Rechnernetze & Verteilte Systeme

Ludwig-Maximilians-Universität München

Sommersemester 2019

Prof. Dr. D. Kranzlmüller

MNM TEAM

Teil 1: Repetitorium

Am Beispiel von Übungsblatt 12

Blatt 12: Das Leben eines HTTP Requests

- Ingesamt 3 große Teilschritte:
  1. **DHCP:** Konfiguration von Alice‘s Laptop via DHCP (Dynamic Host Configuration Protocol)
  2. **DNS und ARP:** DNS-Anfrage sowie MAC-Adressen-Auflösung des Routers
  3. **Routing**: Routing der DNS-Anfrage zum DNS-Server
  4. **HTTP:** TCP und HTTP

Teil 1: DHCP

1. Alice‘s Host (Betriebsystem) erzeugt eine **DHCP Anfrage**, gekapselt in ein UDP Datagramm mit
   - Schicht 4: Quell-Port 68 sowie Ziel-Port (67) → Standardisiert in RFC 2132.
   - Schicht 3: IP Ziel-Adresse 255.255.255.255 (**Broadcast**) sowie Quell-Adresse (0.0.0.0).
   - Schicht 2: Ethernet Rahmen mit Ziel-Adresse FF:FF:FF:FF:FF:FF (Broadcast) sowie Quell-Adresse 00:00:00:00:AA:AA
2. Der Ethernet-Rahmen wird via Switch (Broadcast an alle Ports) an den übermittelt.
3. Der Router empfängt den Rahmen auf dem Interface mit MAC Adresse 00:00:00:00:BB:BB zugestellt und entpackt das IP-Paket sowie UDP Datagramm (**Demultiplexing**)

Teil 1: DHCP (Fortsetzung)

4. Der DHCP Server alloziert eine Adresse aus dem CIDR Block 10.0.2.0/24, in diesem Falle 10.0.2.100 und verpackt diese Information in einem **DHCP ACK**. Weitere Informationen sind die IP-Adresse des DNS Servers (10.128.5.1), das Subnetz (10.0.2.0/24) sowie das Default Gateway (10.0.2.1)
5. Das DHCP ACK wird wiederum in ein UDP Datagramm bzw. ein IP Paket und einen Ethernet-Rahmen verpackt und an den Switch übermittelt.
6. Der Switch leitet das Paket weiter an Alice‘s Laptop.
7. Alice‘s Laptop empfängt den Rahmen und entpackt das IP-Paket, UDP Datagram und DHCP ACK bis zur Anwendungsschicht. Daraus extrahiert das Betriebssystem die IP-Adresse, das Default Gateway und den Subnetz-Block. Alle Pakete außerhalb des Subnetzes werden an das Default-Gateway vermittelt.

Teil 2: DNS und ARP

8. Das Betriebssystem erzeugt eine DNS-Anfrage für den Namen www.google.com
   - Schicht 4: UDP-Datagram mit Ziel-Port 53 (DNS Server).
   - Schicht 3: IP Quell-Adresse 10.0.2.100 und Ziel-Adresse 10.128.5.1 (außerhalb des lokalen Subnetzes)
   - Schicht 2: <nicht bekannt>
9. Der Ethernet-Rahmen wird an das Default-Gateway (10.0.2.1) gesendet. Ermittlung der Schicht 2 Adresse (MAC) via **ARP-Anfrage.**

Teil2: DNS und ARP (Fortsetzung)

10. Es wird eine ARP-Anfrage vorbereitet mit Ziel-IP-Adresse 10.0.2.1 und Ziel-MAC-Adresse FF:FF:FF:FF:FF (Broadcast). Der Rahmen wird über den Switch an den Router vermittelt.
11. Der Router empfängt die Anfrage, stellt fest, dass die gesuchte IP-Adresse mit der des lokalen Interfaces übereinstimmt und bereitet daher eine **ARP-Response** vor.
    - Mit MAC-Adresse des Routers (00:00:00:00:BB:BB).
    - Ethernet Rahmen mit Ziel-Adresse 00:00:00:00:AA:AA (Adresse von Alice‘s Laptop).
12. Alice‘s Laptop empfängt die ARP-Reponse und extrahiert die MAC-Adresse des Routers.
13. Die MAC-Adresse wird in die Ziel-Adresse des Ethernet-Rahmens der DNS-Anfrage übernommen.
    - **Wichtig:** Die Ziel-IP ist der DNS-Server (10.128.5.1), wohingegen die Ziel-MAC das Default-Gateway ist.

Teil 3: Routing zum DNS Server

14. Der Router extrahiert die DNS-Anfrage und prüft in der lokalen Routing Table die IP-Adresse (10.128.5.1). Dabei ist der linke Router im MWN Netz (siehe Abbildung im Übungsblatt) als nächster Hop gelistet, an den der Rahmen weitervermittelt wird.
15. Der MWN Router wiederum prüft die Ziel-Adresse des UDP Datagramms (DNS Anfrage) und ermittelt den nächsten Hop (bestimmt durch ein Intra-Domain Protokoll wie **RIP, OSPF,…**)
16. Über verschiedene Hops erreicht die DNS-Anfrage den DNS-Server (10.128.5.1). Der **DNS Resource Record** enthält die IP-Adresse für Google (94.233.169.105). Es wird eine DNS-Response vorbereitet mit dem Host-zu-IP Mapping
    - UDP Ziel-IP-Adresse 10.0.2.100.
    - Das Paket wird über mehrere Hops an Alice vermittelt.
17. Alice entpackt die Information und kennt daher die IP-Adresse von www.google.com

Teil 4: TCP und HTTP

18. Bevor der HTTP-Request abgeschickt werden kann, muss ein **TCP-Handshake** erfolgen. Daher wird ein lokaler Socket zur Erzeugung eines TCP SYN Paket vorbereitet:
    - Schicht 4: Ziel-Port 443 (HTTPS)
    - Schicht 3: IP-Adresse (64.233.169.105)
    - Schicht 2: MAC-Adresse des Default-Gateways vorbereitet.
19. Das TCP SYN Segment erreicht den Router und wird MWN Netz auf Basis von BGP an Google vermittelt.
20. Das TCP SYN Segment wird vom Google-Server empfangen und ein entsprechender Socket wird lokal initiiert. Das TCP SYNACK wird erzeugt und an Alice zurückgesendet.
21. Das SYNACK wird analog zu den vorherigen Schritten via BGP und Intra-Domain Routing an Alice vermittelt.

Teil 4: TCP und HTTP (Fortsetzung)

18. Alice erzeugt nach Erhalt des SYNACK einen HTTP GET Request als Payload des nächsten TCP Segments. Vermittlung erfolgt analog zu Schritten 18-20.
19. Der Server Google.com erzeugt eine HTTP Response und platziert den Webseiten-Inhalt (HTML) als Payload in ein TCP Segment.
20. Alice‘s Browser rendert den HTML Inhalt und zeigt schließlich die Webseite.

Ausblick auf WS 19/20

Vorlesungen am Lehrstuhl Kranzlmüller

- Computer Networks Engineering (Master-Praktikum)
  - Detaillierte Untersuchung von Protokollkonzepten (verschiedene RFCs).
  - Netzprogrammierung: Eigenständige Implementierung von Standardprotokollen (bspw. ARP)
  - Berücksichtigung von spezifischen Einschränkungen bei „constrained Devices“ (IoT), bspw. Raspberry Pi, Nucleo Boards, Arduinos…
  - Software Defined Networks
- Parallel Computing (Master Vorlesung bzw. vertiefte Themen Bachelor)
  - Hochskalierbare verteilte Systemprogrammierung.
  - Verfahren für wissenschaftliche (komplexe) Berechnungen wie bspw. Wettervorhersagen, **Big Data** sowie Machine Learning
  - Erlangung eines detaillierten Verständnisses von Rechnerarchitektur, C und C++
- IT-Sicherheit
  - Sicherheitskonzepte in Rechnernetzen.