

## 2. Foliensatz Computernetze

Prof. Dr. Christian Baun

Frankfurt University of Applied Sciences  
(1971–2014: Fachhochschule Frankfurt am Main)  
Fachbereich Informatik und Ingenieurwissenschaften  
[christianbaun@fb2.fra-uas.de](mailto:christianbaun@fb2.fra-uas.de)



# Lernziele dieses Foliensatzes

- Bitübertragungsschicht (Teil 1)
  - Vernetzungstechnologien
    - Ethernet
    - Token Ring
    - Wireless LAN (WLAN)
    - Bluetooth
  - Übertragungsmedien
    - Koaxialkabel
    - Twisted-Pair-Kabel
    - Lichtwellenleiter











# Arbeitsweise von Token Ring

Bildquelle: Scott Adams (<http://dilbert.com>)

- Die Teilnehmer reichen den Token-Rahmen immer weiter
  - Möchte ein Endgerät Daten senden, wartet es auf den Token-Rahmen
    - Dann hängt das Endgerät seine **Nutzdaten** an das Token an
    - Es ergänzt das Token um die nötigen **Steuersignale**
    - Es setzt das **Token-Bit** von 0 (*Freies Token*) auf 1 (*Datenrahmen*)
  - Erreicht ein Datenrahmen-Token sein Ziel, kopiert der Empfänger die Nutzdaten und **quittiert den Datenempfang**
    - Der Sender empfängt die Quittung und sendet das Token mit den nächsten Nutzdaten oder setzt ein Frei-Token auf den Ring

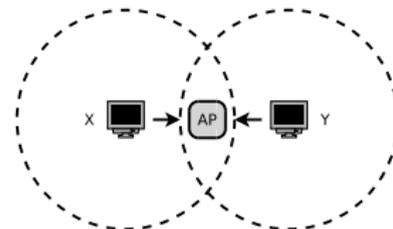


# Herausforderungen beim Funknetzen (1/2)

- WLAN ist die bekannteste Technologie für drahtlose Computernetze
  - Das Übertragungsmedium hat einige spezielle Eigenschaften
    - Diese sind der Grund für folgende Herausforderungen

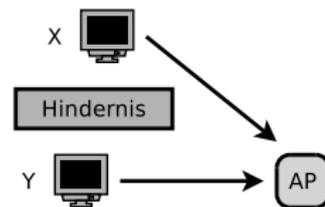
## 1 Fading (abnehmende Signalstärke)

- Elektromagnetische Wellen werden durch Hindernisse (z.B. Wände) und im freien Raum allmählich abgeschwächt



## 2 Hidden-Terminal (unsichtbare bzw. versteckte Endgeräte)

- Endgeräte, die mit dem gleichen Gerät (z.B. einer Basisstation) kommunizieren, erkennen einander nicht und stören sich gegenseitig
  - Grund: Hindernisse

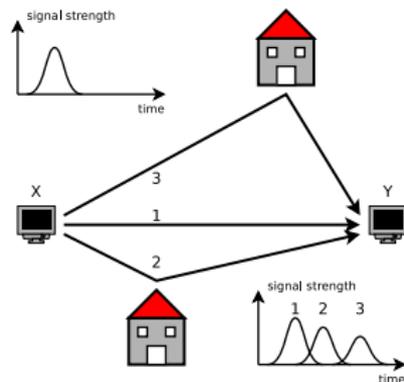


Quelle: Computernetzwerke, James F. Kurose, Keith W. Ross, Pearson (2008)

# Herausforderungen beim Funknetzen (2/2)

## 3 Mehrwegeausbreitung

- Teile der elektromagnetischen Wellen werden reflektiert und legen darum unterschiedlich lange Wege vom Absender zum Ziel zurück
  - Resultat: Unscharfes Signal beim Empfänger weil die Reflektionen beeinflussen nachfolgende Übertragungen
- Ähnliches Problem: Bewegen sich Objekte zwischen Sender und Empfänger, können sich die Ausbreitungswege ändern

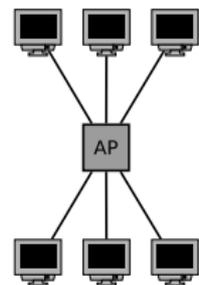
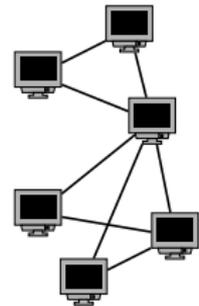


## 4 Interferenzen mit anderen Quellen

- Beispiele: WLAN und Bluetooth
  - Beide Netzwerktechnologien arbeiten auf dem gleichen Frequenzband und können darum interferieren
- Auch elektromagnetisches Rauschen durch Motoren oder Mikrowellengeräte können zu Interferenzen führen

# Ad-hoc-Modus und Infrastruktur-Modus

- Kommunikation zwischen WLAN-Geräten ist möglich im...
- **Ad-hoc-Modus:** Endgeräte bilden ein **vermaschtes Netz**
  - Die Endgeräte kommunizieren direkt miteinander
    - Jedes Endgerät kann mit mehreren anderen Geräten verbunden sein
  - Bei allen Endgeräten müssen der gleiche Netzwerkname – Service Set Identifier (SSID) und dieselben Verschlüsselungsparameter eingestellt sein
- **Infrastruktur-Modus:** Endgeräte melden sich jeweils mit ihrer MAC-Adresse an der Basisstation an
  - Die Basisstation sendet in einstellbaren Intervallen (z.B. 10x pro Sekunde) kleine „Leuchtfeuer-Rahmen“ (*Beacons*), an alle Endgeräte im Empfangsbereich
    - Die Beacons enthalten u.a. den Netzwerknamen (SSID), die Liste der unterstützten Übertragungsraten und die Art der Verschlüsselung



# Datenübertragungsraten bei WLAN

- **Alle Stationen teilen sich die Bandbreite für Up- und Download**
  - Darum liegt die erreichbare Nettoübertragungsrate selbst unter optimalen Bedingungen nur wenig über der Hälfte der Bruttowerte

Wi-Fi	IEEE-Standard	Verabschiedet	Frequenzen			Maximale (Brutto) Übertragungsrate	Realistische (Netto) Übertragungsrate	
			2,4 GHz	5 GHz	6 GHz			
-	802.11	1997	X			2 Mbit/s	1	Mbit/s
-	802.11b	1999	X			11 Mbit/s <sup>1</sup>	5-6	Mbit/s
-	802.11a	1999		X		54 Mbit/s <sup>2</sup>	20-22	Mbit/s
-	802.11h	2003		X		54 Mbit/s <sup>2</sup>	20-22	Mbit/s
-	802.11g	2003	X			54 Mbit/s	20-22	Mbit/s
4	802.11n	2009	X	X		600 Mbit/s <sup>3</sup>	50-60	Mbit/s
5	802.11ac	2013		X		6930 Mbit/s <sup>4</sup>	400-500	Mbit/s
6	802.11ax	2021	X	X		9600 Mbit/s <sup>4</sup>	500-600	Mbit/s
6E	802.11ax	2021	X	X	X	9600 Mbit/s <sup>5</sup>	500-600	Mbit/s
7	802.11be	2024	X	X	X	40000 Mbit/s	noch unklar	

<sup>1</sup> Herstellerabhängig auch 22 Mbit/s bei 40 MHz Kanalbreite  
<sup>2</sup> Herstellerabhängig auch 108 Mbit/s bei 40 MHz Kanalbreite  
<sup>3</sup> Bei 4x4 MIMO und 80 MHz Kanalbreite  
<sup>4</sup> Bei 8x8 MIMO und 160 MHz Kanalbreite. In der Praxis unübliche Werte  
<sup>5</sup> Pro Antenne in der Station bzw. im Endgerät

# Sendeleistung bei WLAN

Bildquelle: Google Bildersuche

- WLAN wurde für den Einsatz innerhalb Gebäuden entwickelt
  - Aus diesem Grund sendet es nur mit einer niedrigen Leistung (maximal 100 mW bei 2,4 GHz, 1 W bei 5 GHz und 200 mW bei 6 GHz)
    - Solche Sendeleistungen gelten als gesundheitlich unbedenklich
    - Zum Vergleich: Die Sendeleistung von GSM-Telefonen, die im Frequenzbereich 880-960 MHz senden, ist ca. 2 W
  - Es existieren auch WLAN-Geräte für 2,4 GHz mit höherer Sendeleistung
    - Der Betrieb solcher Geräte ist in vielen Ländern illegal ⇒ Folie 15



### Wifi Verstärker 1000mW

Professional WLAN Booster / Verstärker 1000mW (30dBm) 2.4GHz 802.11b/g bis 108Mbps

**Ihre Vorteile:**

- Erhöht die Durchreichweite des WLAN
- Erhöht die WLAN-Verbindungsstärke
- Erhöht die WLAN-Verbindungsstabilität
- Erhöht die WLAN-Verbindungsbandbreite
- Erhöht die WLAN-Verbindungsleistung
- Erhöht die WLAN-Verbindungsreichweite

**Nicht mit 30dBm**

**Lieferumfang:**

- 1x Wifi Verstärker
- 1x USB-Kabel
- 1x Netzteil
- 1x Bedienungsanleitung

CE, FCC, RoHS

### ALFA NETWORK

## 1000mW 5dBi

### Plus Mount!

ALFA NETWORK

CE, FCC, RoHS

# Messfahrzeug der Bundesnetzagentur



Gesehen in Ludwigshafen-Oggersheim (26. November 2018)

# WLAN-Standards, Frequenzen und Kanäle

- Die meisten WLAN-Standards verwenden die Frequenzblöcke 2,4000-2,4835 GHz und 5,150-5,725 GHz im Mikrowellenbereich
  - Unterschiede gibt es u.a. bei Frequenzblöcken, Datenübertragungsraten, Modulationsverfahren und den resultierenden Kanalbandbreiten

Wi-Fi	IEEE-Standard	Verabschiedet	Frequenzen			Maximale (Brutto) Übertragungsrate	Realistische (Netto) Übertragungsrate
			2,4 GHz	5 GHz	6 GHz		
–	802.11	1997	X			2 Mbit/s	1 Mbit/s
–	802.11b	1999	X			11 Mbit/s <sup>1</sup>	5-6 Mbit/s
–	802.11a	1999		X		54 Mbit/s <sup>2</sup>	20-22 Mbit/s
–	802.11h	2003		X		54 Mbit/s <sup>2</sup>	20-22 Mbit/s
–	802.11g	2003	X			54 Mbit/s	20-22 Mbit/s
4	802.11n	2009	X	X		600 Mbit/s <sup>3</sup>	50-60 Mbit/s
5	802.11ac	2013		X		6930 Mbit/s <sup>4</sup>	400-500 Mbit/s
6	802.11ax	2021	X	X		9600 Mbit/s <sup>4</sup>	500-600 Mbit/s
6E	802.11ax	2021	X	X	X	9600 Mbit/s <sup>5</sup>	500-600 Mbit/s
7	802.11be	2024	X	X	X	40000 Mbit/s	noch unklar

IEEE 802.11h ist eine Anpassung von IEEE 802.11a um militärische Radarsysteme und Satellitenfunk in Europa nicht zu stören

Einzige Unterschiede zu IEEE 802.11a: Zusätzliche Fähigkeiten Dynamic Frequency Selection (*Dynamisches Frequenzwahlverfahren*) und Transmission Power Control (*Übertragungssendeleistungs-Steuerung*)

Obwohl WLAN weltweit verwendet wird, gibt es rechtliche Unterschiede

Beispiel: In Deutschland darf 5,15-5,35 GHz nur innerhalb geschlossener Räume mit maximal 200 mW Sendeleistung genutzt werden

# Erlaubte Nutzung der WLAN-Frequenzen im 2,4-GHz-Band

- Die Frequenzblöcke sind in Kanäle unterteilt
  - Das Prinzip ist vergleichbar mit Fernseh- oder Radioübertragungen
  - Der Frequenzblock 2,4 GHz ist in 13 Kanäle unterteilt
    - Bandbreite jedes Kanals: 5 MHz
  - In Japan existiert noch ein zusätzlicher 14. Kanal
    - Er ist nur für das Modulationsverfahren DSSS freigegeben
    - Er liegt 12 MHz über dem 13. Kanal

Kanal	Frequenz [GHz]	EU	USA	Japan
1	2,412	X	X	X
2	2,417	X	X	X
3	2,422	X	X	X
4	2,427	X	X	X
5	2,432	X	X	X
6	2,437	X	X	X
7	2,442	X	X	X
8	2,447	X	X	X
9	2,452	X	X	X
10	2,457	X	X	X
11	2,462	X	X	X
12	2,467	X	X	X
13	2,472	X	X	X
14	2,484			X

# Modulationsverfahren der WLAN-Standards

- Die WLAN-Standards verwenden unterschiedliche Modulationsverfahren

IEEE-Standard	Modulationsverfahren	Kanalbreite
802.11	FHSS <sup>1</sup> oder DSSS <sup>2</sup>	22 MHz
802.11a	OFDM <sup>3</sup>	20 MHz
802.11b	DSSS <sup>2</sup>	22 MHz
802.11g	OFDM <sup>3</sup>	20 MHz
802.11h	OFDM <sup>3</sup>	20 MHz
802.11n	OFDM <sup>3</sup>	20 oder 40 MHz
802.11ac	OFDM <sup>3</sup>	20, 40, 80 oder 160 MHz
802.11ax	OFDMA <sup>4</sup>	20, 40, 80 oder 160 MHz
802.11be	Enhanced OFDMA	20, 40, 80, 160 oder 320 MHz

<sup>1</sup> Frequency Hopping Spread Spectrum (Frequenzsprungverfahren)

<sup>2</sup> Direct Sequence Spread Spectrum (Frequenzspreizverfahren)

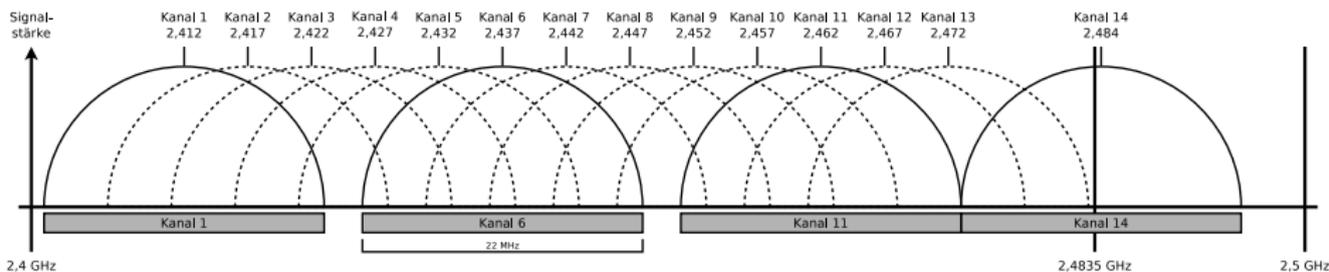
<sup>3</sup> Orthogonal Frequency-Division Multiplexing (orthogonales Frequenzmultiplexverfahren)

<sup>4</sup> Orthogonal Frequency Division Multiple Access

## Warum ist das Modulationsverfahren relevant?

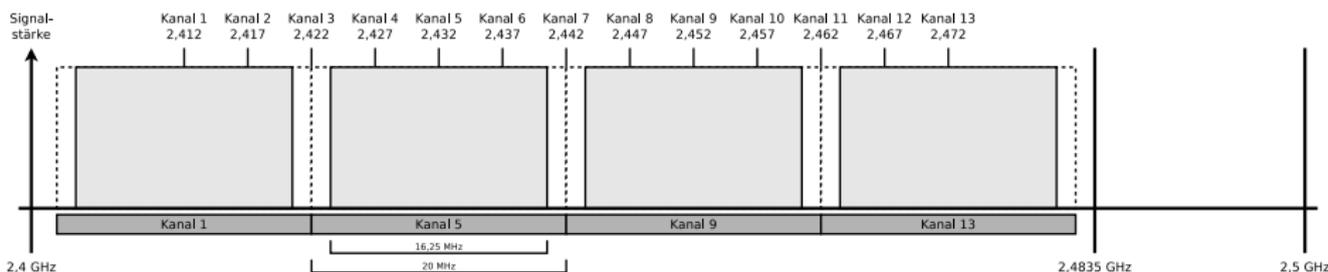
- Es legt die Kanalbreite fest
- Die Kanalbreite legt fest, wie viele Kanäle in den jeweiligen Frequenzbereichen nutzbar sind

# Überlappungsfreie Kanäle bei IEEE 802.11b



- IEEE 802.11b verwendet das Modulationsverfahren **DSSS** mit **22 MHz breiten Kanälen** und einem **5 MHz Kanalrasterabstand**
  - Darum existieren nur 3 (EU und USA) bzw. 4 (Japan) Kanäle, deren Signale sich nicht überlappen
    - Das sind die Kanäle 1, 6, 11 und 14 (nur in Japan)
- DSSS ist ein **Frequenzspreizverfahren**
  - Es verteilt die Nutzdaten über einen breiten Frequenzbereich
  - Das macht es weitgehend unempfindlich gegenüber schmalbandigen Störungen (z.B. Bluetooth)

# Überlappungsfreie Kanäle bei 802.11g und 802.11n

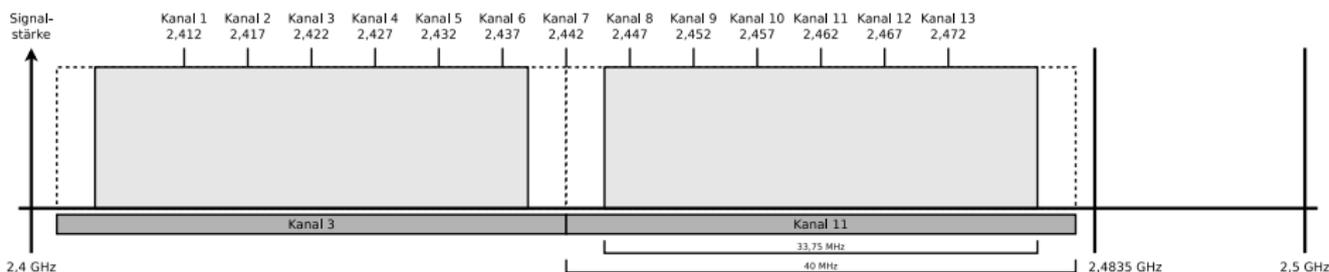


- 802.11g und 802.11n verwenden das Modulationsverfahren **OFDM**
  - Bei diesem handelt es sich um ein **Mehrträgerverfahren**
    - Jeder Kanal ist 20 MHz breit und besteht aus 64 Zwischenträgern zu je 0,3125 MHz, von denen aber nur 52 verwendet werden
    - Die **Nutzbandbreite pro Kanal** ist also nur **16,25 MHz**
    - Es gibt also nur 4 überlappungsfreie Kanäle: 1, 5, 9 und 13

Endgeräte nach 802.11a verwenden auch das Modulationsverfahren OFDM mit 20 MHz breiten Kanälen...

arbeiten aber ausschließlich im Frequenzblock 5,150-5,725 GHz

# Überlappungsfreie Kanäle bei IEEE 802.11n



- Bei 802.11n ist wahlweise ein Betrieb mit 40 MHz Kanalbreite möglich
- Bei 40 MHz breiten Kanälen existieren im Frequenzblock 2,4000-2,4835 GHz nur 2 Kanäle, nämlich Kanal 3 und 11, deren Signale sich nicht überlappen
  - Jeder Kanal besteht aus 128 Zwischenträgern zu je 0,3125 MHz, von denen aber nur 108 verwendet werden
  - Die Nutzbandbreite pro Kanal ist also nur 33,75 MHz

Hochwertige Endgeräte, die 802.11n unterstützen, können zusätzlich den Frequenzblock 5,150-5,725 GHz nutzen





# IEEE 802.11n – Multiple Input Multiple Output (MIMO)

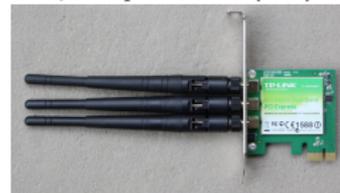
- Die maximale Bruttodatenrate bei IEEE 802.11n liegt je nach Anzahl der Antennen in den Stationen bei 150, 300, 450 oder 600 Mbit/s
  - Der Grund für diese Leistungssteigerung gegenüber IEEE 802.11a/b/g/h ist, dass 802.11n **MIMO** verwendet
- Zusätzlich zur Verbreiterung der Kanäle auf 40 MHz kommen bei MIMO bis zu 4 Antennen zum Einsatz
  - Diese ermöglichen gleichzeitiges Arbeiten in den Frequenzbereichen 2,4 GHz und 5 GHz
- Pro parallelem Datenstrom (pro Antenne) sind maximal 150 Mbit/s Datendurchsatz (brutto) möglich und bis zu 4 Datenströme können gebündelt werden
  - Die entsprechende Anzahl Antennen (bis zu 4) ist jeweils auf beiden Seiten nötig



Bildquelle: pixabay.com (CC0)



Bildquelle: pxhere.com (CC0)



Bildquelle: Eigenes Werk

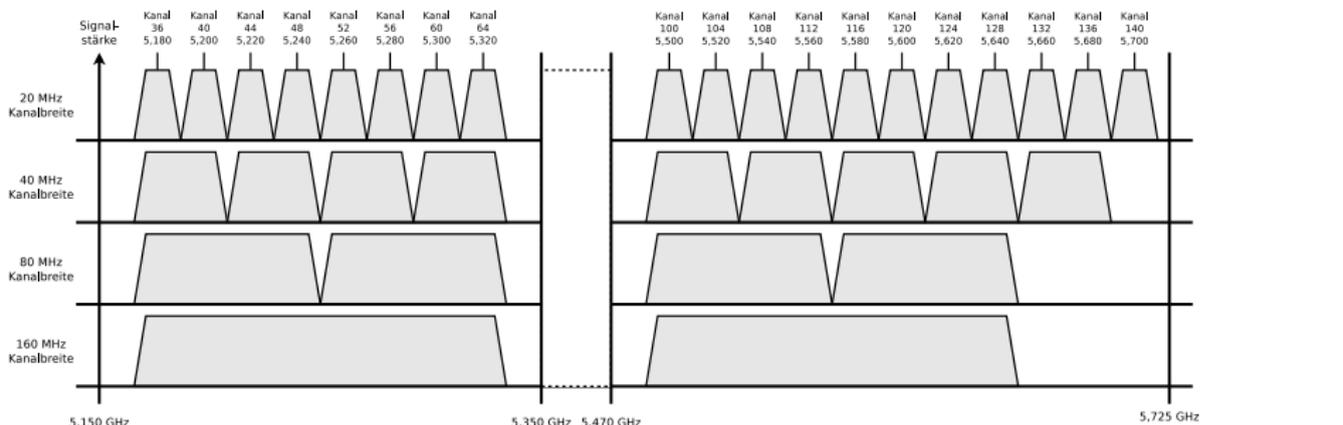
# IEEE 802.11ac

- Auch IEEE 802.11ac verwendet **MIMO**
  - Maximal 8 parallel nutzbare Antennen möglich
  - Ermöglicht breitere Kanäle: 40/80/160 MHz
  - Arbeitet nur im 5-GHz-Band
  - Max. (brutto) Übertragungsrate: 6,936 GBit/s
    - Bei 8×MIMO und 160 MHz Kanalbreite



Bildquelle: Cookiemonster1979. Wikimedia (CC-BY-SA-4.0)

Solche Werte sind in der Praxis unüblich. Ein realistisches Szenario ist z.B. MIMO mit 4 Antennen im Access Point und 80 MHz Kanalbreite. Hier wäre die maximale (Brutto-)Übertragungsrate bei 802.11ac 1733 Mbit/s



# Sicherheit bei WLAN – WEP

- WLAN gemäß 802.11 enthält den Sicherheitsstandard **Wired Equivalent Privacy (WEP)**, der auf dem RC4-Algorithmus basiert
  - XOR-Verknüpfung des Bitstroms der Nutzdaten mit einem aus dem RC4-Algorithmus generierten, pseudozufälligen Bitstrom
  - Arbeitet mit 40 Bit bzw. 104 Bit langen **statischen Schlüsseln**
  - Kann durch Known-Plaintext-Angriffe geknackt werden, weil die Header des 802.11-Protokolls vorhersagbar sind
    - Die Berechnung des WEP-Schlüssels mit Hilfe von einigen Minuten aufgezeichneter Daten dauert mit Werkzeugen wie Aircrack nur wenige Sekunden

## WEP-Verschlüsselung von WLANs in unter einer Minute geknackt

Forschern der Technischen Universität Darmstadt ist ein weiterer Durchbruch beim Knacken WEP-verschlüsselter Funknetzwerke gelungen. Wie Erik Tews, Andrei Pychkine und Ralf-Philipp Weinmann in einem Paper beschreiben, konnten sie die Menge der für einen erfolgreichen Angriff notwendigen mitgeschnittenen Pakete auf weniger als ein Zehntel reduzieren. Ein mit einem 128-Bit-WEP-Schlüssel gesichertes Funknetz ließe sich nach Angaben der Forscher mit ihrem Angriff in unter einer Minute knacken. . .

Nachricht vom 4. April 2007. Quelle: <http://heise.de/-164971>

# Sicherheit bei WLAN – WPA und WPA2

- Besserer Sicherheitsstandard: **Wi-Fi Protected Access (WPA)**
  - Basiert auch auf dem RC4-Algorithmus, enthält jedoch zusätzlichen Schutz durch **dynamische Schlüssel**
    - Verschlüsselt jedes Datenpaket mit einem anderen Schlüssel
  - Kann mit der Brute-Force-Methode oder mit Wörterbuchangriffen auf das benutzte Passwort geknackt werden
- Deutliche Verbesserung: **Wi-Fi Protected Access 2 (WPA2)**
  - Basiert auf dem Advanced Encryption Standard (AES)
  - Ein mit einem ausreichend langen Passwort geschütztes WLAN mit WPA2-Verschlüsselung gilt aktuell als sicher
- Bester Standard aktuell: **Wi-Fi Protected Access 3 (WPA3)**
  - Implementiert ein verbessertes Schlüsselerhandlungs- und -austauschverfahren (kryptografischer Handshake), das auf dem Diffie-Hellman-Algorithmus zur Schlüsselverteilung basiert

Mehr Informationen über RC4, AES, Diffie-Hellman-Algorithmus. . .  $\implies$  Foliensätze 11 + 12

# Bluetooth

- Funksystem zur Datenübertragung auf kurzen Distanzen
  - Wurde entwickelt, um kurze Kabelverbindungen zwischen verschiedenen Geräten zu ersetzen
- Die Entwicklung wurde von der schwedischen Firma Ericsson 1994 begonnen
  - Die Weiterentwicklung erfolgt durch die Interessengemeinschaft Bluetooth Special Interest Group (BSIG)

Bluetooth wurde nach dem dänischen Wikingerkönig Harald Blauzahn benannt

Der war u.a. für seine Kommunikationsfähigkeit bekannt

- Bluetooth-Geräte senden im Frequenzblock 2,402-2,480 GHz
  - WLANs, schnurlose Telefone oder Mikrowellenherde können Störungen verursachen, wenn Sie im gleichen Frequenzband arbeiten
  - Um Störungen zu vermeiden, verwendet Bluetooth ein Frequenzsprungverfahren, bei dem das Frequenzband in 79 verschiedene Frequenzstufen im Abstand von je 1 MHz eingeteilt wird
    - Die Frequenzstufen werden bis zu 1.600 Mal pro Sekunde gewechselt







# Pairing von Bluetooth-Geräten

- Bevor 2 Endgeräte via Bluetooth miteinander kommunizieren können, müssen sie sich kennen
  - Der Vorgang des *Kennenlernens* heißt **Pairing**
- Bis einschließlich Bluetooth 2.0 ist das Pairing aufwendig
  - Beide Benutzer müssen eine identische PIN eingeben
  - Die PIN ist der gemeinsame Schlüssel für Verschlüsselung und Authentifizierung
    - Das garantiert, dass kein drittes Gerät die Verbindung mithört bzw. einen **Man-in-the-Middle-Angriff** ausübt
- Bluetooth 2.1 führte **Secure Simple Pairing** ein
  - Das Verfahren verwendet den Diffie-Hellmann-Algorithmus ( $\implies$  Foliensatz 12) zur Schlüsselverteilung anstatt einer PIN
  - Die Sicherheit dieses Pairing-Verfahrens hängt davon ab, ob die Endgeräte ein Display haben
    - Haben beide Endgeräte ein Display, müssen die Benutzer jeweils einen gemeinsamen Code durch Tastendruck bestätigen

Hat ein Gerät kein Display zum Anzeigen des Codes, ist keine Bestätigung möglich

Dann ist ein Man-in-the-Middle-Angriff ist dann nach wie vor möglich

# Übertragungsmedien

- Es existieren verschiedene Übertragungsmedien für Computernetze
- ① **Leitungsgebundene Übertragungsmedien**
  - **Elektrischer Leiter** aus Kupfer: Daten werden über Twisted-Pair-Kabel (verdrillte Kabel) oder Koaxialkabel als elektrische Impulse übertragen
  - **Lichtwellenleiter**: Daten werden als Lichtimpulse übertragen
- ② **Nicht-leitungsgebundene Übertragung** (drahtlose Übertragung)
  - **Gerichtet**:
    - **Funktechnik**: Daten werden als elektromagnetische Wellen (Radiowellen) im Radiofrequenzbereich übertragen. Beispiele sind WLAN und Satelliten-Direktfunk
    - **Infrarot**: Daten werden als elektromagnetische Wellen im Bereich des unsichtbaren Spektrums übertragen. Ein Beispiel ist IrDA
    - **Laser**: Daten werden via Laser-Bridge als Lichtimpulse übertragen
  - **Ungerichtet**:
    - Ungerichtete Übertragung basiert immer auf Funktechnik. Anwendungsbeispiele sind Mobilfunk, LTE, terrestrischer Rundfunk und Satelliten-Rundfunk



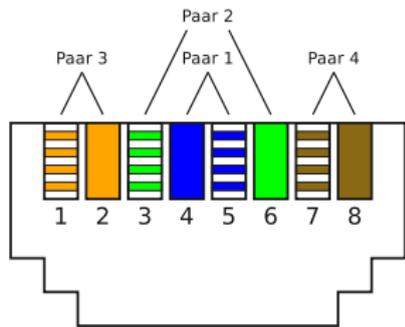
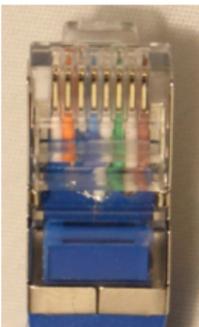






# Twisted-Pair-Kabel – *verdrillte Kabel* (1/2)

- Die Adern von Twisted-Pair-Kabeln sind paarweise miteinander verdrillt
- Verdrillte Adernpaare bieten besseren Schutz gegen magnetischen Wechselfelder und elektrostatische Beeinflussungen von außen als Adern, die nur parallel geführt sind
- Alle Varianten des Ethernet-Standards, bei denen Twisted-Pair-Kabel das Übertragungsmedium sind, verwenden Stecker und Buchsen nach dem Standard 8P8C, die meist RJ45 genannt werden























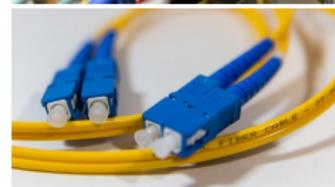
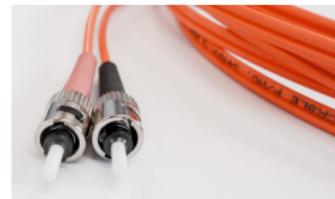




# Lichtwellenleiter

Bildquelle: pixabay.com (CC0)

- Werden häufig auch Glasfaserkabel genannt
- Verwenden Licht als Informationsträger
  - Lichtquelle: Normale LED oder Laser-LED
  - Wellenlänge: 850, 1300 oder 1550 nm
  - Ausbreitungsgeschwindigkeit des Lichts im Glas: ca. 200.000 km/s
- Vorteile gegenüber Koaxial- und TP-Kabeln
  - Ermöglichen hohe Datenübertragungsraten über große Distanzen
  - Keine elektromagnetische Abstrahlung
  - Unempfindlich gegen elektromagnetische Einflüsse
- Nachteile:
  - Höhere Kosten für die Verkabelung und aktive Komponenten (LEDs)
  - Vorhandene TP-Kabel-Infrastruktur kann nicht verwendet werden
- Wird nur da eingesetzt, wo Kupferkabel nicht leistungsfähig genug sind



# Aufbau von Lichtwellenleitern

Bildquelle (Kabel): pxhere.com (CC0)

- Ein Lichtwellenleiter besteht (von innen nach außen) aus:
  - 1 Einem lichtübertragenden Kern (*Core*) aus Quarzglas
  - 2 Um den Kern befindet sich ein Mantel (*Cladding*)
    - Hat einen niedrigeren Brechungsindex als der Kern und bewirkt durch Totalreflexion an der Grenzschicht zum Kern die Führung der Strahlung
  - 3 Den Mantel umschließt eine Schutzbeschichtung (*Coating* oder *Buffer*)
  - 4 Die letzte Schicht ist die äußere Schutzhülle (*Jacket*)

