Hochschule Fulda
University of Applied Sciences

Kommunikationsnetze und -protokolle

Praxis Übung 1

Max Göb, Michael Antoni, Christoph Hardegen, Prof. Dr. Sebastian Rieger

Lernziele

- Kommunikation in Netzwerken analysieren
- Nachvollziehen der Kommunikation beim Aufruf einer Webseite
- Festigung der Kenntnis des ISO/OSI 7 Schichten Modells
- Differenzierung von verbindungsorientierter und -loser Kommunikation

Zeitliche Planung der Bearbeitung des Übungsblatts:

Aufgaben 1-3: 1. Übungssitzung (Übung 1a)

Aufgaben 4-6: 2. Übungssitzung (Übung 1b)

Aufgabe 7: 3. Übungssitzung (Übung 1c)

Aufgabe 1: Analyse von Netzwerkverkehr

1.1 Was ist ein Sniffer und wozu wird er eingesetzt?

1.2 Recherchieren Sie, was man unter Mirror Ports von Switches versteht.

1.3 Problemstellung: Sie möchten einen Netzwerkport mit einer Datenrate von 100 Mbit/s (duplex) überwachen. Welche Datenrate benötigt der Mirror Port, an dem Sie angeschlossen sind? Welche Datenrate benötigt er mindestens wenn Sie 5 Ports mit jeweils 100 Mbit/s duplex überwachen möchten?

Aufgabe 2: Wireshark als Sniffer

2.1 Starten Sie Wireshark und sehen Sie sich die Capture Options an. Was ist ein Interface?

2.2 Wählen Sie das Interface aus, über das Ihre Verbindung zum Labornetzwerk besteht, und starten sie den Capture Vorgang (Trace).

2.3 Öffnen Sie in einem beliebigen Browser die Webseite

http://kommprothttp.informatik.hs-fulda.de/

Alternativ können Sie auch andere Seiten, die noch mit HTTP (nicht HTTPS) funktionieren verwenden. Z.B.: http://www.neverssl.com

2.4 Stoppen Sie den Trace und machen Sie sich mit der Oberfläche von Wireshark vertraut. Welche Bereiche bietet das Wireshark Fenster in dem der Trace angezeigt wird und welche Art von Informationen werden dort angezeigt?

2.5 Welchen Vorteil bieten Display-Filter (vgl. auch Aufzeichnung der Vorlesung) im Vergleich zu Capture Filtern? Testen Sie Filtereinstellungen indem Sie z.B. nach den Protokollen `dns`, `http`, `tcp`, `udp` und `ip` filtern.

2.6 Identifizieren Sie innerhalb der Traces die Quell- und Zieladresse in den Header-Informationen von IPv4.

2.7 Überlegen Sie, welche (legalen und illegalen) Konsequenzen durch diese Transparenz entstehen. Welche technischen Herausforderungen stellen sich beim Sniffen? Diskutieren Sie mögliche Abwehrmaßnahmen.

Aufgabe 3: Adressierung im Internet

3.1 Wie ist das Internet aufgebaut? Welche Netzkomponente koppelt individuelle Teilnetze und wie werden Systeme adressiert?

3.2 Warum werden im Internet, beispielsweise bei dem Zugriff von Webseiten, keine IP-Adressen, sondern Namen, wie z.B. *hs-fulda.de*, verwendet?

3.3 Ermitteln Sie die IP-Adresse des Webservers, auf dem die Webseite http://www.hs-fulda.de bereitgestellt wird. Verwenden Sie dazu das Konsolenprogramm `nslookup`. Über `nslookup -?` bekommen sie eine Hilfestellung zu den Übergabeparameter.

3.4 Sie bekommen bei einer erfolgreichen Namensauflösung mehrere IP-Adressen von `nslookup` angezeigt. Warum? Um welche Adressen könnte es sich hierbei handeln?

Führen Sie das Konsolenprogramm `ipconfig /all` aus und prüfen Sie, ob Sie eine der zwei IP-Adressen zuordnen können.

3.5 Wenn sie die IP-Adresse des Webservers ermittelt haben, dann rufen sie die Webseite in Ihrem Browser über `http://<IPADRESSE des Web-Servers> ab`.

3.6 Wiederholen Sie den Vorgang mit den Webseiten www.heise.de und www.fulda.de oder www.alsfeld.de. Ermitteln Sie mittels `nslookup` die IP-Adresse des Webservers und rufen Sie die Seite mittels `http://<IPADRESSE des Web-Servers>` auf.

3.7 Recherchieren Sie, worum es sich bei dem HTTP Host Header handelt. Spezifizieren Sie die Filtereinstellung von Wireshark auf den folgenden Ausdruck mit: `http.host == kommprothttp.informatik.hs-fulda.de`. Suchen Sie den Host in den Informationen des Hypertext Transfer Protocols beim Zugriff auf http://kommprothttp.informatik.hs-fulda.de/.

Aufgabe 4: Hostnamen im DNS

4.1 Wie ist der DNS-Namensraum aufgebaut? Wie werden DNS-Informationen verwaltet?

4.2 Welche Strategien zur Auflösung von Hostnamen sind Ihnen bekannt? Skizzieren Sie den jeweiligen Ablauf.

4.3 Verwenden Sie das Konsolenprogramm `nslookup` um sowohl einen Forward (A-Record) als auch Reverse Lookup (PTR-Record) für www.fulda.de durchzuführen. Mittels `-q=any` oder `-q=all` erhalten Sie auch noch weitere Record-Typen, die in der Lehrveranstaltung genannt werden, z.B. beim Aufruf mit `nslookup -q=all hs-fulda.de` oder für `heise.de`. Recherchieren Sie welche Aufgabe MX (`-q=mx`) und NS (`-q=ns`) Records übernehmen.

Aufgabe 5: Adressierung mit DHCP

5.1 Welche Aufgabe übernimmt das Anwendungsprotokoll DHCP in Netzen?

5.2 Verwenden Sie Wireshark, um sich die automatische Netzkonfiguration eines Rechners anhand der ausgetauschten Nachrichten anzuschauen. Unter Windows können Sie mittels `ipconfig /renew` eine erneute Kommunikation mit dem DHCP-Server initiieren, während Wireshark die Kommunikation mitschneidet. Welche Konfigurationsparameter werden vergeben? Noch besser ist `ipconfig /release` zuvor zu verwenden, aber **ACHTUNG:** Dann wird ihr Rechner kurz vom Netz getrennt, da er bis zum erfolgreichen `ipconfig /renew` keine IP-Adresse mehr hat.

Aufgabe 6: Übertragung von Traces auf das ISO/OSI Referenzmodell

Wo sehen Sie in Wireshark die Schichten des TCP/IP-Modells? Wie können Sie dort deren Aufgaben erkennen?

Vervollständigen Sie die folgende Tabelle mit Hilfe der Traces. Tragen Sie nur Protokolle ein, die für den Aufruf einer Webseite verwendet wurden.

ISO/OSI Modell	TCP/IP Modell	Protokolle

Aufgabe 7: Verbindungslose und verbindungsorientierte Kommunikationen

Um die mit [x] gekennzeichneten Aufgaben bearbeiten zu können, müssen Sie als Gruppe unseren learn-sdn-hub benutzten. Bitte wählen Sie sich dafür in Moodle in eine Gruppe ein, die aus max. 4 Studierenden bestehen darf. Der Ablauf ist wie folgt:

1. Öffnen Sie in Ihrem Browser folgende Webseite: https://prona.informatik.hs-fulda.de/ (von zu Hause müssen Sie hierfür zunächst ins VPN der Hochschule)
2. Verwenden Sie als Username den Namen Ihrer Gruppe und als Passwort „kommprot“. Sie können das Passwort anschließend unter Einstellungen ändern.

Starten Sie für den dritten Teil unserer Übung (1c) „KommProt-Uebung1c“.

7.1 Was sind die Unterschiede zwischen einer verbindungslosen und verbindungsorientierten Kommunikation? Welche Funktionen werden in beiden Fällen erbracht?

7.2 Welche Transportprotokolle existieren zur Unterstützung beider Kommunikationsformen? Identifizieren Sie Anwendungsprotokolle, die eine verbindungslose/ verbindungsorientierte Kommunikation unterstützen bzw. erfordern. Welche Gründe sprechen jeweils für eine verbindungslose und/oder verbindungsorientierte Lösung?

7.3 [x] Machen Sie sich mit den Terminals der in learn-sdn-hub gestarteten Umgebung vertraut. Nehmen Sie sich hierfür das **CheatSheet** zur Hilfe.

Welche IPs haben die beiden Container der beiden Terminals HOST1 und HOST2? Sind die beiden Terminals untereinander erreichbar? Lassen Sie sich mit traceroute oder mtr die Route zu einer beliebigen Internetseite anzeigen (z.B. google.de).

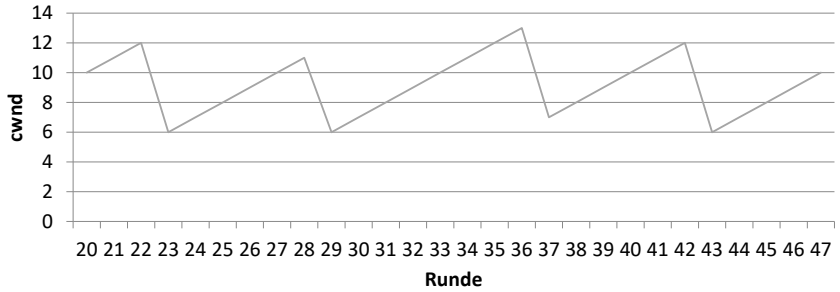
7.4 [x] Führen Sie einen iperf3 Speedtest mit TCP zwischen den beiden Terminals durch, starten Sie dafür auf einem Terminal den Server und auf dem anderen den Client. Welche Datenmenge wird bei dem Speedtest transferiert und welche Bandbreite resultiert daraus?

7.5 [x] Führen sie den iperf3 Speedtest mit UDP durch. Warum kann man bei iperf3 mit UDP nicht einfach die aktuell maximal mögliche Übertragungsrate ermitteln und muss stattdessen eine Rate vorgeben?

7.6 Wie wird die Staukontrolle bei verbindungsorientierten Transportprotokollen (TCP) unterstützt? Betrachten Sie dabei sowohl den Tahoe als auch Reno Algorithmus, indem Sie den jeweiligen Verlauf skizzieren und dabei die ablaufenden Phasen sowie zugehörige Ereignisse und Schwellwerte kennzeichnen.

7.7 Was versteht man unter der Latenz bzw. Round Trip Time (RTT) bei einer Kommunikation? Welche Faktoren haben Einfluss auf die Latenz bzw. RTT?

7.8 Welchen Einfluss hat die RTT auf die Staukontrolle bei verbindungsorientierten Transportprotokollen (TCP)? Welche Übertragungsrate entsteht im folgenden Bild in Runde 29 bei einer RTT von 100 ms und einer MSS von 1460 Bytes?



$$Rate[Byte/s] = \frac{MSS[Bytes]}{RTT[s]}$$

7.9 [x] Clonen Sie sich in beiden Terminals folgendes Git Repository:

git clone https://github.com/prona-p4-learning-platform/SpeedtestClientServerExample.git

Wechseln Sie in das Verzeichnis und betrachten Sie mit einem Editor (z.B. nano) die Socket-Implementierung von Client1/Server1 und Client2/Server2 und vollziehen Sie deren grobe Funktionsweise und Unterschiede nach.

7.10 [x] Können Sie erkennen, welcher Client und Server ein verbindungsloses oder verbindungsorientiertes Transportprotokoll verwendet? Dokumentieren Sie die notwendigen Operationen in Form eines Ablaufdiagramms.

7.11 [x] Kompilieren und starten Sie in einem Terminal den Server und in dem anderen Terminal den zugehörigen Client um mit dem Server zu kommunizieren. Identifizieren Sie am Server aufgebaute TCP-Verbindungen mit Hilfe des Konsolenprogramms `netstat` (oder, wie in der Vorlesung, mit dem neueren Befehl: `ss`). *(Hinweis: Damit Sie die*

*Shell nicht mit dem Server blockiert starten, können Sie den Prozess in Hintergrund setzen, in dem Sie am Ende des Befehles ein **&** schreiben. Den Befehl können Sie dann mit **killall java** beenden.)*