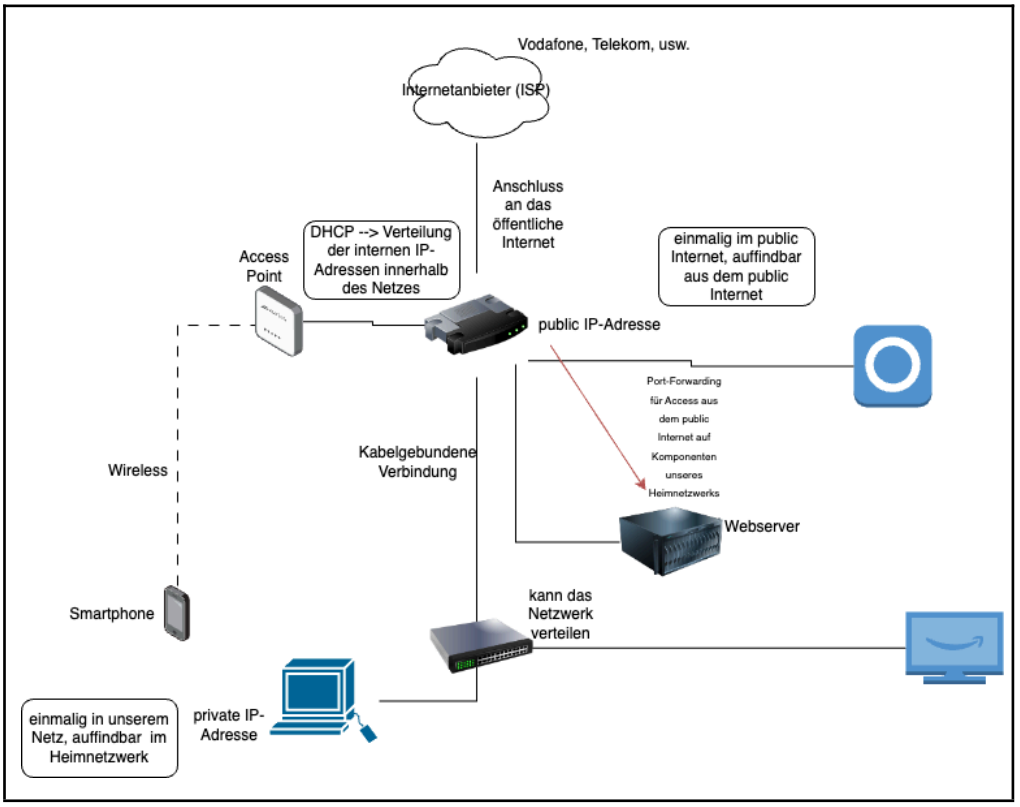
1.3.1 IT-Netzwerke

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).

s.o.

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

DHCP (vom Router für dynamische IP-Adressierung), TCP/IP für Datenpakete die zwischen Endpunkten versendet werden, HTTP bspw. wenn wir einen Webserver einrichten und darauf zugreifen, Drucker IPP, ...

OSI-Schicht		Einordnung	TCP/IP-Referenzmodell	Einordnung	Protokollbeispiele	Einheiten	Kopplungselemente
7	Anwendung (Application)	Anwendungs-orientiert	Anwendung	Ende zu Ende (Multihop)	DHCP DNS FTP HTTP HTTPS LDAP MQTT NCP RTP SMTP XMPP	Daten	Gateway, Content-Switch, Proxy, Layer-4-7-Switch
6	Darstellung (Presentation)						
5	Sitzung (Session)						
4	Transport (Transport)	Transport-orientiert	Transport		TCP UDP SCTP SPX	TCP = Segmente UDP = Datagramme	
3	Vermittlung-/Paket (Network)		Internet		ICMP IGMP IP IPsec IPX	Pakete	Router, Layer-3-Switch
2	Sicherung (Data Link)		Netzzugriff	Punkt zu Punkt	IEEE 802.3 Ethernet IEEE 802.11 WLAN TLAP FDDI MAC Token Ring ARCNET	Rahmen (Frames)	Bridge, Layer-2-Switch, Wireless Access Point
1	Bitübertragung (Physical)				1000BASE-T Token Ring ARCNET	Bits, Symbole	Netzwerkkabel, Repeater, Hub, Antenne, Äther

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

Router → hat öffentliche IP-Adresse, d.h. von außen (aus dem Internet) erreichbar.
Endgeräte im Heimnetzwerk → private IP-Adressen, nur innerhalb des Netzwerks erreichbar

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.

(Screenshot von Ausgabe von ip a bzw. ipconfig)

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

IPv4: 4 Oktette mit Punkten getrennt.
0.0.0.0. kleinste IP-Adresse bis 255.255.255.255 größte IP-Adresse
192.168.1.0 → 11000000.10101000.00000001.000000000
4.3 Milliarden mögliche Adressen
IPv6: 8 mal 2 Byte (1 Byte = 8 Bit) Stellen in Hexadezimal
340 Undezimillionen mögliche Adressen

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?

/24 Subnetzmaske hier werden die ersten 24 Bit auf 1 gesetzt:
11111111.11111111.11111111.00000000
Die ersten 24 Stellen Netzanteil und dann Hostanteil, d.h.
Möglichkeiten unseren Hosts Adressen zuzuweisen.
8 Stellen → 2^8 - 2 = 254 mögliche Hosts in unserem Subnetz

4. Wann könnte Subnetting hilfreich sein?

- Bei größeren Netzwerken in z.B. Firmennetzwerken mit vielen Usern → viel Traffic/Netzwerklast
- Sicherheit → Wir isolieren Teile des Netzes, Angriffe sind schwieriger

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

z.B. eine IP-Adresse von unserem Netz 192.168.1.0/24
Wir nehmen einfach eine “größere” Subnetzmaske, hier 25.
Das bedeutet 111111111.11111111.11111111.10000000 (neue Subnetzmaske)
14

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.