



**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: Begüm Peker**

**Team-Mitglied 2: Ellen Peppmüller**

# 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.umass.edu](http://www.umass.edu) an und verfolgen Sie die gesendeten und empfangenen Pakete mittels WireShark. Setzen Sie einen Filter auf ihre eigene IP-Adresse und versuchen Sie, während des Versuchs keinen anderen Verkehr zu erzeugen. Beantworten Sie die folgenden Fragen für die **erste Ausführung** des Ping-Befehls für diese Adresse.

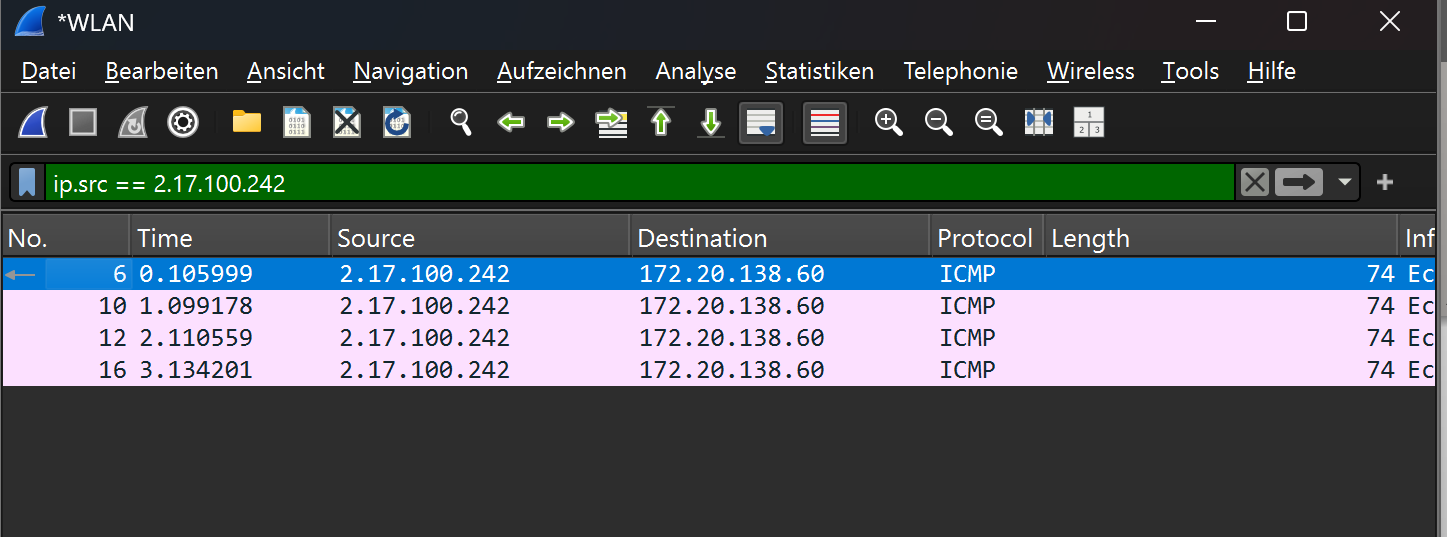
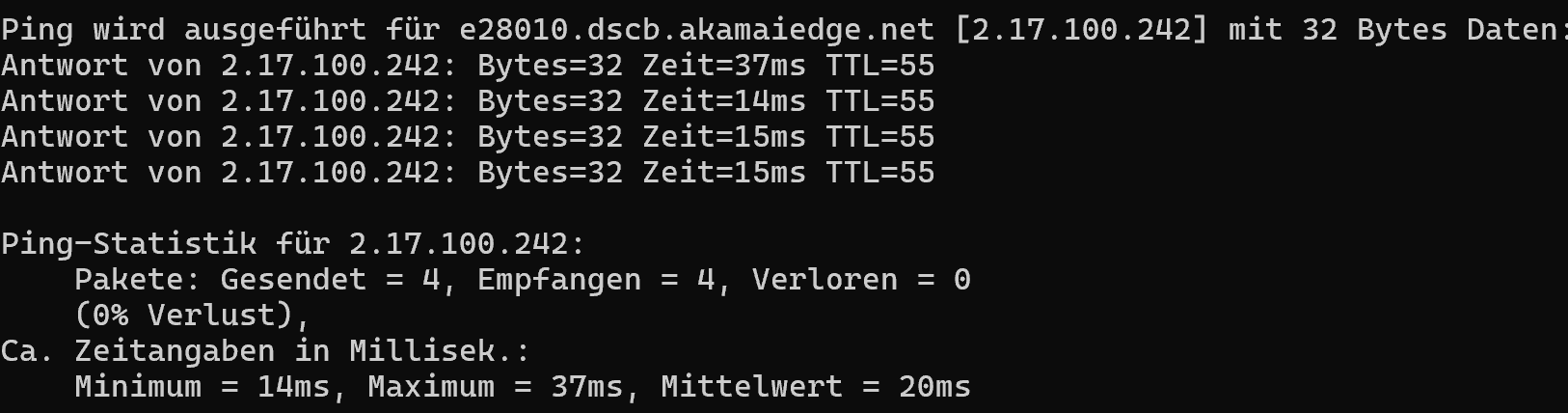
1. Welche Pakete werden gesendet, wenn der Ping-Befehl ausgeführt wird? Kopieren Sie die entsprechenden Pakete aus WireShark. Führen Sie den Ping-Befehl gegebenenfalls für mehrere IP-Adressen aus, um diese Pakete zu identifizieren.

* ICMP:   
  3 0.035734 172.20.138.60 2.17.100.242 ICMP 74 Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 4)  
  4 0.047675 2.17.100.242 172.20.138.60 ICMP 74 Echo (ping) reply id=0x0001, seq=23/5888, ttl=55 (request in 3)  
  5 1.049233 172.20.138.60 2.17.100.242 ICMP 74 Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 6)  
  6 1.064303 2.17.100.242 172.20.138.60 ICMP 74 Echo (ping) reply id=0x0001, seq=24/6144, ttl=55 (request in 5)  
  7 2.071505 172.20.138.60 2.17.100.242 ICMP 74 Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 8)  
  8 2.089526 2.17.100.242 172.20.138.60 ICMP 74 Echo (ping) reply id=0x0001, seq=25/6400, ttl=55 (request in 7)  
  9 3.080233 172.20.138.60 2.17.100.242 ICMP 74 Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 10)  
  10 3.093849 2.17.100.242 172.20.138.60 ICMP 74 Echo (ping) reply id=0x0001, seq=26/6656, ttl=55 (request in 9)

1. Vor der Übertragung der eigentlichen Ping-Pakete wird (bei Verwendung eines neuen Hostnamens/ einer neuen URL) ein anderes Protokoll ausgeführt? Bestimmen Sie dieses Protokoll. Führen Sie den Ping-Befehl gegebenenfalls für mehrere **neue** Web-Seiten aus.

* DNS?

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



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.

* *ip.addr == 172.20.138.60 and dns or icmp*

1. Implementieren Sie eine Versuchsreihe in Python (Tipp: ping aus dem Modul icmplib). 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. Pingen Sie die Adressen jeweils 100mal und stellen Sie die Ping-Zeit grafisch dar.

Hinweise:

* Mit „ping -?“ erhalten Sie eine Übersicht der Optionen, mit denen Sie den Ping-Befehl aufrufen können.
* Mit ipconfig /displaydns und ipconfig /*flushdns* können Sie unter Windows den DNS-Cache anzeigen und löschen*.*
* Mit nslookup können Sie explizit einen DNS-Lookup für einen Hostnamen ausführen.

# TraceRoute

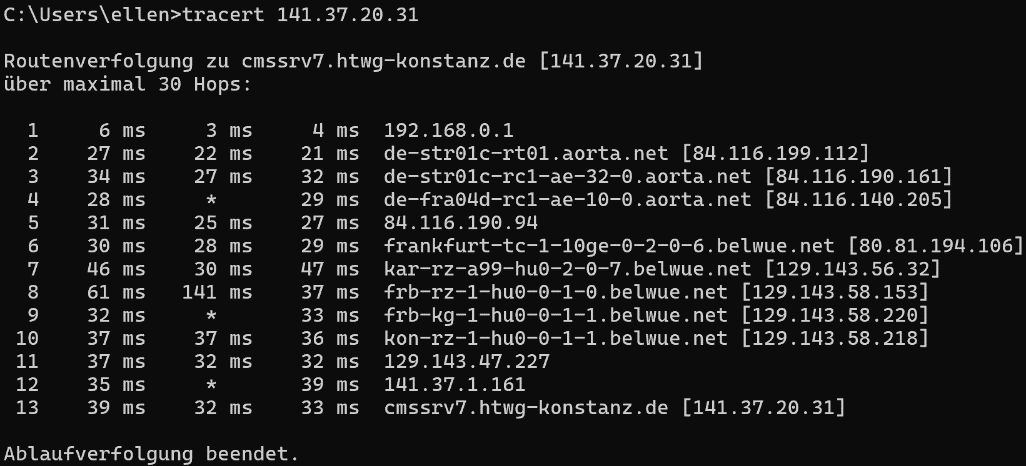
Verwenden Sie das Tool "TraceRoute", um Pfade durch das Internet zu entdecken. Da die Firewall der Hochschule Ping-Pakete teilweise blockiert, können Sie „traceroute“ auf den Laborrechnern nicht nutzen. Sie müssen daher auf Online-Tools zurückgreifen, wie Sie sie beispielweise auf folgenden Web-Seiten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

* <https://traceroute-online.com/>
* <https://gsuite.tools/traceroute>
* <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?

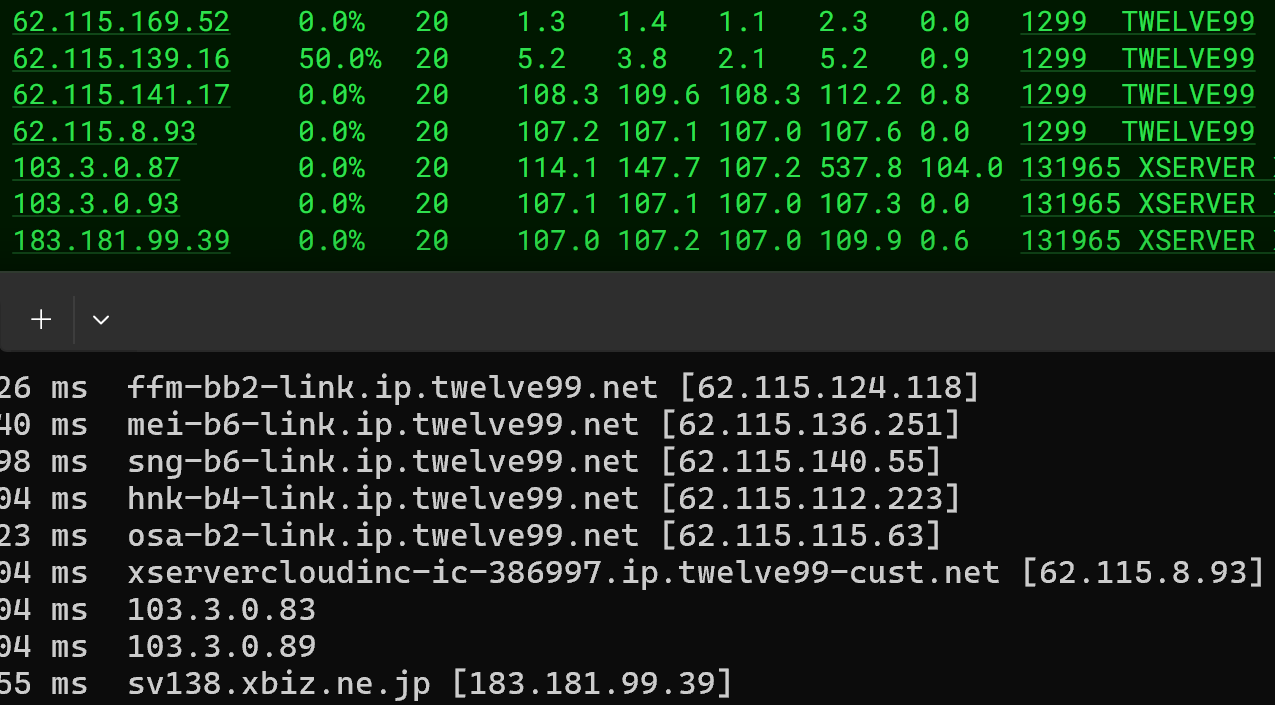
Tracert zeigt Hops die das Paket durchläuft, um von meinem Rechner zum Zielpunkt zu kommen.  
Jeder Hop ist Router oder Knotenpunkt im Netzwerk.

* C:\Users\ellen>tracert 172.20.138.60
* Routenverfolgung zu EllenSurface23.htwg-konstanz.de [172.20.138.60]
* über maximal 30 Hops:
* 1 <1 ms <1 ms <1 ms EllenSurface23.htwg-konstanz.de [172.20.138.60]
* Ablaufverfolgung beendet.
* 
* Routenverfolgung zu HTWG Server dauert wesentlich länger und durchläuft Rechenzentren von Freiburg, Frankfurt, Karlsruhe und Konstanz bis Server erreicht. Bei eigener IP sofort erreicht.  
  BelWü: Landeshochschulnetz das Unis und FHs verbindet

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.asnlookup.com/>.

* [AS3209](https://www.asnlookup.com/asn/AS3209) VODANET, [AS6830](https://www.asnlookup.com/asn/AS6830) LibertyGlobal (NL), [AS553](https://www.asnlookup.com/asn/AS553) BELWUE (Uni Stgt)
* IP-Adresse in asnlookup eingeben und ASN Nummer und Name einsehen

1. Betrachten Sie nun mehrere Online-Tools, so dass Sie den Traceroute-Befehl von mindestens zwei 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) (Sie können auch eine beliebige entfernte Seite wählen) 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.

* 



Ntt.co.jp (traceroute online, ping.pe, terminal)

# 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, einen Ping-Befehl auf den Core-Network-Routern (diese können sie auf der linken Seite durch Anklicken auswählen) auszuführen. Tragen Sie dann jeweils die IP-Adresse oder den Hostnamen des Rechners, den Sie anpingen möchten, auf der rechten Seite ein. In der Aufgabe sind das auch wieder Router von Hurricane Electric. Die Hostnamen sehen Sie, wenn Sie mit der Maus über die Routernamen fahren.

Hinweis: Die Web-Seite von Hurricane Electric ist teilweise überlastet und reagiert daher sehr zäh. Sie können für diese Aufgabe auch auf andere ISPs mit Looking -Glass-Funktionalität ausweichen z.B.

NTT: <https://www.gin.ntt.net/looking-glass-landing/>

Cogent: <https://cogentco.com/en/looking-glass>

Arelion: <https://www.arelion.com> / <https://lg.twelve99.net>

IPTP Networks: <https://www.iptp.net>

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. Sie schicken also nicht ein Ping-Pakete um die Welt, sondern teilen die Strecke in drei (oder mehr) Ping-Pakete auf.
   1. Router A->Router B
   2. Router B-> Router C
   3. Router C->…
   4. …->Router A
2. 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.
3. 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.