



openHPI-Kurs Wie funktioniert das Internet?

WLAN – Kabellose Netze

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut
Universität Potsdam

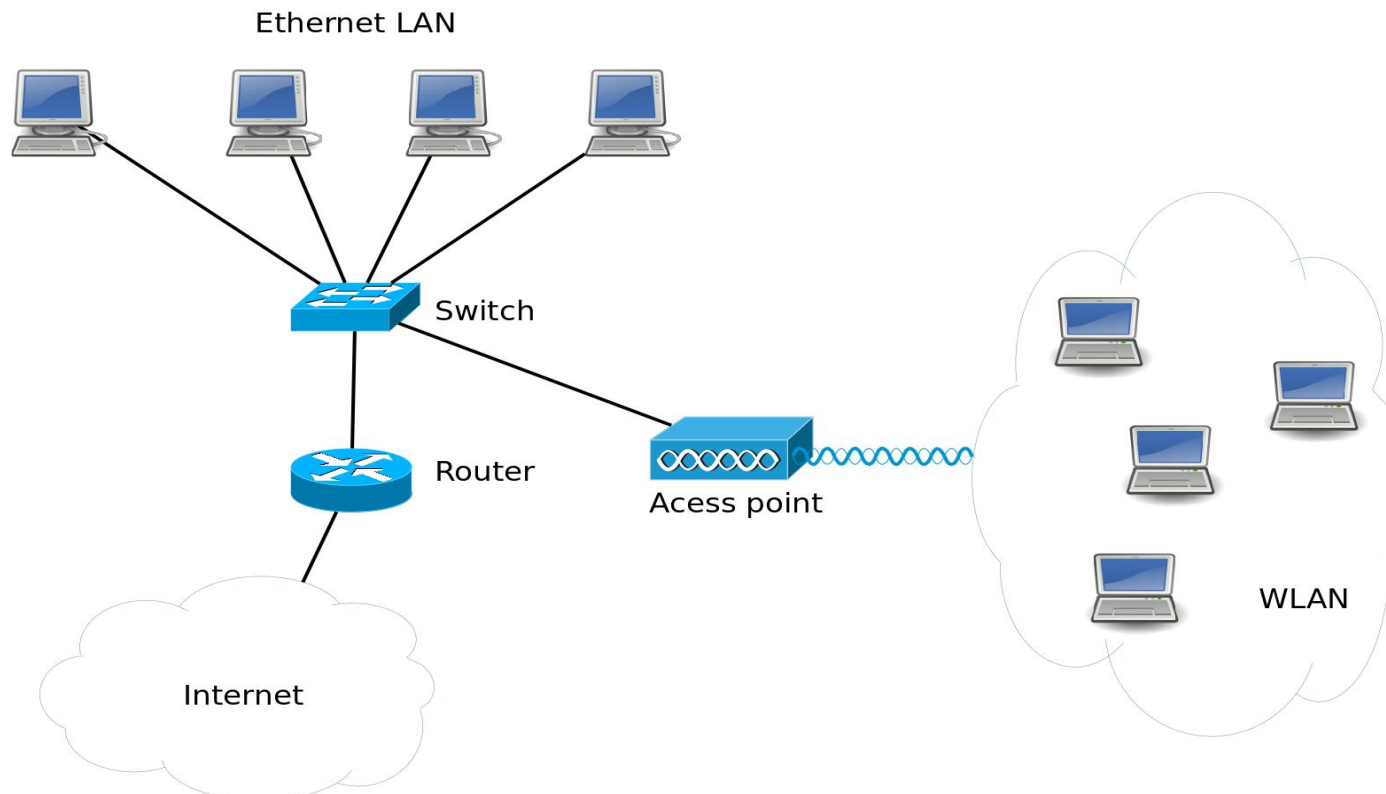
WLAN – Kabelloses Netz (1/3)

Funkbasierte Netzwerke – **Wireless LAN** – WLAN – werden immer beliebter

- WLANs erlauben ubiquitäres Computing – „jederzeit an jedem Ort“
- Geschichtlicher Ursprung: ALOHAnet (1971) – Funknetz zur Vernetzung der Hawaiianischen Hauptinseln mit einem Zentralrechner (9.600 bps)
- WLANs besitzen Sterntopologie – zentrale Basisstationen – **Access Points** – sorgen für Weiterleitung der Datenpakete an erreichbare Rechner
- IEEE 802.11 spezifiziert WLAN-Standard, z.B.
 - 802.11a – 54 Mbps im 5 GHz Frequenzband
 - 802.11b – 11 Mbps im 2,4 GHz Frequenzband
 - 802.11i – Verbesserung der Sicherheit

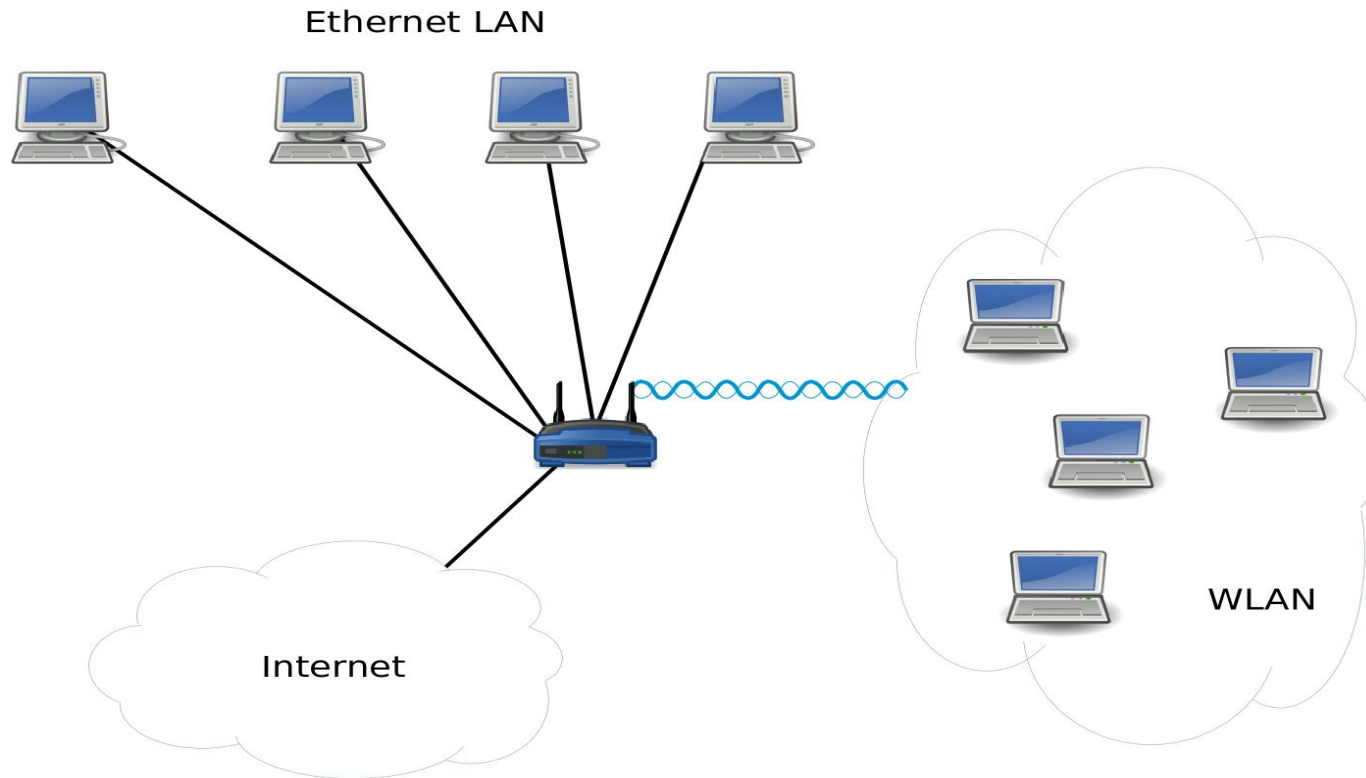
WLAN – Kabelloses Netz (2/3)

Anbindung eines WLAN an ein sternenförmiges Ethernet-Netzwerk und das Internet über dedizierte Zwischensysteme – **Switch / Router / Access Point:**

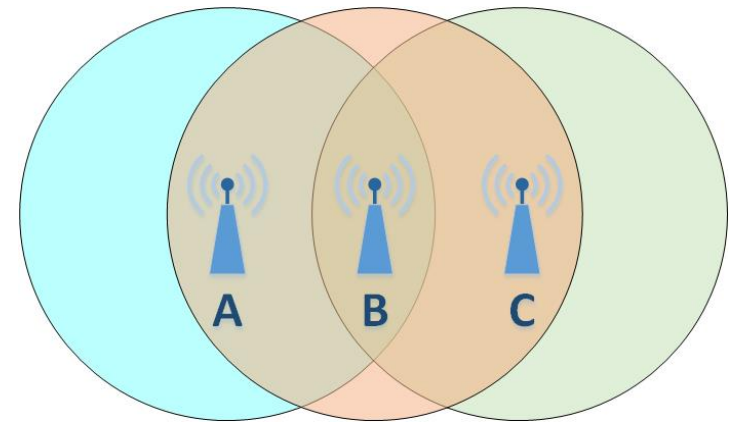


WLAN – Kabelloses Netz (3/3)

Heute werden die einzelnen, dedizierten Geräte in „All-in-One“-Geräten zusammengefasst:

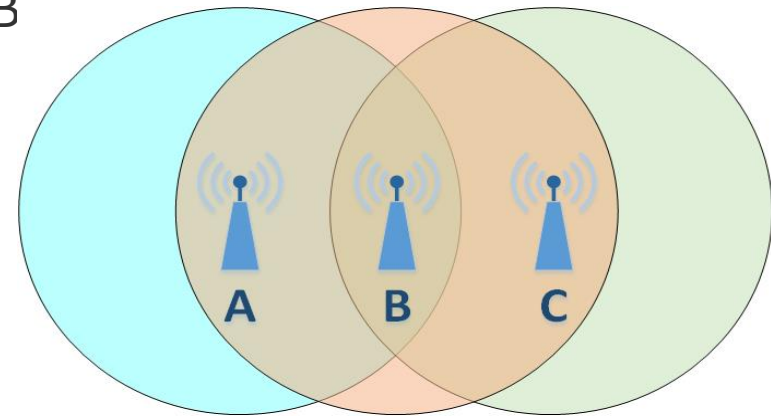


- Vielfachzugriffsregelung erfolgt ähnlich wie mit *CSMA/CD* im Ethernet. Dennoch können Kollisionen auftreten, zum Beispiel beim *Hidden-Station*-Problem
 - Die Knoten A und C können Knoten B erreichen, sind jedoch voreinander verdeckt
 - Bei Knoten B kollidieren die gleichzeitig eintreffenden Signale der Knoten A und C
- Zur Vermeidung von **Kollisionen** wird „**Carrier Sense Multiple Access/Collision Avoidance**“ (CSMA/CA) angewendet



Carrier Sense Multiple Access/Collision Avoidance:

- A sendet "Request To Send" (RTS) an B
- B sendet "Clear To Send" (CTS) an A
- A sendet "Data Sending" (DS) an B
- A sendet Datenpaket an B und
- B sendet "Acknowledgement" (ACK) an

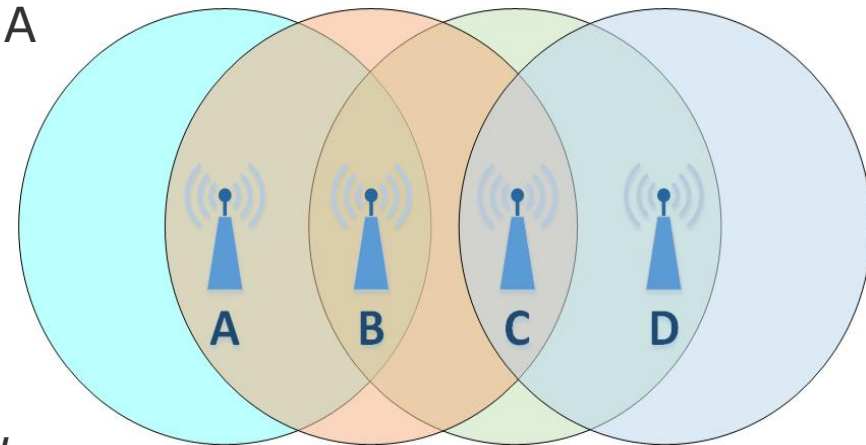


Alle Knoten, die ein RTS/CTS hören, warten

- Kollisionen können nur noch bei RTS/CTS auftreten, jedoch nicht bei der Übertragung von Nutzdaten
- Im Fall einer Kollision warten beide Sender eine **zufällige** Zeitspanne, bevor sie ein neues RTS senden

Das **Exposed-Station-Problem** sorgt für weitere Komplikationen

- D kann nicht mit Knoten C kommunizieren, obwohl D außerhalb der Sende-/Empfangsbereiche von A und B liegt und keine Kollisionen auftreten
- C hatte das CTS von Knoten B an Knoten A gehört und antwortet deshalb D nicht
- „Multiple Access with Collision Avoidance for Wireless“ (MACAW) Verfahren kann hier angewendet werden:
 - Knoten D sendet ein „Request to Send“ an C
 - C antwortet diesmal nach einer kurzen Pause mit einem „Request for Request To Send“ (RRTS) an D
 - Es folgt das bereits vorgestellte Protokoll von CSMA/CA



Sicherheit in kabellosen Netzen (1/2)

- Aufgrund der Natur des Übertragungsmediums ist das Sicherheitsniveau in funkbasierten Netzen wesentlich geringer als in kabelgebundenen
- Zum Abhören und zur nichtautorisierten Benutzung ist kein physikalischer Zugang notwendig
- Auch Entdeckung eines WLANs ist nicht schwierig
→ „Parkplatz-Attacke“
- Angriffe auf WLANs
 - Passive Angriffe zur Entschlüsselung des Datenverkehrs durch statistische Analyse
 - Aktive Angriffe...

Sicherheit in kabellosen Netzen (2/2)

- Zum Schutz von WLANs wurde ursprünglich in IEEE 802.11b das Verschlüsselungsprotokoll **WEP** – Wired Equivalent Privacy – definiert
- WEP-Protokoll basiert auf geheimem symmetrischen Schlüssel, der zwischen AP und teilnehmenden Rechnern vereinbart wird
 - Aber **Achtung**: WEP basiert auf unsicherem Verschlüsselungsalgorithmus RC4 und kann leicht geknackt werden

Sicherheit in kabellosen Netzen (2/2)

- Heute sollen in WLANs deshalb statt WEP sicherere Verschlüsselungsprotokolle eingesetzt werden
 - WPA bzw.
 - **besser** noch **WPA2**
 - **WPA2** nutzt **AES** (Advanced Encryption Standard) als sicheres Verschlüsselungsverfahren
- **Achtung:** Wird das sogenannte Wi-Fi Protected Setup (WPS) genutzt, dann kann Angreifer **Brute-Force-Attacke** durchführen, um an die WPS PIN zu gelangen und damit dann WPA/WPA2 umgehen ...