# 4. Bezdrátové sítě

Vývoj Ethernetu se neubíral pouze cestou zrychlování a zvětšování dosahu „po drátech“, ať již po kroucené dvoulince či po optických vláknech. Časem zákonitě došlo i na myšlenku, zda to nezkusit bez drátů. A to i bez jména „Ethernet“, kterého se bezdrátová verze časem zbavila. Dnes o ní nejčastěji hovoříme jako o technologii Wi-Fi.

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.

## Úzkopásmové vysílání

Při klasickém vysílání (tzv. „úzkopásmovém“) je energie vyzařovaná vysílačem soustředěna do úzkého rozsahu frekvencí, a svou intenzitou musí převýšit úroveň šumu, neboť příjemce vyhodnocuje fakticky jen to, co přesáhne hladinu šumu.



## Širokopásmové vysílání - Wifi

Ovšem 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. Naopak tomu, kdo potřebné informace o způsobu rozprostření nemá, se přijímaný signál jeví jen jako neužitečný šum. Výsledným efektem je pak větší robustnost přenosů, a naopak menší šance vzájemného ovlivňování různých přenosů.



Po uvedení tohoto způsobu byla zhotovena nová skupina.  
  
Bezdrátová varianta Ethernetu od začátku měla svou vlastní pracovní skupinu, očíslovanou jako IEEE 802.11. Teprve v roce 1997 se totiž podařilo najít v rámci pracovní skupiny 802.11 shodu na tom, jak by celé řešení mělo vypadat. Takže teprve tehdy se zrodil první standard bezdrátové varianty Ethernetu, označovaný podle svého původu jako „IEEE 802.11“.

Nepleťte si tento standart s dnešními Wi-fi. Dokázal totiž přenášet data (nominální) rychlostí jen 1 či 2 megabity za sekundu. Už měl ale vyvinuty ty přístupové metody, které používá i dnešní Wi-FI.

# Varianty vysílání

První varianta bezdrátového Ethernetu, kterou je standard IEEE 802.11 (pozor, ještě bez dalšího rozlišujícího písmene na konci), počítala celkem se třemi způsoby vysílání a přenosu dat bezdrátovým éterem.

## Frequency hopping

Jde o rychlé přeskakování z jedné frekvence na druhou, resp. z jednoho úzkého frekvenční-ho kanálu na jiný, způsobem který může vypadat jako zcela náhodný, ale oběma komunikujícím stranám je do-předu znám (je tzv. pseudonáhodný).

## Difuse InfraRed

Další možností, kterou mohl bezdrátový Ethernet využívat, byly infračervené přenosy. Ovšem tato varianta se používala zcela minimálně, protože bylo zapotřebí mít dobrou viditelnost mezi jednotlivými body.

## Direct Sequence Spread Spectrum

Naopak jako nejperspektivnější se ukázala třetí varianta, označovaná jako „přímé rozprostření do spektra“, resp. „s přímou modulací kódovou posloupností“. Ta už nepočítá s přeskoky či jinými změnami frekvencí, ale s tím, že se trvale vysílá v širším rozsahu frekvencí. Navíc se zde nevysílají přímo jednotlivé datové bity, ale místo nich celé sekvence bitů, označované jako tzv. chipy. Můžeme si to představit tak, že pokud je třeba přenést nulový datový bit, vyšle se místo něj skupina bitů tvořících chip. Pokud se naopak má přenést jedničkový datový bit, vyšle se místo něj stejná sekvence bitů (chip), ale invertovaná.



# 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, a to poměrně výrazně. Například když se hovoří o tom, že IEEE 802.11b pracuje „v pásmu 2,4 GHz“, ve skutečnosti to znamená jen možnost fungování v rozsahu 2,400 až 2,4835 GHz, neboli v pásmu širokém pouze 83,5 MHz.

Přitom technologie IEEE 802.11b potřebují ke své práci frekvenční kanály o šířce 22 MHz. Na otázku, kolik se jich „vejde“ do pásma 2,400 až 2,4835 GHz, alias 83,5 MHz, je jednoduchá odpověď: pokud se nemají překrývat, pak jen tři!

Praxe ale počítá s přeci jen větším počtem kanálů, které ovšem „nahušťuje“ do stejně širokého rozsahu – tak-že se přitom nutně z části překrývají. Konkrétně tak, že odstup mezi těmito kanály, širokými 22 MHz, je pouze 5 MHz.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |
| 14 | 2466-2488 | - | - | x |

## Nominální vs. efektivní přenosová rychlost

Jen pro připomenutí, nominální rychlost vypovídá spíše o tom, jak dlouho trvá přenos jednoho bitu, bez ohledu na to, zda jde o bit užitečný či režijní. Tzv. efektivní přenosová rychlost, která bere v úvahu již jen užitečná data, bývá v praxi menší, a to až o desítky procent, protože už bere v úvahu nejrůznější režii a také všelijaké nutné prodlevy, opakované přenosy apod.

# Řízení přístupu

Stejně jako jeho „drátový“, musel se i bezdrátový Ethernet nějak vyrovnat se sdílenou povahou použitého přenosového média. Sdílenou proto, že podobně jako na původním koaxiálním kabelovém segmentu může i bezdrátově vysílat vždy jen jeden uzel (a ostatní mohou poslouchat). Ale jakmile začne vysílat více uzlů současně (ve vzájemném dosahu), dochází ke kolizi: jejich vysílání se „střetávají“ a vzájemně nenávratně promíchávají. U drátového Ethernetu řešila problém přístupu ke sdílenému média přístupová metoda CSMA/CD. Předpokládala, že je možný příposlech nosné (CS, Carrier Sense), a tedy že každý uzel si může nejprve poslechnout, zda nevysílá někdo jiný. U bezdrátového Ethernetu je příposlech nosné stále možný, a tak ho zájemci o vysílání používají. Jen se liší v tom, jak zareagují v případě, kdy zjistí, že někdo již vysílá. U drátového Ethernetu, v rámci přístupové metody CSMA/CD, uzel čeká na konec vysílání, a jakmile toto skončí, začne vysílat sám.

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

Důvodem pro tuto zajímavou odlišnost je to, že u bezdrátového vysílání nelze (jednoduše) detekovat kolize. Rádiová rozhraní jsou totiž obvykle jen poloduplexní, v tom smyslu že buďto přijímají nebo naopak vysílají, ale nikoli současně. Proto nedokáží vysílat a současně s tím skrze příjem monitorovat, zda v éteru nedošlo ke kolizi.

Ostatně, proto také přístupová metoda bezdrátového Ethernetu není (a nemůže být) metodou CSMA/CD, neboli s detekcí kolize (CD, Collision Detect). Místo toho se označuje jako CSMA/CA, přičemž ono „CA“ na konci značí „Collision Avoidance“, neboli předcházení kolizím.

# 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:

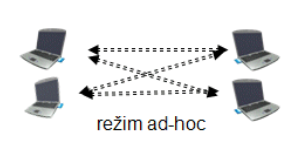
* **režim infrastruktury (infrastructure mode)**

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 za-bezpečení 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 od-poslouchávat i na delší vzdálenost bez nutnosti fyzického kontaktu s počítačovou sítí. WEP byl prolomen v srpnu 2001.

**WEPplus** (někdy označován jako WEP+) je vylepšení původního WEP zabezpečení od Agere Systems, které se snaží odstranit takzvané slabé inicializační vektory, pomocí kterých může útočník velmi rychle spočítat použitý šifrovací klíč použité proudové šifry RC4 a může tak nejen bezdrátový provoz odposlouchávat, ale může se do bezdrátové sítě zabezpečené pomocí WEP i připojit.

**WEP2** je vylepšení původního WEP zabezpečení, které se snaží odstranit bezpečností nedostatky původního WEP. WEP2 rozšiřuje inicializační vektory a zesiluje 128bitové šifrování.

**WPA** (Wi-Fi Protected Access, tj. chráněný přístup k Wi-Fi) je obchodní označení pro zabezpečení bezdrá-tových sítí. Po prolomení zabezpečení WEP v roce 2001 definovala Wi-Fi Alliance v roce 2002 zabezpečení WPA pro Wi-Fi sítě jako část tehdy připravovaného standardu IEEE 802.11i.

**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.

# Rychlost v jednotlivých standartech

|  |  |  |  |
| --- | --- | --- | --- |
| **Přehled standardů IEEE 802.11** | | | |
| **Standard** | **Pásmo [GHz]** | **Maximální rychlost [Mbit/s]** | **Fyzická vrstva** |
| původní [IEEE 802.11](http://cs.wikipedia.org/wiki/IEEE_802.11) | 2,4 | 2 | [DSSS](http://cs.wikipedia.org/wiki/Direct_Sequence_Spread_Spectrum) |
| [IEEE 802.11a](http://cs.wikipedia.org/wiki/IEEE_802.11a) | 5 | 54 | [OFDM](http://cs.wikipedia.org/wiki/OFDM) |
| [IEEE 802.11b](http://cs.wikipedia.org/wiki/IEEE_802.11b) | 2,4 | 11 | [DSSS](http://cs.wikipedia.org/wiki/Direct_Sequence_Spread_Spectrum) |
| [IEEE 802.11g](http://cs.wikipedia.org/wiki/IEEE_802.11g) | 2,4 | 54 | [OFDM](http://cs.wikipedia.org/wiki/OFDM) |
| [IEEE 802.11n](http://cs.wikipedia.org/wiki/IEEE_802.11n) | 2,4 nebo 5 | 600\* | [OFDM](http://cs.wikipedia.org/wiki/OFDM), [MIMO](http://cs.wikipedia.org/wiki/MIMO) |
| [IEEE 802.11ac](http://cs.wikipedia.org/wiki/IEEE_802.11ac) | 2,4 nebo 5 | 1800 | [OFDM](http://cs.wikipedia.org/wiki/OFDM), [MIMO](http://cs.wikipedia.org/wiki/MIMO) |