



Wireless LAN

nach IEEE 802.11

Entstanden im Rahmen der Vorlesung LNWN II
im Sommersemester 2002



INHALTSVERZEICHNIS

1	WIRELESS LAN NACH DEM IEEE 802.11 STANDARD	3
1.1	IEEE 802.11	3
1.2	IEEE 802.11B	3
1.3	IEEE 802.11A	3
2	NETZWERKTOPOLOGIEN	5
2.1	AD-HOC NETZWERK	5
2.2	INFRASTRUKTUR NETZWERK	6
3	SICHERHEIT	7
3.1	WEP (WIRED EQUIVALENT PRIVACY)	7
3.2	AUTHENTIFIZIERUNG	7
3.3	VIRTUAL PRIVATE NETWORK (VPN)	7



1 Wireless LAN nach dem IEEE 802.11 Standard

1.1 IEEE 802.11

1997 hat IEEE mit dem Standard 802.11 eine erste Version eines Standards für Wireless LANs (W-LANs) verabschiedet. Die IEEE 802.11 arbeitet im 2,4 GHz ISM¹-Band und zukünftige leistungsfähigere Versionen werden im 5GHz ISM-Bereich arbeiten.

1.2 IEEE 802.11b

Wireless LANs nach **IEEE 802.11b** mit **11 Mbit/s** Datenrate und Nutzung des **2.4 GHz** Bandes sind inzwischen etablierte und akzeptierte Technologien. Nach Verabschiedung des Standards IEEE 802.11a in 2001 und der Verfügbarkeit erster Produkte die auf diesem Standard basieren, wird jetzt auch der Weg zu grösseren Bandbreiten bis **54 Mbit/s** und dem alternativen **5 GHz** Band geöffnet. Für den Anwender stellt sich heute die Frage, welche Technologien in der Praxis bereits einsetzbar sind, welche Vor- und Nachteile sie gegenüber den etablierten Technologien besitzen und wie ein Migrationspfad bzw. eine Koexistenz aussehen könnte.

1.3 IEEE 802.11a

Wireless LANs nach diesem Standard arbeiten im **5 GHz** Frequenzband und erlauben Datenraten bis **54 Mbit/s**. Das verwendete Modulationsverfahren ist **OFDM** (Orthogonal Frequency Division Multiplexing), das sich von dem in 802.11b verwendeten Verfahren DSSS (Direct Sequency Spread Spectrum) völlig unterscheidet.

Produkte, die auf diesem Standard basieren sind heute **in Europa nach ETSI nicht zulassungsfähig**.

Der Grund hierfür liegt darin, dass bestimmte Teile des vom Standard definierten Frequenzbandes in Europa von Funkdiensten und RADARs ebenfalls benutzt werden, wodurch gegenseitige Störungen möglich sind.

Es gibt Bestrebungen, durch zusätzliche Methoden zur effektiven Nutzung des Frequenzbandes diese Interferenzen zu vermeiden. Dies würde bedeuten, dass Wireless LANs bei Detektion von Interferenzen automatisch ein Frequenz- und Leistungs-Management durchführen.

¹ ISM – Industrial Scientific and Medical nennt man den Frequenzbereich zwischen 2,4 GHz und 2,483 GHz. Dieser Frequenzbereich steht nahezu weltweit zur Verfügung und kann für unlicenzierte Übertragungen gebührenfrei genutzt werden



Gegenüberstellung der Standards:

Zunächst einmal besticht die hohe Datenrate von 54 Mbit/s, die mit Produkten nach 802.11a erreicht werden können.

Da aus physikalischen Gründen die Funkausbreitung in höheren Frequenzbereichen stärker bedämpft wird, sind mit 5 GHz-Technologien grundsätzlich **geringere Reichweiten als mit 2.4 GHz-Technologien** erzielbar. Die höhere Dämpfung macht sich in der Praxis weniger im Freifeld, wohl aber bei der Durchdringung von Hindernissen wie Wänden bemerkbar. Dies bedeutet, dass speziell in Gebäuden die Funkzellen in 5 GHz Wireless LANs deutlich kleiner als in 2.4 GHz LANs sind. Um vergleichbare Abdeckungen erzielen zu können, werden deshalb mehr Funkzellen benötigt, also eine höhere Dichte an Access Points.

Technologien im 5 GHz Frequenzband bieten den Vorteil, dass hier weniger Störungen im Funkbereich zu erwarten sind, da das entsprechende Band nur für Wireless LANs zugelassen und „noch ungenutzt“ ist.

Die folgende Tabelle zeigt einen Vergleich einiger Key-Parameter:

Parameter	802.11b	802.11a
Datenrate (Mbps)	11	54
Durchsatz (Mbps)	5,5	28
Max Zellenradius	57	12
Kosten pro Funkmodul	100%	120%
Kosten für Infrastruktur bei gleicher abzudeckender Fläche und voller Datenrate	100%	2250%
Zulassung	global	US, JP, EU ²

Produkte nach 802.11a sind bereits auf dem Markt verfügbar, allerdings wie schon erwähnt nicht für den Betrieb nach ETSI (also in Europa) zugelassen.

Da 802.11a ein anderes Modulationsverfahren als 802.11b benutzt bzw. einen ganz anderen Frequenzbereich, ist eine Interoperabilität zu 802.11b im Sinne einer Abwärtskompatibilität zunächst nicht möglich. Wohl aber eine Koexistenz, da keine direkten Wechselwirkungen möglich sind.

Es wird jedoch erwartet, dass verschiedene Hersteller **Dual Band Module** anbieten werden, die verschiedene Technologien abdecken.

Fazit:

802.11b ist eine bewährte und ausgereifte Technologie, bei der seit dem Eintritt in die Phase des Massenmarkts mit stetig weiter sinkenden Preisen zu rechnen ist. Aus Zulassungsgründen (802.11a) wird mit den Alternativen, die höhere Datenraten bieten, in Europa nicht vor Ende 2002 zu rechnen sein. Generell scheint eine globale Regulierung, wie sie für den 2.4 GHz Bereich existiert, für Technologien im 5 GHz Band

² Die Zulassung in der Europäischen Union wird aktuell noch diskutiert.



nicht für das gesamte nutzbare Frequenzband zu erreichen sein, was eine Akzeptanz hemmen wird.

Für Neu-Installationen wird sicher eine reine 5 GHz/54 Mbit/s Lösung in Erwägung zu ziehen sein, wobei durch die wesentlich höheren Kosten für neue Technologien der Kosten/Nutzen-Faktor im Hinblick auf die „nur“ fünffache Datenrate genau überlegt werden sollte.

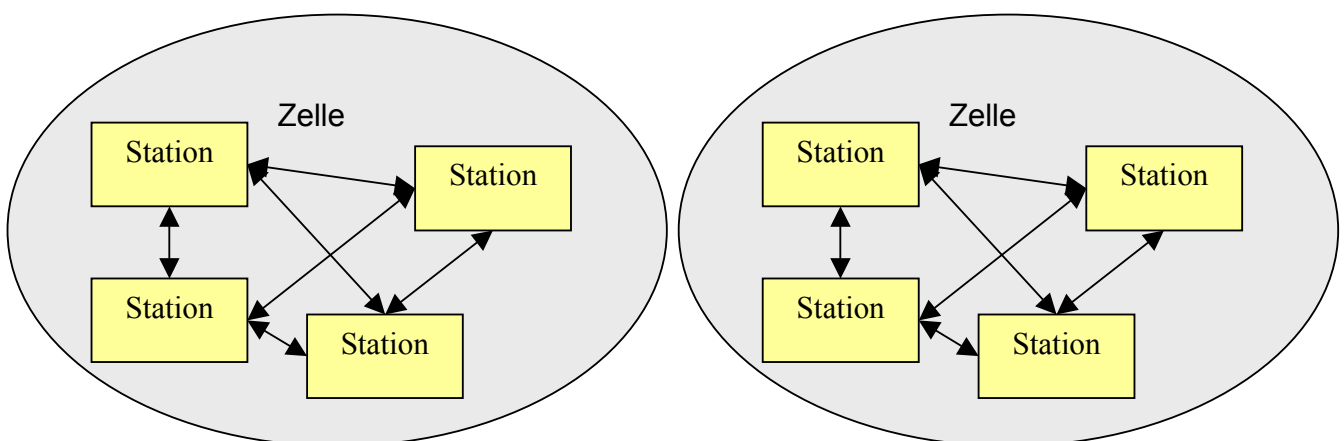
Im Sinne von Koexistenz und Migration, also für „gemischte“ Umgebungen und im Sinn einer Skalierbarkeit werden sicherlich Dual Band Karten, die verschiedene Technologien abdecken, die Wahl sein.

2 Netzwerktopologien

2.1 Ad-hoc Netzwerk

Ein Ad-hoc-Netzwerk entsteht durch den spontanen Zusammenschluss von mobilen Stationen, ohne Bereitstellung weiterer Infrastrukturkomponenten. Wenn die Stationen sich in Funkreichweite befinden, kommunizieren die Rechner direkt miteinander. Die Vorteile eines Ad-hoc-Netzwerkes liegen in der einfachen Konfiguration und der kostengünstigen Infrastruktur. Dieser Netzwerktopologie benötigt keine feste Installation und erlaubt eine beliebige Anzahl von Nutzern.

Allerdings ist das Ad-hoc-Netzwerk in der Reichweite begrenzt, es ist unstrukturiert und es ist möglich, dass einige Verbindungen aufgrund der geografischen Gegebenheiten nicht hergestellt werden können.

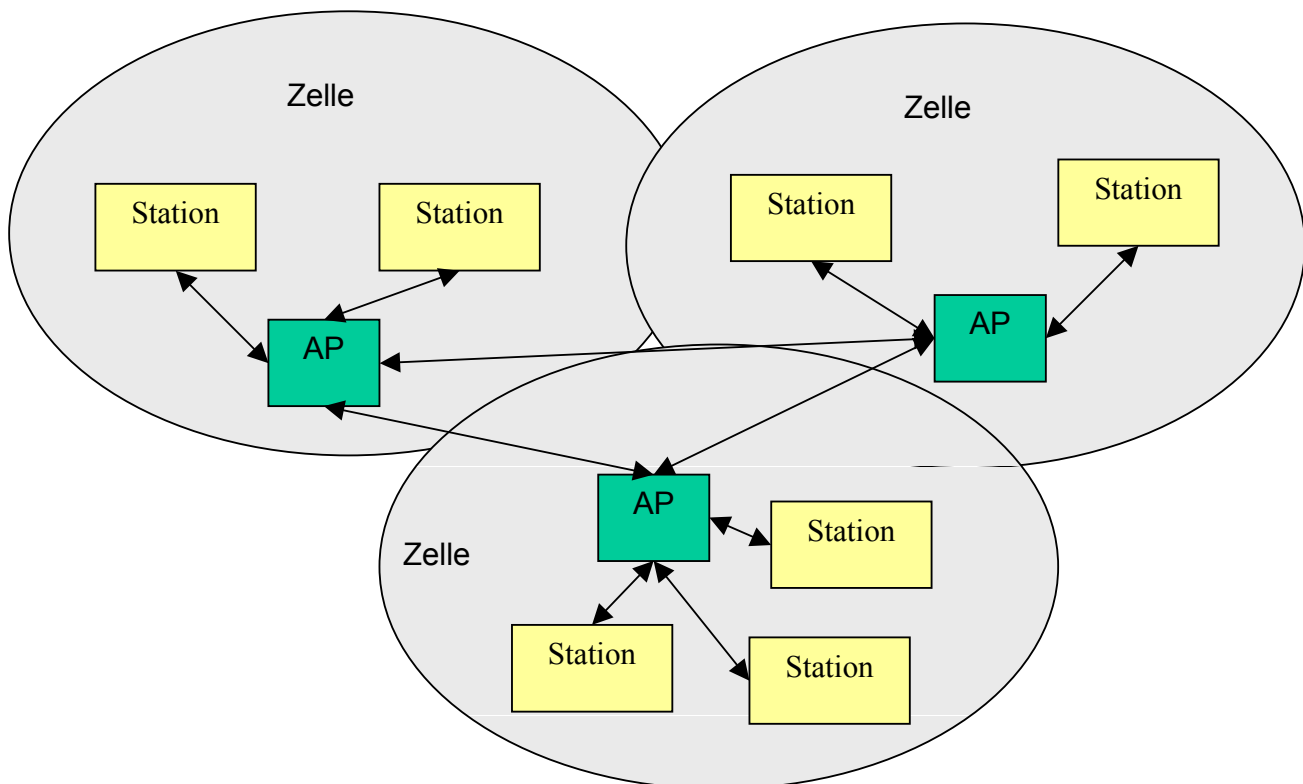




2.2 Infrastruktur Netzwerk

Das Infrastruktur Netzwerk zeichnet sich durch die Mehrzahl an Zellen und die Verbindung der einzelnen Zellen untereinander durch die Access Points aus. Ein Access Points (AP) ist die zentrale Station der Zelle und verwaltet alle Verbindungen zu den Stationen. Die Stationen einer lokalen Zelle können nur über den AP mit den Stationen einer anderen Zelle kommunizieren.

Wandert eine mobile Station von einer Zelle in eine andere muss ein *Handover*³ erfolgen. Um diesen Vorgang möglichst reibungslos gestalten zu können, überlappen sich die Zellen. Somit wird eine unterbrechungsfreie Kommunikation der mobilen Stationen gewährleistet.



³ Handover: Übergabeverfahren in der mobilen Kommunikation. Ein Handover erfolgt beim Wechsel der Zellen, der Client wird von dem Access Point der neuen Zelle verwaltet.



3 Sicherheit

3.1 WEP (Wired Equivalent Privacy)

WEP stellt ein Verfahren zur Verschlüsselung der im Funk übertragenen Datenpakete dar. Je nach verwendeter Schlüssellänge spricht man von WEP 64 oder WEP 128. Dies entspricht Schlüssellängen von 64 bzw. 128 Bit, wobei jeweils 24 Bit den sogenannten Initialisierungsvektor darstellen (eine von der Hardware von Datenpaket zu Datenpaket veränderte zufällige Zahl) und der Rest (40 bzw. 104 Bit) vom Anwender definiert wird.

3.2 Authentifizierung

Die Authentifizierung erfolgt über die autorisierte und zugangsberechtigte MAC-Adresse der Wi-Fi-Karte⁴, die dem AP bekannt ist.

3.3 Virtual Private Network (VPN)

Als praktisch absolut sicher gilt derzeit VPN, eine sichere End-zu-End Verbindung über das IP-Protokoll. Dabei wird im Falle von Wireless LANs eine sichere Verbindung zwischen jedem Wireless Client und einem VPN-Gateway im Netzwerk hergestellt. Die Access Points verhalten sich dabei transparent. Es erfolgt eine Authentifizierung des Clients am eigentlichen Netzwerk, nicht im Funk. Die übertragenen Daten können zudem unter Verwendung sicherer Verfahren wie **IPsec**⁵ verschlüsselt werden. VPN's wurden bislang für sichere Verbindungen zu bzw. zwischen Netzwerken über das Internet eingesetzt und haben sich bewährt.

⁴ Wi-Fi (Wireless Fidelity): In Anlehnung an HiFi verweisen die Hersteller von Wireless LAN Systemen auf die Wireless Fidelity und meinen damit die hohe Daten und Betriebssicherheit ihrer Funknetzwerke.

⁵ IPsec(IPSecurity): IPsec definiert die Vorgehensweise für die Datenintegrität, die Vertraulichkeit der Inhalte, sowie die Verwaltung der kryptografischen Schlüssel.