

WLAN & Sicherheit

IEEE 802.11

Präsentation von
Petar Knežić & Rafael Rutkowski

Verbundstudium TBW
Informations- und Kommunikationssysteme
Sommersemester 2007

Inhalt

- Grundlagen
- IEEE 802.11
- Betriebsarten
- IEEE-Standards
- Sicherheit

Grundlagen

- WLAN steht für Wireless Local Area Network.
- Synonyme: Wireless LAN.
- **Drahtloses lokales Funknetz.**
- Meistens nach dem Standard **IEEE 802.11.**

IEEE 802.11

- WLAN ist der umgangssprachliche Begriff für die genaue Bezeichnung **IEEE 802.11**.
- **IEEE** - Institute of Electrical and Electronics Engineers hat 1997 diesen Standard definiert.
- Funktechnik im Frequenzbereich von **2,4-GHz** oder **5-GHz** zur Übertragung von Daten.
- Bietet die Möglichkeit drahtlos ins Internet zu gehen.
- Oder den Datenaustausch zwischen zwei oder mehreren Rechnern zu ermöglichen.

Vor- und Nachteile

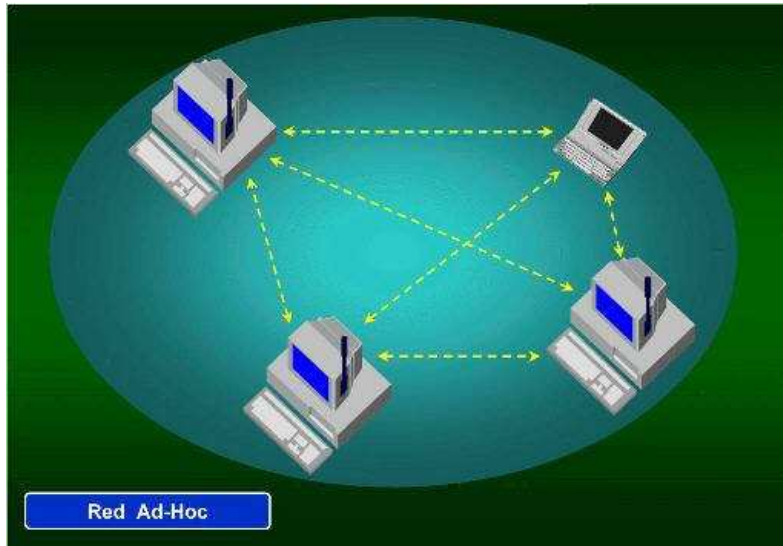
Vorteile:

- Durch Entfall der Verkabelung **niedrige Installationskosten** und **geringer Installationsaufwand**
- Mehr **Bewegungsfreiheit** z.B. durch Einsatz von Laptops.
- Durch **Hotspot** Zugang zum Internet. Zahlreiche öffentliche Plätze wie Flughäfen, Bahnhöfe, Hotels, Restaurants bietet es an.

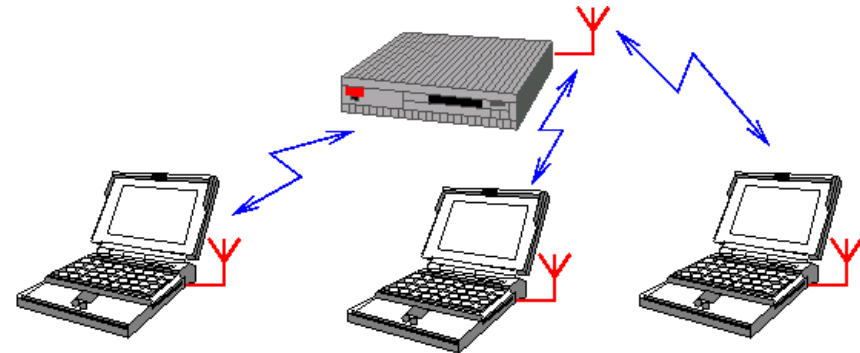
Nachteile:

- Im Vergleich zu verkabelten Netzen **geringere Geschwindigkeit**.
- Durch Wände, Decken, Bäume die den Funkverkehr stören wird die **Reichweite begrenzt**.
- Der Datenverkehr kann **leicht abgehört** werden, wenn die Verbindung nicht sicher ist.

Betriebsarten



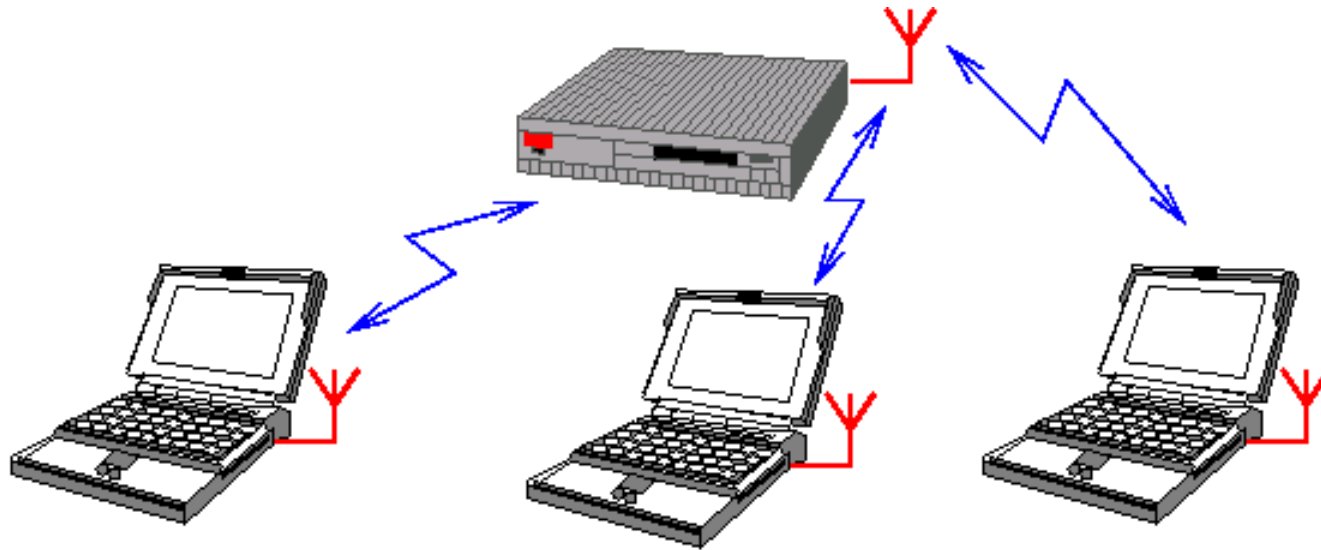
Quelle: <http://www.serviport.es/imasde/wlan/adhoce.jpg>



Quelle: <http://rnvs.informatik.tu-chemnitz.de/wlan/infra.png>

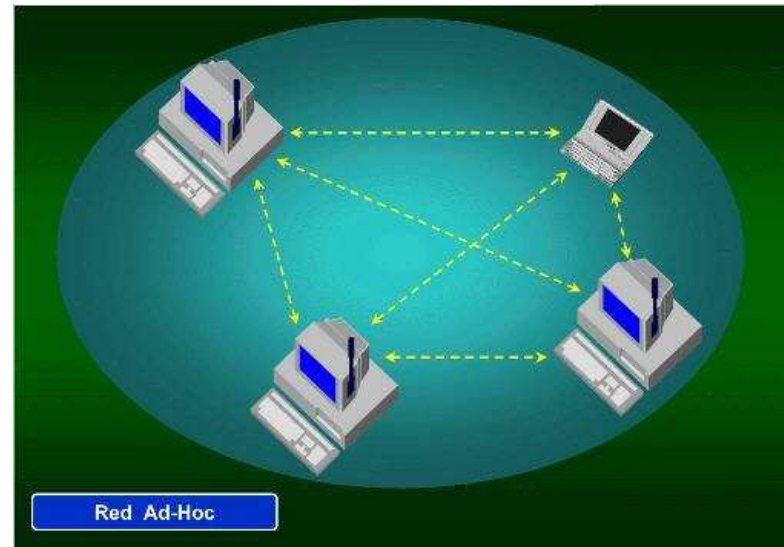
- Es gibt zwei Arten von Wireless-LAN Netzen:
 - Infrastruktur-Modus
 - Ad-Hoc-Modus

Betriebsarten – Infrastruktur-Modus



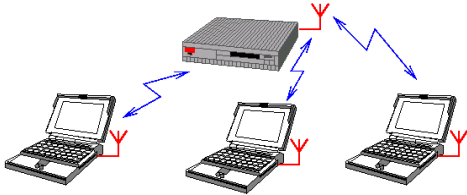
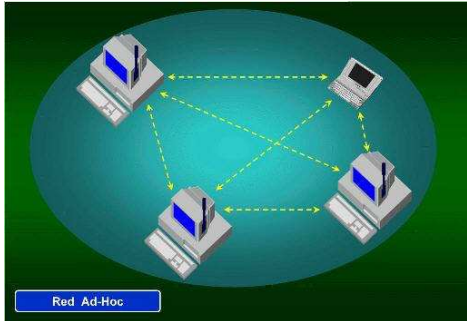
- Der Infrastruktur-Modus ist die klassische Betriebsart.
- Eine Basisstation „WLAN-Access-Point“ wird festgelegt.
- Basis-Station koordiniert die einzelnen Rechner.
- Die Rechner kommunizieren drahtlos mit Basis-Station.
- Basis-Station wird über Kabel an einen Internet-Provider angeschlossen.

Betriebsarten – Ad-hoc-Modus



- Kein gemeinsamer Knotenpunkt (WLAN-Access-Point).
- Jeder Nutzer ist somit ein unabhängiger Access Point.
- Netzwerkteilnehmer kommunizieren direkt miteinander.
- Ad-hoc-Netze lassen sich schnell aufbauen.
- Keine Kommunikation mit anderen Netzen möglich.

Betriebsarten

Modus	Vorteile	Nachteile
Infrastruktur 	• Kann mit anderen Netzwerken kommunizieren	• Erfordert Planung • Aufwendiger • Erfordert Basisstation
Ad-hoc 	• Keine Planung notwendig • Schneller Aufbau möglich • Keine Basisstation notwendig	• Kommunikation mit anderen Netzen nicht möglich

IEEE-Standards

- Die gängigsten Standards sind:
 - **IEEE 802.11 a**
 - **IEEE 802.11 b**
 - **IEEE 802.11 g**
- Zukünftig wird sich höchst wahrscheinlich der Standard **IEEE802.11 n** durchsetzen.
- Die Standards unterscheiden sich hauptsächlich durch:
 - **Frequenzbereich**
 - **Maximale Datenrate**
 - **Reichweite**

Die Technik von IEEE 802.11

- Als Übertragungsmedium dient Luft, diese hat die Eigenschaft **elektromagnetische Wellen** zu übertragen.
- Die Information werden im **2,4 GHz** oder **5 GHz Frequenzbereich** vom Sender zum Empfänger gesendet.
- Die Übertragung der Signale funktioniert durch die Aufbringung von Informationen auf sich ausbreitende Wellen.
- Derzeit sind Übertragungsraten von 54 Mbit/s üblich.

IEEE-Standards

Merkmal	IEEE Standard		
	802.11a	802.11b	802.11g
Frequenzbereich	5 GHz	2,4 GHz	2,4 GHz
Maximale Datenrate	54 Mbit/s	11 Mbit/s	54 Mbit/s
Reichweite bei max. Datenrate	15 m	30 m	12 m

- Der **IEEE 802.11n** Standard wird derzeit verabschiedet.
- Geplant ist voraussichtlich eine **Maximale Datenrate von 300 MBit/s**.



Sicherheit

Sicherheit

- Alle Daten werden die durch die Luft ausgetauscht .
- Sie können leicht und spurlos abgehört und für missbräuchliche Zwecke verwendet werden.
- Die Sicherheitsaspekte beim WLAN sind deutlich wichtiger als bei kabelgebundenen Netzen.
- Es gibt Sicherheitsmechanismen. Jedoch sind diese überwindbar.
- Wichtige oder vertrauliche Informationen sind nicht ausreichend geschützt!
- **Es gibt derzeit keine 100% Sicherheit beim WLAN!**

Sicherheit

- Der IEEE 802.11 Standard hat einige Mechanismen integriert:
 - Passwörter
 - Netzwerkname (SSID)
 - MAC-Adresse
 - WEP-Verschlüsselung
 - WPA-Verschlüsselung
 - WPA2-Verschlüsselung

Sicherheit - Passwörter

- Das WLAN kann durch Passwort geschützt werden.
- Dieses sollte regelmäßig geändert werden.

Sicherheit - Netzwerkname

- Es kann eine Netzwerkname vergeben werden.
- Die Grundeinstellung ist meistens das sich jeder (any) in das Netzwerk einwählen kann.
- Durch Vergabe des Namens können nur Teilnehmer mit der gleichen SSID am Netzwerk teilnehmen.

Sicherheit – MAC-Adresse

- MAC steht für **Media Access Control**.
- MAC-Adresse muss vergeben werden.
- Nur bekannte MAC-Adressen werden als Teilnehmer zugelassen.
- MAC dient als Filter.

Sicherheit – WEP-Verschlüsselung

- WEP ist die Standard-Verschlüsselung für WLAN.
- Zugang zum Netz wird geregelt und die Datenintegrität wird sichergestellt.
- Verschlüsselung durch Strom-Chiffre.
- Basiert auf RC4-Algorithmus.
- Schlüssel mit 64 oder 128 Bit.

Sicherheit – WPA-Verschlüsselung

- WPA ist eine weitere Verschlüsselungsmethode für WLAN.
- Im Vergleich zu WEP bietet WPA zusätzlichen Schutz durch dynamische Schlüssel.
- Diese basieren auf TKIP (Temporal Key Integrity Protocol).
- WPA basiert auf RC4 Stromchiffre.

Sicherheit – WPA2-Verschlüsselung

- Da der RC4 Algorithmus als gebrochen gilt nutze WPA2 den AES Algorithmus.
- AES steht für **A**dvanced **E**ncryption **S**tandard.

Ende der Präsentation!

**Vielen Dank für Eure
Aufmerksamkeit!**