

## Princip bezdrátové komunikace

- spočívá v přenosu dat mezi zařízeními prostřednictvím elektromagnetických vln bez potřeby fyzického spojení pomocí kabelů. Zařízení používají rádiové vlny k vytvoření bezdrátového spojení, které umožňuje přenos dat mezi zařízeními, jako jsou počítače, smartphony, tablety nebo další bezdrátová zařízení.

## Přínosy bezdrátové komunikace zahrnují:

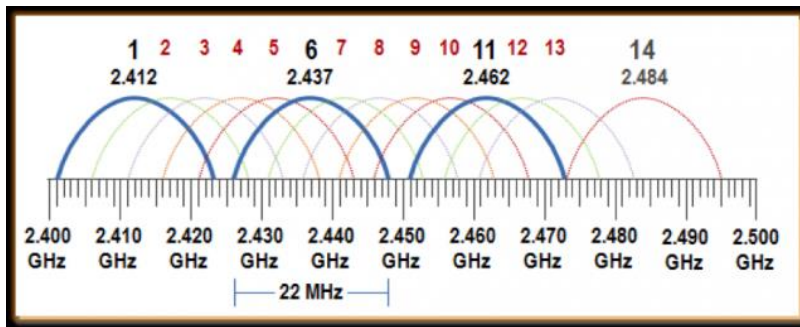
- **Mobilita:** Bezdrátová komunikace umožňuje zařízením komunikovat bez omezení kabely, což umožňuje větší mobilitu uživatelů. Umožňuje uživatelům přístup k síti a komunikaci odkudkoli v dosahu bezdrátové sítě.
- **Flexibilita:** Bezdrátové sítě jsou flexibilní a mohou být snadno přizpůsobeny různým prostředím a požadavkům. Nemusíte instalovat fyzické kabely nebo se starat o jejich údržbu.
- **Skalovatelnost:** Bezdrátové sítě umožňují snadnou rozšiřitelnost, což umožňuje přidání nových zařízení do sítě bez nutnosti rozšiřování kabelové infrastruktury.
- **Snadná instalace:** Instalace bezdrátových sítí je obvykle jednodušší a rychlejší než instalace kabelových sítí, což šetří čas a náklady spojené s implementací.
- **Pohodlnost:** Bezdrátové sítě umožňují jednodušší a pohodlnější připojení k síti, bez nutnosti fyzického připojení kabely.

## Omezení bezdrátové komunikace zahrnují:

- **Omezený dosah:** Dosah bezdrátových sítí může být omezený a závisí na mnoha faktorech, jako je síla signálu, překážky v prostoru, interference atd.
- **Interference:** Bezdrátové sítě mohou být náchylné k rušení a interferencím způsobeným jinými zařízeními, která používají stejné frekvenční pásma, což může mít za následek sníženou kvalitu a stabilitu spojení.
- **Bezpečnost:** Bezdrátové sítě mohou být náchylné k různým bezpečnostním hrozbám, jako jsou odposlech, neoprávněný přístup, útoky typu "man-in-the-middle" atd., což vyžaduje adekvátní bezpečnostní opatření.

## Co se týče technologií a standardů bezdrátových sítí (WLAN), existuje několik různých standardů, které jsou používány pro bezdrátovou komunikaci. Mezi nejběžnější patří:

- **IEEE 802.11:** Jedná se o soubor standardů definovaných IEEE pro bezdrátovou komunikaci. Mezi nejběžnější standardy patří 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac a 802.11ax, které se liší v rychlosti, dosahu a používaném frekvenčním pásmu.
- **Frekvenční pásma:** Bezdrátové sítě pracují v různých frekvenčních pásmech, které jsou regulovány pro bezdrátovou komunikaci. Nejběžnější frekvenční pásma používaná pro WLAN jsou 2,4 GHz a 5 GHz.
- **Kanály:** Bezdrátové sítě používají kanály pro komunikaci. Kanály jsou definovány v rámci frekvenčního pásma a umožňují různým zařízením komunikovat bez vzájemného rušení. Kanály mohou být široké nebo úzké a jejich volba závisí na používaném standardu a prostředí sítě.



- **Formy uspořádání v síti:** Bezdrátové sítě mohou mít různé formy uspořádání, jako je infrastrukturní mód, kde jsou zařízení připojena k centrálnímu přístupovému bodu (Access Point), nebo ad-hoc mód, kde zařízení komunikují přímo mezi sebou bez centrálního bodu.
- **Základní typy bezdrátových zařízení:** Mezi základní typy bezdrátových zařízení patří přístupové body (Access Points), které slouží jako centrální body pro připojení klientů do sítě, a klienti, jako jsou počítače, smartphony, tablety, tiskárny atd., které jsou připojeny k přístupovým bodům.
- **Identifikátory:** Bezdrátové sítě používají identifikátory pro jednoznačné identifikování jednotlivých sítí a klientů. Nejběžnějším identifikátorem je Service Set Identifier (SSID), což je název sítě, který se zobrazuje při vyhledávání dostupných sítí na zařízeních klientů. Dalším identifikátorem je Media Access Control (MAC) adresa, která je přiřazena každému síťovému rozhraní a slouží k jednoznačnému identifikování zařízení v síti.

## Celkově lze shrnout některé přínosy a omezení bezdrátových sítí (WLAN) následovně:

### Přínosy WLAN:

- **Mobilita:** Bezdrátové sítě umožňují přístup k síti z různých míst a za různých podmínek, což poskytuje uživatelům vyšší míru mobility a flexibility.
- **Snadná instalace a škálovatelnost:** Bezdrátové sítě lze snadno nainstalovat a rozšířit, což umožňuje rychlou implementaci sítě v nových prostorách nebo rozšíření stávající sítě.
- **Snížení nákladů na kabeláž:** Bezdrátové sítě nepotřebují fyzickou kabeláž, což může snížit náklady na instalaci a údržbu sítě.
- **Flexibilita umístění zařízení:** Bezdrátová zařízení mohou být umístěna tam, kde je kabeláž obtížná nebo nemožná, což umožňuje lepší umístění zařízení pro optimální pokrytí a výkon sítě.
- **Možnost sdílení sítě:** Bezdrátové sítě umožňují jednodušší sdílení sítě mezi různými zařízeními a uživateli, což usnadňuje komunikaci a spolupráci.

### Omezení WLAN:

- **Omezený dosah:** Dosah bezdrátových sítí může být omezený, zejména ve srovnání s kabelovými sítěmi. Signál může být oslaben překážkami, jako jsou stěny, a interferencí z jiných zařízení.
- **Omezená šířka pásma:** Bezdrátové sítě mají omezenou šířku pásma ve srovnání s kabelovými sítěmi, což může ovlivnit rychlost a výkon sítě.
- **Bezpečnostní rizika:** Bezdrátové sítě mohou být náchylné k různým bezpečnostním hrozbám, jako jsou neoprávněný přístup, odposlech nebo útoky typu "man-in-the-middle". Správné zabezpečení a konfigurace bezdrátových sítí je klíčovým faktorem pro minimalizaci bezpečnostních rizik.
- **Interference:** Bezdrátové sítě mohou být náchylné na rušení od jiných zařízení, která používají stejné frekvenční pásmo, což může ovlivnit výkon a spolehlivost sítě.
- **Správa a konfigurace:** Správa a konfigurace bezdrátových sítí může být náročnější ve srovnání s kabelovými sítěmi, zejména pokud jde o správu kanálů, identifikátorů a bezpečnostních nastavení.

## Bezpečnostní mechanismy WLAN:

- Šifrování: Použití šifrování, jako je například WPA (Wi-Fi Protected Access) nebo WPA2, které zajišťuje šifrování komunikace mezi klienty a přístupovým bodem, a tím chrání data před neoprávněným přístupem.
- Autentizace: Použití autentizačních mechanismů, jako je například WPA-PSK (Pre-Shared Key) nebo WPA2-Enterprise, které zajišťuje ověření klientů před povolením přístupu do sítě.
- Filtrace MAC adres: Omezení přístupu do sítě pouze na povolené MAC adresy, což umožňuje kontrolu přístupu zařízení na základě jejich jedinečné MAC adresy.
- Výkonnostní nastavení: Použití nastavení, která minimalizují výkon sítě, jako je například vypnutí SSID broadcastu, aby se snížila viditelnost sítě, a tím minimalizovalo riziko neoprávněného přístupu.
- Monitoring a aktualizace: Pravidelné monitorování a aktualizace přístupových bodů, firmware a bezpečnostních nastavení, aby se minimalizovala rizika spojená s bezpečností sítě.

Je důležité si uvědomit, že bezpečnost bezdrátových sítí je dynamický proces a vyžaduje pravidelnou aktualizaci a správu, aby se minimalizovala rizika spojená s používáním bezdrátových sítí.