

Übung 3 - Traceroute

1 Einführung

In der vergangenen Übung haben Sie mit dem POP3-Protokoll ein Protokoll der Anwendungsschicht (Application Layer) kennengelernt.

In der vorliegenden Übung werden Sie erste Einblicke in die Netzwerkschicht (Network Layer) erhalten. Sie werden sich dazu 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.

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`



Hinweis - 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`.

Übung 3 - Traceroute

3.1 Pingscript

Um in Zukunft zügig zu ermitteln, ob alle für die Übung relevanten Systeme zur Verfügung stehen, schreiben Sie ein Skript `pingall.sh`, mit dem Sie schnell die Erreichbarkeit von Hosts im gelben und im blauen Testnetz (ab 141.64.63.193) überprüfen können.



Hinweis – Schreiben Sie das Skript ggf. nachdem Sie die anderen Aufgaben erledigt haben. Gestalten Sie die Ausgabe Ihres Skript derart, daß pro Zeile eine Information über einen Host angezeigt wird und alle überflüssigen Informationen nicht angezeigt werden. Außerdem soll pro Zeile der Name des betreffenden Rechners ausgegeben werden.

Beispiel:

```
192.168.0.40 ist erreichbar (kermit.home.net)
192.168.0.41 ist erreichbar (piggi.home.net)
192.168.0.42 ist erreichbar (fozzy.home.net)
192.168.0.43 ist nicht erreichbar (gonzo.home.net)
192.168.0.44 ist erreichbar (scooter.home.net)
```

Das Skript ist Teil der Übungslösung und ist zusammen mit den übrigen Lösungen zum Abgabetermin per E-Mail zu übersenden. Während der Rücksprache müssen Sie das Skript vorführen.

3.2 Routenverfolgung mit Linux

Sie werden eine sogenannte Routenverfolgung mit `traceroute` durchführen. Zeichnen Sie dazu die von `traceroute` erzeugten Datenpakete mit Hilfe von `wireshark` 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 `wireshark` Interfaces).

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 Linux 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`)



Hinweis –

VNC ist ein Werkzeug für den grafischen Fernzugriff auf Hosts. Um auf einen entfernten Host zuzugreifen gehen Sie wie folgt vor:

- 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 dem `wireshark` zu verbinden.

Übung 3 - Traceroute

- Führen Sie per `traceroute` eine Routenverfolgung zur IP-Adresse von `www.utoronto.ca` aus und protokollieren Sie die von `traceroute` erzeugten Pakete sowie deren Antwort-Pakete in einem Ablaufdiagramm.
- Sichern Sie die mitgeschnittene Datei unter Ihrer Gruppenbezeichnung und machen Sie den Sniffer (`wireshark`) wieder frei.
- Wiederholen Sie den letzten Vorgang und protokollieren Sie mit `wireshark` nun den Netzwerkverkehr im blauen Teil des Testnetzes.

Dokumentieren Sie auf der nächsten Seite den Ablauf der Routenverfolgung in dem zur Verfügung gestellten Ablaufdiagramm. Zu den Paketen der Routenverfolgung sind die folgende Informationen zu dokumentieren:

- die Richtung der Pakete
- die verwendeten Protokolle der Schichten 2 und 3
- der sogenannten TTL-Count
- der Protokolltyp
- die Ports



Hinweis – Sie werden möglicherweise von der großen Zahl der erzeugten Pakete überrascht sein und sich fragen, ob Sie tatsächlich alle diese Pakete in einem Ablaufdiagramm darstellen sollen. Vor der Klärung dieser Frage analysieren Sie bitte, wie eine Routenverfolgung im Detail abläuft. Überlegen Sie bitte anschließend, ob und wie Sie ggf. die Anzahl der erzeugten Pakete beeinflussen können.

Übung 3 - Traceroute

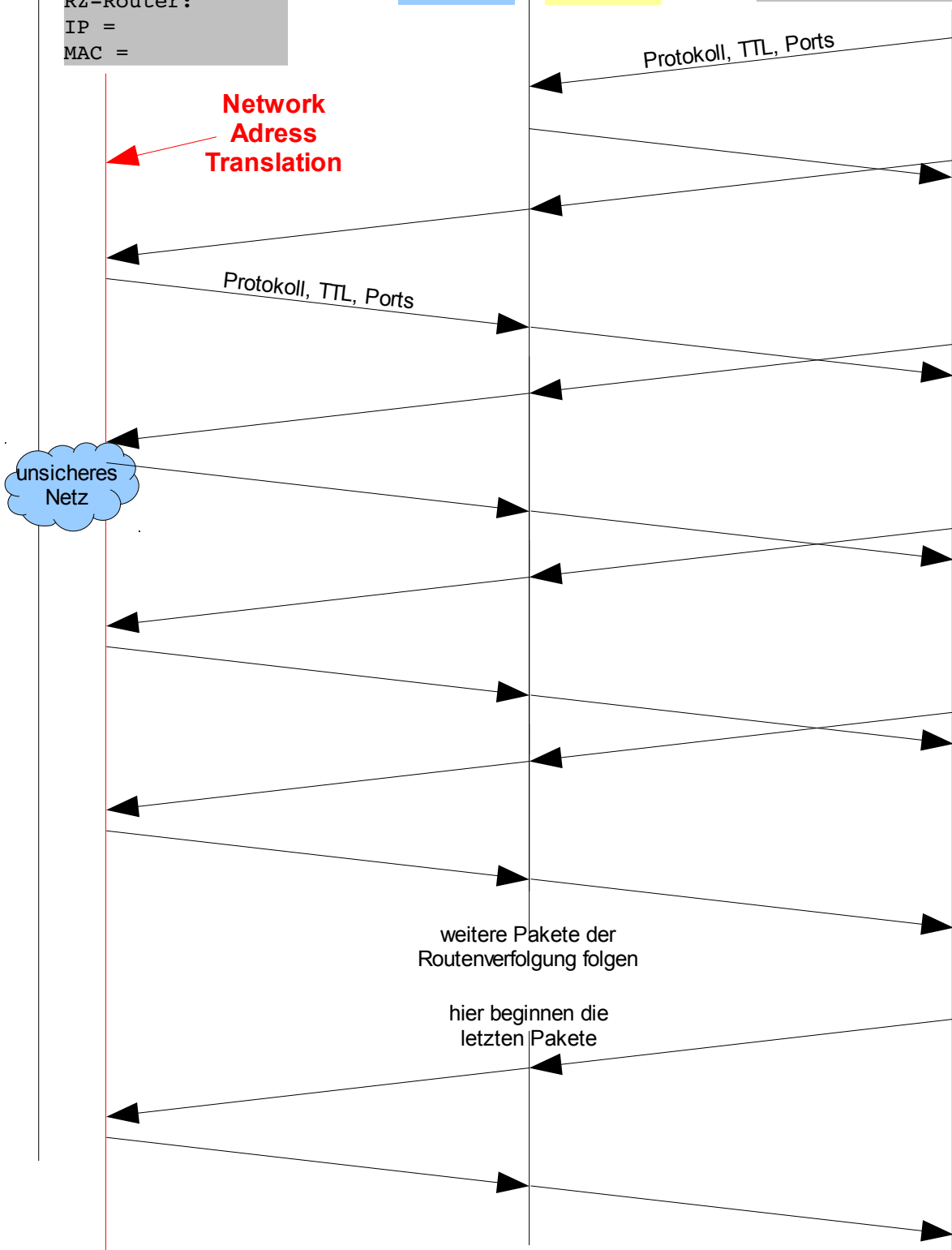
University Toronto
IP =

Knoten:
IP =
MAC =

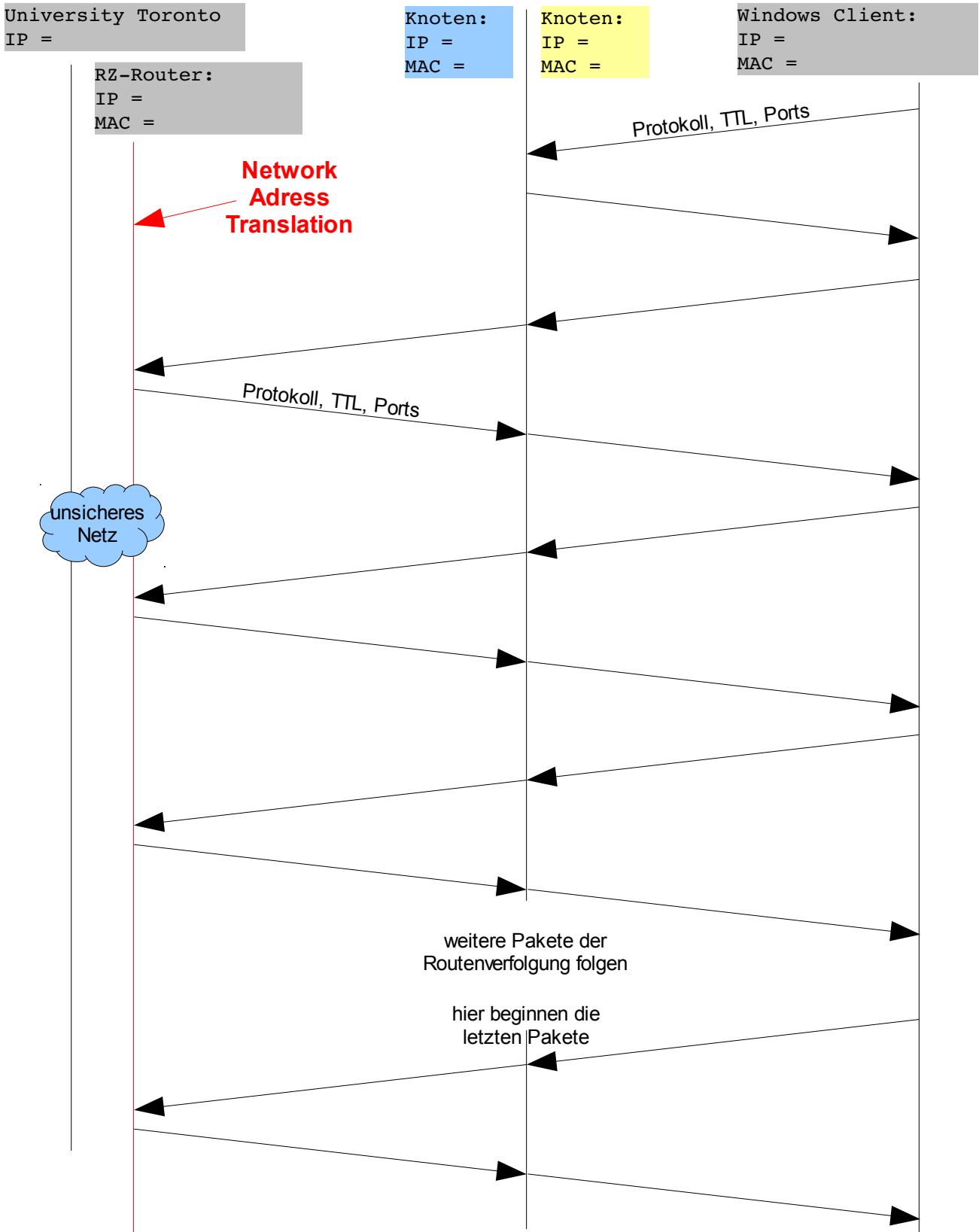
Knoten:
IP =
MAC =

Linux Client:
IP =
MAC =

RZ-Router:
IP =
MAC =



Übung 3 - Traceroute



Übung 3 - Traceroute

3.3 Netzwerkanalyse mit MS Windows

Verbinden Sie sich per vnc mit den MS Windows Systemen `wolfram` oder `wismut`. Führen Sie nun bitte die gleichen Schritte aus dem Abschnitt 3.2 aus, bearbeiten Sie die dort gestellten Fragestellungen für eine Routenverfolgung von einem der MS Windows Systeme und dokumentieren Sie die Routenverfolgung im Ablauf für Windows Systeme.

3.4 Unterschiede bei der Netzwerkanalyse mit Linux und MS Windows

Bitte beantworten Sie nun noch die folgenden Fragen.

- In welcher Protokolleigenschaft unterscheiden sich die Versionen des Werkzeuges zur Routenverfolgung auf MS Windows (`tracert`) und Linuxsystemen (`traceroute`)?
- Beschreiben Sie die Funktion der TTL bei der Routenverfolgung.
- Welche Funktion hat die TTL während einer „normalen“ Datenübertragung innerhalb von IP-Paketen? Wo finden Sie solche „normalen“ Pakete in Ihren Ablaufdiagrammen? Welchen Startwert besitzt die TTL bei solchen IP-Paketen?

3.5 allgemeine Routenverfolgung

Starten Sie eine Routenverfolgung zu `137.229.9.250`

- Sie erhalten für jeden Knoten mehrere unterschiedliche Zeitangaben. Von welcher Laufzeit Angabe für die Gesamtstrecke gehen Sie aus? Warum?
- Welchen Weg legt das Signal zum Ziel zurück. Gehen Sie von einer Signalausbreitung von $7,5 \text{ ns/m}$ aus.
- Wem gehört diese IP?

3.6 Verfeinern der Sicht auf die Routenverfolgung

Starten Sie eine Routenverfolgung von Ihrer Sun zum DNS-Server im blauen Netz und bearbeiten Sie die folgenden Fragestellungen.

- Was bedeuten die 3 Zeiten in jeder Zeile?
- Dokumentieren Sie die Pakete, die `traceroute` für die Routenverfolgung erzeugt in dem Ablaufdiagramm auf der nächsten Seite.
- Vergleichen Sie den Ablauf mit den ersten beiden Ablaufdiagrammen. Was wird in diesem Diagramm dargestellt, was Sie in den ersten Diagrammen nicht darstellen konnten?

Übung 3 - Traceroute

