WLAN (Wireless Local Area Network)

Definition:
WLAN steht für "Wireless Local Area Network" und bezeichnet ein drahtloses Netzwerk, das es Geräten ermöglicht, sich ohne Kabelverbindung miteinander zu verbinden und auf das Internet zuzugreifen.

Funktionsweise:
WLAN nutzt Funkwellen, um Daten zwischen einem Router und den verbundenen Geräten (wie Laptops, Smartphones und Tablets) zu übertragen. Der Router fungiert als Zugangspunkt, der die Verbindung zum Internet herstellt.

Für WLANs nach IEEE 802.11 stehen mehrere Frequenzbereiche zur Verfügung, die aber weltweit regional unterschiedlich reguliert sind. Erschwerend ist die unterschiedliche Unterstützung in der Hardware und Software.

- unter 1 GHz
- 2,4 GHz (Haupt-Frequenzbereich)
- 5 GHz
- 6 GHz (zukünftige Nutzung in der EU)
- 60 GHz

Das heißt nicht, dass alle WLAN-Geräte alle Frequenzbereiche beherrschen. Der meistgenutzte Bereich liegt bei 2,4 GHz, gefolgt von 5 GHz und 6 GHz. Weiterhin existieren noch Frequenzbereiche unterhalb von 1 GHz und bei 60 GHz, die mit WLAN-Technik genutzt werden dürfen.

Normalerweise werden nur High-End-WLAN-Basisstationen die drei Bänder 2,4 GHz, 5 GHz und 6 GHz gleichzeitig bedienen können. Im niedrigen Preissegment wird man sich auf 2,4 GHz und vielleicht noch 5 GHz beschränken müssen.

Standards:
Die gängigsten WLAN-Standards sind:

- 802.11: Bis zu 2 Mbit/s.
- 802.11b: Bis zu 11 Mbit/s.
- 802.11g: Bis zu 54 Mbit/s.
- 802.11a/h/j Bis zu 54 Mbit/s.
- 802.11n: Bis zu 600 Mbit/s und nutzt MIMO-Technologie (Multiple Input Multiple Output).
- 802.11ac: Bis zu 6.936 Mbit/s und ist für den Einsatz in modernen Netzwerken optimiert.

- 802.11ax Wi-Fi 6 Bis zu 9.608 Mbit/s Der neueste Standard, der höhere Geschwindigkeiten, bessere Effizienz und eine verbesserte Leistung in überlasteten Umgebungen bietet.
- 802.11be Wi-Fi7 Bis zu 23.050 Mbit/s
- 802.11bn Wi-Fi 8: (erwartet 2029)

Datenraten:

Schaut man sich die Angaben der Hersteller und Händler zur Bruttodatenrate ihrer Produkte an und vergleicht die Werte, die man damit in der Praxis erreicht, riecht das fast schon nach einem Reklamationsgrund. Tatsache ist, dass die Bruttodatenraten, wie sie auf den Produktverpackungen und vom Standard angegeben sind, in der Praxis nie erreicht werden können.

Dazu muss man wissen, dass alle WLAN-Standards des IEEE mit ihrer theoretisch maximalen Übertragungsgeschwindigkeit spezifiziert werden. In der Praxis sind die angegebenen Übertragungsraten aber viel geringer, als angegeben. So erreichen WLANs nach IEEE 802.11g mit 54 MBit/s in der Praxis selten mehr als 16 MBit/s. Ein WLAN nach IEEE 802.11n mit 150, 300, 450 und 600 MBit/s erreicht selten mehr als die Hälfte davon. Der Standard IEEE 802.11ac verspricht brutto eine Datenrate von sagenhaften 7 GBit/s. Doch diese Werte sind davon abhängig, welche Funkkanalbreite, Übertragungsart und die Anzahl der Antennen verwendet wird. Doch auch das ist reine Theorie. Denn in der Praxis muss jede Funktechnik mit weiteren Einschränkungen kämpfen. Die typischen Datenraten liegen aufgrund spezifischer Funkbedingungen in der Praxis noch weit darunter. Doch auch das sind nur Richtwerte. Was in der Praxis dann wirklich möglich ist, ist von den lokalen Begebenheiten abhängig. Decken, Wände, Möbel und andere Funknetzwerke stören die Funkübertragung eines WLANs. Je nach Umgebungsbedingungen, Anzahl der teilnehmenden Stationen und deren Entfernung erreicht man also nur einen Bruchteil der typischen Datenrate.

Die Differenz zwischen der Brutto-Übertragungsgeschwindigkeit und dem, was in der Praxis tatsächlich möglich ist, ist der Tatsache geschuldet, dass es sich bei der WLAN-Funktechnik um einen geteilten Übertragungskanal handelt, den mehrere Teilnehmer gleichzeitig nutzen müssen und deshalb ein spezielles Verfahren den Zugriff darauf aushandelt. Das CSMA/CA genannte Verfahren regelt wann eine Station senden darf. Die anderen Stationen müssen während dieser Zeit warten. Anschließend fällt dann noch eine Pause an. Die Funkschnittstelle ist deshalb nie zu 100% belegbar. Für jeden einzelnen Teilnehmer bedeutet das, es bleibt nur ein Bruchteil der typischen Übertragungsgeschwindigkeit übrig.

Sicherheitsprotokolle:

Um die Sicherheit von WLAN-Netzwerken zu gewährleisten, werden verschiedene Protokolle verwendet, darunter:

- WEP (Wired Equivalent Privacy): Ein älteres und unsicheres Protokoll.

- WPA (Wi-Fi Protected Access): Bietet verbesserte Sicherheit im Vergleich zu WEP.

- WPA2: Der Standard für die meisten modernen Netzwerke, der eine starke Verschlüsselung bietet.

- WPA3: Der neueste Standard, der zusätzliche Sicherheitsfunktionen bietet.

Passwort Sicherheit:

Hacker haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren, ganze Wörterbücher einschließlich gängiger Kombinationen aus Wörtern und angefügten Zahlen testen oder einmal im Internet veröffentlichte Zugangsdaten bei allen möglichen Diensten durchprobieren. Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen und immer nur für einen Zugang genutzt werden.

Hinzu kommt, dass Passwörter nicht nur zum Schutz von vertraulichen Daten dienen. Ein Beispiel: Inzwischen ist es üblich, dass man sich bei unterschiedlichen Anbietern im Internet jeweils ein Konto oder einen Zugang (Account) anlegen kann. Die Anmeldung an diesem Account wird mit einem Passwort geschützt. Was könnte passieren, wenn sich jemand unter Ihrem Namen dort anmeldet? Wer möchte schon gerne, dass Fremde unter dem eigenen Namen E-Mails verschicken oder teure Waren im Internet ersteigern können?

Grundsätzlich gilt: **Je länger, desto besser**. Für ein gutes Passwort sind Länge und Komplexität entscheidend. Ein kurzes und komplexes Passwort sollte **mindestens acht Zeichen** lang sein und aus **vier verschiedenen Zeichenarten** (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) bestehen. Ein langes und weniger komplexes Passwort sollte mindestens 25 Zeichen lang sein. Bei Verschlüsselungsverfahren für WLAN wie zum Beispiel WPA2 oder WPA3 sollte das Passwort mindestens 20 Zeichen lang sein. Hier sind so genannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren.

Für ein Passwort können in der Regel **alle verfügbaren Zeichen** genutzt werden, beispielsweise **Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+…)**. Manche Anbieter von Onlinediensten machen technische Vorgaben für die verwendbaren bzw. zu verwendenden Zeichen. Wenn Ihr System Umlaute zulässt, bedenken Sie, dass bei Reisen ins Ausland auf landestypischen Tastaturen diese Zeichen eventuell nicht vorhanden sind.

Nicht als Passwörter geeignet sind Namen von Familienmitgliedern, des Haustiers, des besten Freundes, des Lieblingsstars, Geburtsdaten und so weiter. Passwörter sollten zudem nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern wie "asdfgh" oder "1234abcd" bestehen. Manche Anbieter gleichen Passwörter gegen eine sogenannte "black list" ab, in der genau solche nicht geeigneten Passwörter hinterlegt sind. Möchte man sie nutzen, erhält man einen Hinweis, dass das Passwort in dieser Form nicht zugelassen bzw. nicht sicher ist.

Ein Passwort ist sicher, wenn es beispielsweise

- 20 bis 25 Zeichen lang ist und zwei Zeichenarten genutzt werden (beispielsweise eine Folge von Wörtern). Es ist dann lang und weniger komplex.
- 8 bis 12 Zeichen lang ist und vier Zeichenarten genutzt werden. Es ist dann kürzer und komplex.
- 8 Zeichen lang ist, drei Zeichenarten genutzt werden und es zusätzlich durch eine Mehr-Faktor-Authentisierung abgesichert ist (beispielsweise durch einen Fingerabdruck, eine Bestätigung per App oder eine PIN). Dies ist generell empfehlenswert.

WLAN optimieren:

1. Router-Standort: Stelle sicher, dass dein Router an einem zentralen Ort in deiner Wohnung oder deinem Haus platziert ist, um eine gleichmäßige Abdeckung zu gewährleisten. Vermeide es, ihn in Ecken oder in der Nähe von Wänden oder Metallteilen zu positionieren.

2. Interferenzen minimieren: Halte den Router von anderen elektronischen Geräten fern, die Störungen verursachen können, wie Mikrowellen oder schnurlose Telefone.

3. Firmware-Updates: Überprüfe regelmäßig, ob es Firmware-Updates für deinen Router gibt. Diese können Leistungsverbesserungen und Sicherheitsupdates enthalten.

4. WLAN-Kanal wechseln: In dicht besiedelten Gebieten kann es hilfreich sein, den WLAN-Kanal zu wechseln, um Störungen durch Nachbarn zu vermeiden. Tools zur WLAN-Analyse können dir helfen, den besten Kanal zu finden.

5. Passwortschutz: Stelle sicher, dass dein WLAN mit einem starken Passwort geschützt ist, um unbefugten Zugriff zu verhindern, der die Geschwindigkeit beeinträchtigen könnte.

6. Gerätepriorisierung: Einige Router bieten die Möglichkeit, bestimmten Geräten Priorität einzuräumen, was besonders nützlich ist, wenn mehrere Geräte gleichzeitig verbunden sind.

7. Mesh-Systeme: Wenn du ein großes Zuhause hast oder in einem mehrstöckigen Gebäude lebst, könnte ein Mesh-WLAN-System eine gute Lösung sein, um die Abdeckung zu verbessern.

8. WLAN-Repeater: Wenn du in bestimmten Bereichen schwaches Signal hast, kann ein WLAN-Repeater helfen, die Reichweite zu erhöhen.