# 13. WLAN, PoE, Radius

## Teoretická část

**Vysvětlete a popište vše, co více o Wireless LAN(Wi-fi, Bluetooth) – Frekvence,** **antény,** **zabezpečení a HW.**

**Popište, k čemu slouží POE.**

**Vysvětlete a popište, jakou roli hraje ve WLAN Radius server. Popište, jak pracuje a jaké používá zabezpečovací metody.**

## Praktická část

1. **Nakreslete a popište vyzařovací směry a úhly jednotlivých antén.**
2. **Nakreslete a vysvětlete jakým způsobem se AP a klient spojí a jak se šíří signál.**

## Doplňující otázky

1. **Popište výhody a nevýhody WI-Fi a BT sítí.**

# WLAN

WLAN je zkratka anglických slov Wireless Local Area Network nebo též Wireless LAN. Znamenají „bezdrátová místní síť“.  
Je to typ místních sítí, které jako přenosové médium používají elektromagnetické rádiové vlny v pásmech řádu GHz (gigahertzů).

V roce 1985 takto americký regulátor uvolnil pro bezlicenční využití celkem tři rozsahy frekvencí ve dvou pásmech, označovaných jako “ISM“ (pro využití v oblasti průmyslu, vědy a zdravotnictví), a UNII (Unlicensed National Information Infrastructure). Jsou to pásma bezlicenční.

I pro pásma, využívaná na bezlicenční principu, vždy existují určitá pravidla, která říkají, co a jak se v nich smí a co naopak nesmí. Například, jaké vysílací výkony nesmí být překročeny. Nebo když dojde k rušení, že musí přestat vysílat ten, kdo začal jako poslední. Všechna takováto pravidla pak jsou zakotvena v “generálních licencích“.



Americký regulátor podmínku, že v těchto nově bezlicenčních pásmech mají být používána řešení „široko-pásmová“, fungující na principu rozprostření do širšího spektra (spread spectrum), která jsou podstatně šetrnější k životnímu prostředí.

## Širokopásmové vysílání

Při “širokopásmovém“ přenosu se využívají takové techniky, které umožňují, aby vysílač vysílal v širším rozsahu frekvencí (aby své vysílání doslova „rozprostřel do širšího spektra“), a mohl vysílat jen s nižší intenzitou, která ani nemusí přesahovat hladinu šumu. Podstatné je to, aby příjemce věděl, jakým způsobem k „rozprostření do šířky“ došlo, a uměl zpětně extrahovat užitečný signál, smíchaný s šumem.

# Rozsahové kanály

Dosahování co možná nejvyšších (nominálních i efektivních) přenosových rychlostí je u technologií IEEE 802.11 komplikováno také tím, že rozsahy frekvencí v příslušných bezlicenčních pásmech jsou omezené. Rozsah 2,400 až 2,4835 GHz, pásmo široké pouze 83,5 MHz. Přitom technologie IEEE 802.11b potřebují ke své práci frekvenční kanály o šířce 22 MHz. Praxe ale počítá s přeci jen větším počtem kanálů, které ovšem „nahušťuje“ do stejně širokého rozsahu.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kanál č.** | **Rozsah frekvencí** | **USA** | **Evropa** | **Japonsko** |
| 1 | 2401-2423 | x | x | x |
| 2 | 2406-2428 | x | x | x |
| 3 | 2411-2433 | x | x | x |
| 4 | 2416-2438 | x | x | x |
| 5 | 2421-2443 | x | x | x |
| 6 | 2426-2448 | x | x | x |
| 7 | 2431-2453 | x | x | x |
| 8 | 2436-2458 | x | x | x |
| 9 | 2441-2463 | x | x | x |
| 10 | 2446-2468 | x | x | x |
| 11 | 2451-2473 | x | x | x |
| 12 | 2456-2478 | - | x | x |
| 13 | 2461-2483 | - | x | x |

## Přístupová metoda CSMA/CA

V případě bezdrátového Ethernetu: uzel, který zjistí, že právě vysílá někdo jiný, to okamžité „vzdá“, odmlčí se na náhodně dlouhou dobu a teprve pak vše zkouší znovu.

# Topologie Wi-Fi

V případě bezdrátových sítí Wi-Fi máme v zásadě stejné dvě možnosti propojení, jako u drátového Ethernetu. Jen se jim pochopitelně říká jinak. Označují se totiž jako „režimy“, a to:

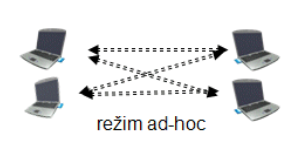
* **režim infrastruktury (infrastructure mode)**

V případě režimu infrastruktury je koncový uzel označován jednoduše jako „stanice“, zatímco analogií rozbočovače (HUB) je zde tzv. přístupový bod (v angličtině Access Point, zkratkou AP). Beze změny, oproti drátové variantě, je to, že v tomto komunikace vždy prochází přes přístupový bod, zatímco koncové stanice nikdy nekomunikují přímo mezi sebou.



* **režim ad-hoc (ad-hoc mode)**

Naopak v režimu ad-hoc žádný přístupový bod (AP) není, a jednotlivé koncové stanice zde komunikují mezi sebou přímo. Díky bezdrátovému charakteru může jít o komunikaci mezi více dvojicemi koncových uzlů (nikoli ale ve stejném čase). V případě drátového propojení by k něčemu takovému bylo zapotřebí u každého uzlu více ethernetových rozhraní, ale u bezdrátového řešení stačí jen jediné rádiové rozhraní. Proto si režim ad-hoc můžeme představit, jako komunikaci mezi více koncovými stanicemi, ovšem vždy jen „po dvojicích“ a přímo, bez prostředníka.



# Autentizace a asociace u Wi-Fi

U bezdrátových sítí Wi-Fi je ale všechno jinak. Zde je vazba mezi koncovými stanicemi a přístupovým bodem podstatně volnější a také dynamická, protože se může měnit v čase (stanice se mohou pohybovat).

Přístupové body Wi-Fi jsou za tímto účelem vybaveny řadou služeb, mezi které patří (mimo jiné) schopnost:

* **autentizace:** v rámci této funkce přístupový bod zjišťuje, o jakou stanici jde, resp. zda je skutečně tím, za koho se vydává.
* **asociace:** v rámci této funkce dochází ke vzniku logické vazby mezi přístupovým bodem a konkrétní stanicí. Stanice je „přidružena“ (tzv. asociována) k danému přístupovému bodu.
* **de-asociace:** opak asociace, dochází k uvolnění (zrušení) vazby mezi přístupovým bodem a koncovou stanicí.

# Zabezpečení sítě

**WEP** (Wired Equivalent Privacy, tj. soukromí ekvivalentní drátovým sítím) je v označení pro zastaralé zabezpečení bezdrátových sítí podle původního standardu IEEE 802.11. Cílem WEP bylo poskytnout zabezpečení obdobné drátovým počítačovým sítím (např. kroucená dvojlinka), protože rádiový signál je možné snadno odposlouchávat i na delší vzdálenost bez nutnosti fyzického kontaktu s počítačovou sítí. WEP byl prolomen v srpnu 2001.

**WPA2** implementuje všechny povinné prvky IEEE 802.11i. Konkrétně přidává nový algo-ritmus CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) založený na AES, který je považován za zcela bezpečný. Od 13. března 2006 je certifikace WPA2 povinná pro všechna nová zařízení, jež chtějí být certifikována jako Wi-Fi.

**SSID** (Service Set Identifier) je jedinečný identifikátor každé bezdrátové (WiFi) počítačové sítě. Přístupový bod (AP) vysílá pravidelně každých několik sekund svůj identifikátor v takzvaném majákovém rámci (beacon frame) a klienti si tak mohou snadno vybrat, ke které bezdrátové síti se připojí. Parametr SSID se skládá z řetězce ASCII znaků dlouhého maximálně 32 znaků.

## Bezpečnostní opatření

Existuje řada bezpečnostních opatření, které se liší ve své efektivitě a praktičnosti.

### Skrytí SSID

Nejjednodušší, ale neefektivní metodou zabezpečení bezdrátové sítě, je skrytí [SSID](https://cs.wikipedia.org/wiki/SSID) (identifikátoru bezdrátové sítě). Přístupový bod poté nevysílá identifikátor SSID. Tato metoda poskytuje velmi malou ochranu proti většině útoků, protože je možné identifikátor SSID velmi jednoduše odposlechnout (přenáší se v otevřené formě).

### Filtrování MAC adres

Jedna z nejjednodušších technik je povolení přístupu pouze předem schváleným [MAC adresám](https://cs.wikipedia.org/wiki/MAC_adresa). Většina přístupových bodů obsahuje filtr MAC adres. Vzhledem k tomu, že se přenášené MAC adresy nijak nešifrují, může je útočník jednoduše odposlechnout a následně naklonovat na svoji síťovou kartu. Poté se může vydávat za libovolného klienta a přístup mu je povolen.

### Statické IP adresy

Přístupové body většinou klientům přidělují [IP adresy](https://cs.wikipedia.org/wiki/IP_adresa) pomocí [DHCP](https://cs.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol). Vyžadování ručního nastavení IP adresy klientem ztíží průnik do sítě méně sofistikovaným útočníkům, ale poskytuje malou ochranu proti zkušeným vetřelcům.

## 

## Připojení k AP

Klienti se k přístupovému bodu připojují (ascociují se), přičemž mohou být vůči nim uplatněna omezení a přístup odepřen. Komunikace mezi klienty probíhá prostřednictvím přístupového bodu, tj. minimálně dva skoky (nejprve na přístupový bod a z něj pak na příslušnou protistanici). Klient tak udržuje spojení jen s přístupovým bodem a nemusí mít cílovou stanici ani v přímém rádiovém dosahu. Přístupový bod může rozpoznat, zda klient přešel do úsporného režimu a do jeho probuzení dočasně uchovat přicházející data, což může vést k úsporám výdrže baterií klienta.

## Šíření signálu:

Při navrhování Wi-Fi sítě, natočení antén a rozmístění Wi-Fi routerů musíte také brát v úvahu povahu prostředí, ve kterém bude signál šířen. Jde hlavně o materiály, ze kterých jsou složeny zdi a stropy či jiné elementy ve vnitřních prostorách, které by mohly ovlivnit šíření signálu. Venku jde zase o stromy, další domy, ale i oblačnost či mlhy.

Rádiový signál podléhá prostředí stejně jako světlo. Může být zcela odražen (hladké neabsorbující povrchy), čímž je zcela změněn jeho směr. Nebo může být lomen, kdy je část signálu odražena a část projde materiálem dále, ale pod jiným úhlem. Dále může dojít k difrakci vln, které jsou deformovány, resp. ohnuty například předmětem v místnosti nebo budovou. Na nerovných površích se spoustou hran pak může dojít k odražení signálu do více směrů, a tím k jeho rozptýlení. A nakonec může signál narazit na takový materiál, který jej může zcela absorbovat a neefektivně přeměnit na teplo.

## Antény

Wi-Fi antén je více druhů a každá se hodí na specifické použití. Základními třemi druhy jsou všesměrové (omni-directinal), sektorové (semi-directional) a úzcesměrové (highly-directional). Všesměrové můžete potkat na Wi-Fi routerech v různých velikostech, a tedy s různým ziskem udávaným v decibelech v porovnání s izotropní anténou (dBi).

Ačkoliv se může zdát, že čím větší anténa a její zisk, tím lepší, není tomu vždy pravda. S vyšším ziskem antény se totiž nezvyšuje oblast pokrytí, ale jeho dosah. Vysílání z všesměrové Wi-Fi antény si můžete přestavit jako „koblihu“ kolmou k anténě, kde je její průměr, a tedy dosah signálu, přímo úměrný zisku antény. Se zvyšujícím se průměrem ale klesá tloušťka této „koblihy“. To znamená, že s anténou s větším ziskem (např. 7 dBi) skvěle pokryjete přízemí, ale v dalším patře nebude signál. Nebo bude, ale jen velmi slabý – pocházející z tzv. postranních laloků.

# POE

PoE (Power over Ethernet) je napájení po datovém síťovém kabelu, bez nutnosti přivést napájecí napětí k přístroji dalším samostatným kabelem.

Již nyní se s obdobou tohoto standardu můžeme setkat u napájení Wifi AP, kde se však využívají jen volné páry vodičů, a zapojení tak nelze aplikovat u gigabitových sítí.

Napájení po ethernetu se začalo výrazně prosazovat s nástupem internetové telefonie - [VoIP](https://cs.wikipedia.org/wiki/VoIP). Dosavadní analogové nebo digitální (ISDN) telefony jsou co do napájení velmi nenáročné a vystačí obvykle s jedním párem vodičů zajišťujících jak komunikaci tak i napájení.

VoIP má své nesporné výhody, ale napájení přístrojů — [IP telefonů](https://cs.wikipedia.org/wiki/IP_telefon) zvláštním kabelem bylo jednou ze zřejmých a závažných nevýhod. Běžné síťové přepínače neposkytovaly na svých rozhraních napájení pro připojené přístroje (PC, tiskárny, servery, datové terminály), předpokládal se vždy samostatný zdroj. Nástup VoIP na přelomu tisíciletí vyvolal tlak na řešení této otázky. Proto se kromě injektorů a pasivních napájecích panelů objevily i přepínače s napájecími porty. Jejich vyšší cena je vyrovnána zjednodušeným zapojením, možností centrální správy nyní nově i včetně napájení, úsporou kabelů atd. jak bylo uvedeno výše.

## Smysl PoE

* Ušetřit kabely
* Zjednodušit připojování přístrojů; zapojuje se jen 1 datový konektor místo 2 (data + napájení)
* Umožnit správci sítě snadný dálkový restart napájeného přístroje na konci kabelu vypnutím a zapnutím napájení pomocí příkazu na portu (síťový LAN přepínač s napájecími porty)..

## Přístroje napájeny přes Ethernet

* webové LAN kamery
* bezdrátové přístupové body ([Wi-Fi](https://cs.wikipedia.org/wiki/Wi-Fi) access-pointy)
* IP telefony

# RADIUS SERVER

**RADIUS (Remote Authentication Dial In User Service**, česky **Uživatelská vytáčená služba pro vzdálenou autentizac**i) je [**AAA protokol**](https://cs.wikipedia.org/wiki/AAA_protokol) (**authentication, authorization and accounting**, česky autentizace, autorizace a účtování) používaný pro přístup k síti nebo pro [IP](https://cs.wikipedia.org/wiki/Internet_Protocol) mobilitu. Může pracovat jak lokálně tak i v roamingu.

Mezi nejdůležitější vlastnosti patří jeho vysoká síťová bezpečnost, neboť transakce mezi klientem a RADIUS serverem je autentizována pomocí sdíleného tajemství, které není nikdy posíláno přes síť. Všechna uživatelská jména jsou přes síť zasílána šifrovaně.

## Postup ověření uživatele

Postup autentizace je následující: uživatel vydá klientovi Požadavek na autentizaci, klient vytvoří Požadavek na přístup (Access Request) obsahující uživatelské jméno, heslo a ID portu, přes který je uživatel připojen. Požadavek na přístup je odeslán RADIUS serveru a čeká se na odpověď. Pokud nepřijde do určeného času (timeoutu) žádná odezva, Požadavek na přístup se opakuje, zpravidla 3 až 5 krát.

Pokud není splněna některá z podmínek, RADIUS server odešle Zamítnutí přístupu (Access Reject). Do datové oblasti paketu je dovoleno umístit maximálně textovou zprávu, která smí být zobrazena pomocí klienta uživateli. Žádné další atributy nejsou v odpovědi Access Reject povoleny.

Jestliže jsou všechny podmínky splněny, RADIUS server odešle Povolení přístupu (Access Accept), kde v datové oblasti paketu jsou uloženy všechny potřebné konfigurační informace (IP adresa, maska sítě, login uživatele a vše, co je potřeba předat požadované službě).

## Praktická část

1. Nakreslete a popište vyzařovací směry a úhly jednotlivých antén.

Všesměrová:

Sektorová:

Směrová:

# BT vs WLAN

Bluetooth je pouze PAN. = Osobní/malinká síť

WLAN je Wireless LAN. = Lokální/větší síť