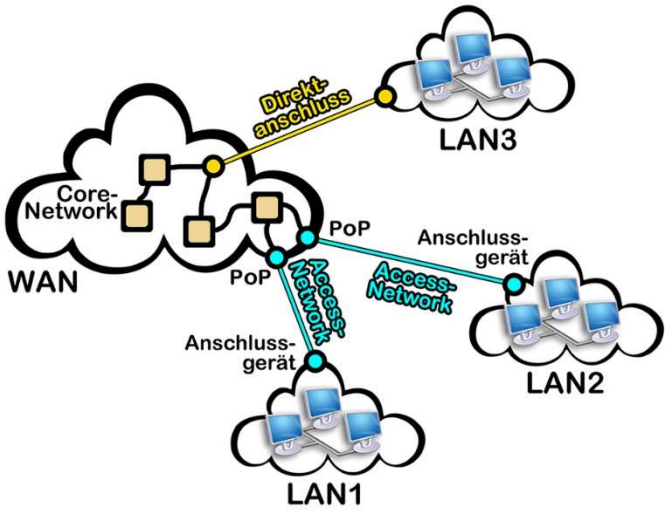
A: Der Zugang ins Internet (WWW - World-Wide-Web)

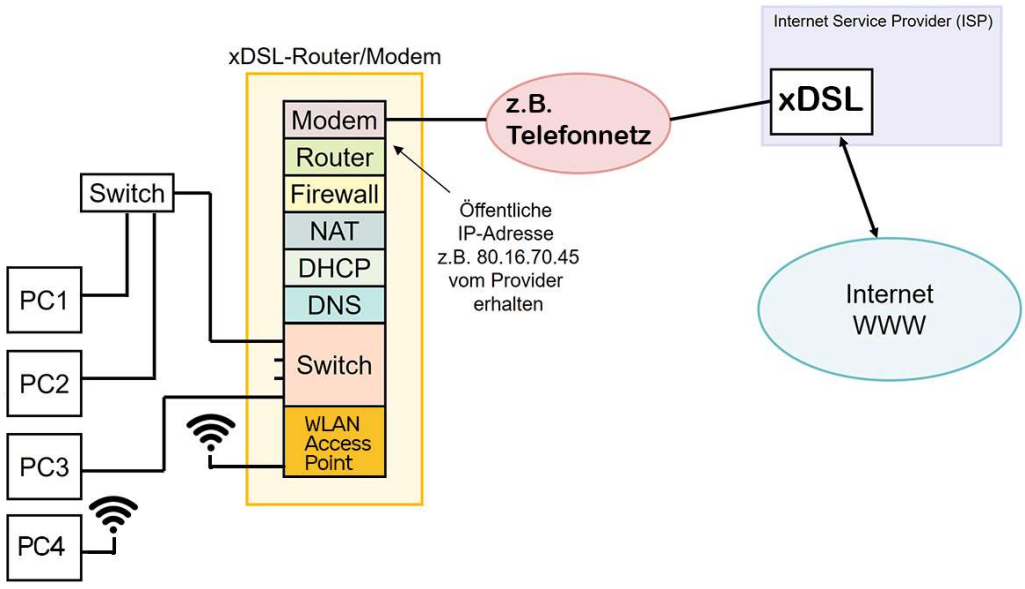
Damit sie aus ihrem LAN (Local Area Network) ins Internet gelangen, brauchen sie einen entsprechenden Anschluss ins WAN (Wide Area Network) oder Core-Network.

Das kann auf verschiedene Arten erfolgen:

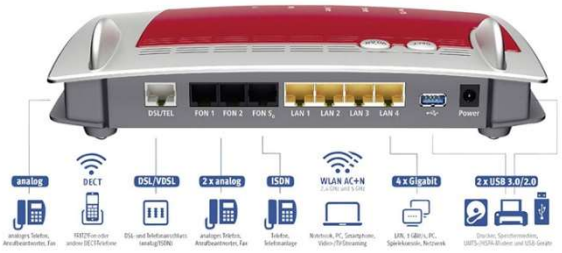
- Direktanschluss ans Core-Network (Direkter Glasfaseranschluss)
  Das Core-Network (Provider-Backbone) ist das Kernstück des Telekommunikationsnetzwerks, welches von den Verbindungsnetzwerkbetreibern unterhalten wird.
- Mit Anschlussgerät ans Access-Network des Internet-Service-Providers ISP (Teilnehmerkabelanschluss, ADSL, VDSL, SDSL, Glasfaseranschluss)



In vielen Fällen, besonders bei Privatpersonen, erfolgt der Internetzugang via eines ADSL-Anschlussgerätes ans Access-Network des Internet-Service-Providers wie z.B. Swisscom oder Sunrise/UPC. Dazu benötigen sie in ihrem LAN ein Router, der zum ISP führt.



Dieser Router wird entweder vom ISP zur Verfügung gestellt oder man erwirbt sich ein Exemplar im Fachhandel wie z.B. diese Fritz!Box:



Es handelt sich hier allerdings um mehr als nur einen Router. Der Router verbindet IP-Netze und arbeitet somit auf OSI-Layer 3 bzw. Network-Layer. xDSL-Router verfügen aber meist über viel mehr Funktionen wie:

- **Signalaustausch** über das Telefonnetz mit **xDSL-Modem** (ADSL oder SDSL)
  - ADSL : Asymmetric Digital Subscriber Line. Uplink weist nicht dieselbe Bandbreite auf – meist langsamer – als der Downlink.
  - SDSL : Symmetric Digital Subscriber Line. Uplink und Downlink weisen dieselbe Bandbreite auf. Dies ist z.B. für LAN-WAN-LAN-Verbindungen erforderlich.
- **Signalaustausch** über ein **Koaxialkabel** oder **Glasfaseranschluss**.
- **Router**: Der Router verbindet das Intranet mit der Aussenwelt bzw. routet Datenpakete vom und zum Internet.
- **DHCP**-Dienst: Für eine automatische Zuweisung von IP-Adressen an die PC's.
- **DNS**-Dienst: Für die Namensauflösung URL zu IP-Adresse.
- **NAT**: Network-Adress-Translation. Übersetzt interne (private) IP-Adressen in eine externe (öffentliche) IP-Adresse und umgekehrt.
- **Firewall**: Für einen «einfachen» Schutz vor unerwünschten Datenpaketen.
- **WLAN-Access-Point**: Wireless Local Area Network, Drahtloses lokales Netzwerk.
- **Switch**: Drahtgebundene Netzwerkvermittlungsstelle
- **USB**-Druckeranschluss (Druckerserver)
- **DECT**-Schnurlos-Telefonanschlüsse

Die Bezeichnung Multifunktionsgerät wäre wahrscheinlich treffender als nur Router. Im Fachhandel sind selbstverständlich auch reine Router im Angebot, die ausschliesslich die eine Funktion «Routing» beherrschen.

ISP-Auftrag: Sie sollen **zwei ISP-Angebote** (Keine Glasfaser!) für **ihren Wohnort** evaluieren und die Resultate in einer tabellarischen Aufstellung präsentieren. Klären sie folgendes ab:

- Technologie (ADSL, SDSL, VDSL, Glasfaser, Koaxialkabel, Drahtlos?)
- Welche Leistung (Datendurchsatzrate Up- und Download) wird zu welchem Preis angeboten? (Best Effort?)
- Wird der Router kostenlos mitgeliefert?
- Einmalige Gebühren wie z.B. Aufschaltgebühren, Installationskosten etc.
- Support, Hotline-Verfügbarkeit, kostenpflichtige (?) Vor-Ort-Servicedienstleistungen
- Vertragsdauer, Kündigungsfristen, Ansprechpartner
- Netz-Verfügbarkeit (7x24h * 365 Tage?) Wartungsintervalle etc.
- Skalierbarkeit (Wenn die Leistung nicht mehr reicht und der «Hahn aufgedreht» werden muss.)

B: WLAN - Wireless Local Area Network (Drahtloses lokales Funknetzwerk)

***Frage**: Ist wirklich alles Gold was glänzt? Kabelsalat war gestern, das «Heute» ist kabellos?! So mindestens verkünden es die Marketingabteilungen der führenden Technologieunternehmen. Und siehe da: Aktuelle Notebook besitzen kaum noch RJ45-Netzwerkbuchsen und verbliebene kabelgebundene Schnittstellen wie USB, HDMI und Displayport sind wohl ein Auslaufmodell. Bei modernen Tablets und Smartphones wurde sogar das letzte verbliebene Kabel gekappt: Stromversorgung geht auch berührungslos! Hat Kupfer oder Glas in der Netzwerktechnik wirklich ausgedient? Was meinen sie dazu?*

Die **WLAN-Norm IEEE 802.11** definiert wichtige WLAN-Eigenschaften wie z.B.:

- **Sendeleistung**: Die Sendeleistungen liegen zwischen 100mW bis 1W.
- **Datenrate:**
  - **Bruttodatenrate**: Maximale Datenrate, die unter Nutzung der höchsten Kanalbreite/Bandbreite (20MHz, 40MHz, 80MHz, 160MHz) und maximaler Anzahl Sende/Empfangseinheiten (1-8, MIMO) des jeweilige WLAN-Standards theoretisch zu erzielen ist.
  - **Nettodatenrate**: Die Bruttodatenrate kann aus verschiedenen Gründen in der realen Welt nicht erreicht werden. Für die Netzwerkdimensionierung muss von einer Nettodatenrate von ca. 15% bis 50% der Bruttodatenrate ausgegangen werden.
- **Frequenzband**: 2.4GHz (2.4-2.4835 GHz), 5GHz (5.47-5.735GHz)
- **Bandbreite/Kanalbreite**: Jeder Accesspoint arbeitet auf einer Frequenz (2.4GHz, 5GHz) und da auf einem bestimmten Kanal. Das 2,4-GHz-Band wurde in 13 Kanäle aufgeteilt, das 5GHz-Band in wesentlich mehr. Auch APs mit MIMO-Antennentechnik arbeiten auf einer Frequenz und da in einem Kanal.
- **Antennentechnik**: In den WLAN-Anfängen kamen SISO-Antennen zum Einsatz. Die heutigen Bandbreiten werden aber nur mit MIMO oder MU-MIMO erreicht:
  - **SISO**: Single Input, Single Output mit jeweils einer Antenne auf Sender- und Empfängerseite.
  - **MIMO**: Multiple Input Multiple Output mit jeweils mehreren Antenne auf Sender- und Empfängerseite.
  - **MU-MIMO**: Multi-User-MIMO. Effizienzsteigerung → AP kann mehreren Clients gleichzeitig verschiedene Datensätze schicken → Funkkanal wird schneller wieder frei.
- **Maximale Reichweite**: Mit normalen 2.4GHz-AP's erschliesst man so zwischen 50m bis 100m, mit solchen im 5GHz-Bereich ca. 20m bis 100m. Die genauen Angaben entnehme man dem entsprechenden Datenblatt. Grundsätzlich entscheidend ist:
  - **Max. Sendeleistung**
  - Innenbereich oder Aussenbereich.
  - **Antennenart**: Stabantenne, Sektorantenne oder Richtantenne. Z.B. mit einer Richtantenne kann die Reichweite signifikant erhöht werden.
  - **Frequenzbereich**: Je höher die Frequenz, umso tiefer die Reichweite, wegen Störeinflüssen. Vereinfacht ausgedrückt: Je höher die Frequenz, umso mehr muss «Sichtkontakt» bestehen.
  - **Dämpfung der WLAN-Funkwellen** durch Baumaterialien: Holz, Gips und Glas (Möbel, Zwischenwände etc.) dämpfen Funkwellen nur gering, Wasser, Mauersteine etwas mehr und massive Betonwände oder gar Liftschächte, Brandschutztüren, also generell Stahlbetonkonstruktionen sehr stark.

Die **Betriebsarten** eines WLAN-AccessPoints (AP):

Das Wichtigste zum Thema **WLAN-Sicherheit**:

Die Sicherheit von WLANs basiert auf einer Kombination aus **Authentifizierung** und **Verschlüsselung**. Ein offenes WLAN stellt sich wie ein offenes Scheunentor dar. Beim Surfen über das offene WLAN hinterlässt die IP-Adresse des WLAN-Betreibers eine Spur im Netz. Diese IP-Adresse kann im Nachhinein dem Anschlussinhaber zugeordnet werden. Der Anschlussinhaber wird daher im Rahmen einer Rechtsverletzung als erster Verdächtiger ermittelt.

- Wenn immer möglich mit mind. **WPA2** (WIFI Protected Access 2 (IEEE802.11i) verschlüsselt verbinden. WPA2 gilt als hinreichend sicher, wenn das WLAN-Passwort möglichst lang und komplex ist. Befindet sich das Passwort in einem Wörterbuch, dann bestehen gute Chancen, dass ein Angreifer das Passwort herauszufinden kann. ***WEP ist geknackt und sollte nicht mehr verwendet werden***.
- Im kommerziellen oder großräumigen Einsatz sollte ein WLAN immer im **Enterprise Mode mit IEEE 802.1x** gesichert werden.
- **WPS** ausschalten.
- Die **WLAN-Reichweite** bzw. Antenne und Sendeleistung den Bedürfnissen anpassen um ein «Mithören» nicht zu fördern.
- Default-**Admin-Passwort** ändern.
- Aktuelle **Patches** einspielen.
- **SSID** wählen, die keine Rückschlüsse auf die Firma oder Namen zulässt.
- **Logische Trennung** von LAN und WLAN (verschiedene Netze)
- **Firewall** zwischen WLAN und LAN.

MAC-Adressfilter einsetzen ist fraglich. Ein Hacker wird sich einfach seinen WLAN-Adapter mit der MAC-Adresse eines berechtigten WLAN-Adapters überschreiben und schon ist der MAC-Filter umgangen.

Auch das Verstecken des SSID-Broadcasts hat wenig Nutzen und wird auch nicht offiziell unterstützt bzw. ist für Hacker kein wirkliches Hindernis, denn sobald sich ein Client an einem WLAN mit versteckter SSID anmeldet, wird dabei die SSID übertragen. Es entsteht sogar eine Sicherheitslücke: Normalerweise würde der WLAN-Access-Point regelmässig über sein WLAN informieren. Wenn er das nicht tut, dann muss der WLAN-Client, der einmal damit verbunden war, aktiv nach diesem WLAN suchen. Deshalb broadcastet dieser Client regelmäßig die SSID von sich aus heraus. Er ruft praktisch ständig nach dem versteckten WLAN. Auch wenn das gar nicht in der Nähe ist.

WLAN-Auftrag:

- Untersuchen sie die **WLAN-Verhältnisse** an ihrem **Wohnort** mit einer **Heatmapping-Software**. Mapping-Tools sind in der Regel kostenpflichtig. Eine kostenlose Möglichkeiten bzw. Testversion für 30 Tage findet man bei SolarWinds: WiFi Heat Map. ***(Dies ist als Hausaufgabe zu lösen! Die Software können sie aber an der Schule herunterladen und ausprobieren.)*** (https://www.solarwinds.com/network-performance-monitor/use-cases/wifi-monitor)
    - Grafische Darstellung der WLAN Abdeckung.
      Dazu müssen sie vorerst den Grundriss ihrer Wohnung massstabgerecht grob skizzieren.
    - Positionen der Access Points (Auch diejenigen ihrer Nachbarn, die in ihrer Wohnung erreichbar sind.)
    - Einstellungen der Access Points wie Frequenzbereich (2.4GHz, 5GHz, SSID, WLAN-Sicherheit, WPA, Hotspot etc.)
- Sie haben den Auftrag, bei ihnen zuhause einen neuen WLAN-AccessPoint zu installieren. Doch vorerst müssen sie sich im Fachmarkt informieren, welche Geräte aktuell und lieferbar sind. Dabei interessieren die folgenden Merkmale, die sie tabellarisch zusammenfassen:
    - **Gerätebezeichnung**, Hersteller, Preis, Lieferfristen
    - WLAN-**Frequenzbänder**
    - WLAN Standard gemäss **IEEE 802.11**
    - Zu erwartende **Datenrate** Brutto und Netto
    - **Antennentechnik** (externe Antennen?)
    - **WLAN-Sicherheit** (Verschlüsselung)
    - Die zukünftige **SSID**
    - Optimaler **Standort** in ihrer Wohnung
    - Weitere Eigenschaften…
- Nehmen wir an, sie hätten noch drei Geschwister. Alle möchten gleichzeitig einen Netflix-Film von z.B. 4GB über WLAN herunterladen. Wie beurteilen sie diese Situation?

C: Glasfasertechnologie im Netzwerk (Lichtwellenleiter/Optical Fibre)

- Eher **starres Medium**, wo bei zu engem **Biegeradius** die Übertragungsleistung leidet (Diffuse Zone) oder das Glas vollständig bricht.
- Billiger in der Kabelherstellung aber teuer in der Verarbeitung, da spezielle und kostspielige **Abisolier- und Spleissmaschinen** für die Glasfaser-Steckermontage benötigt werden. Die Investitionen sind dabei jenseits von kostengünstigen Crimpzangen, wie sie etwa bei der RJ45-Steckermontage benötigt werden.
- Weitgehend **immun** gegen magnetische und elektrostatische **Störeinflüsse**. Also das ideale Medium für rauhe Umgebungen wie z.B. Maschinenfabriken, Kraftwerke.
- Eine Lichtverbindung lässt prinzipiell eine **hohe Datenübertragung** und eine Überbrückung von **grossen Distanzen** zu. Eine hohe Datenübertragung erfordert aber auch eine entsprechend leistungsfähige (schnelle) Elektronik an den beiden Kabelenden. Darum: Performance ist, wie bei den Kupferverbindungen vom spezifizierten **Ethernetstandard** abhängig, wie z.B. den beiden folgenden:
  - **1000Base-LX**: 802.3z(1998); Stern/Duplex; 1Gbps; Long-Wavelength (1300nm)
    50µm / 62.5µm Multimode → Segmentlänge ≤ 550m
    10µm → Segmentlänge ≤ **5000m**
  - **1000Base-SX**: 802.3z(1998); Stern/Duplex; 1Gbps; Short-Wavelength (850nm)
    62.5µm Multimode → Segmentlänge ≤ 275m
    50µm Multimode → Segmentlänge ≤ 550m
- **LAN: Duplex/Bidirektional**: Ein Lichtwellenleiter für Senden und einer für Empfangen.
- Eine Vielzahl von **Steckverbindungen** sind erhältlich wie z.B. F-SMA, FC/PC, ST, SC und weitere.
- Zurzeit, d.h. bevor «Computing with Light» massentauglich wird, muss das elektrische Signal vor der Lichtwellenleiterstrecke in ein **optische Signal** und danach wieder in ein **elektrisches Signal umgewandelt** werden.
- Wie beim Kupferkabel (z.B. CAT7) sind auch die **Lichtwellenleiter kategorisiert** (OM1-5, OS1,2). Die kostengünstigere **Multimodefaser** (OM1-5) wird eher für den LAN-Bereich und somit kurze Distanzen eingesetzt, die **Monomodefaser** (OM1,2) dagegen zur Überbrückung von grossen Distanzen bis zu 100km wie z.B. bei Seekabeln erforderlich.

Lichtwellenleiter-Auftrag:

- Erkundigen sie sich bei ihrem ISP wie z.B. Swisscom, ob an ihrem Wohnort auch Glasfaser verfügbar wäre, und welche Übertragungsrate dann angeboten würde. Meistens handelt es sich bei den ISPs um das teuerste und performanteste Angebot. Wird ein Router mitgeliefert?
- Sie möchten nicht den WAN-Router verwenden, der ihnen ihr ISP anbietet. Sie möchten ihren eigenen! Evaluieren sie im Fachhandel ein WAN-Router mit WAN-seitigem Glasfaseranschluss. Stellen sie die Spezifikationen tabellarisch zusammen. Dazu sollen u.a. gehören:
  - Welcher Ethernetstandard bzw. IEEE-Norm wird erfüllt?
  - Maximal erreichbarer Datenübertragungsdurchsatz?
  - WAN-seitiger Steckertyp (Lichtwellenleiter)?
  - Kosten und Verfügbarkeit?