


# Lekce 7: Řízení přístupu

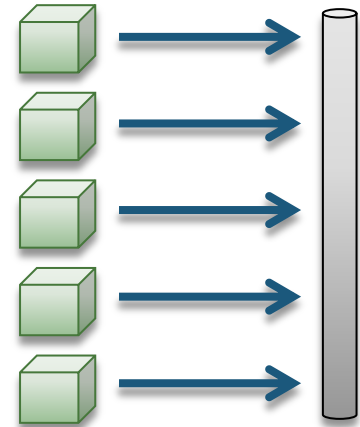
*Jiří Peterka*

# proč řízení přístupu?

- jde o situace, kdy máme:

- 1 společné (sdílené) přenosové médium
- N uzlů (či terminálů/koncových zařízení)
  - které se (typicky) nenachází na stejném místě
  - které chtějí využít společné přenosové médium pro vysílání
    - pro odeslání (přenos) svých dat

tzv. vícenásobný přístup  
(  multiple access)



- potřebujeme:

- dosáhnout toho, aby N uzlů dokázalo korektně „přistupovat“ k 1 společnému (sdílenému) přenosovému médiu
  - a nedocházelo přitom k nežádoucím situacím
    - ztrátě/poškození dat, konfliktům, kolizím, deadlock-ům atd.



- řešením je

- použít vhodné **řízení přístupu** ke sdílenému médiu (**media access control, MAC**), realizované pomocí **přístupových metod** (**media access control methods**)

- jaké podoby řízení vícenásobného přístupu můžeme chtít dosáhnout?

- a) toho, aby jednotlivé uzly mohly používat sdílené přenosové médium současně
  - přitom se budou nějak dělit o jeho celkovou kapacitu
- b) toho, aby jednotlivé uzly používaly sdílené přenosové médium střídavě
  - aby uzel, který získá přístup k médiu, jej měl (na omezenou dobu) výlučně pro sebe

# analogie: shromáždění lidí

– s potřebou řízení přístupu se lze setkat i jinde, mimo oblast počítačových sítí

- **například:**

– shromáždění více lidí, kteří chtějí společně diskutovat

- sdíleným médiem je zde „éter“ (či „držení slova“, resp. přístup k mikrofonu)
- nežádoucí situací je to, když mluví více lidí současně
  - není jim rozumět

– řešením je řízení diskuse, pomocí pravidel:

- když chceš mluvit, zvedni ruku
- nemluv, dokud nejsi vyzván
- neskákej jinému do řeči
- když dostaneš slovo, mluv jen po omezenou dobu
  - pak skonči

• jde o centralizovanou metodu řízení přístupu

- nějaká centrální autorita řídí diskusi
  - může přitom postupovat podle různých pravidel

• odpovídá variantě b)

- jednotliví diskutující se střídají



• může to ale fungovat i jinak („dav“):

- soutěž: snaží se vzájemně překřičet, jeden zvítězí, ostatní zmlknou
  - bez centrální autority
  - nemusí vždy vést k výsledku

# kde je řízení přístupu zapotřebí?

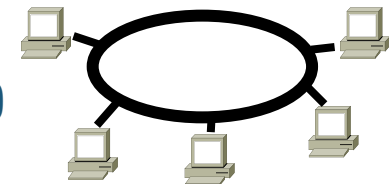
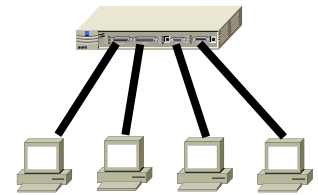
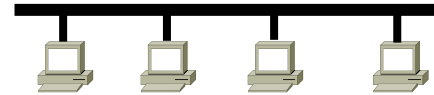
- **obecně:**

- všude tam, kde je používáno nějaké sdílené přenosové médium

- **v praxi:**

- u lokálních sítí (sítí LAN)

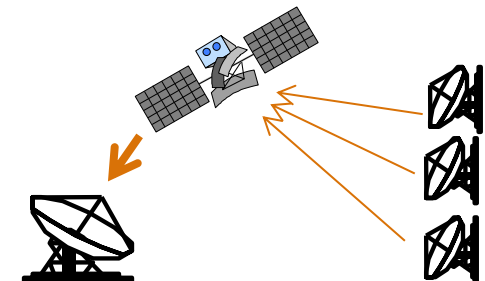
- s „drátovým“ přenosovým médiem: koax, kroucená dvoulinka, optika
  - ve všech topologiích (sběrníková, kruhová, do hvězdy/do stromu, ....)
    - své přístupové metody má mj. Ethernet, Token Ring, 100VG Any-LAN, ....
- s „bezdrátovým“ přenosovým médiem („éter“)
  - své přístupové metody mají sítě Wi-Fi, sítě Bluetooth, ....



- **ale také:**

- u „rozlehlejších“ sítí: MAN i WAN

- s „bezdrátovým“ přenosovým médiem
  - obecně: bezdrátové sítě P-MP (Point to MultiPoint), nikoli sítě P-P (Point to Point)
  - například:
    - mobilní sítě
    - sítě WiMAX
    - obousměrné satelitní sítě (pro zpětný směr)
- někdy i s „drátovým“ přenosovým médiem
  - kabelové HFC sítě (DOCSIS)
    - pro zpětný kanál, pokud jsou používány pro obousměrný přenos



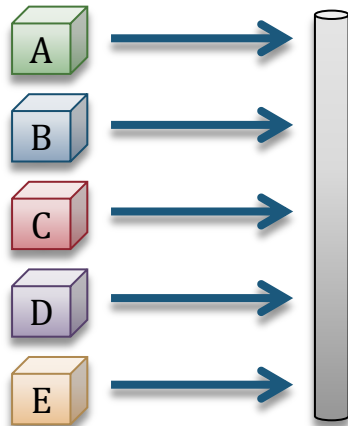
# řízení přístupu vs. multiplexování

- řízení přístupu ke sdílenému médiu se liší od jeho multiplexování

- ne nutně ve způsobu fungování, ale spíše v účelu a důvodu svého nasazení
  - v obou případech dochází k určitému rozdělení přenosového média

- řízení přístupu

- je  $N$  uzlů
  - které se nachází různě „od sebe“
    - nikoli na stejném místě
      - ale všechny v dosahu sdíleného média
  - každý uzel má zájem získat přístup („přistoupit“) k přenosovému médiu a vyžít ho pro přenos (odeslání) svých dat
    - zájem může být trvalý či různě „nárazový“
  - každý uzel generuje jen 1 datový tok



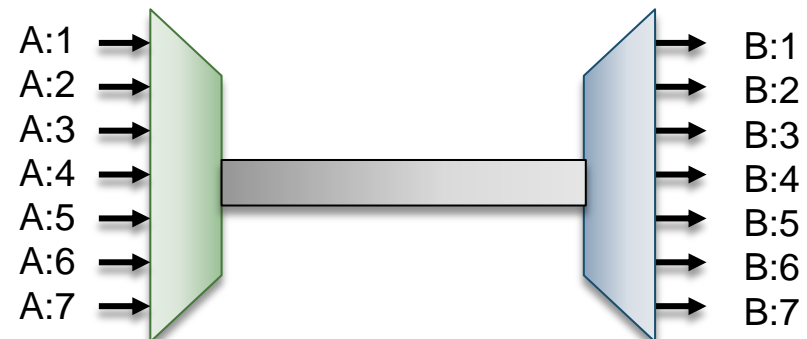
- multiplexování

- jen 2 uzly
  - médium propojuje pouze tyto 2 uzly



- $N$  je různých datových toků

- které jsou nezávislé na sobě
  - nesmí se smíchat
- všechny tyto datové toky jsou dostupné v 1 místě
  - ve „vstupním“ uzlu



# dvě varianty řízení přístupu

- řízení přístupu ke sdílenému médiu může mít 2 základní podoby

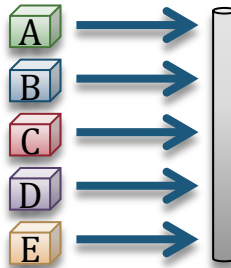
- jejich rozlišení a označení ale není dosud „příliš zažité“

- získání výlučného přístupu**

- v době, kdy sdílené médium používá („přistupuje k němu“) jeden uzel, by jej neměly používat jiné uzly

- cílem je:**

- přidělení sdíleného média do výlučného „držení“ (použití)
  - na omezenou dobu
    - pro přenos jednoho linkového rámce
    - po jejím uplynutí může být médium přiděleno jinému uzlu atd.



- získání nevýlučného přístupu**

- v době, kdy sdílené médium používá („přistupuje k němu“) jeden uzel, jej mohou používat i jiné uzly

- ale musí být možné odlišit od sebe vysílání (přenosy) jednotlivých uzlů

- cílem je:**

- oddělit od sebe jednotlivé přenosy
  - tak aby si „nepřekážely“
    - navzájem se neovlivňovaly



- příklady z praxe:**

- přístupová metoda CSMA/CD v Ethernetu
- přístupová metoda CSMA/CA u Wi-Fi
- přístupová metoda Token Passing u sítí Token Ring, Token Bus, u optických sítí


- příklady z praxe:**

- přístupové metody CDMA a TDMA
  - používané např. mobilních sítích

# řízení (nevýlučného) přístupu

- **používaná řešení jsou „podobná“ technikám multiplexu**
  - fungují na stejném principu jako multiplex, ale s jiným účelem/smyslem
  - příklad:
    - FDM (Frequency Division Multiplexing) je varianta/technika multiplexu
    - FDMA (Frequency Division Multiple Access) je přístupová metoda pro řízení přístupu
      - jde o „řízení přístupu na principu frekvenčního dělení“ (frekvenčního multiplexu)

technika multiplexu		přístupová metoda
frekvenční dělení	FDM (Frequency Division Multiplexing)	FDMA (Frequency Division Multiple Access)
časové dělení	TDM (Time Division Multiplexing)	TDMA (Time Division Multiple Access)
kódové dělení	CDM (Code Division Multiplexing)	CDMA (Code Division Multiple Access)

- techniky obdobné vlnového multiplexu (WDM) a statistického multiplexu (STDM) se pro řízení přístupu (moc) nepoužívají
- **používaná řešení mají charakter přepojování okruhů ( circuit switching)**
  - jsou realizovány na úrovni fyzické vrstvy
    - stejně jako techniky multiplexu
  - umožňují i přenos bitstreamu (nestrukturovaného proudu bitů/bytů)
    - ale umožňují i přenos dat, členěných na bloky (např. rámce)
  - mohou garantovat (a obvykle garantují) určitou přenosovou kapacitu

# příklad: FDMA

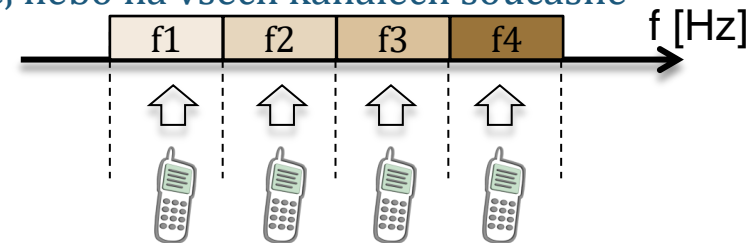
- **používá se zejména v bezdrátových sítích**
  - **princip FDMA:** každý uzel vysílá na jiném frekvenčním kanále
    - díky tomu více uzlů využívají jedno společné přenosové médium („éter“), ale jejich vysílání se „nepromíchá“
    - příjemce může přijímat také jen na určitém kanále, nebo na všech kanálech současně

- **problém:**

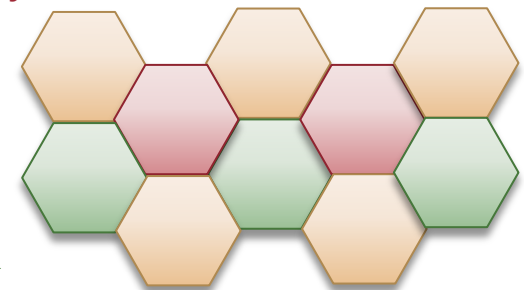
- co když je více uzlů na 1 frekvenční kanál?

- **možná řešení:**

- v rámci každého kanálu zavést nějakou formu výlučného řízení přístupu



- příklad: síť Wi-Fi (IEEE 802.11) pracují v pásmu 2,4 GHz s kanály o šířce 22 MHz
  - tj. jednotlivé kanály jsou odděleny od sebe pomocí FDMA
  - v rámci jednotlivého kanálu používají tyto sítě přístupovou metodu CDMA/CA
    - pro zajištění výlučného přístupu
      - aby se uzly dohodly, kdo z nich kdy využije dostupný frekvenční kanál
- příklad: mobilní síť 1. generace (v ČR např. NMT) pracují s kanály o šířce 25 kHz
  - platí: 1 hovor = 1 frekvenční kanál
    - ale jen u této 1. generace (analogových) mobilních sítí
  - používají buňkový princip
    - pokryté území je rozděleno na buňky (sektory), stejné skupiny frekvenčních kanálů se mohou opakovat v nesousedních buňkách





# příklad: TDMA a CDMA

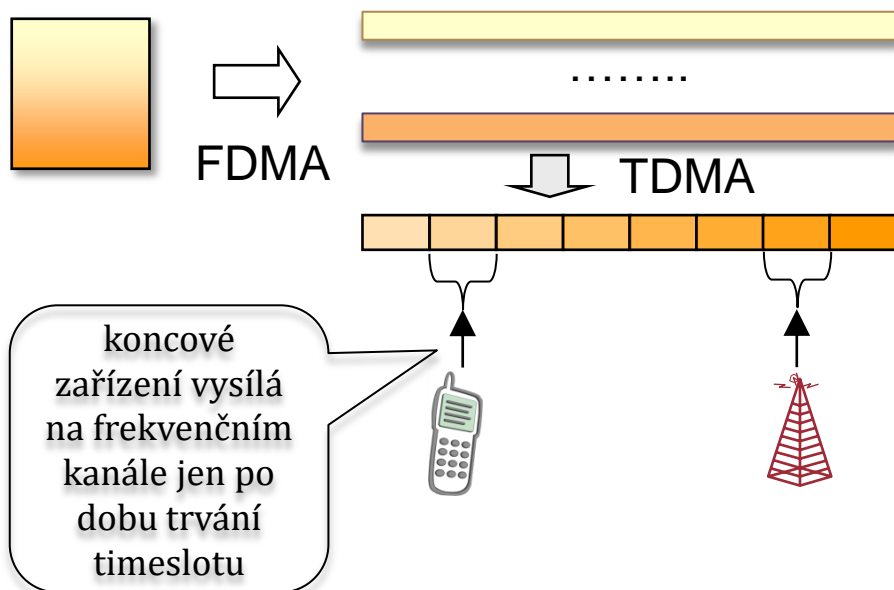
- v mobilních sítích GSM se kombinuje FDMA a TDMA**

- nejprve se „aplikuje“ FDMA

- čímž vzniknou frekvenční kanály o šířce 200 kHz

- pak se „aplikuje“ TDMA

- každý frekvenční kanál (200 kHz) se rozdělí na 8 timeslotů
  - každý hlasový hovor pak používá 1 timeslot



- v mobilních sítích CDMA2000 se kombinuje FDMA a CDMA**

- nejprve se „aplikuje“ FDMA

- vzniknou kanály o šířce 1,2288 MHz

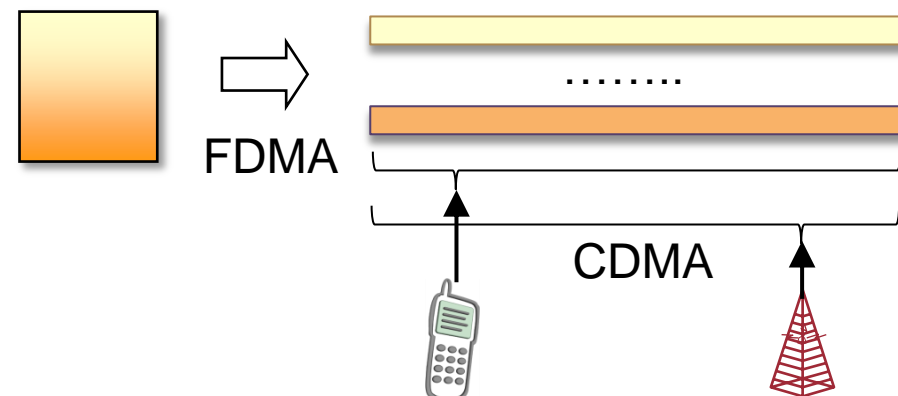
- pak se „aplikuje“ CDMA

- jeden kanál (1,228 MHz) může přenášet až 61 terminálů (hovorů) současně
  - všichni vysílají na stejném kanále, ale jejich vysílání využívají ortogonální chipping kódy
    - a lze je od sebe zase oddělit

- v sítích 3G/UMTS (W-CDMA)**

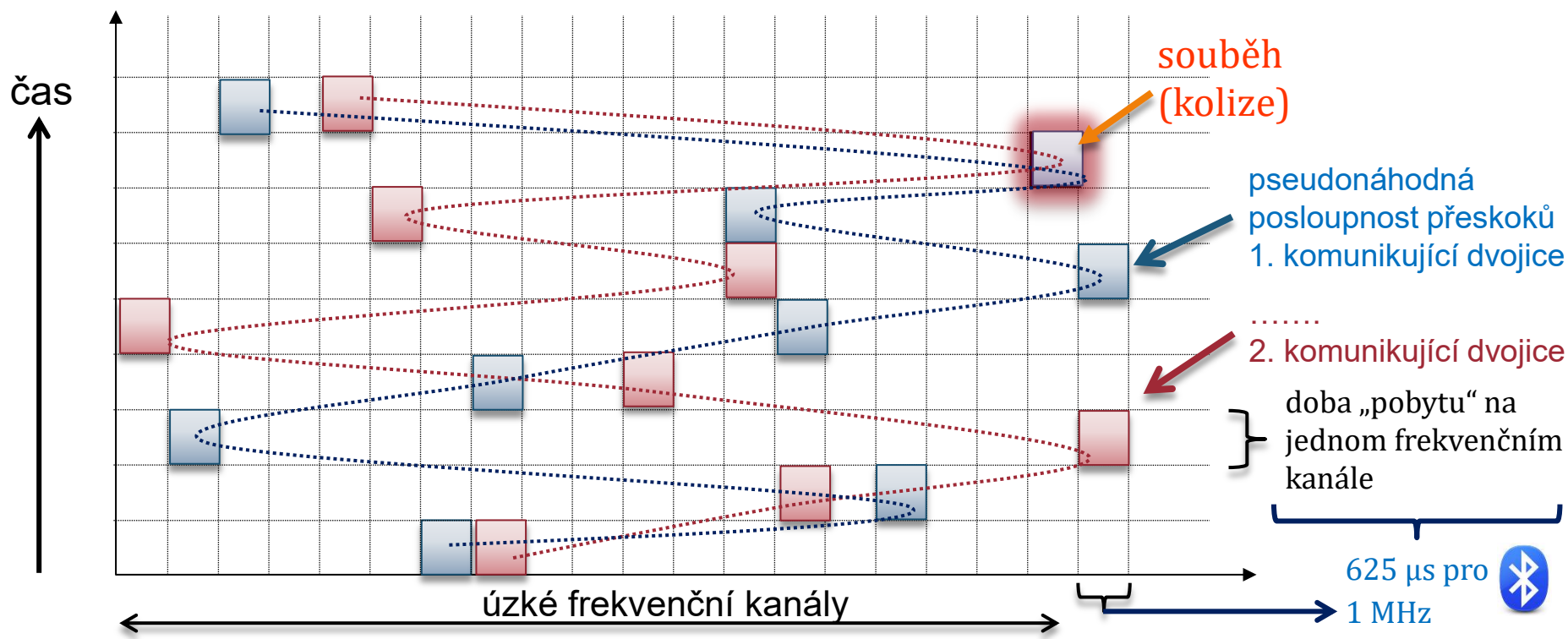
- kanály mají šířku 5 MHz

- až 350 hovorů současně



# příklad: Frequency Hopping


- metodou řízení (nevýlučného) přístupu je i tzv. Frequency Hopping
  - jde o velmi rychlé přeskakování mezi úzkými frekvenčními kanály
    - používá se např. v technologii Bluetooth, kde se přeskakuje každých  $625 \mu\text{s}$  ( $1600\times$  za 1 sec.)
  - předskakuje se podle pseudonáhodné posloupnosti
    - která je jiná pro každou komunikující dvojici !!!
  - pravděpodobnost souběhu (kolize: více přenosů na stejném kanále ve stejném časovém intervalu) je velmi malá
    - a může být řešena opravnými mechanismy na vyšších vrstvách (např. opakovaným přenosem)




# výlučný vs. nevýlučný přístup

## • připomenutí:

### – metody řízení nevýlučného přístupu

-  channel (based) access methods
- fungují na fyzické vrstvě
- výsledek je obdobný jako u přepojování okruhů
  - přístup ke sdílenému médiu je trvalý
    - nevýlučný ....
  - k dispozici je jen část kapacity sdíleného média
  - data lze přenášet kdykoli (trvale)
    - neměly by existovat časové intervaly, kdy možnost přenosu (odesílání) není dostupná
      - časový multiplex se „nepočítá“
  - přenášená data nemusí být nijak členěna
    - může jít o posloupnost bitů/bytů

### – metody řízení výlučného přístupu

-  packet based access methods
- nemohou fungovat na fyzické vrstvě
- výsledek je obdobný jako u přepojování paketů
  - přístup ke sdílenému médiu je „jen někdy“
    - ale zato výlučný: ve stejné době nemá nikdo jiný přístup k médiu
  - přenosové médium je přidělováno celé
    - k dispozici je celá přenosová kapacita média
    - data lze přenášet „jen někdy“
      - pouze v době, kdy má odesílající uzel přístup ke sdílenému médiu
  - přenášená data musí být členěna na bloky
    - typicky: na linkové rámce
    - protože přenosové médium se obvykle přiděluje na dobu přenosu jednoho bloku
    - jednoho linkového rámce
    - a pak se zase „vrací“ a může být přiděleno (do výlučného držení) zase jinému uzlu

i když i zde jde také  
o přístupové metody

o přístupových  
metodách se hovoří  
spíše zde

# kam patří řízení (výlučného) přístupu?

## • otázka:

- na které vrstvě mají být implementovány mechanismy pro řízení výlučného přístupu ke sdílenému médiu?

## • odpověď:

- musí to být nad fyzickou vrstvou

- protože k fungování přístupových metod již musí být zajištěna možnost přenosu (vysílání a přijímání) jednotlivých bitů

- musí to být pod linkovou vrstvou

- protože k přenosu celých linkových rámců je již třeba mít zajištěn výhradní přístup ke sdílenému médiu

## • teoretická možnost řešení (ISO/OSI):

- přidat novou vrstvu mezi fyzickou a linkovou vrstvou

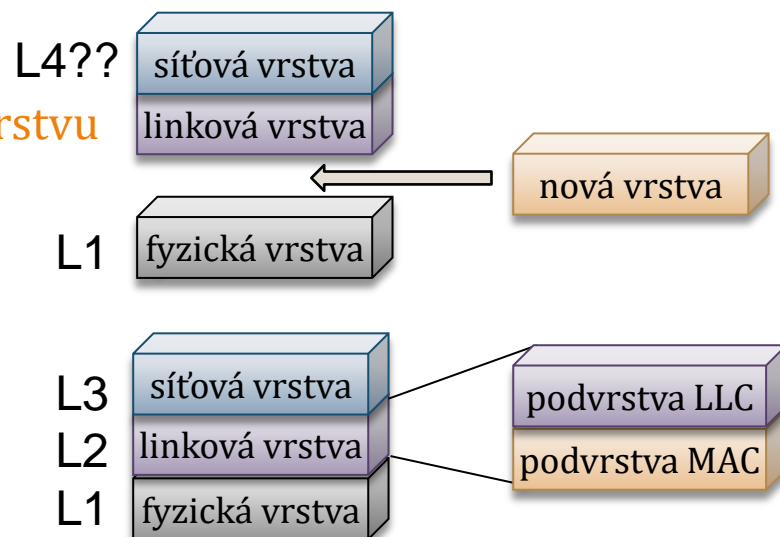
- a tím rozšířit 7vrstvý model na 8vrstvý

## • reálné řešení (v ISO/OSI):

- rozdělit linkovou vrstvu na dvě podvrstvy

- vyšší podvrstvu (**LLC, Link Layer Control**)
  - dělá to, co původně dělala celá linková vrstva
- nižší podvrstvu (**MAC, Media Access Control**)
  - řeší přístup ke sdílenému médiu

RM ISO/OSI s nimi nepočítal – vznikl pro rozlehlé sítě, které nepoužívají sdílená přenosová média



# možnosti řízení (výlučného) přístupu

- způsob řízení (výlučného) přístupu může mít několik stupňů volnosti

- podle toho se pak dají klasifikovat příslušné přístupové metody

## a) může být **deterministický**, nebo **nedeterministický**

těž: neřízený

- **deterministický**: vše se řídí pravidly, která neobsahují žádný prvek náhody

- „*vždy to dopadne dobře*“: pravidla jsou nastavena tak, aby v konečném čase vedla k cíli
  - aby některý z uzlů, který usiluje o získání přístupu, jej také skutečně získal
    - díky tomu lze garantovat právo přístupu ke sdílenému médiu
- „*vždy to dopadne stejně*“: je-li stejný výchozí stav, je stejný i výsledek
  - též: známe-li výchozí stav, dokážeme predikovat výsledek
- nevýhodou je složitější (a dražší) implementace

příklad: deterministické jsou přístupové metody sítí Token Ring či 100 VG Any-LAN

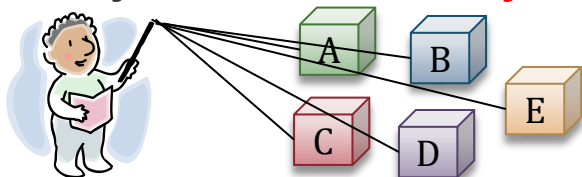
- **nedeterministický**: řídí se pravidly, která obsahují nějaký prvek náhody

- „*nemusí to dopadnout dobře*“: nemusí vést k cíli v konečném čase
  - není garantováno (na 100%), že některý z uzlů získá přístup k médiu
- získá ho jen s určitou pravděpodobností, v praxi velmi blízkou k 100%
  - ale ne rovnou !!!
- „*může to dopadnout různě*“: i při stejném výchozím stavu může být výsledek různý
  - též: výsledek nedokážeme predikovat, ani když známe výchozí stav
- výhodou je snazší a jednodušší implementace
  - a nižší režie na vlastní fungování



příklad: nedeterministické jsou přístupové metody sítí Ethernet či Wi-Fi

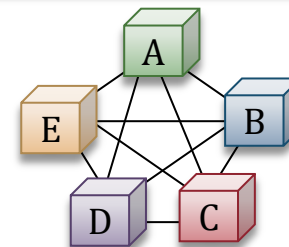
## možnosti řízení (výlučného) přístupu

b) může být **centralizovaný**, nebo **distribuovaný**

– **centralizovaný**: existuje nějaká centrální autorita, která rozhoduje o přidělení přístupu

- obvykle se rozhoduje deterministicky
  - dokáže garantovat právo přístupu
- **výhoda**:
  - může být adaptivní
    - centrální autorita může měnit strategii svého rozhodování
  - může pracovat s prioritami
    - i zohledňovat další kritéria
- **nevýhoda, nebezpečí**:
  - při výpadku či nedostupnosti centrální autority je celá síť mimo provoz
    - žádný uzel nezíská přístup k médiu

příklad: centralizovaná je přístupová metoda sítě 100 VG Any-LAN



– **distribuovaný**: neexistuje žádný centrální prvek, vše je realizováno součinností jednotlivých uzlů

- **předpoklad**:
  - každý uzel se musí chovat korektně a dodržovat pravidla přístupové metody
- může fungovat deterministicky i nedeterministicky
- **výhoda**:
  - nemá „single point of failure“
    - funguje i při libovolně velkém výpadku
- **nevýhoda**:
  - složitější implementace, musí pamatovat na různé nestandardní situace

příklad: distribuované jsou mj. přístupové metody Ethernetu, sítě Wi-Fi, sítě Token Ring atd.

# možnosti řízení (výlučného) přístupu

- c) může mít soutěžní, rezervační, dotazovací, předávací nebo jiný charakter
- další možné dělení postupů při zajišťování výlučného přístupu ke sdílenému médiu se liší podle toho, jaký je jejich celkový charakter
  - **soutěžní:** mezi uzly, které aktuálně usilují o získání přístupu ke sdílenému médiu, dochází ke vzájemné soutěži.
    - pravidla soutěže mohou být deterministická, či nedeterministická
      - u deterministických pravidel je obvykle zaručeno, že ze soutěže vzejde právě jeden vítěz
        - který získá právo výlučného přístupu ke sdílenému médiu
      - u nedeterministických pravidel nemusí být zaručeno, jak soutěž dopadne – nemusí z ní vzejít žádný vítěz
  - **rezervační:** existuje možnost „zarezervovat si“ sdílené médium
    - prostřednictvím vhodného mechanismu, například pomocí (kolujícího) rezervačního rámce
  - **dotazovací:** u centralizovaných metod je obvyklé, že se centrální autorita dotazuje jednotlivých uzlů
    - nebo naopak tyto uzly posílají své žádosti centrální autoritě
  - **předávací:** jednotlivé uzly si vzájemně předávají „něco“ (tzv. peška, token), který opravňuje k přístupu ke sdílenému médiu
    - na podstatě „peška/tokenu“ nezáleží
    - ale:
      - musí existovat logický kruh, v rámci kterého si jej předávají
        - musí být ošetřeno rozpojení kruhu, ztráta peška atd.
  - **jiné:** přístupová metoda má ještě jiný charakter
    - například určitého „rozpočítávání“



# přístupová metoda ALOHA

- jde o nedeterministickou (neřízenou) distribuovanou přístupovou metodu

- vznikla pro potřeby akademické sítě ALOHAnet na Havajských ostrovech (1970/1)

- rádiové přenosy probíhají na velkou vzdálenost mezi ostrovy: až 600 km
- pro minimalizaci kolizí jsou použity dva přenosové kanály
  - vyhrazený kanál (100 kHz na 413,475 MHz), používá jej centrální uzel pro rozesílání dat
  - sdílený kanál (100 kHz na 407,350 MHz), používaný pro zasílání zpráv a potvrzení centrálními uzlu
    - potřeba řízení přístupu se týká (pouze) tohoto sdíleného kanálu



- princip fungování přístupové metody ALOHA:

- „*potřebuješ-li něco odeslat, na nic se neohlížeš a odešli to ....*“

- tj. uzel se neohlíží na to, zda právě někdo vysílá či nikoli
- může dojít ke kolizi (od souběžného vysílání) a přenášená data nemusí být doručena
  - výsledek není zaručen, nelze garantovat doručení ....

- příjemce posílá potvrzení o úspěšně doručených datech

- odesílatel se řídí potvrzením:

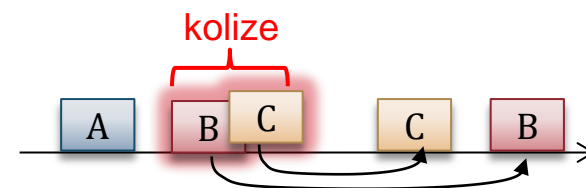
- pokud v časovém limitu obdrží (kladné) potvrzení, považuje přenos za úspěšný
- pokud v časovém limitu neobdrží potvrzení, považuje přenos za neúspěšný

- počká náhodně zvolenu dobu

- pak opakuje pokus o přenos

- ovšem s omezením max. počtu pokusů (obvykle 15)

tzv. čistá ALOHA



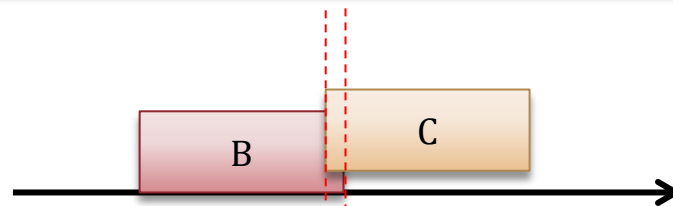
prvek náhody – jde o nedeterministickou metodu



# Slotted Aloha

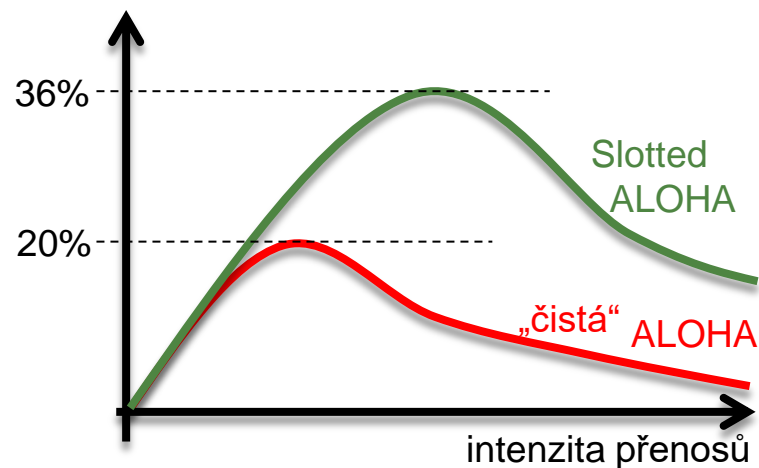
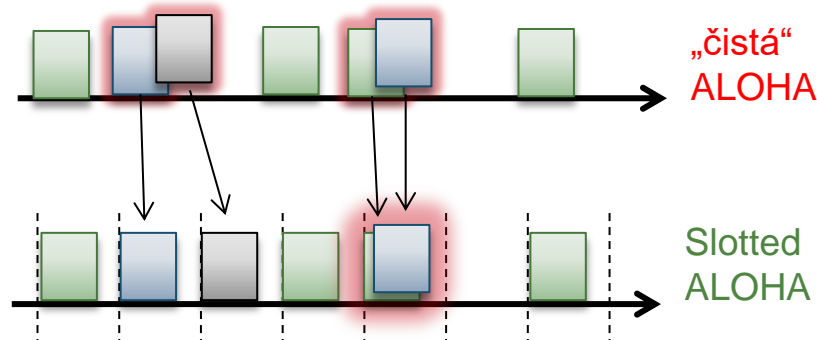
- **tzv. „čistá“ ALOHA**

- fungovala dobře pro velmi nízkou zátěž
- s rostoucí zátěží začala narůstat četnost kolizí
  - problém: stačilo i jen malé „překrytí“ dvou různých vysílání a data byla poškozena kolizí
  - teoretické maximum vytížení sdíleného média bylo cca 20%
    - a při vyšší zátěži využitost naopak klesala (kvůli nárůstu kolizí)

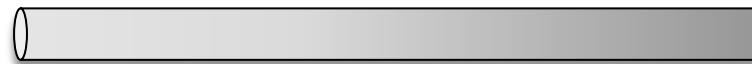


- **řešení: Slotted ALOHA**

- centrální uzel vysílá časový signál
  - který všem uzlům vymezuje začátky stejně velkých časových slotů
- uzel, který chce začít vysílat, musí počkat na začátek časového úseku (timeslotu)
- efekt:
  - buďto ke kolizi vůbec nedojde
    - vysílání různých uzlů se uskuteční v různých časových úsecích
  - nebo je kolize „důkladná“
    - vysílání se nikdy nepřekryjí „jen málo“
- důsledek:
  - max. vytížení sdíleného média stoupl na cca 36%



# příposlech nosné



- další snížení četnosti kolizí je možné díky tzv. příposlechu nosné

-  CS, Carrier Sense

- princip:

- uzel, který chce začít vysílat, si nejprve „poslechne“, zda právě nevysílá někdo jiný

- poslouchá tzv. nosnou (carrier), proto „příposlech nosné“ (carrier sense)

- vlastně se ptá: **je přenosové médium právě volné?**

- a pokud někdo vysílá, sám vysílat nezačne

- neskočí mu „do řeči“ a tím nezpůsobí kolizi

- předpoklad:

- příposlech nosné má smysl jen tam, kde je krátké přenosové zpoždění

- aby se uzel dozvěděl o aktuální situaci a mohl na ni reagovat
    - a nikoli o historii, která se již odehrála a nelze do ní zasáhnout/ovlivnit ji

- důsledek:

- příposlech nosné se používá jen v lokálních sítích (LAN), nikoli v rozlehlých (WAN)

- a to jak drátových (např. Ethernet), tak bezdrátových (IEEE 802.11/Wi-Fi)
    - u sítě ALOHAnet se příposlech nosné nepoužíval – i kvůli velkým vzdálenostem

- otázka:

- co má dělat uzel, který zjistí, že médium je právě obsazeno?



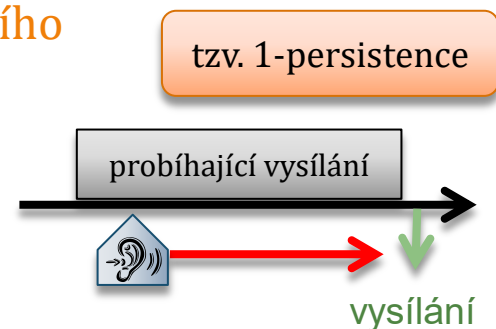
# persistentnost

- **znovu stejná otázka:**
  - co má dělat uzel, který díky příposlechu nosné zjistí, že médium je právě obsazeno?
    - kromě toho, že nezačne vysílat hned, aby nezpůsobil kolizi?

- **možnosti:**

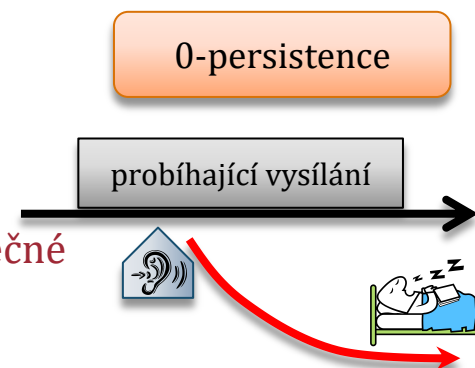
- *být vytrvalý* ( **persistent**): čekat na konec právě probíhajícího vysílání, a pak začít vysílat sám

- výhoda: neztrácí zbytečně čas (nesnižuje tím latenci)
- nevýhoda: pokud se takto chovají i ostatní uzly, je možné, že na konec téhož vysílání čekají i další uzly – a pak (po skončení právě probíhajícího vysílání) dojde s jistotou ke kolizi



- *nebýt vytrvalý* ( **non persistent**): nečekat na konec právě probíhajícího vysílání a „rovnou to vzdát“

- odmlčet se na náhodně zvolenou dobu, a pak to zkoušet znovu
- nevýhoda: rozhodnutí „rovnou to vzdát“ může být předčasné a zbytečné
  - pokud žádný jiný uzel nečeká na konec probíhajícího vysílání



- „hodit si kostkou“: s pravděpodobností  $p$  se zachovat persistentně

- a s opačnou pravděpodobností nepersistentně



# vliv persistence

- **persistence uzlu ovlivňuje četnost kolizí i latenci**

- **v případě 1-persistence:**

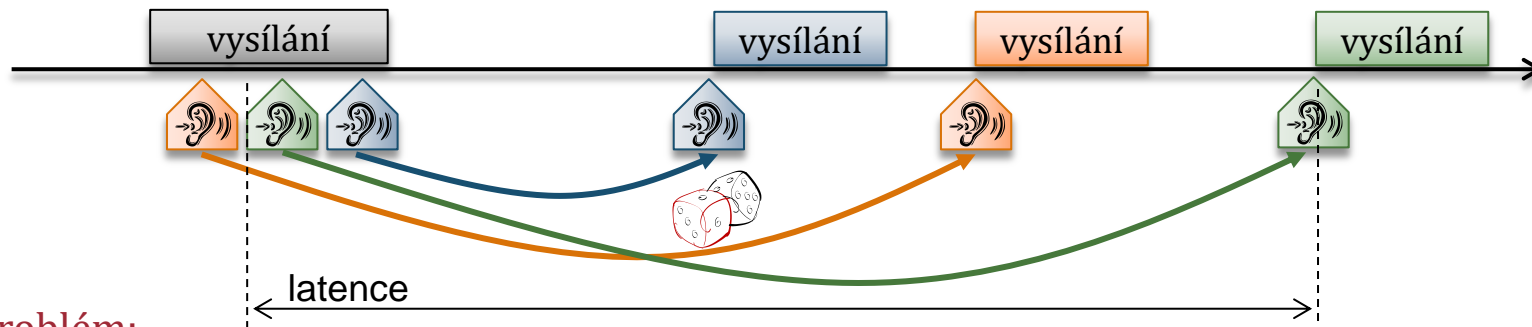
- může se stát, že více uzlů bude čekat na konec právě probíhajícího vysílání
- jakmile vysílání skončí, začnou vysílat všechny „čekající“ uzly – a **dochází ke kolizi**



- pravděpodobnost takovéto kolize je tím vyšší, čím vyšší je četnost požadavků jednotlivých uzlů na vysílání

- **v případě 0-persistence:**

- i když zájem o vysílání projeví více uzlů, prvek náhody zajistí vhodné rozložení jejich požadavků v čase
- každý se odmlčí a každý to bude znovu zkoušet v jinou (náhodně zvolenou) dobu



- problém:

- **výrazně to zvyšuje latenci** (kvůli odmlčení/čekání)
  - může to být zbytečné - při nízké četnosti požadavků jednotlivých uzlů na vysílání

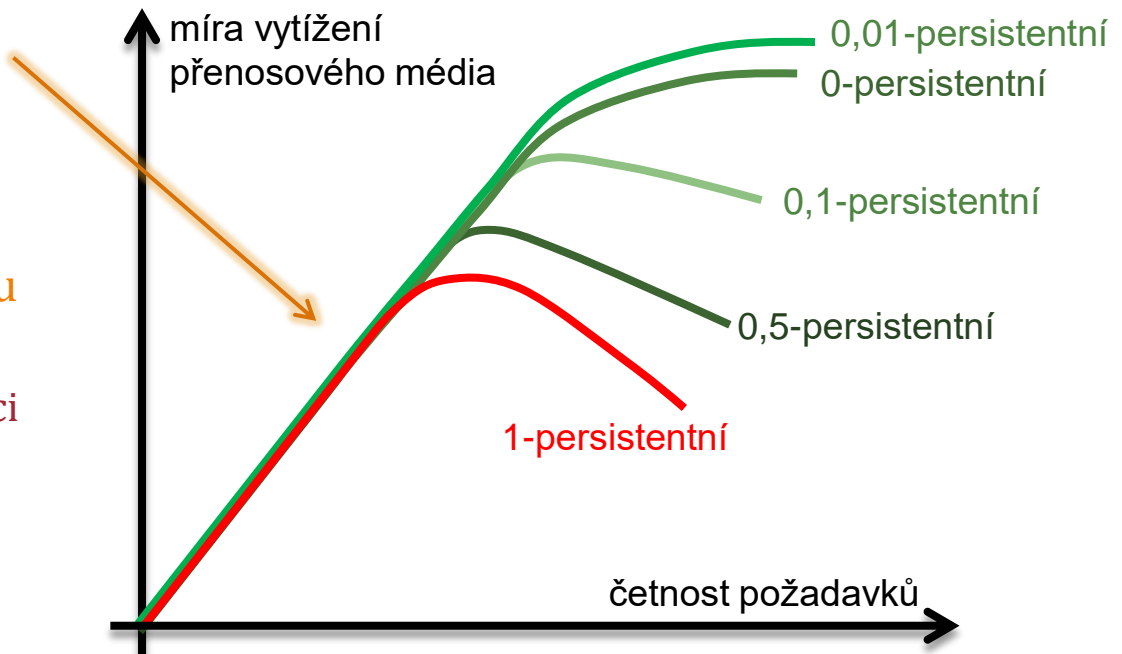
# vliv persistence

- **persistence má významný vliv i na míru vytížení přenosového média**

- vytížení ve smyslu procenta (užitečně využití) přenosové kapacity
- **obecný předpoklad:**
  - čím více bude kolizí, tím hůře
    - takže „méně persistentní“ metody budou dosahovat lepších výsledků
- **empirické zjištění:**
  - nejvyšší míru vytížení přenosového média dosahují metody s 0,01 persistencí
  - nejnižší naopak 1-persistentní metody
    - kvůli růstu rezie, který způsobuje narůstající četnost kolizí
  - při „nízké zátěži“ se všechny metody chovají stejně
    - nezávisle na persistenci

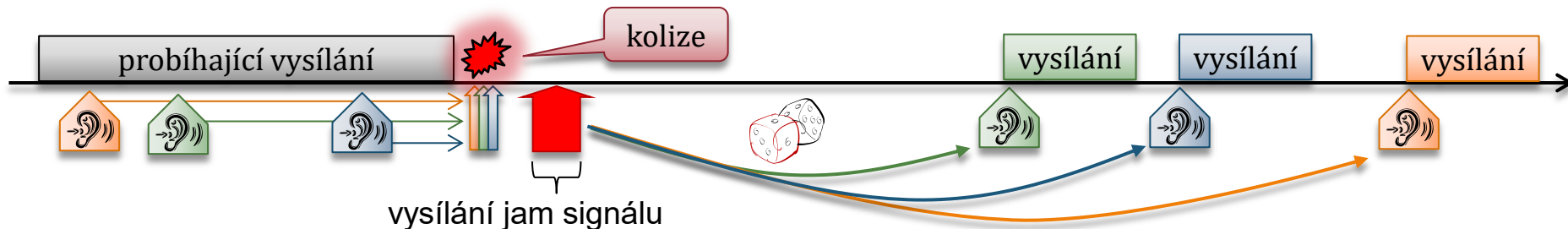
- **v praxi:**

- přístupová metoda Ethernetu (CSMA-CD) je **1-persistentní**
  - hlavně kvůli minimální latenci
- přístupová metoda sítí Wi-Fi (CSMA/CA) je **0-persistentní**
  - asi kvůli vyšší míře vytížení přenosového média (éteru)



# metoda CSMA/CD

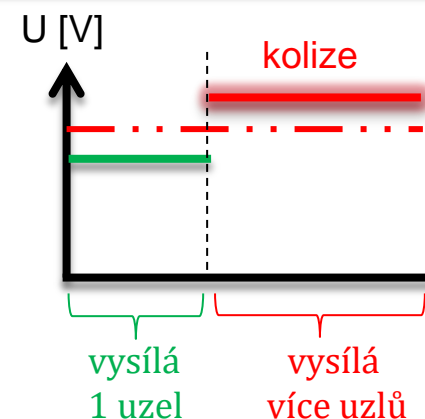
- **přístupová metoda, použitá např. v Ethernetu**
  - **CS: Carrier Sense**
    - používá příposlech nosné
    - chová se 1-persistentně
      - což zvyšuje pravděpodobnost kolizí
  - **MA: Multiple Access**
    - používá sdílené médium, ke kterému mají přístup všechny uzly
      - ke kolizím tedy může docházet
- **problém kolizí řeší alespoň dodatečně (když už k nim došlo)**
  - **používá detekci kolizí (proto CD: Collision Detect)**
    - snaží se rozpoznat (detekovat), že ke kolizi došlo
    - jednotlivé uzly pomáhají ostatním uzlům, aby kolizi správně rozpoznaly
      - kolizi ještě záměrně utvrzují, vysíláním tzv. **jam signálu**
    - snaží se minimalizovat další (opakovaný) výskyt kolize
      - k tomu používá prvek náhody
        - při výskytu kolize se uzel odmlčí na náhodně zvolenou dobu
      - prvku náhody ještě „pomáhá“
        - pokud se uzel znovu dostane do kolize, zdvojnásobí si interval, ze kterého volí náhodnou dobu



# kolize a kolizní domény

## • kolize (v Ethernetu, s metodou CSMA/CD)

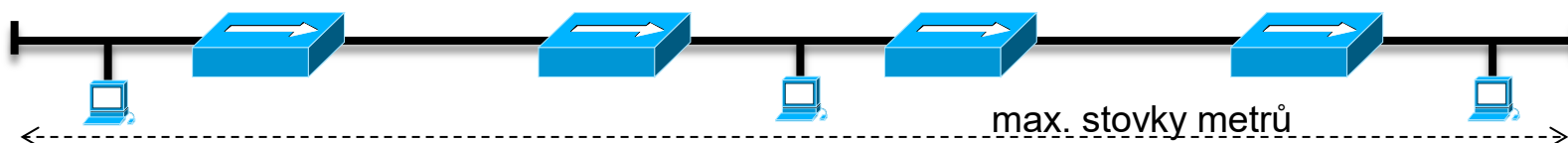
- je nežádoucí stav, způsobený tím, že vysílá více uzlů současně
- otázka: jak se to pozná?
  - odpověď: u koaxiálních kabelů dojde k určitému zvýšení napětí
    - nad hranici, obvyklou pro vysílání jednoho uzlu



## • kolizní doména

- jde o určitý „rozsah“
  - všechny uzly v kolizní doméně musí kolizi včas a korektně zaznamenat
    - „informace o kolizi“ (jam signál) se musí včas rozšířit po celé kolizní doméně
      - v čase, který odpovídá přenosu nejmenšího možného linkového rámce (51,2  $\mu$ sec)
  - kolizní doména končí na nejbližším přepínači (switch-i) nebo na „konci kabelu“
- podle toho „rozsahu“ je dimenzována:
  - maximální délka a počet souvislých kabelových segmentů v kolizní doméně
    - včetně počtu opakovačů, které je spojují
      - pravidlo 5:4:3 (max. 5 segmentů, max. 4 opakovače, max. 3 „obydlené“ segmenty)

platí jen pro 10 Mbit/s Ethernet



- minimální velikost linkového rámce
  - 64 bytů / 512 bitů (u 10 Mbit/s Ethernetu)
- délka (trvání) jam signálu

důsledek: kvůli metodě CSMA/CD má Ethernet jen omezený dosah

# metoda CSMA/CD v Ethernetu

- byla vyvinuta pro první verze 10Mbit/s Ethernetu (10Base5, 10Base 2)
  - používající koaxiální kabel (v roli společně sdíleného přenosového média)
    - protože toto médium skutečně bylo sdílené, svou fyzikální podstatou
- má (měla) pro Ethernet zásadní důsledky:
  1. Ethernet je technologií vhodnou jen pro sítě LAN
    - kvůli (značně) omezenému dosahu kolizní domény
      - řádově stovky metrů
    - nelze jej využít pro sítě MAN a WAN
      - kde jsou vzdálenosti mezi uzly podstatně větší
  2. Ethernet nelze využít „v reálném čase“
    - kvůli prvku náhody při řešení kolize je CSMA/CD nedeterministickou přístupovou metodou
      - negarantuje, zda ani za jak dlouho se uzel dostane k přenosu (odvysílání) svých dat
    - hodí se například do kancelářského, domácího či školního prostředí
      - ale ne do prostředí s garantovanými odezvami, například v řízení výroby apod.
- metoda CSMA/CD se používá:
  - i v novějších a rychlejších verzích Ethernetu
    - které pracují s jiným druhem přenosového média, než je koaxiální kabel
      - pokud nefungují plně duplexním způsobem
- metoda CSMA/CD není zapotřebí a již se nepoužívá:
  - v plně duplexních variantách Ethernetu
    - volitelně u 1 Gbit/s, povinně všechny vyšší rychlosti

díky opuštění metody CSMA/CD se (plně duplexní) Ethernet stal technologií i pro sítě MAN a WAN




# řízení přístupu v sítích 802.11



má charakter soutěže  
sobě rovných uzlů

jde o soutěž

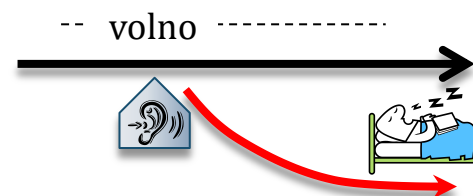
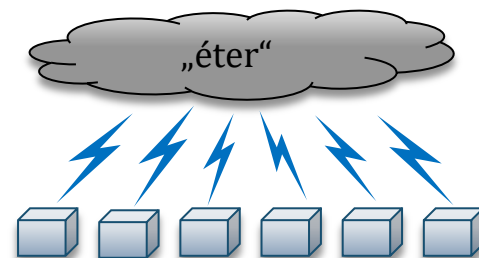
nejde o soutěž

- v bezdrátových sítích LAN (WLAN) dle standardu IEEE 802.11
  - známějších spíše jako síť Wi-Fi
- standardy definují 2 základní varianty řízení přístupu:
  - **DCF (Distributed Coordination Function)** – povinná
    - je založena na přístupové metodě **CSMA/CA**
      - jde o nedeterministickou (neřízenou) a distribuovanou přístupovou metodu
      - lze ji využít v ad-hoc režimu i v režimu infrastruktury WLAN sítě
    - má ještě další volitelnou (pod)variantu: **DCF s RTS/CTS**
      - která řeší problém skryté a předsunuté stanice
  - **PCF (Point Coordination Function)** – volitelná a implementovaná „jen někdy“
    - jde o kombinaci dvou přístupových metod (s jejich pravidelným střídáním):
      - nedeterministické (neřízené) distribuované přístupové metody
        - jde o metodu CSMA/CA, používanou v rámci DCF
          - fakticky jde o „fázi soutěže mezi uzly“ (contention period), kdy jsou si všechny uzly rovny
      - deterministické (řízené) centralizované přístupové metody
        - využívá dotazování jednotlivých uzlů (  polling)
          - jde o „řízenou“ fázi, kdy si uzly nejsou rovny (AP/přístupový bod řídí, ostatní jsou podřízeni)
    - lze využít jen v režimu infrastruktury
      - s přístupovým bodem (AP, Access Point), který plní roli centrální autority



# metoda CSMA/CA

- je distribuovanou přístupovou metodou – soutěží mezi sobě rovnými uzly
  - nemá centrální autoritu
    - či jeden uzel v jiném postavení než ostatní uzly
- není CD (Collision Detect)
  - nesnaží se detekovat kolize
    - protože rádiová rozhraní nedokáží současně vysílat a přijímat
      - každý přijatý rámec je potvrzován, že došlo ke kolizi se pozná podle absence potvrzení
- je **CA (Collision Avoidance)**
  - nikoli ale ve smyslu úplného vyloučení kolizí (avoidance)
    - usiluje jen o snížení jejich počtu – snaží se předcházet kolizím
- je nedeterministickou (neřízenou) přístupovou metodou
  - pro výběr mezi více potenciálními zájemci o vysílání používá prvek náhody
    - než uzel začne vysílat, odmlčí se na náhodně zvolenou dobu
      - jde o random backoff, resp. „náhodný rozstřel“
    - proto: negarantuje právo vysílat (natož pak v konečném čase)
- kromě toho musí zajistit:
  - přednostní právo na přenos potvrzení (ACK) a řídicích rámců (RTS, CTS, NAV)
  - své fungování „uvnitř“ varianty PCF
    - v rámci té části super-rámce, která zajišťuje soutěž mezi uzly



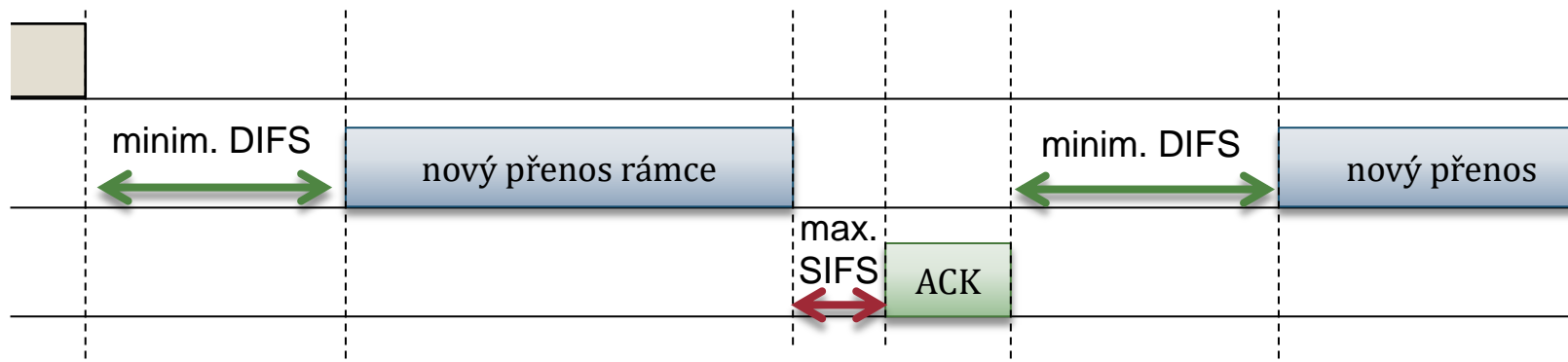
# časové konstanty

- **princip:**

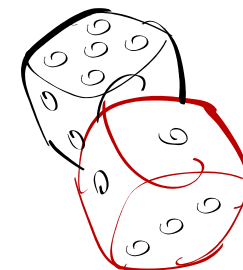
- některé děje musí mít přednost před jinými (a ty musí počkat)
  - odeslání potvrzení musí mít přednost před jinými přenosy
  - výzva podřízené stanici (u PCF) musí mít přednost před zahájením „nového“ přenosu

- **řešení: používají se 3 časové konstanty:  $SIFS < PIFS < DIFS$**

- jejich konkrétní hodnota je různá pro různé varianty sítí IEEE 802.11 (Wi-Fi)
- **SIFS: Short InterFrame Space**
  - (nejpozději) do této doby by příjemce nepoškozeného rámce měl odeslat jeho potvrzení
- **PIFS: PCF InterFrame Space**
  - za tuto dobu koordinátor (v rámci metody PCF) osloví další koncovou stanici (polling)
- **DIFS: DCF InterFrame Space**
  - (nejdříve) za tuto dobu může být zahájen „nový“ přenos (v rámci metody DCF)



# náhodný rozstřel (metoda DCF)

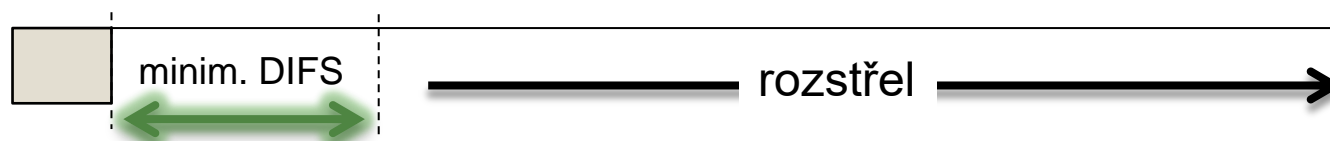


- připomenutí:**

- je to „soutěžní“ metoda, povinná pro všechny implementace
- používá „náhodný rozstřel“
  - prvek náhody, který vybírá mezi více potenciálními zájemci o vysílání

- fungování náhodného rozstřelu:**

- aby náhodný rozstřel mohl začít, musí být přen. médium volné nejméně po dobu DIFS
  - tj. uzel, který se chce účastnit rozstřelu, musí nejprve počkat, dokud nebude médium volné po dobu DIFS



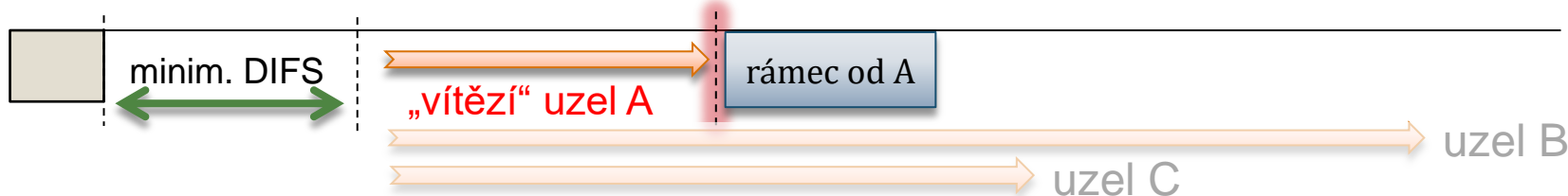
- na začátku rozstřelu si každý (zúčastněný) uzel zvolí náhodnou dobu, na kterou se odmlčí



- ale během této doby nespí, nýbrž monitoruje dění na přenosovém médiu

- vítězem je ten uzel, který se „probudí“ jako první

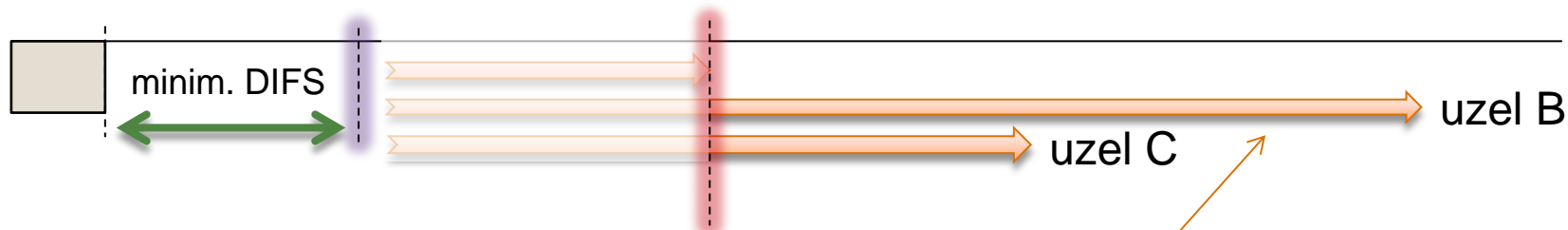
- a během celé doby, kdy čekal, nikdo jiný nezahájil vysílání !!!!



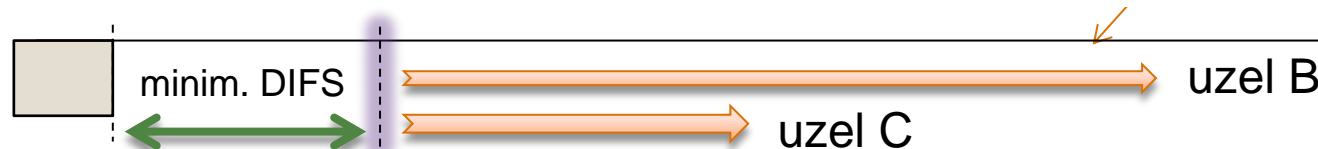
# náhodný rozstřel (metoda DCF)

- **fungování náhodného rozstřelu:**

- ty uzly, které v rozstřelu prohrály, si pamatují, jak dlouhé čekání jim ještě zbývalo



- s tímto „zbytkem“ pak vstupují do nového rozstřelu
  - který opět začíná čekáním na to, až bude médium volné (nejméně) po dobu DIFS



- a takto pokračují, dokud se jim nepodaří zvítězit

- **ani náhodný rozstřel nedokáže zcela zabránit kolizím**

- z náhodného rozstřelu může vzejít více vítězů
  - jejich kolize se pozná jen podle absence (kladného) potvrzení o příjmu přeneseného rámce
- obrana: pokud dojde ke kolizi, „pomůže se náhodě“
  - uzel, který se dostal do kolize, si zvětší (na dvojnásobek) interval, ze kterého volí náhodnou dobu svého odmlčení

# problém skryté a předsunuté stanice

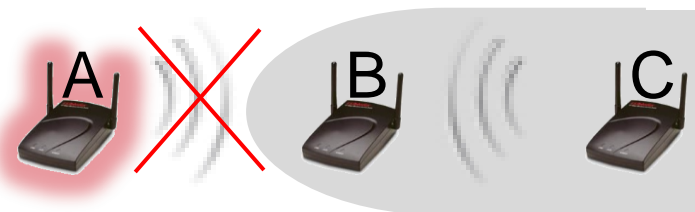
## • problém bezdrátových sítí: omezený dosah signálu

– signál nemusí „dosáhnout“ ke všem stanicím, které spolu chtějí komunikovat

• v praxi: **problém skryté stanice (A chce vysílat k B)**

– C vysílá k B, ale jeho vysílání „nedosáhne“ až k A

- A chce vysílat: při CS zjistí, že médium je volné
- C je pro A skrytou stanicí



## • jiný (opačný) problém: přesah signálu

– signál může „přesahovat“ i ke stanicím, kterým by jinak nemusel bránit v komunikaci

• v praxi: **problém předsunuté stanice (B chce vysílat k A)**

– C vysílá k D, jeho vysílání „slyší“ i B

- a myslí si, že médium je obsazeno
- proto B nevysílá k A
- i když by se vysílání C → D a B → A nerušila



## • řešení obou problémů:

– rozesílání zpráv **RTS** (Request to Send) a **CTS** (Clear to Send) před vlastním přenosem

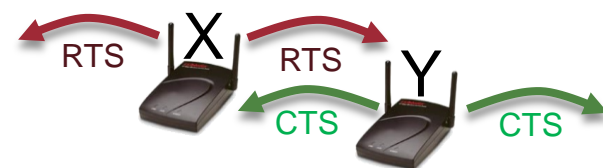
• uzel X, který chce začít vysílat, vyšle do svého okolí zprávu RTS (Y,n)

– tím říká všem uzlům ve svém dosahu: „chci komunikovat s uzlem Y po dobu n“

- a během této doby prosím nenarušujte mou komunikaci ...

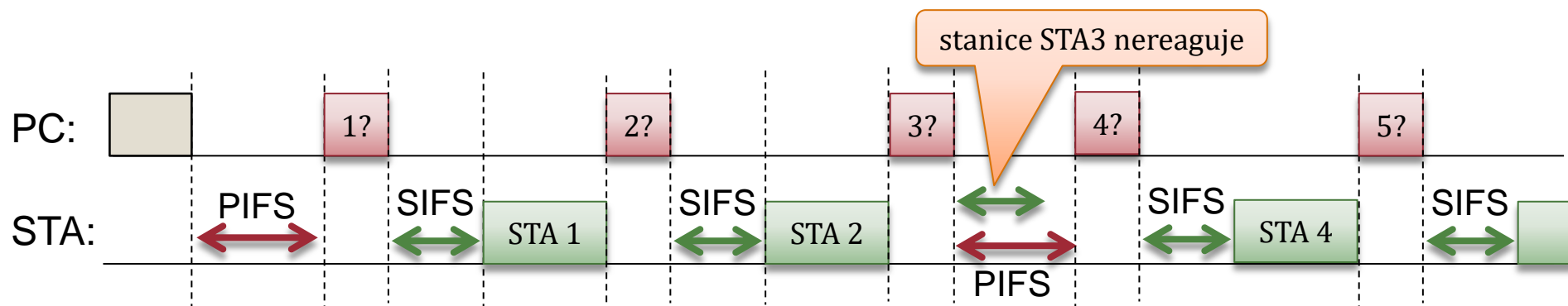
• uzel Y odpoví tím, že do svého okolí rozešle zprávu CTS (X, n)

– „budu komunikovat s uzlem X po dobu n ...“



# nesoutěžní část metody PCF

- **připomenutí: PCF je volitelná přístupová metoda**
  - jde o kombinaci dvou metod: **soutěžní** (DCF) a **nesoutěžní** (centralizované, řízené)
- **řízená a centralizovaná část metody PCF (Point Coordination Function):**
  - roli centrálního koordinátora (Point Coordinator, PC) hraje přístupový bod (AP)
    - také veškerý přenos dat probíhá přes tohoto koordinátora
  - koordinátor (PC) se postupně dotazuje (polling) koncových stanic (STA), zda mají něco k přenosu
    - součástí výzvy (poll) mohou být i data, určená k přenosu od PC k dotazované stanici (STA)
      - součástí může být i potvrzení předchozího úspěšně přeneseného rámce
    - dotázaný koncový uzel (STA) by měl zareagovat (začít vysílat) nejpozději do doby SIFS
      - pokud nemá co k přenosu, vyšle alespoň prázdný rámec (NULL frame)
        - součástí odesílaného rámce může být i potvrzení přijatého rámce (piggybacking)
  - pokud STA do doby SIFS nezareaguje, arbitr do doby PIFS osloví další (STA) v pořadí



# metoda Token Passing

- **deterministická (řízená) a distribuovaná přístupová metoda**
  - používaná například v sítích Token Ring, Token Bus, FDDI a dalších
- **princip:**
  - síť koluje „pešek“ (token)
    - ten, kdo ho drží, má právo přístupu ke sdílenému médiu (právo vysílat)
      - nesmí ho držet příliš dlouho, aby se ke slovu dostaly i další uzly
        - na „fyzikální podstatě“ peška nezáleží – v praxi jde o speciální linkový rámec
  - uzly si předávají peška (token) v určitém pořadí
    - uzly musí tvořit logický kruh, v rámci kterého si peška předávají
      - musí být vhodně ošetřeny nestandardní situace, hlavně přerušení logického kruhu
        - když některý z uzlů v logickém kruhu přestane fungovat (je vypnut), nebo naopak začne fungovat
          - obvykle: řeší jeden z uzlů, který má tyto věci na starosti (active monitor)
            - pokud takový uzel není dostupný, musí jej v roli monitoru zastoupit některý další uzel
            - problém: všechny uzly musí implementovat funkčnost monitoru = **složitě a drahé**

