# Bezdrátové sítě - princip radiového přenosu. Rozdělení a použití elektromagnetických vln, jejich šíření, antény, základní druhy modulací, zabezpečení, autentifikace.

## WLAN (Wireless LAN)

Jedná e o bezdrátový přenos sygnálu obvkle v pásmech 2.4 nebo 5 GHz. Jedná se o přenosy v **bezlicenčním pásmu** (nikoliv licenčním). Existují také WWAN nebo WMAN.

### Standardy:

* IEEE 802.11 (neformálně WIFI)
* V Evropě HiperLAN (High Performance Radio LAN)
  + V eropě místo WLAN používal pojmenování RLAN (Radio LAN)
  + Tento standard nebyl úspěšný jako WIFI a v praxi se nikdy neuchotili
* V USA standardy HomeRF (Home Radio Frequency)

### Bezlicenční pásmo

V bezlicenčním pásmu jsou pořád nějaká pravidla pro využívání těchto pásem:

* Licenční pásma … pravidla jsou zakotvena v individuální licenci
* Bezlicenční pásma … pravidla jsou zakotvena v generální licenci

Frekvenční pásma, k jejich využití nepotřebujeme licenci. Můžeme je rovnou začít používat nepotřebujeme se někde ptát pro souhlas nebo o povolení

### Licenční vs Bezlicenční

Obsah obrázku text, snímek obrazovky, menu, Písmo

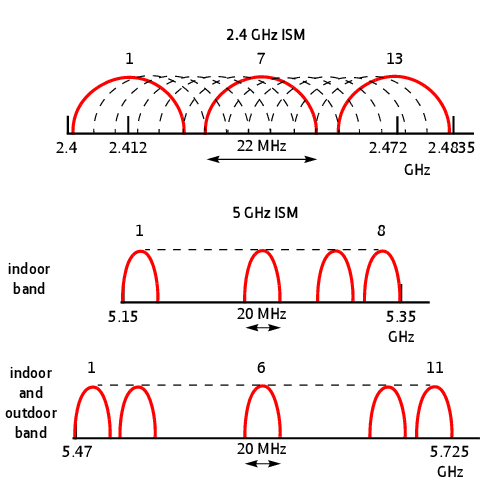
Popis byl vytvořen automaticky

Pásma využitá na bezlicenčním principu nejsou všude stejná.

V ČR

* 2.4 GHz (2400 MHz – 2483 MHz) (83.5MHz)
* 5 GHz (není spojité)
  + 5150 – 4340 MHz (200 MHz) … pouze pro indoor vyzářený výkon 200mW
  + 55470 – 5725 MHz (225MHz) … pouze pro outdoor vyzářený výkon 1W

Na pásmu 2.4 kromě WIFI je také například Bluetooth, mikrovlnné trouby, bezdrátové telefony. Nelze zabránit možnosti vzájemného rušení.



2.4 GHz je rozdělen na **14 kanálů šířky 22MHz**, které mají vzájemný **odstup 5MHz**, ale jsou širší takže se vzájemně překrývají (14 kanál má větší odstup 12MHz) né všude lze využívat všech 14 kanálu například v ČR/EU je dostupných pouze prvních 13 protože čtrnáctý už zasahuje mimo bezlicenční pásmo (USA jen prvních 11.) V ČR/EU jsou jenom tři kanály které se nepřekrývají 1,7,13 v USA 1, 6,11

Obsah obrázku text, Písmo, snímek obrazovky, číslo

Popis byl vytvořen automaticky

V 5G jsou dva nesouvislé bloky. Indoor se zkádá z osmi nepřekrývajících se kanálů (**o šířce a rozestupu 20MHz**). V outdoor pásmu je 11 nepřekrývajících se kanálů (**o šířce a rozestupu 20MHz**).

Obsah obrázku text, snímek obrazovky, Písmo

Popis byl vytvořen automaticky

Obsah obrázku text, snímek obrazovky, Písmo, menu

Popis byl vytvořen automaticky

* FHSS (Frequence hpoing) … vysílá a zkáče na jednotlivých frkvencí
* MIMO … multiple inputs mulitple outputs … vysílá a příma na více anténách
* Beam streaming … využívá směrovací antény místo všesměrových

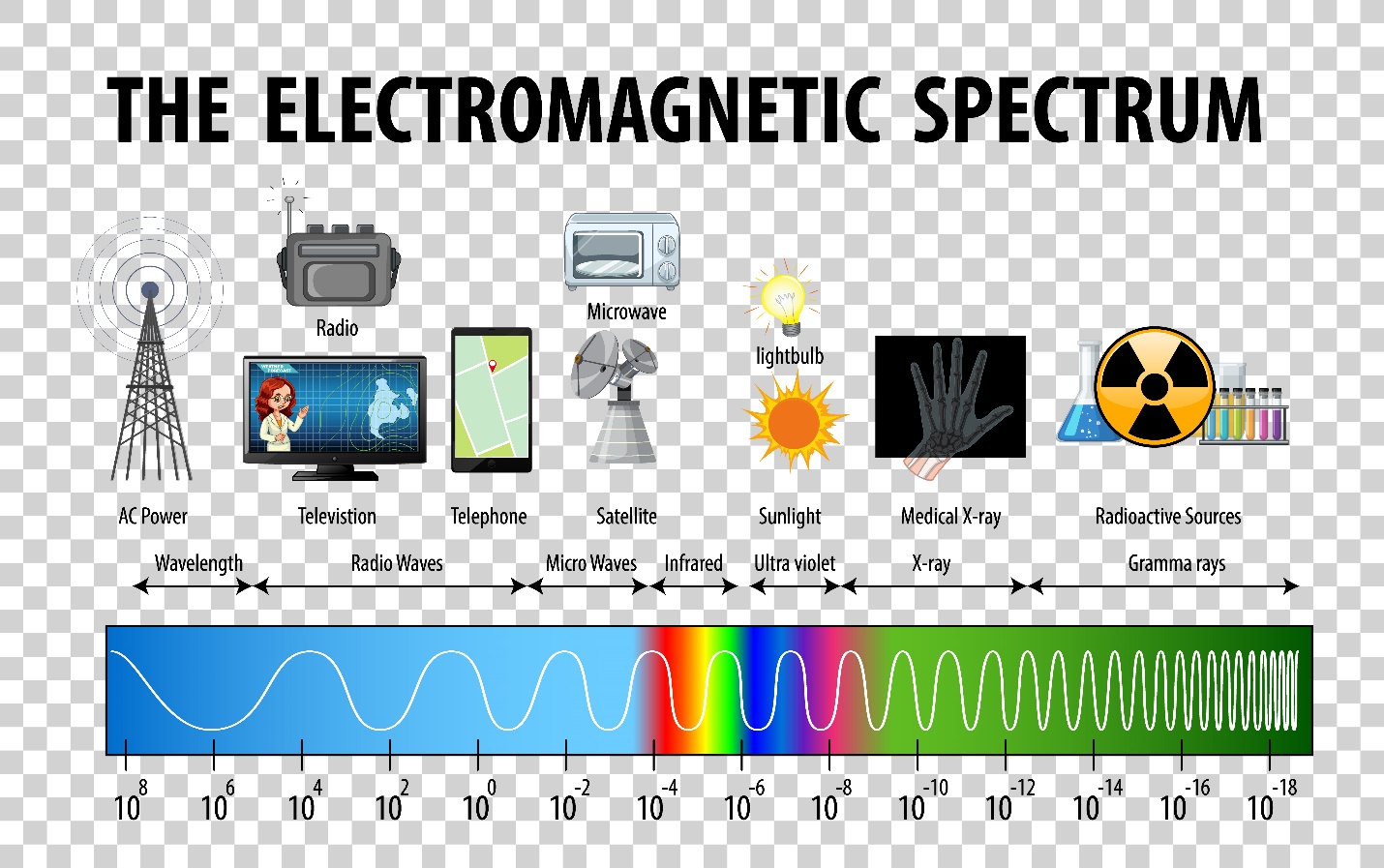
Obsah obrázku text, snímek obrazovky, Písmo, menu

Popis byl vytvořen automaticky

Obsah obrázku text, snímek obrazovky, Písmo, Tisk

Popis byl vytvořen automaticky

## Rozdělení vlnění



## Antény

je elektrotechnické zařízení pro příjem nebo vysílání rádiových vln (rádiového signálu). Antény jsou používány pro příjem rozhlasu, televize, po roce 2000 jsou široce využívány pro mobilní telefony a Wi-Fi.

**Ideální bodová** **anténa** je taková anténa která vyzářuje do všech směrů stejně, ovšem taková bodová anténa neexistuje.

Obsah obrázku text, Písmo, snímek obrazovky

Popis byl vytvořen automatickySkutečná anténa … není nikdy bodová (vyzařuje do nějakého směru více než do jiného), **zisk antény** je kolikrát více vyzařuje v daném směru více než izotopní anténa. V praxi existuje požadavek na maximální výjon e.i.r.o. tedy kolik smí (reálná) anténa vyzařovaz v libovolném směru

### Typy antén:

Každá anténa má svůj vyzařovací diagram který popisuje jak anténa vyzařuje (v jakém směru) a s jakou intenzitou (zisk)

Obsah obrázku text, snímek obrazovky, Písmo, kruh

Popis byl vytvořen automaticky

### Vysílací vyzařovací výkon

Obsah obrázku text, snímek obrazovky, design

Popis byl vytvořen automaticky

Omezení výkonu v generálního výjonu se týká vyzářeného výkonu. Směr ve kterém má anténa největší zisk nesmí překročit povolenou max hodnotu.

### Frekvence

Čím nižší je frekvence

* Lépe proniká překážkami
* Reálný dosah signálu je delší

Čím vyšší je frekvence

* Bývá k dispozici více místa (větší šířka pásma)

Čím větší (širší) je frekvenční kanál

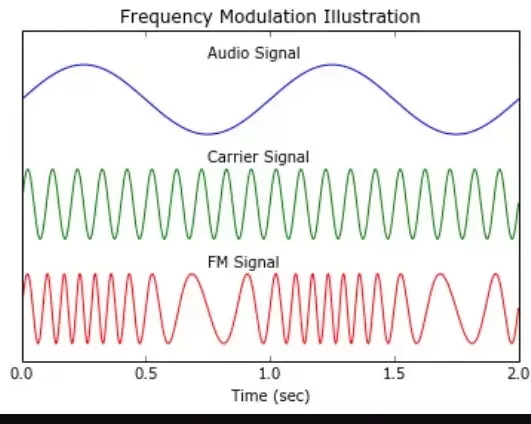
* Tím větší přenosové rychlosti lze dosáhnout (max. přenosová rychlost je lineárně závislá na šířce pásma)

Frekvence v bezlicenčních pásmech mohou mít více uživatelů … (vy smysli na stejných blízkých, překrývajících se) frekvencích můžou probíhat více souběžných přenosů, pomocí stejné WLAN

Frekvence v pásmech jsou sdílené … (vy smysli na stejných blízkých, překrývajících se) frekvencích mohou fungovat používany jiné technologie

## Modulace

* [*amplitudová modulace*](https://cs.wikipedia.org/wiki/Amplitudov%C3%A1_modulace)*(AM)* – Užitečná informace ovlivňuje **amplitudu nosného signálu**. Rozborem lze zjistit, že v signálu se objeví složky rovné součtu a rozdílu frekvencí – tak zvaná postranní pásma. Používá se pro **vysílání rozhlasu v pásmu dlouhých, středních a krátkých vln**. Analogové vysílání televize používalo pro přenos jasové složky obrazu amplitudovou modulaci s částečně potlačeným postranním pásmem. V kombinaci s fázovou modulaci je AM rozšířena pro rádiový přenos dat (včetně např. digitální televize) jako tak zvaná [kvadraturní amplitudová modulace](https://cs.wikipedia.org/wiki/Kvadraturn%C3%AD_amplitudov%C3%A1_modulace" \o "Kvadraturní amplitudová modulace) (QAM).
* [*frekvenční modulace*](https://cs.wikipedia.org/wiki/Frekven%C4%8Dn%C3%AD_modulace)*(FM)* – Užitečná informace je **kódovaná malými změnami frekvence** nosného signálu, postranních pásem je teoreticky nekonečně mnoho, ale stačí jich přenášet jen omezené množství. Protože většina rušení má amplitudový charakter, lze je v přijímači FM odstranit amplitudovou limitací. FM se používá pro **rozhlasové vysílání v pásmu** VKV, především regionálními stanicemi.
* [*fázová modulace*](https://cs.wikipedia.org/wiki/F%C3%A1zov%C3%A1_modulace)*(PM)* – Je **velmi podobná frekvenční modulaci**.
  + výhody a nevýhody jsou podobné jako FM, dalo by se říci, že PM je speciální druh FM
  + použití: **při přenosu digitálních signálů** (PSK – Phase Shift Keying)
* *ON/OFF – modulace* – označovaná též „nemodulovaný signál“ ([anglicky](https://cs.wikipedia.org/wiki/Angli%C4%8Dtina" \o "Angličtina) *Continuous Wave*, *CW*), lze ji též považovat za dvoustavovou stoprocentní [amplitudovou modulaci](https://cs.wikipedia.org/wiki/Amplitudov%C3%A1_modulace" \o "Amplitudová modulace) – užitečná **informace je kódovaná úplným přerušováním nosného signálu**, používá se pro **přenos [Morseovy abecedy](https://cs.wikipedia.org/wiki/Morseova_abeceda" \o "Morseova abeceda)**



## Autentifikace

WPA (Wifi protected access), WPA2, WPA3 jsou tři zabezpečovací certifikační program vyvinuty WI-FI Alliance k zabezpečení bezdrátové sítě po roce 2000. WPA2 se stala tak používaná až pro ní vytvořil IEEE standard 802.11i.

### WPA

Implementovala Temporal Key Integrity Protocol (TKIP). Využívá 64-botvý nebo 128-bitový šifrovací klíč který musí být manuálně zapsaný na bezdrátovém access pointu a zařízení a nesmí být měněno. TKIP employs a per-packet key znamená že generuje nový 128-bitový klíč pro každý paket tím pádem zabraňuje útoku s kterým měl problém jeho předchůdce WEP.

Také obsahuje Message Integrity Check, který je navržen k zabránění útočníkovy změnit paket a znovu ho poslat. WPA využívá algoritmus TKIP pomocí kterého kontroluje message integrity.

### WPA2

Nahrazuje WPA v roce 2004. WPA2, který vyžaduje testování a certifikace od Wi-Fi Alliance implementuje hlavní element IEEE 802.11i zejména obsahuje hlavní podporu CCMP (AES-base šifrovací mód). Stává se hlavním protokolem využívající na WLAN zařízeních. CCMP je samozřejmě mnohem silnější než TKIP.

### WPA3

Jedná se v dnešní době o jeden z nejvíce používaných protokolů na zařízeních které vlastní "Wi-Fi CERTIFIED™" logo od poloviny roku 2020. Jendá se o náhradu za WPA2. Používá ekvivalent 192-bitového kryptografické síly v WPA3-Enterprise mode (AES-256 in GCM mode with SHA-384 as HMAC) a stále využívá CCMP-128 (AES-128 in CCM mode) jako minimun šifrování v WPAR-Personal mode.

WPA3 také nahradilo pre-shared key (PSK) za Simultaneous Authentication of Equals (SAE), metodu původně představenou již v IEEE 802.11s. Výsledkem je více bezpečný počáteční key Exchange v personal mode a forward secrecy (zajistíme za pomocí toho že při každé další komunikaci vytváříme nový privátní klíč).

### WPA-Personal

WPA-Personal je označováno i jako WPA-PSK. Nevyžaduje autentizační server, pro autentizaci je použito sdílené tajemství ([Pre-shared key](https://cs.wikipedia.org/wiki/Pre-shared_key)), což je delší [heslová fráze](https://cs.wikipedia.org/wiki/Heslov%C3%A1_fr%C3%A1ze" \o "Heslová fráze), která je uložena na [přístupovém bodu](https://cs.wikipedia.org/wiki/P%C5%99%C3%ADstupov%C3%BD_bod" \o "Přístupový bod) (AP) i na připojovaném klientovi. Předsdílený klíč je buď 64 hexadecimálních čísel nebo 8 až 64 tisknutelných znaků (klíč je odvozen z heslové fráze a názvu [SSID](https://cs.wikipedia.org/wiki/SSID) použitého jako [sůl](https://cs.wikipedia.org/wiki/S%C5%AFl_(kryptografie)" \o "Sůl (kryptografie))). PSK je dostupné pro WPA i WPA2.

### WPA-Enterprise

WPA-Enterprise je označováno i jako *WPA-802.1X mode*. Vyžaduje autentizační [RADIUS](https://cs.wikipedia.org/wiki/RADIUS) server s podporou protokolu [IEEE 802.1X](https://cs.wikipedia.org/wiki/IEEE_802.1X), což je složitější pro nastavení, avšak umožňuje dodatečné zabezpečení (slovníkové útoky na hesla, hlídání kvality hesel, uživatelé nechtějí prozrazovat vlastní hesla, zatímco sdílené heslo prozradí snadněji). Umožňuje i další varianty [EAP](https://cs.wikipedia.org/wiki/Extensible_Authentication_Protocol) autentizace (např. pomocí certifikátů).

### Wi-Fi Protected Setup

[Wi-Fi Protected Setup](https://cs.wikipedia.org/wiki/Wi-Fi_Protected_Setup) zjednodušuje připojení k zabezpečené síti pomocí číselného PIN kódu, ale vytvořilo [zranitelnost](https://cs.wikipedia.org/wiki/Zranitelnost" \o "Zranitelnost) spočívající v uhádnutí PIN pomocí [útoku hrubou silou](https://cs.wikipedia.org/wiki/%C3%9Atok_hrubou_silou" \o "Útok hrubou silou).