

Praktikumsblatt 1 - Netze

- Laboreinführung und Netzwerktools -

Herzlich Willkommen zum Praktikum Netze!

In den Übungen haben Sie bislang Aufgaben theoretisch gelöst, im Praktikum arbeiten Sie nun praktisch. Machen Sie sich bitte Notizen zu Ihren Lösungen und zu den nachfolgenden Besprechungen. Denn es wird keine Musterlösung zu den Praktikas geben.

Bevor Sie jedoch mit dem Praktikumsblatt beginnen einige Hinweise zur Laborumgebung.

- (a) Auf den Laborrechner ist das Linux Ubuntu 24.04 installiert. Starten Sie den Rechner und loggen Sie sich mit dem folgenden Account ein:
Benutzername: netlab
Passwort: netlab
- (b) Im Laufe des Praktikums werden Sie hauptsächlich mit dem Terminal (auch Konsole genannt) arbeiten. Starten Sie testweise das Terminal auf Ihrem Laborrechner und geben Sie den Linux-Befehl `whoami` ein.
Alle im Praktikum zu verwendeten Linux-Befehle werden Ihnen auf den Praktikumsblätter mitgeteilt.
- (c) Nutzen Sie während des Praktikums auch Ihren eigenen Rechner. Im Laufe des Semesters bekommen Sie immer wieder Aufgaben, die Sie auf Ihrem Rechner und in Ihrer Netzwerkumgebung zu Hause ausführen sollen.
- (d) Für den ersten Start steht für Sie auf LEA eine Auflistung von Netzwerkbefehlen für die Betriebssysteme Linux, Windows und macOS zur Verfügung (pdf-File „Netzwerkbefehle-Praktikum-Netze“;
<https://lea.hochschule-bonn-rhein-sieg.de/goto.php/file/1791537/download>
- (e) Um vollständig auf die Laborumgebung zugreifen zu können, assoziieren Sie sich mit Ihrem Notebook mit dem Labor-WLAN „C055“ (siehe Aushang Schrank).

Aufgabe 1: Netzwerktool ping

Das Programm `ping` ist ein nützliches und einfaches Netzwerk-Tool. Mit diesem kann unter anderem festgestellt werden, ob ein bestimmter Rechner im Netzwerk erreichbar ist. Dazu sendet der Rechner Daten an einen anderen Rechner im Netzwerk und wartet auf eine Antwort. Ping verwendet hierzu das Protokoll ICMP (Internet Control Message Protocol).

- (a) Auf welcher OSI-Schicht befindet sich das Protokoll ICMP?



- (b) Überprüfen Sie, ob der Rechner mit der IPv4-Adresse 194.95.66.105 zu erreichen ist. Geben Sie im Terminal folgenden Befehl ein:

```
ping 194.95.66.105
```

Hinweis: Unter Linux beenden Sie den ping-Befehl mit <Strg><c>.

- (c) Was bekommen Sie als ping-Antwort angezeigt? Beschreiben Sie die einzelnen ausgegebenen Informationen?

- (d) Recherchieren Sie, was eine `ttl` ist? Welche Funktion hat sie im Internet?

- (e) Mit `time` gibt ping eine Zeit an.

- Um welche Zeit handelt es sich hier genau?
- Welche Möglichkeiten (Methoden) gibt es, diese Zeit zu messen?
- Wofür dienen Messungen in Netzen bzw. Internet?
- Handelt es bei Ihnen ausgegebenen `time`-Wert um eine gute Zeit?
- Pingen Sie einen weit entfernten Rechner (z.B. USA, China) an und vergleichen Sie den `time`-Wert mit dem `time`-Wert aus b).

- (f) Weitere Möglichkeiten zu ping können Sie über die Manpages abrufen. Geben Sie hierzu den Befehl

```
man ping
```

in die Konsole ein. Probieren Sie mal

```
ping -c 3 194.95.66.105
```

Was bewirkt die Option `c`?

Hinweis: Die Manpages beenden Sie mit `q` (für quit).

- (g) Führen Sie einen ping von Ihrem eigenen Notebook auf den Rechner mit der IPv4-Adresse 194.95.66.105 aus. Gibt es Unterschiede bei der Ausgabe?

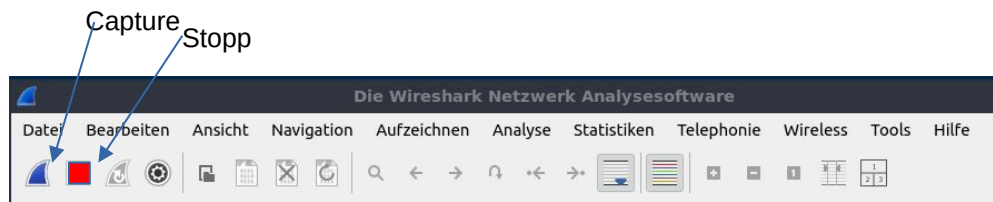
Aufgabe 2: Protokollanalyse

Um die Kommunikationsvorgänge im Netz sichtbar zu machen, ist ein Protokollanalysator unverzichtbar. Im Praktikum Netze setzen wir den Analysator "Wireshark" ein. Wireshark ist eine frei verfügbare Software und kann unter <http://www.wireshark.org/download.html> herunter geladen werden. Die zugehörige Online-Dokumentation finden Sie unter <http://www.wireshark.org/docs/>.



Starten Sie das auf dem Desktop befindlichen Programm „Wireshark“.

- a) Starten Sie die Capture-Funktion (Aufzeichnung) in dem Sie das Netzwerk-Interface `eth0` auswählen und in der Menüleiste auf das Shark-Symbol klicken. Führen Sie nun wie unter Aufgabe 1b) einen ping auf den Rechner mit der IP-Adresse 194.95.66.105 aus. Stoppen Sie anschließend die Aufzeichnung und den ping.



- b) Suchen Sie aus Ihrem Mitschnitt ein ping-Paket heraus und markieren es. Machen Sie sich mit der Kommunikationsdarstellung in den drei Fenstern von Wireshark vertraut.
- c) Welche Informationen (Bedeutung) zu dem ping-Paket bekommen Sie in dem oberen Wireshark-Fenster angezeigt?

No.

Time

Source

Destination

Protocol

Length

Info



- d) In dem unteren linken Wireshark-Fenster werden die Protokolle nach OSI-Schichten für die jeweiligen Pakete aufgeführt. Im Falle von „ping“ sind das die Protokolle Ethernet, IPv4 und ICMP.

Wenn Sie nun auf das Tag- (>) Symbol vor den Protokollen klicken, bekommen Sie den Header der Protokolle angezeigt. Schauen Sie sich den Ethernet-Header:

- Auf welcher OSI-Schicht befindet sich das Ethernet-Protokoll?
- Wie nennt man die beim Ethernet verwendeten Adressen?
- Was bedeutet „GigaByteTech“ oder „MellanoxTech“ in den Adressen?
- Handelt sich bei den Adressen um eine Unicast-, Multicast- oder Broadcast-Adresse? Decodieren Sie hierzu das I/G-Bit der Adresse (siehe Vorlesung „Ethernet und WLAN“)

- e) Öffnen Sie nun das ICMP-Protokoll. Neben dem ICMP-Header gibt es hier auch eine Payload, Data (40 bytes), die Sie im 3. Wireshark-Fenster decodiert bekommen. Was sind das für Daten, die hierbei gesendet werden?

- f) Wie beurteilen Sie die Privacy bei der Nutzung von Wireshark? Was müssen Sie beachten, wenn Sie Wireshark z.B. in einem Unternehmensnetz einsetzen?

- g) Damit Sie unter der Vielzahl von Paketen diejenigen auffinden, die Sie interessieren, sollten Sie geeignete Filter setzen können. Machen Sie sich dafür mit den Display-Filter vertraut: <https://wiki.wireshark.org/DisplayFilters>

- h) Welchen Display(Anzeige-)-Filter müssen Sie setzen, damit Sie nur

- TCP-Pakete

.....

- Pakete mit einer bestimmten IP-Adresse

.....

- Pakete mit einer bestimmten MAC-Adresse

.....

- TCP-Pakete mit einer bestimmten Adresse



.....

dargestellt bekommen?

Hinweis: Im weiteren Verlauf des Praktikums werden Sie immer wieder bestimmte Kommunikationsverläufe aufzeichnen, die dann anschließend genau analysiert werden. Zur Nachvollziehbarkeit ist es sinnvoll, dass Sie sich die jeweiligen Capture-Files oder Screens davon sichern (nicht auf den Laborrechnern, da diese durch Image-Synchronisierungen überschrieben werden).

Aufgabe 3

Installieren Sie Wireshark (<http://www.wireshark.org/download.html>) auf Ihren Rechner und starten Sie ein Test-Capture in Ihrem Netz zu Hause. Was gilt es hierbei zu beachten? Sollten Sie mit dem Praktikumsblatt nicht fertig geworden sein, führen Sie die verbliebenen Aufgaben und zugehörige Dokumentation zu Hause fort.

Viel Spaß und Erfolg!