

Übung 3 - Traceroute

1 Einführung

In diesem Kapitel werden Sie sich mit der Routenverfolgung in Computernetzen beschäftigen. Nachdem Sie bereits die Programme `ping` und `nslookup` kennengelernt und erfolgreich eingesetzt haben, werden Sie in dieser Übung das Werkzeug `traceroute` kennenlernen und die Protokolleigenschaften der Schichten 3 und 4 näher betrachten.

Bitte tragen Sie sich diejenigen Computersysteme Ihrer Testumgebung in Ihre Tabelle ein, die Sie heute neu kennenlernen.

2 Vorbereitung und nützliche Literatur

Zum näheren Verständnis der eingesetzten Werkzeuge und der in den Aufgaben behandelten Themen, finden Sie in den folgenden Literaturhinweisen weitere Informationen.

Literatur:

- RFC 1574, „Essential Tools for the OSI Internet“
- RFC 792, „Internet Control Message Protocol“
- <http://www.faqs.org/docs/Linux-HOWTO/Firewall-Howto.html>
- Lesen Sie auf Ihren Sun Workstations die Manualpages zu den Befehlen `ping` und `traceroute` (Auf MS Windows Systemen finden Sie entsprechende Befehle. Ein Programm, das die gleiche Funktion wie das Unix-Programm `traceroute` zur Verfügung stellt, heißt auf MS Windows Systemen `tracert`.)

Praktische Vorbereitung:

- Prüfen Sie ob und welche Rechner Sie im Testnetz erreichen.
- Prägen Sie sich die Namen und IP-Adressen der Rechner aus der Übung 2 ein.

3 Aufgaben

Alle von Ihnen durchzuführenden Analysen erfolgen ausschließlich aus dem Testnetz heraus. Dazu müssen Sie sich mit verschiedenen Arbeitsplatzcomputern in Ihrem Testnetz verbinden.

Verwenden Sie dazu bitte das Programm `vncviewer`. Der `vncviewer` ist ein Programm für den grafischen Fernzugriff auf entfernte Computer.

Um die Aufgaben zügig bearbeiten und alle relevanten Informationen ermitteln zu können, starten Sie parallel auf Ihrem Partnerrechner das bereits bekannte Netzwerkanalysewerkzeug `wireshark`.

Hinweise zum Fernzugriff per vnc

- Öffnen Sie eine Terminalkonsole und geben Sie den Programmnamen `vncviewer` ein.
- geben Sie den Name oder die IP-Adresse des entfernten Computers ein.
- Als Passwort verwenden Sie das bereits bekannte Passwort, daß Sie verwendet haben, um sich mit `radon` oder `chlor` zu verbinden.

3.1 Netzwerkanalyse mit Linux

Übung 3 - Traceroute

Verbinden Sie sich mit `vnc` auf die Arbeitsplatzclients `lanthan` oder `luthetium` und bearbeiten Sie die folgenden Fragestellungen.

- Analysieren Sie, in welchem IP-Adressraum sich Ihre Arbeitsplatzclients befinden
- Unter welchem Pfad ist das Netzwerkanalysewerkzeug `traceroute` auf Ihrem System installiert? (Sie finden `traceroute` unter Linux nicht? Lesen Sie dazu die Manualpages von `whereis`)
- Im nächsten Schritt werden Sie eine Routenverfolgung mit `traceroute` durchführen. Zeichnen Sie dazu die von `traceroute` erzeugten Datenpakete auf. Stellen Sie im `wireshark` den Capture-Filter derart ein, daß Sie nur die Pakete in Verbindung mit Ihrem Trace sehen! Beginnen Sie Ihre Analysen im gelben Teil unseres Testnetzes (beachten Sie die korrekte Wahl des Interfaces in `wireshark`). Für Ihre Dokumentation kommt es hierbei auf
 - die Richtung,
 - die Protokolle der Schichten 2 und 3,
 - den sogenannten TTL-Count und
 - den Protokolltyp,
 - sowie die Ports an.
- Sichern Sie die mitgeschnittene Datei unter Ihrer Gruppenbezeichnung und machen Sie den Sniffer (`wireshark`) wieder frei.
- Führen Sie per `traceroute` eine Routenverfolgung zur IP-Adresse von `www.auckland.ac.nz` aus und protokollieren Sie die von `traceroute` erzeugten Pakete sowie deren Antwort-Pakete in einem Ablaufdiagramm.
- Wiederholen Sie den letzten Vorgang und protokollieren Sie mit `wireshark` nun den Netzwerkverkehr im blauen Teil des Testnetzes.

3.2 Netzwerkanalyse mit MS Windows

Verbinden Sie sich per `vnc` mit den MS Windows Systemen `wolfram` und `wismut`.

Führen Sie nun bitte die gleichen Schritte aus dem Abschnitt 3.1 aus und bearbeiten Sie die dort gestellten Fragestellungen für eine Routenverfolgung von einem der MS Windows Systeme.

3.3 Unterschiede bei der Netzwerkanalyse mit Linux und MS Windows

Bitte beantworten Sie nun noch die folgenden Fragen.

- a) Beschreiben Sie die Unterschiede zwischen der Routenverfolgung aus dem gelben und blauen Netzsegment heraus.
- b) In welcher Protokolleigenschaft unterscheiden sich die Versionen des Werkzeuges zur Routenverfolgung auf MS Windows (`tracert`) und Linuxsystemen (`traceroute`)?

3.4 allgemeine Routenverfolgung

Starten Sie eine Routenverfolgung zu `137.229.9.250`

- a) Welchen Weg legt das Signal zum Ziel zurück. Gehen Sie von einer Signalausbreitung von $7,5 \text{ ns/m}$ aus.
- b) Wem gehört diese IP?

Übung 3 - Traceroute

- c) Sie erhalten für jeden Rechner mehrere unterschiedliche Zeitangaben. Von welcher Laufzeit Angabe für die Gesamtstrecke gehen Sie aus? Warum?

3.5 Verfeinern der Sicht auf traceroute

Starten Sie eine Routenverfolgung von Ihrer Sun zum DNS-Server im blauen Netz und bearbeiten Sie die folgenden Fragestellungen. Erfassen Sie den Trace mit Wireshark. Filtern Sie Ihre aufgezeichneten Netzwerkpakete derart, dass Sie die beteiligten Protokolle Ihres Systems sehen.

- a) Was bedeuten die 3 Zeiten in jeder Zeile?
b) Dokumentieren Sie die einzelnen Protokollschritte, die `traceroute` durchläuft. Bitte dokumentieren Sie gesondert die Unterschiede der Pakete auf dem Weg zum Zielrechner (Hinweis: es sind mindestens 5x3 Pakete für die Lösung erforderlich).