

Wireshark Aufgabe

Aufgabe 1

➔ Einleitung

Aufgabe 2

1. Welche Pakete werden gesendet, wenn der Ping-Befehl ausgeführt wird? Kopieren Sie die entsprechenden Pakete aus Wireshark. Führen Sie den Ping-Befehl gegebenenfalls für mehrere IP Adressen aus, um diese Pakete zu identifizieren.

No.	Time	Source	Destination	Protocol	Length	Info
148	0.762125	fe80::7254:25ff:fe00::1	ff02::1	ICMPv6	158	Router Advertisement from 70:54:25:65:a8:d3
475	2.746373	2a02:8071:8287:59c0::	ff02::1:1:ff00::acd5	ICMPv6	86	Neighbor Solicitation for 2a02:8071:8287:59c0::acd5 from 70:54:25:65:a8:d3
573	3.665498	fe80::7254:25ff:fe00::1	ff02::1:1:ff00::1aef	ICMPv6	86	Neighbor Solicitation for 2a02:8071:8287:59c0::1aef from 70:54:25:65:a8:d3
584	3.763567	fe80::7254:25ff:fe00::1	ff02::1	ICMPv6	158	Router Advertisement from 70:54:25:65:a8:d3
585	3.782016	2a02:8071:8287:59c0::	ff02::1:1:ff00::acd5	ICMPv6	86	Neighbor Solicitation for 2a02:8071:8287:59c0::acd5 from 70:54:25:65:a8:d3
709	4.807093	2a02:8071:8287:59c0::	ff02::1:1:ff00::acd5	ICMPv6	86	Neighbor Solicitation for 2a02:8071:8287:59c0::acd5 from 70:54:25:65:a8:d3
1031	6.766163	fe80::7254:25ff:fe00::1	ff02::1	ICMPv6	158	Router Advertisement from 70:54:25:65:a8:d3
1295	8.194968	2a02:8071:8287:59c0::	2a02:26f0:10c:4b2::	ICMPv6	94	Echo (ping) request id=0x0001, seq=9, hop limit=128 (reply in 1380)
1300	8.224312	2a02:26f0:10c:4b2::	2a02:8071:8287:59c0::	ICMPv6	94	Echo (ping) reply id=0x0001, seq=9, hop limit=59 (request in 1295)
1445	9.200287	2a02:8071:8287:59c0::	2a02:26f0:10c:4b2::	ICMPv6	94	Echo (ping) request id=0x0001, seq=10, hop limit=128 (reply in 1450)
1450	9.224999	2a02:26f0:10c:4b2::	2a02:8071:8287:59c0::	ICMPv6	94	Echo (ping) reply id=0x0001, seq=10, hop limit=59 (request in 1445)
1523	9.769231	fe80::7254:25ff:fe00::1	ff02::1	ICMPv6	158	Router Advertisement from 70:54:25:65:a8:d3
1575	10.203094	2a02:8071:8287:59c0::	2a02:26f0:10c:4b2::	ICMPv6	94	Echo (ping) request id=0x0001, seq=11, hop limit=128 (reply in 1580)
1580	10.235615	2a02:26f0:10c:4b2::	2a02:8071:8287:59c0::	ICMPv6	94	Echo (ping) reply id=0x0001, seq=11, hop limit=59 (request in 1575)
1720	11.207297	2a02:8071:8287:59c0::	2a02:26f0:10c:4b2::	ICMPv6	94	Echo (ping) request id=0x0001, seq=12, hop limit=128 (reply in 1726)
1726	11.227354	2a02:26f0:10c:4b2::	2a02:8071:8287:59c0::	ICMPv6	94	Echo (ping) reply id=0x0001, seq=12, hop limit=59 (request in 1720)

▼ Frame 1295: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{6BC81858-B96F-489B-904F-6A128F716188}		0000	70 54 25 65 a8 d3 d8 bb c1 cc a3 11 86 dd 60 00	pTtE.....
Section number: 1		0010	00 00 00 28 3a 80 2a 02 80 71 82 87 59 c0 00 00	...{.*:q.Y...
> Interface id: 0 (\Device\NPF_{6BC81858-B96F-489B-904F-6A128F716188})		0020	00 00 00 00 41 d8 2a 02 26 f0 01 0c 04 b2 00 00	...A.*.&.....
Encapsulation type: Ethernet (1)		0030	00 00 00 00 3f 78 80 00 76 33 00 01 00 09 61 62	...?x...v3...ab
Arrival Time: Nov 14, 2022 16:55:26.254433000 W. Europe Standard Time		0040	63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72	cdefghij klmnopqr
[Time shift for this packet: 0.000000000 seconds]		0050	73 74 75 76 77 61 62 63 64 65 66 67 68 69	stuvwabc defghi
Epoch Time: 1668441326.254433000 seconds				
[Time delta from previous captured frame: 0.003515000 seconds]				
[Time delta from previous displayed frame: 1.428050000 seconds]				
[Time since reference or first frame: 8.194968000 seconds]				
Frame Number: 1295				
Frame Length: 94 bytes (752 bits)				
Capture Length: 94 bytes (752 bits)				
[Frame is marked: False]				
[Frame is ignored: False]				
[Protocols in frame: ethertype:ipv6:icmpv6:data]				
[Coloring Rule Name: ICMP]				
[Coloring Rule String: icmp icmpv6]				
> Ethernet II, Src: Micro-St_cia3:11 (d8:bb:c1:cc:a3:11), Dst: ARRI56Gro_5a:8:d3 (70:54:25:65:a8:d3)				
> Internet Protocol Version 6, Src: 2a02:8071:8287:59c0::41d8, Dst: 2a02:26f0:10c:4b2::3f78				
> Internet Control Message Protocol v6				

2. Welche Protokolle werden zur Übertragung dieser Pakete genutzt?

Bei nsa.gov wird das Protokoll ICMPv6 genutzt (auch sichtbar an der IPv6 Adresse)

```
Pinging e16248.dscb.akamaiedge.net [2a02:26f0:3100:2b4::3f78] with 32 bytes of data:
Reply from 2a02:26f0:3100:2b4::3f78: time=18ms
Reply from 2a02:26f0:3100:2b4::3f78: time=16ms
Reply from 2a02:26f0:3100:2b4::3f78: time=16ms
Reply from 2a02:26f0:3100:2b4::3f78: time=16ms

Ping statistics for 2a02:26f0:3100:2b4::3f78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 16ms
```

Bei der Stadtwerke Konstanz dagegen ICMP (sichtbar an den IPv4 Adressen)

```
Pinging www.stadtwerke-konstanz.de [31.47.82.53] with 32 bytes of data:
Reply from 31.47.82.53: bytes=32 time=33ms TTL=57
Reply from 31.47.82.53: bytes=32 time=32ms TTL=57
Reply from 31.47.82.53: bytes=32 time=32ms TTL=57
Reply from 31.47.82.53: bytes=32 time=31ms TTL=57

Ping statistics for 31.47.82.53:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 33ms, Average = 32ms
```

3. Welche Ergebnisse liefert der Ping-Befehl? Wie können Sie diese Ergebnisse aus den in WireShark aufgezeichneten Paketen bestimmen?

```
Pinging e16248.dscb.akamaiedge.net [2a02:26f0:10c:4b2::3f78] with 32 bytes of data:
Reply from 2a02:26f0:10c:4b2::3f78: time=29ms
Reply from 2a02:26f0:10c:4b2::3f78: time=24ms
Reply from 2a02:26f0:10c:4b2::3f78: time=32ms
Reply from 2a02:26f0:10c:4b2::3f78: time=20ms

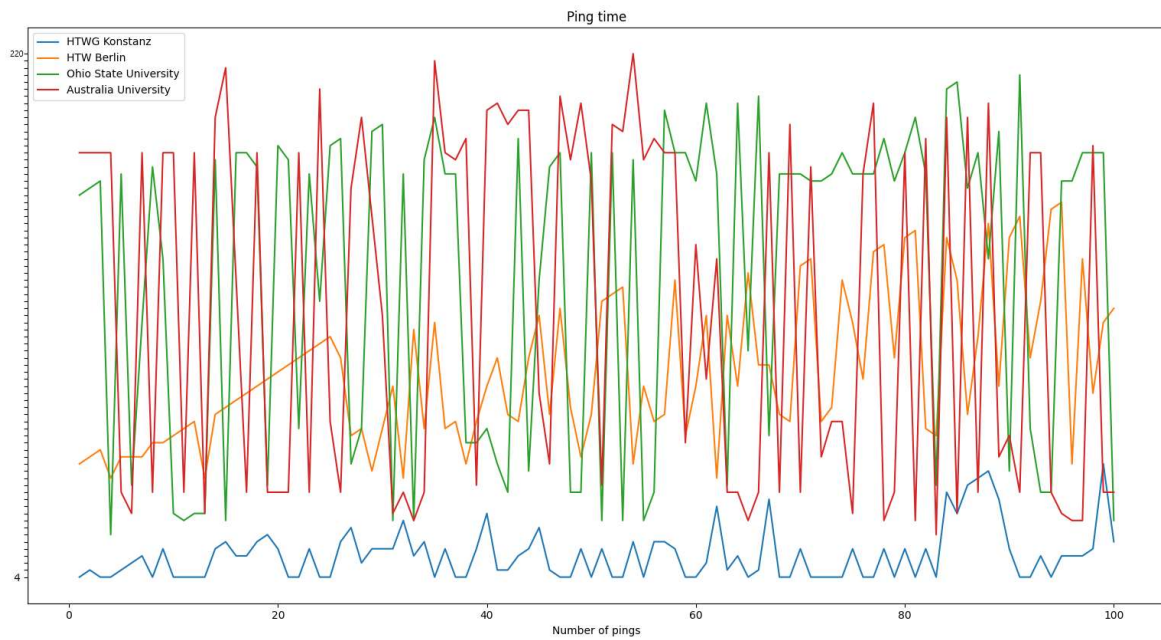
Ping statistics for 2a02:26f0:10c:4b2::3f78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 32ms, Average = 26ms
```

No.	Time	Source	Destination	Protocol	Length	Info
148	0.762125	fe80::7254:25ff:fe00::1	ff02::1	ICMPv6	158	Router Advertisement from 70:54:25:65:a8:d3
475	2.746373	2a02:8071:8287:59c0::ff02::1	ff00::acd5	ICMPv6	86	Neighbor Solicitation for 2a02:8071:8287:59c0::acd5 from 70:54:25:65:a8:d3
573	3.665498	fe80::7254:25ff:fe00::1	ff00::1aeef	ICMPv6	86	Neighbor Solicitation for 2a02:8071:8287:59c0::1aeef from 70:54:25:65:a8:d3
584	3.763567	fe80::7254:25ff:fe00::1	ff02::1	ICMPv6	158	Router Advertisement from 70:54:25:65:a8:d3
585	3.782018	2a02:8071:8287:59c0::ff02::1	ff00::acd5	ICMPv6	86	Neighbor Solicitation for 2a02:8071:8287:59c0::acd5 from 70:54:25:65:a8:d3
709	4.807093	2a02:8071:8287:59c0::ff02::1	ff00::acd5	ICMPv6	86	Neighbor Solicitation for 2a02:8071:8287:59c0::acd5 from 70:54:25:65:a8:d3
1031	6.765163	fe80::7254:25ff:fe00::1	ff02::1	ICMPv6	158	Router Advertisement from 70:54:25:65:a8:d3
1295	8.194968	2a02:8071:8287:59c0::2a02:26f0:10c:4b2::	...	ICMPv6	94	Echo (ping) request id=0x0001, seq=9, hop limit=128 (reply in 1300)
1300	8.224312	2a02:26f0:10c:4b2::2a02:8071:8287:59c0::	...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=9, hop limit=59 (request in 1295)
1445	9.200287	2a02:8071:8287:59c0::2a02:26f0:10c:4b2::	...	ICMPv6	94	Echo (ping) request id=0x0001, seq=10, hop limit=128 (reply in 1450)
1450	9.224999	2a02:26f0:10c:4b2::2a02:8071:8287:59c0::	...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=10, hop limit=59 (request in 1445)
1523	9.769231	fe80::7254:25ff:fe00::1	ff02::1	ICMPv6	158	Router Advertisement from 70:54:25:65:a8:d3
1575	10.203804	2a02:8071:8287:59c0::2a02:26f0:10c:4b2::	...	ICMPv6	94	Echo (ping) request id=0x0001, seq=11, hop limit=128 (reply in 1580)
1580	10.235615	2a02:26f0:10c:4b2::2a02:8071:8287:59c0::	...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=11, hop limit=59 (request in 1575)
1720	11.207297	2a02:8071:8287:59c0::2a02:26f0:10c:4b2::	...	ICMPv6	94	Echo (ping) request id=0x0001, seq=12, hop limit=128 (reply in 1726)
1726	11.227354	2a02:26f0:10c:4b2::2a02:8071:8287:59c0::	...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=12, hop limit=59 (request in 1720)

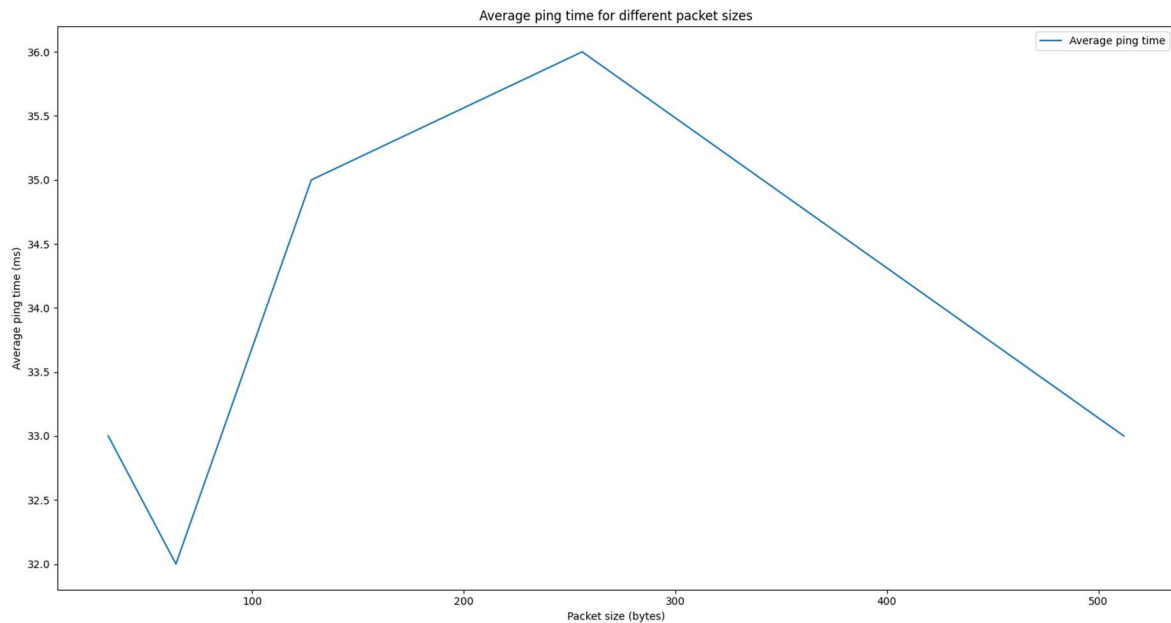
<p>▼ Frame 1300: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{68C81B58-896F-4898-904F-6A128F716188}</p> <p>Section number: 1</p> <p>Interface id: 0 (\Device\NPF_{68C81B58-896F-4898-904F-6A128F716188})</p> <p>Encapsulation type: Ethernet (1)</p> <p>Arrival Time: Nov 14, 2022 16:55:26.28377000 W. Europe Standard Time [Time shift for this packet: 0.00000000 seconds]</p> <p>Epoch Time: 1668441326.28377000 seconds [Time delta from previous captured frame: 0.003368000 seconds] [Time delta from previous displayed frame: 0.029344000 seconds] [Time since reference or first frame: 8.224312000 seconds]</p> <p>Frame Number: 1300</p> <p>Frame Length: 94 bytes (752 bits)</p> <p>Capture Length: 94 bytes (752 bits)</p> <p>[Frame is marked: False]</p> <p>[Frame is ignored: False]</p> <p>[Protocols in frame: eth:ethertype:ipv6:icmpv6:data]</p> <p>[Coloring Rule Name: ICMP]</p> <p>[Coloring Rule String: icmp icmpv6]</p> <p>Ethernet II, Src: AMRISGro_65:a8:d3, Dst: Micro-St_ccca3:11 (d8:bb:c1:cc:a3:11)</p> <p>Internet Protocol Version 6, Src: 2a02:26f0:10c:4b2::3f78, Dst: 2a02:8071:8287:59c0::41d8</p> <p>Internet Control Message Protocol v6</p> <p>Type: Echo (ping) reply (129)</p> <p>Code: 0</p> <p>Checksum: 0x7533 [correct]</p> <p>[Checksum Status: Good]</p> <p>Identifier: 0x0001</p> <p>Sequence: 9</p> <p>[Response To: 1295]</p> <p>[Response Time: 29.344 ms]</p> <p>Data (32 bytes)</p> <p>Data: 6162836465666768696a6b6c6d6e6f7071727374757677616263646566676869</p> <p>[Length: 32]</p>	<pre> 0000 d8 bb c1 cc a3 11 70 54 25 65 a8 d3 86 dd 60 0a pT &..... 0010 60 a4 00 28 3a 3b 2a 02 26 f0 01 0c 04 b2 00 00 ...(:)* &..... 0020 00 00 00 00 3f 78 2a 02 80 71 82 87 59 c0 00 00 ...?x* .q.Y... 0030 00 00 00 00 41 d8 81 00 75 33 00 01 00 09 61 62 ...A...u3...ab 0040 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 cdefghij klmnopq 0050 73 74 75 76 77 61 62 63 64 65 66 67 68 69 stuvwabc defghi </pre>
--	--

4. Erstellen Sie einen Filter für diese beiden Protokolle (zusätzlich zu dem Filter auf ihre IP-Adresse), um nur diese beiden Protokolle zu filtern. Testen Sie den Filter, indem Sie weitere Adressen pingen. (icmpv6 || icmp) && (ip.src==local IPv4 || ipv6.src==local IPv6)

1. Pingen Sie die Adressen jeweils 100mal und speichern Sie das Ergebnis in einer Datei. Stellen Sie die Ping-Zeit mit einem Tool ihrer Wahl (Excel, Matlab, etc.) grafisch dar.



2. Wählen Sie die Adresse mit den längsten Ping-Zeiten und stellen Sie den Einfluss der Paketgröße grafisch dar.



Aufgabe 3

1. Führen Sie den traceroute-Befehl für den Web-Server der Hochschule und für ihre eigene IP-Adresse aus. Welche Ergebnisse erhalten Sie?

```
C:\Users\ >tracert www.htwg-konstanz.de

Tracing route to cms.htwg-konstanz.de [2001:7c0:5f0:f020::20:17]
over a maximum of 30 hops:

  1    1 ms    1 ms    1 ms  fritz.box [2001:16b8:a5fe:1500:7eff:4dff:fea1:21d9]
  2   13 ms   12 ms   12 ms  2001:1438::62:214:63:147
  3   11 ms   11 ms   11 ms  2001:1438:0:1::15:21
  4   17 ms   16 ms   17 ms  fra020isp005.versatel.de [2001:7f8::22b1:193:80]
  5   18 ms   23 ms   18 ms  frankfurt-tc-1-10ge-0-2-0-6.belwue.net [2001:7f8::229:0:2]
  6   21 ms   19 ms   19 ms  kar-rz-a99-hu0-2-0-0.belwue.net [2001:7c0:2:10c8::]
  7   21 ms   24 ms   21 ms  stu-nwz-a99-hu0-1-0-0.belwue.net [2001:7c0:2:10c1::]
  8   27 ms   29 ms   22 ms  stu-al30-1-hu0-0-1-0.belwue.net [2001:7c0:2:1104::1]
  9   23 ms   23 ms   23 ms  tue-wae-1-te0-0-0-15.belwue.net [2001:7c0:2:1064::1]
 10   26 ms   25 ms   24 ms  kon-bib-1-te0-0-0-11.belwue.net [2001:7c0:2:104a::1]
 11   25 ms   23 ms   24 ms  cmsrv6.htwg-konstanz.de [2001:7c0:5f0:f020::20:17]

Trace complete.
```

```
C:\Users\ >tracert 192.168.178.80

Tracing route to DESKTOP-ASCAJSC.fritz.box [192.168.178.80]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  DESKTOP-ASCAJSC.fritz.box [192.168.178.80]

Trace complete.
```

2. Bestimmen Sie, in welchem Netz sich der Rechner befindet, von dem der traceroute Befehl gestartet wird. Bestimmen Sie außerdem, durch welche Netze die Pakete geroutet werden. Sie können bestimmen, zu welchem Netz ein Router gehört, in dem Sie die ASN (Autonomous System Number) des Routers bestimmen, die Netze eindeutig kennzeichnet. Nutzen Sie dazu beispielsweise das Online Tool <https://www.ultratools.com/tools/asnInfo>.

- 2001:16b8:a5fe:1500:7eff:4dff:fea1:21d9 :
Der Rechner von welchem der Befehl ausgeführt wird befindet sich im lokalen LAN (Fritz-Box Router). Dies ist auch dem unteren Bild zu entnehmen.
- 2001:1438::62:214:63:147
AS: 8881 **AS Name:** VERSATEL, DE
- 2001:1438:0:1::15:21
AS: 8881 **AS Name:** VERSATEL, DE
- fra020isp005.versatel.de [2001:7f8::22b1:193:80]
AS: None **AS Name:** Not found
- kar-rz-a99-hu0-2-0-0.belwue.net [2001:7c0:2:10c8::]
AS: 553 **AS Name:** BELWUE BelWue-Koordination, DE
- stu-nwz-a99-hu0-1-0-0.belwue.net [2001:7c0:2:10c1::]
AS: 553 **AS Name:** BELWUE BelWue-Koordination, DE
- stu-al30-1-hu0-0-1-0.belwue.net [2001:7c0:2:1104::1]
AS: 553 **AS Name:** BELWUE BelWue-Koordination, DE
- tue-wae-1-te0-0-0-15.belwue.net [2001:7c0:2:1064::1]
AS: 553 **AS Name:** BELWUE BelWue-Koordination, DE
- kon-bib-1-te0-0-0-11.belwue.net [2001:7c0:2:104a::1]
AS: 553 **AS Name:** BELWUE BelWue-Koordination, DE

10. cmssrv6.htwg-konstanz.de [2001:7c0:5f0:f020::20:17]

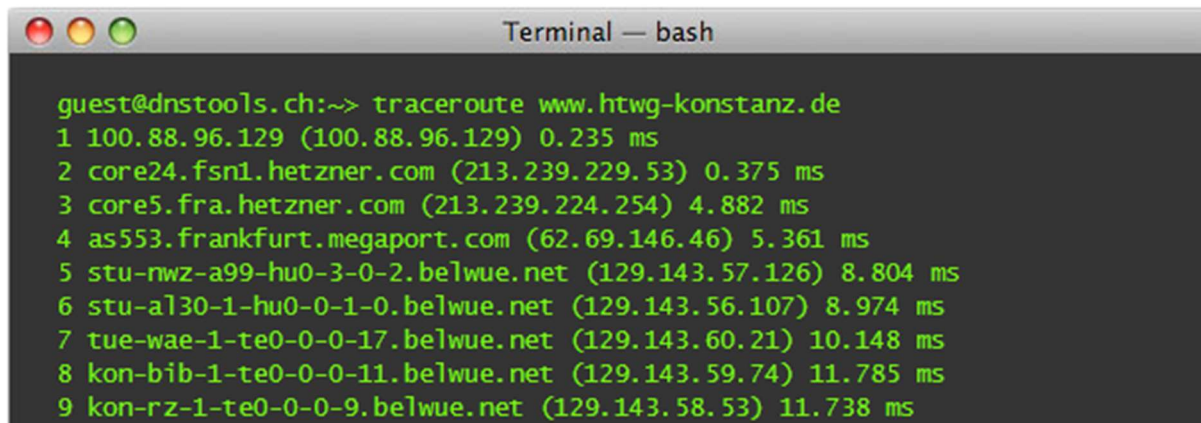
AS: 553

AS Name: BELWUE BelWue-Koordination, DE

Zu sehen ist, dass die Route über VERSATEL (Internet-Provider) läuft und in Karlsruhe in das Landeshochschulnetz "Baden-Württembergs extended LAN" geht von wo es über das Hochschulnetz nach Konstanz geleitet wird. Cool? Cool!

3. Betrachten Sie nun mehrere Online-Tools, so dass Sie den Traceroute-Befehl von mindestens drei unterschiedlichen Netzen aus starten können. Führen Sie den Traceroute-Befehl nun nicht mehr nur für den Web-Server der Hochschule sondern zusätzlich für www.ntt.co.jp und www.google.com aus. Bestimmen Sie, welche Teile der Route für die unterschiedlichen Kombinationen aus Online-Tool und Zielrechner identisch sind.

HTWG Konstanz



```
Terminal — bash

guest@dnstools.ch:~> traceroute www.htwg-konstanz.de
 1 100.88.96.129 (100.88.96.129) 0.235 ms
 2 core24.fsn1.hetzner.com (213.239.229.53) 0.375 ms
 3 core5.fra.hetzner.com (213.239.224.254) 4.882 ms
 4 as553.frankfurt.megaport.com (62.69.146.46) 5.361 ms
 5 stu-rwz-a99-hu0-3-0-2.belwue.net (129.143.57.126) 8.804 ms
 6 stu-al30-1-hu0-0-1-0.belwue.net (129.143.56.107) 8.974 ms
 7 tue-wae-1-te0-0-0-17.belwue.net (129.143.60.21) 10.148 ms
 8 kon-bib-1-te0-0-0-11.belwue.net (129.143.59.74) 11.785 ms
 9 kon-rz-1-te0-0-0-9.belwue.net (129.143.58.53) 11.738 ms
```

Abbildung 1: <http://www.dnstools.ch/visual-traceroute.html>

Zu sehen ist, dass die Route erst über Internationale Knotenpunkte nach Frankfurt geleitet wird. Von dort wird es regional nach Stuttgart weitergeleitet, wo es dann wieder ins BelWue geleitet wird. Warum dies diesmal nicht in Karlsruhe ins Hochschulnetz geht, sondern in Stuttgart lässt sich nicht genau sagen. Zu sehen ist aber auch, dass der zweite Pfad (siehe Abbildung 2) in Stuttgart ins BelWue Netz geht. Sobald sich die Pakete im BelWue Netz befinden werden Sie immer auf dem gleichen Weg nach Konstanz geroutet.






















Hop	IP / Host Name	ISP	Netblock	Country	Loss	Response
1	172.17.0.1				0.0%	0.15ms
2	10.206.5.139				0.0%	0.40ms
3	10.206.35.8				0.0%	0.71ms
4	10.206.32.2				0.0%	4.51ms
5	100-0.gw1.cj11.us.linode.com 173.255.239.101	LINODE-AP Linode, LLC, US	173.255.239.0/24		0.0%	3.22ms
6	ae0-100.gw2.cj11.us.linode.com 173.255.239.9	LINODE-AP Linode, LLC, US	173.255.239.0/24		0.0%	0.88ms
7	ae31.r01.lga01.iem.netarch.akamai.com 23.203.156.16	AKAMAI-ASN1, NL	23.203.156.0/24		0.0%	2.15ms
8	nyk-b6-link.ip.twelve99.net 62.115.50.170	TWELVE99 Arelion, fka Telia Carrier, SE	62.115.0.0/16		0.0%	2.22ms
9	nyk-bb1-link.ip.twelve99.net 62.115.135.130	TWELVE99 Arelion, fka Telia Carrier, SE	62.115.0.0/16		0.0%	2.69ms
10	ldn-bb4-link.ip.twelve99.net 62.115.112.245	TWELVE99 Arelion, fka Telia Carrier, SE	62.115.0.0/16		0.0%	70.86ms
11	prs-bb2-link.ip.twelve99.net 62.115.133.239	TWELVE99 Arelion, fka Telia Carrier, SE	62.115.0.0/16		0.0%	80.41ms
12	ffm-bb2-link.ip.twelve99.net 62.115.114.99	TWELVE99 Arelion, fka Telia Carrier, SE	62.115.0.0/16		0.0%	87.69ms
13	ffm-b5-link.ip.twelve99.net 62.115.114.91	TWELVE99 Arelion, fka Telia Carrier, SE	62.115.0.0/16		50.0%	86.89ms
14	belwue-ic130164-ffm-b5.ip.twelve99-cust.net 213.248.88.26	TWELVE99 Arelion, fka Telia Carrier, SE	213.248.64.0/18		0.0%	87.28ms
15	stu-nw2-a99-hu0-3-0-2.belwue.net 129.143.57.126	BELWUE Belwue-Koordination, DE	129.143.0.0/16		0.0%	93.17ms
16	stu-al30-1-hu0-0-1-0.belwue.net 129.143.56.107	BELWUE Belwue-Koordination, DE	129.143.0.0/16		0.0%	94.37ms
17	tue-wae-1-te0-0-0-15.belwue.net 129.143.57.86	BELWUE Belwue-Koordination, DE	129.143.0.0/16		0.0%	94.91ms
18	kon-bib-1-te0-0-0-11.belwue.net 129.143.59.74	BELWUE Belwue-Koordination, DE	129.143.0.0/16		0.0%	96.46ms
19	kon-rz-1-te0-0-0-9.belwue.net 129.143.58.53	BELWUE Belwue-Koordination, DE	129.143.0.0/16		0.0%	96.41ms
20	129.143.47.226	BELWUE Belwue-Koordination, DE	129.143.0.0/16		0.0%	96.98ms
21	cmssrv6.htwg-konstanz.de 141.37.20.17	BELWUE Belwue-Koordination, DE	141.37.0.0/16		0.0%	103.27ms

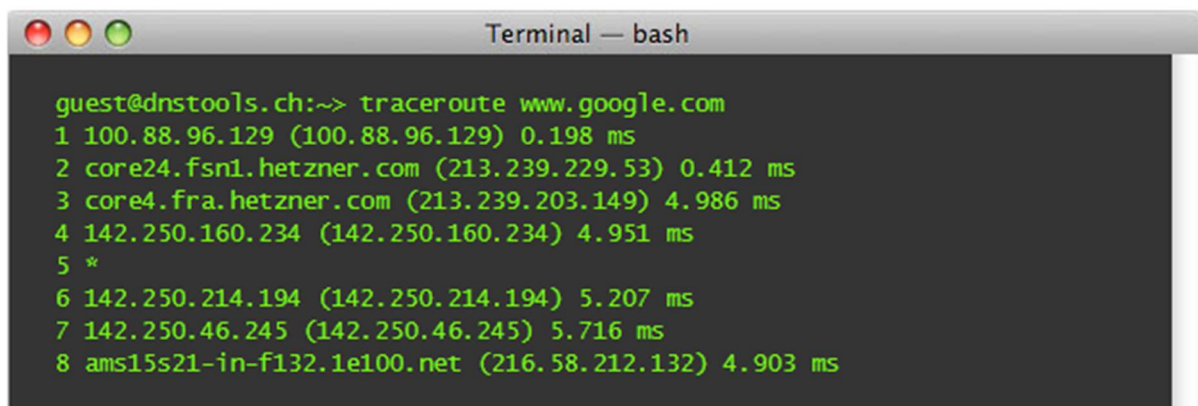
Abbildung 2: <https://traceroute-online.com/>

Google

```
Tracing route to www.google.com [2a00:1450:4001:827::2004]
over a maximum of 30 hops:

  1  <1 ms      1 ms      1 ms      2a02:8071:8287:59c0:7254:25ff:fe65:a8d3
  2  15 ms      12 ms     11 ms     2a02:8071:8200::1
  3   9 ms      12 ms     13 ms     2a02:8071:80fe:34b2::1
  4  17 ms      21 ms     23 ms     de-str01c-rc1-lo0-0.v6.aorta.net [2001:730:2d00::5474:807d]
  5  20 ms      25 ms     22 ms     de-fra04d-rc1-lo0-0.v6.aorta.net [2001:730:2d00::5474:8015]
  6  27 ms      30 ms     23 ms     2a00:1450:8152::1
  7  29 ms      *         28 ms     2001:4860:0:1::5006
  8  23 ms      22 ms     23 ms     2001:4860:0:1::509f
  9  24 ms      22 ms     26 ms     fra24s04-in-x04.1e100.net [2a00:1450:4001:827::2004]

Trace complete.
```



Terminal — bash

```
guest@dnstools.ch:~> traceroute www.google.com
1 100.88.96.129 (100.88.96.129) 0.198 ms
2 core24.fsn1.hetzner.com (213.239.229.53) 0.412 ms
3 core4.fra.hetzner.com (213.239.203.149) 4.986 ms
4 142.250.160.234 (142.250.160.234) 4.951 ms
5 *
6 142.250.214.194 (142.250.214.194) 5.207 ms
7 142.250.46.245 (142.250.46.245) 5.716 ms
8 ams15s21-in-f132.1e100.net (216.58.212.132) 4.903 ms
```

Hop	IP / Host Name	ISP	Netblock	Country	Loss	Response
1	172.17.0.1				0.0%	0.14ms
2	10.206.5.139				0.0%	0.48ms
3	10.206.35.8				0.0%	0.68ms
4	10.206.32.1				0.0%	4.77ms
5	10.0.gw2.cjj1.us.linode.com 173.255.239.102	LINODE-AP Linode, LLC, US	173.255.239.0/24		0.0%	0.77ms
6	ae31.r01.lga01.iem.netarch.akamai.com 23.203.156.16	AKAMAI-ASN1, NL	23.203.156.0/24		0.0%	2.19ms
7	a23-203-156-153.deploy.static.akamaitechnologies.com 23.203.156.153	AKAMAI-ASN1, NL	23.203.156.0/24		0.0%	2.46ms
8	142.251.78.65	GOOGLE, US	142.250.0.0/15		0.0%	1.82ms
9	108.170.236.91	GOOGLE, US	108.170.192.0/18		0.0%	2.51ms
10	lga34s39-in-f4.1e100.net 142.251.40.228	GOOGLE, US	142.251.40.0/24		0.0%	2.68ms



















Bei Google lässt sich erkennen, dass nicht der gleiche Google Server als Ziel genutzt wird sondern wahrscheinlich immer der nächstmögliche. In dem Fall unterscheiden sich die Ziele zueinander. Laut ASN Lookup befinden sich jedoch alle Ziel-Server in der US & A.

NTTグループ公式HP

```
1      1 ms    <1 ms    2 ms    kabelbox.local [192.168.0.1]
2      12 ms    8 ms     12 ms    ip-081-210-177-201.um21.pools.vodafone-ip.de [81.210.177.201]
3      12 ms    20 ms    23 ms    de-str01c-rc1-ae-39-0.aorta.net [84.116.191.213]
4      *       20 ms    14 ms    de-fra04d-rc1-ae-10-0.aorta.net [84.116.140.205]
5      15 ms    19 ms    17 ms    84.116.190.94
6      22 ms    14 ms    17 ms    ae32-100-pcr1.fnt.cw.net [195.2.18.217]
7      33 ms    33 ms    33 ms    ae36-xcr1.ltw.cw.net [195.2.2.73]
8      28 ms    33 ms    34 ms    as2497-gw-xcr1.ltw.cw.net [195.2.14.2]
9      169 ms   165 ms   167 ms    sjc002bb00.IIJ.Net [58.138.83.178]
10     223 ms   224 ms   230 ms    tky001bb01.IIJ.Net [58.138.88.85]
11     230 ms   223 ms   231 ms    tky001ip56.IIJ.Net [58.138.101.34]
12     228 ms   231 ms   231 ms    210.130.134.98
13     238 ms   239 ms   235 ms    103.3.0.3
14     240 ms   245 ms   263 ms    103.3.0.17
15     251 ms   233 ms   234 ms    103.3.0.31
16     235 ms   238 ms   230 ms    sv138.xbiz.ne.jp [183.181.99.39]
```

```
Terminal — bash

guest@dnstools.ch:~> traceroute www.ntt.co.jp
1 100.88.96.129 (100.88.96.129) 0.197 ms
2 core23.fsn1.hetzner.com (213.239.229.49) 0.329 ms
3 core4.fra.hetzner.com (213.239.229.73) 4.882 ms
4 core2.ams.hetzner.com (213.239.203.158) 10.204 ms
5 80.249.211.96 (80.249.211.96) 171.994 ms
6 163.139.136.28 (163.139.136.28) 172.402 ms
7 163.139.136.18 (163.139.136.18) 238.584 ms
8 163.139.130.222 (163.139.130.222) 239.717 ms
9 222.230.187.206 (222.230.187.206) 248.054 ms
10 103.3.0.5 (103.3.0.5) 246.534 ms
11 103.3.0.23 (103.3.0.23) 272.948 ms
```

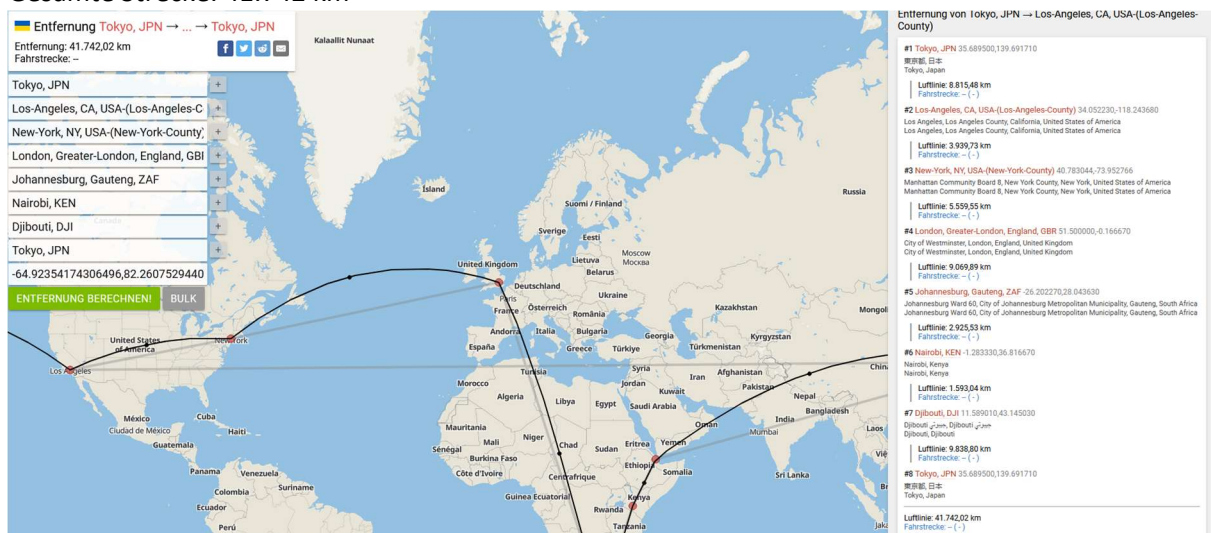
Hop	IP / Host Name	ISP	Netblock	Country	Loss	Response
1	172.17.0.1				0.0%	0.13ms
2	10.206.5.139				0.0%	0.47ms
3	10.206.35.8				0.0%	0.60ms
4	10.206.32.2				0.0%	2.96ms
5	lo0-0.gw2.cj11.us.linode.com 173.255.239.102	LINODE-AP Linode, LLC, US	173.255.239.0/24		0.0%	20.82ms
6	ae31.r01.lga01.iem.netarch.akamai.com 23.203.156.16	AKAMAI-ASN1, NL	23.203.156.0/24		0.0%	2.28ms
7	ae-29.r01.nycmy17.us.bb.gin.ntt.net 140.174.21.217	NTT-LTD-2914, US	140.174.0.0/16		0.0%	3.90ms
8	ae-13.r20.nwrknj03.us.bb.gin.ntt.net 129.250.4.40	NTT-LTD-2914, US	129.250.0.0/16		50.0%	3.17ms
9	ae-4.r24.sttlwa01.us.bb.gin.ntt.net 129.250.6.177	NTT-LTD-2914, US	129.250.0.0/16		50.0%	63.31ms
10	ae-0.a03.sttlwa01.us.bb.gin.ntt.net 129.250.2.99	NTT-LTD-2914, US	129.250.0.0/16		0.0%	62.94ms
11	ae-0.ij.sttlwa01.us.bb.gin.ntt.net 131.103.116.22	NTT-LTD-2914, US	131.103.0.0/16		0.0%	83.51ms
12	tky001bb00.IIJ.Net 58.138.88.129	IIJ Internet Initiative Japan Inc., JP	58.138.0.0/17		0.0%	158.75ms
13	tky001ip56.IIJ.Net 58.138.101.26	IIJ Internet Initiative Japan Inc., JP	58.138.0.0/17		0.0%	158.00ms
14	210.130.134.98	IIJ Internet Initiative Japan Inc., JP	210.130.0.0/16		0.0%	159.02ms
15	103.3.0.3	XSERVER Xserver Inc., JP	103.3.0.0/22		0.0%	167.19ms
16	103.3.0.17	XSERVER Xserver Inc., JP	103.3.0.0/22		0.0%	185.74ms
17	103.3.0.29	XSERVER Xserver Inc., JP	103.3.0.0/22		0.0%	167.87ms
18	sv138.xbiz.ne.jp 183.181.99.39	XSERVER Xserver Inc., JP	183.181.98.0/23		0.0%	167.31ms

Aufgabe 4



Eine detaillierte Aufzeichnung der Traceroute Knoten befindet sich auf der folgenden Seite. Es ist mittels der genannten Seite nicht möglich Pakete direkt zwischen drei Servern einmal um den Globus zu senden sondern lediglich von bis zu drei Servern zu einem Ziel. Hierbei wird in der Regel der kürzeste bzw. schnellste Pfad gewählt. Je nach Server und Ziel können Pakete auch noch über einen anderen Server am gleichen Standort gesendet werden. So gibt es z.B.: in London mehrere Server nach Johannesburg wobei einer direkt und ein anderer über Kapstadt läuft. Eine direkte Route von Marseille nach Tokyo war nicht möglich da Marseille als einziger Knotenpunkt nicht in der Liste geführt wurde.

1. Für ein Paket um den gesamten Globus wurde die kleinste Dauer einer Übertragung der unten aufgeführten Knotenpunkte addiert.
2. Daraus ergibt sich eine gesamte Zeit von: 713 ms
3. Gesamte Strecke: 41.742 km



$$t_{prop} = \frac{l}{v_{prop}} = \frac{41.742 \text{ km}}{300.000 \text{ km/s}} = 139,14 \text{ ms}$$

→ Die tatsächlich gemessene Zeit ist um ca. 574 ms länger. Dies liegt zum einen daran, dass die tatsächliche Übertragung nicht mit Lichtgeschwindigkeit erfolgt, die Kabel auch auf den Seestrecken nicht der Luftlinie nach verlaufen (siehe Routenbild) sowie aufgrund einer nicht bekannten Auslastung an den einzelnen Knotenpunkten (Paketpuffern).

Die Gewählte Route verläuft über die folgenden Knotenpunkte

● Server Tokyo [JP]: core1.tyo1.he.net

core1.tyo1.he.net> traceroute 216.218.252.106 source 27.50.33.5 numeric					
Target		216.218.252.106			
Hop Start		1			
Hop End		30			
Hop ↕	Packet 1 ↕	Packet 2 ↕	Packet 3 ↕	Hostname	
1	126 ms	107 ms	118 ms	100ge16-1.core1.lax2.he.net (184.104.195.1)	
2	*	*	*	?	
3	137 ms	119 ms	121 ms	core2.lax1.he.net (216.218.252.106)	

● Server LA [US]: core2.lax1.he.net

core2.lax1.he.net> traceroute 216.218.252.161 source 216.218.252.106					
Target		216.218.252.161			
Hop Start		1			
Hop End		30			
Hop ↕	Packet 1 ↕	Packet 2 ↕	Packet 3 ↕	Hostname	
3	61.463 ms	61.886 ms	61.902 ms	core1.nyc1.he.net (216.218.252.161)	

● Server New York [US]: core1.nyc1.he.net

core1.nyc1.he.net> traceroute 216.218.252.228 source 216.218.252.161					
Target		216.218.252.228			
Hop Start		1			
Hop End		30			
Hop ↕	Packet 1 ↕	Packet 2 ↕	Packet 3 ↕	Hostname	
1	1.819 ms	2.395 ms	2.748 ms	10ge0-91.core2.nyc5.he.net (184.104.193.9)	
3	72.397 ms	72.660 ms	72.948 ms	core3.lon1.he.net (216.218.252.228)	

● Server London [UK]: core3.lon1.he.net

core2.lon3.he.net> traceroute 216.218.252.37 source 216.218.252.57					
Target		216.218.252.37			
Hop Start		1			
Hop End		30			
Hop ↕	Packet 1 ↕	Packet 2 ↕	Packet 3 ↕	Hostname	
2	172.648 ms	174.342 ms	*	core2.jnb1.he.net (216.218.252.37)	

● Server Johannesburg [ZA]: core2.jnb1.he.net

core2.jnb1.he.net> traceroute 216.218.252.183 source 216.218.252.37					
Target		216.218.252.183			
Hop Start		1			
Hop End		30			
Hop ↕	Packet 1 ↕	Packet 2 ↕	Packet 3 ↕	Hostname	
1	59.489 ms	59.578 ms	*	core1.nbo1.he.net (216.218.252.183)	

● Server Nairobi [KE]: core1.nbo1.he.net

core1.nbo1.he.net> traceroute 216.218.252.170 source 216.218.252.183 numeric					
Target		216.218.252.170			
Hop Start		1			
Hop End		30			
Hop ↕	Packet 1 ↕	Packet 2 ↕	Packet 3 ↕	Hostname	
1	84 ms	84 ms	85 ms	core1.jib1.he.net (216.218.252.170)	

● Server Djibouti [DJ] core1.jib1.he.net

core1.jib1.he.net> traceroute 216.218.252.151 source 216.218.252.170 numeric					
Target		216.218.252.151			
Hop Start		1			
Hop End		30			
Hop ↕	Packet 1 ↕	Packet 2 ↕	Packet 3 ↕	Hostname	
1	80 ms	80 ms	80 ms	port-channel12.core3.sin1.he.net (184.105.65.237)	
2	155 ms	146 ms	147 ms	core1.tyo1.he.net (216.218.252.151)	