Übung – Nachverfolgen der Internetverbindung

# Hinweis:

Nutzen Sie statt der Kommandozeilentools die folgenden Internet-Services:

* <https://www.heise.de/netze/tools/ping/>
* <https://www.heise.de/netze/tools/traceroute/>

1. Zielsetzung

* Bestimmen der Netzwerkverbindung mit einem Zielhost
* Nachverfolgen einer Route zu einem Remote-Server mithilfe von tracert

1. Hintergrund/Szenario

Daten strömen von einem Quell-Endgerät zu einem Zielgerät. Software zur Routennachverfolgung listet den Pfad auf, den diese Daten nehmen.

Diese Software wird normalerweise über die Kommandozeile folgendermaßen ausgeführt:

**tracert** <Name des Zielnetzwerks oder Adresse des Endgeräts>

(Microsoft Windows-Systeme)

oder

**traceroute** <Name des Zielnetzwerks oder Adresse des Endgeräts>

(UNIX- und Linux-Systeme sowie Cisco Geräte wie Switches und Router)

Sowohl **tracert** als auch **traceroute** bestimmen die Route, die Pakete in einem IP-Netzwerk nehmen.

Das **tracert**- (oder **traceroute**-) -Tool wird häufig zur Problembehebung im Netzwerk verwendet. Es wird eine Liste von Routern angezeigt, die die Daten durchlaufen. Anhand dieser Liste kann der Benutzer den Pfad identifizieren, über den ein bestimmtes Ziel im Netzwerk oder durch verschiedene Verbundnetzwerke erreicht wird. Jeder Router stellt einen Punkt dar, an dem ein Netz mit einem anderen Netz verbunden ist und über den das Paket weitergeleitet wurde. Die Anzahl der durchquerten Router wird als die Anzahl der Hops bezeichnet, die die Daten von der Quelle zum Ziel durchlaufen haben.

Kommandozeilenbasierte Tools zur Routennachverfolgung sind normalerweise in das Betriebssystem des Endgeräts eingebettet. Diese Aktivität sollte auf einem Computer ausgeführt werden, der Zugang zum Internet und Zugriff auf eine Kommandozeile hat.

1. Erforderliche Ressourcen

PC mit Internetzugang

* 1. Bestimmen der Netzwerkverbindung mit einem Zielhost

Um die Route zu einem entfernten Netzwerk nachzuverfolgen, muss der PC über eine aktive Verbindung zum Internet verfügen. Verwenden Sie den **Ping**-Befehl, um zu überprüfen, ob ein Host erreichbar ist. Informationspakete werden mit der Anweisung zu antworten an den Remote-Host gesendet. Der PC misst, ob jedes Paket eine Antwort erhält und wie lange diese Pakete brauchen, um das Netzwerk zu durchqueren.

* + 1. Geben Sie in der Eingabeaufforderung **ping www.cisco.com** ein, um festzustellen, ob diese Website erreichbar ist.



* + 1. Pingen Sie nun eine der in unterschiedlichen Teilen der Welt befindlichen Regional Internet Registry-Websites (RIR) an, um festzustellen, ob diese erreichbar sind:

Afrika: **www.afrinic.net**

Australien: **www.apnic.net**

Südamerika: **www.lacnic.net**

Nordamerika: **www.arin.net**

**Hinweis**: Zum Zeitpunkt der Erstellung dieses Dokuments antwortet die europäische RIR [www.ripe.net](http://www.ripe.net/) nicht auf ICMP-Echo-Anfragen.

Die von Ihnen ausgewählte Website wird in Teil 2 zum Einsatz des Befehls **tracert** verwendet.

* 1. Nachverfolgen einer Route zu einem Remote-Server mithilfe von tracert

Nachdem Sie **Ping** verwendet haben, um zu bestimmen, ob die von Ihnen gewählten Websites erreichbar sind, verwenden Sie nun **tracert**, um den Pfad zur Erreichung des Remote-Servers zu bestimmen. Sehen Sie sich jeden durchquerten Netzwerkabschnitt genau an.

Jeder Hop in den **tracert**-Ergebnissen zeigt die Routen an, die die Pakete nehmen, wenn sie sich zum endgültigen Ziel bewegen. Der PC sendet drei Pakete mit ICMP-Echo-Anfragen an den Remote-Host. Jeder Router auf dem Pfad dekrementiert den Time-to-Live-Wert (TTL) um 1, bevor er das Paket zum nächsten System weiterleitet. Dekrementieren bedeutet stufenweise verringern, also herunterzählen. Wenn der dekrementierte TTL-Wert 0 erreicht, sendet der Router die Meldung „ICMP Time Exceeded“ (ICMP-Zeitüberschreitung) zusammen mit seiner IP-Adresse und der aktuellen Uhrzeit zurück an die Quelle. Wenn das letztendliche Ziel erreicht ist, wird eine ICMP-Echo-Antwort zurück an den Quell-Host gesendet.

* + 1. Verfolgen Sie in der Eingabeaufforderung die Route zurück zu [www.cisco.com](http://www.cisco.com/).

C:\Benutzer\Benutzer1> **tracert** www.cisco.com

Routenverfolgung zu e144.dscb.akamaiedge.net [23.67.208.170]

über maximal 30 Hops:

1 1 ms <1 ms <1 ms 192.168.1.1

2 14 ms 7 ms 7 ms 10.39.0.1

3 10 ms 8 ms 7 ms 172.21.0.118

4 11 ms 11 ms 11 ms 70.169.73.196

5 10 ms 9 ms 11 ms 70.169.75.157

6 60 ms 49 ms \* 68.1.2.109

7 43 ms 39 ms 38 ms Equinix-DFW2.netarch.akamai.com [206.223.118.102]

8 33 ms 35 ms 33 ms a23-67-208-170.deploy.akamaitechnologies.com [23.67.208.170]

Trace complete.

In diesem Beispiel sendet der Quell-Host drei Pakete mit ICMP-Echo-Anfragen mit dem TTL-Wert 1 an den ersten Hop (192.168.1.1). Wenn der Router 192.168.1.1 die Echo-Anfragen-Pakete empfängt, dekrementiert er den TTL-Wert auf 0. Der Router sendet die Meldung „ICMP Time Exceeded“ (ICMP-Zeitüberschreitung) zurück an die Quelle. Dieser Vorgang wird fortgesetzt, bis der Quell-Host die letzten drei Pakete mit ICMP-Echo-Anfragen mit dem TTL-Wert 8 (Hop Nr. 8 im Beispiel oben) sendet. Dies ist das endgültige Ziel. Nachdem die ICMP-Echo-Anfragenpakete am endgültigen Ziel angekommen sind, antwortet der Router der Quelle mit ICMP-Echo-Antworten.

Bei den Hops 2 und 3 sind diese IP-Adressen private Adressen. Diese Router bilden das typische Setup für den Point-of-Presence (POP) bei Internet-Service-Providern (ISP). Die POP-Geräte verbinden Benutzer mit einem ISP-Netzwerk.

* + 1. Führen Sie nun einen **tracert** zu einer der RIR-Websites aus Teil 1 durch.

Afrika: **www.afrinic.net**

Australien: **www.apnic.net**

Südamerika: **www.lacnic.net**

Nordamerika: **www.arin.net**

* + 1. Ein webbasiertes „Whois“-Tool finden Sie unter <http://whois.domaintools.com/>. Damit können Sie ermitteln, welche Domains von der Quelle bis zum Ziel durchlaufen wurden.

Listen Sie die mit einem Whois-Tool wie <http://whois.domaintools.com/> ermittelten Domains aus Ihren tracert-Ergebnissen unten auf.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_