Počítačové sítě, v. 3.6

Katedra softwarového inženýrství,
Matematicko-fyzikální fakulta,
Univerzita Karlova, Praha

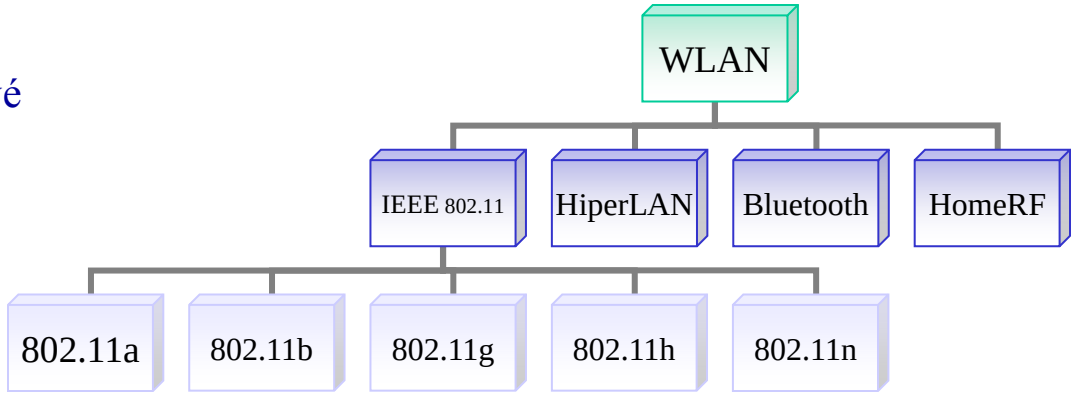
Lekce 5: Bezdrátový Ethernet (IEEE 802.11)

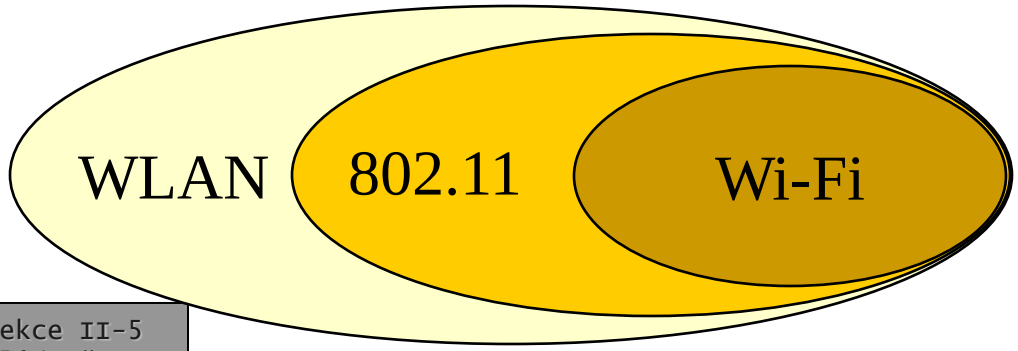
od bezdrátovému Ethernetu k Wi-Fi

- snahy o další rozvoj Ethernetu se ubíraly různými cestami
  - jiná (drátová) přenosová média
    - kroucená dvoulinka, optická vlákna
  - vyšší rychlosti
    - 100Mbit/s, 1Gbit/s, 10Gbit/s, ….
  - "jiné využití"
    - metropolitní Ethernet, "carrier-grade“ Ethernet, Ethernet v první míli (EFM)
  - bezdrátový Ethernet
    - snaha zbavit se závislosti na drátech
      - aby nebylo nutné instalovat kabeláž
    - původně zamýšleno spíše pro "průmyslové využití"
      - pro propojování různých zařízení (spíše než počítačů)
- další vývoj "bezdrátového Ethernetu":
  - využití pro propojení počítačů na krátkou vzdálenost
    - hlavně "indoor", jen málo "outdoor"
      - v rámci sítí LAN
  - přestala se akcentovat vazba na Ethernet
    - začíná se obecně hovořit jako o jedné variantě sítí WLAN
- předpoklady úspěchu:
  - dostupné frekvence
    - pro bezlicenční použití
      - pásma 2,4 GHz a 5 GHz
  - standardizace
    - ujala se IEEE, pracovní skupina 802.11
    - standard **IEEE 802.11** a další
      - 802.11b, 8011.a, 802.11g, 802.11h
  - praktické dodržování standardů, kompatibilita
    - ujala se asociace WECA
      - Wireless Ethernet Compatibility Alliance
  - "marketing"
    - brand **Wi-Fi**

WLAN vs. Wi-Fi

- **WLAN** (Wireless LAN)
  - je obecné označení pro bezdrátové sítě LAN
- "bezdrátový Ethernet" (IEEE 802.11) je pouze jednou z technologií, které mohou být použity v rámci WLAN
  - dalšími technologie jsou např. Bluetooth, HIPERLAN, HomeRF, ….
- technologie IEEE 802.11 jsou dnes používány i mimo WLAN
  - např. v prostředí WirelessMAN, Wireless WAN
  - pro to nebyly původně určeny

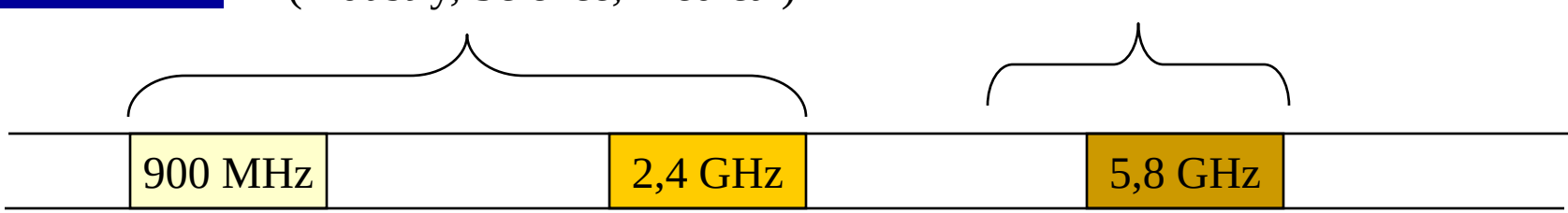




- **Wi-Fi** není to samé jako WLAN či IEEE 802.11…
  - Wi-fi je "nálepka" (známka)
  - uděluje se těm produktům, které vyhovují standardům (802.11…) a splňují požadavky na vzájemnou kompatibilitu
  - uděluje je organizace Wi-Fi Alliance
    - dříve WECA, Wireless Ethernet Compatibility Alliance

historie "bezdrátového Ethernetu"

FCC Federal Communications Commission



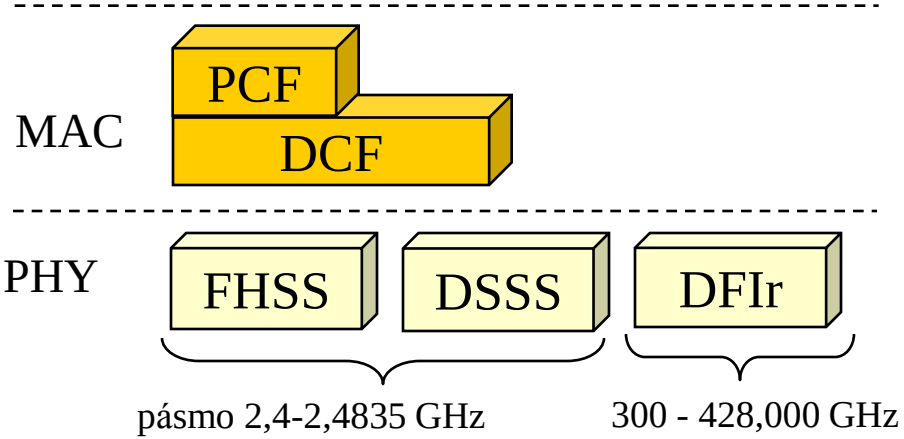
- 1985: americký regulátor (FCC, Federal Communications Commission) uvolňuje tři "odpadková" frekvenční pásma
  - v pásmu 900 MHz, 2.4 GHz
    - později též v pásmu 5.8 GHz (UNII)
  - umožňuje jejich využití bez licence (uvolňuje je jako "bezlicenční")
    - do té doby nebyla žádná bezlicenční pásma (jen radioamatérská)
  - tato pásma ale již byla dříve alokována pro jiné účely než pro komunikace
    - např. pro mikrovlnné trouby
- byl to obrovský impuls pro rozvoj bezdrátových řešení

- (technické) důsledky:
  - podmínkou pro využití těchto pásem pro komunikace bylo využití takových technik, které se dokáží vyhnout rušení
    - od mikrovlnných trub apod.
  - řešením je rozprostření do širšího spektra
    - použití technik jako je Frequency Hopping či Spread Spectrum
- (další) důsledky
  - řešení v pásmu 2,4 GHz se snáze šíří po celém světě
    - někde jsou "drobné" problémy s vyhrazením pásma pro jiné účely
  - řešení v pásmu 5 GHz je "hodně americké"
    - jinde ve světě se prosazuje obtížněji

historie "bezdrátového Ethernetu"

- 1986-7: objevují se první proprietární řešení
  - např. Proxim, Symbol
    - využívající pásma ISM a UNII
    - jsou navzájem nekompatibilní
  - objevuje se potřeba společného standardu
    - aby si proprietární řešení rozuměla navzájem
- 1988: vzniká pracovní skupina IEEE **802.11**
  - z iniciativy společnosti NCR
    - chtěla bezdrátově propojit své pokladny
- 1989-97: hledání technického řešení
  - 1990: vzniká AT&T WaveLAN
    - používá techniku DSSS
  - 1996: první čipset pro bezdrátový Ethernet
    - Harris (Intersil): PRISM WLAN chipset
- 1997: dosažena dohoda na společném standardu
  - IEEE 802.11
    - "bezdrátový Ethernet"

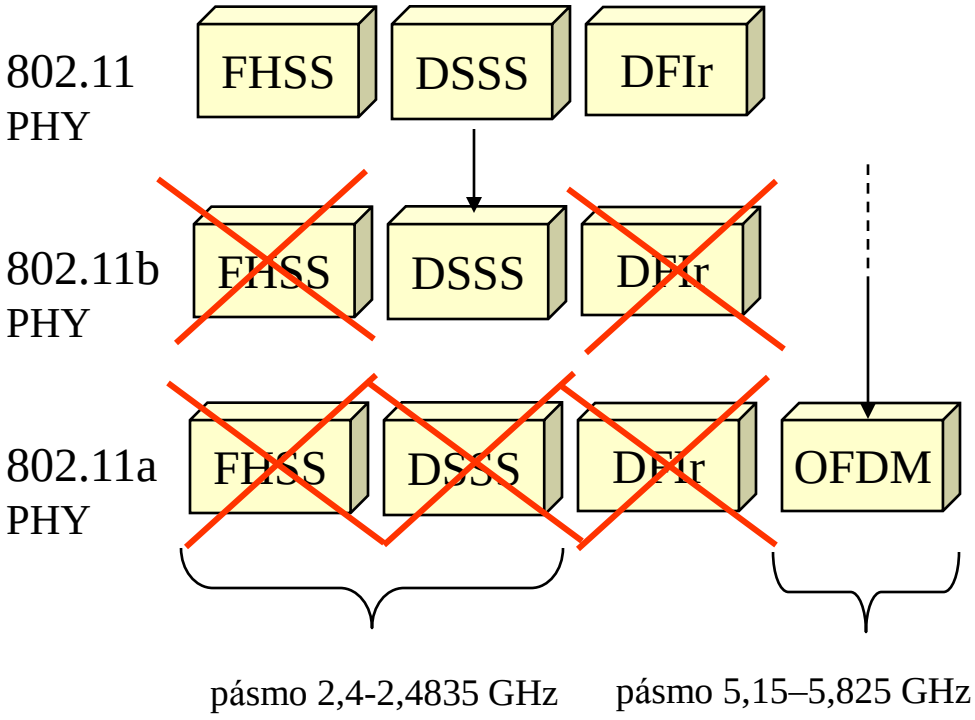
- co standard pokrývá:
  - podvrstvu MAC (řízení přístupu):
    - varianta PCF
      - Point Coordination Function
    - varianta DCF
      - Distributed Coordination Function
  - fyzickou vrstvu (PHY)
    - FHSS
      - Frequency Hopping Spread Spectrum
    - DSSS
      - Direct Sequence Spread Spectrum
    - DFIr
      - Diffused Infrared (v praxi se neprosadilo)
- maximální přenosová rychlost:
  - 2 Mbit/s
    - resp. 1 Mbit/s, podle použitého řešení PHY



další vývoj IEEE 802.11

- 1997: standard 802.11 byl již při svém schválení zastaralý
  - ihned začaly práce na jeho vylepšení
    - hlavně: zvýšení rychlosti
- vznikají nové pracovní skupiny
  - Task Group "A"
    - snaží se využít nově přidělené pásmo UNII (5,8 GHz)
    - vyvíjí úplně novou techniku modulace (řešení PHY)
      - OFDM, Ortogonal Frequency Division Multiplexing
    - dosahuje rychlosti 54 Mbit/s
  - Task Group "B"
    - snaží se zrychlit dosavadní řešení v pásmu 2,4 GHz
    - opouští techniku DFIr
      - nikdy se neujala
    - opouští techniku FHSS
      - kvůli předpisům FCC by nešlo zrychlit přenosy
    - dosahuje rychlosti 11 Mbit/s

- 1999: jsou schváleny nové standardy
  - 802.11a
    - 54 Mbit/s v pásmu 5 GHz
      - použitelné v USA
  - 802.11b
    - 11 Mbit/s, v pásmu 2,4 GHz

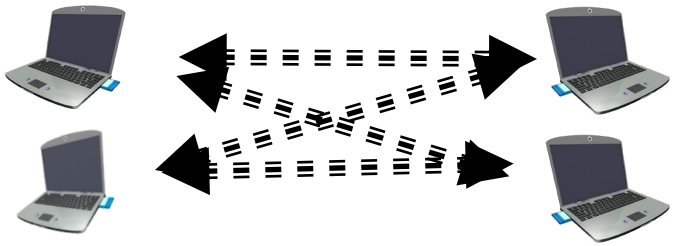


RLAN a HIPERLAN

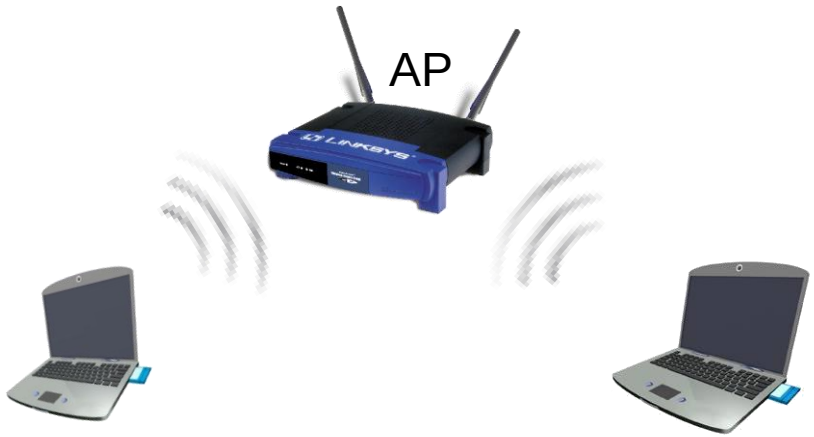
- standardy IEEE 802.11 jsou "americké"
  - ale používají se po celém světě
- existovala/existuje i „evropská vývojová větev“:
  - místo WLAN hovoří o RLAN
    - Radio Local Area Network
  - a HIPERLAN
    - HIgh PErformance Radio Local Area Network
- původně byla tato větev samostatná
  - neměla nic společného s IEEE 802.11
    - nebyla kompatibilní
  - standardy vydává ETSI a CEPT
    - The European Telecommunications Standards Institute
    - Conference of European Posts and Telecommunications
- 1991:
  - CEPT vydává doporučení pro RLAN v pásmu 2,4 GHz
    - požadavek: používání technik rozprostřeného spektra
    - 1994: první instalace, se směrovou anténou
- 1997:
  - ETSI vydává normu ETS 300 652 pro HIPERLAN1
    - pásmo 5 GHz
    - max. přenosová rychlost až 23,5 Mbit/s
    - nebylo nikdy komerčně využito/realizováno
- 2000:
  - ETSI vydává standard HIPERLAN2
    - již "založený" na IEEE 802.11a, ale ne identický
      - "šetrnější k éteru"
    - rozšíření nedosahuje takové úrovně, jako IEEE 802.11

architektura IEEE 802.11: dva základní režimy fungování

- pro dvoubodový spoj
- pro vícebodové propojení
  - kdy dva terminály komunikují přímo mezi sebou
  - označováno jako:
    - obecně: peer-to-peer mode
    - IEEE 802.11: "**ad-hoc mode**"

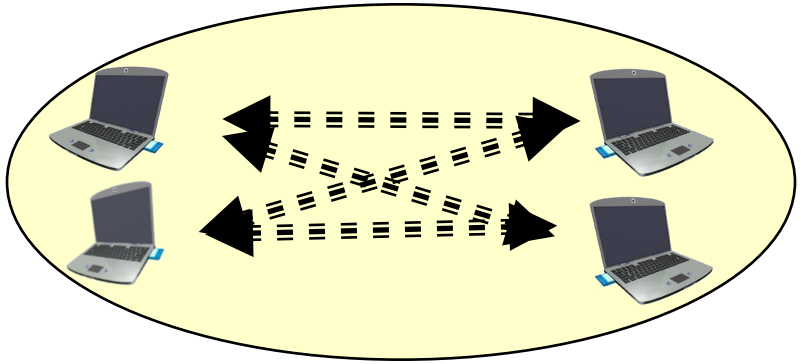


- "do hvězdy"
  - 1 přístupový bod (**AP**, Access Point)
    - dále n terminálů (**STA**, Station)
      - terminály nekomunikují přímo mezi sebou
      - ale jen s AP, resp. přes AP
  - AP je analogií základnové stanice v mobilních sítích
  - přenosová kapacita je sdílena všemi právě aktivními terminály
  - v IEEE 802.11 označováno jako:
    - "**infrastructure mode**"

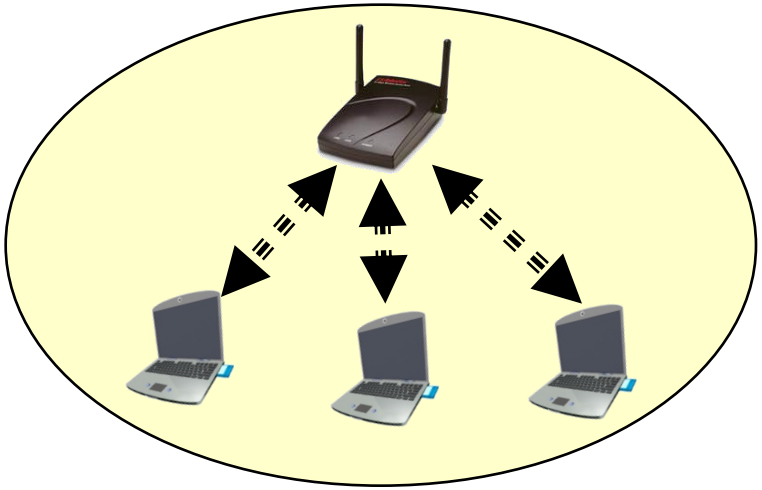


architektura IEEE 802.11

- BSS (Basic Services Set)
  - nejmenší prvek architektury bezdrátových sítí IEEE 802.11
  - analogie buňky v mobilních sítích
  - dva či více počítačů, které se navzájem rozpoznaly a komunikují spolu
- BSS nemusí obsahovat přístupový bod (AP)
  - pak jde o tzv. IBSS
    - Independent BSS
    - není provázán s okolím
    - uzly komunikují v režimu ad-hoc
- častěji BSS obsahuje přístupový bod
  - přístupový bod (AP, Access Point) je zamýšlen jako rozhraní mezi bezdrátovou sítí a sítí "drátovou" (okolím)
  - jakmile je AP přítomen v BSS, veškerá komunikace prochází přes AP
    - uzly by spolu neměly komunikovat přímo
    - uzly v rámci BSS komunikují v režimu infrastruktury



IBSS (Independent BSS)
žádný AP, uzly komunikují přímo mezi sebou

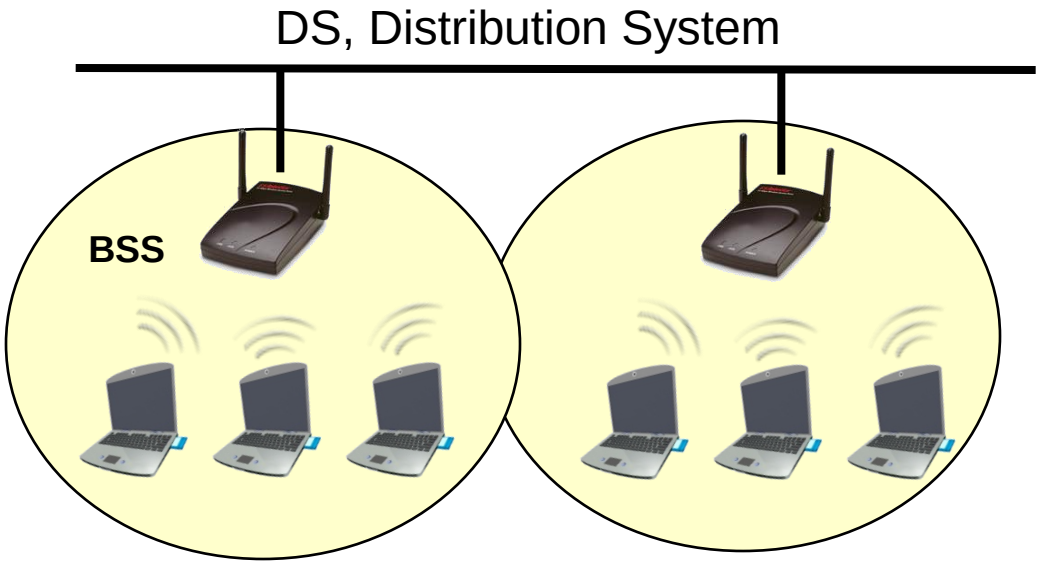


BSS (Basic Service Set)
1 AP připojený ke drátové síti, více terminálů "do hvězdy" režim "infrastructure"

DS, Distribution System

- BSS je analogií buňky
  - v mobilní síti
- BSS (nikoli IBSS) je obvykle napojen na další sítě
  - drátové i bezdrátové
- ke vzájemnému propojení BSS slouží tzv. Distribution System (DS)
  - předpokládá se, že DS je spíše "drátová" síť
- DS propojuje na úrovni linkové vrstvy
  - propojení je "neviditelné" pro podvrstvu LLC
  - DS propouští broadcast

- DS (Distribution System) může být:
  - drátový (Wired Distribution System)
    - častější, nejvíce se používá "drátový" Ethernet (opakovače, přepínače, mosty)
  - bezdrátový (Wireless Distribution System)
    - může propojovat dvě drátové sítě
      - Wireless Bridge
    - nebo i dvě bezdrátové sítě

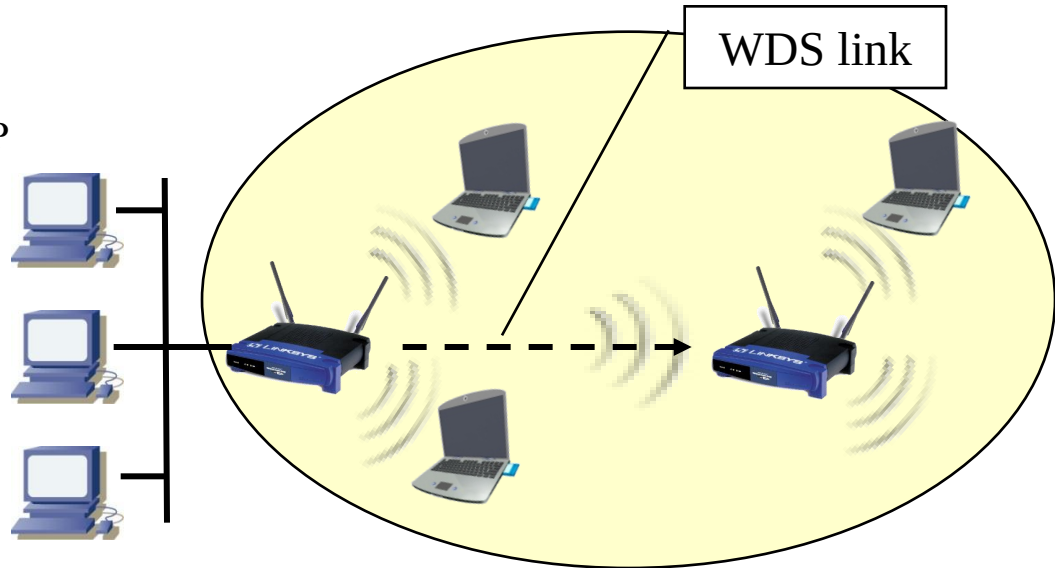


způsob implementace DS není ve standardu IEEE 802.11 definován !!

varianty DS: WDS a Repeating WDS

- WDS, Wireless Distribution System
  - propojuje dvě "drátové" sítě, bezdrátovým způsobem
  - provoz mezi oběma AP nepřijímá žádný jiný uzel
    - "WDS link" je spojení mezi dvěma AP
- toto řešení bývá v praxi označováno také jako "wireless bridging"
  - propojení dvou zařízení v režimu "wireless bridge"
  - bezdrátová obdoba klasického mostu

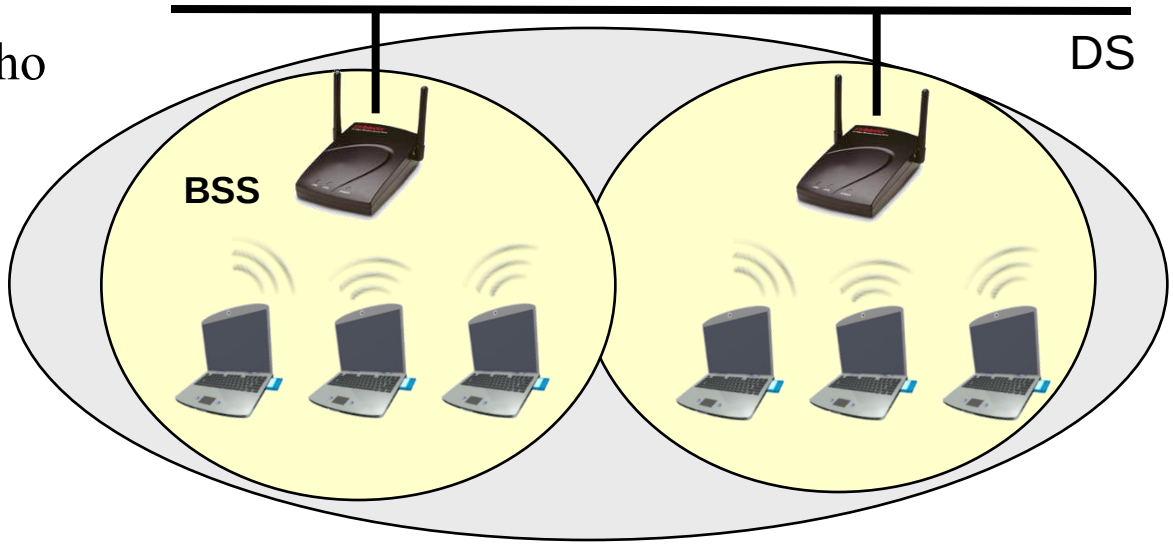
- Repeating WDS, Wireless Repeater
  - jeden uzel funguje jako běžný přístupový bod (AP)
  - druhý uzel má 2 RF rozhraní
    - jedno se chová jako klient (stanice) vůči prvnímu AP
    - druhé se chová jako AP, snaží se emulovat první AP (stejná MAC adresa, SSID, šifrování atd.)
- slouží ke zvětšení dosahu bezdrátové sítě



ESS, Extended Service Set

- propojením několika BSS vzniká ESS
  - Extended Service Set
- odpovídá "bezdrátové síti"
  - síti WLAN
  - je to jedna broadcast doména
- umožňuje "mobilitu"
  - přechod z jedné buňky (BSS) do druhé (i do jiné ESS)
- AP jsou součástí distribučního systému (DS)
  - předpokládá se, že nejsou mobilní (pohyblivé)
- všechny AP ve stejném ESS mají stejný identifikátor
  - SSID (≅ jméno sítě)
  - ale mají odlišné BSSID (≅ jméno buňky)

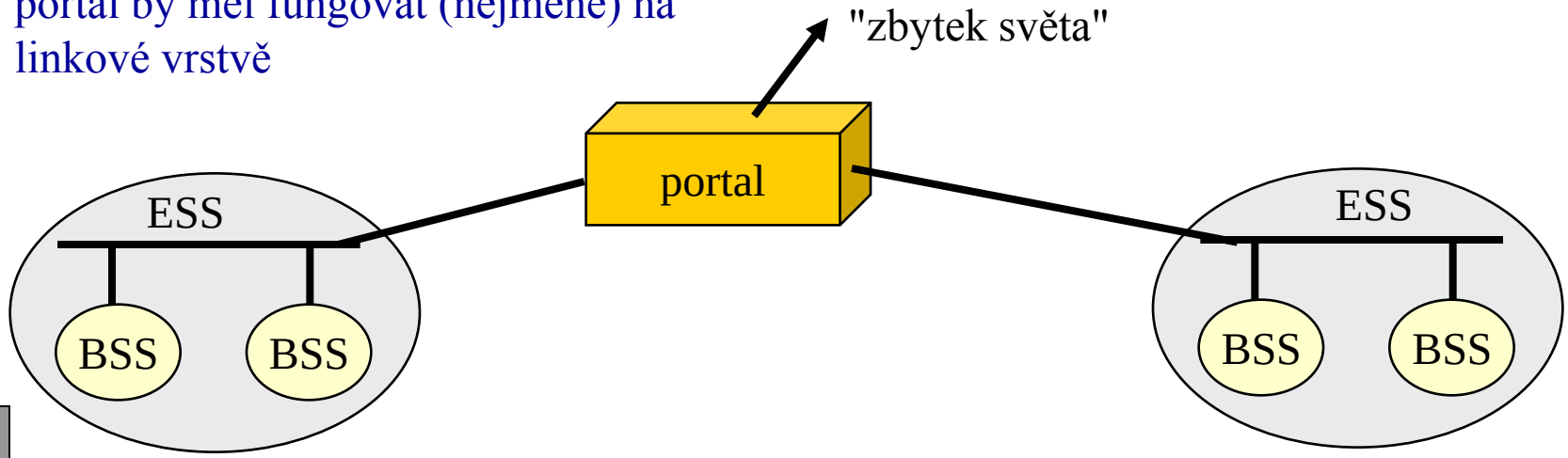
- každá stanice vždy "patří" jen do jedné BSS
- možnosti "mobility":
  - "no transition"
    - stanice zůstává ve stejné BSS
  - "BSS-transition"
    - stanice přechází mezi různými BSS, ale zůstává v rámci stejné ESS
  - "ESS transition"
    - stanice přechází do jiné ESS



ESS (Extended Service Set)
více BSS propojených skrze Distribution System (DS)

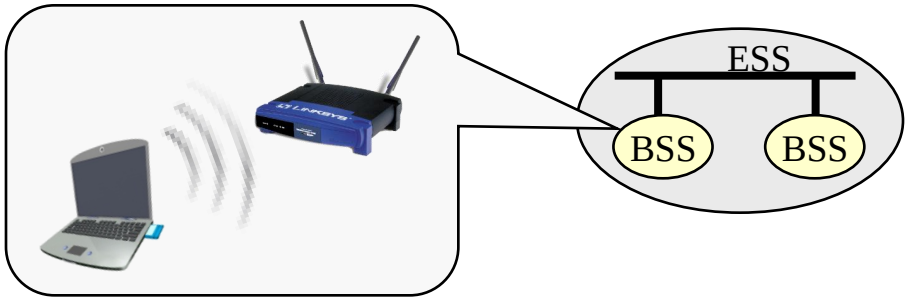
hierarchie a mobilita

- standard IEEE 802.11 požaduje možnost provázání bezdrátových sítí s "drátovými"
  - 802.11 vs. 802.X
- přechod realizuje zařízení označované jako portál
  - je bodem přístupu k DS
  - veškerá data mezi drátovou a bezdrátovou sítí musí procházet přes portál
  - portál by měl fungovat (nejméně) na linkové vrstvě
- "mobilita"
  - v rámci BSS (no-transition)
    - nevyžaduje žádnou akci
  - mezi BSS
    - postačuje Reassociation
  - mezi ESS
    - analogie roamingu
    - není podporováno
    - stanice si může zajistit sama!!
      - lze řešit v SW stanice



funkce DS

- standard IEEE 802.11 definuje služby, které DS poskytuje:
  - skrze AP, které jsou součástí DS
- rozdělení služeb:
  - Station Services (SS)
    - týkají se vztahu/komunikace mezi AP a stanicí
  - Distribution System Services (DSS)
    - týkají se "příslušnosti" stanic do buněk a k distribučním systémům (DS)
- Station Services:
  - Authentication
    - autentizace
    - stanice se ověřuje vůči AP:
      - Open System Authentication: žádné ověření, vyhoví každá stanice
      - pomocí WEP (Wired Equivalent Privacy), resp. "shared key"
        - » stanice musí vlastnit sdílený klíč
        - » klíč je stejný pro všechny stanice



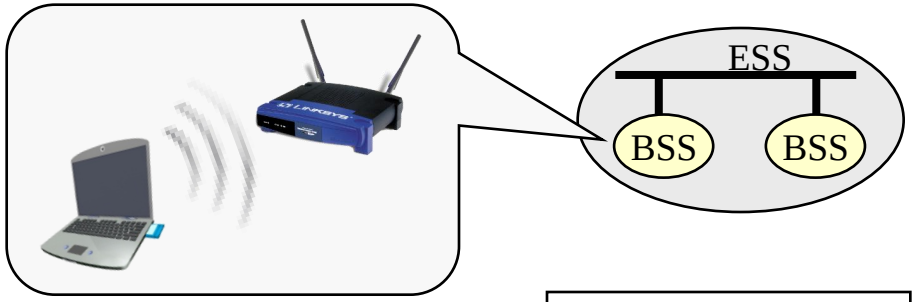
  - Deauthentication
    - ukončení vzájemné vazby mezi AP a stanicí
      - například když stanice přechází z jedné buňky (DSS) do jiné
  - Privacy
    - zajištění důvěrnosti
    - řeší se šifrováním
    - možnosti:
      - žádné šifrování (data se přenáší v plaintextu)
      - WEP (Wired Equivalent Privacy)
        - » symetrické šifrování
  - MAC Service Data Unit (MSDU) Delivery
    - vlastní přenos linkových rámců
      - na úrovni MAC podvrstvy

otázka bezpečnosti

- WEP (Wired Equivalent Privacy) je hodně „slabé“ řešení
  - používá 40-bitové šifrování RC4 (dnes již snadno prolomitelné)
    - slabiny WEP-u jsou známy již od roku 2001
- duben 2004: Wi-Fi Alliance (nikoli IEEE) zavádí WPA
  - WiFi Protected Access
    - je určen k tomu, aby nahradil WEP a nevyžadoval změnu v HW
      - ale jen jako dočasné řešení, než IEEE 802 přijde s „řádným“ řešení
    - poskytuje silnější šifrování a autentizaci uživatelů
  - zahrnuje:
    - protokol TKIP (Temporal Key Integrity Protocol)
      - který dynamicky generuje nové klíče pro každý jednotlivý paket, což znesnadňuje útoky
    - prvky 802.1x pro autentizaci uživatelů
- červenec 2004: IEEE schvaluje standard 802.11i
  - známý jako WPA2 (WiFi Alliance zajišťuje testování interoperability)
    - dnes je podpora WPA2 povinná pro všechna zařízení, která chtějí projít certifikací

funkce DS

- pozorování:
  - u "drátových sítí" je skrze zapojení jasné, "kdo kam patří"
    - do jaké sítě/segmentu
  - u bezdrátových sítí to tak jasné být nemusí
    - proto se stanice explicitně přihlašují (asociují) k buňkám sítě, resp. k jejich přístupovým bodům (AP)
- Distribution System Services
  - Association
    - stanice se "asociuje" s konkrétním AP v jedné BSS
    - v rámci toho musí proběhnout autentizace stanice vůči tomuto AP
    - teprve pak může stanice přenášet nějaká data z/do AP
  - Reassociation
    - opakovaná asociace, při přechodu mezi AP v rámci různých BSS (stejné ESS)
    - postačuje pro zajištění "BSS-transition"



iniciuje stanice nebo AP

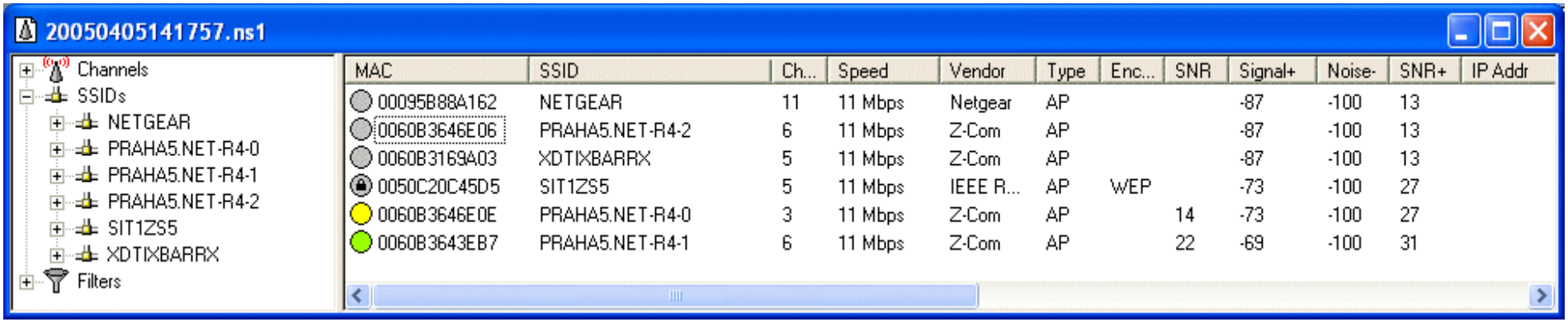
  - Disassociation
    - zrušení asociace
    - stanice poté již nemůže přijímat/odesílat data skrze AP
  - Distribution
    - přenos dat v rámci ESS po DS
    - odesilatel předá "svému" AP, ten využije DS k distribuci (přenosu) dat k příslušnému AP, které předá koncovému příjemci
  - Integration
    - přenos dat mimo danou ESS
    - skrze tzv. portál

iniciuje stanice

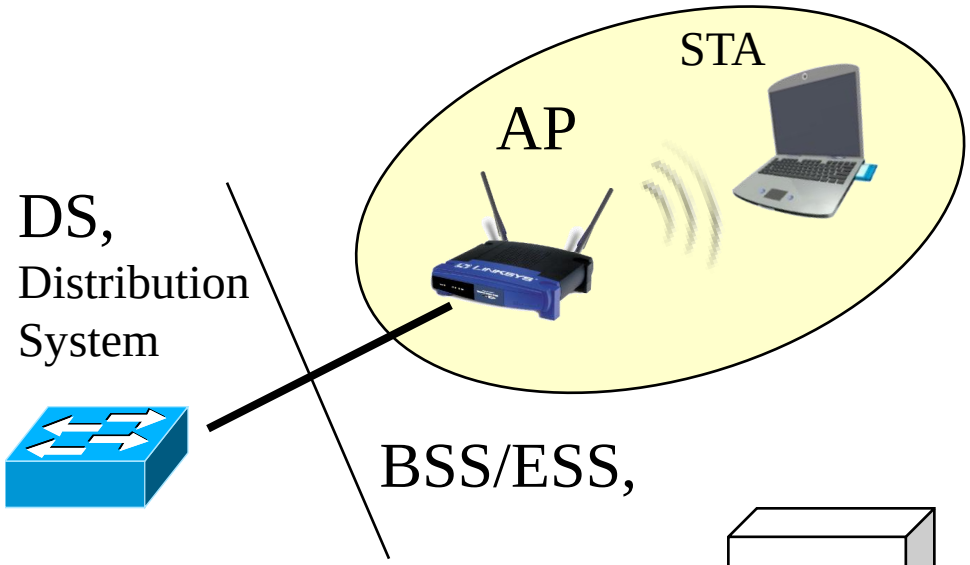
identifikátory

- **SSID**
  - Service Set Identifier
  - 32-znakové jméno sítě
    - v rámci ESS musí být všude stejné
    - přenáší se v rámcích nezašifrovaně
      - lze snadno odposlechnout
  - v rámci ESS (IBSSS) musí být všude stejné
- ESSID
  - Extended SSID (pouze rozšíření SSID)

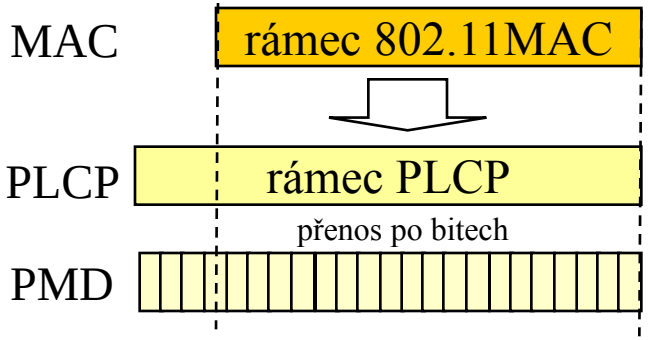
- BSSID
  - Basic Service Set Identifier
  - má 6 bytů
  - je jiné v každé BSS
  - BSS v režimu infrastruktury:
    - BSSID je MAC adresou AP
  - BSS v režimu ad-hoc:
    - BSSID je generováno náhodně



protokolová architektura 802.11



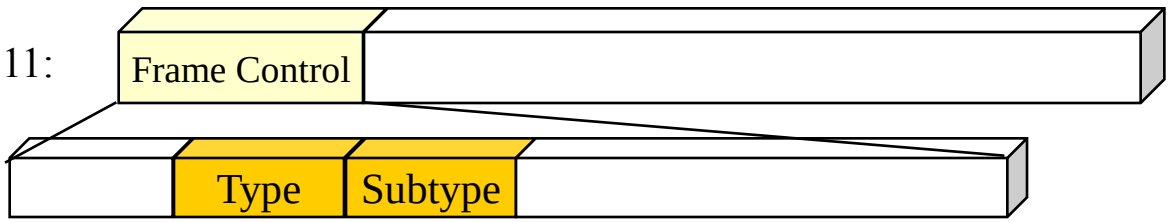
- fyzická vrstva IEEE 802.3 je ve skutečnosti rozdělena do dvou podvrstev
  - vyšší: PLCP
    - Physical Layer Convergence Protocol
    - zajišťuje detekci nosné a rozhraní k PMD
  - nižší: PMD
    - Physical Media Dependent
    - zajišťuje modulaci a kódování signálů



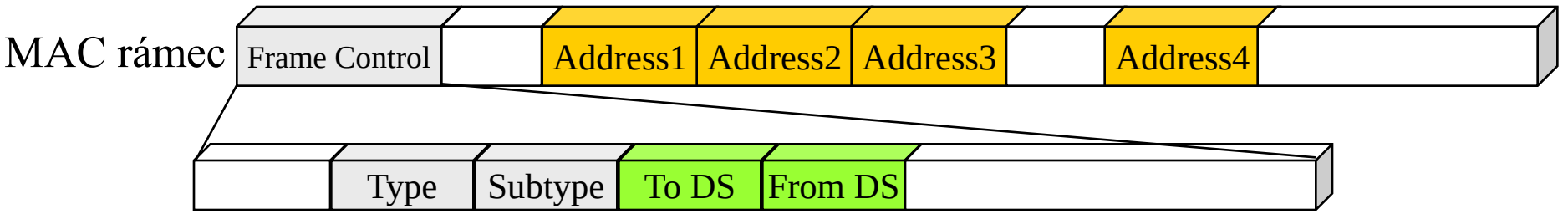
druhy a formáty rámců

- bezdrátové sítě dle IEEE 802.11 používají různé druhy rámců:
  - PLCP rámce
    - jsou závislé na řešení na úrovni PMD:
      - PLCP rámce pro FHSS
      - PLCP rámce pro DSSS
    - zajišťují funkce související s šířením signálu
      - zejména indikují rychlost, s jakou jsou přenášena data
  - MAC rámce
    - **řídící rámce** (Control Frames)
      - RTS/CTS, pro fungování přístupové metody
      - ACK, pro potvrzování přijatých datových rámců
    - **rámce pro správu** (Management Frames)
      - Beacon ("maják")
        - » využívá AP k inzerování své přítomnosti
      - Probe, Probe Response
        - » pro zjišťování přítomnosti a schopnosti uzlů
      - Association Request/Response
        - » žádost/odpověď na asociaci stanice s AP
      - Re-association Request/Response
        - » žádost/odpověď na asociaci s jiným AP v téže ESS
      - Disassociation
        - » žádost o ukončení asociace stanice s AP
      - Authentication
        - » žádost o autentizaci uzlu vůči AP
      - De-authentication
        - » žádost o ukončení autentizace uzlu vůči AP
    - **datové rámce** (Data Frames)

MAC rámec IEEE 802.11:

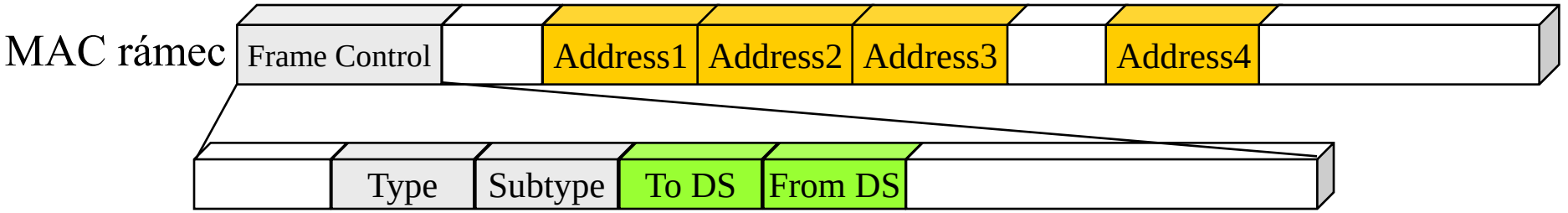


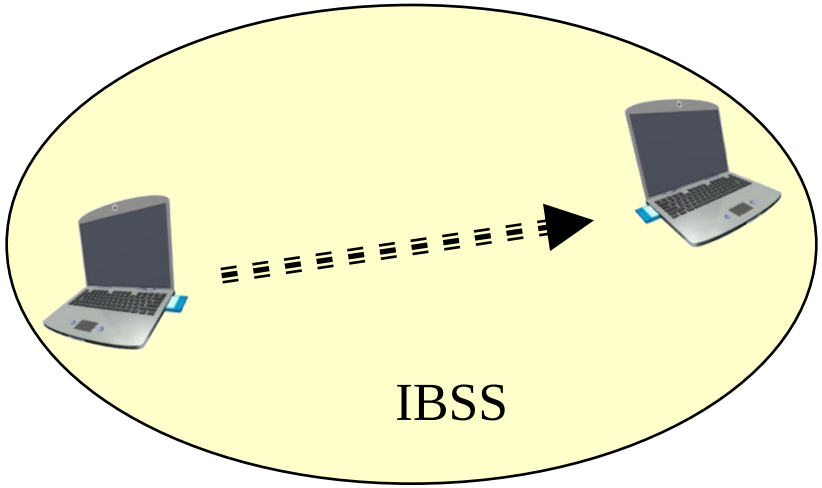
adresy v MAC rámcích



- v MAC rámcích IEEE 802.3 se uvádí jen dvě adresy
  - MAC adresy odesilatele a příjemce
- v MAC rámcích IEEE 802.11 se uvádí až 4 adresy
  - kvůli tomu, že komunikace může "přestupovat" přes přístupové body (AP) a procházet přes distribuční systém (DS)
    - "logický" a "fyzický" příjemce se mohou lišit
  - je třeba pamatovat na to, že potvrzovací rámce ACK se mohou posílat jinému uzlu, než je původní odesilatel (zdroj dat)
- je nutné rozlišit následující situace:
  - režim ad-hoc:
    - přímá komunikace dvou uzlů
  - režim infrastruktury:
    - přenos od AP ke stanici
    - přenos od stanice k AP
    - přenos přes DS
  - k rozlišení těchto 4 možností slouží dva bity
    - To DS
      - příjemcem je/není AP/DS
    - From DS
      - odesilatelem je/není AP/DS
- adresa "Address1" je vždy adresou příjemce
  - podle ní uzel posuzuje, zda se jej právě vysílaný rámec týká či netýká

adresy v MAC rámcích: ad-hoc síť

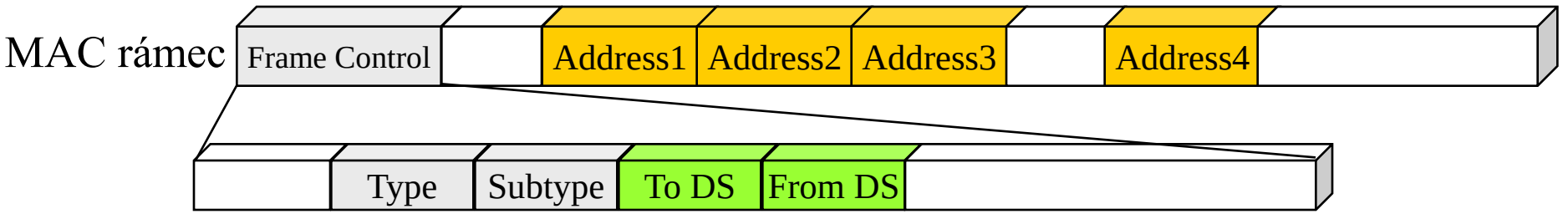


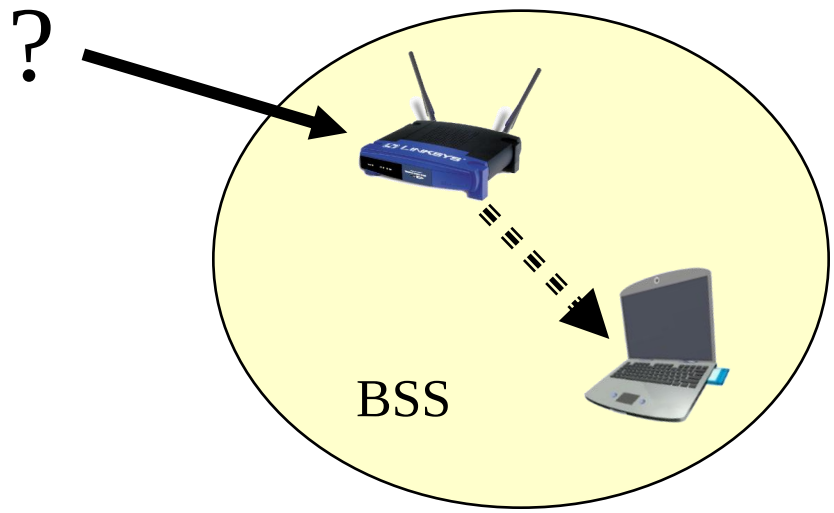


- přímá komunikace dvou uzlů
  - v režimu ad-hoc, v rámci IBSS

- To DS = 0
  - příjemcem je uzel, nikoli AP (resp. DS)
- From DS = 0
  - odesilatelem je uzel, nikoli AP (resp. DS)
- Address1:
  - DA: Destination address
    - MAC adresa příjemce
- Address2:
  - Sender Address:
    - MAC adresa odesilatele

adresy v MAC rámcích: "od AP"



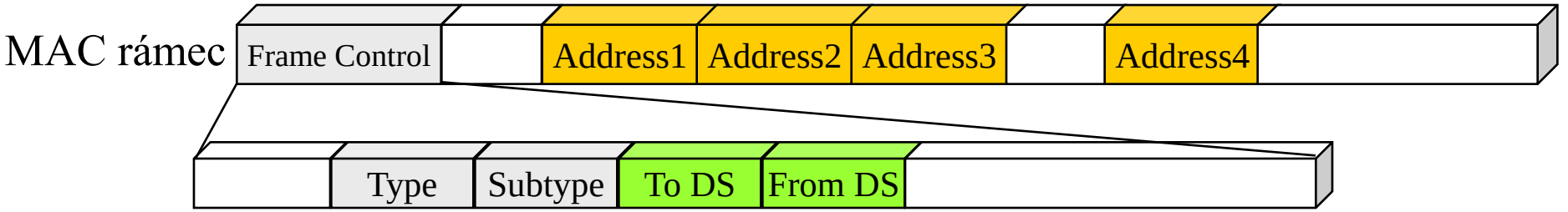


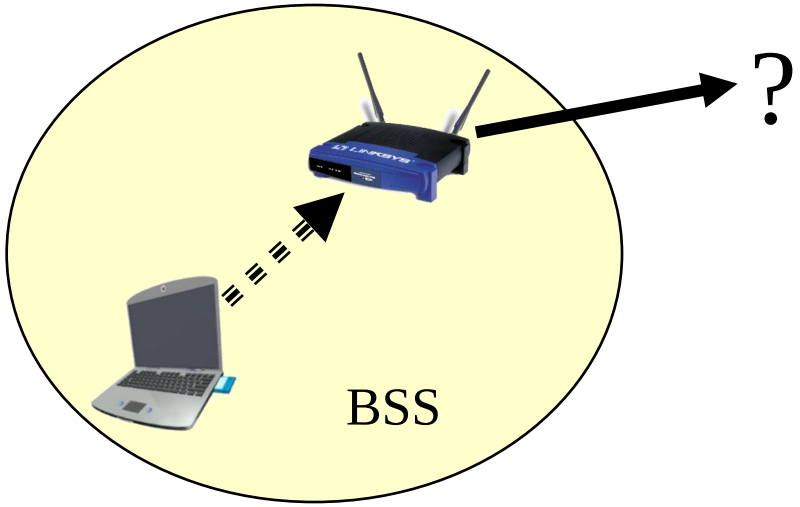
- přenos od AP ke stanici
  - v režimu infrastruktury,
  - v rámci BSS
- je třeba vzít v úvahu, že "logickým odesilatelem" může být jiný uzel než je AP
  - na úrovni linkové vrstvy

- To DS = 0
  - příjemcem je uzel, nikoli AP/DS
- From DS = 1
  - odesilatelem je AP, nikoli uzel
- Address1:
  - DA (Destination Address): logický a fyzický příjemce
    - MAC adresa stanice
- Address2:
  - BSSID: fyzický odesilatel
    - MAC adresa AP
- Address3:
  - SA (Sender Address): logický odesilatel
    - MAC adresa toho uzlu, od kterého data pochází

může, ale nemusí platit ADDRESS2 = ADDRESS3 !!!

adresy v MAC rámcích: "k AP"



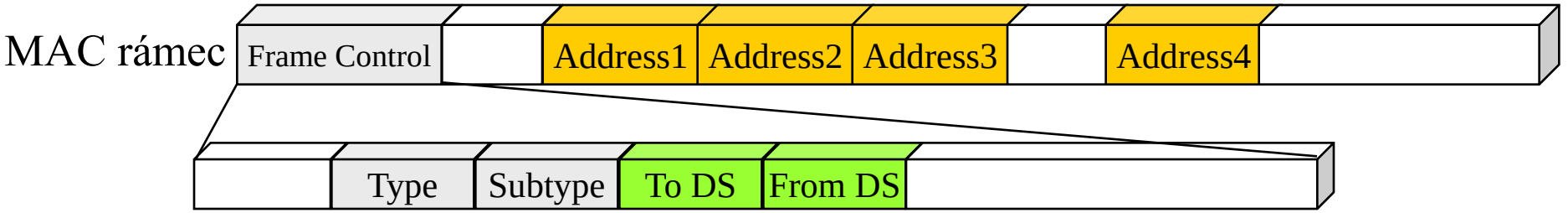


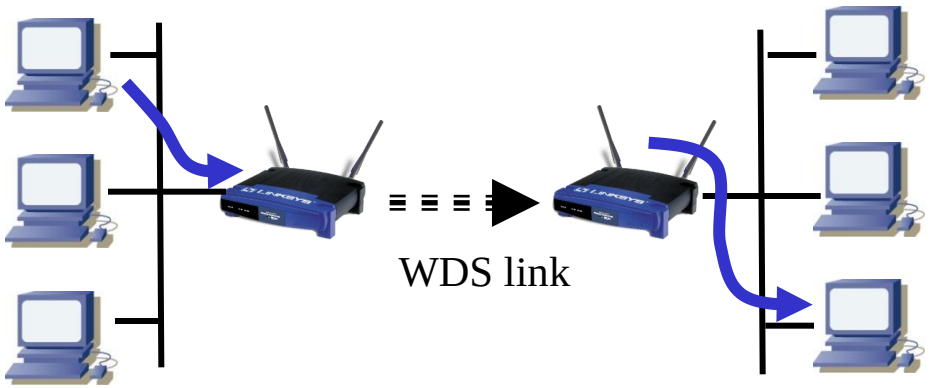
- přenos od stanice k AP
  - v režimu infrastruktury,
  - v rámci BSS
- je třeba vzít v úvahu, že "logickým příjemcem" může být jiný uzel než je AP
  - na úrovni linkové vrstvy

- To DS = 1
  - příjemcem je AP, nikoli uzel
- From DS = 0
  - odesilatelem je uzel, nikoli AP/DS
- Address1:
  - BSSID: fyzický příjemce
    - MAC adresa AP
- Address2:
  - SA (Sender Address): logický a fyzický odesilatel
    - MAC adresa stanice
- Address3:
  - DA (Destination Address): logický příjemce
    - MAC adresa toho uzlu, kterému jsou data určena

může, ale nemusí platit ADDRESS1 = ADDRESS3 !!!

adresy v MAC rámcích: "přes DS"

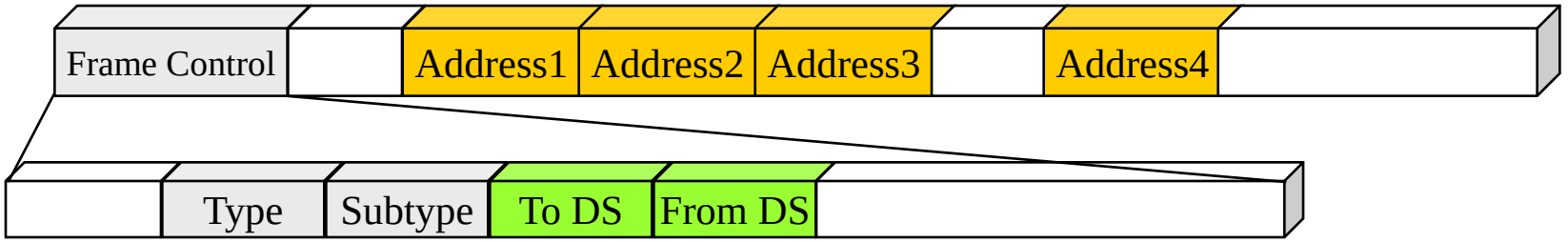




- přenos mezi dvěma segmenty, které jsou propojeny na úrovni linkové vrstvy pomocí WDS (Wireless Distribution System)
  - data si fyzicky předávají přístupové body (AP)
  - logickým odesilatelem i příjemce jsou ale jiné uzly než tyto AP

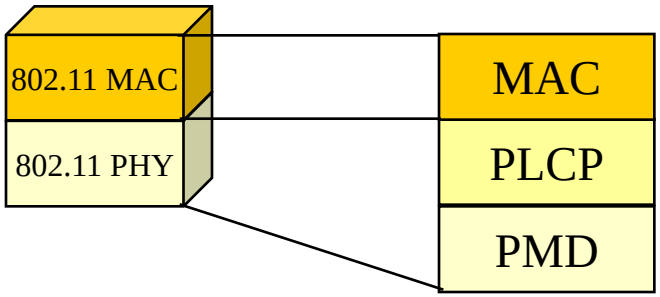
- To DS = 1
  - příjemcem je AP/DS, nikoli uzel
- From DS = 1
  - odesilatelem je AP/DS, nikoli uzel
- Address1:
  - RA, Receiver Address: fyzický příjemce
    - MAC adresa přijímajícího AP
- Address2:
  - TA (Transmitter Address): fyzický odesilatel
    - MAC adresa odesílajícího AP
- Address3:
  - Destination Address: logický příjemce
    - MAC adresa toho uzlu, kterému jsou data určena
- Address4:
  - SA (Sender Address): logický odesilatel
    - MAC adresa uzlu, od kterého data pochází

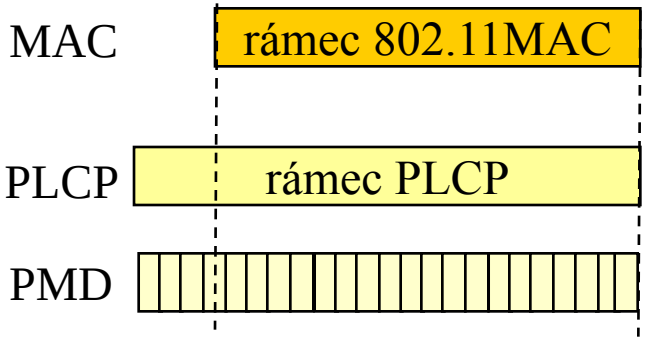
další údaje z MAC rámců



- v položce "Frame Control" je (mj.):
  - verze protokolu:
  - Retry:
    - příznak, zda jde o opakovaný přenos
  - Power Management:
    - 1: po odvysílání rámce přechází odesilatel do úsporného režimu (power-save mode)
    - 0: nepřechází
  - More Data:
    - že budou následovat ještě další data
      - příjemce může využít pro rozhodnutí, zda přejít/nepřejít do úsporného režimu
  - WEP (Wired Equivalent Privacy)
    - zda je/není použito zabezpečení pomocí WEP
- v MAC rámci jsou dále položky:
  - Duration/ID
    - doba, po kterou bude médium obsazeno
    - pro varianty přístupové metody s RTS/CTS, pro nastavení vektoru NAV
  - Sequence Control:
    - rámce jsou číslovány, kvůli potvrzování
  - Data:
    - přenášená data (max. 2312 bytů)
  - Checksum (CRC):
    - v rozsahu 32 bitů

rámce PLCP

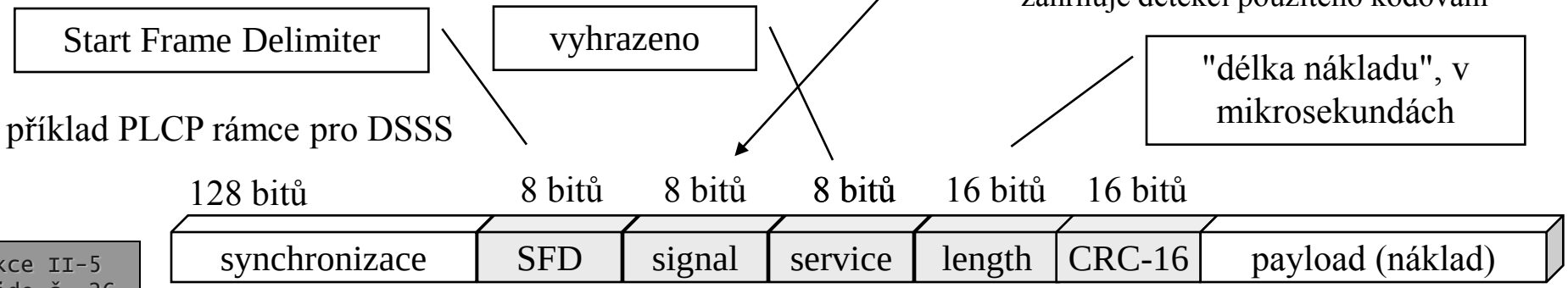




- fyzická vrstva se rozpadla na dvě podvrstvy:
  - PLCP (Physical Layer Convergence Protocol)
  - PMD (Physical media Dependent)
- podvrstva PLCP má vlastní rámce
  - zajišťují "podporu" příslušnému způsobu bezdrátového přenosu
  - rámce PLPC se liší pro FHSS, DSSS a DFIr

- rámce PLPC umožňují zajistit:
  - synchronizaci příjemce a odesilatele
    - a nastavit "technické parametry příjmu"
      - kompenzaci frekvenčního posunu
      - detekci vysílacího výkonu (pro rozpoznání obsazeného média)
      - …
  - zjistit (datovou) přenosovou rychlost
    - původně jen 1 Mbit/s a 2 Mbit/s
    - zahrnuje detekci použitého kódování

příklad PLCP rámce pro DSSS



úspora napájení - power management

- stanice jsou často napájeny z baterií
  - musí proto šetřit s energií
- princip šetření:
  - vysílat jen s takovým výkonem, jaký je skutečně nutný
    - otázka regulace výkonu
  - vypínat rádiovou část (transceiver), kdykoli je to jen možné
    - funkce power managementu umožňují zjistit, kdy to možné je a kdy nikoli
- možné stavy zařízení v režimu úspory napájení:
  - awake
    - zařízení je "vzhůru" a může přijímat i vysílat
  - sleep
    - zařízení "spí" a není schopné přijímat
- principy fungování úspory:
  - když stanice přijme rámec a mají pokračovat další rámce, zůstane "vzhůru"
    - dozví se to skrze příznak "More Data" v položce Frame Control MAC rámce
  - stanice, která "spí", se musí pravidelně probouzet a zjišťovat, zda nejsou pro ni připravena data
    - odesilatel (AP) musí dočasně bufferovat (uchovávat) data, určená spícím stanicím
- musí existovat mechanismy, které umožňují:
  - určit stanicím, kdy se mají "probudit"
    - **TSF, Timing Synchronization Function**
  - určit stanicím, zda jsou pro ně připravena nějaká data k přenosu (v bufferech odesilatele)
    - **TIM, Traffic Indication Map**
      - v podstatě vektor, udávající pro které stanice je co připraveno

TSF, TIM - beacon frames

- **TSF** (Timing Synchronization Function) počítá s pravidelným rozesíláním speciálních management rámců
  - "beacon frame"
    - angl. beacon = maják
- v sítích v režimu infrastruktury je rozesílá přístupový bod AP
  - v ad-hoc sítích je to složitější
    - snaží se vysílat všechny uzly, ale "vítězí" jen jeden
- beacon rámce jsou rozesílány pravidelně
  - interval není pevně stanoven
    - AP si jej může volit sám
    - obvykle každých 100 ms
  - ne vždy se vyslání beacon rámce podaří přesně včas
    - kvůli obsazenému médiu
    - pak se vyslání rámce může opozdit
      - čeká se dokud nebude médium volné
    - ale původně naplánované intervaly se nemění
      - další rámec se snaží odvysílat v původně určeném okamžiku
- beacon rámce by měly přijímat i "spící" stanice
  - měly by se pravidelně probouzet a přijímat

- co beacon rámce obsahují:
  - beacon interval:
    - údaj o tom, za jak dlouho je plánováno vyslání dalšího beacon rámce
      - podle tohoto údaje se spící stanice dozví, kdy by se měla zase vzbudit
  - timestamp (časové razítko):
    - slouží k tomu, aby si stanice udržovaly své hodiny v synchronizaci
  - **TIM** (Traffic Indication Map)
    - vektor s informacemi o tom, pro které stanice jsou v AP připravena v bufferu data
  - SSID (Service Set identifier)
    - fakticky jméno sítě, vysíláno v plaintextu
    - (všesměrové) vysílání tohoto údaje v rámci beacon rámce lze potlačit
  - podporované rychlosti přenosu
    - jakými rychlostmi dokáže AP přenášet data
  - "schopnosti"
    - indikace toho, co musí splňovat stanice, aby se mohly zapojit (asociovat) do sítě
    - např. povinnost používat WEP
  - "další parametry"
    - např. u FHSS podrobnosti o "plánu přeskoků"

roaming

- přechod mezi přístupovými body je v terminologii IEEE 802.11 obvykle označován jako **roaming**
  - ve smyslu přechodu mezi různými sítěmi (ESS)
- standard IEEE 802.11 však roaming nedefinuje
  - neříká, jak mají přístupové body a DS komunikovat a spolupracovat na vzájemném předávání si stanic
  - teprve novější doplněk 802.11f definuje podporu roamingu
    - skrze IAPP, Inter-Access Point Protocol
- roaming si ale mohou zajistit stanice samy
  - i bez specifické podpory roamingu ze strany AP

v praxi je kolem roamingu mnoho proprietárních řešení, nekompatibilit a dalších problémů

- postup roamingu (z pohledu stanice):
  - stanice usoudí, že komunikace se stávající AP není dostatečně kvalitní (vůbec možná), a začne hledat jiný AP
  - hledání nového AP může být:
    - pasivní (passive scanning)
      - stanice pouze přijímá beacon rámce, a na jejich základě se rozhoduje
    - aktivní (active scanning):
      - stanice sama vysílá rámce "probe" na všech kanálech
      - čeká na "probe response", ze které získá potřebné údaje o novém AP
      - rámec "probe response" je obdobný beacon rámci, jen neobsahuje časové razítko
  - stanice vybírá z dostupných AP nejvhodnější
    - na základě síly signálu
  - stanice posílá zvolenému AP žádost o přidružení
    - association request
  - pokud AP přijme žádost, vrátí kladnou odpověď
    - association response
  - AP, který žádost akceptoval, předá informaci o nové stanici do svého DS
    - aby tato byla dostupná i z ostatních BSS