Jak funguje Wi-Fi

aneb co jste chtěli vědet o Wi-Fi a nebylo se koho zeptat

Lukáš Turek
8an@praha12.net

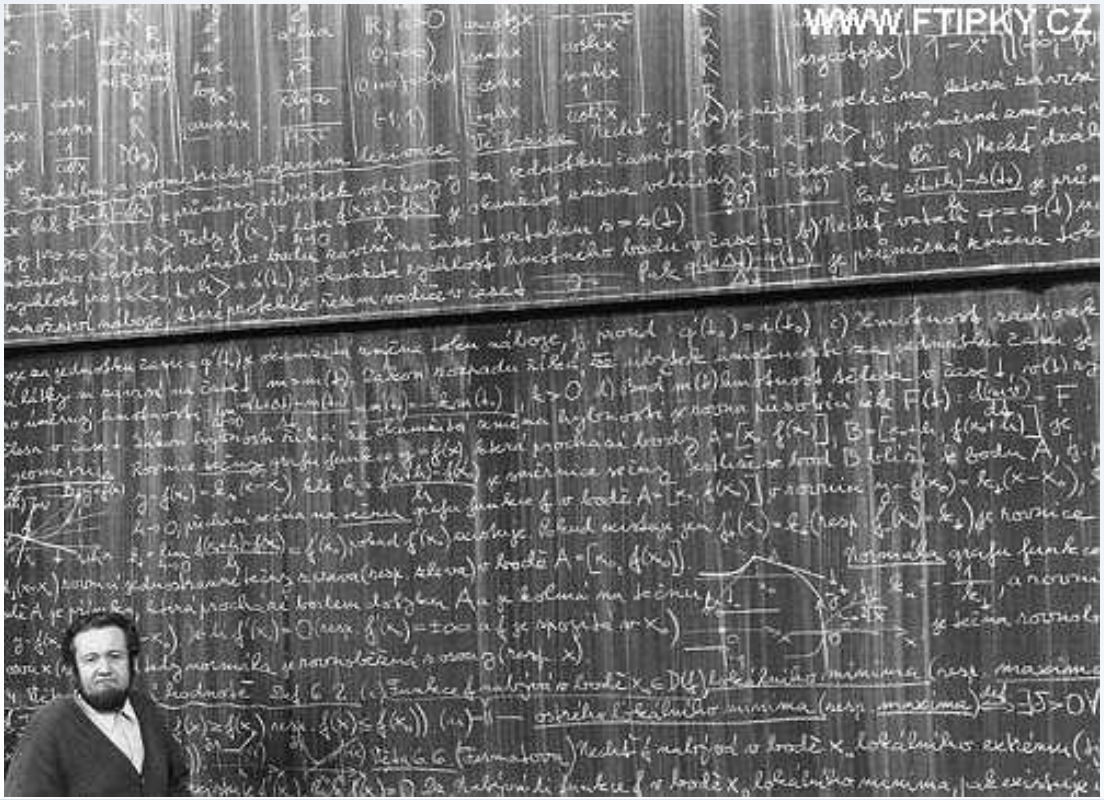
6.1.2008

O čem to bude

- Obecný úvod
- Modulace
  - přenos bitů
  - Proč nepoužíváme 802.11g?
- Přístupová metoda
  - koordinace vysílání více stanic
  - Proč tolik vadí Bittorent a moc nefunguje traffic shaping?
- Linková vrstva
  - Přenos paketů
  - Proč se přes Ovislinky v režimu klient nedá routovat?
- Nebudu mluvit o zabezpečení
  - to by bylo téma na několik přednášek...

Organizace přednášky

- Pokud budete mít dotaz, ptejte se hned
- Dvě části, v polovině přestávka
  - 10 minut nebo týden
  - podle toho kolik bude dotazů a jak budete z mého výkladu zničeni...



Standard 802.11

- Standardy pro bezdrátové lokální sítě v bezlicenčních pásmech
- Organizace IEEE
  - *Institute of Electrical and Electronics Engineers, Inc.*
  - http://standards.ieee.org/getieee802/802.11.html
- Kompatibilitu kontroluje Wi-Fi Alliance
  - „Wi-Fi“ je ochranná známka
- Jako náhrada sítí LAN
  - proto označení WLAN – Wireless LAN
  - použití vně budov se nepředpokládalo
    - to je spíše česká specialita
    - Wi-Fi tedy není efektivní na point-to-point spoje

Historie 802.11

- 1997: 802.11
  - dnes označováno „802.11 legacy”
  - pásmo 2.4 GHz, 1-2 Mbit/s
  - modulace FHSS (frequency hopping) nebo DSSS
  - ve standardu bylo tolik možností volby, že výsledné produkty nebyly vzájemně kompatibilní, nerozšířilo se
  - Alvarion BreezeNet
- 1999: 802.11b
  - až 11 Mbit/s (reálná rychlost přenosu dat je cca 40%)
  - pásmo 2.4 GHz
    - v Evropě 13 kanálů, ale překrývají se
  - modulace DSSS (*Direct-sequence Spread Spectrum*)
  - široce rozšířeno ⇒ velké zarušení pásma 2.4 GHz

Historie 802.11

- 1999: 802.11a
  - pásmo 5GHz, nominální rychlost 54 Mbit/s
  - modulace OFDM *(Orthogonal frequency-division multiplexing)*
  - v ČR povoleno pouze uvnitř budov, venku jen v části pásma s rozšířením 802.11h
    - automatický výběr kanálů a regulace výkonu
  - 11 nepřekrývajících se kanálů použitelných i vně budov
    - přesto se už začínají objevovat problémy s rušením
- 2003: 802.11g
  - pásmo 2.4GHz, zpětně kompatibilní s 802.11b
    - pomocí RTS/CTS, výrazně snižuje propustnost
  - modulace OFDM převzatá z 802.11a, až 54 Mbit/s
    - potřebuje lepší kvalitu signálu než 802.11b
    - menší odolnost proti rušení

Historie 802.11

- 2007: 802.11n (draft)
  - nominální rychlost teoreticky až 600Mbit
    - současná zařízení jen 300Mbit
  - efektivní rychlost v současnosti okolo 120Mbit
    - ale jen na pár metrů, se vzdáleností rychle klesá
  - Může pracovat v pásmu 2.4 GHz i 5 GHz
    - vyšší rychlosti dosahuje v 5 GHz pásmu
  - lepší modulace, agregace paketů, 40MHz kanály
  - MIMO technologie (víc antén, až 4)
  - Pro použití na dálkové spoje asi moc vhodné nebude
    - zabere 2 kanály, kterých máme málo už teď
    - méně odolné proti rušení
    - zatím nejsou MIMO antény pro dálkové spoje
    - plně efektivní je jen v prostředí s odrazy signálu

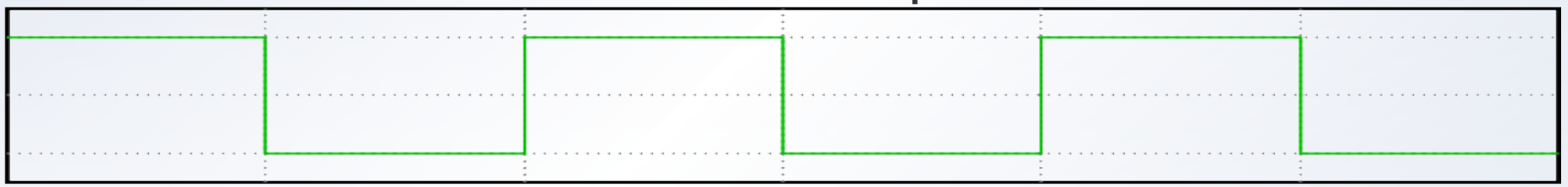
Frekvence a kanály

Channel	1	: 2412	Mhz	11g
Channel	2	: 2417	Mhz	11g
Channel	3	: 2422	Mhz	11g
Channel	4	: 2427	Mhz	11g
Channel	5	: 2432	Mhz	11g
Channel	6	: 2437	Mhz	11g
Channel	7	: 2442	Mhz	11g
Channel	8	: 2447	Mhz	11g
Channel	9	: 2452	Mhz	11g
Channel	10	: 2457	Mhz	11g
Channel	11	: 2462	Mhz	11g
Channel	12	: 2467	Mhz	11g
Channel	13	: 2472	Mhz	11g
Channel	14	: 2484	Mhz	11b
Channel	34	: 5170	Mhz	11a
Channel	36	: 5180	Mhz	11a
Channel	38	: 5190	Mhz	11a
Channel	40	: 5200	Mhz	11a
Channel	42	: 5210	Mhz	11a
Channel	44	: 5220	Mhz	11a
Channel	46	: 5230	Mhz	11a
Channel	48	: 5240	Mhz	11a
Channel	50	: 5250	Mhz	11a

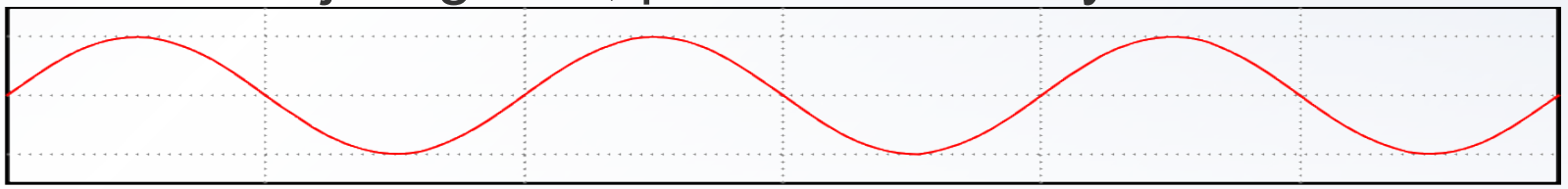
Channel	52	: 5260	Mhz	11a
Channel	56	: 5280	Mhz	11a
Channel	58	: 5290	Mhz	11a
Channel	60	: 5300	Mhz	11a
Channel	64	: 5320	Mhz	11a
Channel	100	: 5500	Mhz	11a
Channel	104	: 5520	Mhz	11a
Channel	108	: 5540	Mhz	11a
Channel	112	: 5560	Mhz	11a
Channel	116	: 5580	Mhz	11a
Channel	120	: 5600	Mhz	11a
Channel	124	: 5620	Mhz	11a
Channel	128	: 5640	Mhz	11a
Channel	132	: 5660	Mhz	11a
Channel	136	: 5680	Mhz	11a
Channel	140	: 5700	Mhz	11a
Channel	149	: 5745	Mhz	11a
Channel	152	: 5760	Mhz	11a
Channel	153	: 5765	Mhz	11a
Channel	157	: 5785	Mhz	11a
Channel	160	: 5800	Mhz	11a
Channel	161	: 5805	Mhz	11a
Channel	165	: 5825	Mhz	11a

Fyzická vrstva

- Definuje, jak se přenáší jednotlivé datové bity
- Přenos se musí vejít do omezeného frekvenčního pásma
  - do jednoho 20 MHz kanálu
  - digitální signál nelze vysílat přímo jako např. u Ethernetu
    - přenos ostrých hran by vyžadoval nekonečnou frekvenci, v reálu 10Mbit Ethernet zabírá pásmo 0-10 Mhz



- Používá se modulace nosné frekvence
  - základ je sinusovka, u které se podle typu modulace mění frekvence, amplituda, nebo fáze
  - modulace je digitální, parametr se tedy mění skokově

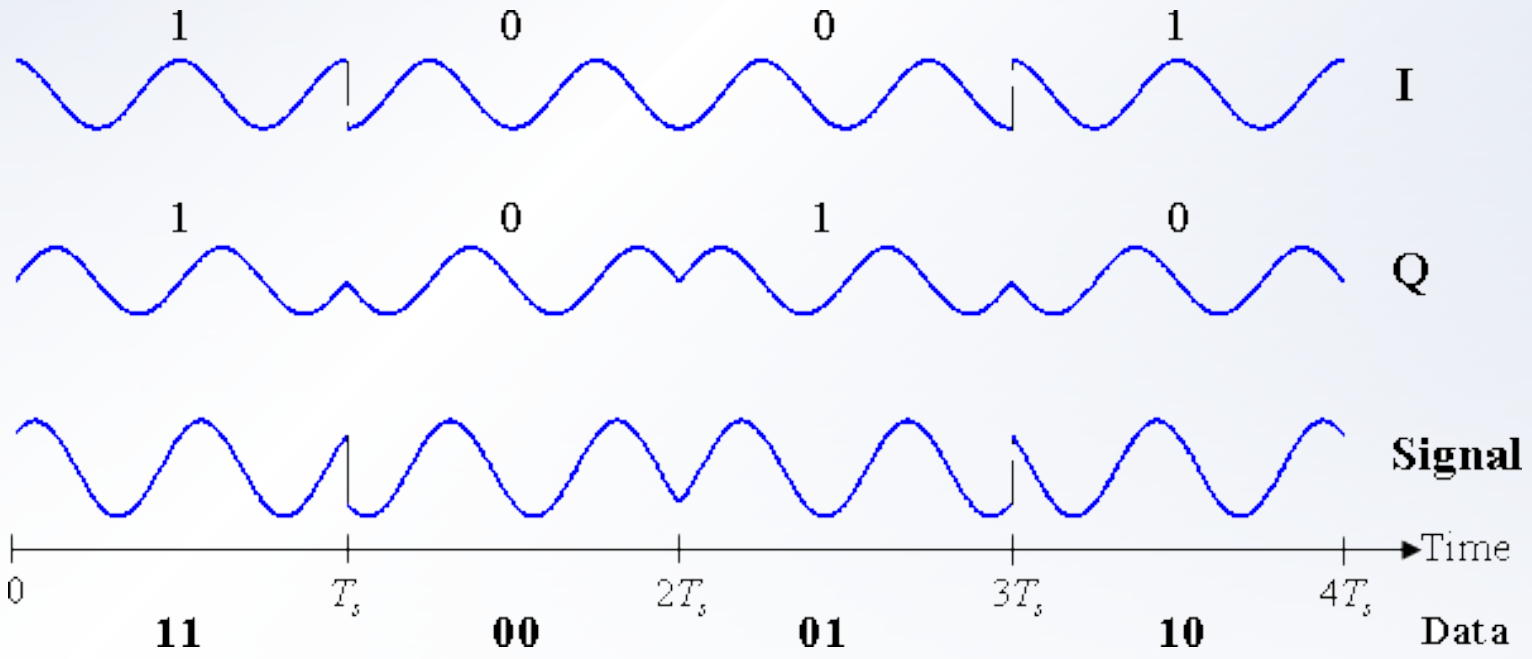


Modulace v 802.11

- V reálu je převod bitů na analogový signál složitější
- Verze 802.11 definují různé metody modulace
  - FHSS (*Frequency Hopping Spread Spectrum*)
    - náhodné přeskakování po kanálech
    - jen v první verzi 802.11, dnes použitelné jen jako rušička
  - DSSS (Direct Sequence Spread Spectrum)
    - použito v 802.11b
    - jeden bit se kóduje do sekvence bitů
  - OFDM
    - v 802.11g a 802.11a, modifikovaně v 802.11n
    - pásmo se dělí do překrývajících podpásem, každé nese část dat

Modulace DSSS

- Základ je fázová modulace
  - změna fáze signálu kóduje několik bitů
    - na 11 Mbit kóduje 8 bitů, na 5.5 Mbit 4 bity
  - Kódování se nazývá CCK (*Complementary Code Keying*)
    - detaily vynechám, je to docela komplikované



Modulace DSSS

- Pro větší odolnost se jeden bit kóduje 8 vysílanými bity
  - tzv. *chipping code*
  - příjemce musí tento kód znát a být synchronizovaný
    - aby poznal který bit je první v kódu
  - místo 0 se vysílá chipping code, místo 1 jeho negace
  - příjemce chipping code odečte (operace XOR), a pokud je ve výsledku víc jedniček, přečte 1, jinak 0

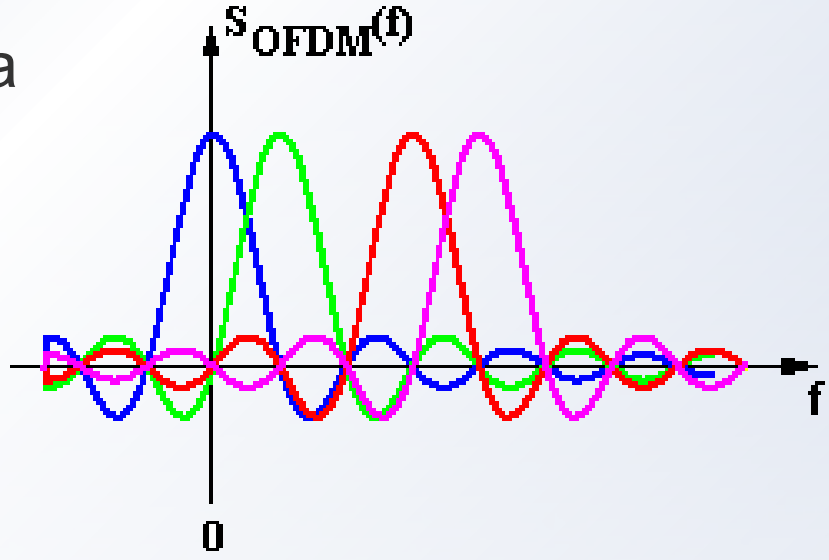
Data:	0	1	0	1
Kód:	01101011	01101011	01101011	01101011
Signál:	01101011	10010100	01101011	10010100

Modulace DSSS

- Tento způsob přenosu je odolný proti šumu
  - i když se změní 3 bity, je možné signál rekonstruovat
- I rušení od jiného vysílání DSSS nemusí vadit
  - teprve změní-li se polovina přenášených bitů, je datový bit poškozen
  - jsou-li kódy ortogonální, je možné rekonstruovat správná data vždy
    - to se používá u CDMA, u 802.11b ne
- Nepřidávají se další samoopravné kódy
  - pouze CRC pro detekci chyby, ale to je u 802.11 vždy

Modulace OFDM

- Úplně jiný přístup než DSSS
- Frekvenční pásmo je rozděleno na části
  - každá část má vlastní nosnou frekvenci, na níž je modulována část přenášených dat
  - části se částečně překrývají
    - součet částí je větší než celek
  - 802.11ag dělí 20 MHz pásmo na 52 subpásem, ale jen 48 z nich používá pro přenos dat
  - 802.11n používá 108 subpásem na kanálech šířky 40 MHz

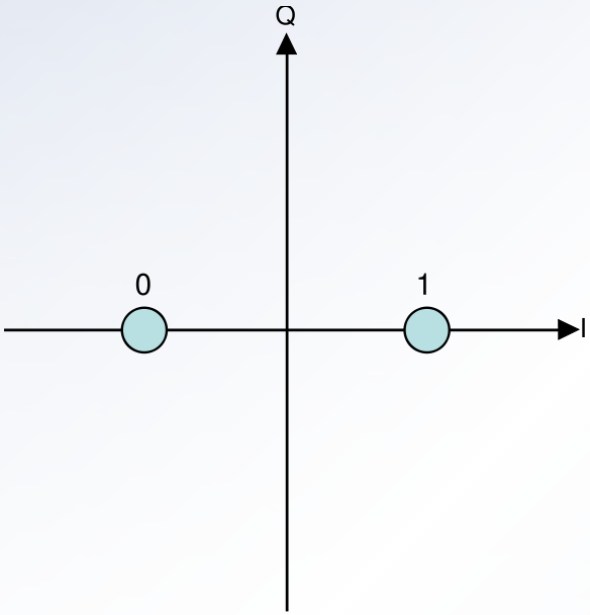


OFDM - kódování

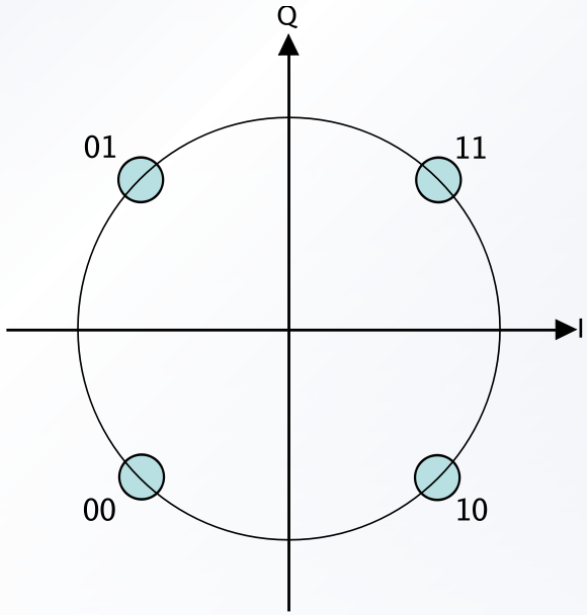
- Přenášené bity se kódují do změn fáze dvou harmonických vln, posunutých o 90° ($\pi/2$)

$$s(t) = I(t)\cos(2\pi f_0 t) + Q(t)\sin(2\pi f_0 t)$$

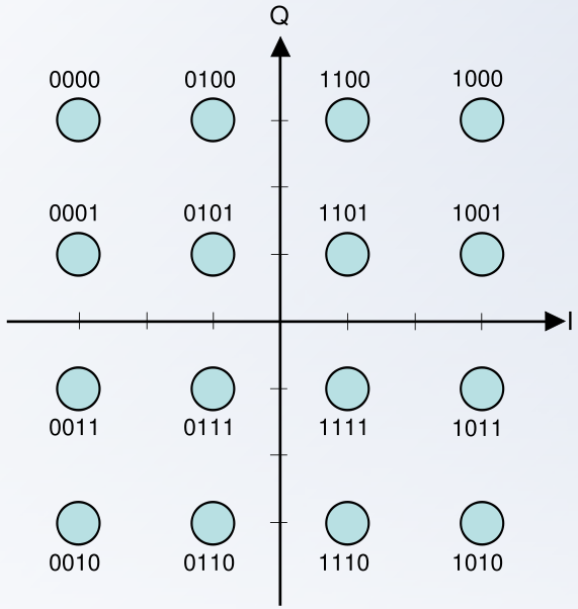
- Různá kódování se liší počtem stavů na jeden symbol
  - BPSK (2), QPSK (4), 16-QAM (16), 64-QAM (64)



BPSK



QPSK



16-QAM

OFDM – přenosová rychlost

- Každé z 48 subpásem přenáší stejný díl dat
- Délka symbolu je 3.2 µs
  - mezi přenášené symboly se vkládá ochranný interval 0.8 µs
    - kvůli odrazům signálu (jako „duchy“ v televizi)
  - posílá se tedy jeden symbol každé 4 µs
- Počet bitů přenášený symbolem závisí na kódování
  - BPSK: 1, QPSK: 2, 16-QAM: 4, 64-QAM: 6
- Mezi datové bity se vkládají další pro opravy chyb
  - poměry 1:2, 2:3, 3:4
- Přenosová rychlost je dána kombinací parametrů
  - kódování, opravné kódy
  - ne všechny kombinace jsou přípustné

$$rate = (carriers \bullet coded\_bits \bullet code\_rate) / 4$$

Přenosová rychlost - tabulka

Modulace	Bitů na symbol	Poměr kódování	Počet nosných	Rychlost
BPSK	1	1/2	48	6
BPSK	1	3/4	48	9
QPSK	2	1/2	48	12
QPSK	2	3/4	48	18
16-QAM	4	1/2	48	24
16-QAM	4	3/4	48	36
64-QAM	6	2/3	48	48
64-QAM	6	3/4	48	54

Porovnání DSSS a OFDM

- DSSS je odolnější proti rušení
  - jeden bit je přenášen jako víc bitů, i když se několik z nich poškodí, lze původní bit rekonstruovat
  - OFDM zabere skutečně celý kanál (nosných frekvencí je mnoho), DSSS používá jednu nosnou frekvenci, nejvyšší výkon je uprostřed kanálu, směrem k okrajům klesá
- Vyšší přenosová rychlost OFDM vyžaduje vyšší výkon
  - větší odstup signálu od šumu (Shannonův teorém)
  - asi 10dB, a přesně o tolik víc je povoleno v pásmu 5 GHz
  - proto je OFDM použitelné v 802.11a v pásmu 5 GHz, ale ne u 802.11g v pásmu 2.4 GHz
- Na AP v zarušeném pásmu 2.4 GHz nemá 802.11g smysl

Přestávka

Přístupová metoda

- Vzduch je sdílené médium, vysílat může jen jeden
  - podobně jako Ethernet po koaxiálním kabelu
    - stanice při vysílání poslouchá, jestli data na kabelu jsou skutečně ta co vysílá, pokud ne, došlo ke kolizi
- Na Wi-Fi nejde použít stejnou metodu jako na Ethernetu
  - rádiová část se přepíná mezi vysíláním a příjmem
    - nemůže poslouchat v době, kdy vysílá
    - teprve po odeslání celého paketu pošle příjemce potvrzení
    - pokud potvrzení nedošlo, přenos se opakuje
  - stanice alespoň mohou poslouchat v době kdy nevysílají, aby nezačaly vysílat když už vysílá někdo jiný
    - ale stále se mohou rozhodnout vysílat dvě najednou
- Přístupová metoda CSMA/CA
  - *Carrier Sense Multiple Access / Collision Avoidance*

Přístupová metoda – detaily

- Čas se měří ve slotech
  - u 802.11b má slot 20 µs
  - u 802.11a je nastavitelný, na BSD `dev.ath.0.slottime`
    - nastavuje se podle vzdálenosti, default 9 µs
- Z délky slotu se odvozují časové konstanty
  - SIFS
    - doba čekání před posláním potvrzení
      - aby se obě strany stihly přepnout (z vysílání na příjem a naopak)
    - 802.11b: 10 µs, 802.11a: 16 µs
  - DIFS
    - jak dlouho čeká odesílatel, než začne vysílat
      - po tuto dobu musí být médum volné
    - 2x slot + SIFS
    - 802.11b: 50 µs, 802.11a: 34 µs

Efektivita 802.11

- Před přenosem samotných dat se navíc vysílá **preamble**
  - posloupnost nul a jedniček pro synchronizaci příjemce
  - na 802.11b má 192 µs *(long)* nebo 96 *(short)*
    - výchozí je dlouhá, krátká je použitelná jen uvnitř budov
  - na 802.11a jen hlavička o délce 20 µs
- Potvrzení (ACK) má 14 bajtů
- Celkem přenos jednoho paketu na 802.11b trvá:
  - DIFS: 50 µs
  - preamble: 192 µs
  - data: ? µs (podle délky)
  - SIFS: 10 µs
  - ACK preamble: 192 µs
  - ACK data: 11 µs
  - **Součet: 455 µs**

Efektivita 802.11

- Režie související s přenosem jednoho paketu je 455 µs
  - přenos 1500B dat rychlostí 11 Mbit trvá
    1500 * 8 / 11 = 1090 µs
  - režie je tedy skoro třetina
    - při započítání TCP ACK (přes 500 µs) dokonce polovina
  - za 455 µs je možno přenést 625 bajtů
    - tedy u paketů pod 625 bajtů je režie větší než přenos dat!
  - P2P programy posílají spoustu malých paketů okolo 100B
    - tady je režie šestinásobek užitečného přenosu!
- Traffic shaping s režií nepočítá
  - jednoduše sčítá velikosti paketů
  - nezná ani jakou rychlostí jsou pakety vysílány
    - přenos 28 paketů po 54 bajtech na 1Mbit zabere 100x více času než 1500B v jednom paketu na 11Mbit!

ACK timeout

- Předchozí výpočet byl jen pro úspešný případ
  - data byla doručena v pořádku, nedošlo ke kolizi nebo rušení
- Pokud nebyl přenos úspěšný, odesílatel nedostane ACK
  - jak dlouho má čekat, než zkusí přenos opakovat?
    - od ukončení odesílání alespoň dobu šíření signálu tam, SIFS, dobu přenosu potvrzení a dobu šíření signálu zpět
- Signál se šíří rychlost světla, ta není nekonečná
  - přibližně 300 000 km/s
  - 1km urazí světlo za 3.3 μs
    - to je srovnatelná hodnota s SIFS a DIFS!
    - tam a zpátky ⇒ násobí se dvěma
- Skutečný výpočet hodnot pro Atheros je trochu jiný
  - 21 + 2 · (vzdálenost / 300)

Mechanismus RTS/CTS

- Uživatel P2P navíc uploaduje
- CSMA/CA předpokládá, že se stanice navzájem slyší
  - jedna může detekovat, že jiná vysílá
  - to u uploadu neplatí
    - má-li uživatel úzce směrovou anténu, slyší jen AP, ne klienty
    - u odchozích dat tedy dochází ke kolizím a musí se přeposílat
- Řešení: RTS/CTS
  - klient pošle RTS (*Request to send*)
    - s informací, jak dlouho bude přenos probíhat
  - AP odpoví CTS (*Clear to send*)
    - to slyší všichni, dozví se, jak dlouho mají mlčet
  - ale to se musí zapnout u každého klienta!
    - nastavuje se velikost rámce, od kdy se má RTS/CTS použít
    - doporučuji nastavit 256, ale je to jen můj odhad

QoS

- Přístupová metoda 802.11 je nedeterministická
  - není zaručeno, jak dlouho bude trvat doručení paketu
  - s vyšším zatížením roste latence víc než lineárně
    - ke stovkám nebo i tisícům milisekund
- To je problém pro real-time aplikace
  - VoIP, streaming videa, on-line hry, …
  - vyžadují zaručenou kapacitu a malé konstantní zpoždění
- Původní 802.11 definovalo přístupovou metodu PCF
  - AP řídí veškeré přenosy na síti
  - není povinná, podporuje jen málo zařízení
    - aby ji bylo možno použít, musí ji podporovat všechna zařízení
- QoS do 802.11 zavádí dodatek 802.11e

802.11e

- Zavádí třídy provozu (*Traffic Classes*)
- K DCF a PCF přibyla HCF (*Hybrid Coordination Function)*
- Dvě přístupové metody
  - EDCA *(Enhanced Distributed Channel Access)*
    - stanice, která chce vysílat data s vyšší prioritou, čeká kratší dobu, než začne vysílat
    - doba, po jakou může stanice vysílat, je omezena
  - HCCA *(HCF Controlled Channel Access)*
    - stanice oznamují svoje požadavky na přenosovou kapacitu
    - AP může iniciovat CAP (Controlled Access Phase), kdy řídí všechny přenosy

- Navíc možno vypnout potvrzování a přeposílání rámců
- Certifikace Wi-Fi Multimedia (WMM)
  - HCCA není povinné

Linková vrstva

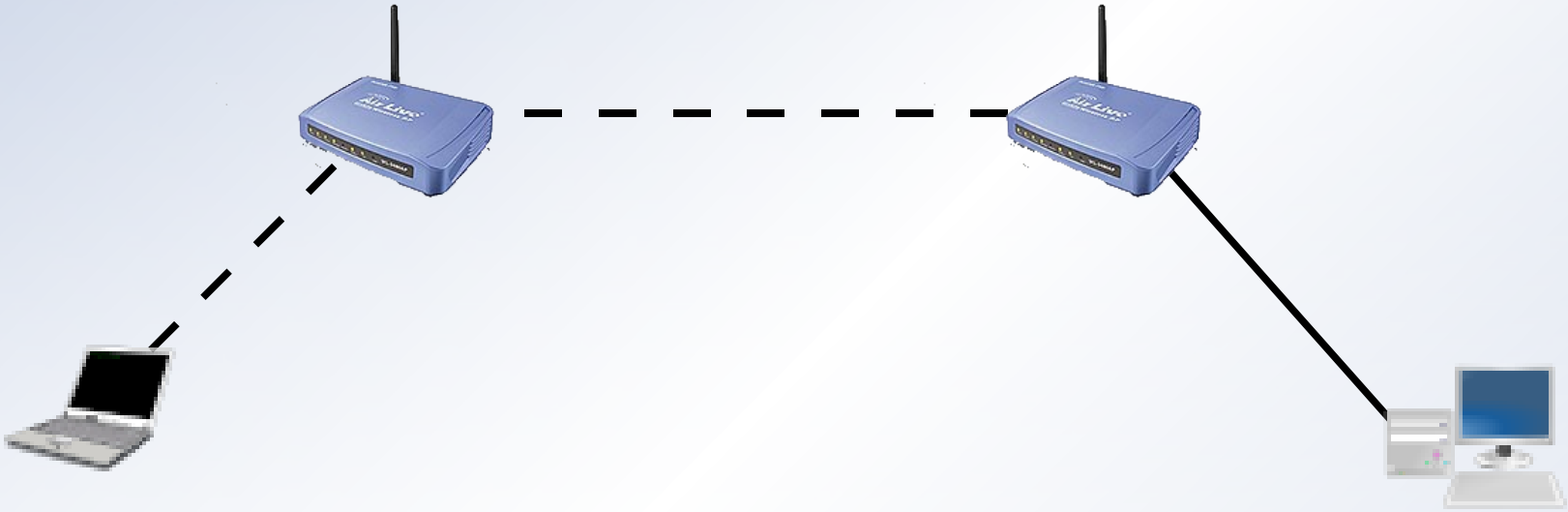
- Definuje adresování stanic v síti (mimo jiné)
- Základ převzat z Ethernetu
  - například MAC adresy a část hlaviček rámců
- Jsou ale podstatné rozdíly
  - Switch na Ethernetu funguje automaticky
    - pokud na nějaký port přijde paket od nějakého počítače, switch bude pakety pro tento počítač posílat na tento port
    - pokud switch neví, kam paket poslat, pošle ho všude
  - AP takto fungovat nemůže, musí své klienty znát
    - aby zbytečně neposílal pakety několikrát, když je stanice nemůže potvrdit, protože neexistuje
    - u WPA a 802.1x má každá stanice jiný šifrovací klíč
    - někteří klienti mohou používat 802.11b a jiní 802.11g
    - připojení může vyžadovat autentizaci

Přístupový bod

- Přístupový bod je centrální prvek sítě
  - klienti se k němu připojují a autentizují
- AP přeposílá pakety mezi klienty
  - ti na sebe nemusí přímo vidět
  - stahování dvou klientů od sebe tedy zatěžuje pásmo 2x !
    - navíc to při použití HWAP nejde nijak omezovat!
- Klient ale musí nějak adresovat AP
  - k AP nevede drát jako do switche, musí nějak poznat rámce, kterými se má zabývat
  - potvrzení posílá příjemce AP, ne původnímu odesílateli
    - ten už dostal potvrzení od AP a dál se o rámec nestará
- Výsledek: v rámcích musí být alespoň 3 MAC adresy
  - odesílatel, příjemce a AP

Bezdrátový most

- Situace může být složitější



- Příjemce je připojen k jinému AP
  - jsou potřeba 4 MAC adresy
    - skutečný odesílatel a příjemce
    - odesílatel a příjemce na bezdrátovém spoji
- Tato situace nastává při bezdrátovém spojení dvou LAN
  - to je i P2P spoj přes dva Ovislinky!

Wireless Distribution System

- Několik AP, i mezi sebou komunikují bezdrátově
  - musí být na stejném kanále
    - stačí jedna anténa, ale dělí se o kapacitu pásma
  - AP ve WDS režimu může zároveň připojovat klienty
  - přístupové body tvořící WDS se musí navzájem znát
    - typicky se definují na každém MAC adresy ostatních
  - všechna zařízení WDS nepodporují
    - dnes už většina, ale nemusí být kompatibilní
  - není kompatibilní s WPA
    - WDS tedy nelze pořádně zabezpečit
- AP v režimu WDS se chová jako switch
  - nemění MAC adresy odesílatele a příjemce pakety
  - udržuje si tabulku, přes které AP ve WDS má přeposlat paket pro danou MAC

Bridge v režimu klient

- Obyčejný klient AP, který funguje jako bridge, není WDS!
  - AP o tom neví, nijak speciálně s ním nekomunikuje
  - pošle mu jenom rámec s jeho vlastní MAC adresou
- Jde to řešit dvěma způsoby
  - bridge se na AP asociuje jednou za každý počítač
    - jakoby podvrhne svojí MAC adresu
    - na AP musí být všechny MAC povolené
    - přes takovýto bridge jde routovat, pakety se normálně doručují podle MAC adresy routeru za bridgem
  - místo bridge se použije Proxy ARP
    - tohle dělají Ovislinky, Aircy a podobně haraburdí
    - všechny počítače se schovají za jednu MAC adresu
    - je to vlastně takový NAT na linkové vrstvě, se všemi důsledky

Proxy ARP

- ARP protokol
  - překlad mezi IP adresami a MAC adresou
  - do sítě se pošle broadcast „kdo má IP x.x.x.x?“
  - obvykle odpoví vlastník IP adresy, ale nemusí to tak být!
    - to jde zneužít na hezké útoky...
    - počítač může zastupovat jiné počítače
- Proxy ARP
  - počítač má dvě síťová rozhraní
  - ARP dotaz na jednom z nich přepošle na druhé
    - dostane-li odpověď, uloží si záznam do tabulky, a odpoví na původní dotaz se svojí vlastní MAC adresou
  - pakety pro počítače za ním tedy chodí jemu
    - na jeho MAC adresu
    - podle IP adresy v paketech a své ARP tabulky je přeposílá

Router za Proxy ARP

- Proxy ARP není brige!
  - bridge nemění MAC adresy, chová se přesně jako switch
- Co je vlastně router?
  - na jeho MAC adresu chodí pakety s cizí IP adresou
  - router je podle routovací tabulky přeposílá dál
- Router za Proxy ARP
  - pakety do sítí za routerem router chodí na MAC Proxy ARP
  - Proxy ARP pošle ARP dotaz tuto IP adresu
    - nikdo neodpoví, router odpovídá jen na svou IP adresu!
    - paket je tedy zahozen, Proxy ARP neví kam ho poslat
  - Ovislink pravděpodobně záznam do ARP tabulky přidává i přijde-li datový paket z nějaké IP adresy
    - třeba ping z počítače za routerem někam přes Proxy ARP
    - spojení ven povolí spojení i dovnitř, podobně jako NAT

Konec

- VSTÁVAT!
- Děkuji za pozornost.
- Tuto prezentaci najdete na http://8an.praha12.net/slides/wifi.pdf