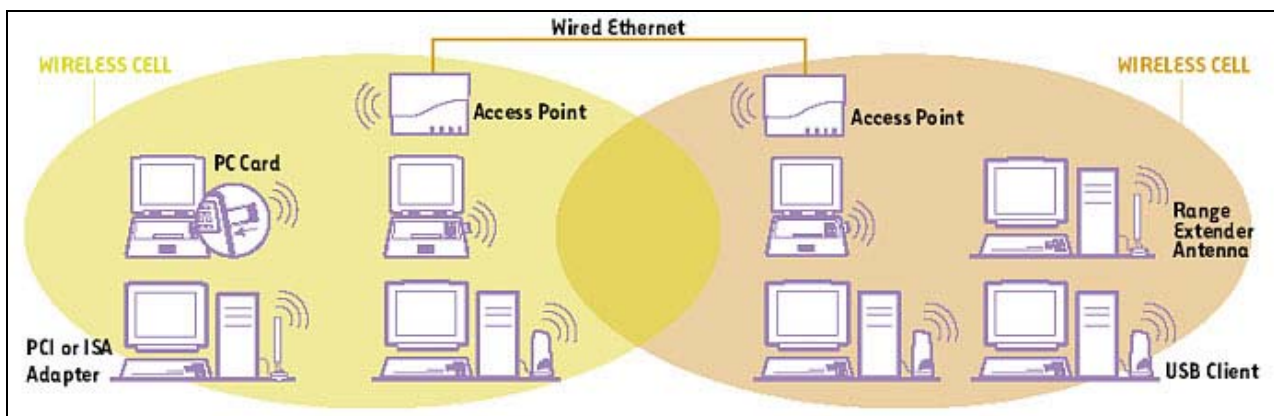


Wireless Local Area Network (WLAN)

Ein WLAN (W = **Wireless**, LAN = **Local Area Network**), d.h. ein drahtloses lokales Netzwerk, ermöglicht den kabellosen Netzzugang mittels Funkwellen. Ein Rechner (i.d.R. ein Notebook) mit einer Funkkarte, erhält in einem durch die Größe des Funkfeldes (Wireless Cell) eingegrenzten Bereich, Zugang zum Netz. Mehrere Klienten können gleichzeitig in einem Funkfeld arbeiten.

Die Anbindung der drahtlosen Klienten erfolgt über einen so genannten Access Point (AP), welche die Verbindung zum "verdrahteten, normalen" Netzwerk (Wired LAN) herstellt. Der AP arbeitet protokoll-unabhängig im 2,4 oder 5 Gigahertz-Frequenzband und erlaubt Geschwindigkeiten von bis zu 54 MBit/s. In Abhängigkeit von der Entfernung zwischen AP und Klient und der Anzahl der Klienten beträgt die Netto-Datenrate oft nur 50 %. Der Access Point selbst ist mit 10, 100 oder 1000 MBit/s ans LAN (Wired Ethernet) angebunden.

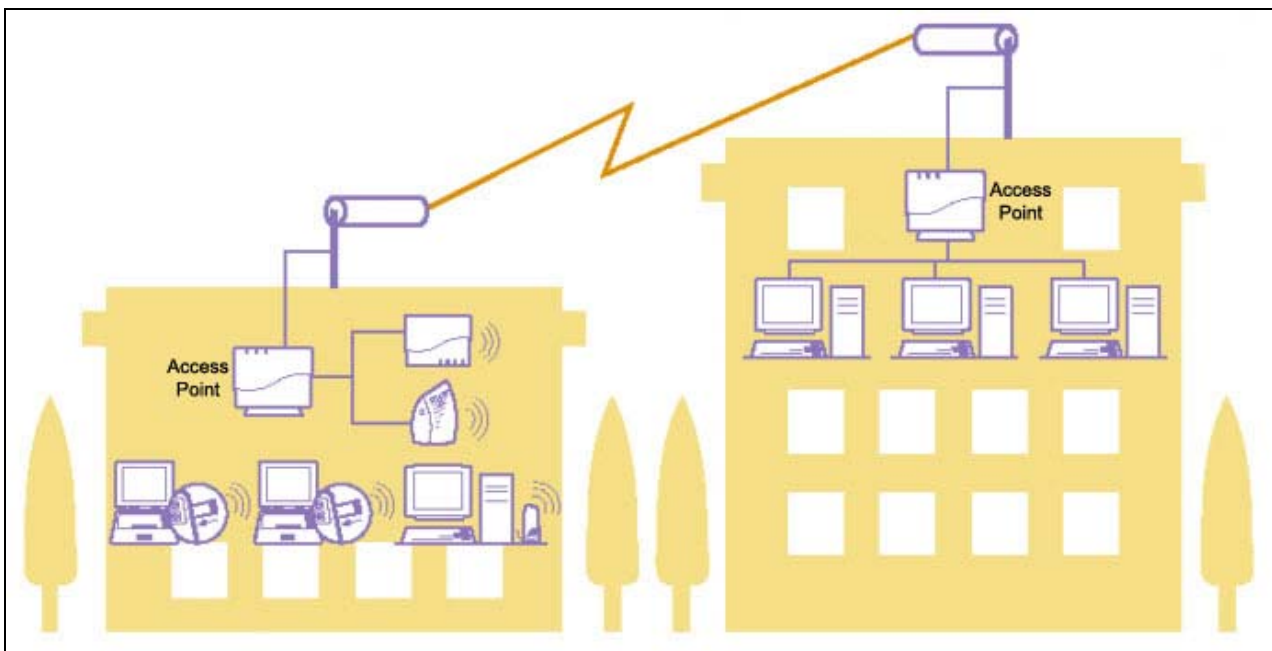


Der Funkbereich, den ein AP abdecken kann, hängt von den physikalischen Gegebenheiten ab. Bei freier Sicht zwischen Klient und AP kann die Entfernung mehrere 100 Meter betragen. In "schlechten" Gebäuden sinkt die Reichweite meist auf unter 50 Meter. Mit zunehmender Entfernung des Klienten vom AP sinken Qualität und Transferrate der Übertragung. Entscheidende, die Qualität der Übertragung beeinflussende Faktoren, sind dabei die verwendeten Baumaterialien der Gebäude, die Zahl der Wände zwischen AP und Klient, deren Dicke und vergleichbare Faktoren.

Um die Entfernungs-Beschränkungen abzuschwächen, können in Gebäuden mehrere APs installiert werden. Diese arbeiten in unterschiedlich konfigurierten Frequenzbereichen und können sich auch überlappen, so dass beispielsweise zwei benachbarte Access Points ein Areal teilweise gemeinsam abdecken. Wechselt ein Klient seinen Standort und kommt in den Bereich eines anderen APs, so schaltet der Klient automatisch auf den anderen AP um, sobald die Übertragungsqualität zu seinem ursprünglichen AP ein gewisses Level unterschritten hat. Dieses Verfahren wird als **Roaming** bezeichnet.

Verbindung zweier Standorte

Der Vollständigkeit halber sei noch erwähnt, dass mittels gerichteter Antennen auch Entfernungen von mehreren Kilometern überbrückt werden können. Diese Technik wird aber in der Regel nur verwendet, um zwei Access Points drahtlos miteinander zu verbinden, beispielsweise um ein entferntes Gebäude mit einem LAN an ein bestehendes Netz anzuschließen.



An der Hochschule Reutlingen werden mit solchen Funkstrecken die Studentenwohnheime an den Campus-Backbone angebunden.

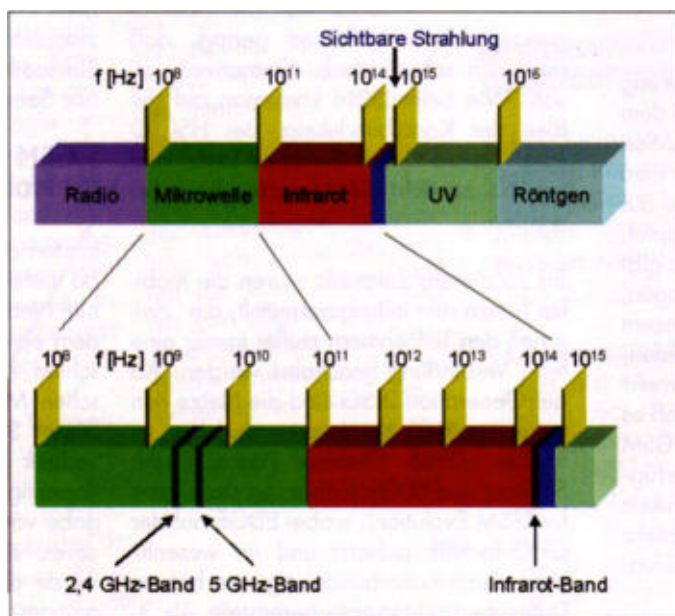
Gesundheitliche Gefährdung

WLAN-Produkte geben wie alle Hochfrequenzgeräte elektromagnetische Hochfrequenzenergie ab. Bei Geräten für das WLAN ist jedoch eine deutlich geringere Emission elektromagnetischer Energie zu verzeichnen als bei anderen Funkgeräten, wie beispielsweise Mobiltelefonen. Da moderne WLAN-Produkte den Richtlinien der HF-Sicherheitsstandards und -empfehlungen entsprechen, besteht beim Gebrauch dieser Funk-Produkte keine Gefährdung für die Gesundheit. Diese Standards und Empfehlungen basieren auf wissenschaftlichen Erkenntnissen und sind das Ergebnis von Beratungen verschiedener Wissenschaftsgremien und -komitees, die sich laufend mit der umfangreichen Forschungsliteratur beschäftigen und diese auswerten.

Heutige und zukünftige Standards

Wie bereits beschrieben, geschieht die Datenübertragung beim WLAN mittels Funkwellen. Dies macht es nötig, dass wie bei Handys oder Radiosendern die verwendete Frequenz sowie die Übertragungsverfahren festgelegt sind. Genauso wie 100Base-TX (Twisted Pair) oder 1000Base-SX (LWL), wurde auch dieser Netzwerkstandard von der Organisation "Institute of Electrical and Electronic Engineers (IEEE)" genormt.

Der seit 1997 existierende Standard **IEEE-802.11** ermöglicht eine Datenübertragung mit Bandbreiten von 1 bis 2 MBit/s und sieht unter anderem eine Übertragung im weltweit verfügbaren und lizenzfreien ISM-Band (Industrial, Science, Medical) mit Frequenzen von 2,4 bis 2,485 Gigahertz vor. Das 2,4-GHz-Frequenzband darf in den meisten Ländern der Welt bis 100 Milliwatt Sendeleistung vollkommen lizenz-, gebühren- und genehmigungsfrei benutzt werden.



Die heutigen drahtlosen Netzwerke der nächsten Generation, mit weitaus höheren Bandbreiten, sind in den Standards IEEE-802.11a und IEEE-802.11b genormt. Der schon einige Zeit im Einsatz befindliche Standard **IEEE-802.11b** arbeitet dabei im selben Frequenzband wie IEEE-802.11, erlaubt durch ein spezielles Übertragungsverfahren jedoch Geschwindigkeiten von bis zu 11 MBit/s. Der ebenfalls im Jahr 1999 genormte Standard **IEEE-802.11a** operiert im 5 GHz-Bereich und bietet Bandbreiten von bis zu 54 MBit/s, Komponenten werden jedoch erst seit 2003 angeboten.

Auf Grund von nationalen Besonderheiten, beispielsweise wegen des vom Militär verwendeten 5 GHz Frequenzbandes, wurden die beiden Erweiterungen **IEEE-802.11g** und **IEEE-802.11h** eingeführt. Zukünftig wird es auch noch **IEEE-802.11n** geben.



Die Standards im Überblick:

Standard	Frequenz [GHz]	Bruttorate [MBit/s]	Bemerkungen
802.11	2,4	1-2	Funk-LAN Spezifikation des IEEE im ISM-Band. Veraltet, wird praktisch nicht mehr benutzt!
802.11a	5	54	In Europa und Deutschland ist die Benutzung derzeit nur mit Auflagen erlaubt.
802.11b	2,4	11	Hohe Marktdurchdringung; abwärtskompatibel zu 802.11.
802.11g	2,4	54	In Europa favorisiert; abwärtskompatibel zu 802.11 und 802.11b.
802.11h	5	54	Anpassung des Standards 802.11a für den Einsatz in Europa.
802.11n	2,4	540	Neuer Standard in der Entwicklungsphase. Erste Hardwareprodukte seit 2007 verfügbar.
802.11i	-	-	802.11-Erweiterung der Sicherheits- und Authentifizierungs-Mechanismen.
802.1x	-	-	Spezifikation eines Port-basierten Authentisierungs-Mechanismus durch IEEE.

Neben den WLAN-Standards, findet sich in vorstehender Tabelle auch der Standard IEEE-802.1x. Er definiert ein von WLAN unabhängiges Zugangs-Verfahren zum Netz auf Benutzerebene. Mehr dazu ist im nächsten Kapitel zu finden.



Zugangskontrolle und Abhörsicherheit

Lange Zeit galten WLANs als sicher in Bezug auf nicht autorisierten Zugriff und Abhören, vorausgesetzt, die standardmäßig implementierten Features wurden fachgerecht konfiguriert. Obwohl schon länger bekannt war, dass es prinzipiell möglich ist, die für die Sicherheit relevanten Parameter aus den mittels Funk übertragenen Paketen zu ermitteln, standen die dazu nötigen Mittel (beispielsweise "Wireless Sniffer") und die Kenntnis, wie aus den abgefangenen Paketen die relevanten Parameter extrahiert werden, nicht der Allgemeinheit zur Verfügung. Dies hat sich grundlegend geändert. Abhör-Software für PCs mit Wireless-Karte ist inzwischen kommerziell erhältlich und die Verfahren zur Paket-Analyse sind in diversen Veröffentlichungen zugänglich.

Im folgenden werden die einzelnen Sicherheits-Features und ihre Schwächen, sowie Lösungen für eine bessere Sicherheit beschrieben:

- **SSID (System Set Identifier) oder WNN (Wireless Network Name)**
Ursprünglich diente die SSID zur logische Strukturierung von Funknetzen. Da sich nur ein Klient mit passender SSID an einem Access Point anmelden konnte, wird die SSID auch unter dem Aspekt der Zugangskontrolle gesehen. Die schützende Wirkung der SSID ist aber in letzter Konsequenz gering, da die SSID auf dem Klienten im Klartext eingetragen wird.
- **ACL (Access Control List)**
Die Access Points werden für ACL so eingestellt, dass sie die Ethernet-Adresse (MAC address), der in den PCs verwendeten Funkkarten, als zugriffsberechtigt abfragen. Bei der Verbindungsaufnahme eines Klienten zu einem AP, schaut der Access Point in seiner Konfiguration oder fragt bei einem Server (mit beispielsweise RADIUS) nach, ob diese Karte zugelassen ist. Ist das nicht der Fall, findet keine Kommunikation statt, die über den AP hinausgeht.
- **WEP (Wired Equivalent Privacy)**
WEP stellt ein Verfahren zur Verschlüsselung der mittels Funk zwischen dem AP und der Funkkarte übertragenen Datenpakete dar. Je nach verwendeter PC-Karte, werden die Pakete mit Schlüsseln von 64, 128 oder 152 Bit verschlüsselt. Dabei werden jeweils 24 Bit, dem so genannten Initialisierungsvektor (von Datenpaket zu Datenpaket veränderte zufällige Zahl), von der Hardware und der Rest (40, 104, 128 Bit) vom Anwender definiert. Bei der Verschlüsselung selbst handelt es sich um ein symmetrisches Verfahren (RC4-Algorithmus), mit den bekannten Nachteilen. Durch das Sammeln von Schlüsselpaaren sind *Known-Plaintext-Angriffe* möglich. Es gibt frei erhältliche Programme, die sogar ohne vollständigen Paketdurchlauf in der Lage sind, einen schnellen Rechner vorausgesetzt, das Passwort zu entschlüsseln.
Der weitere Kommunikationsweg zwischen AP und dem Ziel des IP-Paketes ist unverschlüsselt, es sei denn, der Anwender selbst sichert seine Kommunikation durch entsprechende bekannte Protokolle oder Mechanismen (ssh, https etc.) ab.



➤ **WPA (Wi-Fi Protected Access)**

WPA ist der Nachfolger des WEP und ist eine Teilmenge des neuen Sicherheitsstandards 802.11i. Er bietet eine erhöhte Sicherheit durch die Verwendung von **TKIP** (Temporal Key Integrity Protocol) und gilt zur Zeit als nicht zu entschlüsseln, solange man bei der Einrichtung keine trivialen Passwörter verwendet, die über eine Wörterbuch-Attacke geknackt werden können. Empfehlung: Mit einem Passwortgenerator Passwörter erzeugen, die Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen enthalten und nicht kürzer als 32 Zeichen sind! TKIP verwendet wie WEP den RC4-Algorithmus für die Verschlüsselung. Der Schlüssel ändert sich temporär - daher auch der Name des Protokolls, und zwar immer dann, wenn ein Datenpaket von 10 KB übertragen wurde. Der temporäre Schlüssel wird im RC4-Algorithmus benutzt.

➤ **WPA2 (Wi-Fi Protected Access 2)**

Die zweite Version von WPA ist das Äquivalent der WiFi zu 802.11i, das mit dem Verschlüsselungsalgorithmus **AES** (Advanced Encryption Standard) arbeitet und in neueren Geräten meist unterstützt wird.

AES ist ein symmetrisches Kryptosystem, das mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit arbeitet und gilt momentan als das sicherste Verfahren.

SSID und **ACL** gewähren also eine Zugangskontrolle zum Netz, **WEP**, **WPA** und **WPA2** sorgt für Abhörsicherheit durch Verschlüsselung. Solange diese Parameter nicht explizit bekannt sind, ist jedes Wireless LAN relativ sicher. Analysiert man jedoch die mit einem Software-Tool aufgefangenen Funkpakete, lassen sich die MAC-Adressen der aktiven Klienten sowie die SSID leicht ermitteln, da diese Parameter unverschlüsselt im Funk übertragen werden. Somit ist bereits ein Zugang zum WLAN über eine Anmeldung am Access Point möglich. Aus einer (allerdings großen) Anzahl an Datenpaketen kann auch der WEP-Schlüssel durch einen Algorithmus rekonstruiert werden.

Die beiden Standards IEEE-802.11i und IEEE-802.1x bieten ausreichende Sicherheit, sowohl im Wired als auch im Wireless LAN. Der Standard **IEEE-802.11i** definiert einen sichereren Schlüssel für die Verschlüsselung der Datenpakete (WPA bzw. WPA2). Der Standard **IEEE-802.1x** definiert ein von Funk unabhängiges Authentifizierungs-Verfahren auf Benutzerebene, das über den Zusatz EAP (Enhanced Authentication Protocol) eine sichere und dynamische Vergabe der WEP-Schlüssel erlaubt. Die Authentifizierung wird über die Einbindung eines Authentifizierungs-Servers (wie beispielsweise RADIUS und Kerberos) realisiert, die dynamische Schlüsseländerung bewirkt, sodass die Gültigkeitsdauer eines Schlüssels nicht ausreichend für dessen Rekonstruktion ist.

Als Fazit daraus folgt, dass es mit entsprechenden Mitteln immer möglich ist, sich alle Daten für den Zugang zum Funknetz und die Entschlüsselung der übertragenen Inhalt zu besorgen. Daraus resultiert, dass jedes WLAN bezüglich Sicherheit dem Internet vergleichbar ist. Es sind also zusätzliche Sicherheitsmassnahmen erforderlich, wenn Daten zu schützen sind und der nicht autorisierte Zugang zum eigenen Netz verhindert werden soll. Solche Techniken existieren und sind von der WLAN-Technik unabhängig.