

# Praktikum Rechnernetze

## Versuch 1

vom 28.04.2020

Troubleshooting TCP/IP

Protokoll Gruppe 1

Yannick Möller (ym018)

Bernd Maier (bm075)

Michael Vanhee (mv068)

Rebecca Mombrei (rm048)

## Vorbereitung

Zur Vorbereitung wurden die Funktion und die Berechnung von IP-Adressen und Subnetzen mit Hilfe der nachfolgenden Tabelle wiederholt.

IP-Adresse	Subnetz-Maske	Klasse	Netz-Adresse	Anzahl Subnetze	Broadcast-Adresse	Anzahl Hosts
192.168.100.195	255.255.255.240	/28 C	192.168.100.192	$2^4 / 16$	192.168.100.207	14
192.168.100.172	255.255.255.224	/27 C	192.168.100.160	$2^3 / 8$	192.168.100.191	30
192.168.100.130	255.255.255.224	/27 C	192.168.100.128	$2^3 / 8$	192.168.100.159	30
192.168.100.188	255.255.255.192	/26 C	192.168.100.128	$2^2 / 4$	192.168.100.191	62
192.168.1.42	255.255.255.0	/24 C	192.168.1.0	$2^0 / 1$	192.168.100.255	254

## Aufgabenteil 1 - Tools des Betriebssystems

### IP-Konfiguration des PC

Mit dem Befehl **ipconfig** bzw. **ipconfig /all** lassen sich die Netzwerkadapter des Computers mit ihren Eigenschaften in der Shell anzeigen.

Mithilfe des Kommandos **hostname** lässt sich der Klartextname des PCs abfragen.

Diesen Versuch haben wir komplett an den eigenen Heimrechnern durchgeführt.

	Bernd Maier	Yannick Möller	Rebecca Mombrei	Michael Vanhee
IP-Adresse	192.168.178.34	192.168.178.51	192.168.178.37	192.168.0.42
Subnetzmaske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.178.1	192.168.178.1	192.168.178.1	192.168.0.1
DNS-Server	192.168.178.1	192.168.178.1	192.168.178.1	192.168.0.2
Hostname	desktop	Yannick-PC	Beccas-HP	CXMP.local
Router/Netzwerk	Fritz!Box	Fritz!Box	Fritz!Box	Linksys OpenWRT, unRAID Pi-Hole

## Korrekte Installation der Netzwerkkarten-Treiber überprüfen

Nachdem der Netzwerktreiber eines Geräts erfolgreich installiert worden ist, kann man dies mit einem einfachen PING testen, notfalls auch im lokalen Netzwerk.

Über einen **ping** an den Router, lässt sich die Verbindung im eigenen Netzwerk überprüfen. Im konkreten Fall ist der Rechner über DLAN und das Stromnetz mit der Fritz!Box verbunden.

```
C:\Users\Yannick>ping 192.168.178.1

Ping wird ausgeführt für 192.168.178.1 mit 32 Bytes Daten:
Antwort von 192.168.178.1: Bytes=32 Zeit=2ms TTL=64
Antwort von 192.168.178.1: Bytes=32 Zeit=2ms TTL=64
Antwort von 192.168.178.1: Bytes=32 Zeit=2ms TTL=64
Antwort von 192.168.178.1: Bytes=32 Zeit=2ms TTL=64

Ping-Statistik für 192.168.178.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 2ms, Maximum = 2ms, Mittelwert = 2ms
```

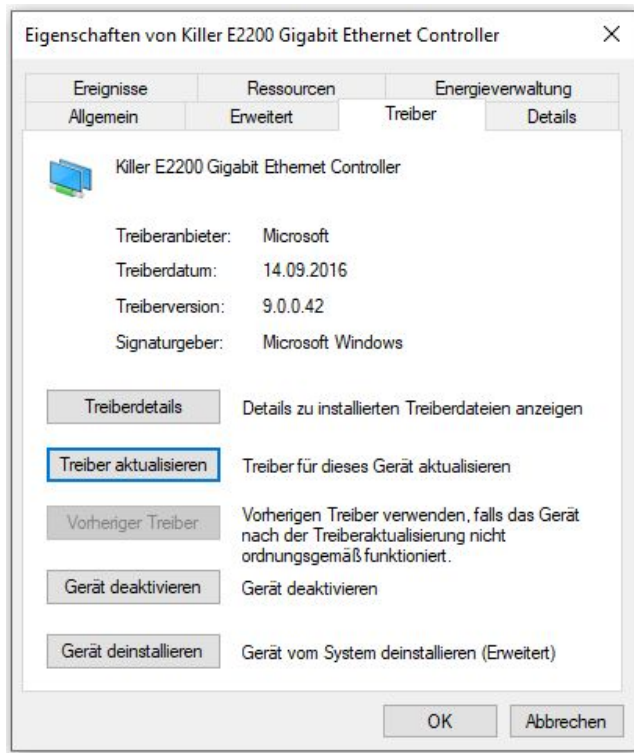
Über einen **ping** an eine IP-Adresse (in dem Fall der DNS-Server von Google) lässt sich die Verbindung ins Internet überprüfen. In diesem Fall dauerte ein Ping im Mittelwert 27ms.

```
C:\Users\Yannick>ping 8.8.8.8

Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Antwort von 8.8.8.8: Bytes=32 Zeit=30ms TTL=56
Antwort von 8.8.8.8: Bytes=32 Zeit=30ms TTL=56
Antwort von 8.8.8.8: Bytes=32 Zeit=35ms TTL=56
Antwort von 8.8.8.8: Bytes=32 Zeit=15ms TTL=56

Ping-Statistik für 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 15ms, Maximum = 35ms, Mittelwert = 27ms
```

Ferner kann man auch über den Windows **Geräte-Manager** direkt die Treiber-Details auslesen und ggf. aktualisieren.



Unter Mac- & Linux Geräten lässt sich eine ähnliche Abfrage zu den Details der IP-Konfigurationen über den Befehl **ifconfig -a** ausführen.

```
blauwiggie@CXMPC: ~
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether ac:de:48:00:11:22
    inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x4
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (100baseTX <full-duplex>)
    status: active
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 3e:22:fb:29:03:71
    media: autoselect
    status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 3c:22:fb:29:03:71
    inet 192.168.0.152 netmask 0xfffff00 broadcast 192.168.0.255
    inet6 fe80::c4f:66a1:dc65:4053%en0 prefixlen 64 secured scopeid 0x6
    inet6 2a02:8070:4ac:1400:8fc:3baa:eb14:d2d6 prefixlen 64 autoconf secured
    inet6 2a02:8070:4ac:1400:7c36:751b:781:8d7b prefixlen 64 autoconf temporary
    inet6 2a02:8070:4ac:1400::aedb prefixlen 64 dynamic
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    options=400<CHANNEL_IO>
    ether 0e:22:fb:29:03:71
    media: autoselect
    status: inactive
```

Nach dem Befehl **"ipconfig /flushdns"** ist der Cache geleert, nach einem einmaligen Aufruf der Website ["www.google.com"](http://www.google.com) wird dieser aber sofort wieder mit unzähligen Einträgen überschwemmt.

Bernd Maier (bm075), Yannick Möller (ym018), Rebecca Mombrei (rm048), Michael Vanhee (mv068)

## Address Resolution Protocol ARP

Mit Hilfe der ARP-Tabelle lassen sich bekannte IP-Adressen zu physikalischen MAC-Adressen zuordnen.

Nach Ausführung des Befehls **arp -a** wird die ARP-Tabelle ausgegeben (links ein Ausschnitt).

Schnittstelle: 192.168.178.37 --- 0xb			Schnittstelle: 192.168.178.37 --- 0xb		
Internetadresse	Physische Adresse	Typ	Internetadresse	Physische Adresse	Typ
192.168.178.1	38-10-d5-b8-47-a1	dynamisch	192.168.178.1	38-10-d5-b8-47-a1	dynamisch
192.168.178.20	00-11-32-0a-b5-04	dynamisch	192.168.178.20	00-11-32-0a-b5-04	dynamisch
192.168.178.28	fc-3f-db-23-ce-e6	dynamisch	192.168.178.28	fc-3f-db-23-ce-e6	dynamisch
192.168.178.62	62-ff-4d-d4-dc-16	dynamisch	192.168.178.62	62-ff-4d-d4-dc-16	dynamisch
192.168.178.80	24-5e-be-22-36-56	dynamisch	192.168.178.77	a8-db-03-61-2f-77	dynamisch
192.168.178.83	ac-6f-bb-69-33-3a	dynamisch	192.168.178.80	24-5e-be-22-36-56	dynamisch
192.168.178.93	bc-83-85-e0-e2-88	dynamisch	192.168.178.83	ac-6f-bb-69-33-3a	dynamisch
192.168.178.109	32-3a-fd-02-23-b0	dynamisch	192.168.178.93	bc-83-85-e0-e2-88	dynamisch
192.168.178.255	ff-ff-ff-ff-ff-ff	statisch	192.168.178.109	32-3a-fd-02-23-b0	dynamisch
224.0.0.22	01-00-5e-00-00-16	statisch	192.168.178.255	ff-ff-ff-ff-ff-ff	statisch
224.0.0.251	01-00-5e-00-00-fb	statisch	224.0.0.22	01-00-5e-00-00-16	statisch
224.0.0.252	01-00-5e-00-00-fc	statisch	224.0.0.251	01-00-5e-00-00-fb	statisch
239.255.255.250	01-00-5e-7f-ff-fa	statisch	224.0.0.252	01-00-5e-00-00-fc	statisch
255.255.255.255	ff-ff-ff-ff-ff-ff	statisch	239.255.255.250	01-00-5e-7f-ff-fa	statisch
			255.255.255.255	ff-ff-ff-ff-ff-ff	statisch

Nach Senden eines **ping** an ein Handy wird dessen IP-Adresse (192.168.178.77) und die MAC-Adresse in die ARP-Tabelle eingetragen (siehe Ausschnitt rechtes Bild).

Die MAC-Adresse ist **global** vergeben und besteht aus zwei Teilen. Die ersten 6 hexadezimalen Zeichen liefern die Herstellerkennung, die letzten 6 Zeichen die Gerätekennung.

Die Herstellerkennung 00-0B-61 ist beispielsweise die Friedrich Lütze GmbH & Co. KG.

Für den Fall dass sich im Netzwerk ein weiterer PC mit einer bereits vergebenen IP-Adresse registrieren möchte wird dies unterbunden. Eines der beiden Endgeräte wird also "deaktiviert" und verliert die Verbindung. Gründe hierfür sind z.B. eine Zuweisung der gleichen statischen IP-Adresse durch den Netzwerkadministrator oder ein Fehler im DHCP-Server.

	Vorteile	Nachteile
Statische ARP-Tabelle	<ul style="list-style-type: none"> <li>- können manuell hinzugefügt werden</li> <li>- statische Einträge bleiben bis zum Ausschalten erhalten</li> </ul>	<ul style="list-style-type: none"> <li>- statische Einträge belegen Speicher im ARP-Cache, auch wenn sie nicht gebraucht werden</li> </ul>
Dynamische ARP-Tabelle	<ul style="list-style-type: none"> <li>- automatische Erneuerung bei zu vielen Einträgen</li> <li>- automatischer Eintrag neuer Geräte, damit nicht jedes Mal die MAC-Adresse neu abgefragt werden muss</li> </ul>	<ul style="list-style-type: none"> <li>- Einträge werden nach einer bestimmten Zeit gelöscht</li> <li>- Der ARP-Cache hat nur eine bestimmte Größe</li> </ul>

Da der ARP-Cache nur eine bestimmte Größe hat, werden alte Einträge nach einer bestimmten Zeit entfernt. Die Einträge aus dem ARP-Cache haben standardmäßig eine Gültigkeit von 5 Minuten. Nach Ablauf der Zeit werden die Einträge gelöscht.

Bernd Maier (bm075), Yannick Möller (ym018), Rebecca Mombrei (rm048), Michael Vanhee (mv068)

## PING

Bei einem simplen **ping** Befehl wird auch lediglich die IP-Adresse angezeigt, erweitert man den Befehl um den Parameter “-t” wird der Computer-/Servername direkt aufgelöst und angezeigt:

```
C:\Users\esken>ping -a 8.8.8.8

Ping wird ausgeführt für dns.google [8.8.8.8] mit 32 Bytes Daten:
Antwort von 8.8.8.8: Bytes=32 Zeit=28ms TTL=57
Antwort von 8.8.8.8: Bytes=32 Zeit=39ms TTL=57
Antwort von 8.8.8.8: Bytes=32 Zeit=28ms TTL=57
Antwort von 8.8.8.8: Bytes=32 Zeit=41ms TTL=57

Ping-Statistik für 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 28ms, Maximum = 41ms, Mittelwert = 34ms
```

Bei einem **ping** mit größerer Länge gehen öfter Pakete verloren.

```
C:\Users\Yannick>ping -a -t 192.168.178.36 -l 65500

Ping wird ausgeführt für YannickOnePlus3.fritz.box [192.168.178.36] mit 65500 Bytes Daten:
Antwort von 192.168.178.36: Bytes=65500 Zeit=83ms TTL=64
Antwort von 192.168.178.36: Bytes=65500 Zeit=49ms TTL=64
Antwort von 192.168.178.36: Bytes=65500 Zeit=731ms TTL=64
Antwort von 192.168.178.36: Bytes=65500 Zeit=323ms TTL=64
Antwort von 192.168.178.36: Bytes=65500 Zeit=155ms TTL=64
Antwort von 192.168.178.36: Bytes=65500 Zeit=132ms TTL=64
Zeitüberschreitung der Anforderung.
Antwort von 192.168.178.36: Bytes=65500 Zeit=64ms TTL=64
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 192.168.178.36:
    Pakete: Gesendet = 12, Empfangen = 7, Verloren = 5
    (41% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 49ms, Maximum = 731ms, Mittelwert = 219ms
```



```
C:\Users\Yannick>ping -t 192.168.178.36

Ping wird ausgeführt für 192.168.178.36 mit 32 Bytes Daten:
Antwort von 192.168.178.36: Bytes=32 Zeit=149ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=3ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=54ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=164ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=80ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=96ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=103ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=112ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=227ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=37ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=252ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=273ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=76ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=806ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=444ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=4ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=776ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=351ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=153ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=294ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=180ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=690ms TTL=64
Zeitüberschreitung der Anforderung.
Antwort von 192.168.178.36: Bytes=32 Zeit=280ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=56ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=170ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=394ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=80ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=332ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=226ms TTL=64
Antwort von 192.168.178.36: Bytes=32 Zeit=244ms TTL=64

Ping-Statistik für 192.168.178.36:
    Pakete: Gesendet = 31, Empfangen = 30, Verloren = 1
    (3% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 3ms, Maximum = 806ms, Mittelwert = 236ms
```

Bei einem dauerhaften **ping** von einem Rechner, der per LAN verbunden ist, an ein Smartphone im WLAN desselben Netzwerks gab es sehr unterschiedliche Zeitwerte.

Wie gross ist der maximale Wert, den Ping über ein Ethernet-Netz erlaubt?

Betrachten Sie dazu den Aufbau eines Ethernet-Rahmens und berücksichtigen Sie, dass der ICMP Header mindestens 8 Byte "verbraucht"?

Abweichend von der Versuchsbeschreibung liegt die Range für die Länge der Pakete bei:

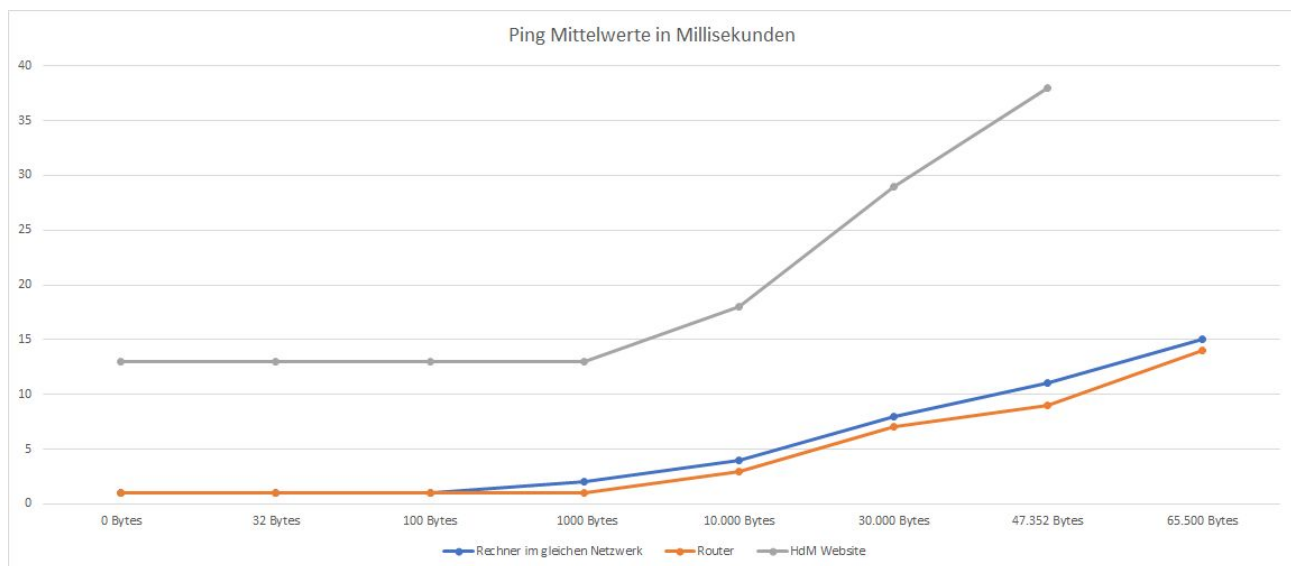
```
C:\Users\esken>ping -l 65527 8.8.8.8
Ungültiger Wert für die Option -l. Der Gültige Bereich liegt zwischen 0 und 65500.
```

Bernd Maier (bm075), Yannick Möller (ym018), Rebecca Mombrei (rm048), Michael Vanhee (mv068)

## Warum weisen manche ISP **ping** Pakete ab, sobald sie das Netz des ISP betreten?

Nehmen wir zum Vergleich die HdM. Auch dort wird durch ICMP (Internet Control Message Protocol) unterbunden, dass eine Antwort zurückgeliefert wird. Ähnliches passiert auch in manch anderen Netzen. Gründe dazu gibt es viele, das Prinzip in der Computer- und Netzwerksicherheit heißt "Security through obscurity" ("Sicherheit durch Unklarheit").

## Vergleich mittlerer Antwortzeiten von ping-Paketen unterschiedlicher Länge

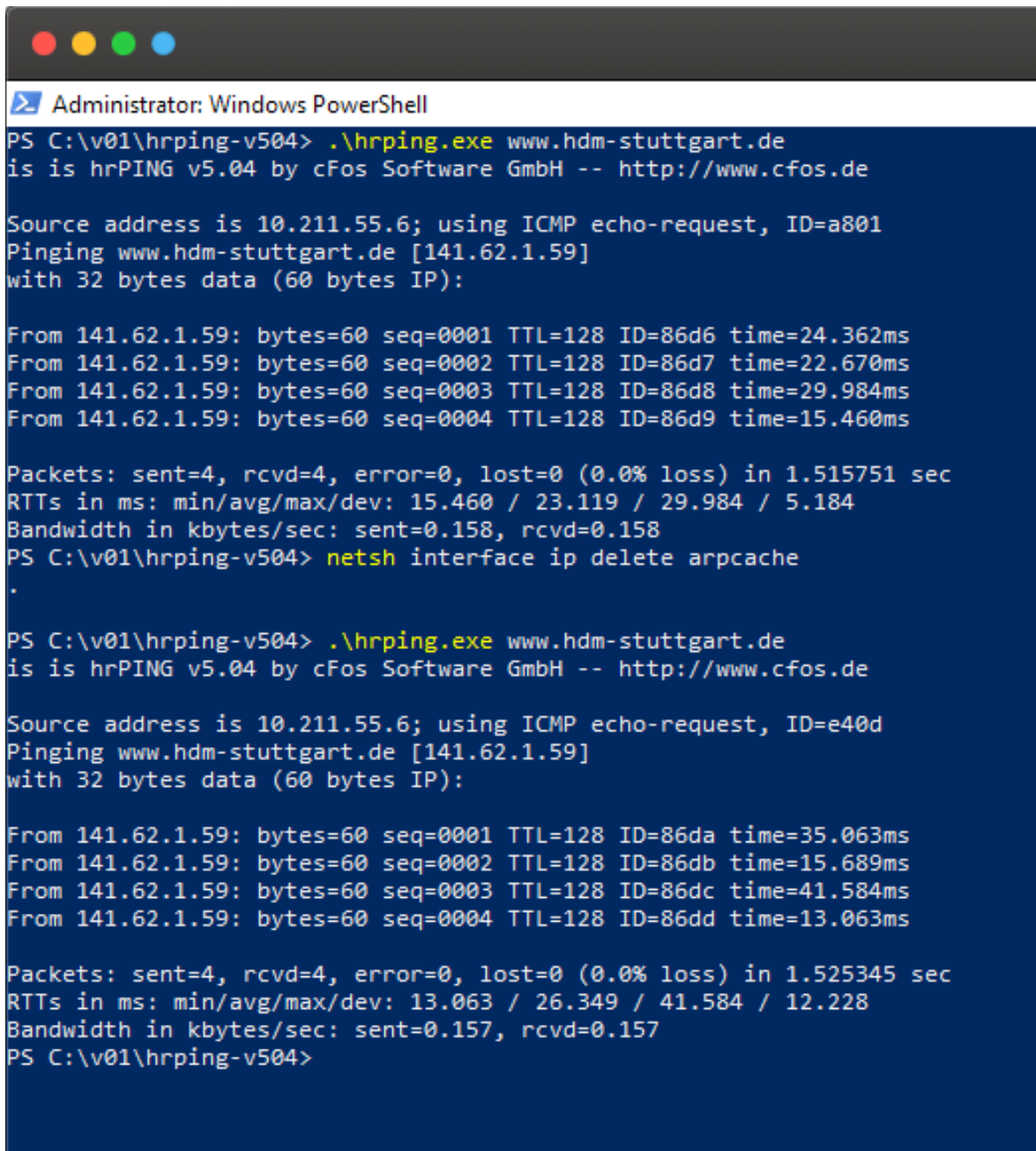


Das Diagramm zeigt die mittleren Antwortzeiten von 50 pings je Länge zum eigenen Router, einem Rechner im gleichen Netzwerk und der HdM-Website, also einer Adresse außerhalb des Netzwerks. Der Router hat kürzere Antwortzeiten als der Rechner im gleichen Netzwerk, da die ping-Pakete immer zuerst an den Router gesendet werden, und dieser die Pakete an den anderen Rechner weiterleitet. Am längsten sind die Antwortzeiten der HdM-Website, da die ping-Pakete über mehrere Router geleitet werden. Auffällig ist außerdem, dass die HdM-Website auf pings nur bis zur Paketlänge von 47.352 Bytes reagiert. Alle größeren Pakete führen zu einer Zeitüberschreitung.



## hrping

Wie zu erkennen ist, sind die Antwortzeiten im ersten hrping noch OK. Nachdem der komplette ARP-Cache mit "netsh interface ip delete arpcache" gelöscht worden ist, sind die Antwortzeiten beim ersten und dritten Ping deutlich höher, dafür gleichen sie sich mit dem zweiten und vierten wieder aus.



```
Administrator: Windows PowerShell
PS C:\v01\hrping-v504> .\hrping.exe www.hdm-stuttgart.de
is is hrPING v5.04 by cFos Software GmbH -- http://www.cfos.de

Source address is 10.211.55.6; using ICMP echo-request, ID=a801
Pinging www.hdm-stuttgart.de [141.62.1.59]
with 32 bytes data (60 bytes IP):

From 141.62.1.59: bytes=60 seq=0001 TTL=128 ID=86d6 time=24.362ms
From 141.62.1.59: bytes=60 seq=0002 TTL=128 ID=86d7 time=22.670ms
From 141.62.1.59: bytes=60 seq=0003 TTL=128 ID=86d8 time=29.984ms
From 141.62.1.59: bytes=60 seq=0004 TTL=128 ID=86d9 time=15.460ms

Packets: sent=4, rcvd=4, error=0, lost=0 (0.0% loss) in 1.515751 sec
RTTs in ms: min/avg/max/dev: 15.460 / 23.119 / 29.984 / 5.184
Bandwidth in kbytes/sec: sent=0.158, rcvd=0.158
PS C:\v01\hrping-v504> netsh interface ip delete arpcache
.

PS C:\v01\hrping-v504> .\hrping.exe www.hdm-stuttgart.de
is is hrPING v5.04 by cFos Software GmbH -- http://www.cfos.de

Source address is 10.211.55.6; using ICMP echo-request, ID=e40d
Pinging www.hdm-stuttgart.de [141.62.1.59]
with 32 bytes data (60 bytes IP):

From 141.62.1.59: bytes=60 seq=0001 TTL=128 ID=86da time=35.063ms
From 141.62.1.59: bytes=60 seq=0002 TTL=128 ID=86db time=15.689ms
From 141.62.1.59: bytes=60 seq=0003 TTL=128 ID=86dc time=41.584ms
From 141.62.1.59: bytes=60 seq=0004 TTL=128 ID=86dd time=13.063ms

Packets: sent=4, rcvd=4, error=0, lost=0 (0.0% loss) in 1.525345 sec
RTTs in ms: min/avg/max/dev: 13.063 / 26.349 / 41.584 / 12.228
Bandwidth in kbytes/sec: sent=0.157, rcvd=0.157
PS C:\v01\hrping-v504>
```

## tracert

Verfolgung der Route zum Server einer neuseeländischen Hochschule:

```
C:\Users\Rebecca>tracert www.aut.ac.nz

Routenverfolgung zu bax.aut.ac.nz [156.62.238.90]
über maximal 30 Hops:

 1    1 ms    1 ms    1 ms    fritz.box [192.168.178.1]
 2    5 ms    4 ms    4 ms    62.155.245.86
 3   12 ms   13 ms   10 ms    217.0.195.197
 4   10 ms   10 ms   10 ms    217.0.195.197
 5   10 ms   13 ms   10 ms    ffm-b4-link.telial.net [213.248.93.186]
 6  150 ms  150 ms  150 ms    ffm-bb2-link.telial.net [62.115.114.90]
 7    *      *      *      Zeitüberschreitung der Anforderung.
 8   99 ms  100 ms   99 ms    rest-bb1-link.telial.net [62.115.122.159]
 9  158 ms  158 ms  157 ms    las-b21-link.telial.net [62.115.137.37]
10  157 ms  157 ms  158 ms    tnzusa-ic-316539-las-b21.c.telial.net [62.115.145.207]
11  152 ms  153 ms  152 ms    ae0-10.lebr7.global-gateway.net.nz [202.50.232.41]
12  283 ms  279 ms  279 ms    xe1-0-5.tkbr12.global-gateway.net.nz [202.50.232.17]
13  274 ms  274 ms  274 ms    ae4-10.tkbr11.global-gateway.net.nz [122.56.119.110]
14  279 ms  279 ms  279 ms    aut-int.tkbr11.global-gateway.net.nz [202.50.234.154]
15  277 ms  276 ms  276 ms    wahaapu1-3.aut.ac.nz [156.62.3.247]
16  283 ms  282 ms  283 ms    156.62.1.251
17    *      *      *      Zeitüberschreitung der Anforderung.
18  289 ms  289 ms  288 ms    bax.aut.ac.nz [156.62.238.90]

Ablaufverfolgung beendet.
```

Die Pakete werden über den zentralen Peering-Point in Frankfurt am Main (ffm) und Los Angeles (las) geleitet. Die langen Antwortzeiten ergeben sich dadurch, dass die Pakete den Hin- und Rückweg durch mehrere Ozeane zurücklegen müssen.

Verfolgung zu [www.aol.com](http://www.aol.com)

```
C:\Users\esken>tracert www.aol.com

Routenverfolgung zu media-router-aol1.prod.g03.yahoodns.net [188.125.72.167]
über maximal 30 Hops:

 1    4 ms    3 ms    5 ms    fritz.box [192.168.178.1]
 2   38 ms   22 ms   38 ms    mt7321-2.sdt.net [195.245.0.40]
 3   23 ms   24 ms   23 ms    mt70is.sdt.net [195.245.0.235]
 4   28 ms   26 ms   28 ms    gate60d.sdt.net [195.245.0.233]
 5   33 ms   33 ms   34 ms    pat2.ams.yahoo.com [80.249.209.163]
 6   52 ms   52 ms   55 ms    ae-5.pat2.iry.yahoo.com [66.196.65.154]
 7   53 ms   52 ms   52 ms    et-11-1-2.msrl.ir2.yahoo.com [66.196.65.23]
 8   57 ms   53 ms   53 ms    lo0.fab3-1-gdc.ir2.yahoo.com [77.238.190.4]
 9   51 ms   52 ms   52 ms    usw2-1-lbb.ir2.yahoo.com [77.238.190.105]
10   51 ms   51 ms   51 ms    media-router-aol1.prod.media.vip.ir2.yahoo.com [188.125.72.167]
```

Wie man sehen kann wird die Anfrage vom Router an den ISP sdt.net weitergereicht und von dort über verschiedene Server an ans Ziel übermittelt.

Bernd Maier (bm075), Yannick Möller (ym018), Rebecca Mombrei (rm048), Michael Vanhee (mv068)

Mithilfe von **tracert -w** lässt sich das Zeitlimit bis zur Überschreitung angeben. Wird dieser Wert hochgestellt, gibt es keine Zeitüberschreitungen mehr.

Im nachfolgenden Screenshot mit **tracert -w 1000 [www.hdm-stuttgart.de](http://www.hdm-stuttgart.de)** lässt sich der Weg vom Heimrechner zur HdM aufzeichnen. Der DECIX in Frankfurt und das BELWUE sind eindeutig erkennbar.

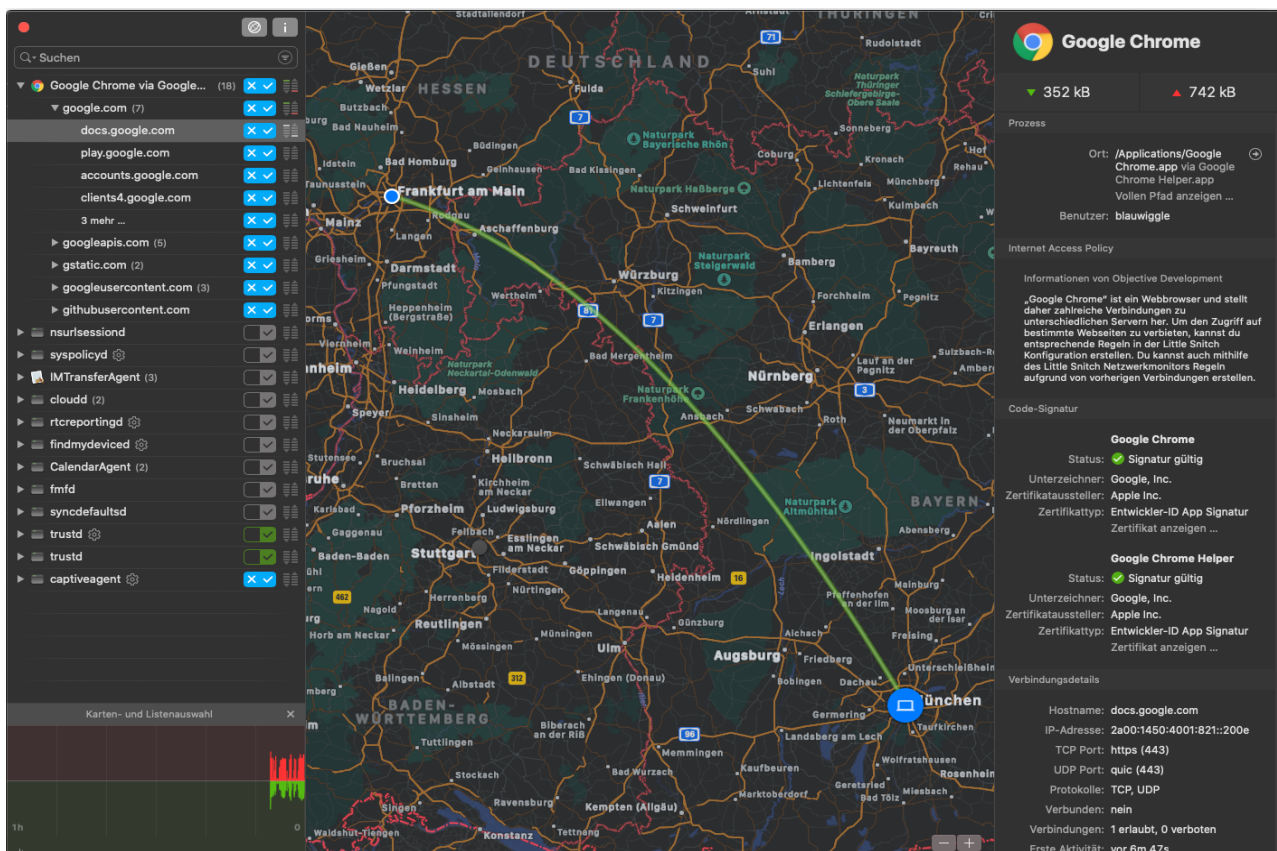
```
C:\Users\Yannick>tracert -w 1000 www.hdm-stuttgart.de

Routenverfolgung zu www.hdm-stuttgart.de [141.62.1.59]
über maximal 30 Hops:

 1  18 ms    6 ms    8 ms  fritz.box [192.168.178.1]
 2  21 ms   11 ms   10 ms  stu1903aihr001.versatel.de [62.214.63.95]
 3  15 ms   20 ms   10 ms  62.214.38.173
 4  13 ms   19 ms   23 ms  62.214.37.130
 5  33 ms   20 ms   41 ms  Frankfurt-TC-1-10GE-0-2-0-6.belwue.net [80.81.194.106]
 6  21 ms   22 ms   20 ms  fra-decix-1-te0-1-0-7.belwue.net [129.143.59.249]
 7  23 ms   24 ms   21 ms  stu-nwz-a99-hu0-2-0-0.belwue.net [129.143.60.112]
 8  18 ms   17 ms   17 ms  stu-nwz-1-te0-7-0-17.belwue.net [129.143.60.69]
 9  20 ms   20 ms   21 ms  stu-hdm-1-te0-0-5.belwue.net [129.143.56.46]
10  23 ms   37 ms   44 ms  firewall.hdm-stuttgart.de [141.62.60.1]
11  19 ms   41 ms   41 ms  iz-www-1.hdm-stuttgart.de [141.62.1.59]

Ablaufverfolgung beendet.
```

Am DE-CIX ist der Knotenpunkt für ganz Deutschland, der gesamte Traffic läuft durch diesen Knotenpunkt.



Bernd Maier (bm075), Yannick Möller (ym018), Rebecca Mombrei (rm048), Michael Vanhee (mv068)



Über die Seite der DENIC konnten bis vor einigen Monaten Abfragen gestellt werden, welche Domain welchem Eigentümer gehören. Durch neue Datenschutzbestimmungen sind Abfragen durch Dritte nicht mehr, beziehungsweise nur noch unter bestimmten Umständen (bei Rechtsverletzungen, durch Behörden o.Ä.), möglich.

## Die Domain hdm-stuttgart.de ist bereits registriert.

Letzte Aktualisierung: 22.04.2015

### Technische Daten

#### Nameserver

dns1.belwue.de
dns3.belwue.de
iz-net-2.hdm-stuttgart.de 141.62.1.2
iz-net-3.hdm-stuttgart.de 141.62.1.3
iz-net-4.hdm-stuttgart.de 141.62.1.4

## PathPing

Hier wurde die Route zur HdM von einem Heimrechner aufgezeichnet. Angeschlossen über LAN an eine Fritz!Box (Zeile 1) mit einem 1&1-Vertrag (versatel, Zeile 2)

```
C:\Users\Yannick>pathping www.hdm-stuttgart.de

Routenverfolgung zu "www.hdm-stuttgart.de" [141.62.1.53]
über maximal 30 Hops:
 0 Yannick-PC.fritz.box [192.168.178.51]
 1 fritz.box [192.168.178.1]
 2 stu1903aihr001.versatel.de [62.214.63.95]
 3 62.214.38.173
 4 62.214.37.134
 5 Frankfurt-TC-1-10GE-0-2-0-6.belwue.net [80.81.194.106]
 6 fra-decix-1-te0-1-0-7.belwue.net [129.143.59.249]
 7 stu-nwz-a99-hu0-2-0-0.belwue.net [129.143.60.112]
 8 stu-nwz-1-te0-7-0-17.belwue.net [129.143.60.69]
 9 stu-hdm-1-te0-0-5.belwue.net [129.143.56.46]
10 firewall.hdm-stuttgart.de [141.62.60.1]
11 iz-www-2.hdm-stuttgart.de [141.62.1.53]

Berechnung der Statistiken dauert ca. 275 Sekunden...
Quelle zum Abs. Knoten/Verbindung
Abs. Zeit Verl./Ges.= % Verl./Ges.= % Adresse
 0
 1 7ms 0/ 100 = 0% 0/ 100 = 0% Yannick-PC.fritz.box [192.168.178.51]
 2 15ms 0/ 100 = 0% 0/ 100 = 0% fritz.box [192.168.178.1]
 3 17ms 0/ 100 = 0% 0/ 100 = 0% stu1903aihr001.versatel.de [62.214.63.95]
 4 19ms 0/ 100 = 0% 0/ 100 = 0% 62.214.38.173
 5 --- 100/ 100 =100% 100/ 100 =100% 62.214.37.134
 6 20ms 0/ 100 = 0% 0/ 100 = 0% Frankfurt-TC-1-10GE-0-2-0-6.belwue.net [80.81.194.106]
 7 26ms 0/ 100 = 0% 0/ 100 = 0% fra-decix-1-te0-1-0-7.belwue.net [129.143.59.249]
 8 22ms 0/ 100 = 0% 0/ 100 = 0% stu-nwz-a99-hu0-2-0-0.belwue.net [129.143.60.112]
 9 24ms 0/ 100 = 0% 0/ 100 = 0% stu-nwz-1-te0-7-0-17.belwue.net [129.143.60.69]
10 --- 100/ 100 =100% 100/ 100 =100% stu-hdm-1-te0-0-5.belwue.net [129.143.56.46]
11 23ms 0/ 100 = 0% 0/ 100 = 0% firewall.hdm-stuttgart.de [141.62.60.1]
Ablaufverfolgung beendet.
```

Wie man am Beispiel des Knotens in Frankfurt (Z.5) und der Firewall der HdM (Z.10) sehen kann, wird hier kein Ping per **ICMP** gestattet.

Bernd Maier (bm075), Yannick Möller (ym018), Rebecca Mombrei (rm048), Michael Vanhee (mv068)

## netstat

Mit **netstat** kann man Statistiken sehen, welche Ports geöffnet sind oder zu welchen Rechnern Verbindungen geöffnet sind. Hier kann man beispielsweise sehen, ob man mit einem Backdoor infiziert ist. Die 10.211.55.6 IP liegt daran, dass hier der Parallels Desktop virtuelle Netzwerkadapter verwendet wird, der eine Bridge zum macOS nutzt.

```
Administrator: Windows PowerShell X + v

Aktive Verbindungen

Proto  Lokale Adresse      Remoteadresse        Status
-----
TCP    10.211.55.6:49670    40.90.137.126:https   HERGESTELLT
TCP    10.211.55.6:49671    51.143.111.7:https    WARTEND
TCP    10.211.55.6:49672    51.105.249.228:https  HERGESTELLT
TCP    10.211.55.6:49673    a104-96-33-158:http   HERGESTELLT
TCP    10.211.55.6:49674    a23-63-147-63:https   HERGESTELLT
TCP    10.211.55.6:49675    52.114.132.12:https   WARTEND
TCP    10.211.55.6:49680    52.158.24.209:https   WARTEND
TCP    10.211.55.6:49681    52.114.132.12:https   WARTEND
TCP    10.211.55.6:49683    a-0001:https          HERGESTELLT
TCP    10.211.55.6:49684    13.107.21.200:https   HERGESTELLT
TCP    10.211.55.6:49685    204.79.197.222:https  HERGESTELLT
TCP    10.211.55.6:49686    204.79.197.254:https  HERGESTELLT
TCP    10.211.55.6:49687    13.107.42.254:https   HERGESTELLT
TCP    10.211.55.6:49688    51.116.239.131:https  HERGESTELLT
TCP    10.211.55.6:49689    93.184.220.29:http    HERGESTELLT
TCP    10.211.55.6:49690    104.18.24.243:http    HERGESTELLT
TCP    10.211.55.6:49694    52.114.75.149:https   WARTEND
TCP    127.0.0.1:26887      vRechnernetze:49677   HERGESTELLT
TCP    127.0.0.1:26887      vRechnernetze:49691   HERGESTELLT
TCP    127.0.0.1:49677      vRechnernetze:26887   HERGESTELLT
TCP    127.0.0.1:49678      vRechnernetze:49679   HERGESTELLT
TCP    127.0.0.1:49679      vRechnernetze:49678   HERGESTELLT
TCP    127.0.0.1:49691      vRechnernetze:26887   HERGESTELLT
TCP    127.0.0.1:49692      vRechnernetze:49693   HERGESTELLT
TCP    127.0.0.1:49693      vRechnernetze:49692   HERGESTELLT

PS C:\>
```



## Route

Die Routingtabelle gibt Aufschluss darüber, wie welche Geräte welche Route nehmen. **route print** liefert folgende Routingtabelle:

```
IPv4-Routentabelle
=====
Aktive Routen:
  Netzwerkziel    Netzwerkmaske    Gateway    Schnittstelle    Metrik
    0.0.0.0        0.0.0.0        192.168.178.1    192.168.178.34    35
    127.0.0.0        255.0.0.0    Auf Verbindung    127.0.0.1    331
    127.0.0.1        255.255.255.255    Auf Verbindung    127.0.0.1    331
  127.255.255.255    255.255.255.255    Auf Verbindung    127.0.0.1    331
    192.168.178.0    255.255.255.0    Auf Verbindung    192.168.178.34    291
    192.168.178.34    255.255.255.255    Auf Verbindung    192.168.178.34    291
    192.168.178.255    255.255.255.255    Auf Verbindung    192.168.178.34    291
    224.0.0.0        240.0.0.0    Auf Verbindung    127.0.0.1    331
    224.0.0.0        240.0.0.0    Auf Verbindung    192.168.178.34    291
    255.255.255.255    255.255.255.255    Auf Verbindung    127.0.0.1    331
    255.255.255.255    255.255.255.255    Auf Verbindung    192.168.178.34    291
=====
Ständige Routen:
  Keine

IPv6-Routentabelle
=====
Aktive Routen:
  If Metrik Netzwerkziel    Gateway
    1    331 ::1/128    Auf Verbindung
   14    291 fe80::/64    Auf Verbindung
   14    291 fe80::b453:8454:5ac0:cf3/128
                                Auf Verbindung
    1    331 ff00::/8    Auf Verbindung
   14    291 ff00::/8    Auf Verbindung
=====
Ständige Routen:
  Keine
```

Die unterschiedliche Länge der zwei Routing-Tabellen (s. oben und nächste Seite) ergibt sich dadurch, dass bei der zweiten Tabelle durch das auf dem Computer installierte Programm VMware zusätzliche Routing-Einträge erstellt wurden.

```
C:\Users\Rebecca>route print
=====
Schnittstellenliste
23...96 e9 79 9e 3b e7 .....Microsoft Wi-Fi Direct Virtual Adapter
3...94 e9 79 9e 3b e7 .....Microsoft Wi-Fi Direct Virtual Adapter #3
11...98 e7 f4 63 b1 4d .....Realtek PCIe FE Family Controller
20...00 ff a6 61 49 72 .....TAP-Windows Adapter V9
5...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
18...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
15...94 e9 79 9e 3b e7 .....Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
1.....Software Loopback Interface 1
=====

IPv4-Routentabelle
=====
Aktive Routen:
   Netzwerkziel   Netzwerkmaske   Gateway   Schnittstelle   Metrik
   0.0.0.0        0.0.0.0        192.168.178.1  192.168.178.37   35
   127.0.0.0      255.0.0.0      Auf Verbindung  127.0.0.1        331
   127.0.0.1      255.255.255.255 Auf Verbindung  127.0.0.1        331
   127.255.255.255 255.255.255.255 Auf Verbindung  127.0.0.1        331
   192.168.137.0   255.255.255.0   Auf Verbindung  192.168.137.1    281
   192.168.137.1   255.255.255.255 Auf Verbindung  192.168.137.1    281
   192.168.137.255 255.255.255.255 Auf Verbindung  192.168.137.1    281
   192.168.149.0   255.255.255.0   Auf Verbindung  192.168.149.1    291
   192.168.149.1   255.255.255.255 Auf Verbindung  192.168.149.1    291
   192.168.149.255 255.255.255.255 Auf Verbindung  192.168.149.1    291
   192.168.178.0   255.255.255.0   Auf Verbindung  192.168.178.37   291
   192.168.178.37   255.255.255.255 Auf Verbindung  192.168.178.37   291
   192.168.178.255 255.255.255.255 Auf Verbindung  192.168.178.37   291
   192.168.206.0   255.255.255.0   Auf Verbindung  192.168.206.1    291
   192.168.206.1   255.255.255.255 Auf Verbindung  192.168.206.1    291
   192.168.206.255 255.255.255.255 Auf Verbindung  192.168.206.1    291
   224.0.0.0       240.0.0.0       Auf Verbindung  127.0.0.1        331
   224.0.0.0       240.0.0.0       Auf Verbindung  192.168.178.37   291
   224.0.0.0       240.0.0.0       Auf Verbindung  192.168.137.1    281
   224.0.0.0       240.0.0.0       Auf Verbindung  192.168.206.1    291
   224.0.0.0       240.0.0.0       Auf Verbindung  192.168.149.1    291
   255.255.255.255 255.255.255.255 Auf Verbindung  127.0.0.1        331
   255.255.255.255 255.255.255.255 Auf Verbindung  192.168.178.37   291
   255.255.255.255 255.255.255.255 Auf Verbindung  192.168.137.1    281
   255.255.255.255 255.255.255.255 Auf Verbindung  192.168.206.1    291
   255.255.255.255 255.255.255.255 Auf Verbindung  192.168.149.1    291
=====
Ständige Routen:
Keine
```

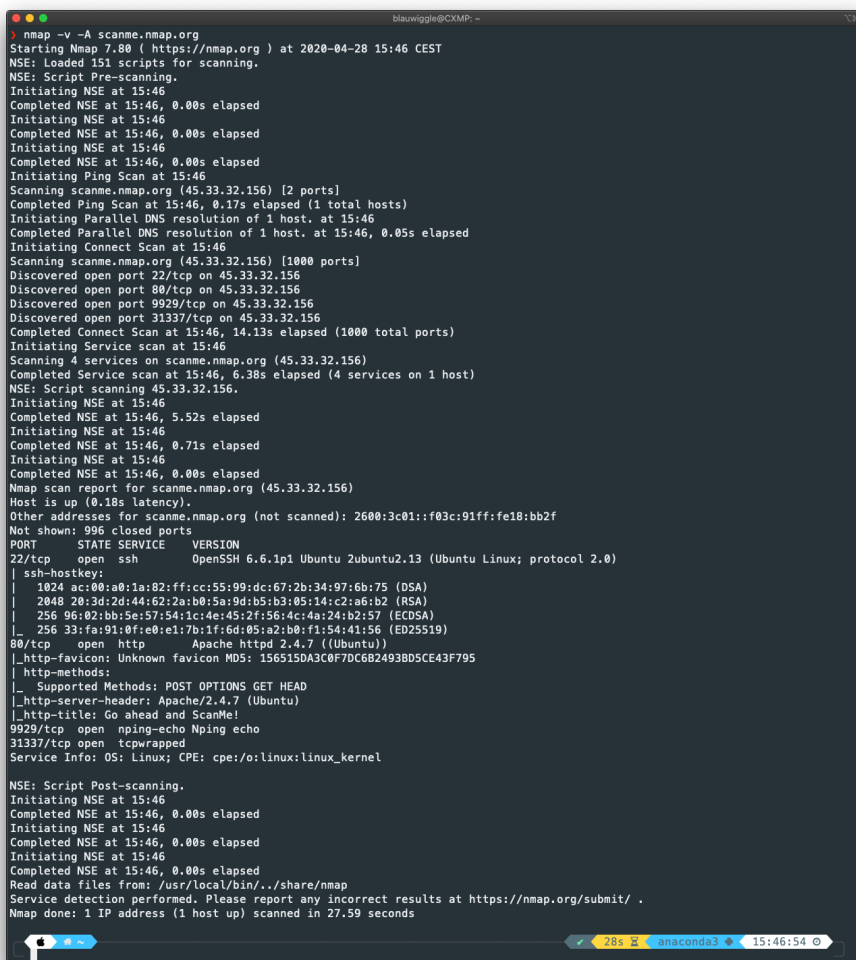
```
IPv6-Routentabelle
=====
Aktive Routen:
If Metrik Netzwerkziel   Gateway
11 291 ::/0                fe80::3a10:d5ff:feb8:47a1
1 331 ::1/128              Auf Verbindung
11 291 2003:e0:771c:4800::/56 fe80::3a10:d5ff:feb8:47a1
11 291 2003:e0:771c:4800::/64 Auf Verbindung
11 291 2003:e0:771c:4800:133:acf:343f:e372/128 Auf Verbindung
11 291 2003:e0:771c:4800:8c7e:3545:b5c0:25f4/128 Auf Verbindung
11 291 fe80::/64            Auf Verbindung
3 281 fe80::/64            Auf Verbindung
5 291 fe80::/64            Auf Verbindung
18 291 fe80::/64            Auf Verbindung
18 291 fe80::344e:a82f:6e9b:eb59/128 Auf Verbindung
11 291 fe80::8c7e:3545:b5c0:25f4/128 Auf Verbindung
5 291 fe80::b598:b91d:e8e1:243d/128 Auf Verbindung
3 281 fe80::dd00:459b:a22b:42f9/128 Auf Verbindung
1 331 ff00::/8             Auf Verbindung
11 291 ff00::/8             Auf Verbindung
3 281 ff00::/8             Auf Verbindung
5 291 ff00::/8             Auf Verbindung
18 291 ff00::/8             Auf Verbindung
=====
Ständige Routen:
Keine
```

## Aufgabenteil 2 - Shareware / Freeware

### NMAP

Mit NMAP kann man eigentlich nahezu alles machen. Ursprünglich wurde er als freier Portscanner entworfen, dabei steht der Name für Network Mapper. Das Tool eignet sich besonders für Netzwerkadministratoren sowie für Angreifer, die verschiedene Angriffsvektoren durchgehen möchten. Dabei kann NMAP so umfangreich konfiguriert werden, dass selbst automatisierte Abläufe zuverlässig umgesetzt werden können. In Verbindung mit weiteren Tools, können ganze Netzwerke auf Schwachstellen überprüft werden. Um den Bogen zurück zu Versuch 1 zu spannen, mit dem zusätzlich installierbaren Tool “arp-scan” kann beispielsweise das gesamte eduroam gescannt und protokolliert werden.

`nmap -v -A scanme.nmap.org`



```
nmap -v -A scanme.nmap.org
Starting Nmap 7.90 ( https://nmap.org ) at 2020-04-28 15:46 CEST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating Ping Scan at 15:46
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 15:46, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:46
Completed Parallel DNS resolution of 1 host. at 15:46, 0.05s elapsed
Initiating Connect Scan at 15:46
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 15:46, 14.13s elapsed (1000 total ports)
Initiating Service scan at 15:46
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 15:46, 6.38s elapsed (4 services on 1 host)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 15:46
Completed NSE at 15:46, 5.52s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.71s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh             OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:el:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http            Apache httpd 2.4.7 ((Ubuntu))
|_ http-favicon: Unknown favicon MD5: 156519DA3C0F7DC6B2493BD5CE43F795
|_ http-methods:
|_   Supported Methods: POST OPTIONS GET HEAD
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo      Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Read data files from: /usr/local/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.59 seconds
```

Bernd Maier (bm075), Yannick Möller (ym018), Rebecca Mombrei (rm048), Michael Vanhee (mv068)



## Wireshark

Wireshark ist das wohl weltweit beliebteste Programm zur Analyse von Netzwerken. Nach der kostenlosen Installation auf dem eigenen Rechner erkennt die Software verfügbare Netzwerke und ermöglicht das Mitschneiden von Netzwerkframes. Wireshark stellt damit ein ideales Werkzeug zur Fehlerbehebung im Netzwerk, Optimierung, Sicherheitsprüfung (Forensik) und Programmanalyse dar. Ferner kann sämtlicher Datenverkehr in den verschiedensten Formaten als Mitschnittdatei gespeichert werden.

\*Ethernet

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

ip.addr == Aufzeichnungsoptionen

No.	Time	Source	Destination	Protocol	Length	Info
1062	117.617507	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=761/63746, ttl=64 (request in ...)
1063	118.626142	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=762/64002, ttl=128 (reply in ...)
1064	118.633057	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=762/64002, ttl=64 (request in ...)
1068	119.637204	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=763/64258, ttl=128 (reply in ...)
1069	119.641802	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=763/64258, ttl=64 (request in ...)
1070	120.651309	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=764/64514, ttl=128 (reply in ...)
1071	120.654916	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=764/64514, ttl=64 (request in ...)
1077	121.665644	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=765/64770, ttl=128 (reply in ...)
1078	121.671272	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=765/64770, ttl=64 (request in ...)
1081	122.678163	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=766/65026, ttl=128 (reply in ...)
1082	122.681630	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=766/65026, ttl=64 (request in ...)
1088	123.692335	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=767/65282, ttl=128 (reply in ...)
1089	123.695931	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=767/65282, ttl=64 (request in ...)
1091	124.703743	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=768/3, ttl=128 (reply in ...)
1092	124.711059	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=768/3, ttl=64 (request in ...)
1095	125.717330	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=769/259, ttl=128 (reply in ...)
1096	125.721974	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=769/259, ttl=64 (request in ...)
1097	126.730458	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=770/515, ttl=128 (reply in ...)
1098	126.735108	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=770/515, ttl=64 (request in ...)
1104	127.744447	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=771/771, ttl=128 (reply in ...)
1105	127.750695	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=771/771, ttl=64 (request in ...)
1106	128.756218	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=772/1027, ttl=128 (reply in ...)
1107	128.759902	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=772/1027, ttl=64 (request in ...)
1121	129.771380	192.168.178.34	192.168.178.1	ICMP	74	Echo (ping) request id=0x0001, seq=773/1283, ttl=128 (reply in ...)
1122	129.774877	192.168.178.1	192.168.178.34	ICMP	74	Echo (ping) reply id=0x0001, seq=773/1283, ttl=64 (request in ...)

> Frame 981: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{D06FD11F-0063-49C1-AFDE-B7BA2664706C}, id 0

> Ethernet II, Src: Micro-St\_f6:72:a7 (d4:3d:7e:f6:72:a7), Dst: AVMAudio\_54:f9:01 (e8:df:70:54:f9:01)

> Internet Protocol Version 4, Src: 192.168.178.34, Dst: 192.168.178.1

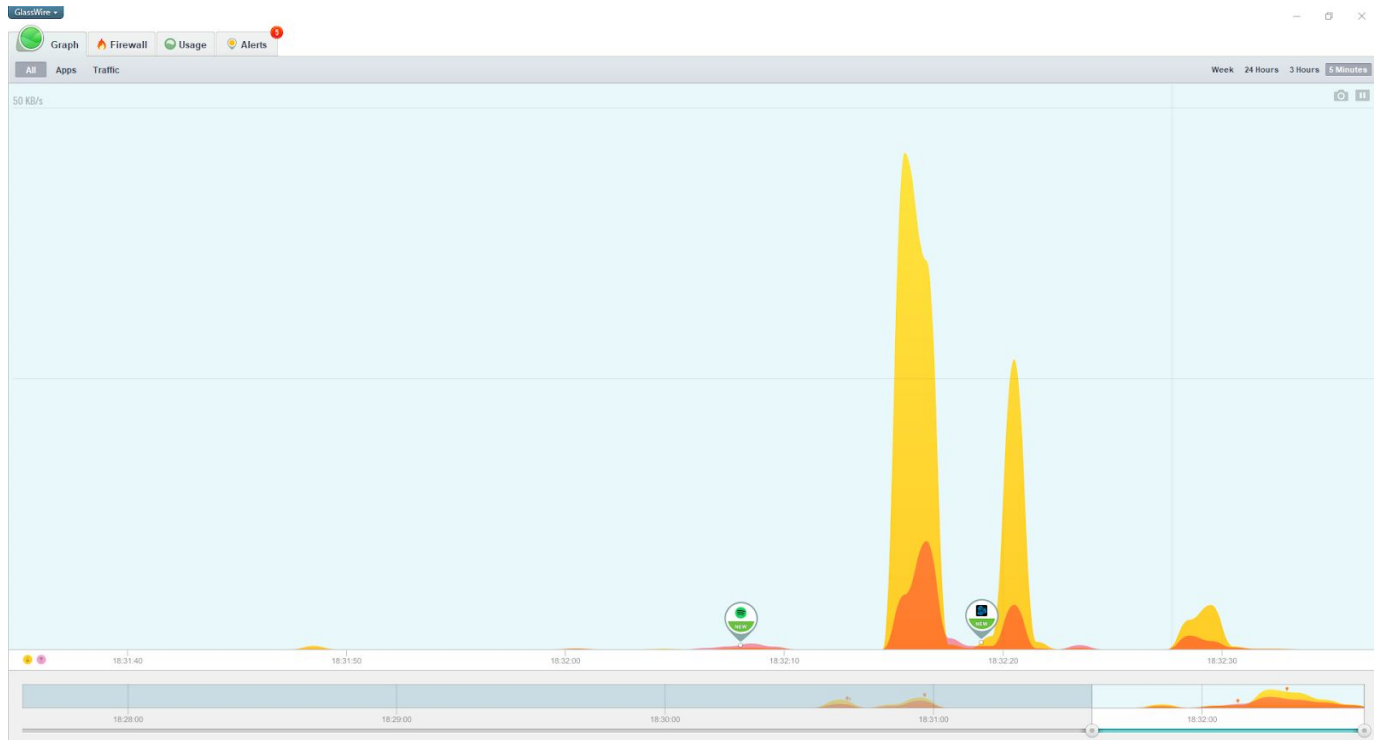
> Internet Control Message Protocol

```

0000  e8 df 70 54 f9 01 d4 3d 7e f6 72 a7 08 00 45 00  ..pT...~r...E.
0010  00 3c e7 dc 00 00 80 01 00 00 c0 a8 b2 22 c0 a8  <....."....
0020  b2 01 08 00 4a 6f 00 01 02 ec 61 62 63 64 65 66  ....Jo...abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                  wabcdefg hi

```

## GlassWire



Mithilfe von GlassWire werden zur Laufzeit Netzwerkanfragen angezeigt.

## Sonstige hilfreiche Websites & Tools

Rechner für Subnetze <https://www.heise.de/netze/tools/netzwerkrechner/>

IP-Location Finder: (z.B.) <https://www.iplocation.net/>

MAC Programm um die "Internetverbindung sichtbar zu machen":

<https://www.obdev.at/de/products/littlesnitch/index.html>