



**Vorlesung Rechnernetze**

Laborübung  
Ping und Traceroute

**Prof. Dr. Dirk Staehle**

**Daniel Scherz (M.Sc.)**

Die Abgabe erfolgt durch Hochladen der bearbeiteten Word-Datei in Moodle.

**Bearbeitung in Zweier-Teams**

**Team-Mitglied 1: Alexander Schapelt**

**Team-Mitglied 2: Walter Vötsch**

**Team-Mitglied 3: Josef Müller**

# Einleitung

"Ping" und "TraceRoute" sind einfache Werkzeuge, um den Pfad durch das Internet besser verstehen zu können. In der Vorlesung werden diese in Kapitel 2 kurz beschrieben. Mit WireShark wollen wir hinter die Kulissen schauen. Ping und TraceRoute werden unter Windows in der Kommandozeile (cmd) mit den Befehlen ping und tracert ausgeführt. Unter Linux lautet der Befehl traceroute.

# Ping

Pingen Sie die Web-Seite [www.nsa.gov](http://www.nsa.gov) und verfolgen Sie die gesendeten und empfangenen Pakete mittels WireShark. Setzen Sie einen Filter auf ihre eigene IP-Adresse und verursachen Sie, soweit möglich während des Versuchs keinen anderen Verkehr zu erzeugen. Beantworten Sie die folgenden Fragen für die **erste Ausführung** des Ping-Befehls für diese Adresse.

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.

Verwendete Befehle:

* Powershell: ping -n -1 [www.nsa.gov](http://www.nsa.gov)
* Wireshark:
  + NSA: ip.addr == 104.74.140.223
  + HTWG: ipv6.addr == 2001:7c0:5f0:f020::20:17

0000 3c a6 2f 57 ec b4 48 2a e3 1a d7 00 86 dd 60 00 <./W..H\*......`.

0010 00 00 00 28 3a 80 2a 02 80 70 01 8c e3 00 5c 28 ...(:.\*..p....\(

0020 d9 77 ee 95 2b 12 20 01 07 c0 05 f0 f0 20 00 00 .w..+. ...... ..

0030 00 00 00 20 00 17 80 00 d8 94 00 01 00 13 61 62 ... ..........ab

0040 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 cdefghijklmnopqr

0050 73 74 75 76 77 61 62 63 64 65 66 67 68 69 stuvwabcdefghi

Pakete:

----

# Packet 958 from C:\Users\Josef\AppData\Local\Temp\wireshark\_Ethernet 2\_20201103094922\_a07984.pcapng

* 959
* 180.058884
* 2a02:8071:82a7:6b00:74f3:4e7:9e5a:2118 (dst: ich)
* 2a02:26f0:1700:1b9::3f78 (src: nsa)
* ICMPv6
* 94
* Echo (ping) request id=0x0001, seq=973, hop limit=128 (reply in 960)

----

# Packet 1321 from C:\Users\Josef\AppData\Local\Temp\wireshark\_Ethernet 2\_20201103094922\_a07984.pcapng

* 1322
* 261.015568
* 2a02:26f0:1700:1b9::3f78
* 2a02:8071:82a7:6b00:74f3:4e7:9e5a:2118
* ICMPv6
* 94
* Echo (ping) reply id=0x0001, seq=1053, hop limit=55 (request in 1321)

1. Welche Protokolle werden zur Übertragung dieser Pakete genutzt?

* ICMP(v6)
* Ethernet

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

Minimale, maximale und durchschnittliche Zeit für hin und zurück.

Zeit steht im Frame: „Time delta from previous captured Frame”

0000 58 8a 5a 03 92 32 ac 22 05 e0 02 cb 86 dd 60 04 X.Z..2."......`.

0010 e0 93 00 28 3a 39 2a 02 26 f0 00 ce 02 95 00 00 ...(:9\*.&.......

0020 00 00 00 00 3f 78 2a 02 80 71 82 a7 6b 00 74 f3 ....?x\*..q..k.t.

0030 04 e7 9e 5a 21 18 81 00 66 06 00 01 08 bc 61 62 ...Z!...f.....ab

0040 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 cdefghijklmnopqr

0050 73 74 75 76 77 61 62 63 64 65 66 67 68 69 stuvwabcdefghi

----

# Packet 10497 from C:\Users\Josef\AppData\Local\Temp\wireshark\_Ethernet 2\_20201103094922\_a07984.pcapng

- 10498

- 1367.437434

- 2a02:26f0:ce:295::3f78

- 2a02:8071:82a7:6b00:74f3:4e7:9e5a:2118

- ICMPv6

- 94

- Echo (ping) reply id=0x0001, seq=2236, hop limit=57 (request in 10495)

1. 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.

icmp || icmpv6

- ipv6.addr == 2a02:8071:82a7:6b00:74f3:4e7:9e5a:2118 && (icmp || icmpv6)

Starten Sie eine Versuchsreihe. Suchen Sie sich IP-Adressen/Hostnamen von Rechnern, die sich an unterschiedlichen Orten befinden z.B. im Labor, an der HTWG, in Deutschland, in Australien oder in Nordamerika. Beispiele sind Server von Universitäten, Staaten, Zeitungen, Firmen, etc.

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.

ping -n 100 <URL> | findstr Zeit= >> <file> dann find and replace

Hinweis: Mit „ping -?“ erhalten Sie eine Übersicht der Optionen, mit denen Sie den Ping-Befehl aufrufen können.

Tipp: Verwenden Sie in Excel die Funktion „Externe Daten abrufen“ Unterkategorie „Aus Text“ im Menü Daten, um die gespeicherten Dateien zu laden. Geben Sie entsprechende Trennzeichen ein, um die gewünschte Spalte zu erhalten.

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

Hinweis: Am einfachsten können Sie die Daten generieren, indem Sie die folgende als Batch-Skript ausführen, nachdem Sie ihre Parameter eingesetzt haben. Das Ergebnis können Sie dann wieder mit dem Tool ihrer Wahl darstellen.

for %%a IN (<Paktelängen>) DO (ping -l %%a -n <anzahl> <url> | findstr Mittelwert >> <datei>)

# TraceRoute

Verwenden Sie das Tool "TraceRoute", um Pfade durch das Internet zu entdecken. Da die Firewall der Hochschule Ping-Pakete teilweise blockiert, können Sie „traceroute“ auf den Laborrechnern nicht nutzen. Sie müssen daher auf Online-Tools zurückgreifen, wie Sie sie beispielweise auf folgenden Web-Seiten finden:

* <https://traceroute-online.com/>
* <http://www.dnstools.ch/visual-traceroute.html>
* <https://centralops.net/co/>
* <https://lg.he.net/>

Weitere Online-Tools finden Sie einfach über Google. Wenn Sie die Übung zu Hause durchführen und traceroute funktioniert, können Sie den Befehl natürlich auch dort ausführen.

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

Siehe [Tracert.xslt](Tracert.xlsx)

1. 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>.

- Eigener Rechner:

- Regional Internet Registrar: ripencc

- IP-Besitzer: LIBERTYGLOBAL Liberty Global (Hier Unitymedia)

Siehe [Tracert.xslt](Tracert.xlsx) linke Tabellen. Bei diesen wurde der tracert Befehl verwendet

1. 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](http://www.ntt.co.jp) und [www.google.com](http://www.google.com) aus. Bestimmen Sie, welche Teile der Route für die unterschiedlichen Kombinationen aus Online-Tool und Zielrechner identisch sind.

Siehe [Tracert.xslt](Tracert.xlsx) linke Tabellen. Wenn zwei oder mehrere Zellen dieselbe Hintergrundfarbe besitzen, haben sie denselben Knoten.

Beobachtung:

- zwischen zwei Netzen gibt es häufig eine MAC Adresse, die keine Zuordnung hat

# Network Latency

Nutzen Sie das „Looking Glas“-Tool von Hurricane Electric (lg.he.net), um Laufzeiten im Core-Netzwerk eines Tier-1-Providers zu messen. Das Tool ermöglicht es Ihnen, Ping- oder Traceroute-Befehle auf den Core-Network-Routern (diese können sie auf der linken Seite durch Anclicken auswählen) auszuführen. Tragen Sie dann jeweils die IP-Adresse oder URL des Rechners, den Sie anpingen möchten, auf der rechten Seite ein.

1. Betrachten Sie das Netz von Hurricane Electric und bestimmen Sie eine weltumspannende Route (<https://www.he.net/HurricaneElectricNetworkMap.pdf>). Führen Sie dazu Traceroute auf einem oder mehreren Routern zu einem Zielrouter aus, um 3 Router zu finden, zwischen denen die Pakete die Welt umlaufen. Die URL eines Routers erhalten Sie, indem Sie im „Looking Glas“ mit der Maus auf den Namen des Routers fahren.

Guam -> Cape Town (Guam, Honolulu, LA, Ashburn, NYC, London, Cape Town)

| Hop | Packet 3 | Hostname |
| --- | --- | --- |
| 1 | 67.226 ms | **100ge8-1.core1.hnl1.he.net** (184.105.223.249) |
| 2 | 112.291 ms | **100ge0-32.core2.lax2.he.net** (184.104.193.233) |
| 3 | 119.141 ms | **100ge10-2.core1.lax2.he.net** (184.104.192.233) |
| 4 | 112.848 ms | **100ge2-2.core1.lax1.he.net** (72.52.92.121) |
| 5 | 167.305 ms | **100ge12-1.core1.ash1.he.net** (184.105.80.201) |
| 6 | 171.746 ms | **100ge1-1.core1.nyc4.he.net** (184.105.223.166) |
| 7 | 237.407 ms | **100ge7-1.core1.lon2.he.net** (72.52.92.165) |
| 8 | 386.559 ms | **core1.cpt1.he.net** (216.218.252.112) |

(Cape Town -> Tokyo ist der Rückweg)

| Hop | Packet 3 | Hostname |
| --- | --- | --- |
| 1 | 16.819 ms | **10ge11-12.core1.jnb1.he.net** (184.105.222.145) |
| 2 | 24.039 ms | **10ge0-24.core1.dur1.he.net** (184.105.222.62) |
| 3 | 70.712 ms | **10ge0-48.core1.mba1.he.net** (184.104.192.85) |
| 4 | 149.652 ms | **10ge14-6.core1.jib1.he.net** (184.105.81.142) |
| 5 | 227.967 ms | **10ge3-19.core1.sin1.he.net** (184.105.65.237) |
| 6 | 260.595 ms | **100ge14-2.core1.hkg1.he.net** (184.105.222.101) |
| 7 | 342.707 ms | **core1.tyo1.he.net** (216.218.252.151) |

1. Was ist die einfache Verzögerung (One-Way-Delay), die ein Ping-Paket auf dieser Route benötigt. Messen Sie dazu die Ping-Zeiten von Router zu Router.

386.301ms / 2 = 193,1505ms

(311,563ms / 2 = 155,7815ms Rückweg)

1. Was ist die theoretische Minimallaufzeit eines Pakets auf dieser Route, wenn Sie eine Ausbreitung mit Lichtgeschwindigkeit auf direktem Weg voraussetzen (z.B. <http://www.luftlinie.org/>)? Um welchen Faktor ist die tatsächlich gemessene Zeit länger als das theoretische Minimum? Führen Sie Erklärungen für die längeren Laufzeiten an.

c = 300 000km/s s = 14 183 km -> s/c = 0.0473s = 47.3ms (ttx vernachlässigt)

Faktor f = 193,1505ms / 47.3ms = 4,085

Erklärung:

1. Kein direkter Weg
2. Keine Lichtgeschwindigkeit
3. Verzögerung pro hop

(Rückweg etwa gleich (s = 14 737 km))