Übungszettel 10 Ruth und Maria, Abgabe am 14.07.20

Aufgabe 1: Transportschicht

Geben Sie ggf. Ihre genutzten Quellen an.

1. TCP vs. UDP; IP-basierte Protokolle

Erläutern Sie den Unterschied zwischen TCP und UDP.
Welche anderen IP-basierten Protokolle gibt es?

Antwort:
Generell dienen die Transportprotokolle UDP (User Datagram Protocol) und TCP (Transmission Control Protocol) für eine sog. Ende-zu-Ende-Kommunikation. Dabei werden Daten nicht zwischen Rechnern, sondern über ein Socket Pair zwischen Prozessen virtuell übertragen. Dies geschieht transparent und unabhängig von der darunter liegenden Technologie. Beide laufen zwar über das unzuverlässige IP, aber Fehler von IP wie z.B. Datenpaketverlust können auf der OSI-Schicht 4 behoben werden.

Das UDP ist ein ganz einfaches verbindungsloses Transportprotokoll. Es ist ein unzuverlässiges Datagramm-Protokoll und stellt damit nicht sicher, dass die Daten wirklich beim Empfänger ankommen. Aber es de-/multiplext die Datenströme, die bspw. auf der IP-Schicht eingehen, in Richtung der Prozesse. Zudem können in UDP Prüfsummen (auch im IP-Kopf) berechnet werden. Bildlich vergleichbar ist UDP mit einer Postkarte.

Das TCP ist das vorherrschende Protokoll im Internet. Es baut eine Verbindung auf und gewährleistet im Zuge dessen eine zuverlässige Datenübertragung zwischen zwei Prozessen. Bis hierhin wäre das ältere, klassische Telefon ein passender Alltagsvergleich. Darüber hinaus verwendet TCP ein Drei-Wege-Handschlag (three-way handshake), wobei aus Effizienzgründen bei der dritten Nachricht bereits Daten im Huckepack (piggy backing) mitgeschickt werden können.

Weitere auf IP aufsitzende Transportprotokolle sind SCTP (Stream Control Transmission Protocol, arbeitet verbindungsorientiert, zuverlässig) und DCCP (Datagram Congestion Control Protocol, arbeitet verbindungslos, unzuverlässig). Daneben gibt es noch folgende anwendungsorientierte Protokolle, die im Kontext von Internet verwendet werden:
• http (Protokoll, um auf www zuzugreifen)
• ftp (Protokoll, um Dateien zwischen zwei Rechnern zu senden)
• Telnet (Protokoll zur Dateiübertragung zw. Client und Server, z.B. um auf eine Datenbank zuzugreifen)

2. Manipulation von Time to Live (TLL)

Was passiert, wenn ein Paket mit einer TTL abgesendet wird, die nicht ausreicht, um das Ziel zu erreichen? Was für Fehlerinformationen bekommen wir und wie? Angenommen wir senden bspw. UDP-Pakete zu einem Ziel los, und fangen dabei mit einer TTL von eins an. Wenn das Paket nicht ankommt, senden wir nochmal mit einer höheren TTL – bis das Paket ankommt. Warum könnte man das machen wollen außer um schlicht herauszufinden wie „weit“ es zum Ziel ist?

Antwort:
Die TLL eines Datenpakets ist beim IP die “verbleibende maximale Lebenszeit im Netzwerk in Sekunden”. Die letzte Station des Datenpakets sendet an den Sender die “ICMP-Antwort Typ 11: Time exceeded mit Code 0: Time to live exceeded in transit”. Praktisch entspricht der TLL-Wert auch der Anzahl der passierten Zwischenstationen (Hops) wie z.B. einem Router oder einer Firewall, welche im Durchlauf mindestens um 1 reduziert wird. Diese Eigenschaft wird bspw. auf das Verfahren “Programm Traceroute” angewendet. Mit Traceroute ist feststellbar, welche Router das Paket auf dem Weg zu seinem Ziel durchläuft. Somit können Umwege oder ausgefallene Router identifiziert werden.

3. Verbindungsauf/-abbau bei TCP, three-way-handshake, SYN & FIN
Wie sieht ein typischer Verbindungsauf- und -abbau bei TCP aus? Warum gibt es einen Handshake „in beide Richtungen“? Was soll ein SYN signalisieren, was FIN?

Antwort:
Verbindungsaufbau:
Gegeben sei ein Host A und ein Host B. Zum Verbindungsaufbau wird ein sog. Drei-Wege-Handschlag (three-way handshake) gemacht. Dabei steht SYN für Synchronize und ACK für Acknowledge. Das SYN-Paket ist der Verbindungsaufbau-Wunsch von A. Schickt A dieses SYN-Paket, antwortet B daraufhin mit einem SYN-ACK-Paket als Bestätigung dafür, dass die Verbindung angekommen ist und akzeptiert wird. Im dritten Schritt schickt A das ACK-Paket zurück an B, welches schon mit Daten kombiniert werden kann.

Beim Verbindungsaufbau werden Ressourcen eines Speicherbereichs gebunden, welche erst nach einer bestimmten Zeit wieder freigegeben werden. Bei zu lange eingefrorenen Ressourcen kann es bei zu vielen SYN-Verbindungsanfragen zu einer sog. denial-of-service-attack (DoS) - einem Angriff auf die Dienstverfügbarkeit - kommen.

Grund für three-way-handshake:
In realistischen Netzen auf Schicht 3 können Daten verloren gehen, umsortiert und dupliziert werden. Generell reicht eine Bestätigung des Empfängers nicht aus, sondern der Initiator des Verbindungsauf- oder abbaus schickt eine weitere Bestätigungsnachricht zurück. Mit dem three-way handshake wissen beide Seiten garantiert, dass die Verbindung steht. Zusammengefasst sorgt der three-way-handshake also für einen gemeinsamen Kontext respektive eine gemeinsame Sichtweise zwischen Sender und Empfänger auf eine Verbindung.

Zusätzlich kommen sog. Sequenznummern zum Einsatz. D.h. der Verbindungsvorgang ist nicht lediglich ein gegenseitiges Akzeptieren, sondern teilt gleich mit, welche Nummern die Daten haben, die gerade gesendet werden. Somit kann in TCP jedes nummerierte Byte identifiziert werden und damit auch Duplikate aufgedeckt werden. Sequenznummern sind in diesem Sinn auch wichtig, um bereits empfangene Datenpakete zu bestätigen.

Verbindungsabbau:
Auch beim Abbau der Verbindung soll mit einem three-way handshake sichergestellt werden, dass beide Seiten einen konsistenten Zustand haben. A möchte eine Verbindung abbauen, teilt das B mit, welcher bestätigt, die Verbindung auch abzubauen. Letztere Bestätigung kann aber unterwegs verloren gehen. Auch eine darauf folgende Bestätigung von A kann unterwegs verloren gehen. Dieses unlösbare Problem, dass nie ein garantierter koordinierbarer Verbindungsabbau mit dem unzuverlässigen Datenaustausch bestätigt werden kann, wird als

“Two Army Problem” bezeichnet. In der Praxis werden hier einfach Risiken eingegangen. A schickt ein Disconnect Request (DR) und nutzt zusätzlich ein Timer. Das Paket für den Verbindungsabbruch lautet “FIN”. B schickt mit starten eines Timers eine Verbindungsabbau-Anfrage und -Bestätigung FIN/ACK zurück, woraufhin A ein ACK an B sendet. Sollte hierbei ein ACK bei B nicht ankommen, wird mithilfe der Timeouts bei A und B nach einer bestimmten Zeit davon ausgegangen, dass die Verbindung abgebaut ist. Die Verbindung ist frühestens nach dem letzten ACK und spätestens nach dem Timeout geschlossen.

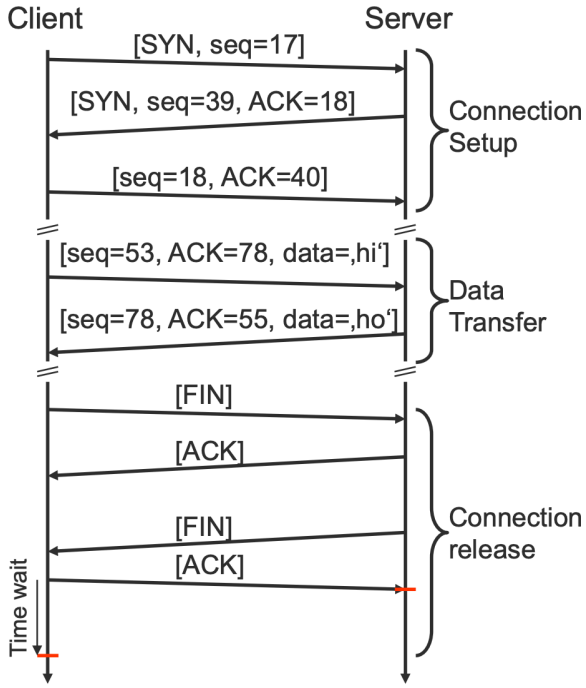

Abb. Verbindungsaufbau, Datenübertragung Verbindungsabbau in TCP

4. Flow Control

Angenommen Sie wollen sich von der KVV-Seite den neuesten Übungsbogen herunterladen und verfolgen zeitgleich einen Livestream. Weiterhin bestehen keinerlei technische Probleme in Ihrer Verbindung zum FU-Server. Wie kann es dennoch passieren, dass Sie den Übungsbogen nicht von der KVV-Seite herunterladen können?

Antwort:

Es kann sein, dass bei zu viel Traffic das Datenpaket unterwegs vom Sender aus verloren gegangen ist, aber da wir davon ausgehen, dass keine technischen Probleme bestehen, ist wahrscheinlich der Puffer des Empfängers voll. Damit bezieht sich der vorliegende Fall nicht auf einen error control, sondern auf einen fehlerhaften flow control.
Hier sind wegen des Livestreams noch zu viele Daten vom Sender zum Empfänger (Begriff der “ausstehenden Pakete“/ „outstanding pakets”) unterwegs. Diese Pakete “im Fluge” kann der Empfänger noch nicht bestätigt haben. Es besteht nicht genügend Pufferplatz und somit können die ankommenden Daten nicht mehr im Speicher abgelegt werden. Die Folge von dieser fehlerhaften Flusssteuerung (Buffer Allocation) ist, dass der Empfänger überlastet ist und folglich die Datenrate reduziert. Hinzu kommt, dass der Livestream wahrscheinlich über UDP läuft und der Übungsbogen der KVV-Seite über TCP. TCP hat die Eigenschaft, dass es sich zurückhaltend (sog. Exponential backoff) und fair (teilt sich die verfügbare Datenrate fair auf) verhält. Hingegen hat UDP nicht die “congestion control” (Staukontrolle) eingebaut,

sodass UDP TCP leicht zurückdrängen kann. Damit weicht TCP zurück und die UDP-Pakete kommen durch. Deswegen drosseln heutzutage Router im Internet den UDP-Verkehr automatisch, weil ansonsten andere Datenübertragungen wie hier nicht mehr funktionieren. Und es werden auch neue Protokolle TCP-friendly entwickelt, d.h. sie sollten in einer Stausituation nicht mehr Datenrate benötigen als eine vergleichbare TCP-Verbindung. Einen solchen Mechanismus hat z.B. DCCP (Datagram Congestion Control Protocol) eingebaut.

5. Anwendung von UDP und TCP und Begründung für jene Anwendung
Nennen Sie sowohl für UDP als auch TCP je mindestens zwei Beispielanwendungen, die dieses Protokoll verwenden. Begründen Sie, warum dies für diese Anwendung sinnvoll ist.

Antwort:
UDP wird meistens für DNS-Anfragen, VPN-Verbindungen und Audio-/ Video-Streaming benutzt. Der Grund hierfür ist, dass eine kontinuierliche Datenübertragung gewährleistet werden soll und damit Echtzeit-Verbindungen unterstützt. Ein zeitweiser Verlust von Datenpaketen beim UDP ist hinnehmbar, aber größere Unterbrechungen wie beim TCP-Verbindungsaufbau werden den obigen Anwendungen nicht gerecht.

Für Telnet, E-Mail oder WWW wird TCP verwendet. Der Grund hierfür ist, dass bei dieser Ende-zu-Ende-Kommunikation im Internet eine zuverlässige Datenübertragung in beide Richtungen wichtig ist.

Quellen:

- Vorlesung 11 Transport
- SMTP, SFTP SPX, DHCP, IP oder UDP, Ratgeber: Was ist was bei den Netzwerkprotokollen: https://www.tecchannel.de/a/ratgeber-was-ist-was-bei-den-netzwerkprotokollen,2038150 (Stand: 13.07.20)
- Wiki: Liste von TCP/IP-basierten Netzwerkdiensten: https://de.wikipedia.org/wiki/Liste_von_TCP/IP-basierten_Netzwerkdiensten (Stand: 13.07.20)
- Wiki: Internetprotokolle: https://de.wikipedia.org/wiki/Internetprotokollfamilie (Stand: 13.07.20)
- Wiki: Datagram Congestion Control Protocol: https://de.wikipedia.org/wiki/Datagram_Congestion_Control_Protocol (Stand: 13.07.20)
- Digital Guide Ionos, Was ist Traceroute (tracert)?: https://www.ionos.de/digitalguide/server/tools/mit-traceroute-den-weg-von-datenpaketen-verfolgen/#:~:text=Traceroute%20ist%20ein%20Kommandozeilen%2DTool,letztendlich%20zum%20angepeilten%20Host%20gelangen. (Stand: 13.07.20)
- Wiki: Time to Live: https://de.wikipedia.org/wiki/Time_to_Live (Stand: 13.07.20)
- Elektronik-Kompendium, UDP - User Datagram Protocol: https://www.elektronik-kompendium.de/sites/net/0812281.htm#:%7E:text=UDP%20ist%20ein%20verbindungsloses%20Transport,Aufgabe%2C%20wie%20das%20verbindungsorientierte%20TCP.&text=Typischerweise%20wird%20UDP%20bei%20DNS,%2D%20und%20Video%2DStreaming%20verwendet (Stand: 13.07.20)
- Elektronik-Kompendium, TCP - Transmission Control Protocol: https://www.elektronik-kompendium.de/sites/net/0812271.htm (Stand: 13.07.20)

- Wiki: Transmission Control Protocol: https://de.wikipedia.org/wiki/Transmission_Control_Protocol (Stand: 13.07.20)