WLAN (Wireless LAN, Wi-Fi) IEEE 802.11:

Hier werden elektromagnetische Wellen statt Strom zur Übertragung verwendet. Für die entsprechenden Normierungen sorgt die IEEE-Arbeitsgruppe 802.11, welche die Layer 1 und 2 für diese Funktechniken definiert. Die Normen selbst werden mit einem angehängten Buchstaben spezifiziert (z.B. 802.11b, 802.11i usw.) und nach z mit 2 angehängten Buchstaben (wie bei den KFZ-Kennzeichen, z.B. 802.11ac). Für die Übertragung wurden 2 Frequenzbereiche festgelegt:

- **2,4 GHz (genauer 2,4 GHz – 2,48 GHz):** Das ISM-Band (Industrial, Scientific and Medical Band) ist in Europa schon lange für den Funkverkehr weitgehend freigegeben worden. Es darf praktisch von allen Funkgeräten verwendet werden (Wlan, Bluetooth, Videoübertrager, Babyphone, Mikrowelle, Fernsteuerungen etc.). Deshalb wird es vor allem in Europa überwiegend eingesetzt. Wegen der starken Nutzung und des engen Frequenzbereichs ist die Gefahr für Kollisionen sehr hoch.

- **5 Ghz (5,2 GHz - 5,8 GHz):** Dieser Frequenzbereich war in den USA schon lange freigegeben, in Europa erst später. Dadurch ist er eher in den USA als in der EU verbreitet. Auch ist die Sendeleistung in der EU stärker limitiert als beim ISM-Band, wodurch sich die geringere Verbreitung hierzulande erklärt. Wegen der zunehmenden Überlastung des ISM-Bandes wird dieser Frequenzbereich aber auch in EU gerne als Alternative eingesetzt. Die neueste Übertragungsnormen (802.11ac, ax) nutzen ausschließlich diesen Frequenzbereich.

Ein WLan-Gerät mit nur einer (internen!) Empfangs-Sendeanlage kann nur einen dieser zwei Bereiche bedienen. Erst mit 2 eingebauten Sende-/Empfangseinheiten ist die Nutzung beider Frequenzbereiche möglich (Dual-Band-Geräte). Manche Geräte können trotzdem nur eine dieser Einheiten wahlweise nutzen, andere nutzen beide simultan. Die Antennen werden natürlich für beide Frequenzbereiche gemeinsam benutzt.

IEEE 802.11 b,g:

Diese Normen beschreiben die Nutzung des 2,4 GHz ISM Bandes mit Datenraten von maximal 11 Mbit/s (802.11b) bzw. bis maximal 54 Mbit/s (802.11g). Der g-Standard ist prinzipiell abwärtskompatibel zum b-Standard und kann „gemischt“ betrieben werden. Jede Funkzelle belegt einen Funk-Kanal mit 25 MHz Breite (20 MHz Nutzung und 5 MHz Abstand), es sind insgesamt 14 Kanäle definiert. Die einzelnen Kanäle sind 25 MHz „breit“ (20 MHz Nutzbereich und oben und unten 2,5 MHz Randbereich) und um 5 MHz versetzt, z.B. Kanal 1: 2,400 GHz – 2,425 GHz, Kanal 2: 2,405 GHz – 2,430 GHz usw. Man sieht, dass sich benachbarte Kanäle stark überlappen, erst bei einem Unterschied von 5 Kanalnummern findet überhaupt keine Überlappung statt, bei einem Unterschied von 4 Kanalnummern

überlappen sich nur mehr die Randzonen. Optimale Nutzungsstrategien sind daher 1-6-11, oder 2-7-12…, brauchbar sind auch 1-5-9-13. Schlecht ist z.B. die Wahl von Kanal 3 oder 4, da dadurch viele benachbarten Kanäle blockiert werden. Kommt es zu Frequenzkollisionen, so leiden alle Beteiligten unter Paketverlusten und das resultiert in einer Verringerung des Durchsatzes.

IEEE 802.11 a:

Diese Norm definiert Kanäle mit 20 MHz Nutzbreite im 5GHz-Bereich und einer Übertragungsgeschwindigkeit bis maximal 54Mbit/s. Durch den größeren Frequenzbereich lassen sich mehr Kanäle parallel ohne Kollisionen benutzen. Die definierten Kanalnummern lassen sich alle kollisionsfrei nutzen, da sie in Viererschritten angeordnet sind (36, 40 , 44 …).

IEEE 802.11 n (= WiFi 4):

Dieser Standard wurde 2009 beschlossen und definiert Übertragungsraten bis hin zu 600 Mbit/s. Neben besseren „Datenverpackungs-Algorithmen" (Modulation) und Verbreiterung der Funkkanäle auf das Doppelte (40 MHz) ist vor allem die MIMO-Technik (Multiple Input-Multiple Output) für die nominelle Durchsatz-Steigerung verantwortlich. Man versucht über gleichzeitig und unabhängig betriebene Antennen bis zu 4 getrennte Datenverbindungen (sog. Streams) zwischen den Teilnehmern aufzubauen: Die Verbesserungen kann man folgendermaßen quantifizieren:

- Verbesserte Modulation gegenüber 801.11g(a): von 54 MBit/s auf 75 Mbit/s (40% mehr).
- Doppelt so breite Frequenzbänder: von 20 MHz auf 40 MHz (100% mehr)
- Bis zu 4 Streams (300% mehr)

Alle 3 Maßnahmen zusammen würden den Durchsatz theoretisch um den Faktor 1.4 * 2.0 * 4.0 = 11.2 steigern, woraus sich die 600 Mbit/s ergeben. Verzichtet man auf das größere Frequenzband und verwendet nur 2 statt 4 Streams, wäre der maximale Durchsatz 150 Mbit/s. Dieser Wert ist eher realistisch, weil Endgeräte selten mehr als 2 Antennen besitzen und somit maximal 2 Streams möglich sind. Außerdem findet man im ISM-Band kaum freie Kanäle mit 20MHz Breite, erst recht nicht mit 40MHz Breite. Es kann in der Praxis durchaus sein, dass der Verzicht auf 40MHz eine Durchsatzsteigerung bewirkt. Im 5 5GHz-Bereich stehen die Chancen gut, einen freien 40 MHz Kanal zu finden.

802.11n besitzt als einzige Norm **keinen vorgegeben Frequenzbereich**, die Geräte können entweder das 2,4 GHz oder das 5 GHz Band oder beide benutzen. Dummerweise erkennt ein Käufer deshalb an der Bezeichnung 802.11n nicht, für welche Frequenzen das Gerät geeignet ist, sodass es durchaus möglich ist, inoperable Kombinationen anzuschaffen. Hier nützt nur ein Blick auf alle übrigen unterstützten Normen:

802.11 b,g,n da b und g nur 2,4 GHz benutzen, gilt n wohl auch nur für diesen Bereich
802.11 a,n da a nur 5 GHz benutzt, gilt n wohl auch nur für diesen Bereich
802.11 a,b,g,n hier liegt wohl eine Dualband-Konfiguration vor.

IEEE 802.11 ac (=WiFi 5, Gigabit Wlan):

Dieser 2013 beschlossene Standard ermöglicht theoretische Übertragungsraten von (derzeit) bis zu ca. 5Gbit/s. Er arbeitet ausschließlich im 5GHz Bereich und verwendet gegenüber 802.11n eine verbesserte Modulation, verbreiterte Frequenzbänder (80 oder sogar 160 MHz) sowie eine verfeinerte MIMO-Technik mit bis zu 8 parallelen Streams, sodass man auf diesen absurd hohen Durchsatz kommt.

Aber selbst im 5 GHz Bereich kann es eng werden: Der obere Teil dieses Frequenzbereiches ist eigentlich für Radargeräte der Wetterdienste reserviert und darf nur dann privat genutzt werden, wenn es keine Wetterradars gibt. Also müssen alle Geräte, die auch diesen reservierten Bereich nutzen wollen, eine automatische Erkennungs- und Ausweichschaltung besitzen (DFS = Dynamic Frequency Selection). Billigere Geräte ersparen sich diese Schaltung und dürfen daher nur den unteren Teil der 5GHz-Frequenzen verwenden, wo nur ein solcher 160 MHz Kanal möglich ist. Erst mit DFS lassen sich mehrere 160 MHz breite Kanäle gleichzeitig ohne Überlappung nutzen.

Da nur wenige Clients mit mehr als 2 Antennen ausgestattet sind, hat man diese Norm nach und nach um Multi-Client-Fähigkeiten MU-MIMO erweitert (MultiUser MIMO): Der Access Point verwendet z.B. 2 Antennen für Client 1 und gleichzeitig die anderen 2 für Client 2 oder er verwendet jeweils nur eine Antenne für bis zu 4 Clients gleichzeitig. Die neueste Technik heißt Wave 2 und erlaubt den Access Points, 2 getrennnte Sendeanlagen im 5GHz Band gleichzeitig zu betreiben (dafür sind dann 6 oder gar 8 Antennen nötig, die Accesspoints ähneln immer mehr einem Igel).

IEEE 802.11 ax (WiFi 6, 10/2018):

Gegenüber WiFi 5 wurden die theoretischen Zahlen weiter erhöht. Die eigentlichen Verbesserungen geschahen jedoch unter der Oberfläche: dieser Standard verspricht eine bessere Ausnutzung der Frequenzen, höhere Stabilität, verbesserte Energie-Effizienz sowohl im 5 GHz als auch im 2,4 GHz-Bereich. Außerdem wurden Techniken für die Vernetzung größerer räumlicher Bereiche in den Standard integriert (Mesh-Wlans). Ferner können optional noch breitere Funkkanäle verwendet werden, wodurch Durchsatz und Latenz (Ping-Zeit) verbessert werden.

IEEE 802.11 ad (Multi-Gigabit Wlan):

Im Gegensatz zu allen bisherigen WLan-Normen sendet 802.11ad im 60 GHz Bereich und stellt somit keine Konkurrenz zu herkömmlichen Drahtlosnetzen dar. Die Geschwindigkeit soll mehrere Gbit/s erreichen und die Reichweite auf wenige Meter beschränkt sein. Haupteinsatzgebiet wird die drahtlose Übertragung von hochauflösenden Videos zu Projektoren und TVs sein. Geräte mit diesem Standard sind noch wenig verbreitet.

Was hat der Anwender von diesen Dingen?

In der Praxis hat ein Anwender Geräte mit völlig unterschiedlicher Technik. Zu einem relativ neuen Handy, das Wifi-5 tauglich ist, gibt es Spielkonsolen, TV, Kindles, die nicht einmal 802.11n beherrschen (also keine parallelen Streams aufbauen können). Was nützt dann ein teurer Wifi 5 oder 6 Router mit 8 Antennen? Erstaunlicherweise sehr viel, denn einige der Verbesserungen lassen sich in der Tat auch mit alten Endgeräten nutzen: Moderne Router lokalisieren ihre Klienten im Raum und verwenden dann nur jene Antenne(n) zur Kommunikation für ein bestimmtes Endgerät, die den bestmöglichen Empfang bietet. So entsteht eine Art Richtfunk (Beam Forming), der sehr viel effizienter ist als eine Rundum-Abstrahlung. Klienten in unterschiedlichen Richtungen werden gleichzeitig über verschiedene Antennen bedient, sodass sowohl der Einzeldurchsatz als auch der Gesamtdurchsatz deutlich gesteigert wird. Die vielen Antennen lassen sich ausrichten und ermöglichen dadurch auch die Abdeckung von Räumen, für die vorher ein eigener Router eingesetzt werden musste. Deshalb ist es sehr sinnvoll, den WLan-Router zu modernisieren, auch wenn die angeschlossene Gerätschaft selbst alt ist.

Einige Begriffe erklärt

SSID oder ESSID (Service Set Identifier): Das ist die alphanumerische Bezeichnung einer Funkzelle. Benutzen 2 Geräte denselben Namen für die SSID, so gehören sie zur selben Funkzelle (auch wenn das nicht beabsichtigt ist). Es empfiehlt sich also, den Standardnamen (wie NETGEAR oder Linksys) auf jeden Fall durch eine Eigenkreation zu ersetzen. Die SSID ist übrigens **Case-Sensitiv**. Jeder Möchtegern-Netzwerkguru empfiehlt, die Ankündigung der SSID aus "Sicherheitsgründen" abzuschalten, da man dann "für die Hacker unsichtbar" bleibt. Das entspricht etwa der Entfernung der eigenen Hausnummer von der Haustüre, um von Dieben nicht mehr gefunden zu werden. Eine absolut sinn- und nutzlose Maßnahme, die den Wlan-Betrieb nur erschwert und keineswegs sicherer macht. Viel besser ist die Wahl einer SSID, die Rückschluss auf den Betreiber zulässt. Dann dürfen aber als Passwort nur nichtpersönliche Begriffe (also nicht Name der Mutter, Freundin, Kinder) verwendet werden, um das Erraten schwieriger zu machen. Manche Accesspoints können auch mehrere SSIDs gleichzeitig verwalten (z.B. eine für Gäste mit einfachem Passwort, welches oft gewechselt wird, und eine andere für die Eigentümer).

Kanalwahl bzw. Frequenzwahl: Hier stellt man ein, wie breit der Nutzungskanal (bei n oder ac Betrieb) sein soll und welche Frequenzen er nutzen soll. Hier kann man entweder einer Automatik vertrauen (oder man muss es im Falle DFS auch), oder man konfiguriert das manuell, nachdem man mit geeigneten Programmen oder Apps fürs Handy die

Nachbarschaft auf WLans untersucht. Vor allem den am besten empfangbaren WLans sollte man im Sinne des Datendurchsatzes unbedingt ausweichen. Hat man aber Nachbarn mit Automatik (wieder einmal ein Beispiel, wie man intelligenten Handbetrieb durch sinnlose Automatiken ersetzt), muss man selbst wohl oder übel auch auf die Automatik setzen, da sich die genutzten Frequenzen ständig ändern.

Effektive Übertragungsgeschwindigkeit: Diese hängt neben der eingesetzten Technik (a,g,n,ac, ax) vor allem von der Empfangsgüte ab. Man kann die theoretischen Maximalgeschwindigkeiten der Verfahren nie überschreiten, meist wird man sogar deutlich darunter bleiben. Wenn der Empfang zu schlecht ist, drosseln die Stationen automatisch ihr Tempo und schalten auf robustere und langsamere Verfahren zurück. Besonders deutlich wirken sich große Entfernung und Funk-Hindernisse zwischen den Stationen aus (z.B. Stahlbetondecken). Die erzielte und angezeigte Verbindungsgeschwindigkeit (z.B. 180 Megabit/s) bedeutet ebenfalls nicht, dass der Datendurchsatz in ähnlicher Größenordnung liegt. Zum einen werden nicht nur Nutzdaten sondern auch Kontrollinformationen übertragen, zum anderen betrifft das nur die Strecke zum Accesspoint und nicht zum eigentlichen Kommunikationspartner. Ist dieser ebenfalls an dieses WLan angebunden, so müssen die Daten ja beide Strecken nacheinander durchlaufen, der Durchsatz wird daher mindestens halbiert. Ist der Partner im Internet, so ist meist die Internetanbindung zum Internet Service Provider (ISP) der eigentliche Flaschenhals.

adhoc Verbindungen vs. Infrastruktur-Modus: Eine adhoc-Verbindung ist eine Punkt zu Punkt Funkzelle, in der alle Teilnehmer gleichberechtigt sind und jeder jede paarweise Verbindung konfigurieren muss. Pakete werden direkt vom Sender zum Ziel gesendet. Beim Infrastruktur-Modus gibt es eine zentrale Instanz (den Access-Point), der die Funkzelle aufbaut und verwaltet. Er regelt den Zugang zur Funkzelle und auch die Kommunikation in der Funkzelle. Sämtliche Pakete werden nur zwischen dem Access-Point einerseits und den Teilnehmern andererseits ausgetauscht. Ein Teilnehmer-Teilnehmer-Paket geht infolgedessen mindestens 2 Mal über den Äther. adhoc-Verbindungen werden gerne für die Kommunikation mit mobilen Endgeräten verwendet (z.B. Gopro, Drohnen)

WLAN-Router: Diese für den Heimgebrauch gebauten Geräte sind praktische Kombinationsgeräte bestehend aus einem Internet-Access-Router mit NAT, einem Switch (zumeist mit 4 Anschlüssen) und einem WLan-Access-Point. Diese PlugNPlay-Geräte sind schon für die Benutzung eines privaten Netzwerks als Heimnetzwerk vorkonfiguriert und liefern per DHCP IPv4-Adressen an die angeschlossenen internen Geräte aus. Allenfalls ist noch eine Konfiguration des Internetzugangs zum Providernetzwerk erforderlich (z.B. per ADSL, ADSL2, DOCSIS3 (TV-Kabel) oder UMTS (3g Handynetze), LTE (4g Handynetze)). Moderne Varianten beherrschen auch schon den IPv6 Betrieb zusätzlich.

Verschlüsselung: Da Funkwellen sich relativ weit ausbreiten können, ist der Zugang zum Funknetz auch aus nichterwünschten Bereichen möglich (z.B. Hacker vor dem Haus oder in der Nachbarwohnung!). Dagegen hilft der Einsatz von Verschlüsselung zur Authentisierung (Zugangskontrolle) und zur Datensicherung. Im einfachsten Fall wird ein einziges Passwort für beide Zwecke verwendet. Dieses Passwort muss dem Accesspoint und auch allen Benutzern bekannt sein (PSK: PreShared Key). Die Datenpakete werden mit diesem Passwort (oder daraus abgeleiteten Schlüsseln) verschlüsselt. Je nach Verschlüsselungs-Verfahren nennt man das WEP (sehr unsicher, sollte nicht mehr verwendet werden), TKIP (etwas besser, aber auf RC4 basierend, was von der NSA angeblich in Echtzeit entschlüsselt werden kann), WPA (das ist keine offizielle Norm, daher auch nicht mehr empfehlenswert) oder WPA2 = 802.11i (das beste derzeitige Verfahren, wenn man als Verschlüsselungsverfahren AES einstellt!). Grundsätzlich kann man auch die Authentisierung von der Datensicherheit trennen. Das geschieht z.B. bei dem WPA2-Enterprise Verfahren. Die Authentisierung erfolgt mittels des 802.1X- Verfahrens gegen einen RADIUS-Server (Remote Authentication DIalup User Service): Der Benutzer tippt seinen Benutzernamen und sein Passwort in eine Eingabemaske ein (kein gemeinsamer PreShared Key!), der RADIUS-Server bestätigt die Gültigkeit dieser Daten und authentisiert damit den User. Jetzt wird vom Accesspoint ein neuer Schlüssel erzeugt und nur mehr für die Kommunikation mit diesem User verwendet. Dadurch kann jeder WLan-Teilnehmer nur mehr die für ihn selbst bestimmten Pakete lesen, alle übrigen Pakete derselben Funkzelle bleiben geheim. Die Uni Innsbruck betreibt mittlerweise ihre SSIDs UIBK sowie EDUROAM mit diesem Verfahren. Während ersteres die User nur gegen die Uni Innsbruck validiert, ist letzteres auch für Angehörige von Fremduniversitäten nutzbar (ROAM für Roaming). Umgekehrt haben Innsbrucker Uni-Mitglieder auch Zugang an Partneruniversitäten. All das funktioniert aber nur, wenn man diese WLan-Verbindung exakt nach Vorgabe konfiguriert. Ein falsches Verfahren hier oder ein fehlendes Häkchen da verhindert oft genug eine erfolgreiche Verbindung.

Mittlerweile ist der Standard WPA3 (2018) erschienen, der alles (vieles) besser als WPA2 machen soll. Das Hauptproblem ist, dass ALLE angeschlossenen Endgeräte diesen Standard beherrschen müssen, bevor man ihn aktivieren kann.