Übungsblatt 4 – Wireshark

Aufgabe A – OSI-Modell & Transport Layer + IP

Da Sie in der kommenden Übung mithilfe *Wiresharks* Ihren Netzwerkverkehr untersuchen sollen, müssen Sie zumindest grundlegend verstanden haben auf welche Protokolle Sie dort stoßen werden.

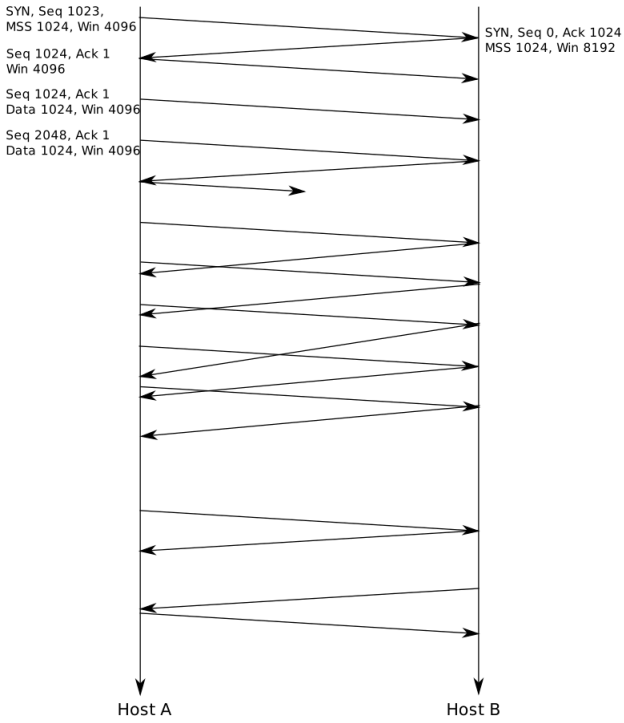
1. Schauen Sie folgendes Video: https://youtu.be/iDCi_CJAyXs (Transport Layer)
2. Recherchieren Sie die Funktion, sowie den Aufbau des *TCP*-Protokolls. https://youtu.be/_WP9be9W3xE
   a) Auf welcher Ebene im OSI-Modell arbeitet *TCP*?
   b) Welche Aufgabe übernimmt das oben genannte Protokoll?
   c) Aus welchen Segmenten besteht ein *TCP*-Datagram?
   d) Zeigen Sie beispielhaft den Aufbau eines *TCP*-Datagram.
3. Recherchieren Sie die Funktion, sowie den Aufbau des *UDP*-Protokolls. https://youtu.be/xWsD6a3KsAI
   a) Auf welcher Ebene im OSI-Modell arbeitet *UDP*?
   b) Welche Aufgabe übernimmt das oben genannte Protokoll?
   c) Aus welchen Segmenten besteht ein *UDP*-Datagram?
   d) Zeigen Sie beispielhaft den Aufbau eines *UDP*-Datagram.
4. Worin unterscheiden sich *TCP* und *UDP* grundlegend?
5. Recherchieren Sie die Funktion, sowie den Aufbau des IP-Protokolls.
   a) Auf welcher Ebene im OSI-Modell arbeitet IP?
   b) Welche Aufgabe übernimmt das oben genannte Protokoll?
   c) Aus welchen Segmenten besteht ein IP-Paket im allgemeinen?
6. Recherchieren Sie die Funktion, sowie den Aufbau von Ethernet (*IEEE 802.3* Protokollfamilie).
   a) Auf welcher Ebene im OSI-Modell arbeitet *Ethernet*?
   b) Welche Aufgabe übernimmt das oben genannte Protokoll?
   c) Aus welchen Segmenten besteht ein Ethernet-Frame?

Aufgabe B – TCP: 3-Way-Handshake

Da TCP ein verbindungsorientiertes Protokoll ist, ist der Aufbau eines Sockets etwas komplizierter. Beide Seiten müssen sichergehen, dass die Verbindung korrekt funktioniert.

1. Recherchieren Sie wie der 3-Way-Handshake bei TCP funktioniert [S. 252f]Kurose2012

2. Gegeben sei Folgendes Sequenzdiagramm einer TCP Verbindung.



   Die horizontalen Pfeile repräsentieren die Zeit. Die Beschriftungen sollen die Header-Felder der TCP-Segmente beschreiben. Eine 3-Way-Handshake wird von Host A initialisiert.

3. Erläutern Sie den Austausch der ersten drei Segmente und Werte der Header-Felder.

4. Host A übermittelt 7 Segmente mit einer Nutzlast (Payload) von 1024 Byte an Host B, anschließend schließt A die Verbindung. Die ersten beiden Segmente samt Nutzdaten sind im Sequenzdiagramm bereits beschriftet. Vervollständigen Sie die restlichen Segmente samt Werte anhand folgender Informationen:

   a) Eines der Segmente ging verloren (signalisiert durch eine Pfeil der nicht die rechte Seite erreicht)

b) Nehmen Sie an, das Host *A* den Fast-Retransmit unterstützt und keine Timeouts durch ein verlorenes Segment auftritt.

Aufgabe C – ICMP

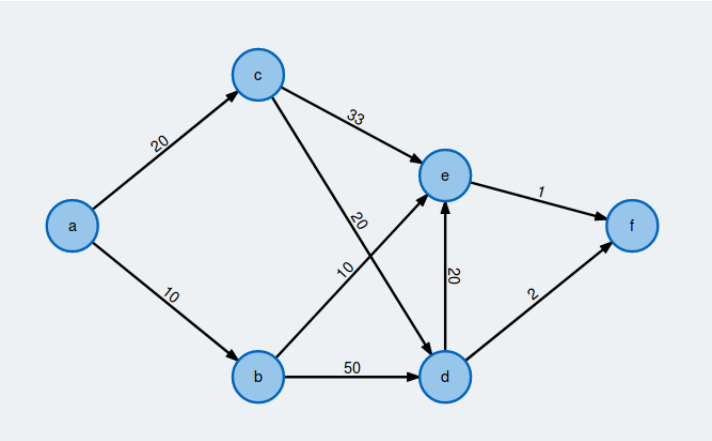
Bevor es zum Thema Routing geht, soll im Folgenden noch das ICM-Protokoll betrachtet werden. Dieses dient in vielen Fällen als Diagnoseprotokoll.

1. Lesen Sie den Abschnitt 4.4.3 zu ICMP [2, S. 353].
2. Was ist die Funktion des Internet Control Message Protocol (ICMP)?
3. ICMP hat verschiedene Message-Codes (einige brauchen wir in den Übungen 4 und 5!). Erläutern Sie was diese Nachrichten kodieren sollen – was ist der Zweck der Message-Codes?
4. Recherchieren Sie welchen Hinweis Ihnen die verschiedenen *ICMP*-Messages geben.
   i) Echo
   ii) Echo Reply

Aufgabe D – Routing

1. Im wesentlichen gibt es zwei fundamentale Routing-Algorithmen. Dies sind das Distanz-Vektor- und Link-State-Routing. Diese ermöglichen es den kürzesten Weg durch einen Graphen zu finden (Shortest-Path-Problem).
   Für gewöhnlich wird für das Distanz-Vektor-Routing der Bellman-Ford-Algorithmus verwandt, das Link-State-Routing nutzt den Dijkstra-Algorithmus. [2, S. 363ff]
   a) Recherchieren Sie wie das Link-State-Routing unter Nutzung des Dijkstra-Algorithmus funktioniert [2, S. 366].
   b) Recherchieren Sie wie das Distanz-Vektor-Routing unter Nutzung des Bellman-Ford-Algorithmus funktioniert [2, S. 371].
   c) In welchen Protokollen finden diese beiden Protokollen Verwendung? Ist diesen Protokollen etwas gemein?
   d) Erläutern Sie die fundamentalen Unterschiede beider Lösungsansätze.
   e) Warum wird keines der beiden Verfahren für das Exterior-Gateway-Protokoll (EGP) genutzt?
   f) Diskutieren Sie ob der Bellman-Ford-Algorithmus für das Link-State-Routing und der Dijkstra-Algorithmus für das Distanz-Vektor-Routing genutzt werden könnte.

2. Gegeben sei folgender Graph:



Finden Sie den kürzesten Weg vom Knoten a zum Knoten f!

a) Nutzen Sie zunächst den Dijkstra-Algorithmus.

b) Nutzen Sie den Bellman-Ford-Algorithmus.

Aufgabe E – Traceroute

1. Lesen Sie die folgenden Artikel:
https://en.wikipedia.org/wiki/Traceroute,
https://linux.die.net/man/8/traceroute.
Beantworten Sie anschließend folgende Fragen:

a) Wofür wird Traceroute genutzt?

b) Wie wird Traceroute umgesetzt, d.h. wie läuft eine „Routen-Verfolgung“ ab?

c) Welche ICMP-Messages werden für die Realisierung genutzt?

d) Welche Limitationen ergeben sich aus dieser Umsetzung?

e) Dokumentieren Sie die Syntax, sowie die Bedeutung von Traceroute beispielhaft.

2. Lesen Sie folgendes Paper zu Paris-Traceroute [1] von der ACM International Measurement Conference (IMC) 2006:
http://conferences.sigcomm.org/imc/2006/papers/p15-augustin.pdf

a) Warum ist eine „neue“ Traceroute-Applikation notwendig?

b) Nennen Sie drei Topologie-Anomalien die durch Paris-Traceroute erkannt werden kann.

c) Recherchieren Sie wie *paris-traceroute* zu nutzen ist! Notieren Sie sich entsprechend die Kommandos und deren Bedeutung.

Literatur

[1] Brice Augustin u. a. „Avoiding Traceroute Anomalies with Paris Traceroute“. In: *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*. IMC '06. Rio de Janeriro, Brazil: ACM, 2006, S. 153–158. ISBN: 1-59593-561-4. DOI: 10.1145/1177080.1177100. URL: http://doi.acm.org/10.1145/1177080.1177100.

[2] James F. Kurose und Keith W. Ross. *Computer Networking: A Top-Down Approach (6th Edition)*. 6th. Pearson, 2012. ISBN: 0132856204, 9780132856201.