Wireless LAN

Standards

Standard	Name	Bandbreite	Frequenz	Jahr
IEEE 802.11		2 Mbit/s	2,4 GHz	1997
IEEE 802.11a		54 Mbit/s	5 GHz	1999
IEEE 802.11b		11 Mbit/s	2,4 GHz	1999
IEEE 802.11g		54 Mbit/s	2,4 GHz	2003
IEEE 802.11n	Wi-Fi 4	600 Mbit/s	2,4 GHz / 5 GHz	2009
IEEE 802.11ac	Wi-Fi 5	1,3 Gbit/s	5 GHz	2013
IEEE 802.11ax	Wi-Fi 6	5 Gbit/s	2,4 Ghz / 5 GHz	2019

Geräte

- 802.11 NIC
- Access-Point (Autonomous / Controller-Based): verbindet 802.11 WLAN mit 802.3 Ethernet
- Wireless-Router: Access-Point, Switch, Router, Modem
- Antenne
  - Omnidirectional
  - Directional
  - MIMO (Multiple Input Multiple Output): mehrere Sende- und Empfangsantennen

Topologien

Siehe kohnlehome.de/netz/wlan-topologien.pdf

Frame-Header

- Frame Control: Protocol Version, frame Type, ...
- Duration: Remaining time to receive next Frame
- Address 1: Receiving Device or AP
- Address 2: Transmitting Device or AP
- Address 3: Destination MAC
- Sequence Control:
- Address 4: only in Ad-Hoc-mode

CSMA/CA

- half-duplex
- wait till channel is idle
- Client sends RTS (Ready To Send)
- Client waits for CTS (Clear To Send)
- All transimissions are acknowledged

Wireless Client and AP Association

- Vorgang
  - Discover a wireless AP
  - Authenticate with AP
  - Associate with AP
- Modi
  - Passive Mode: AP advertises SSID
  - Active Mode: Client must know SSID and sends Probe Request

CAPWAP (Control and Provisioning of Wireless Access Points)

- WLC (Wireless LAN Controller) manages multiple APs and WLANs.
- based on LWAPP (Lightweight Access Point Protocol)
- UDP ports 5246 and 5247
- Split MAC Architecture
  - AP MAC Functions
    - Beacons and probe responses
    - ACK and Retransmission
    - Frame queueing, prioritization
    - MAC layer data encryption and decryption
  - WLC MAC Functions
    - Authentication
    - Association and re-association of roaming clients
    - Frame translation to other protocols
    - Termination of 802.11 traffic on a wired interface decryption
- DTLS (Datagram Transport Layer Security) Encryption für control channel
- FlexConnect: Verbindung WLC - AP über WAN
  - connected mode: WLC und AP haben Verbindung
  - standalone mode: AP hat Verbindung zu WLC verloren, kann aber trotzdem alleine arbeiten

Frequency Channel Saturation

- DSSS (Direct-Sequence Spread Spectrum): Frequenzbereich wird ausgeweitet (802.11b)
- FHSS (Frequency-Hopping Spread Spectrum): schnelles Wechseln zwischen Kanälen (802.11)
- OFDM (Orthogonal Frequency-Division Multiplexing): mehrer Kanäle gleichzeitig nutzen (802.11a/g/n/ac)
- OFDMA (Orthogonal Frequency-Division Multiaccess): (802.11ax)

Channels

- 2,4 GHz: 13 Kanäle, non overlapping: 1, 6, 11
- 5 GHz: 24 Kanäle

Wireless Security

WLAN Threats

- DoS Attacks
- Rogue Access Points
- Man-in-the-Middle Attack

Secure WLANs

- SSID Cloaking
- MAC Address Filtering
- Authentication Methods
  - Open system authentication
  - PSK (Shared key authentication)
    - WEP
    - WPA (TKIP: Temporal Key Integrity Protocol)
    - WPA2 (AES: Advanced Encryption Standard, CCMP: Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)
    - WPA3
  - AAA (Authentication, Authorization, and Accounting), RADIUS (Remote Authentication Dial-In User Service): 802.1X mit EAP (Extensible Authentication Protocol
  - Automatisch
    - WPS (Wi-Fi Protected Setup)
    - DPP (Device Provisioning Protocol), auch für IoT