06 - Sítě standardu IEEE 802.11

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Standard | Alias | Pásmo | Max. Rychlost [Mbit/s] | Modulace |
| 802.11a | Wifi 1 | 5 | 54 | OFDM |
| 802.11b (krok zpět) | Wifi 2 | 2.4 | 11 | DSSS |
| 802.11g | Wifi 3 | 2.4 | 54 | OFDM |
| 802.11n | Wifi 4 | 2.4/5 | 600 | MIMO OFDM |
| 802.11ac | Wifi 5 | 5 | 3466 | MU-MIMO OFDM |
| 802.11x | Wifi 5 | 2.4/5/6 | 10530 | MU-MIMO OFDMA |

# Dělení podle dosahu

* NFC – Near Field Communication
  + Vzdálenost pár centimetrů (bezkontaktní placení)
* WPAN (Personal)
  + Malá vzdálenost, několik metrů
  + Bluetooth, ZigBee
* WLAN – IEEE 802.11
* WWAN – Mobilní sítě

# Fyzická vrstva

* Modulační signál (vstupní signál) + nosný signál = modulovaný signál (vhodný pro přenos)

## AFH – Adaptive Frequency Hopping

* Hopping = rapidní měnění nosné frekvence (změny zná vysílač i přijímač)
  + odolnost proti odposlechu
* Obsahuje mechanismus pro zjištění „dobrých a špatných“ kanálů (špatný kanál může být rušen nebo využíván)
* Přeskakuje mezi dobrými frekvencemi za účelem snížení rušení
* Využíváno technologií Bluetooth

## DSSS – Direct-Sequence Spread Spectrum

* Umělé zavedení redundance – bity určené k přenosu jsou prokládané pseudonáhodnými bity
* Díky tomu je signál méně citlivý na rušení
* Pro zařízení bez znalosti mechanismu se signál jeví jako šum
* Využívá 802.11b

## OFDM – Orthogonal Frequency-Division Multiplexing

* Kódování signálu na více nosných frekvencích pomocí různých modulací, které jsou ortogonální
* Jsou blízko sebe, dokonce se překrývají, ale jsou nezávislé/oddělitelné
* Využíván 802.11a/g/n/ac

## OFDMA – Orthogonal Frequency-Division Multiple Access

* OFDM při obsluze více uživatelů používá point-to-point a rychle mezi nimi přepíná
* OFDMA využívá point-to-multipoint – více uživatelů v jednom okamžiku
* Využíván 802.11ax, LTE, 5G

## QAM – Quadrature Amplitude Modulation

* Kombinuje amplitudovou a fázovou modulaci – dokáže přenášet více informací

## MIMO – Multiple-Input Multiple-Output

* Využívá více antén pro paralelní přenos signálů
* Zařízení příjemce musí také podporovat MIMO a paralelní signály si převede do signálu původního
* Značení např. 4x4 znamená 4 spojení na 4 anténách

## MU-MIMO – Multi-User MIMO

* Dokáže v jeden okamžik komunikovat s více zařízeními najednou
* Např. 4 antény se rozdělí mezi 4 zařízení

# Ad hoc

* WLAN, kde jsou zařízení propojena přímo, bez prostředníka (AP)
* Bluetooth

# Wi-Fi Direct

* Forma přímého p2p připojení
* Sdílení souborů, ovládání tiskárny

# Service Set

* BSS – Basic Service Set
  + Síť vytvořena z jednoho access pointu
* ESS – Extended Service Set
  + Více AP se tváří jako jedno AP (větší pokrytí)

# TWT – Target Wake Time

* Definuje čas, ve který se mohou IoT zařízení připojit k síti
* Šetří baterii
* Novinka ve Wi-Fi 6

# ESSID

* Extended Service Set Identifier
* Společný identifikátor sítě wifi ve formátu ESS (více AP)
* BSSID – MAC adresa access pointu

# Beamforming

* Signál je automaticky směrován k poloze umístění bezdrátových zařízení

# Zabezpečení bezdrátových sítí

## WEP – Wired Equivalent Privacy

* Šifrování omunikace
* Symetrická šifra
* Snadno prolomitelné

## WPA – Wi-Fi Protected Access

* Reakce na nedostatky WEP
* Šifra RC4
* TKIP – Temporary Key Integrity Protocol – Pro každý paket je používán jiný klíč (považován za nedostatečně bezpečný)

## WPA2

* Šifra AES
* Prolomeno – KRACK (2017)

## WPA-Personal (WPA-PSK – pre-shared key)

* Domácí použítí, nevyžaduje autentifikační server

## WPA-Enterprise

* Využití autentifikačního serveru (RADIUS)

## IEEE 802.1X

* Standard popisující zabezpečení přístupu do sítě a odesílání EAP zpráv po místní síti
* Suplikant, autentifikátor a autentifikační server
* Suplikant (klient) se nemůže dostat do chráněné části síte, dokud není jeho identita ověřena
* Suplikant předá požadované údaje autentifikátoru
* Ten se přepošle autentifikačnímu serveru, který rozhodne, jestli může suplikant přistoupit k síti, či nikoli

## EAP – Extensible Authentication Protocol

* Autentifikační framework
* Umožňuje výrobcům snadno vyvíjet a nasazovat nové autentifikační metody (EAP metody)

## AAA – Authentication, Authorization, Accounting

* Autentifikace – identita uživatele (kdo jsi?)
* Autorizace – k čemu máš přístup?
* Účtování – monitorování využívání sítě

## RADIUS

* AAA client/server protokol
* Back-end pro 802.1x autentifikaci