfrage gestartet?

TODO: Add interpretation

Welcher Rahmentyp wird für die Anfrage verwendet?

TODO: Add description (Ethernet II)

No.	Time	Source	Destination	Protocol	Length	Info
234	110.515570213	Linux-2.local	Broadcast	Ethernet	42	who has 141.02.66.5 Tell 141.02.66.5
235	110.515867208	Linux-3.local	Linux-2.local	ARP	60	141.02.66.6 is at 46:52:62:0e:54:2b
233	115.673164730	Linux-3.local	Linux-2.local	ARP	60	who has 141.02.66.6 Tell 141.02.66.6
232	115.673186703	Linux-2.local	Linux-3.local	ARP	42	141.02.66.5 is at 46:52:62:0e:54:0b

Layer-2-Protokolle

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

Die Broadcasts sind ARP-Requests.

No.	Time	Source	Destination	Protocol	Length	Info
173	70.088137436	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
174	71.090585778	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
175 72.0906751987	Linux-3.local	224.0.0.251	MDNS	82	Standard query 0x0088 PTR _popkey-hkp._tcp.local. "Qn" question	
177	72.0906752048	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
178	72.0906752052	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
178 77.0996399389	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002	
179	79.090088805	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
180	81.090082308	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
181	83.090082308	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
182	84.090548741	Libremes-226.rnlabor.hdm-stuttgart.de	Broadcast	ARP	60	who has 141.62.66.29? Tell 141.62.66.226
183	84.731177879	Libremes-226.rnlabor.hdm-stuttgart.de	Broadcast	ARP	60	who has 141.62.66.227? Tell 141.62.66.226
184	85.097465721	Libremes-226.rnlabor.hdm-stuttgart.de	Broadcast	ARP	60	who has 141.62.66.26? Tell 141.62.66.226
185	85.097465721	Libremes-226.rnlabor.hdm-stuttgart.de	Broadcast	ARP	60	who has 141.62.66.27? Tell 141.62.66.226
186	85.954875527	Linux-2.local	opnsense_rnlabor.hdm-stuttgart.de	DNS	86	Standard query 0x9e2a PTR 226.66.62.141.in-addr.arpa
187	85.955623999	opnsense_rnlabor.hdm-stuttgart.de	Linux-2.local	DNS	137	Standard query response 0x9e2a PTR 226.66.62.141.in-addr.arpa PTR libremes-226.rnlabor.hdm-stuttgart.de
188	85.999923094	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
189	86.721457470	Libremes-226.rnlabor.hdm-stuttgart.de	Broadcast	ARP	60	who has 141.62.66.29? Tell 141.62.66.226
190	86.785487391	Libremes-226.rnlabor.hdm-stuttgart.de	Broadcast	ARP	60	who has 141.62.66.227? Tell 141.62.66.226
191	86.802794745	Linux-2.local	opnsense_rnlabor.hdm-stuttgart.de	DNS	86	Standard query 0x9e2a PTR 226.66.62.141.in-addr.arpa
192	86.829745488	Linux-3.local	224.0.0.251	MDNS	81	Standard query 0x0088 PTR _www-9189._tcp.local. "Qn" question
193	89.090099785	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
194	91.087596484	Linux-2.local	opnsense_rnlabor.hdm-stuttgart.de	ARP	42	who has 141.62.66.26? Tell 141.62.66.5
195	91.090617202	opnsense_rnlabor.hdm-stuttgart.de	Linux-2.local	ARP	60	141.62.66.29 is at 00:0c:29:1a:c1:5e:eb:cb
196	91.090617202	opnsense_rnlabor.hdm-stuttgart.de	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
197	93.080537535	HewlettP..aa:0b:be	LLDP_Multicast	LLDP	312	MA/0/4:89.73:an:80:0B LA/2 128 SysID:213-MP-2920-240-R1424 SysID:M 39726A 2920-240 Switch, revision w8.10.10.0015, ROM w8.16.03 ..
198	93.090071026	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002
199	95.090796412	HewlettP..aa:0b:be	Spanning-tree-(For-)	STP	119	MST, Root = 32768/0/90:1a:c1:5e:eb:cb Cost = 22880 Port = 0x80002

Abbildung 17: Aufzeichnung der ARP-Requests

TODO: Add interpretation

Haben Sie noch weitere Protokolle “eingefangen”, die offensichtlich im Labor Rechnernetze keinen Sinn machen?

HTTP und TCP

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

TODO: Add description

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 description

Dokumentieren und erläutern Sie die Verwendung der Portnummern bei der Dienstanfrage und der Beantwortung des Dienstes durch den Server.

TODO: Add description

Klicken Sie auf der Website ein anderes Bild / Link an.

Beobachten und dokumentieren Sie, wie verändert sich der

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

TODO: Add interpretation

No.	Time	Source	Destination	Protocol	Length	Info
176 63.999710054		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
177 63.999882304		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
178 67.999494640		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
173 70.999813730		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
174 71.999585778		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
175 72.999622904		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
177 73.999630000		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
178 77.999630082		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
179 79.999888505		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
81 81.999602260		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
183 82.999622904		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
185 85.999522094		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
187 87.999710112		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
193 89.999999795		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
194 91.999999999		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
195 99.999710120		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
199 95.999764312		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
206 97.999500501		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
201 100.988216973		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
202 101.988216973		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
204 103.989773202		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
206 105.989442753		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
212 109.988240978		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
213 109.989834240		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
222 113.999732841		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002
223 115.999656007		newlettP.an.BbE	Spanning-tree-for...	STP	119	MST_Root = 32768/0/0/1a1c1Sereb:0 Cost = 22920 Port = 0x8002

* Frame 191: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface eno5s3if6, id 9

- IEEE 802.3 Ethernet

* Destination: Spanning-tree-(for-bridges)_00 (01:00:

Address: Spanning-tree-(for-bridges)_88 (01:88:c2:88:60:88)

= LG bit: Globally unique address (factory default)

= IG bit: Group add
- Source: NetLister as:9b:b6:19d:0b:32:as:9b:b6

* SOURCE: HexEdit_80:00:DE [84:09:73:1B:80:DE]
Destination: 192.168.1.255:52000->192.168.1.255:52000

Address: Hewlett-Packard (941-BB-00) 00-00-00-00-00-00
MAC address = 16 bit: Globally unique address /factory defined

..... = 16 bits: Globally
..... = 16 bits: Individual

Length: 185

• Logical-Link Control

→ Spanning Tree Protocol

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	HeuletCP.an.Bb:be	Spanning-tree-(For-	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
394 104.000105982	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
395 106.000056817	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
397 109.000202936	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
398 110.000202936	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
406 192.000560847	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
407 194.000877110	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
408 196.000399860	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
411 200.000399860	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
412 208.000287489	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
413 292.000187163	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
417 204.000254351	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
418 206.000015959	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
420 210.000015959	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
424 218.000289871	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
425 212.000277773	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
426 214.000106947	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
427 216.000078690	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
428 218.000078690	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
430 720.000140852	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1:Se:eb:c9	Cost = 226029	Port = 0x80002
433 222.000177264	HeuletCP.an.Bb:be	Spanning-tree-(For- STP	119 MST	Root = 32768/0/0/0:1a:c1: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 Gerätem 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 ...
58	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	141.62.66.5	141.62.66.207	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	15.993566088	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	16.178463135	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 ...
88	16.44425668	141.62.66.5	141.62.66.207	TELNET	67	Telnet Data ...
90	16.453801998	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) [ethernet], Dst: rnlabor (62:62:8e:54:b8:b0)
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: 34
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	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
26	255	1.444955673	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
31	255	1.451973372	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
89	255	1.498643116	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
98	255	1.3.50059800	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
112	255	1.4.35439355	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
120	255	1.4.35439357	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
1527	255	1.21.51668853	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
1567	255	1.21.65419641	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2831	255	1.25.443188947	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2844	255	1.25.456619749	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2850	255	1.25.456619750	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2849	255	1.25.509882269	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2858	255	1.25.509882265	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2851	255	1.25.509882264	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
2852	255	1.25.509882265	100.64.154.254	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
11948	255	1.471373020	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	felix-xps13.local	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
18852	255	1.134.49841999	100.64.154.254	felix-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	154.339292380	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