

## 1.3.1 IT-Netzwerke

### Recherchearbeit

#### 1. Aufgabe (Heimnetzwerk)

1. Zeichne ein einfaches Netzwerkdiagramm, das mindestens vier Geräte (z.B. Laptop, Smartphone, Server, Router) und deren Verbindungen (Kabel oder WLAN) zeigt.

2. Beschreibe für jedes Gerät seine Rolle im Netzwerk (Endgerät, Router, Switch) und welches Übertragungsmedium genutzt wird (Kupferkabel, WLAN).

3. Zeichne ein, welche Protokolle (z.B. TCP, HTTP) zwischen den Geräten eingesetzt werden, um die Kommunikation zu ermöglichen.

4. Erkläre den Unterschied zwischen privaten und öffentlichen IP-Adressen. Wo finde ich in meinem Heimnetzwerk eine private und wo eine öffentliche IP-Adresse?

#### 2. Aufgabe (IP-Adressen und Subnetting)

1. Gib die IP-Adresse deines Rechners (oder eines Geräts in deinem Netzwerk) mit Hilfe des Kommandos `ipconfig` (Windows) oder `ip a` (Linux/Mac) heraus.

2. Wie sieht eine IP-Adresse in IPv4-Format aus? Was ist der Unterschied zum IPv6-Format?

3. Berechne, wie viele Hosts in deinem Netzwerk (z.B. /24) möglich sind. Gehe in diesem Fall von Schräger 24 aus. Wie sieht die Subnetzmaske aus? Wie viele Geräte können sich in diesem Netzwerk befinden?

4. Wann könnte Subnetting hilfreich sein?

5. Extraaufgabe: Simuliere, wie das Netzwerk durch Subnetting in zwei kleinere Netzwerke unterteilt werden könnte und beschreibe die neue IP-Aufteilung.

### 3. Aufgabe (VMs im Client-Server-Netzwerk)

1. Simuliere mit Hilfe einer Virtualisierungssoftware (z.B. VirtualBox oder Multipass) ein kleines Client-Server-Netzwerk.

2. Richte zwei virtuelle Maschinen ein: Einen "Client" und einen "Server". Der Server soll einen Webserver (z.B. Nginx) laufen lassen, der Client soll per curl-Abfrage auf die Website zugreifen.

3. Dokumentiere die IP-Adressen, die den virtuellen Maschinen zugewiesen wurden, und die Kommunikation zwischen den Geräten (z.B. über den Browser).

4. Zusatzaufgabe: Finde heraus, ob Multipass eine Port-Weiterleitung o.ä. verwendet, damit der Host auf die VMs zugreifen kann. Die VMs in Multipass bilden ein sog. NAT-Netzwerk, das von außen so nicht erreichbar sein sollte.