ÜBUNG 07

Wireshark Basisprotokolle TCP/IP

NETZWERKTECHNIK / SEMESTER 3

1

AGENDA

01 WIRESHARK EINFÜHRUNG

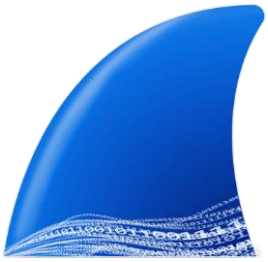
02 ICMP

03 ASDRESSAUFLÖSUNG

tgm

2

01



Wireshark Einführung

3

Was Sie sich von der Analyse von Netzwerkpaketen erhoffen...

[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

4

NETZWERKTECHNIK / SEMESTER 3

Überblick

- Wiederholung des OSI-Modells
- Wireshark
  - Erfassen von Paketen
  - Ein Rundgang durch die Wireshark-Benutzeroberfläche
  - Überprüfen/Analysieren von Paketen
  - Filtern

tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

5

NETZWERKTECHNIK / SEMESTER 3

Encapsulation

- Jede Schicht stellt Dienste für die darüber liegende Schicht bereit
- Jede Schicht nutzt die darunterliegende Schicht
- Daten aus einer Schicht werden in Frames der darunter liegenden Schicht gekapselt
- Das L4-Segment enthält einen Teil des Streams des Anwendungsprotokolls
- L3-Paket enthält ein L4-Segment
- Der L2-Frame hat ein L3-Paket im Datenteil

tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

6

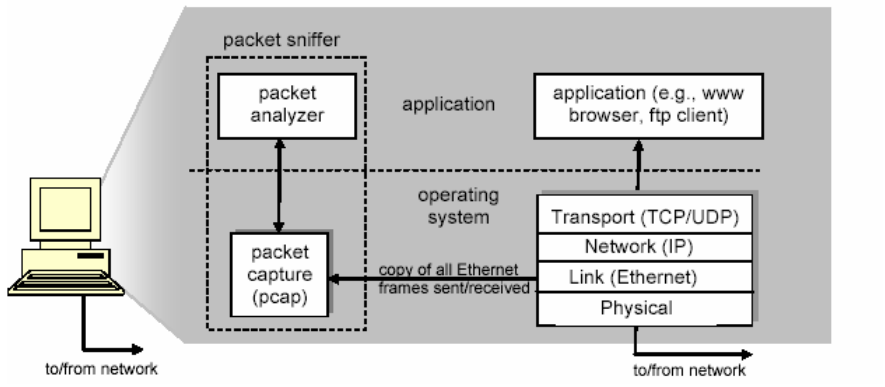
Wireshark

… ist ein kostenloser und Open-Source-Paketanalysator

7

NETZWERKTECHNIK / SEMESTER 3

Architektur

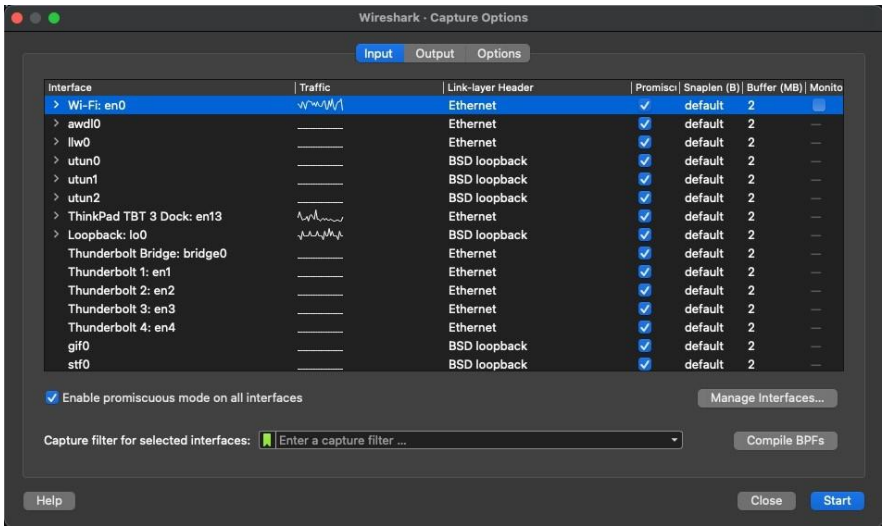


[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

8

NETZWERKTECHNIK / SEMESTER 3

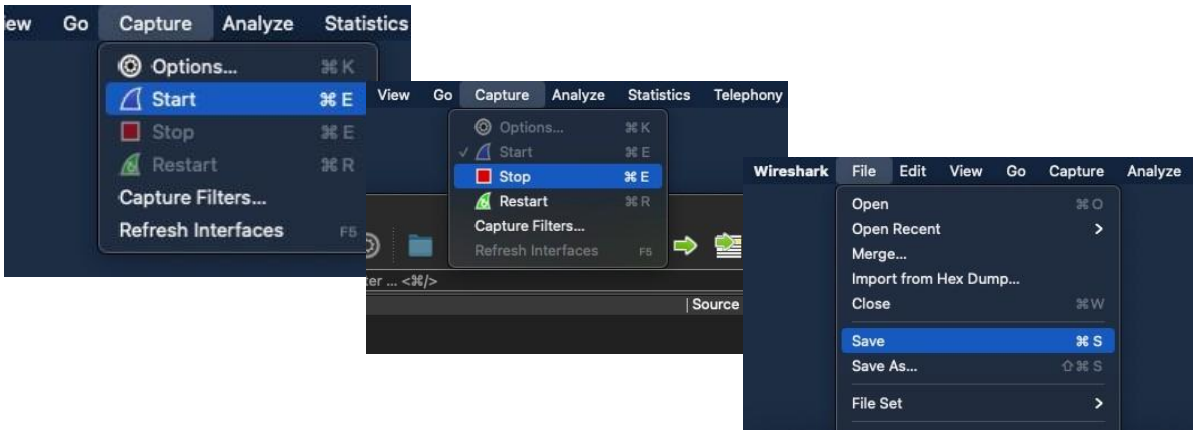
Interface Auswahl



tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

Starten, Stoppen, Speichern



tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

Zum Vergleich - tcpdump

```
reading from file telnet-cooked.pcap, link-type EN10MB (Ethernet)
15:12:38.387203 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [S], seq 2579865836, win 32120, options [mss 1460,sackOK,TS val 10233636 ecr 0,nop,wscale 0], length 0
15:12:38.389728 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [S.], seq 401695549, ack 2579865837, win 17376, options [mss 1448,nop,wscale 0,nop,nop,TS val 2467372 ecr 10233636], length 0
15:12:38.389775 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 1, win 32120, options [nop,nop,TS val 10233636 ecr 2467372], length 0
15:12:38.391363 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 1:28, ack 1, win 32120, options [nop,nop,TS val 10233636 ecr 2467372], length 27 [telnet DO SUPPRESS GO AHEAD, WILL TERMINAL TYPE, WILL NAWS, WILL TSPEED, WILL LFLOW, WILL LINEMODE, WILL NEW-ENVIRON, DO STATUS, WILL XDISPLOC [!telnet]
15:12:38.537538 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 1:4, ack 28, win 17349, options [nop,nop,TS val 2467372 ecr 10233636], length 3 [telnet DO AUTHENTICATION [!telnet]
15:12:38.537605 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 4, win 32120, options [nop,nop,TS val 10233651 ecr 2467372], length 0
15:12:38.537777 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 28:31, ack 4, win 32120, options [nop,nop,TS val 10233651 ecr 2467372], length 3 [telnet WONT AUTHENTICATION [!telnet]
15:12:38.539149 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 31, win 17376, options [nop,nop,TS val 2467372 ecr 10233651], length 0
15:12:38.540860 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 4:29, ack 31, win 17376, options [nop,nop,TS val 2467372 ecr 10233651], length 25 [telnet WILL SUPPRESS GO AHEAD, DO TERMINAL TYPE, DO NAWS, DO TSPEED, DO LFLOW, DO LINEMODE, SB LINEMODE SEND 0x0 SE [!telnet]
15:12:38.541068 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 31:95, ack 29, win 32120, options [nop,nop,TS val 10233651 ecr 2467372], length 64 [telnet SB NAWS IS 0x50 0 0x20 SE, SB LINEMODE 0x3 0x1 0 0 0x3 0x62 0x3 0x4 0x2 0xf 0x5 0 0 0x7 0x62 0x1c 0x8 0x2 0x4 0x9 0x42 0x1a 0xa 0x2 0x7f 0xb 0x2 0x15 0xf 0x2 0x11 0x10 0x2 0x13 0x11 0 0 0x12 0 0 SE, DO SUPPRESS GO AHEAD, SB LINEMODE SEND 0xf SE [!telnet]
15:12:38.542187 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 95, win 17312, options [nop,nop,TS val 2467372 ecr 10233651], length 0
15:12:38.542780 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 29:47, ack 95, win 17312, options [nop,nop,TS val 2467372 ecr 10233651], length 18 [telnet DO NEW-ENVIRON, WILL STATUS, DO XDISPLOC, WILL ENCRYPT, DO ENCRYPT, DO OLD-ENVIRON [!telnet]
15:12:38.542859 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 95:104, ack 47, win 32120, options [nop,nop,TS val 10233651 ecr 2467372], length 9 [telnet DONT ENCRYPT, WONT ENCRYPT, WONT OLD-ENVIRON [!telnet]
15:12:38.543849 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 104, win 17367, options [nop,nop,TS val 2467372 ecr 10233651], length 0
15:12:38.546219 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 47:71, ack 104, win 17376, options [nop,nop,TS val 2467372 ecr 10233651], length 24 [telnet SB TSPEED SEND SE, SB XDISPLOC SEND SE, SB NEW-ENVIRON SEND SE, SB TERMINAL TYPE SEND SE [!telnet]
15:12:38.546430 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 71, win 32120, options [nop,nop,TS val 10233652 ecr 2467372], length 0
15:12:38.547047 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 104:189, ack 71, win 32120, options [nop,nop,TS val 10233652 ecr 2467372], length 85 [telnet SB TSPEED IS 0x39 0x36 0x30 0x30 0x2c 0x39 0x36 0x30 0x30 SE, SB XDISPLOC IS 0x62 0x61 0x6d 0x2e 0x7a 0x69 0x6e 0x67 0x2e 0x6f 0x72 0x67 0x3a 0x30 0x2e 0x30 SE, SB TERMINAL TYPE IS 0x78 0x74 0x65 0x72 0x6d 0x2d 0x63 0x6f 0x6c 0x6f 0x72 SE [!telnet]
15:12:38.548221 IP truncated-ip - 85 bytes missing! 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 104:189, ack 71, win 32120, options [nop,nop,TS val 10233652 ecr 2467372], length 85 [!telnet]
15:12:38.568470 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 71:74, ack 189, win 17376, options [nop,nop,TS val 2467372 ecr 10233652], length 3 [telnet DO ECHO [!telnet]
15:12:38.568581 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 189:192, ack 74, win 32120, options [nop,nop,TS val 10233654 ecr 2467372], length 3 [telnet WONT ECHO [!telnet]
15:12:38.569718 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 192, win 17373, options [nop,nop,TS val 2467372 ecr 10233654], length 0
15:12:38.583509 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 74:86, ack 192, win 17376, options [nop,nop,TS val 2467372 ecr 10233654], length 12 [telnet WILL ECHO, SB LFLOW INFO SE, WONT ECHO [!telnet]
15:12:38.583630 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 192:198, ack 86, win 32120, options [nop,nop,TS val 10233655 ecr 2467372], length 6 [telnet DO ECHO, DONT ECHO [!telnet]
15:12:38.584705 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 198, win 17370, options [nop,nop,TS val 2467372 ecr 10233655], length 0
15:12:38.585489 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 86:101, ack 198, win 17370, options [nop,nop,TS val 2467372 ecr 10233655], length 15 [telnet SB LINEMODE 0x3 0x5 0x80 0 0x11 0x80 0 0x12 0x80 0 SE [!telnet]
15:12:38.596419 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 101, win 32120, options [nop,nop,TS val 10233657 ecr 2467372], length 0
15:12:38.597730 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 101:133, ack 198, win 17376, options [nop,nop,TS val 2467372 ecr 10233657], length 32
15:12:38.616442 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 133, win 32120, options [nop,nop,TS val 10233659 ecr 2467372], length 0
15:12:39.705866 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 133:140, ack 198, win 17376, options [nop,nop,TS val 2467374 ecr 10233659], length 7
15:12:39.716432 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 140, win 32120, options [nop,nop,TS val 10233769 ecr 2467374], length 0
15:12:40.949196 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 198:204, ack 140, win 32120, options [nop,nop,TS val 10233892 ecr 2467374], length 6
15:12:40.950568 IP truncated-ip - 6 bytes missing! 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 198:204, ack 140, win 32120, options [nop,nop,TS val 10233892 ecr 2467374], length 6 [!telnet]
15:12:40.962649 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 140:143, ack 204, win 17376, options [nop,nop,TS val 2467377 ecr 10233892], length 3 [telnet WILL ECHO [!telnet]
15:12:40.962801 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 204:207, ack 143, win 32120, options [nop,nop,TS val 10233893 ecr 2467377], length 3 [telnet DO ECHO [!telnet]
15:12:40.963879 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 207, win 17373, options [nop,nop,TS val 2467377 ecr 10233893], length 0
15:12:40.964875 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 143:152, ack 207, win 17376, options [nop,nop,TS val 2467377 ecr 10233893], length 9
15:12:40.976432 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 152, win 32120, options [nop,nop,TS val 10233895 ecr 2467377], length 0
```

[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

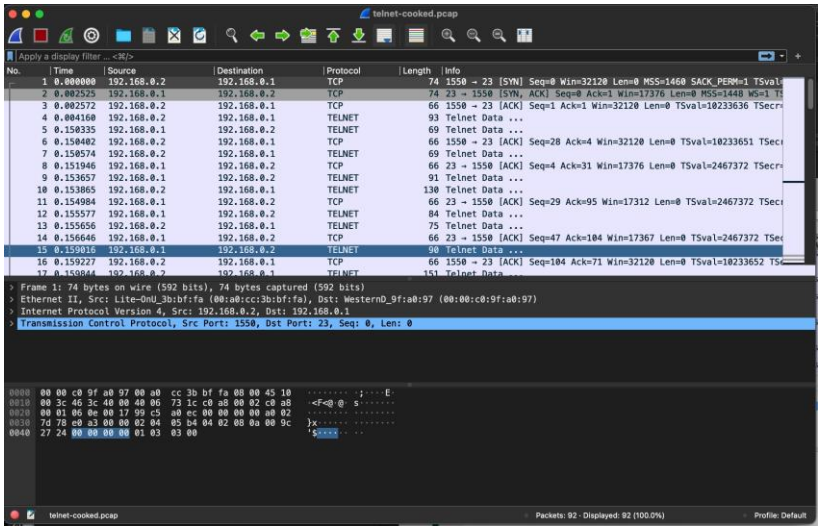
11

UI
Überblick

12

NETZWERKTECHNIK / SEMESTER 3

Überblick



tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

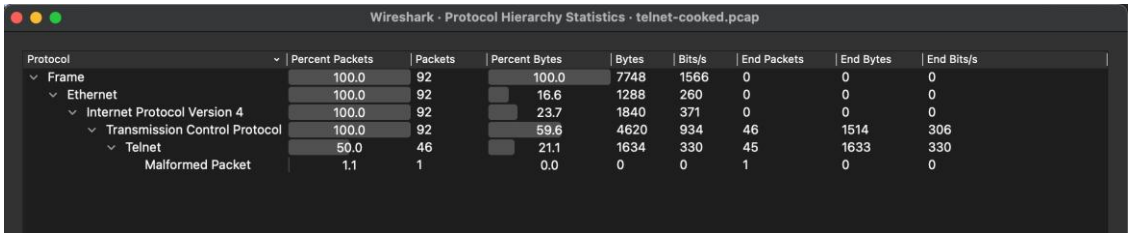
NETZWERKTECHNIK / SEMESTER 3

Statistiken

tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

Protokollhierarchie

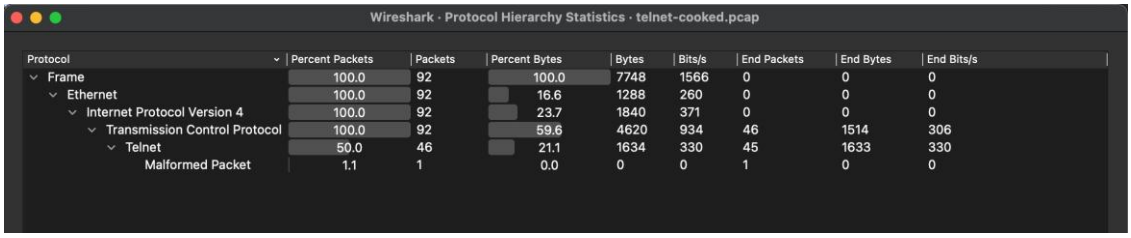


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	92	100.0	7748	1566	0	0	0
Ethernet	100.0	92	16.6	1288	260	0	0	0
Internet Protocol Version 4	100.0	92	23.7	1840	371	0	0	0
Transmission Control Protocol	100.0	92	59.6	4620	934	46	1514	306
Telnet	50.0	46	21.1	1634	330	45	1633	330
Malformed Packet	1.1	1	0.0	0	0	1	0	0

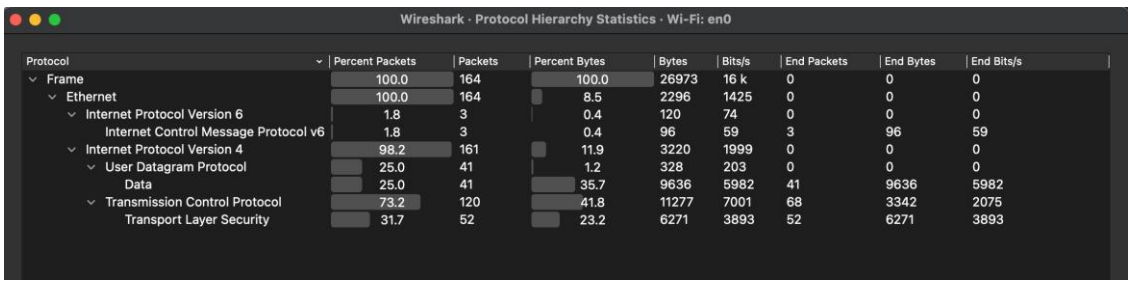
tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

Protokollhierarchie



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	92	100.0	7748	1566	0	0	0
Ethernet	100.0	92	16.6	1288	260	0	0	0
Internet Protocol Version 4	100.0	92	23.7	1840	371	0	0	0
Transmission Control Protocol	100.0	92	59.6	4620	934	46	1514	306
Telnet	50.0	46	21.1	1634	330	45	1633	330
Malformed Packet	1.1	1	0.0	0	0	1	0	0



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	164	100.0	26973	16 k	0	0	0
Ethernet	100.0	164	8.5	2296	1425	0	0	0
Internet Protocol Version 6	1.8	3	0.4	120	74	0	0	0
Internet Control Message Protocol v6	1.8	3	0.4	96	59	3	96	59
Internet Protocol Version 4	98.2	161	11.9	3220	1999	0	0	0
User Datagram Protocol	25.0	41	1.2	328	203	0	0	0
Data	25.0	41	35.7	9636	5982	41	9636	5982
Transmission Control Protocol	73.2	120	41.8	11277	7001	68	3342	2075
Transport Layer Security	31.7	52	23.2	6271	3893	52	6271	3893

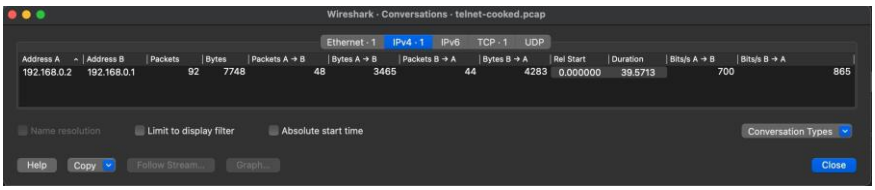
tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

Konversationen

17

NETZWERKTECHNIK / SEMESTER 3

Konversationen



[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

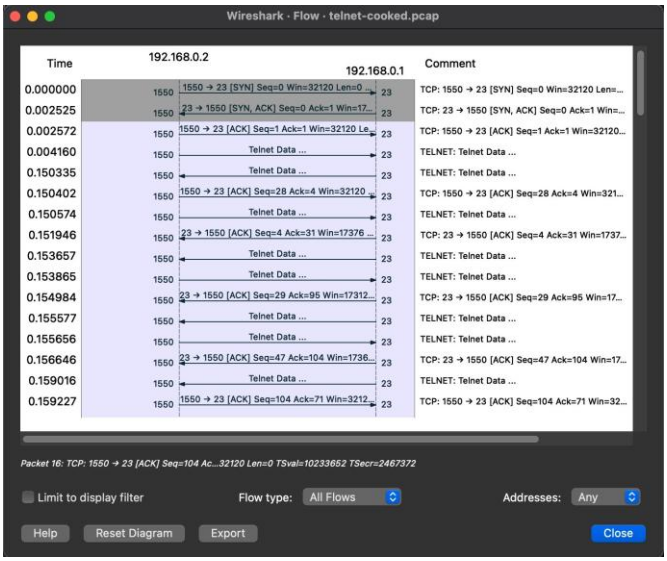
18

Flow Grafik

19

NETZWERKTECHNIK / SEMESTER 3

Flow



[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

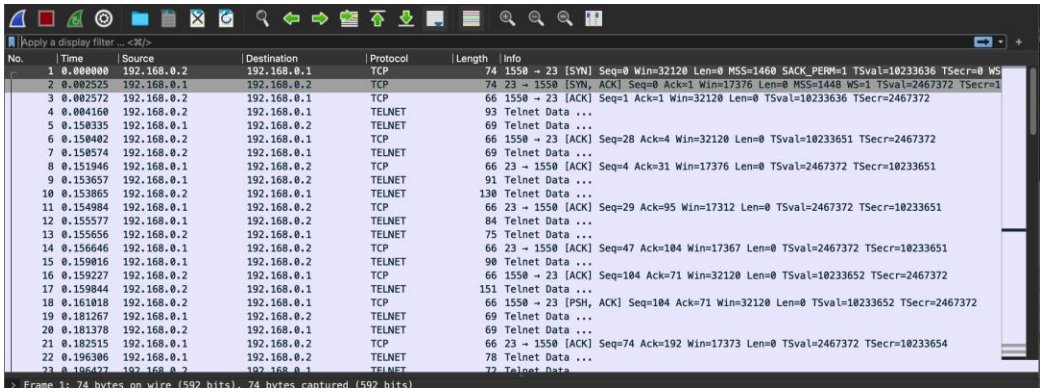
20

Analyse

21

NETZWERKTECHNIK / SEMESTER 3

Paketliste



[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

22

NETZWERKTECHNIK / SEMESTER 3

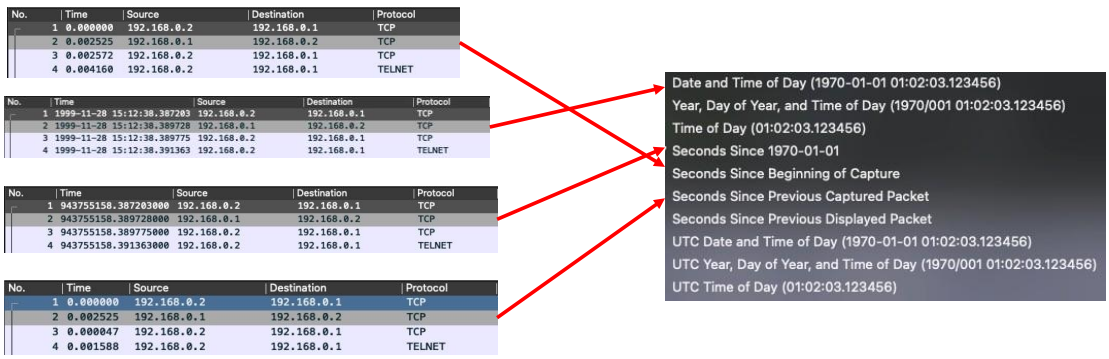
Paketliste

- Zeit – der Zeitstempel, bei dem das Paket die Schnittstelle überquert hat.
- Quelle – der ursprüngliche Host des Pakets.
- Ziel – der Host, an den das Paket gesendet wurde.
- Protokoll – das Protokoll auf höchster Ebene, das Wireshark erkennen konnte.
- Länge – die Länge des Pakets auf der Leitung in Bytes.
- Info – eine Informationsmeldung, die sich auf das Protokoll in der Protokollspalte bezieht.

tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

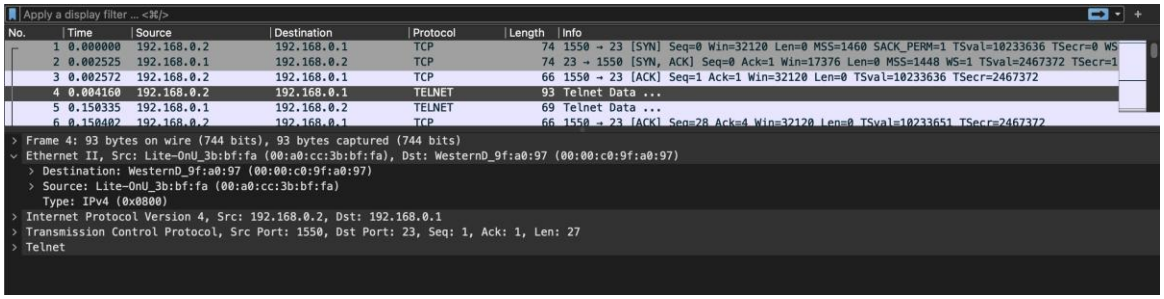
Zeitformat ändern



tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

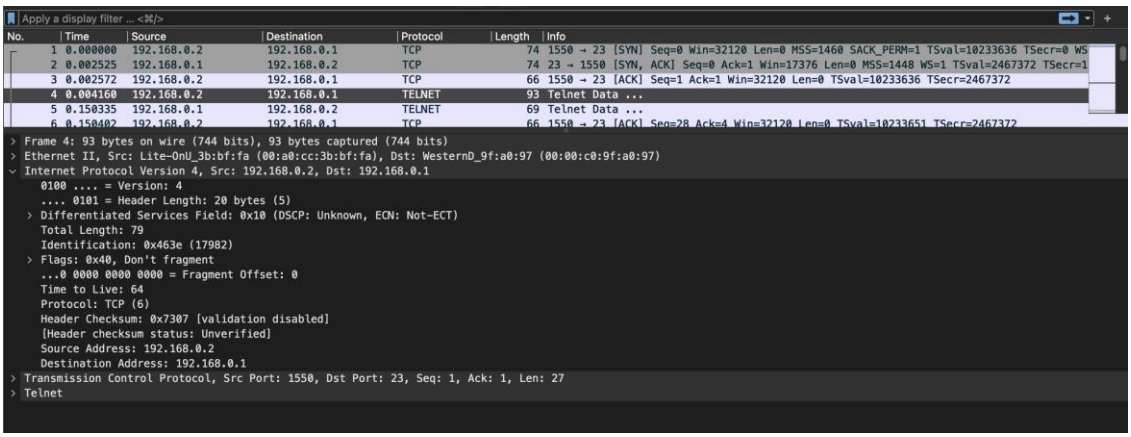
Layer 2



tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

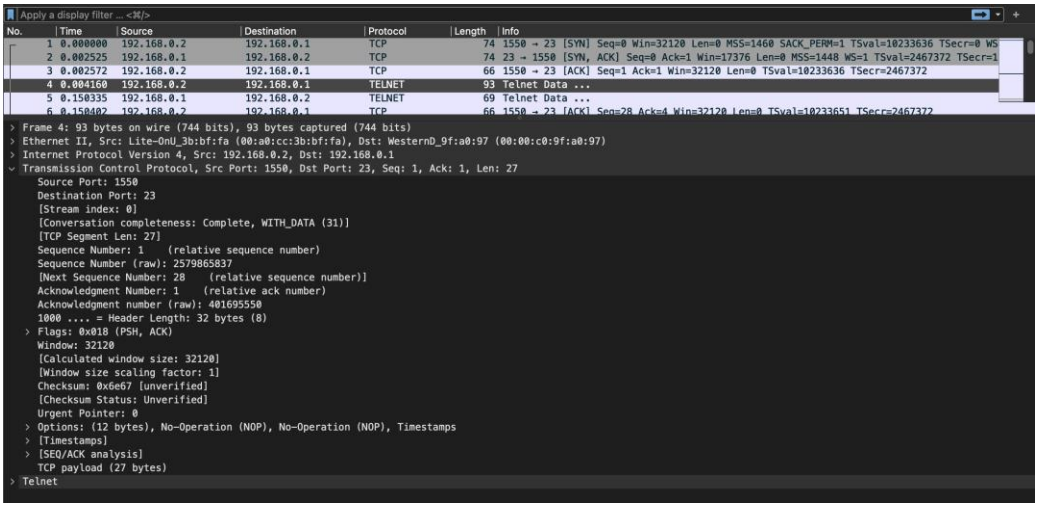
Layer 3



tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

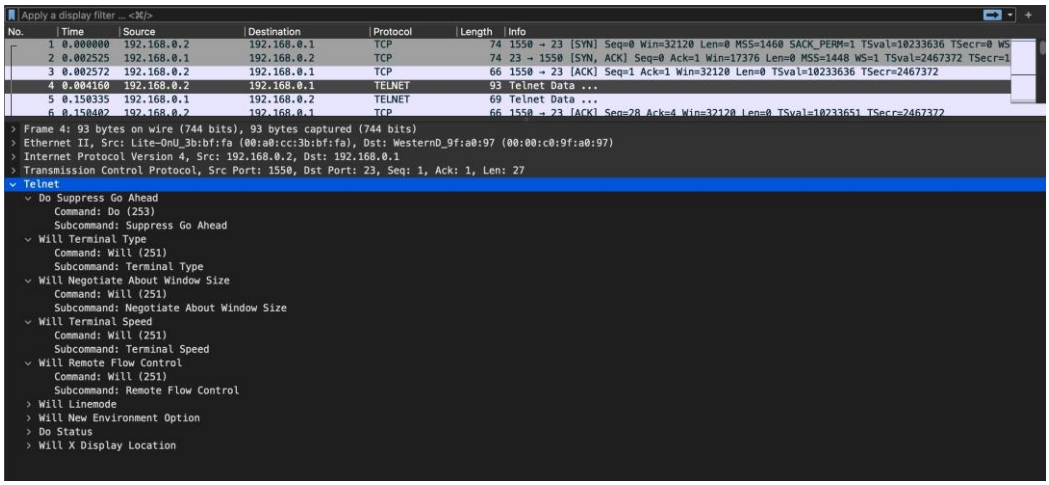
Layer 4



[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

Layer 7



[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

RAW Paket

```
> Will Linemode
> Will New Environment Option
> Do Status
> Will X Display Location

0000  00 00 c0 9f a0 97 00 a0  cc 3b bf fa 08 00 45 10   ........ .;....E.
0010  00 4f 46 3e 40 00 40 06  73 07 c0 a8 00 02 c0 a8   .OF>@.@. s.......
0020  00 01 06 0e 00 17 99 c5  a0 ed 17 f1 63 3e 80 18   ........ ....c>..
0030  7d 78 6e 67 00 00 01 01  08 0a 00 9c 27 24 00 25   }xng.... ....'$.%
0040  a6 2c ff fd 03 ff fb 18  ff fb 1f ff fb 20 ff fb   .,...... ..... ..
0050  21 ff fb 22 ff fb 27 ff  fd 05 ff fb 23            !..".. '. ....#
```

[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

Filter

NETZWERKTECHNIK / SEMESTER 3

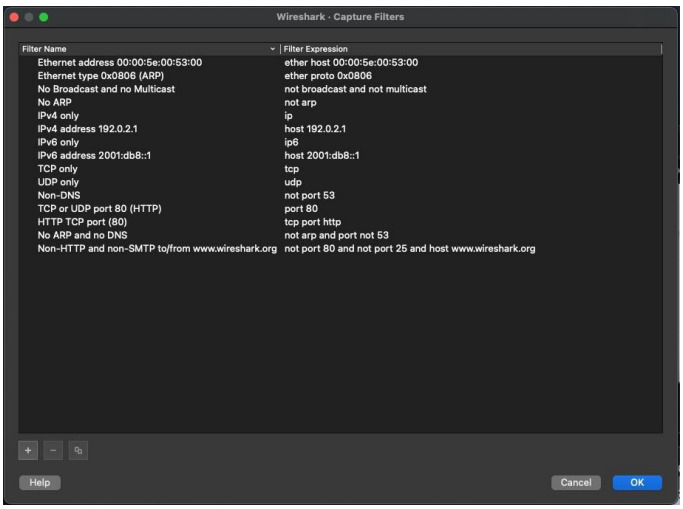
Filter

[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

31

NETZWERKTECHNIK / SEMESTER 3

Capture Filter

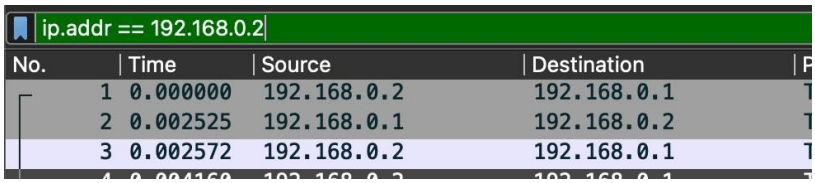


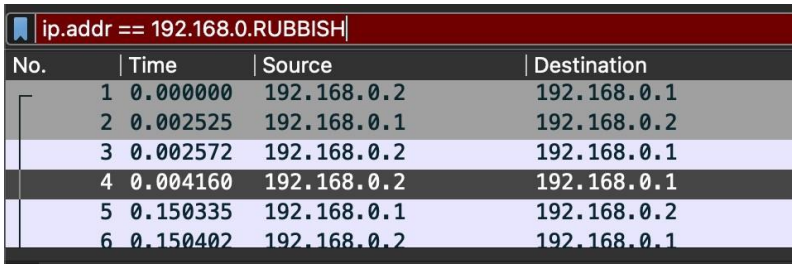
[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

32

NETZWERKTECHNIK / SEMESTER 3

Display Filter





tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

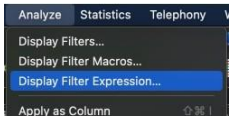
Beispiele für Display Filter

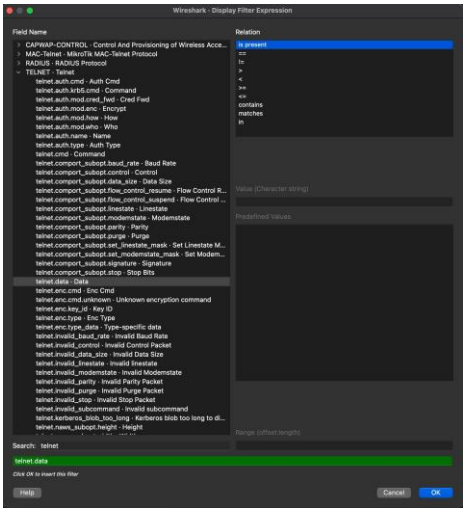
- http.request – Zeigt alle HTTP-Anfragen an.
- http.request || http.response – Zeigt alle HTTP-Anfragen und -Antworten an.
- ip.addr == 127.0.0.1 – Zeigt alle IP-Pakete an, deren Quelle oder Ziel localhost ist.
- tcp.len < 100 – Zeigt alle TCP-Pakete an, deren Datenlänge weniger als 100 Byte beträgt.
- http.request.uri matches "(gif)$" - Zeigt alle HTTP-Anfragen an, bei denen der URI mit "gif" endet.
- dns.query.name == "www.google.com" - Zeige alle DNS-Abfragen für "www.google.com" an.

tgm [Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

Display Filter Expression Editor

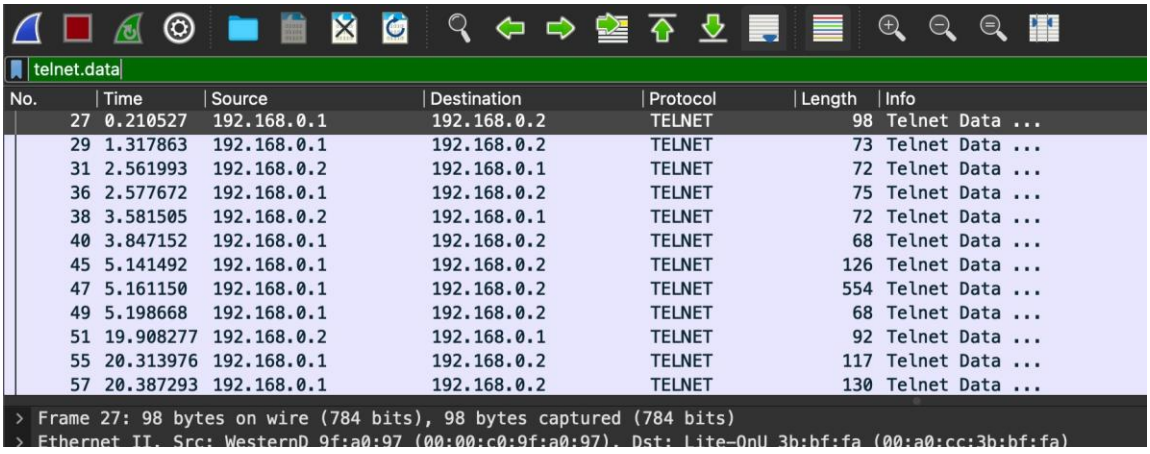




[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

Display Filter Expression Editor



[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

Streams

37

Einem Stream folgen

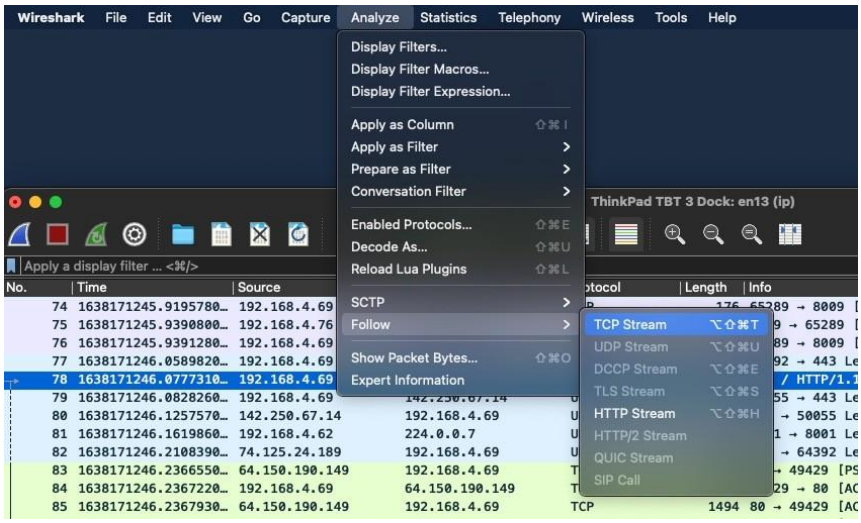
No.	Time	Source	Destination	Protocol	Length	Info
74	1638171245.9195780…	192.168.4.69	192.168.4.76	TCP	176	65289 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=110 TSval=3003906371 TSec
75	1638171245.9390800…	192.168.4.76	192.168.4.69	TCP	176	8009 → 65289 [PSH, ACK] Seq=1 Ack=111 Win=277 Len=110 TSval=6096536 TSecr=
76	1638171245.9391280…	192.168.4.69	192.168.4.76	TCP	66	65289 → 8009 [ACK] Seq=111 Ack=111 Win=2046 Len=0 TSval=3003906390 TSecr=6
77	1638171246.0589820…	192.168.4.69	74.125.24.189	UDP	75	64392 → 443 Len=33
78	1638171246.0777310…	192.168.4.69	64.150.190.149	HTTP	1012	GET / HTTP/1.1
79	1638171246.0828260…	192.168.4.69	142.250.67.14	UDP	75	50055 → 443 Len=33
80	1638171246.1257570…	142.250.67.14	192.168.4.69	UDP	68	443 → 50055 Len=26
81	1638171246.1619860…	192.168.4.62	224.0.0.7	UDP	240	8001 → 8001 Len=198
82	1638171246.2108390…	74.125.24.189	192.168.4.69	UDP	67	443 → 64392 Len=25
83	1638171246.2366550…	64.150.190.149	192.168.4.69	TCP	658	80 → 49429 [PSH, ACK] Seq=1 Ack=947 Win=252 Len=592 TSval=582748517 TSecr=
84	1638171246.2367220…	192.168.4.69	64.150.190.149	TCP	66	49429 → 80 [ACK] Seq=947 Ack=593 Win=2038 Len=0 TSval=3237570255 TSecr=582
85	1638171246.2367930…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=593 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=32
86	1638171246.2367940…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=2021 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3
87	1638171246.2368170…	192.168.4.69	64.150.190.149	TCP	66	49429 → 80 [ACK] Seq=947 Ack=3449 Win=2003 Len=0 TSval=3237570255 TSecr=58

[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

38

NETZWERKTECHNIK / SEMESTER 3

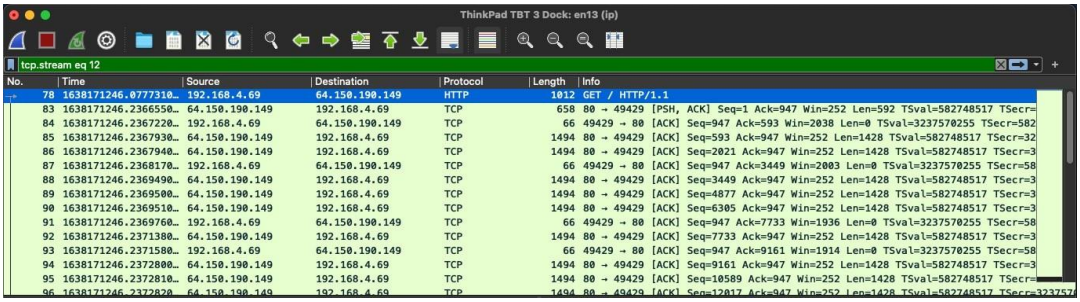
Einem Stream folgen



[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

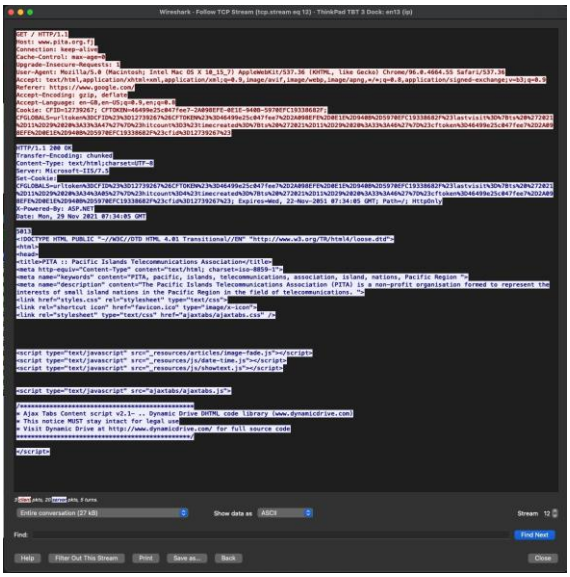
Einem Stream folgen



[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

NETZWERKTECHNIK / SEMESTER 3

Einem Stream folgen



[Quelle: Wireshark Tutorial, Network Startup Resource Center www.ws.nsrc.org]

41

02

Internet Control Message Protocol (ICMP)

QUELLE:

UNIVERSITY OF TORONTO

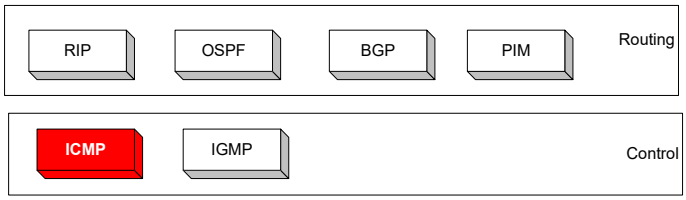
HTTPS://WWW.COMM.UTORONTO.CA/~JORG/TEACHING/ITLAB/SLIDES/MODULE08-ICMP.PPT

42

NETZWERKTECHNIK / SEMESTER 3

Überblick

- Das IP (Internet Protocol) stützt sich auf mehrere andere Protokolle, um die erforderlichen Steuerungs- und Routing-Funktionen auszuführen:
- Steuerungsfunktionen (ICMP)
- Multicast-Signalisierung (IGMP)
- Einrichten von Routing-Tabellen (RIP, OSPF, BGP, PIM, ...)



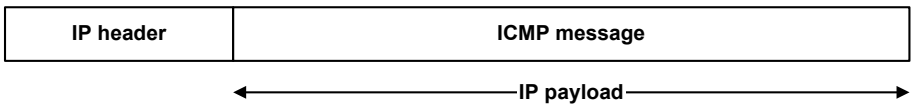
tgm [Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

43

NETZWERKTECHNIK / SEMESTER 3

Überblick

- Das Internet Control Message Protocol (ICMP) ist ein Hilfsprotokoll, das IP unterstützt:
  - Fehlerreporting
  - Einfache Abfragen
- ICMP-Nachrichten werden als IP-Datagramme gekapselt:



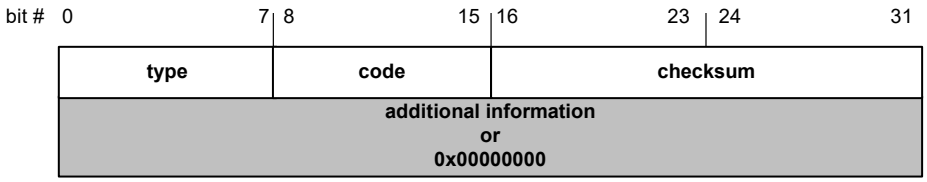
tgm [Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

44

NETZWERKTECHNIK / SEMESTER 3

ICMP-Nachrichtenformat

- 4-Byte-Header:
- Typ (1 Byte): Typ der ICMP-Nachricht
- Code (1 Byte): Untertyp der ICMP-Nachricht
- Prüfsumme (2 Bytes): ähnlich wie die Prüfsumme des IP-Headers. Die Prüfsumme wird über die gesamte ICMP-Nachricht berechnet
- Wenn keine zusätzlichen Daten vorhanden sind, werden 4 Bytes auf Null gesetzt → Jede ICMP-Nachricht ist mindestens 8 Byte lang



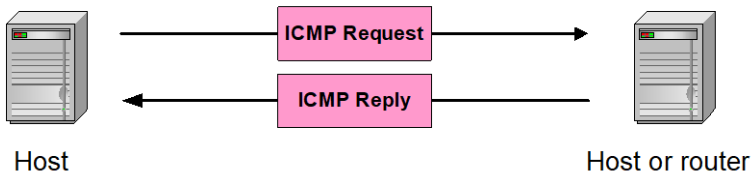
[Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

NETZWERKTECHNIK / SEMESTER 3

ICMP-Nachrichtenformat

ICMP-Abfrage:

- **Request**, die vom Host an einen Router oder Host gesendet wird
- **Reply** an den anfragenden Host zurückgesendet



[Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

Beispiele von ICMP Queries

TYPE/CODE:	DESCRIPTION	
8/0	ECHO REQUEST	Der Ping-Befehl verwendet Echo Request/ Echo Reply
0/0	ECHO REPLY	
13/0	TIMESTAMP REQUEST	
14/0	TIMESTAMP REPLY	
10/0	ROUTER SOLICITATION	
9/0	ROUTER ADVERTISEMENT	

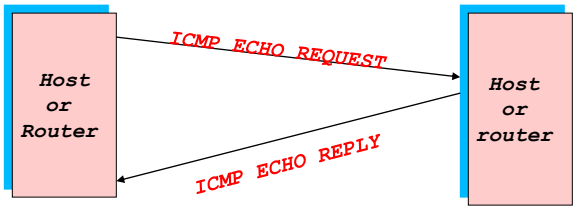
tgm [Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

47

47

Echo Request und Reply

- Pings werden direkt vom Kernel verarbeitet
- Jeder Ping wird in eine ICMP-Echo Request übersetzt
- Der Ping-Host antwortet mit einer ICMP-Echo-Reply

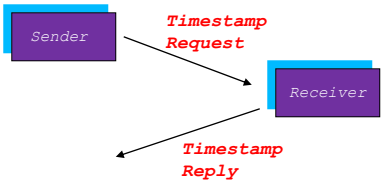


tgm [Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

48

ICMP-Zeitstempel

- Ein System (Host oder Router) fragt ein anderes System nach der aktuellen Uhrzeit.
- Die Zeit wird in Millisekunden nach Mitternacht UTC (Universal Coordinated Time) des aktuellen Tages gemessen
- Der Absender sendet eine Anfrage, der Empfänger antwortet mit einer Antwort

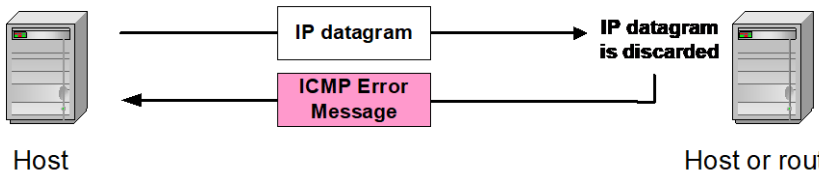


Type (= 17 or 18)	Code (=0)	Checksum
identifier		sequence number
32-bit sender timestamp		
32-bit receive timestamp		
32-bit transmit timestamp		

[Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

ICMP-Fehlermeldungen

- ICMP-Fehlermeldungen melden Fehlerzustände
- Wird in der Regel gesendet, wenn ein Datagramm verworfen wird
- Fehlermeldungen werden häufig von ICMP an das Anwendungsprogramm übergeben

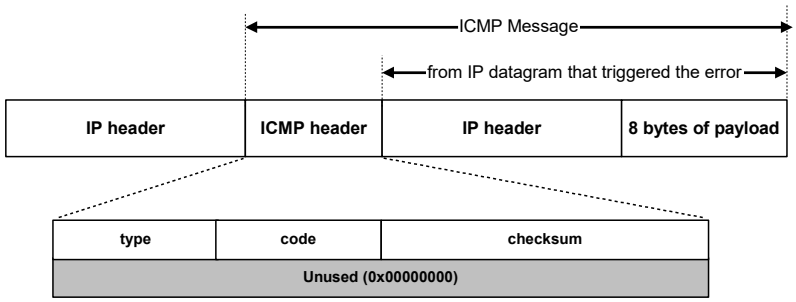


[Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

NETZWERKTECHNIK / SEMESTER 3

ICMP-Fehlermeldungen

- ICMP-Fehlermeldungen enthalten den vollständigen IP-Header und die ersten 8 Byte der Nutzlast (typischerweise: UDP, TCP)



[Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

NETZWERKTECHNIK / SEMESTER 3

Häufige ICMP-Fehlermeldungen

Type	Code	Beschreibung	
3	0–15	Destination unreachable	Notification that an IP datagram could not be forwarded and was dropped. The code field contains an explanation.
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

[Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

NETZWERKTECHNIK / SEMESTER 3

Sub-Typen für „Destination Unreachable“

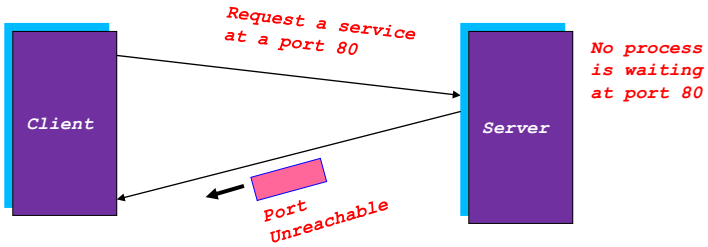
Code	Beschreibung	Sendegrund
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

tgm [Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

NETZWERKTECHNIK / SEMESTER 3

Beispiel ICMP Port „Destination Unreachable“

- RFC 792: Wenn das IP-Modul auf dem Zielhost das Datagramm nicht zustellen kann, weil das angegebene Protokollmodul oder der angegebene Port nicht aktiv ist, sendet der Zielhost eine Nachricht „Destination Unreachable" an den Quellhost.
- Szenario:



tgm [Quelle: https://www.comm.utoronto.ca/~jorg/teaching/itlab/slides/module08-icmp.ppt - letzter Abruf 14.2.2026]

03

Adressauflösung

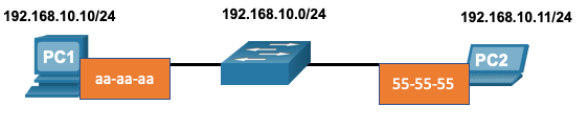
55

Ziel im gleichen Netzwerk

Einem Gerät in einem Ethernet-LAN werden zwei primäre Adressen zugewiesen:

- **Die physikalische Adresse der Schicht 2 (MAC-Adresse)** – wird für die Kommunikation zwischen Netzwerkkarten (NICs) im selben Ethernet-Netzwerk verwendet.
- **Die logische Adresse der Schicht 3 (IP-Adresse)** – wird verwendet, um das Paket vom Quellgerät zum Zielgerät zu senden.

Schicht-2-Adressen werden verwendet, um Frames von einer Netzwerkkarte zu einer anderen im selben Netzwerk zu übertragen. Befindet sich die Ziel-IP-Adresse im selben Netzwerk, entspricht die Ziel-MAC-Adresse derjenigen des Zielgeräts.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

[Quelle: CCNAv7: Switching, Routing, and Wireless Essentials v7.0 (SRWE), by Cisco Networking Academy, Cisco Press]

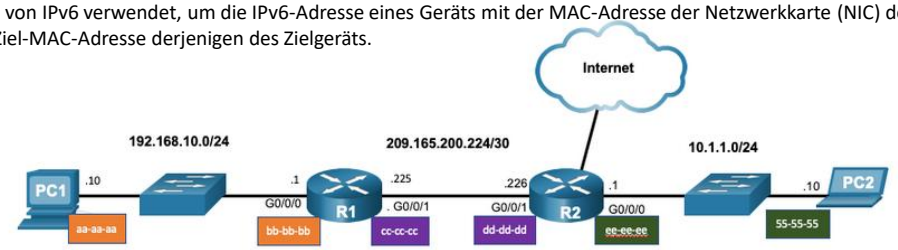
56

NETZWERKTECHNIK / SEMESTER 3

Ziel im Remote Netzwerk

Befindet sich die Ziel-IP-Adresse in einem entfernten Netzwerk, ist die Ziel-MAC-Adresse die des Standardgateways.

- **ARP** wird von IPv4 verwendet, um die IPv4-Adresse eines Geräts mit der MAC-Adresse der Netzwerkkarte (NIC) des Geräts zu verknüpfen.
- **ICMPv6** wird von IPv6 verwendet, um die IPv6-Adresse eines Geräts mit der MAC-Adresse der Netzwerkkarte (NIC) des Geräts zu verknüpfen.Ziel-MAC-Adresse derjenigen des Zielgeräts.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

[Quelle: CCNAv7: Switching, Routing, and Wireless Essentials v7.0 (SRWE), by Cisco Networking Academy, Cisco Press]

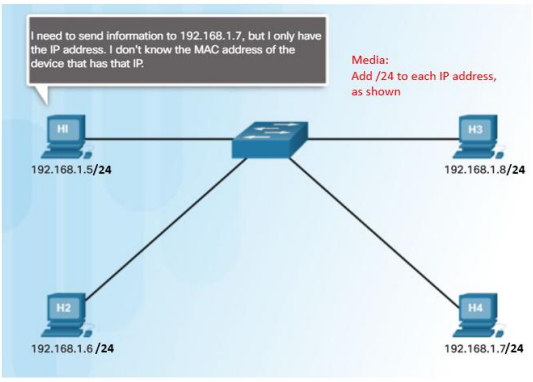
57

NETZWERKTECHNIK / SEMESTER 3

ARP Überblick

Ein Gerät verwendet ARP, um die Ziel-MAC-Adresse eines lokalen Geräts zu ermitteln, wenn es dessen IPv4-Adresse kennt.

- ARP bietet zwei grundlegende Funktionen:
  - **Auflösung von IPv4-Adressen in MAC-Adressen** und
  - **Verwaltung einer ARP-Tabelle** mit Zuordnungen von IPv4- zu MAC-Adressen.



[Quelle: CCNAv7: Switching, Routing, and Wireless Essentials v7.0 (SRWE), by Cisco Networking Academy, Cisco Press]

58

NETZWERKTECHNIK / SEMESTER 3

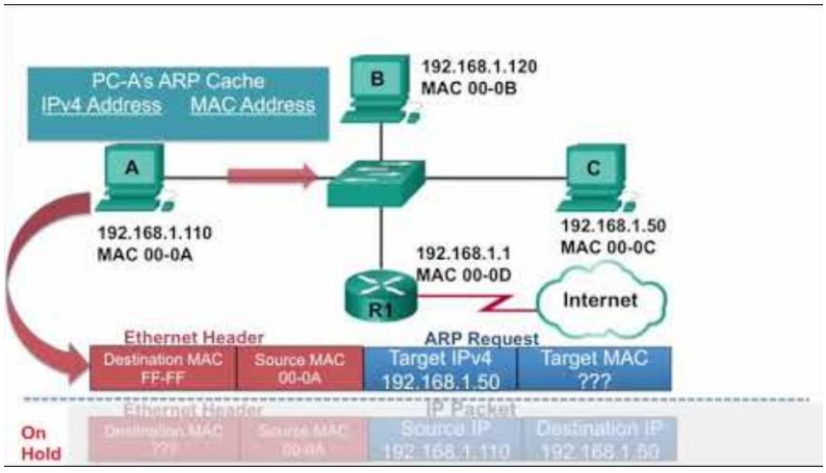
ARP Funktionen

- Um ein Datenpaket zu senden, sucht ein Gerät in seiner **ARP-Tabelle nach einer Ziel-IPv4-Adresse** und der zugehörigen MAC-Adresse.
- Befindet sich die Ziel-IPv4-Adresse **im selben Netzwerk**, sucht das Gerät in der ARP-Tabelle nach dieser Adresse.
- Befindet sich die Ziel-IPv4-Adresse **in einem anderen Netzwerk**, sucht das Gerät in der ARP-Tabelle nach der IPv4-Adresse des **Standardgateways**.
- Wird die IPv4-Adresse gefunden, wird ihre zugehörige MAC-Adresse als Ziel-MAC-Adresse im Datenpaket verwendet.
- Wird **kein Eintrag in der ARP-Tabelle** gefunden, sendet das Gerät eine **ARP-Anfrage**.

tgm [Quelle: CCNAv7: Switching, Routing, and Wireless Essentials v7.0 (SRWE), by Cisco Networking Academy, Cisco Press]

NETZWERKTECHNIK / SEMESTER 3

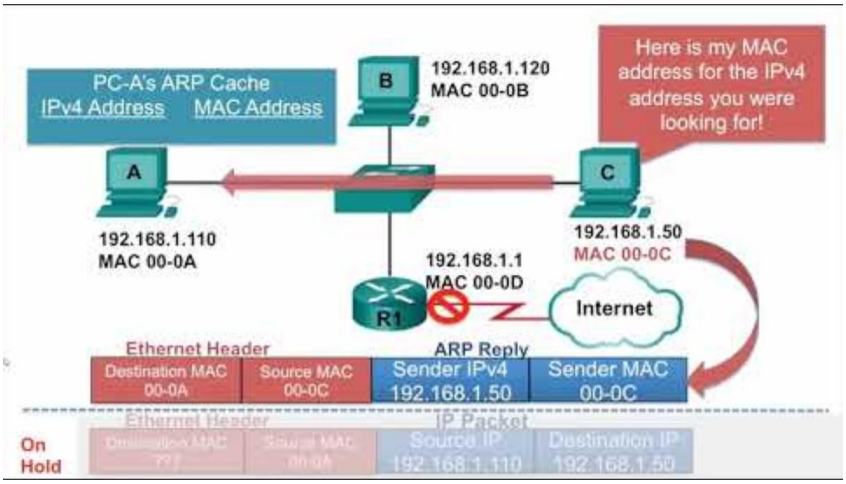
Video ARP Request



tgm [Quelle: https://www.youtube.com/watch?v=dGTbwvhoHww – letzter Abruf 14.2.2026]

NETZWERKTECHNIK / SEMESTER 3

Video ARP Reply

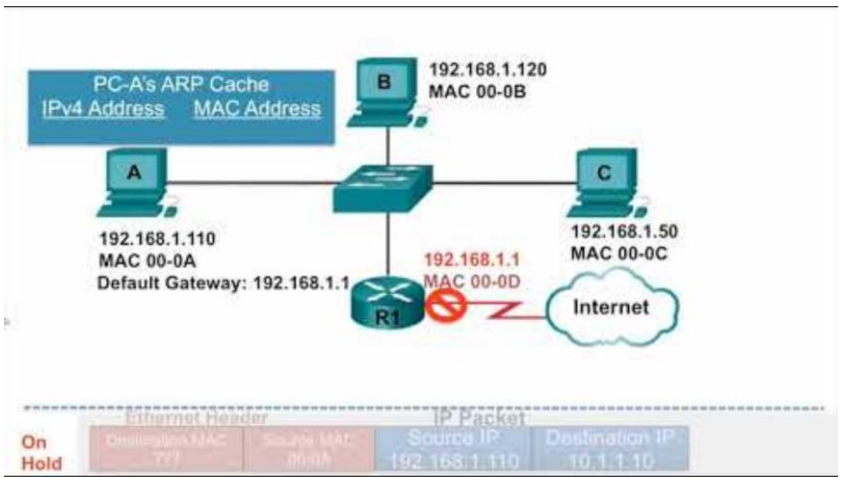


tgm [Quelle: https://www.youtube.com/watch?v=dFEqT7hvBTA – letzter Abruf 14.2.2026]

61

NETZWERKTECHNIK / SEMESTER 3

Video Rolle on ARP in Remote Netzwerken

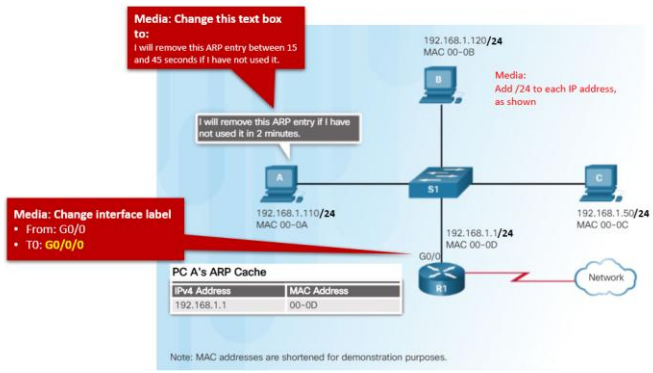


tgm [Quelle: https://www.youtube.com/watch?v=5wpsNlP19QE – letzter Abruf 14.2.2026]

62

Entfernen von Einträgen aus einer ARP-Tabelle

- Einträge in der ARP-Tabelle sind nicht permanent und werden gelöscht, sobald der ARP-Cache-Timer nach einer **festgelegten Zeit** abläuft.
- Die Dauer des ARP-Cache-Timers ist **betriebssystemabhängig**.
- ARP-Tabelleneinträge können auch **manuell** vom Administrator gelöscht werden.



Entfernen von Einträgen aus einer ARP-Tabelle

- Der Befehl `**show ip arp**` zeigt die ARP-Tabelle eines Cisco-Routers an.
- Der Befehl `**arp -a**` zeigt die ARP-Tabelle eines Windows-10-PCs an.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
```

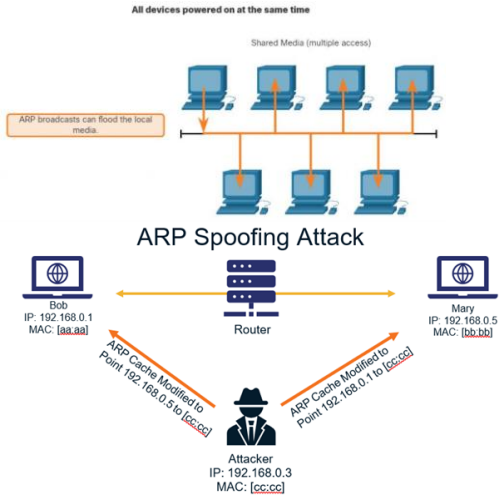
```
C:\Users\PC> arp -a

Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
```

NETZWERKTECHNIK / SEMESTER 1 und 2

ARP-Probleme – ARP-Broadcasting und ARP-Spoofing

- ARP-Anfragen werden von jedem Gerät im lokalen Netzwerk empfangen und verarbeitet.
- **Übermäßige ARP-Broadcasts können zu Leistungseinbußen führen.**
- **ARP-Antworten können von einem Bedrohungsakteur gefälscht werden**, um einen ARP-Poisoning-Angriff durchzuführen.
- Switches auf Unternehmensebene umfassen Abwehrtechniken zum Schutz vor ARP-Angriffen.

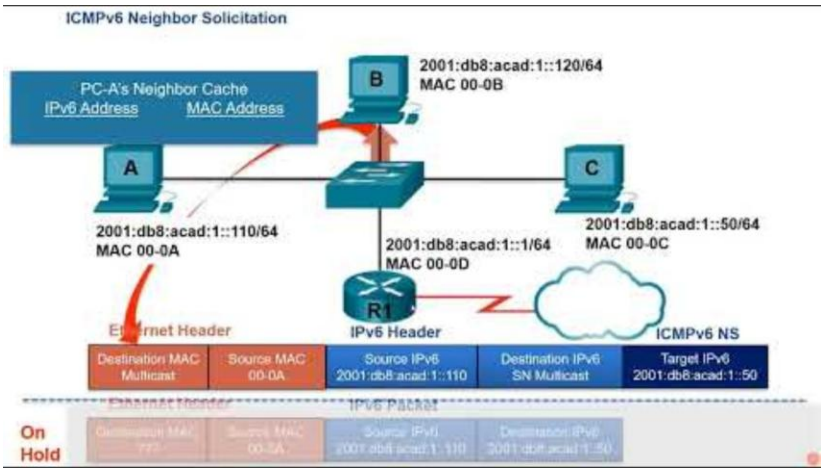


tgm [Quelle: https://www.thesslstore.com/blog/everything-you-need-to-know-about-arp-spoofing/ - letzter Abruf 21.08.2025]

65

NETZWERKTECHNIK / SEMESTER 3

IPv6 Neighbor Discovery



tgm [Quelle: https://www.youtube.com/watch?v=hJ7Mc3LLWXI – letzter Abruf 14.2.2026]

66

NETZWERKTECHNIK / SEMESTER 3

IPv6 Neighbor Discovery Nachrichten

Das IPv6 Neighbor Discovery (ND)-Protokoll bietet:

- **Adressauflösung**
- **Routererkennung**
- **Umleitungsdienste (Redirection)**

- **ICMPv6 Neighbor Solicitation (NS)**- und **Neighbor Advertisement (NA)**-Nachrichten werden für die Kommunikation zwischen Geräten, wie z. B. die Adressauflösung, verwendet.
- **ICMPv6 Router Solicitation (RS)**- und **Router Advertisement (RA)**-Nachrichten werden für die Kommunikation zwischen Geräten und Routern zur Routererkennung verwendet.
- **ICMPv6-Redirect-Nachrichten** werden von Routern zur besseren Auswahl des nächsten Hops verwendet.

NETZWERKTECHNIK / SEMESTER 3

IPv6 Neighbor Discovery – Addressauflösung

- IPv6-Geräte **verwenden ND**, um die MAC-Adresse einer bekannten IPv6-Adresse aufzulösen.
- **ICMPv6 Neighbor Solicitation-Nachrichten** werden über spezielle Ethernet- und IPv6-Multicast-Adressen gesende