

Sítě IEEE 802.11 (WiFi)

Petr Grygárek

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

1

Sítě IEEE 802.11

- Rádiové sítě provozované v nelicencovaném pásmu ISM (Instrumental-Scientific-Medicine)
 - 2,4 GHz
 - 5 GHz
 - V Evropě požadavek dynamické volby kanálu a automatické regulace vysílaného výkonu
- Optimalizované pro použití uvnitř budov
 - V ČR hojně používáno i ve vnějších prostorách,
 - pokrytí skupiny budov, směrové dvoubodové spoje
- Definuje spojovou a fyzickou vrstvu (několik alternativ)

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

2

Provoz v pásmu ISM

- Požadavek regulátora na rozptýření výkonu do širšího frekvenčního pásma
 - Max. vyzářený výkon 100 mW
- Výkon rozdělen do širšího spektra frekvencí, než by bylo nezbytné
 - Redundantní vysílání informace na více frekvencích
 - Rekonstruovatelnost i v přítomnosti šumu
 - Provoz více systémů současně

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

3

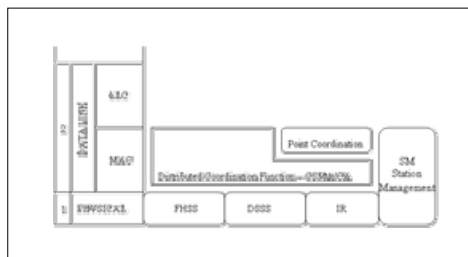
Kanály pásma ISM 2,4 GHz

- Evropa: kanály 1-13, USA: kanály 1-11
- Odstup kanálů 5 MHz, šířka kanálu pro použití rozptýřeného spektra však je 22 MHz
- Kanál zasahuje do 4 sousedních kanálů
- pokud chceme nerušený signál, musíme volit min. odstup centrálních frekvencí 25 MHz
- Lze použít pouze 3 samostatné kanály

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

4

Struktura doporučení IEEE 802.11



© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

5

Základní standardy IEEE 802.11

- 802.11 (původní standard)
 - 1 a 2 Mbps
- 802.11a
 - 5 GHz (USA);
 - 6,9,12,18,24,36,48,54 Mbps
- 802.11b
 - 2,4 GHz (USA, Evropa)
 - rozšíření 802.11 o DSSS 1,2,5,5 a 11 Mbps
- 802.11g
 - 2,4 GHz (USA, Evropa)
 - Obdoba 802.11a, ale v jiném pásmu
- 802.11h
 - 5 GHz (Evropa)
 - Obdoba 802.11a, ale s automatickou regulací výkonu a vyhledávání volné frekvence

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

6

Další podpůrné standardy

- 802.11i – bezpečnost+QoS
 - QoS přemístěna z 802.11e
- 802.11f – rychlý roaming mezi AP
 - Redukce vícenásobné autentizace při přechodu mezi AP
 - Pro mobilní aplikace trvale náročné na malou latenci
 - (telefonie, multimedia, ...)

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

7

WiFi

- „Wireless Fidelity“
- Logo konsorcia zabývajícího se testováním kompatibility produktů sítí IEEE 802.11

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

8

Komponenty rádiové sítě IEEE 802.11

- Přístupový bod
- Distribuční systém
- Bezdrátoví klienti (stanice)
- Přenosové prostředí

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

9

Alternativy použití

- Ad-hoc
 - dočasné přímé propojení několika blízkých počítačů
 - potřeba manuální konfigurace
- Infrastruktura
 - Použití přístupového bodu (Access Point, AP)
 - Přístupový bod může zprostředkovat přechod do pevné sítě
 - a často i funkci DHCP serveru, NAT a další „PnP“ funkce

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

10

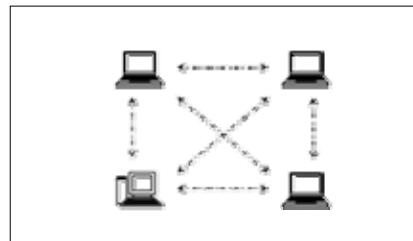
Architektury realizace bezdrátové sítě

- Independent Service Set (IBSS)
 - skupina vzájemně přímo komunikujících stanic
 - neprovádí se relaying rámců
 - není napojení na pevnou síť
- Basic Service Set (BSS)
 - Používá přístupového bodu, stanice komunikují přes něj
- Extended Service Set (ESS)
 - propojení více BSS přes distribuční systém
 - distribuční systém není normou specifikován
 - typicky Ethernet
 - proprietární řešení bezdrátového distribučního systému (WDS).

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

11

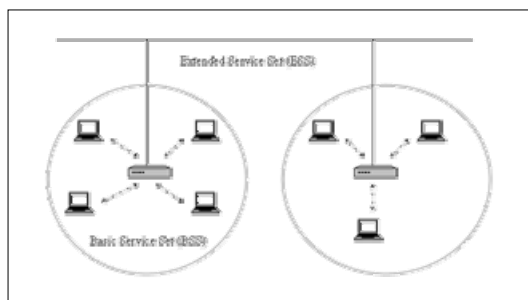
IBSS



© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

12

BSS, EBSS



© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

13

Terminologie

- Service Set = logická skupina stanic
- SSID = Service Set Identifier
- BSS ID = Identifikátor BSS = MAC adresa AP

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

14

Fyzická vrstva

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

15

Frequency Hopping Spread Spectrum

- Vojenský původ (utajení vysílání)
- Frekvenční pásmo rozděleno na 75 (79) kanálů o šířce 1 MHz
- Vysílač kanály střídá, na každém se vysílá max. 400 ms
 - Každá stanice má jinou posloupnost střídání kanálů (hopping pattern)
 - přiděluje přístupový bod (AP)
- Možnost funkce více systémů v témže pásmu současně
 - podle 802.11 v pásmu 2,4 GHz teoreticky 26, prakticky asi 15
- Výrobně jednodušší, nepotřebuje sofistikované výpočty
 - levnější vývoj, jednodušší HW s nižším odběrem energie
- Problém: hopping patterns fixní, používá i zaručené kanály
- 802.11 definuje pro 1 nebo 2 Mb/s

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

16

Direct Sequence Spread Spectrum

- 802.11 definuje pro 1 a 2 Mb/s
- Vysílaná informace se zakóduje tak, že se rozprostře do pásma 22 MHz
 - K dispozici 3 takováto pásma
 - Pro rozprostření použity chip sekvence
 - Jedničkový bit=vyslání chip sekvence, nulový bit=vyslání negace chip sekvence

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

17

High-Rate Direct Sequence

- Vylepšená DSSS
- 802.11b definuje pro 5.5 a 11 Mb/s

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

18

Orthogonal Frequency Division Multiplexing

- Frekvenční pásmo děleno na množství úzkých subkanálů s menší bitovou rychlostí, do nich informace rozdělena
 - signál každého (pomalejšího) subkanálu je robustnější
 - max. 54 Mb/s
- Dosažitelné menší vzdálenosti
 - (zejména ve členitějším terénu)
- Používáno původně normou 802.11a (5 GHz), později i normou 802.11g (2,4 GHz)

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

19

Problémy při šíření signálu

- **Vícecestné odrazy**
 - na přijímači se sčítají různě zpožděné signály
 - zpoždění smí být rozprostřeno do max. 500 ns
- **Problém skrytého uzlu**
 - stanice S detekuje volný kanál ve svém okolí, avšak ten není volný v okolí přijímacího uzlu (typicky AP) - zdroj tohoto signálu je z pohledu stanice S "skrytým uzlem"
 - dáno omezeným dosahem signálu (neúplnou slyšitelností stanic)
 - Řešení: mechanismus RTS-CTS

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

20

Koordinace přístupu k médium

- Distributed Coordination Function (DCF)
 - CSMA/CA
- Point Coordination Function (PCF)
 - pro realtime aplikace (možnost implementace QoS)
 - centrální přidělování pásma AP (polling stanic)
 - kombinuje se s DCF
 - zatím málo implementováno a používáno

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

21

Kolize na rádiovém kanálu

- Detekce kolize na rádiovém médium problematická
 - anténa použita pro vysílání nebo příjem
 - není univerzální vzájemná slyšitelnost stanic
 - (problém skrytého uzlu)
- Lze detekovat volné médium, nelze detekovat kolizi

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

22

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

- Po odvysílání rámce se na určitou dobu médium rezervuje pro potvrzení.
 - v hlavičce vysílaného rámce je doba jeho vysílání (včetně doby pro potvrzení).
- Pokud se vysílač potvrzení nedočká (timeout), počká náhodnou dobu a opakuje pokus
- Broadcast a multicast zprávy se nepotvrzují

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

23

Řešení problému skrytého uzlu

- Stanice, která chce vysílat, pošle RTS - ten definuje zdroj, cíl a předpokládanou dobu přenosu
- Cílová stanice vyšle CTS se zopakovanou dobou trvání přenosu
- Všechny stanice slyšící RTS nebo CTS musí chápat médium po inzerované dobu jako obsazené

O nadcházejícím vysílání (vč. jeho trvání) se dozví všechny stanice v dosahu zdroje i v dosahu cíle.

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

24

Výhody mechanismu RTS-CTS

- Kolize mohou nastávat pouze během vysílání RTS
 - RTS je však krátký rámec, zhoršení efektivity vlivem kolizí není zásadní
- Efektivní pouze pro dlouhé datové rámce (vůči délce RTS rámce)
 - lze vypnout nebo stanovit práh délky vysílaného rámce pro použití RTS-CTS mechanismu

Spojová vrstva

Funkce spojové vrstvy

- zabezpečení CRC
- fragmentace rámců
 - na rádiovém médiu velká možnost zarušení, snaha o snížení režie při opakovaném přenosu dlouhých rámců
 - definuje se práh délky rámce pro fragmentaci
 - fragmenty se posílají jako shluk v rámci jednoho přístupu k médiu
- V hlavičce uveden typ použité modulace pro zbytek rámce
 - Hlavička vysílaná vždy základní rychlostí
- Definováno několik typů mezirámcových mezer
 - souvisí s metodou přístupu k médiu

Vyhledávání přístupového bodu

- Vyhledání AP iniciuje stanice
 - Probe Request na všech kanálech – obsahuje SSID stanice a podporované přenosové rychlosti
- AP odpovídá Probe Response
 - obsahuje mj. SSID, supported rates, přidělené parametry fyzické vrstvy pro komunikaci s danou stanicí (FHSS nebo DSSS)

Asociace s přístupovým bodem

- Asociace – AP mapuje svůj logický port na konkrétní stanici
 - Association Request (ze stanice)
 - obsahuje SSID, supported rates, listen (wakeupt) interval pro příjem rámců od AP (power save mode)
 - Association Response (od AP)
 - status code, Association ID, supported rates
 - Association ID použito pro další správu komunikace na rádiovém kanálu
- Stanice může být asociována současně vždy jen s jedním AP
 - Někdy možnost handoveru na jiné AP při ztrátě signálu
 - kritéria volby nového AP při handoveru závislé na implementaci klienta (kvalita signálu, zahlcení buňky, ...)
- AP umí obvykle řádově desítky asociací
 - (omezující je však spíše dostupná šířka pásma)

Autentizace

- Následuje po asociaci
 - jen stanice vůči síti
- Módy Open a Shared Key
 - Open = bez autentizace
 - Shared Key = autentizuje pomocí sdíleného šifrovacího klíče z WEP
- Zprávy Authentication Request, Authentication Response

Funkce Power-Save

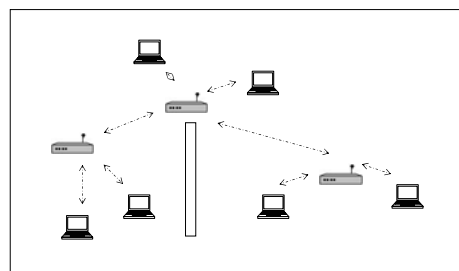
- Umožňuje šetření baterie stanic při zachování možnosti příjmu rámců pro stanici
 - (stanice ve standby režimu)
- AP bufferuje unicast rámce pro stanici
 - Stanice se budí vždy jen periodicky pro příjem informačního (beacon) rámce od AP (wakeup interval)
 - V beacon rámci obsažena informace, pro které stanice má AP bufferovány rámce
 - Když probuzený klient slyší, že AP pro něj bufferuje rámce, žádá o ně AP poll rámcem
- Interval, po kterém se mají stanice budit pro příjem broadcastů, definuje administrátor AP a propaguje se v beacon rámcích
 - Bufferování broadcast/multicast rámců se provádí vždy, když je v buňce alespoň jedna power-save stanice

Speciální zařízení rádiové infrastruktury

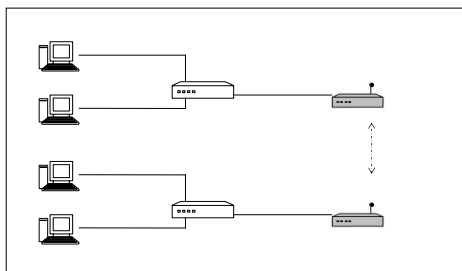
Repeater, Bridge

- Repeater AP
 - čistě bezdrátový most (není připojen na pevnou síť)
 - vysílá i přijímá na stejném kanále – přináší zdvojnásobení zátěže pásma ve svém okolí
 - repeater je klientem jiného AP (je s ním asociován)
- Workgroup Bridge
 - Připojuje pracovní skupinu stanic vybavených pouze Ethernetem do WiFi
 - chová se jako Ethernet switch/hub s WiFi kartou
 - Enkapsuluje Ethernet rámce do WiFi rámců, přijímající AP musí odpovídajícím způsobem deenkapsulovat
- Wireless Bridge
 - Obdoba workgroup bridge, ale hlavním smyslem je (dvoubodově) rádiové propojení LAN na větší vzdálenost

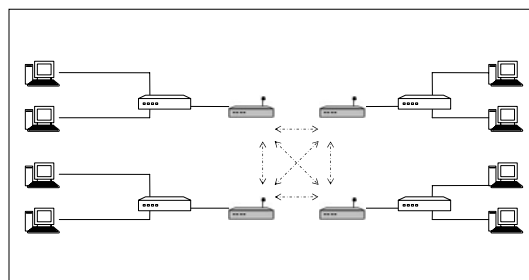
Použití repeateru



Použití Point-to-Point Bridge



Použití Point-to-Multipoint Bridge



Interoperabilita speciálních zařízení

Funkce speciálních zařízení není standardizována

- Názvosloví není zcela ujednoceno
- Nejistá interoperabilita mezi výrobci
- Při propojování bezdrátových sítí vhodné alespoň ověřit, zda AP podporuje „client mode“ = možnost propojení s jiným AP

Bezpečnost

Bezpečnostní mechanismy a architektury

- autentizace, šifrování
- SSID (Service Set Identifier)
 - Název přístupového bodu
 - Nemusí se vysílat (ale neutají se, lze odchyťt)
 - Spíše slouží k identifikaci AP
- WEP – Wired-Equivalent Privacy
 - sdílený klíč (64/128B) slouží současně pro autentizaci i šifrování
 - snadno prolomitelný při dostatku času a dat na kanále
 - řádově za několik hodin
 - volně dostupný crackovací SW
 - užitečné implementovat alespoň mechanismus periodické změny klíčů (TKIP)
- WPA
 - odstraňuje nedostatky WEP (lepší šifrovací algoritmus, dočasné klíče, ...)
 - zatím není široce implementován na bezdrátových stanicích