Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)
Fakultät Informatik
Rechner- und Kommunikationsnetze
Prof. Dr. Dirk Staehle

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: **Julian Mennel**

Team-Mitglied 2: **Maximilian Schmidt**

1 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`.

2 Ping

Pingen Sie die Web-Seite www.nsa.gov 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.
   Antwort:
   Request:
   132 15.318842 192.168.178.46 104.64.17.8 ICMP 74 Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 134)
   Reply:
   134 15.353193 104.64.17.8 192.168.178.46 ICMP 74 Echo (ping) reply id=0x0001, seq=1/256, ttl=58 (request in 132)
2. Welche Protokolle werden zur Übertragung dieser Pakete genutzt?
   Antwort: ICMP oder ICMPV6
3. Welche Ergebnisse liefert der Ping-Befehl? Wie können Sie diese Ergebnisse aus den in WireShark aufgezeichneten Paketen bestimmen?
   Antwort: Der Ping Befehl zeigt mir die IP-Adresse des Ziels, sowie die gesendete Datenmenge, die Zeit, die es von einer Anfrage bis zu einer einkommenden Antwort braucht, als auch, wie lange die Daten im Rechnernetz gültig bleiben (ttl, Wert in Sekunden). Mit geeigneten Filtern (Source oder Destination IP auf Zieladdresse setzen) lässt sich filtern, wie viele Pakete geschickt oder empfangen wurden. Im Gegensatz zum Ping Befehl, zeigt Wireshark die Gesamtgröße des Pakets inklusive Header an, nicht nur die Daten an sich. An den Reply Paketen kann auch der TTL Wert abgelesen werden. Setzt man den Zeitstempel eines Requests als Referenzwert, kann man an der dazugehörigen Reply die Zeit erkennen, die im Ping Befehl gemessen wurde. Jedes Paket hat eine eindeutige von Wireshark vergebene Nummer (Frame), die Nummer der Reply zu einem Request ist als Information mit angegeben, genauso umgekehrt. Bei ICMPV6 wird statt der TTL ein hop limit in Wireshark angegeben. Im ICMP des Reply wird in wireshark auch die Response Time in ms angezeigt.
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.

Antwort: (icmpv6 && ipv6.addr == 2001:7c0:5f0:f020::20:31) || (icmp && ip.addr == 104.70.81.2) Mit diesem Filter werden alle ICMP und ICMPV6 Protokolle, in denen als Ziel- oder Quelladresse die deklarierte Adresse vorkommt. In unserem Beispiel korrespondiert die ipv6 Adresse mit www.htwg-konstanz.de und die ipv4 Adresse mit www.nsa.gov. Will man lediglich nach Anfragen oder Antworten sortieren, so muss man ipv6.dst, oder ipv6.src verwenden (ip.dest, ip.src äquivalent für ipv4 Adressen).

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.

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

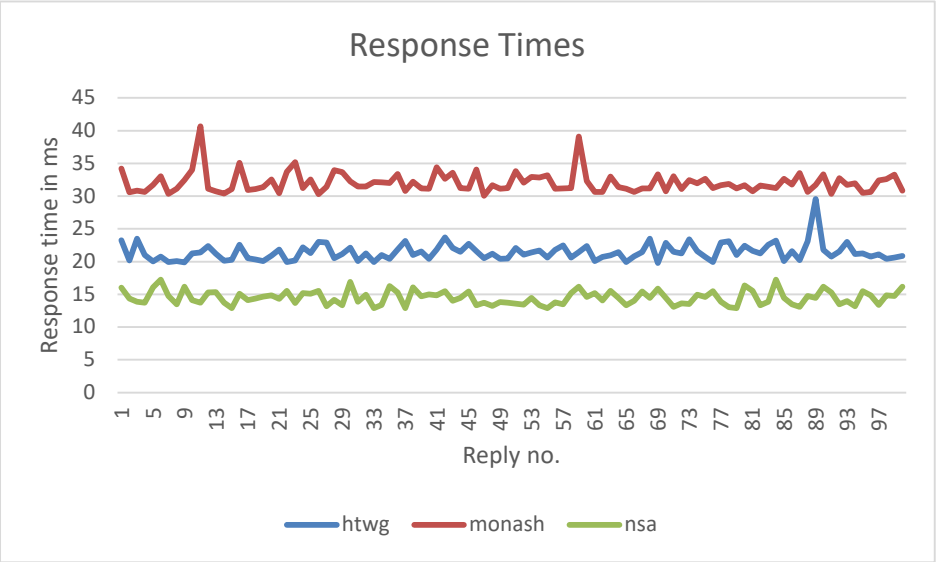
   Tipp: Verwenden Sie in Excel die Funktion „Externe Daten abrufen“ Unterkategorie „Aus Text“ im Menü Daten, um die gespeicherten Dateien zu laden. Geben Sie entsprechende Trennzeichen ein, um die gewünschte Spalte zu erhalten.

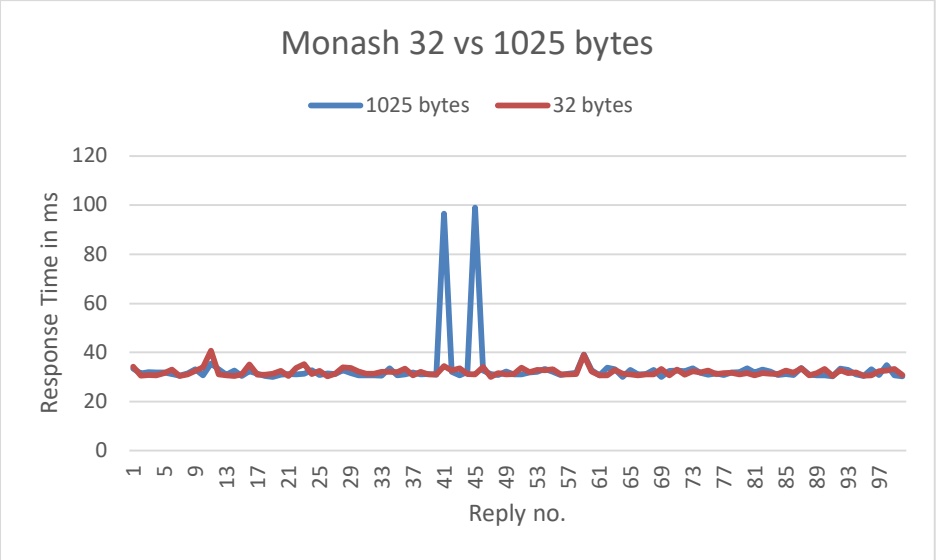
2. Wählen Sie die Adresse mit den längsten Ping-Zeiten und stellen Sie den Einfluss der Paketgröße grafisch dar.

   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>)

   Antwort: Bis auf Ausreißer scheint die Response Time unbeeinflusst von der Paketgröße zu sein. Bei Paketgrößen die größer waren als ein Wert zwischen 1000-2000 kam es außerdem zu Laufzeitüberschreitungen.





3 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?

   Antwort: Zeigt mir alle Knotenpunkte der Route von meinem Rechner bis zur Zieladresse auf. Es werden 3 Pakete verschickt und die Response Times aller drei Pakete zu den Knotenpunkten aufgezeigt. Verfolge ich meine eigene Adresse, wird nur ein Hop zu mir angezeigt mit host.docker.internal.

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.
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.

   Antwort: Bei google.com sehe ich keinerlei Übereinstimmungen mit den ersten drei der oben genannten Tools. Für ntt.co.jp ergibt sich ein ähnliches Bild. Lediglich die Zieladresse scheint übereinzustimmen, allerdings scheint die Seite auf bis zu vier unterschiedlichen Adressen aufzulösen, die mir das Tool von centralops.net auch anzeigt.

4 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.
   Antwort: Tokyo-Singapore-Marseille-Paris-NYC-LA-Tokyo
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.
   Antwort:
   a. Tokyo-Singapore: 75ms
   b. Singapore-Marseille: 136ms
   c. Marseille-Paris: 11.609ms
   d. Paris-NYC: 71.871ms

e. NYC-LA: 69.123ms
f. LA-Tokyo: 125.076ms

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.
   Antwort: Entfernung der Route: 35.160,79km
   Zeit, die Licht für diese Strecke braucht: 117.283771028022 ms
   Einzelne Pings dauern teilweise schon länger als das Licht theoretisch für diese Strecke bräuchte. Die reale Strecke, die durch Verbindungen zurückgelegt werden, sind natürlich etwas größer als die Luftlinie, außerdem müssen die Pakete von den einzelnen Rechnern erst einmal bearbeitet und zwischen den einzelnen Schichten transportiert werden, was Rechenzeit kostet. Scheduling und Pakete, die vor unserer Anfrage verarbeitet werden, können zusätzlich Zeit kosten.