WLAN (Wireless Local Area Network)

Bei einem drahtlosen Netzwerk findet die Übertragung ohne Kabel statt. Es werden elektromagnetische Wellen über die Luft übertragen. Für die drahtlose Übertragung im Computernetzwerk bedeutet dies, dass sich Layer 1 und Layer 2 ändern. Die darüber liegenden Layer können unverändert bleiben. Durch diese Änderung der Übertragungsart ergeben sich einige Vorteile aber auch Nachteile.

Vorteile

- BYOD: Bring your own device
- Kosten: Besonders in bestehenden Gebäuden
- Anpassungsfähigkeit und Skalierbarkeit von Hosts

Nachteile

- Geteiltes Medium für viele Teilnehmer
- Störungen
- Geschwindigkeit und Reichweite
- Security

Antennen

Antennen sind die Grundlage für eine Übertragung über die Luft. Sie geben ein Signal in die Luft ab (Senderantenne) und können es auch wieder aus der Luft aufgreifen (Empfängerantenne). Je nach Anwendung eignen sich verschiedene Arten von Antennen.

- Omnidirektionale Antennen: senden in alle Richtungen (Kugel)
- Direkte Antennen: Können gezielt senden
- MIMO (Muliple Input Multiple Output) Antennen: aktuell meist 8 Antennen

Arten von Wireless Netzwerken

Wie auch schon bei den verkabelten Netzen unterscheidet man Netze nach ihrer Größe. Je nach Größe ergeben sich unterschiedliche Anforderungen und Schwierigkeiten.

- WPAN: Kurze Distanz (ca. 10 m), Frequenz meist 2.4 GHz, z.B. Bluetooth, Zigbee
- WLAN: mittlere Distanz (ca. 100 m), Frequenz ist 2.4 GHz oder 5 GHz , z.B. Wifi
- WMAN: Große Distanz(kann sehr unterschiedlich sein), Frequenz zwischen 2 und 66 GHz, z.B. Wifi, WiMax
- WWAN: rießige Distanzen (bis zu 50 km), Frequenz zwischen 2 und 66 GHz, z.B. WiMax

Technologien von Wireless Netzwerken

Es gibt unterschiedliche Technologien die drahtlos übertragen. Je nach Reichweite und Anwendungsgebiet sind unterschiedliche Technologien sinnvoll. Nicht alle Technologien sind dazu geeignet oder dafür entworfen um Netzwerkdaten zu übertragen. Manche Technologien können dies trotzdem umsetzen.

- Wifi (Standard: IEEE 802.11)
- Bluetooth (Standard: IEEE 802.15)
- WiMax (Standard: IEEE 802.16)
- Satelliten Breitband: kann als Internetzugang genutzt werden, z.B. Starlink (aktuell ca. 5000 Geräte (Stand Oktober 2023) in einer Entfernung von 500 bis 600 km, beantragt sind 22000 Satelliten)
- Mobilfunk Breitband: viele verschiedene Standards die meist nach gravierenden Änderungen (Generationen) unterteilt werden. Bei der Änderung in eine neue Generation ist die Geschwindigkeit immer ein entscheidender Faktor ($3G \to 10x \to 4G \to 100x \to 5G$).

Wifi (802.11)

Geschichte

Jahr	Standard	Frequenz	Geschwindigkeit	Bemerkung
1997	802.11	2.4 GHz	2 Mbit/s	
1999	802.11a	5 GHz	54 Mbit/s	nicht kompatibel mit b und g
1999	802.11b	2.4 GHz	11 Mbit/s	bessere Distanz
2003	802.11g	2.4 GHz	54 Mbit/s	nicht kompatibel mit b
2009	802.11n	2.4 und 5 GHz	600 Mbit/s	MIMO, abwärtskompatibel
2013	802.11ac	5 GHz	bis zu 1.3 Gbit/s	8 Antennen
2019	802.11ax	2.4, 5 und 6 GHz	bis zu 48 Gbit/s	Wifi 6

Es gibt noch viele andere Standards, manche für eigene Anwendungen (z.b. IoT 802.11ah).

Elektromagnetische Welle

Gesendet wird mit elektromagnetischen Wellen. Diese kennt man vom sichtbaren Licht. Dort nimmt der Mensch unterschiedliche Wellenlängen (ca. 400 nm bis 700 nm) als verschiedene Farben wahr. Jene Wellenlängen die zum übertragen von Wifi genutzt werden liegen außerhalb des sichtbaren Lichts. Desto länger die Welle ist, desto kürzer ist seine Frequenz (indirekt Proportional). Kurze Wellen besitzen mehr Energie als lange Wellen.

- 2.4 GHz (1−10 dm) UHF: Ultra High Frequency
- 5 GHz (1−10 cm) SHF: Super High Frequency

Für das 5G Netz wurden neue Frequenzbereiche festgelegt und versteigert.

- Mobilfunk: 600 MHz bis 6 GHz
- WLAN: 24 GHz bis 40 GHz

Komponenten im WLAN

- Endgeräte: Mit Netzwerkkarte und Antennen
- Wireless Router: Multifunktionsgeräte mit eingebautem Switch, Router, Modem Access Point, ...
- Access Points: Schnittstelle zwischen dem drahtlosen Netz und dem verkabelten Netz. Man unterscheidet zwischen Autonomen-Access-Points (schwer erweiterbar) und Controller-Based-Access-Points.

Wifi Frame

Frame Control: Metainformationen, z.B. Protokoll, Art des Frames, ... (2 Bytes)
Duration: Übertragungsdauer, da auch die Framelänge sehr unterschiedlich sein kann. (2 Bytes)
Address 1: Empfänger MAC-Adresse (6 Bytes)
Address 2: Sender MAC-Adresse (6 Bytes)
Address 3: MAC BSSID (WLAN Segment) (6 Bytes)
Sequence Control: Hängt vom AP ab
Address 4: MAC-Adresse vom Access Point (6 Bytes)
Frame Body: Header der restlichen Layer und Daten
FCS: Fehlerüberprüfung mit CRC (4 Bytes)

Operations-Modi

- Ad Hoc: Peer-to-Peer Netzwerk ohne Router
- Infrastruktur: Dahinter ein verkabeltes Netz
- Tethering: Hotspot zur Weiterleitung zwischen zwei Netzen

Kollisionen (CSMA/CA)

Wireless Netzwerke nutzten eine Half Duplex Medium zum Senden. Man kann zeitgleich senden und empfangen. Zusätzlich ist es ein Shared Medium, das heißt viele Teilnehmer sind mit dem gleichen Medium verbunden. Somit kann es zu Kollisionen kommen (CSMA - Carrier Sense Multiple Access). Wifi löst das Problem mit Collision Avoidance (CA), es versucht also Kollisionen zu vermeiden. Fall gerade keiner sendet wird um Zeit beim Access Point angefragt. Dann erhält man einen Zeitslot indem man seine Daten senden und empfangen kann.

Verbinden mit einem Accesspoint

- AP finden (aktiv, passiv)
- Authentifizieren: SSID, Passwort, Network Mode(a, b, g, ...), Security (WPA, WPA2, ...), Channel
- Verbindung herstellen

Channels

Die Frequenzen werden in kleinere Bereiche aufgesplittet. Gleiche Channels können sich gegenseitig stören. Überlappende Access Points sollten verschiedene Channels nutzen.

- 2.4 GHz: Europa 13 Channels (1,6,11 sind nicht überlappend), USA 11 Channels, Japan 14 Channels
- 5 GHz: 24 Channels (alle ohne Überlappung)

WLAN-Angriffe

- Datendiebstahl: Shared medium → Verschlüsselung
- DoS: falsch konfiguriert, Störsender, ...
- Rogue Access Point: zusätzlichen falschen AP ins Netz eingefügt.
- Evil Twin: Einen AP einfügen, der gleich aussieht aber in ein anderes Netz führt.

Sicherheit und Verschlüsselung

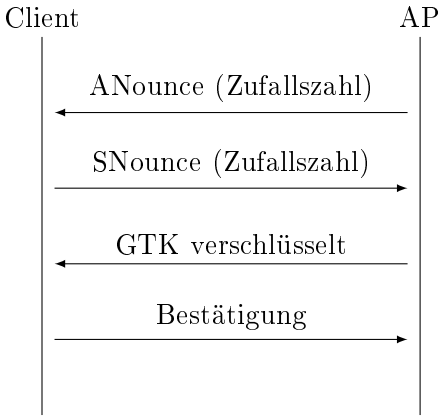
- SSID Beacon verbergen (passiv)
- MAC- Adressen filtern (L2 Security)
- Authentifizierung
  - Open: ohne Passwort (nicht empfohlen)
  - Shared Key: WEP, WPA (TKIP+AES), WPA2, WPA3

Bei WPA2 unterscheidet zwei Varianten zum Authentifizieren:

- Personal: ein Passwort für alles (PSK-Pre Shared Key), eher im privaten Bereich
- Enterprise: Anmeldung mit Usernamen und Passwort, man meldet sich bei einem Server an (z.B. RADIUS), eher im Firmenbereich

WPA2-Personal Handshake: Pre-Shared-Key (4-Way)

Zum Austausch der Schlüssel zwischen dem Access Point und dem Client findet ein 4-Way-Handshake statt. Dabei werden die benötigten Schlüssel generiert. Zum Generieren der Schlüssel muss das Passwort nie übertragen werden, deshalb nennt man die Variante auch PSK (Pre-Shared-Key). Der Schlüssel wurde also davor schon ausgemacht.



PTK (Pairwise Transient Key): für Unicasts jeder hat seinen eigenen Schlüssel mit dem AP

$$\text{PTK} = \text{PRF}(\text{Pwd}+\text{ANounce}+\text{SNounce}+\text{APMAC}+\text{ClientMAC})$$

PRF (Pseudo Random Function): ist eine Pseudo-Zufallsfunktion die dann den Schlüssel erzeugt und den Geräten bekannt ist.
GTK (Group Temporal Key) : für Broadcast und Multicasts im Netz, für alle Teilnehmer gleich.

Das Passwort wird nie über das Medium ausgetauscht, deshalb nennt man das Verfahren Pre Shared Key. Die Nachricht wird nach Layer 2 verschlüsselt. Dieser kann nicht verschlüsselt werden, da der Access Point die Frames identifizieren muss. Danach im verkabelten Netz, wie sonst auch immer, wird wieder nach Layer 4 verschlüsselt (z.b. mit TLS).