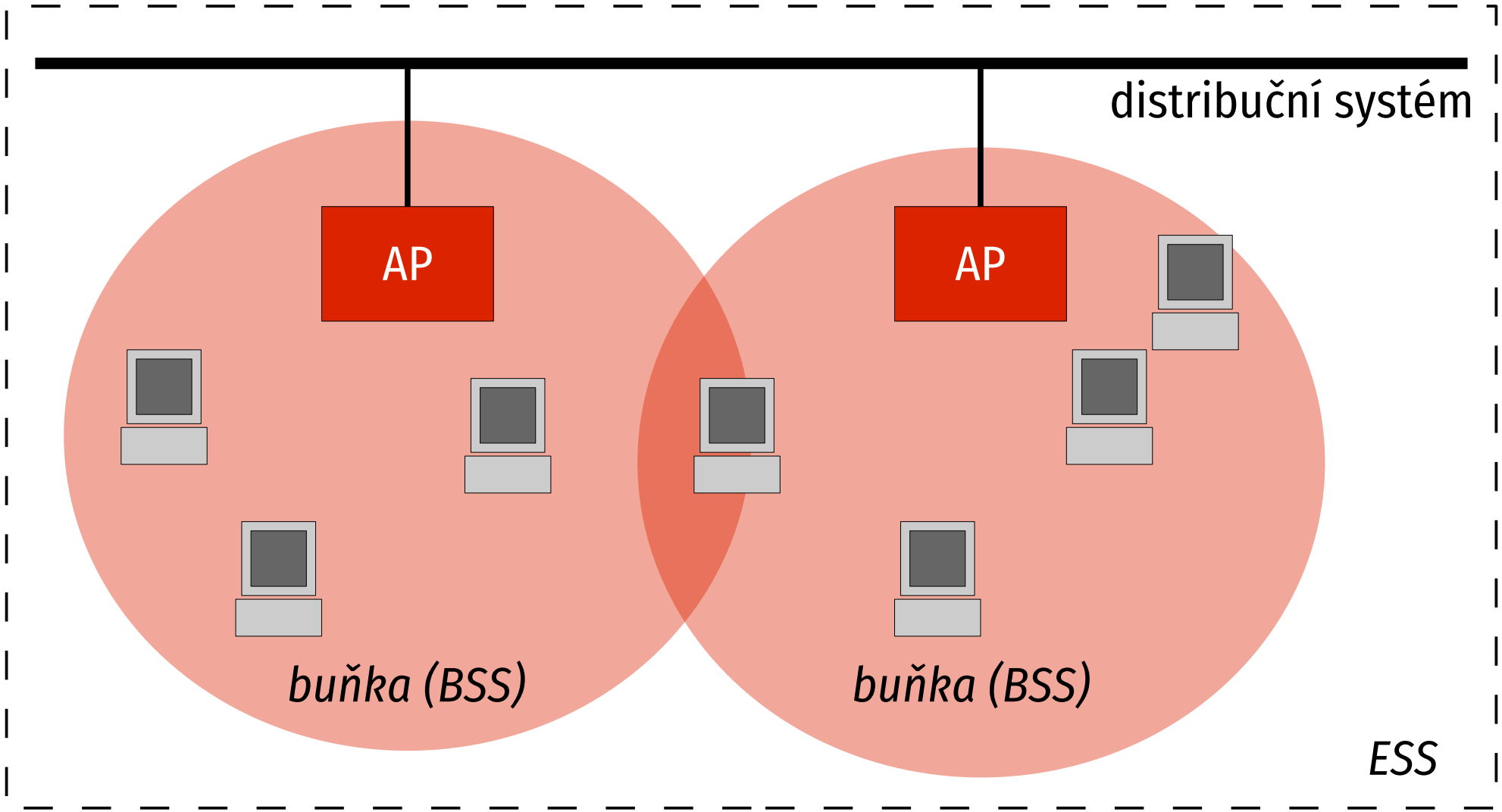
Bezdrátové sítě
IEEE 802.11

Vlastnosti IEEE 802.11

- velmi rychle se rozvíjejí
- **přednosti:**
  - pokrytí plochy, podpora mobility
  - umožňují propojení budov bez optických vláken
- **zápory:**
  - pomalejší
  - větší chybovost

Architektura sítě IEEE 802.11



Buňka (BSS)

- **Basic Service Set**
- skupina stanic komunikujících navzájem
- **nezávislá (ad hoc)**
  - stanice komunikují přímo, problém se vzájemnou slyšitelností
- **infrastrukturní**
  - řízena základnovou stanicí (Access Point, AP)
  - veškerý provoz prochází AP
  - umožňuje lepší služby

Činnost AP

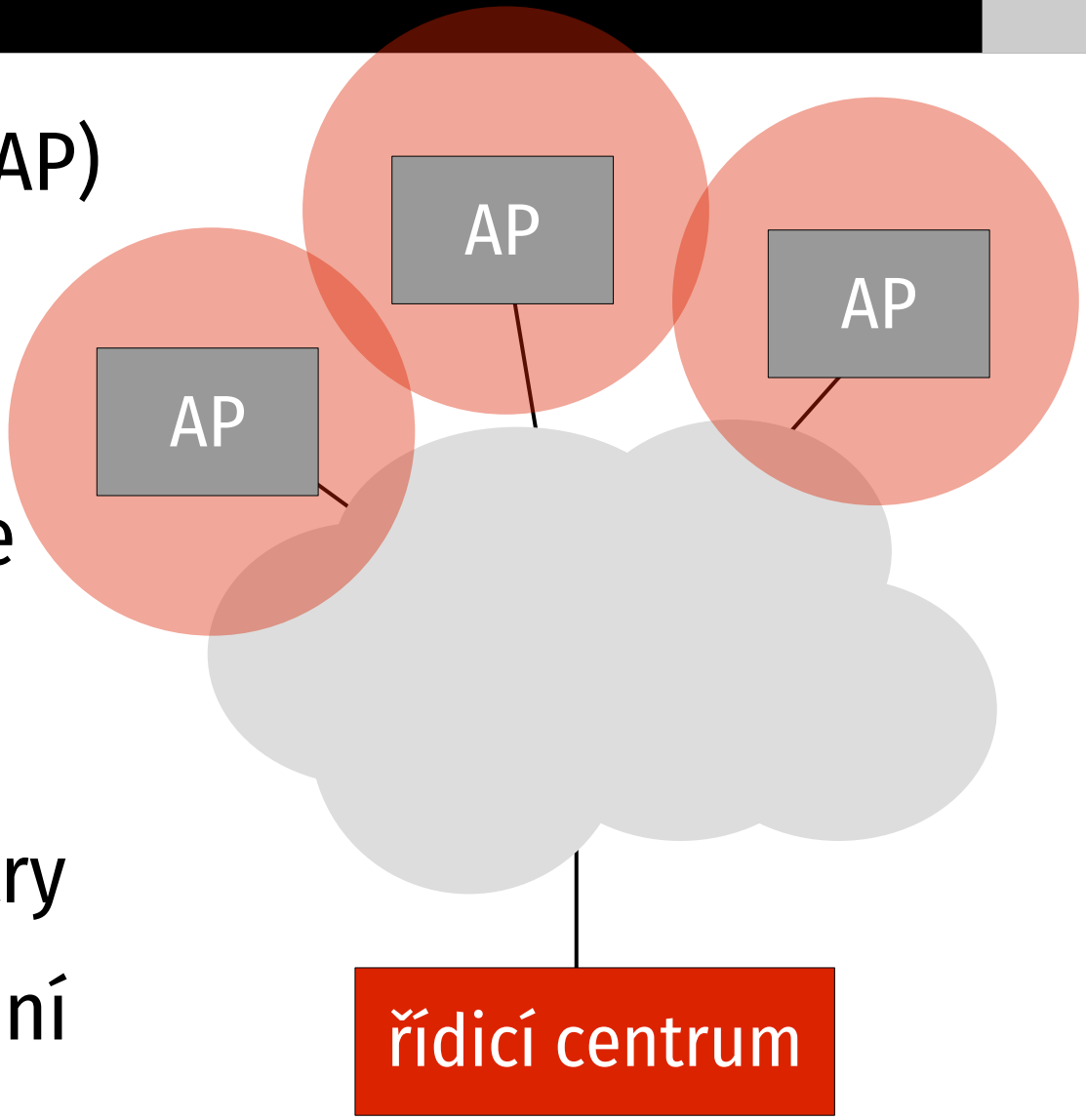
- řídí buňku
- veškeré přenosy procházejí přes AP
- ukládá rámce pro spící stanice (úspora energie)
- pravidelně vysílá Beacon Frame
  - synchronizace času
  - vyzývá nové stanice ke vstupu do buňky
  - systémové parametry
  - pravidelně 10 až 100× za sekundu

ESS

- **Extended Service Set**
- skupina spolupracujících buněk
- propojeny distribučním systémem (lokální sítí)
  - **portál** – zařízení propojující IEEE 802.11 síť s jinou sítí (typicky Ethernetem), obvykle integrován v AP
- vyžaduje komunikaci mezi AP
  - Inter-Access Point Protocol (IAPP)
  - standard IEEE 802.11F, přijat 2003, stažen 2006
  - firemní protokoly

Centrální řízení

- pro velké sítě (desítky AP)
- funkce AP omezeny na provoz buňky
- vše složitější rozhoduje centrum
- umožňuje nastavovat a koordinovat parametry
- obvykle webové rozhraní
- firemní řešení



Kuriozita

- Znáte ji?

Hedy Lamarr (1912–2000)

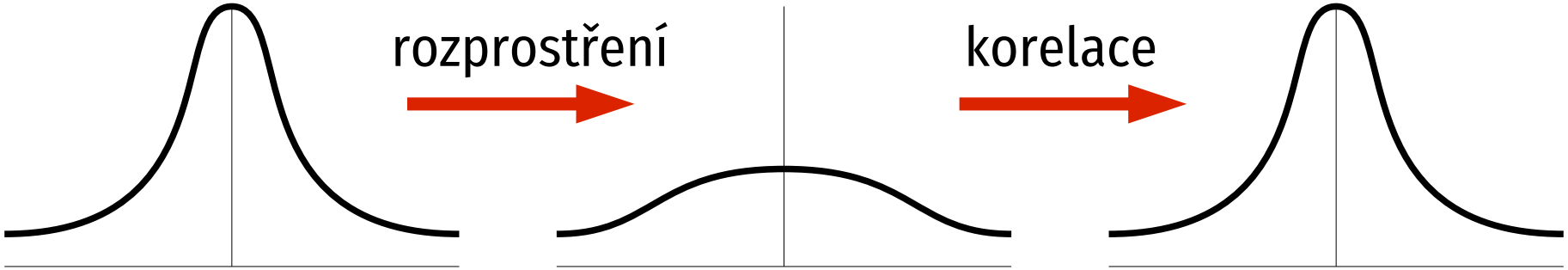
- rakouská herečka, první nahá scéna v historii filmu (Machatého Extase, 1932)
- vynalezla přeskakování frekvencí (US patent)
  - rychlé střídání frekvencí
  - ochrana před rušením
  - použito v IEEE 802.11 (v první generaci)

Fyzická vrstva

- **infračervené světlo**
  - definováno ve standardu, nikdy se nevyrábělo
  - problém: vyžaduje přímou viditelnost
- **mikrovlny**
  - bezlicenční pásma 2,4 a 5 GHz
  - nižší frekvence má lepší prostupnost, ale menší šířku pásma a více konfliktů
  - různé metody vysílání

802.11b

- první masově rozšířená varianta
- v pásmu 2,4 GHz
- Direct Sequence Spread-Spectrum (DSSS) – menší amplituda, ale širší pásmo
- max. 11 Mb/s



Problémy 802.11b

- reálná max. rychlost sotva poloviční (velká režie)
- pásmo 2,4 GHz je přetíženo, problémy s rušením
- v dostupném pásmu je 11 kanálů (13 v Evropě), ale měly by být alespoň o 5 od sebe, aby se nerušily – reálně použitelné jsou kanály 1, 6 a 11 (případně 1, 5, 9, 13)

802.11a

- starší než 802.11b, ale rozšířil se později
- pásmo 5 GHz (podstatně širší, ale vyšší útlum)
- Orthogonal Frequency Division Multiplexing (OFDM) – rozkládá signál do desítek nezávislých frekvencí; tento princip používá i ADSL
- různé modulace + samoopravné kódy
- 8 rychlostí, max. 54 Mb/s

802.11g

- snaha o vyšší rychlost při zachování zpětné kompatibility s 802.11b
- pásmo 2,4 GHz
- Orthogonal Frequency Division Multiplexing
- rychlosti až 54 Mb/s
- podporuje i režimy 802.11b a režim ochrany (řídicí informace se vysílají tak, aby je zachytila i 802.11b zařízení) – pomalejší

802.11h

- v Evropě kladeny technické požadavky na zařízení v bezlicenčním pásmu 5 GHz
  - DFS – dynamická volba kmitočtu
  - TPC – automatická regulace výkonu
- 802.11a je nesplňuje – lze nasadit jen uvnitř budov
- 802.11h doplňuje potřebné vlastnosti, v podstatě evropská verze 802.11a
- novější (2004), málo rozšířená

802.11n

- přijato na podzim 2009
- cíl: čistá přenosová rychlost alespoň 100 Mb/s
- pásmo 2,4 i 5 GHz
- zařízení jsou běžně dostupná na trhu
  - cena se příliš neliší od a/b/g

802.11n – vyšší výkon

- Multiple-Input Multiple-Output (MIMO) – více antén pro vysílání a příjem (min. 2×2)
- minimalizace režijních přenosů
  - agregace rámců
  - blokové potvrzování
- 3 režimy činnosti
  - legacy – zpětně kompatibilní (a/b/g)
  - mixed (a/b/g/n)
  - greenfield (pouze n)

Další vývoj (1)

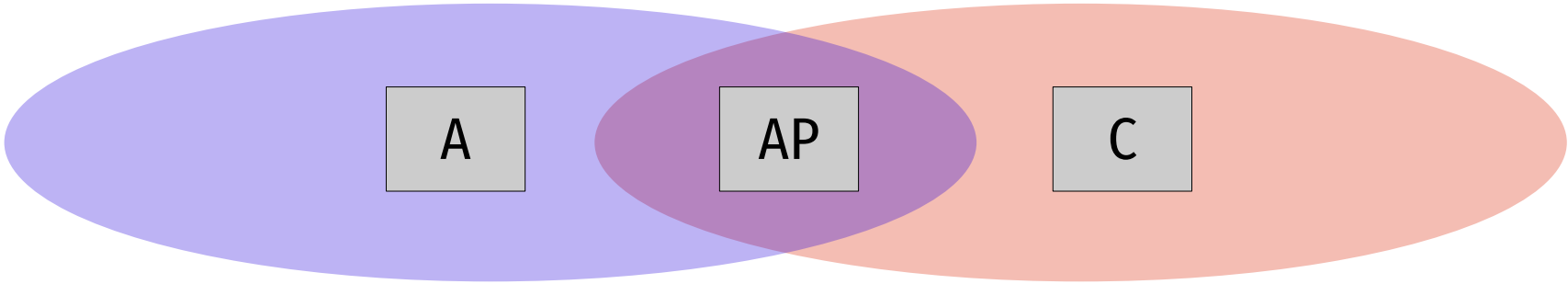
- **802.11ac**
  - přijato v lednu 2014
  - MIMO (až 8 antén)
  - víceuživatelské MIMO – stanice na různých kanálech
  - rychlost linky až 867 Mb/s, celková několik Gb/s
- **802.11ad (WiGig)**
  - přijato 2012
  - tři frekvenční pásma: 2,4 GHz, 5 GHz a 60 GHz
  - až 7 Gb/s

Další vývoj (2)

- **Wi-Fi 6 aneb 802.11ax**
  - přijato 2021, navazuje na 802.11ac
  - nový systém označování
  - pásma 2,4 a 5 GHz, verze 6E navíc 6 GHz
  - MIMO (až 8x8)
  - víceuživatelské MIMO – stanice na různých kanálech
  - celková rychlost až 9,6 Gb/s

Mikrovlnné problémy

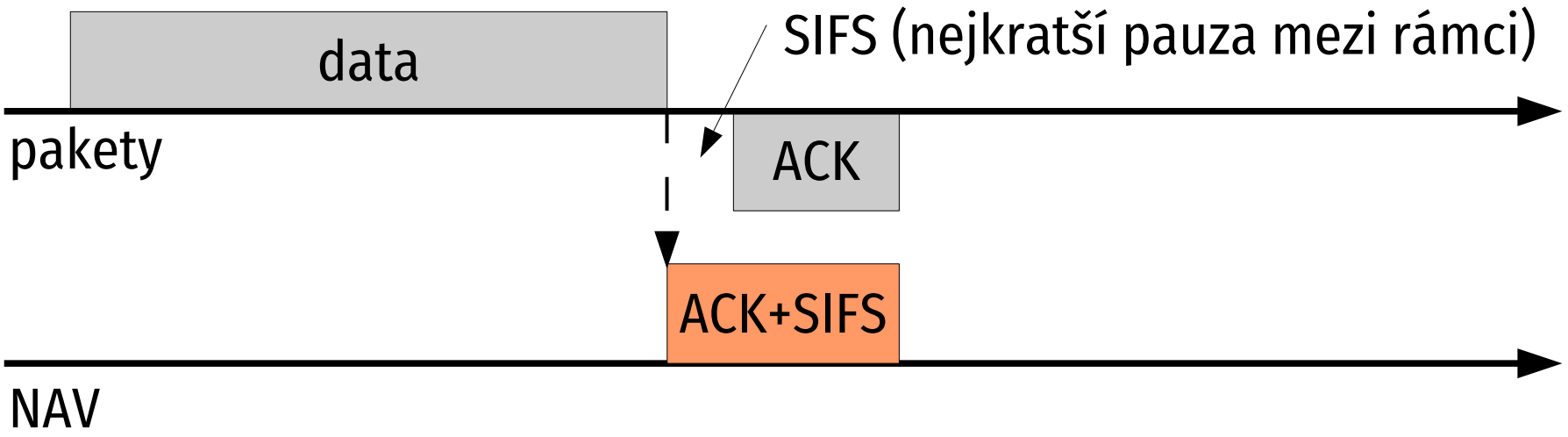
- **nekvalitní médium**
  - rušení, útlum (vzdálenost, překážky)
  - důsledek: **potvrzování**, přenos rámce a jeho potvrzení tvoří atomickou operaci
- **skrytý uzel**
  - A a C se přímo neslyší, jejich signály se ale u AP ruší



Virtuální naslouchání

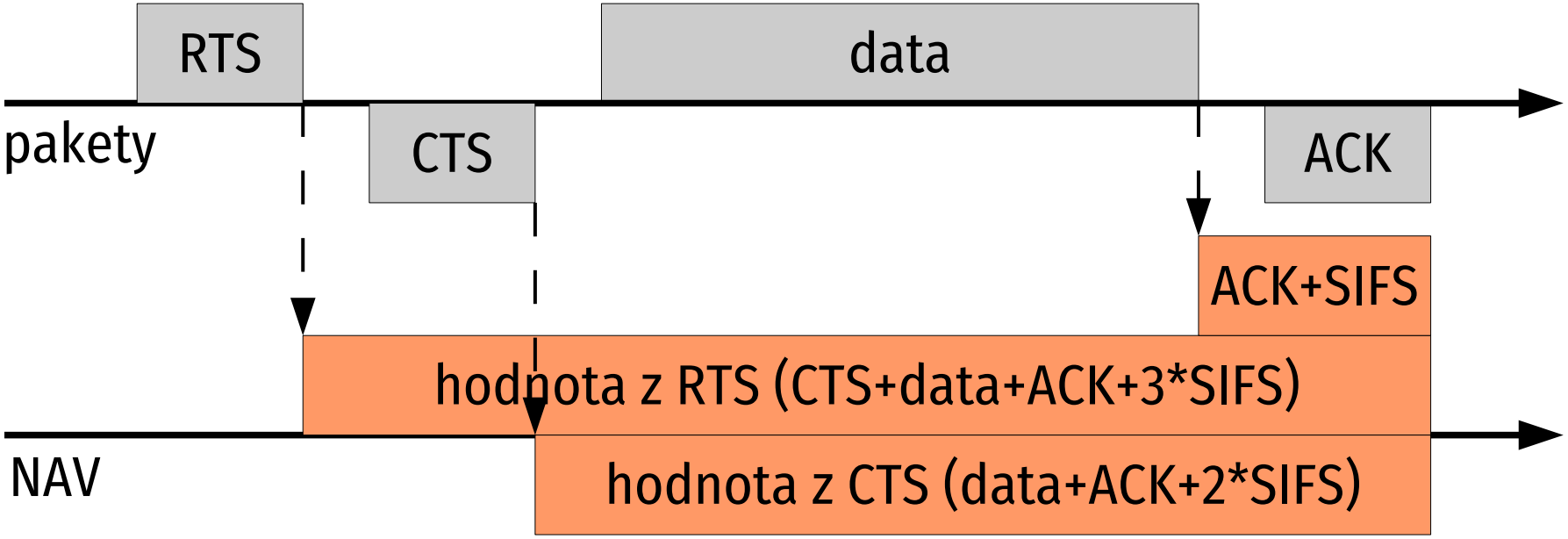
- řeší problém skrytého uzlu
- každá stanice si vede **Network Allocation Vector (NAV)** – čas, po který je médium rezervováno
- je-li NAV nenulový, médium je považováno za obsazené, i když žádný signál nepřichází
- hodnota NAV se přebírá z přenášených rámců

Základní výměna



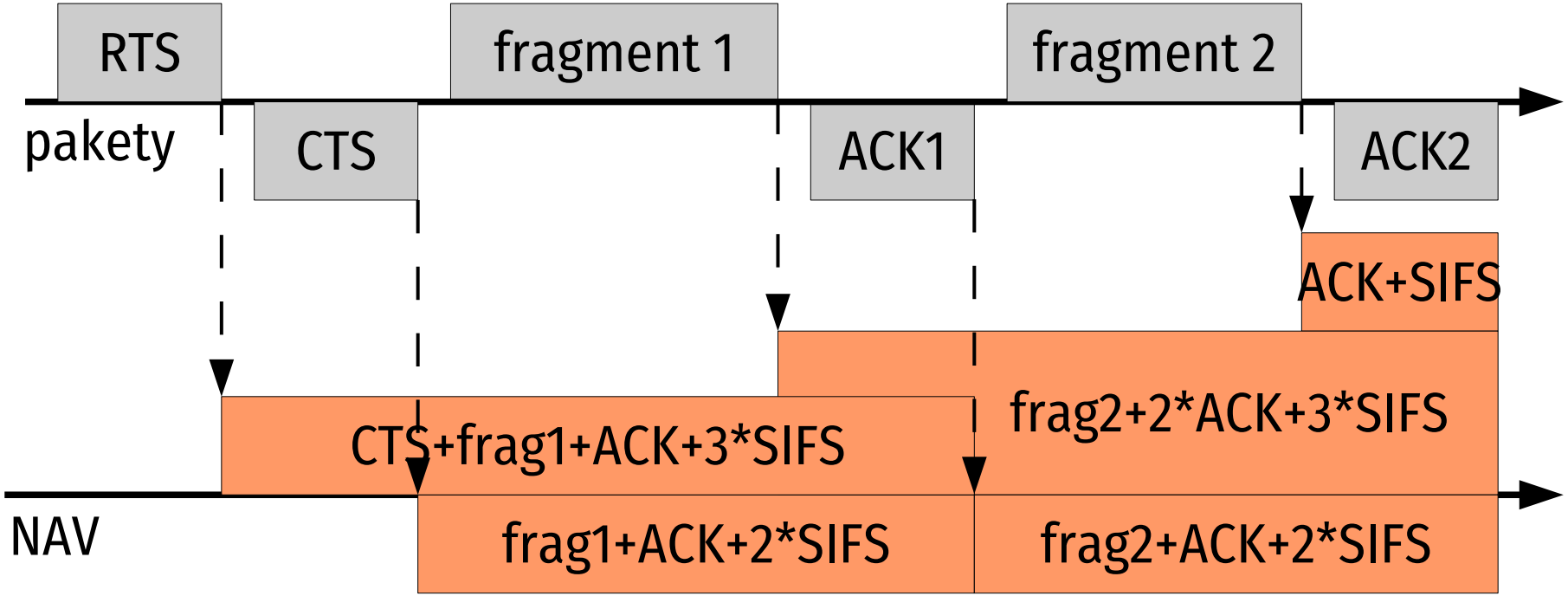
- pro krátké rámce
- vysílající pošle rovnou data, příjemce potvrdí
- NAV si odvozuje každý sám ze známých délek

RTS/CTS výměna



- vysílající avizuje přenos (Request to Send), příjemce potvrdí připravenost (Clear to Send)
- ostatní si nastaví NAV z hodnoty RTS či CTS

Fragmentace



- dlouhé rámce lépe rozložit na několik menších (zvyšuje pravděpodobnost úspěšného doručení)
- NAV se průběžně aktualizuje

Přístup k médiu

- **Distributed Coordination Function (DCF)**
  - bez centrálního řízení, stanice soutěží o médium
  - algoritmus CSMA/CA
- **Point Coordination Function (PCF)**
  - přístupový bod řídí veškeré přenosy
  - málo implementováno
  - kombinuje se s DCF

Intervaly v IEEE 802.11

- **SIFS** – Short Interframe Space
  - mezi rámci tvořícími atomickou operaci
- **PIFS** – PCF Interframe Space
  - mezi rámci při centrálním řízení
- **DIFS** – DCF Interframe Space
  - mezi rámci při distribuovaném řízení
- **EIFS** – Extended Interframe Space
  - při přenosové chybě

CSMA/CA

- **Carrier Sense Multiple Access with Collision Avoidance**
  1. je-li médium volné po dobu DIFS, začne vysílat
     pokud protějšek nepotvrdí příjem, zahájí exp. čekání
  2. je-li obsazeno, počká na uvolnění a zahájí exp. čekání
  3. exponenciální čekání: po uplynutí DIFS začíná soutěžní okno – rozděleno na sloty; stanice náhodně vybere slot a pokud nikdo nezačne dříve, zahájí vysílání (jinak zpět 2); při neúspěchu zdvojnásobí počet slotů
  4. omezený počet pokusů

Formát rámce

2	2	6	6	6	2	6	0–2312	4
řízení	trvání	adresa 1	adresa 2	adresa 3	poř.	adresa 4	data	CRC

- **řízení:** příznaky určující typ rámce (datový, řídicí, správní) a další parametry
- **trvání:** očekávaná doba přenosu následujícího rámce (nastavení NAV)
- **adresy:** odesilatel, příjemce a až dva AP (význam závisí na typu rámce)
- **pořadí:** umožňuje číslovat rámce
- **CRC:** kontrolní součet

Bezpečnost

- dva okruhy problémů:
  - využití sítě neoprávněnými stanicemi
  - odposlech dat
- vstup do buňky:
  - autentizace – ověření, zda smí být vpuštěna
  - asociace – technické začlenění do buňky

Autentizace

- **volný přístup**
  - implicitní nastavení nových AP
- **podle MAC adres**
  - obtížně se udržuje, snadno se falšuje
- **šifrování + heslo**
  - nejčastější, dostatečně bezpečné a jednoduché
- **IEEE 802.1X**
  - centrálně řízené, pro větší počty uživatelů

IEEE 802.1X

- obecné pro lokální sítě (i pro Ethernet)
- **autentizuje uživatele, nikoli hardware**
  umožňuje vzájemnou autentizaci obou stran
- zpočátku provoz počítače blokován, umožněny jen pakety 802.1X, po úspěšné autentizaci se otevře
- na počítači nutný klient, tzv. suplikant; AP ověřuje proti autentizačnímu serveru protokolem RADIUS
- vychází z Extensible Authentication Protocol (EAP)

WEP

- **Wired Equivalent Privacy**
- součást původního 802.11, šifra RC4
- chrání data během bezdrátové přepravy (nikoli v distribučním systému)
  - utajení (aby data nemohl číst neoprávněný uživatel)
  - integrita (aby nemohla být změněna)
  - autentičnost (ověření pravosti zdroje)
- slabiny: nedostatky algoritmu, společné heslo
- **považován za nedostatečný**

IEEE 802.11i

- vylepšené zabezpečení, dva různé protokoly:
- **Temporal Integrity Key Protocol (TKIP)**
  - též WEP2, WPA
  - využívá čipy pro WEP, ale s individuálními a dočasnými klíči (každý rámec jiný) a delšími inicializačními vektory
- **Counter Mode with CBC-MAC Protocol (CCMP)**
  - silnější šifrovací algoritmy, vyžaduje jiný hardware
  - vychází z šifry Advanced Encryption Standard (AES)

Wi-Fi Alliance

- sdružení výrobců HW
- založeno s cílem zlepšit interoperabilitu jednotlivých výrobků
- **certifikát Wi-Fi** zaručuje splnění daných testů
- vydává vlastní specifikace
  - např. dlouhý vývoj 802.11i vedl k vydání **Wi-Fi Protected Access (WPA)**, což je TKIP z návrhu 802.11i

vytvořeno s podporou
projektu ESF