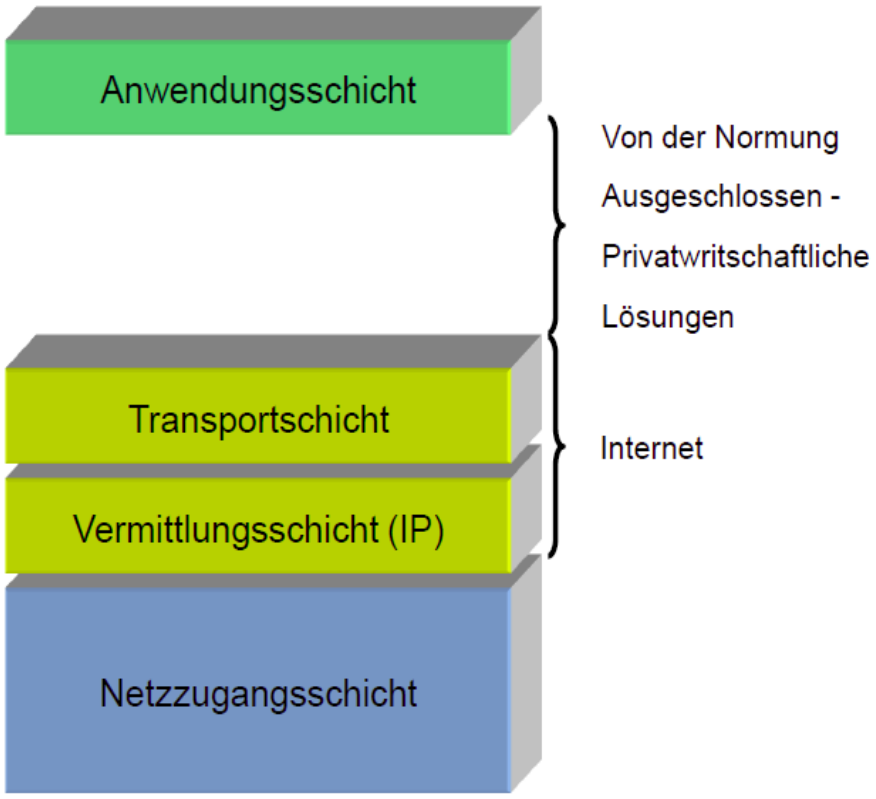
1 Analysis mit Wireshark

Im Rahmen folgender Fragestellungen analysieren wir mithilfe von Wireshark das beiliegende dump_protocols.pcap.

1.1 Welche Netzwerkprotokolle werden in der Kommunikation verwendet?
Es lassen sich mehrere Protokolle identifizieren, mitunter:

◇ DHCP - Dynamic Host Configuration Protocol: Zuweisung von Client & Server.
◇ ARP - Address Resolution Protocol: Zuweisung der MAC-Adressen im Lokalen Netzwerk.
◇ ICMP - Internet Control Message Protocol: Handling von Fehler und Status in IP/TCP/UDP
◇ DNS - Domain Name System: Zuweisung von IPs und Hostnamen.
◇ TCP - Transmission Control Protocol: Datenübertragungsprotokoll, orientiert an sicherer Packetzustellung.
◇ HTTP - HyperText Transfer Protocol: User Agent-Rendering gemäß .htmls

1.2 Ordnen Sie jedes der Protokolle einer Schicht im TCP/IP-Referenzmodell zu und stellen Sie die Hierarchie der einzelnen Protokolle graphisch dar.
Zunächst eine Wiederholung des TCP-IP Schichtenmodelles:



TCP/IP - Modell

Die genutzten Protokolle stehen somit in Folgender Relation zum TCP-IP Modell:

- DHCP - Application Layer, als auch für das OSI-Model
  Grund: DHCP vermittelt eine Client-Server verbindung basierend auf dem ausgeführtem Programm. Gibt es kein Programm, so gibt es weder spezifizierten Klienten noch Server.

- ARP - Network Access Layer, or Data Link Layer for the OSI-Model
  Grund: ARP befasst sich mit der Korrektheit der MAC-Adressen. Diese befinden sich im Datalink Layer (OSI) und somit im Network Access Layer des TCP-IP.

- ICMP - Vermittlungsschicht, or Network Layer für OSI
  Grund: ICMPvX beschäftigt sich mit Fehlercodes des IPvX, weshalb es keinem anderen Layer zuschreibbar ist als dem Network-Layer des OSI-Models. Dementsprechend befindet es sich in der Vermittlungsschicht.

- DNS - Application Layer - parallel mit HTTP, eben so für das OSI-Model
  Grund: DNS beschäftigt sich mit dem Zuschreiben von Aliasen der IP-Adressen, den Hostnamen. Dieser findet jedoch nur im Browser(=Applikationsschicht) nutzen, da aus maschineller Sicht die Hostnamen IP-Adressen wiederspiegeln.

- TCP - Transport Layer für das TCP-IP als auch OSI-Model
  Grund: TCP beschäftigt sich mit dem Datenaustausch über Handshake. Als bekanntes Protokoll dient es der sicheren Übertragung von Frames und ist dementsprechend auf dem Transportlayer angesiedelt.

- HTTP - Application Layer, ebenso für OSI
  Grund: HTTP dient der Übertragung der spezifizierten .htmls eines Servers, gewöhnlicherweise via TCP/IP. Da HTML (& css sowie js oder php, etc.) der Darstellung einer Seite dienen, gilt HTTP der Applikationsschicht.

Graphisch wären die Protokolle etwa so einzugliedern: