



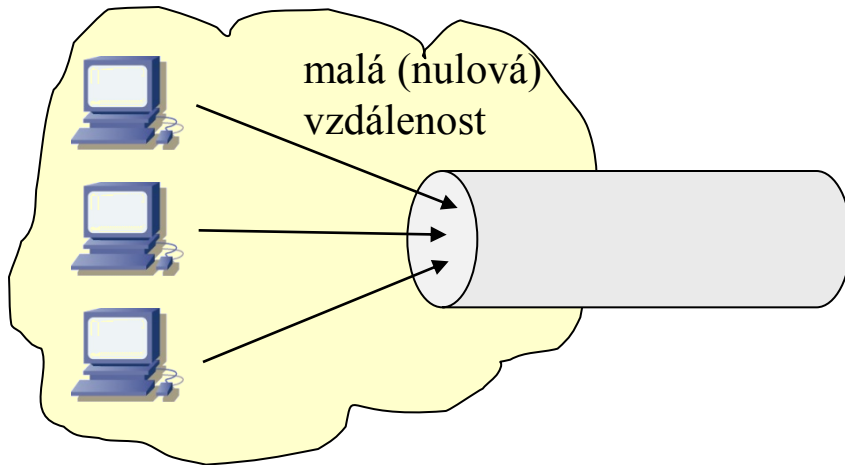
Katedra softwarového inženýrství,
Matematicko-fyzikální fakulta,
Univerzita Karlova, Praha



Lekce 8: Přístupové metody

Jiří Peterka, 2009

multiplexování vs. řízení přístupu

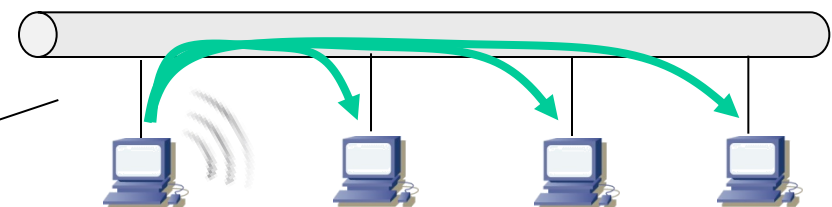
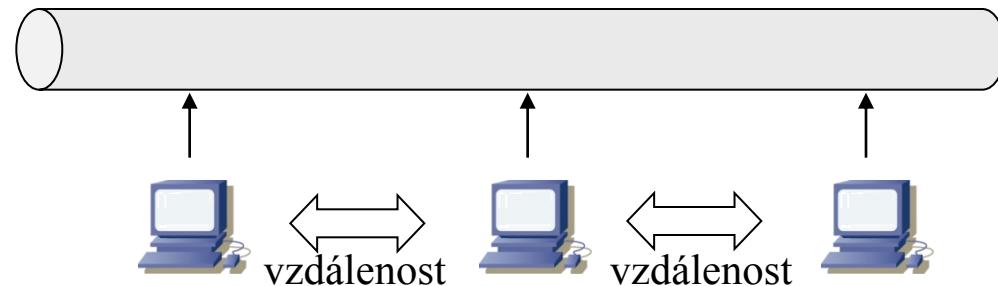


- multiplex(ování):
 - je **n** zájemců o využití **1** přenosového kanálu
 - všichni se "vyskytují" v jednom místě
 - díky tomu lze snadno řešit jejich koordinaci
 - existuje více druhů multiplexů
 - **lze vyhovět všem**
 - "současně"

problémem není současný příjem
(1* vysílání, n* příjem)

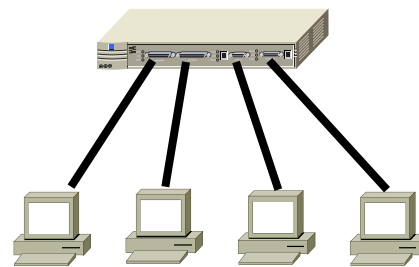
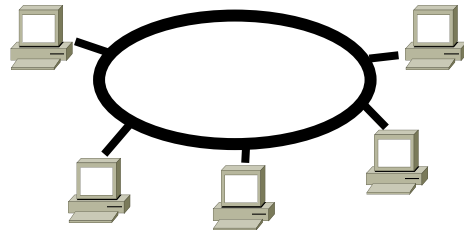
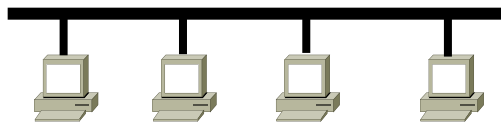
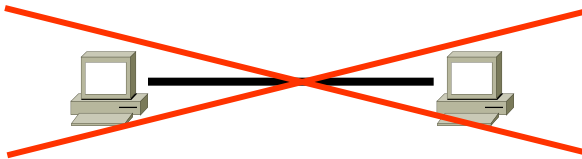
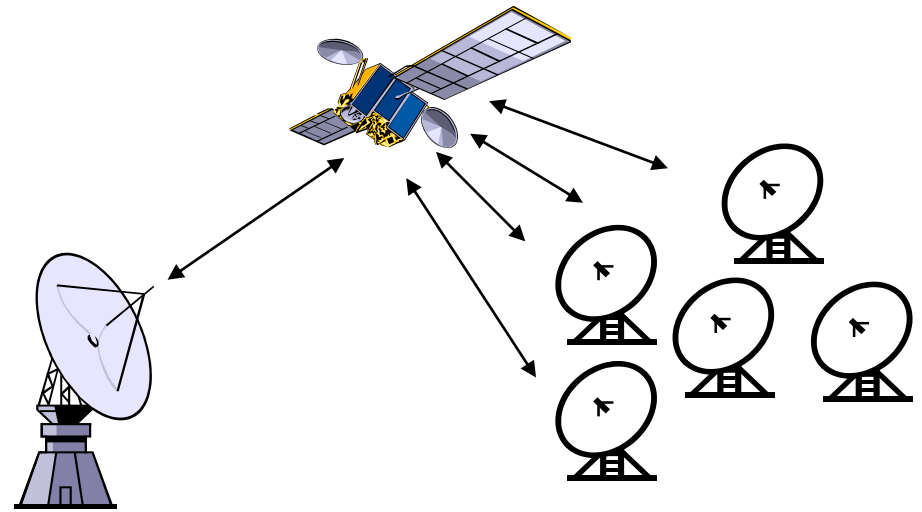
- řízení přístupu:

- je **n** zájemců o využití **1** přenosového kanálu
 - pro vysílání !!!
- nevyskytují se na stejném místě
 - a kromě společného přenosového kanálu nemají jinou možnost vzájemné komunikace
- **lze vyhovět jen jednomu!!**



upřesnění problému (přístupu)

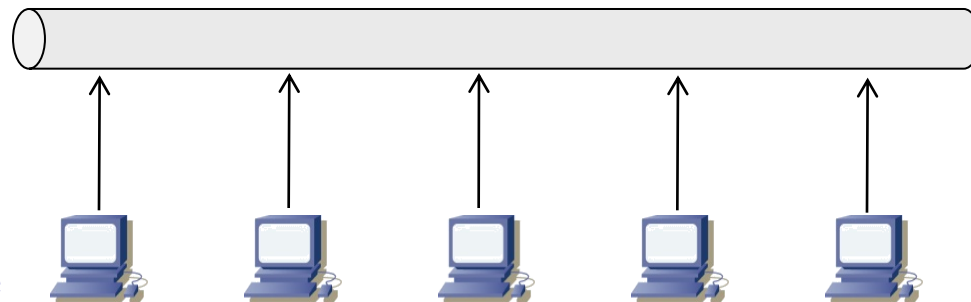
- týká se "vícebodových" topologií
 - kde je k jednomu přenosovému kanálu připojeno více stanic
 - sběrníková topologie
 - topologie do hvězdy/stromu
 - kruhové topologie
 - netýká se dvoubodové topologie



- týká se hlavně sítí LAN
 - které používají "vícebodové" topologie
- sítí WAN se týká jen zřídka
 - WAN většinou používají dvoubodové spoje mezi uzly
 - výjimky:
 - např. satelitní spoje

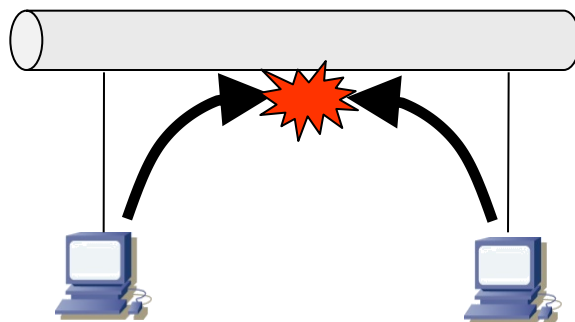
vícenásobný přístup

- přenosový kanál je jeden
 - pro veškerou komunikaci je k dispozici jen jeden přenosový kanál
- stanic (uzlů, terminálů, zařízení, ...) je více
 - a všechny mají přístup k přenosovému kanálu
 - proto: **MA, Multiple Access**
- přenosový kanál je **sdílený**
 - všechny stanice usilují o jeho využití
 - způsob, jakým stanice usilují o sdílený kanál, může mít:
 - řízený charakter
 - charakter soutěže
 - (jiný charakter)
- proto jsou nutné tzv. **přístupové metody** (access methods)
 - pro koordinaci přístupu stanic ke sdílenému médiu
- stanice se chovají autonomně
 - generují požadavky (na přenos, resp. na využití sdíleného přenosového kanálu) s určitou četností
 - nezávisle na činnosti ostatních uzlů
 - po vygenerování jednoho požadavku čekají, dokud není uspokojen
 - teprve pak přichází s dalším požadavkem
 - poněkud zjednodušené, v praxi nemusí nastávat

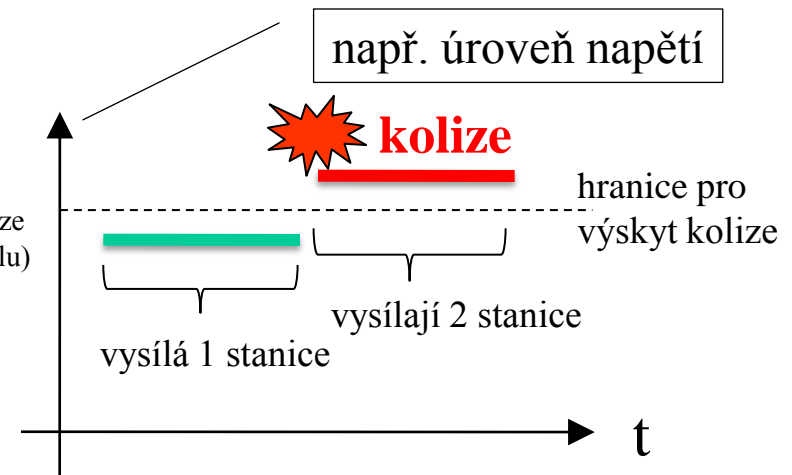


kolize

- do sdíleného kanálu může vysílat více stanic současně
 - přenosový kanál to (obvykle) nijak fyzicky nepoškodí
- ale obsah vysílání to "poškodí"
 - dochází k jeho znehodnocení a nemožnosti správně detekovat (rozpoznat), co bylo původně vysíláno
 - je to nežádoucí situace, označovaná jako **kolize!!!**
 - a je vhodné se jí vyhýbat, pokud je to jen možné



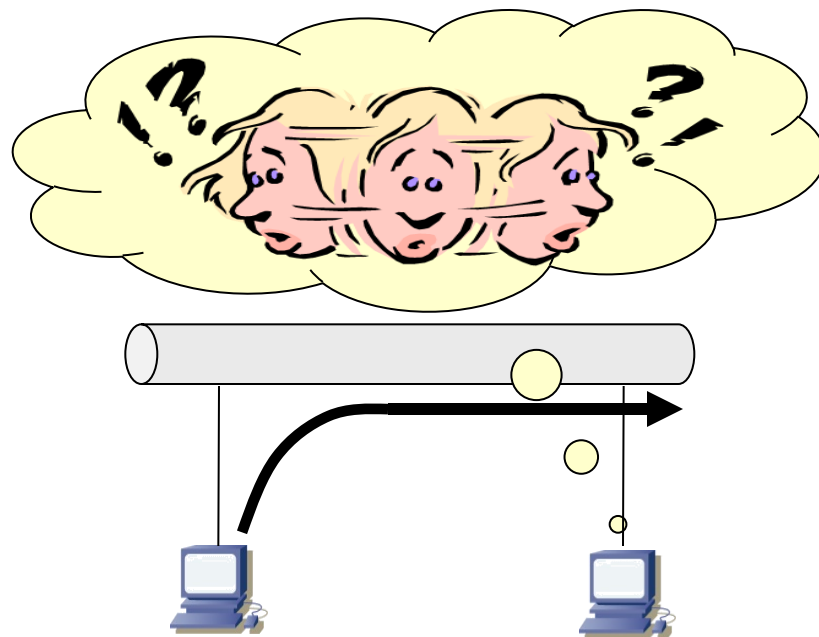
konkrétní projev kolize
(na koaxiálním kabelu)



- detekce kolizí:
 - obvykle je možné kolize detekovat
 - ale ne vždy
 - příklad: rádiové rozhraní obvykle neumožňuje současně vysílat a přijímat
 - » pak nelze detekovat kolize při vlastním vysílání
 - ně vždy se vyplatí kolizemi zabývat
 - například pokud se kolize zjistí jen s příliš velkým zpožděním
 - a realita může být mezitím úplně jiná

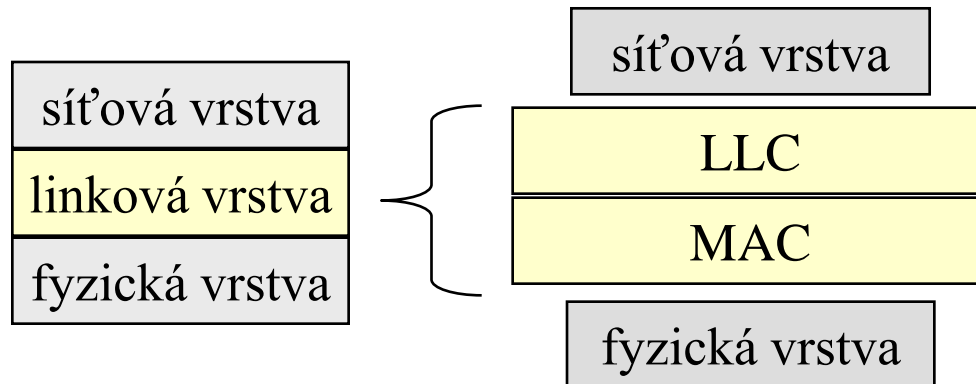
příposlech nosné

- stanice (obvykle) dokáží monitorovat stav sdíleného kanálu (přenosového média)
 - zda je volné
 - zda po něm právě někdo vysílá
 - event. zda právě probíhá kolize
- je to označováno jako "**příposlech nosné**" (**Carrier Sense, CS**)
- lze to využít pro potřeby řízení přístupu ke sdílenému kanálu
 - princip: stanice, která chce začít vysílat, nejprve "poslouchá nosnou", aby zjistila, zda je kanál volný
 - pokud by někdo vysílal, pak do tohoto vysílání nevstupuje
 - aby jej nenarušila
- ne vždy je ale příposlech nosné k dispozici
 - nebo je využitelný – například pokud přichází se zpožděním a vztahuje se k dřívějšímu okamžiku
 - realita mezitím může být úplně jiná
 - nastává například při přenosech na delší vzdálenosti



kde se problém přístupu řeší?

- RM ISO/OSI tento problém neřešil
 - počítal se sítěmi WAN a dvoubodovými spoji, kde problém nenastává
- řešení přístupu bylo nutné vložit do RM ISO/OSI dodatečně
 - ale kam?
 - na jakou vrstvu?
- problém přístupu musí být řešen:
 - nad fyzickou vrstvou
 - využívá se přenos jednotlivých bitů
 - pod linkovou vrstvou
 - než se bude přenášet celý rámec, už by stanice měla mít zajištěn přístup k přenosovému médium
- výsledek:
 - mezi fyzickou a linkovou vrstvou byla umístěná "nová vrstva"
 - fakticky: linková vrstva byla rozdělena na dvě podvrstvy:

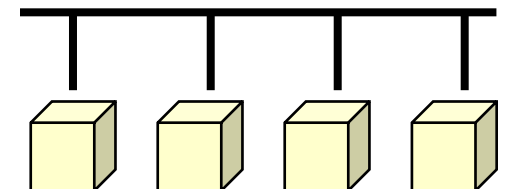
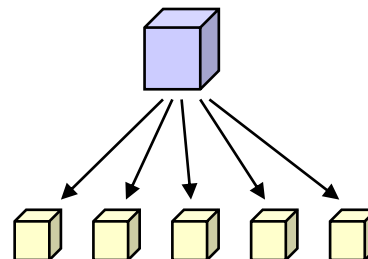


- podvrstvu LLC (Logical Link Control)
 - řízení linkového spoje (framing, spolehlivost – detekce, potvrzování, řízení toku atd.)
- podvrstvu MAC (Media Access Control)
 - řeší přístup ke sdílenému médium

možné varianty řízení přístupu

- **deterministické** (řízené) metody
 - mají jednoznačně definovaná pravidla, výsledek není ovlivněn náhodou a je plně predikovatelný
 - vždy vedou k výsledku
 - např. metody token passing
 - Token Ring, FDDI
- **nedeterministické** (neřízené) metody
 - jejich pravidla obsahují „náhodný“ prvek
 - typu: „počkej náhodně zvolenou dobu“
 - jejich výsledek není predikovatelný
 - nemusí vždy vést k výsledku
 - vedou k výsledku jen s určitou pravděpodobností

- **centralizované** metody
 - počítají s existencí centrálního „arbitra“, který rozhoduje
 - většinou jde o řízené (deterministické)
 - např. HDLC, 100 VG AnyLAN
- **distribuované** metody
 - neexistuje v nich centrální řídicí prvek
 - metodu realizují jednotlivé uzly ve vzájemné součinnosti
 - např. CSMA/CD (Ethernet)



možné varianty řízení přístupu

- metody předcházející kolizím (**CA, Collision Avoidance**)
 - většinou řízené metody, snaží se aby ke kolizím nedocházelo
- metody detekující kolize (**CD, Collision Detection**)
 - připouští výskyt kolizí, ale jsou schopné je rozpoznat a reagovat na ně
 - např. přístupová metoda Ethernetu (CSMA/CD)
- metody bez detekce kolizí
 - nedetekují kolize, nesnaží se jim předcházet, neřeší je
 - například přístupová metoda sítě Aloha
- metody eliminující kolize (**CE, Collision Elimination**)
 - kolize úplně eliminují, tyto nenastávají
 - obvykle jde o plně řízené metody
- rezervační metody
 - počítají s vyhrazením určitých zdrojů
 - dopředu, bez explicitní žádosti
 - na základě žádosti (objednávky)
- soutěžní metody
 - zájemci o sdílený zdroj se utkají v soutěži o něj
 - vítěz smí zdroj použít
 - obvykle nedeterministické a distribuované řešení bez arbitra
 - např. CSMA/CD

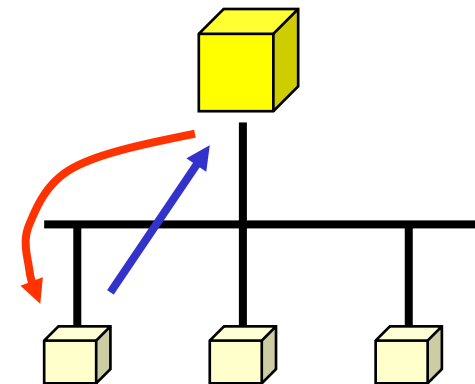
řízené centralizované metody

- počítají s existencí centrálního arbitra
- arbitr se musí dozvědět, kdo a kdy chce vysílat (získat přístup)
 - jinak by muselo jít o statické přidělování (FDM, TDM)
- jak se to arbitr může dozvědět?
 - **metodou výzev (polling)**
 - centrální arbitr se pravidelně (cyklicky) dotazuje všech potenciálních zájemců o vysílání
 - režie spojená s dotazováním je relativně vysoká
 - **z explicitních žádostí uzlů (requests)**
 - musí existovat možnost vyslat žádost směrem k arbitrovi
 - buď předem vyhrazené časové sloty
 - žádosti „cestují“ stejnou cestou jako data
 - nebo samostatné přenosové cesty, např. samostatné signály
 - pak žádost může být vyslána kdykoli

- výhody:
 - inteligence je soustředěna na jedno místo
 - arbitr může aplikovat různé strategie přidělování
 - může je i dynamicky měnit, v závislosti na chování sítě
- nevýhody:
 - funkčnost sítě stojí a padá s funkčností centrálního arbitra
 - single point of failure
 - režie na komunikaci mezi arbitrem a uzly může být významná

1. **Chceš? (výzva)**
2. **Chci/nechci ...**

1. **Chci! (žádost)**
2. **Můžeš ...**

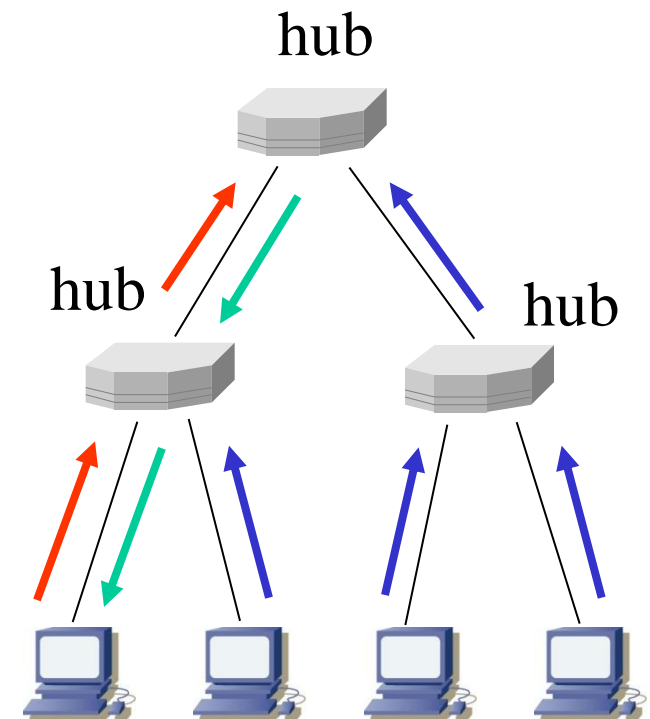


příklad: 100-VG AnyLAN



- technologie, vyvinutá firmou Hewlett-Packard (s podporou IBM a UB)
 - původně jako další vývojové stádium Ethernetu
- přístupová metoda se jmenuje **Demand Priority Protocol**
- je řízenou centralizovanou metodou
 - počítá s existencí arbitra (kořenového hub-u)
 - pracuje na principu žádostí od potenciálních zájemců
 - funguje pouze na kabeláži stromovité topologie!!!!
- základní myšlenky:
 - každý uzel má samostatnou přípojku (vlákno, 4 páry UTP)
 - když uzel nepřenáší data, může svou přípojku využít pro vyslání žádosti (směrem k hub-u) !!
 - stejnou cestou dostává uzel povolení k vysílání
 - arbitr (hub) přiděluje právo vysílat cyklicky (stylem round robin), uvažují se 2 úrovně priorit
- jako řízená metoda je to stabilní i při větších zátěžích

- Normal/High Priority Request
- Grant (právo vysílat)
- idle-up (stanice nežádá)



řízené distribuované metody

- nemají centrálního arbitra
- mají plně deterministická “pravidla hry“
- počítají s důslednou disciplínou všech uzlů
 - že každý dodrží stanovená „pravidla hry“
 - algoritmus přidělování „běží“ na všech uzlech
- varianty:
 - rezervační metody
 - prioritní přístup
 - metody s předáváním pověření (metoda logického kruhu)

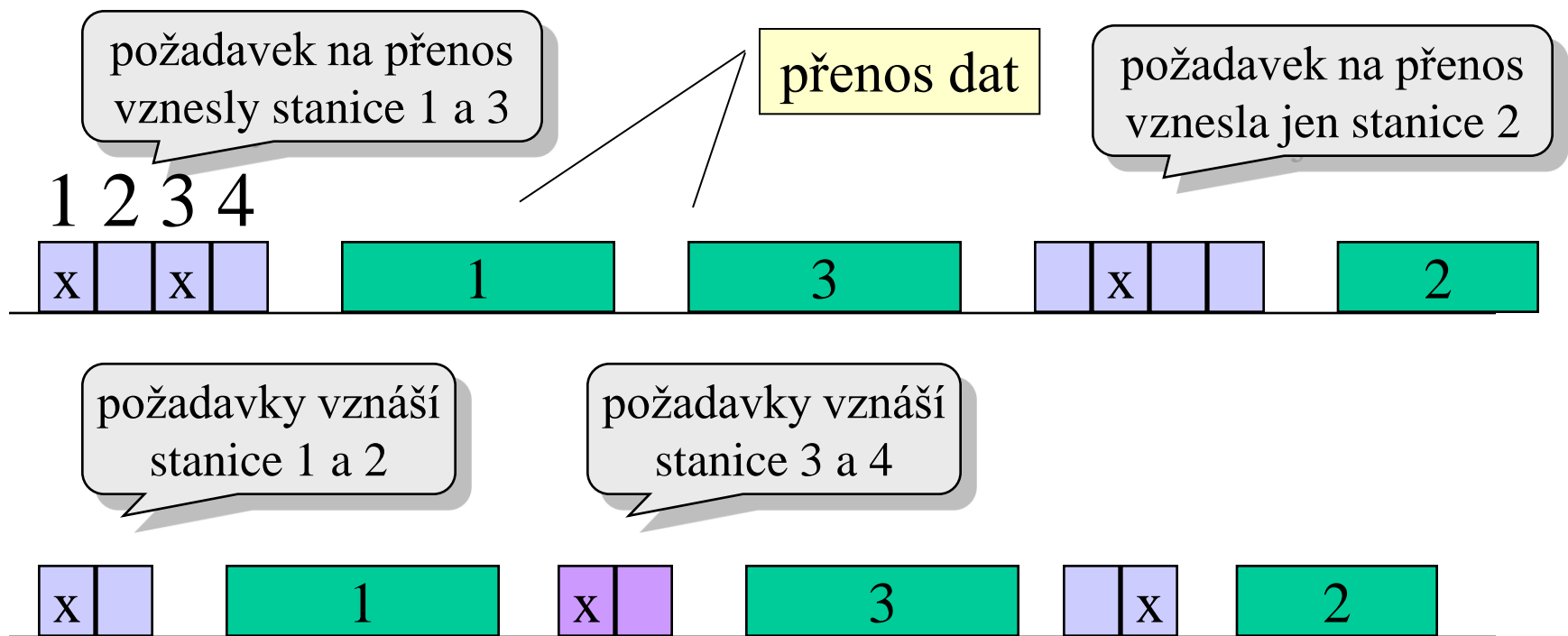
rezervační metody:

- distribuovaná obdoba přidělování na žádost
- typické řešení:
 - „éterem“ koluje (je pravidelně vysílán) zvláštní rezervační rámec
 - každý uzel zde může vyjádřit svůj požadavek
 - každý uzel bude mít úplnou informaci o všech požadavcích všech uzlů
 - rezervační rámec může mít podobu bitové mapy

patří mezi metody CE
(Collision Elimination) –
nedochází u nich ke kolizím

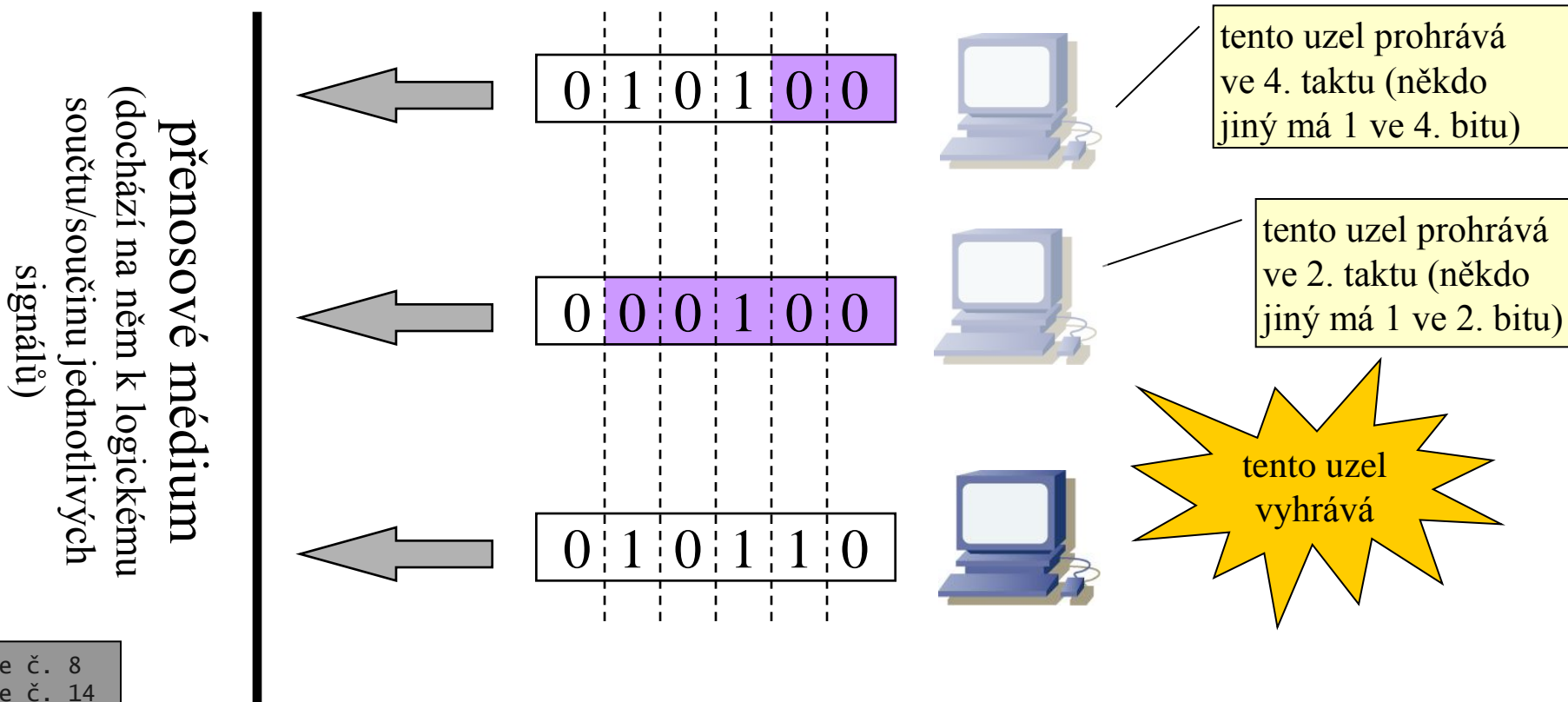
představa rezervační metody (varianta "round robin")

- síť "koluje" rezervační rámec, do kterého každý zájemce vyznačí zda má zájem o vysílání (přenos) či nikoli.
 - rezervační rámec může být rozdělen – pro aktivnější stanice a méně aktivní (a pro aktivnější stanice se posílá častěji – kvůli menší režii)



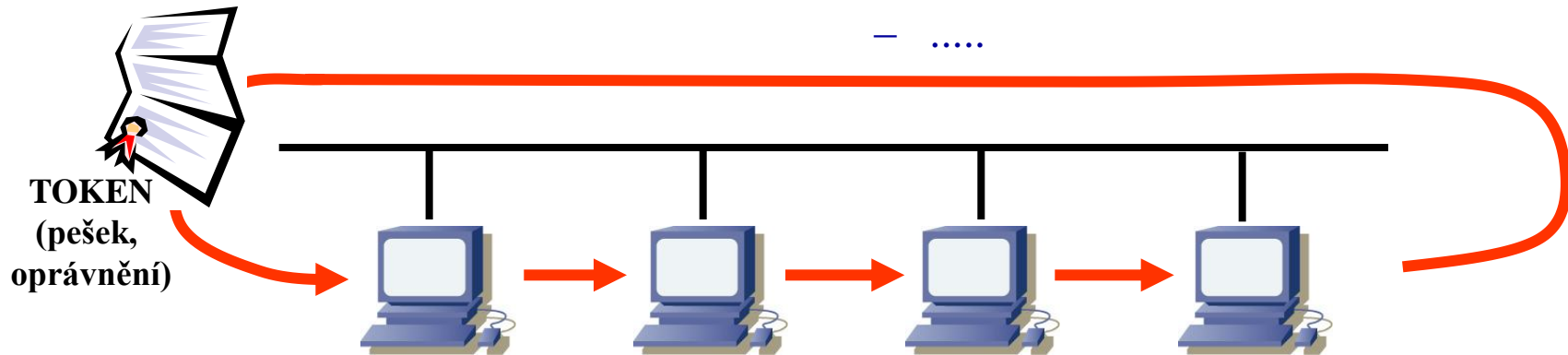
prioritní přístup - představa

- princip:
 - zúčastněné uzly mají možnost se „rozpočítat“
 - existuje způsob, jak žadatelé mohou ze svého středu vybrat (koordinovaným, deterministickým způsobem) jednoho, a ten může vysílat
 - technika „rozpočítávání“ může být různá, podle povahy přenosového média
 - nejčastěji je založena na binárním vyhledávání v adresách žadatelů
 - vyhraje ten, který má nejvyšší adresu



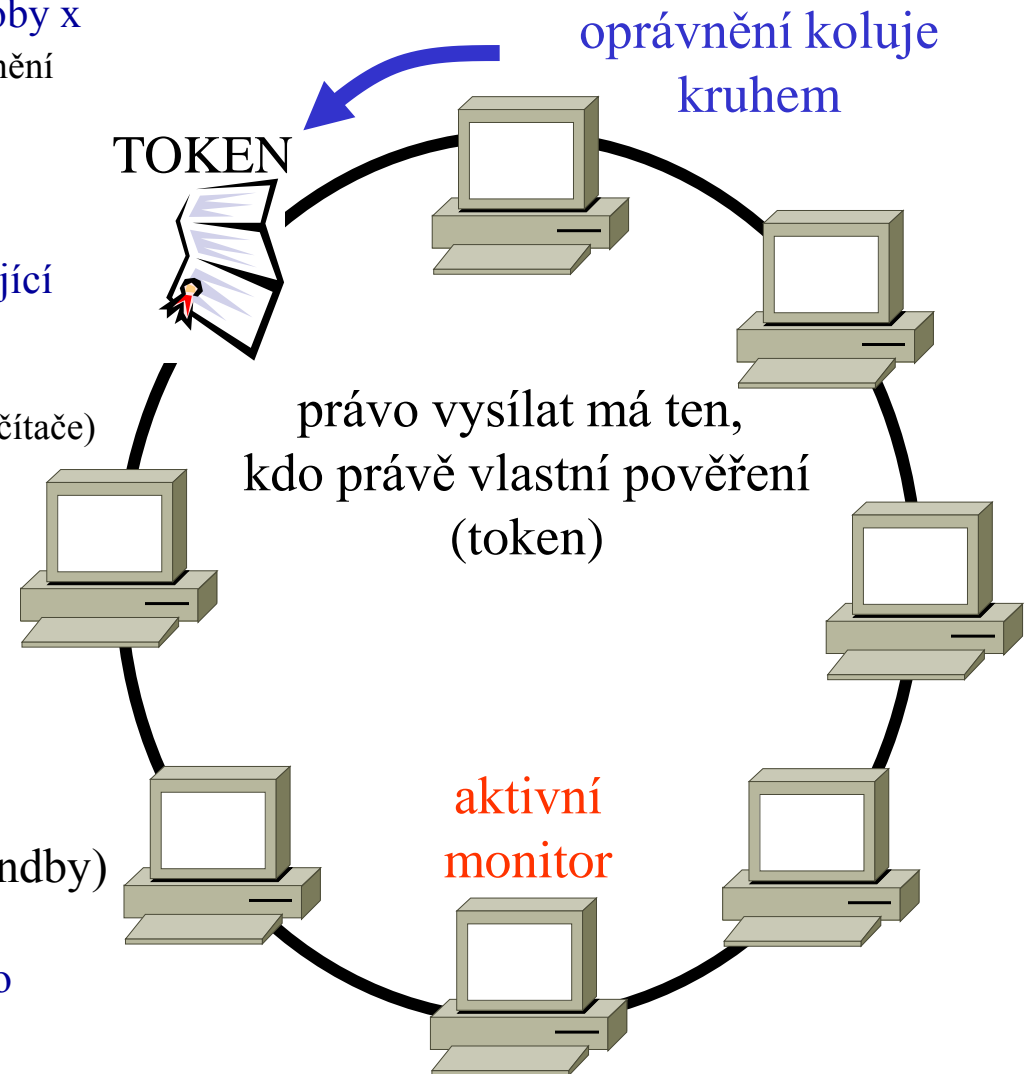
metody „logického kruhu“

- též: metody s předáváním pověření
 - anglicky: Token Passing
 - idea: vysílat může pouze držitel oprávnění
 - oprávnění (token) si jednotlivé uzly disciplinovaně předávají
- token (oprávnění, „pešek“)
 - dává držiteli právo vysílat
 - na věcné podstatě oprávnění (moc) nezáleží
 - bývá to speciální „balíček dat“
- kruh je pouze logický!!!!
 - jde o pořadí, v jakém si uzly oprávnění předávají
 - nemusí to nijak souviset se skutečnou topologií!!!
 - skutečná topologie může být například sběrnicová, stromovitá apod.
- příklady:
 - Token Ring (IBM)
 - Token Bus
 - FDDI
 -



logický kruh – metoda Token Passing

- možnosti:
 - lze garantovat právo k vysílání do doby x
 - když si každý z n uzlů podrží oprávnění nejdéle po dobu x/n
 - lze podporovat i priority
- předpoklady:
 - musí být definována pravidla ošetřující singulární situace, typu:
 - ztráta oprávnění
 - přistoupení nového uzlu (zapnutí počítače)
 - vystoupení z logického kruhu
 -
- vždy jeden z uzlů je v roli tzv. **aktivního monitoru**
 - má řídicí funkce,
 - řeší nestandardní situace
 - rozhoduje ...
- ostatní uzly jsou v roli záložních (standby) monitorů
 - jsou připraveny převzít roli aktivního monitoru

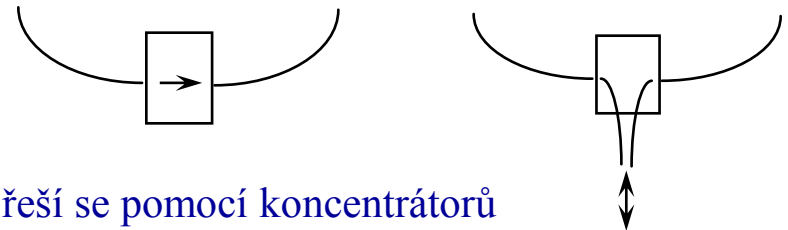


udržování (logického, fyzického) kruhu

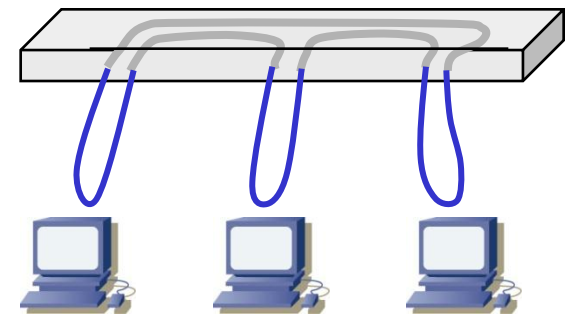
- přidávání nových uzlů:
 - každý uzel má pevně danou adresu
 - uzly jsou v logickém kruhu uspořádány podle adres
 - každý uzel pravidelně vysílá výzvu typu „připoj se“, určenou novým uzlům
 - udává adresu svou a svého následníka
 - vyzývá nově příchozí uzel s adresou „mezi“
 - pokud se ozve 1 nový uzel, OK
 - pokud se ozve více, řeší se následně jinak
- inicializace kruhu, ztráta tokenu:
 - uzel který po definovanou dobu nezaznamená žádný provoz usoudí, že je sám
 - vyšle výzvu „claim token“ (chci generovat oprávnění)
 - pokud nikdo nezareaguje (neprotestuje), vygeneruje oprávnění a vytvoří 1-členný logický kruh
 - „protesty“ se řeší rozpočítáním podle adres (á la prioritní přístup)

- problém s fyzickým přerušením (fyzického, logického) kruhu

- řeší pomocí tzv. bypass-ů
 - technické zařízení, při odpojení uzlu zajistí zachování kruhu – propojí rozpojené větve

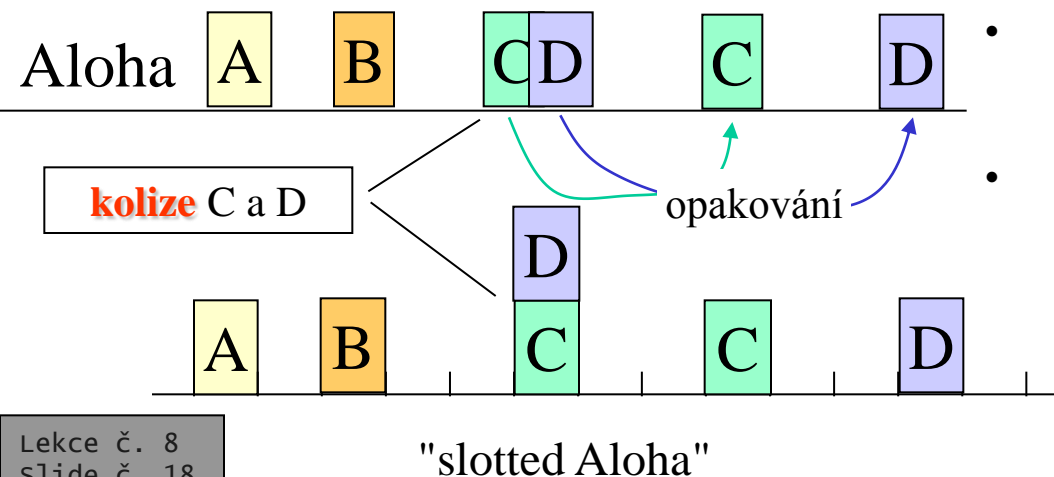
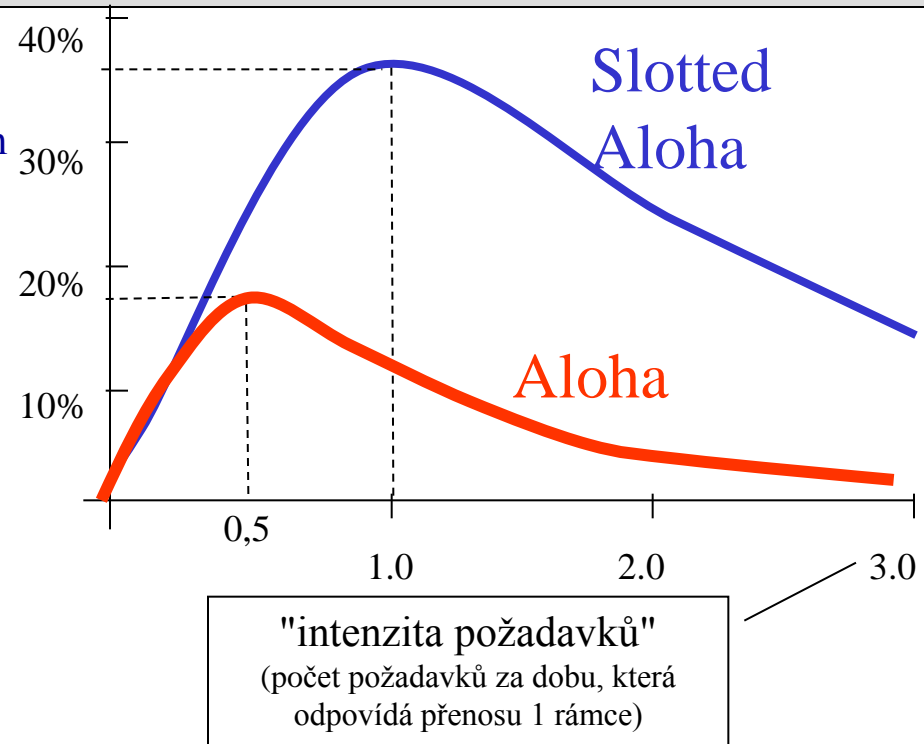


- řeší se pomocí koncentrátorů
 - nahrazují "externí" kruhovou topologii "interní" kruhovou topologií
 - analogie bypassu je realizována uvnitř koncentrátoru, elektronickou cestou
 - stačí odpojit příslušný uzel



neřízené distribuované metody - Aloha

- metoda Aloha (tzv. „čistá“)
 - vznikla na univerzitě na Havajských ostrovech
 - potřebovali přenášet data mezi ostrovy, neměli vhodnou infrastrukturu
 - využívá rádiového přenosu
 - přenosu „éterem“, jedním společným kanálem se všesměrovým šířením
 - nesnaží se monitorovat stav přenosového kanálu (zda právě někdo jiný vysílá) !!!
 - strategie (fungování přístupové metody):
 - odešli když potřebuješ (na nikoho se neohlížeš)
 - pokud nedostaneš včas potvrzení, opakuješ

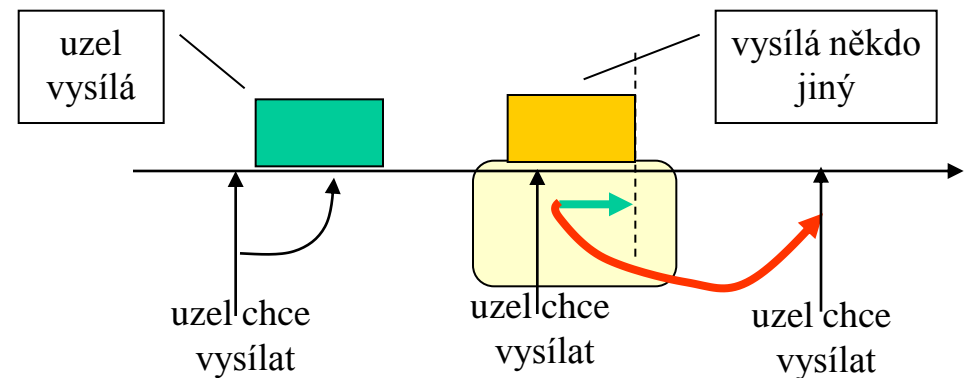


- potvrzování
 - zda byl přenos úspěšný, se pozná až podle toho, že druhá strana potvrdí příjem
- slotted Aloha
 - "éter" je rozdělen časovým multiplexem na sloty odpovídající velikosti rámců
 - uzel může začít vysílat vždy jen na začátku slotu
 - ke kolizi buď nedojde vůbec, nebo se "setkají" celé rámce
 - efektivnost max. do 36%

metody CSMA - persistentnost

- „čistá“ Aloha nemonitorovala provoz na kanále
 - nerozpoznala, že už někdo vysílá
- metody **CS** (Carrier Sense) využívají možnosti „odposlechu nosné“
 - vzdálenost (doba) přenosu je tak malá, že lze rozpoznat "právě probíhající" vysílání
- využití příposlechu (chování uzlu):
 - poslouchej nosnou, a pokud nikdo nevysílá, můžeš začít vysílat sám
- efekt:
 - předchází se tak kolizím
 - ale kolize stále nejsou vyloučeny!!
 - pouze se tím snižuje jejich počet
- otázka:
 - *co dělat, když zájemce o vysílání zjistí, že právě vysílá někdo jiný (že kanál je obsazen)?*

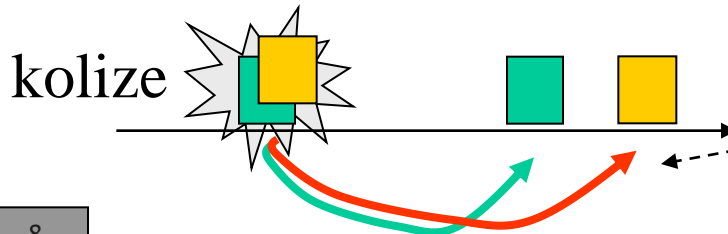
- možnosti:
 - **persistentní chování**: čeká, až vysílání skončí, a pak začne vysílat
 - **0-persistentní, ne-persistentní**: odmlčí se na delší dobu



- **p-persistentnost**:
 - s pravděpodobností **p** **vytrvá** (čeká)
 - s pravděpodobností **1-p** to **vzdá** (odmlčí se)

metody CD (Collision Detect)

- snaží se detekovat výskyt kolizí
 - metody „bez CD“ pokračují ve vysílání, i když ke kolizi došlo
 - tím se zbytečně plýtvá přenosovou kapacitou
 - metody CD využívají schopnost detekce k (téměř) okamžitému ukončení vysílání
 - detekce kolize je analogová záležitost
 - ve skutečnosti se vysílání, způsobující kolizi, nesmí okamžitě ukončit
 - musí ještě určitou dobu trvat, aby jej stihly zaznamenat také ostatní uzly v segmentu (v tzv. kolizní doméně)
 - Ethernet: místo dat se vysílá tzv. **jam signál** (utvrzující kolizi)
- obecně:
 - CSMA/CD je celá skupina přístupových metod
 - CS – s příposlechem nosné
 - MA – s vícenásobným přístupem
 - CD – s detekcí kolizí
 - rozdíl může být např. v persistentnosti
 - jak se uzly chovají, když zjistí že právě probíhá nějaké vysílání
 - nebo v reakci na výskyt kolize
 - jedna konkrétní „instance“ je dle IEEE 802.3 (v Ethernetu)
 - přístupová metoda Ethernetu je typu CSMA/CD
 - je 1-persistentní
 - teprve při zjištění kolize se uzel, zúčastněný v kolizi, odmlčí na náhodně zvolenou dobu

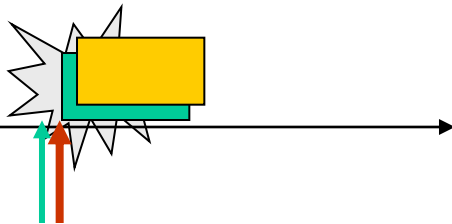


metody CSMA/CD - důvody vzniku kolizí

- kdy může dojít ke kolizi:

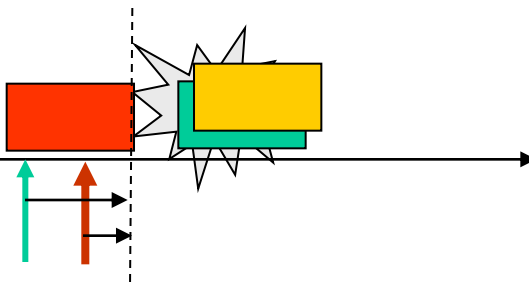
- více uzlů (zájemců o vysílání) současně zjistí, že nikdo nevysílá, a začne vysílat

méně
časté



- více uzlů čeká, až někdo jiný přestane vysílat, a pak začnou všichni najednou

dostí
časté



- jak předcházet "kolizím z netrpělivosti"?

- situaci, kdy více uzlů čeká na ukončení stávajícího vysílání, a pak „spustí“ všichni najednou:

- ať nejsou všichni tak nedočkaví !!!

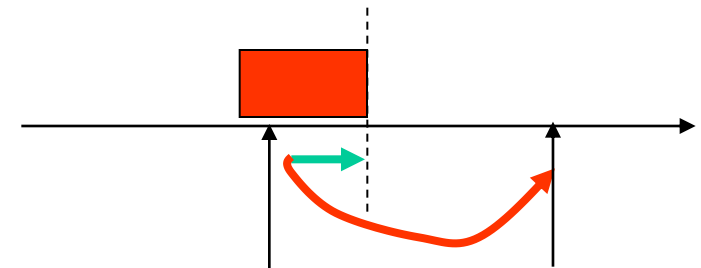
- ať ihned upustí od svého požadavku a odmlčí se na náhodnou dobu

- tj. zkusí to později

- jde o 0 persistentnost

- ať s určitou pravděpodobností ustoupí od svého požadavku (odmlčí se)

- jde o p-persistentnost

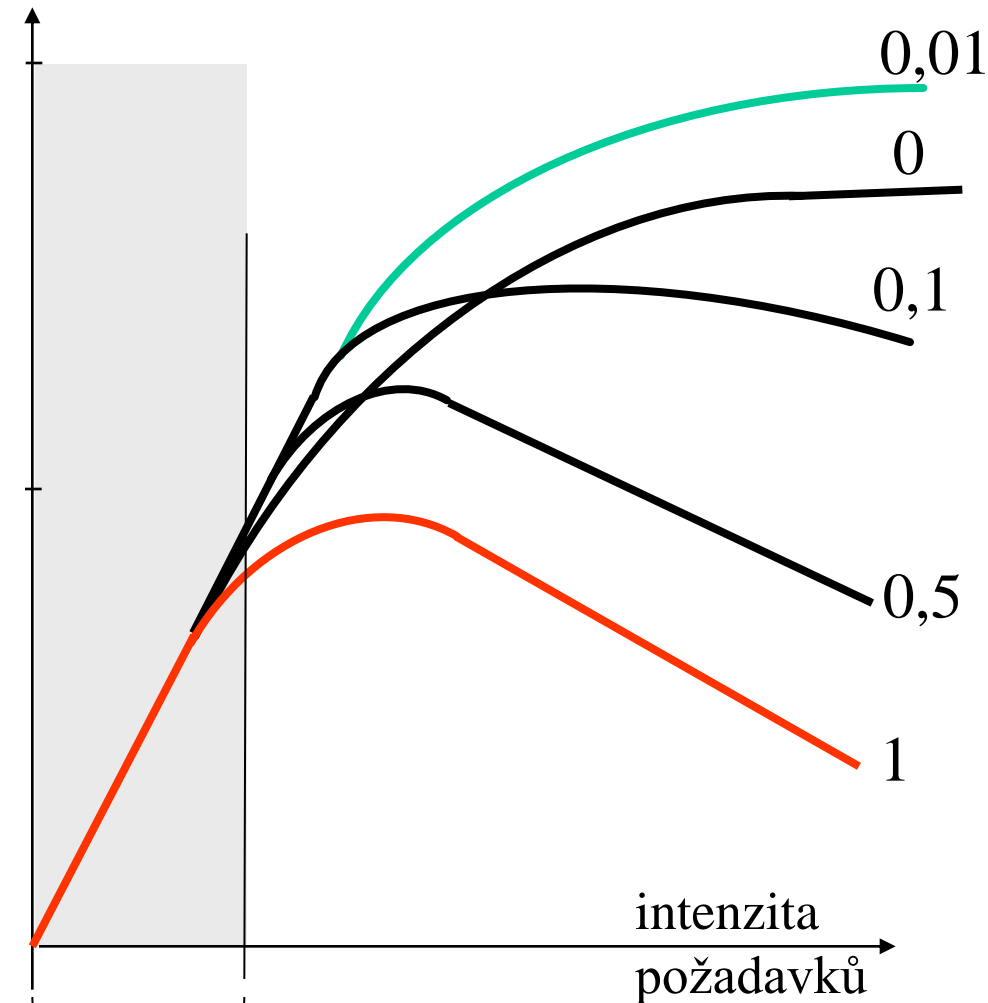


metody CSMA podle persistentnosti

připomenutí:

- nepersistentní (0-persistentní) CSMA:
 - podívá se, jestli někdo vysílá
 - pokud ano, ihned se odmlčí na náhodně zvolenou dobu (počká)
- p-persistentní CSMA
 -
 - s pravděpodobností p čeká na konec vysílání,
 - s pravděpodobností $1-p$ se odmlčí na náhodně zvolenou dobu
- 1-persistentní CSMA:
 -
 - neodmlčí se, čeká na konec vysílání
- společné přenosové médium nejlépe vytěžují metody s velmi nízkou persistentností
 - naopak 1-persistentní metoda je na tom nejhůře !!!

míra využití přenosového média

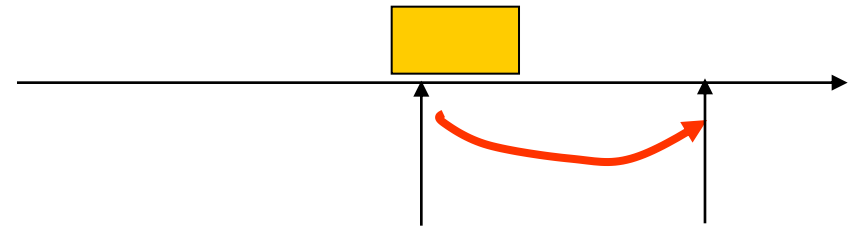


předpokládá se využití v této oblasti (nízké využití)

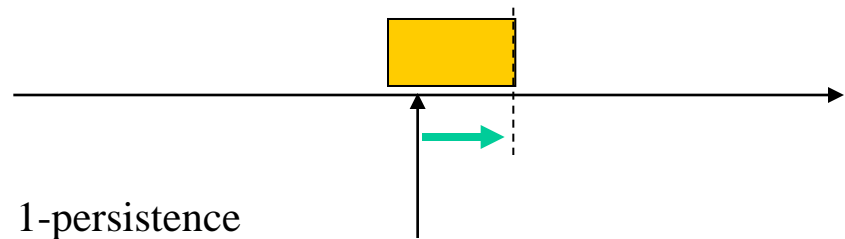
proč je Ethernet 1-persistentní?

- autoři Ethernetu znali "křivky výtěžnosti" (předchozí slide)
 - věděli, že 1-persistence nejhůře vytěžuje sdílené přenosové médium
- přesto si vybrali 1-persistentnost!!
- důvod:
 - nešlo jim tolik o vytížení přenosového média
 - předpokládali relativně slabý provoz
 - dbali také na latenci
 - za jak dlouho se uzel dostane k vysílání
 - od okamžiku, kdy o to projeví zájem
 - zde je jednoznačně výhodnější 1-persistence
 - uzel to "nevzdává zbytečně"

- příklad: 0-persistence



- uzel, který chce vysílat, ale zjistí že právě probíhá jiné vysílání, se ihned odmlčí na náhodně zvolenou dobu
 - s vysokou pravděpodobností to vzdává zbytečně !!!!
 - pravděpodobnost, že by čekal na konec vysílání společně s jiným uzlem, a pak se dostali do kolize, je relativně nízká!!
 - kdyby vytrval, mohl se dostat ke slovu dříve



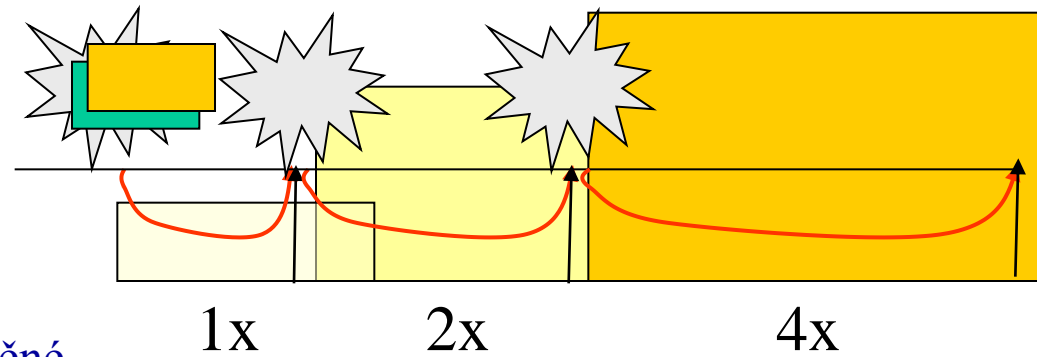
- 1-persistence

- riskuje, že se na konci právě probíhajícího vysílání dostane do kolize s jiným "čekajícím uzlem"
- ale vzhledem k předpokladu nízkého provozu je pravděpodobnost malá – a uzel se dostane ke slovu rychle

řešení kolizí (v metodách CSMA/CD)

- snaha kolizím předcházet
 - pouze snižuje četnost kolizí, ale nedokáže je eliminovat
- co dělat, když už ke kolizi dojde?
 - pokud by se všechny uzly, zúčastněné v kolizi, zachovaly stejně, pak by zákonitě došlo k další (následné) kolizi
- jak se vyhnout následným kolizím?
 - uzly se mezi sebou nemohou domluvit
 - nemají jak/čím
 - proto musí nastoupit "náhodný prvek"
 - uzel se odmlčí na náhodně zvolenou dobu, a teprve pak se pokouší o vysílání znovu

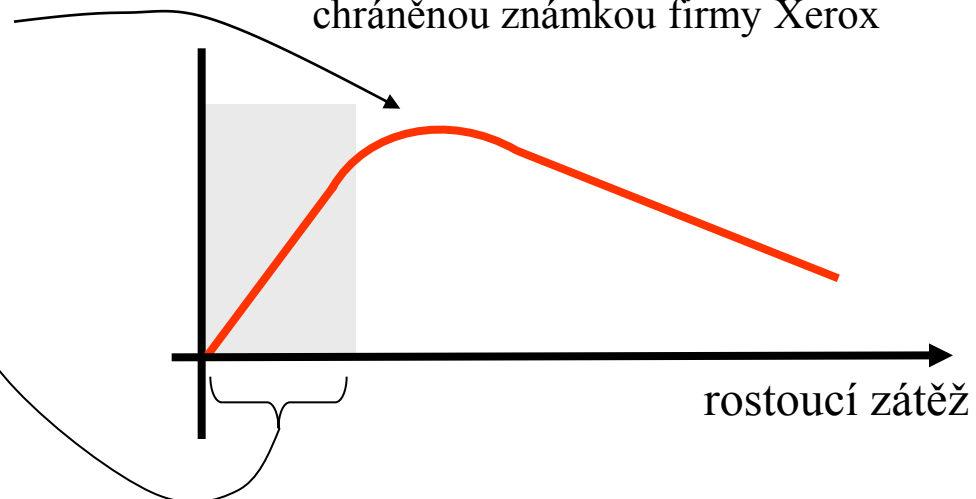
kvůli tomu jde o neřízenou (nedeterministickou) metodu



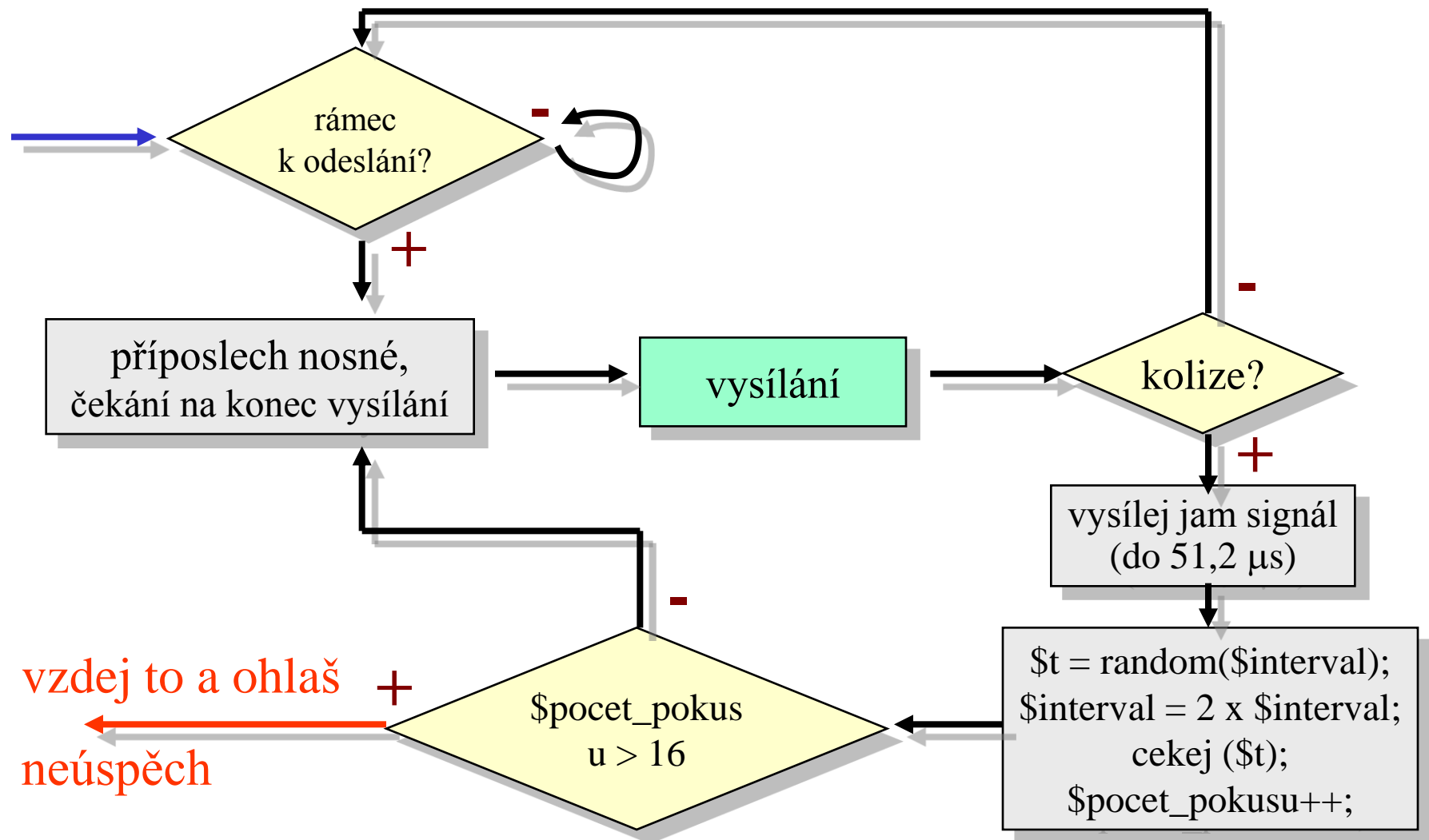
- "náhodě je třeba pomoci"
 - pouhé odmlčení na náhodnou dobu nemusí stačit
 - následným kolizím stále nezabraňuje
 - používá se "zesílení náhody"
 - zvětšuje se interval, ze kterého si uzel náhodně volí délku svého odmlčení
 - při každé následné kolizi se tento interval zdvojnásobí
 - při úspěšném odvysílání se zase vrátí na původní hodnotu
 - v Ethernetu: opakuje se 16x, pak to uzel vzdá
 - tzv. **binary backoff**

obecné vlastnosti metod CSMA/CD

- nezaručují výsledek
 - že zájemci se v konečném čase podaří odvysílat
 - kvůli náhodnému prvku (jsou neřízené)
 - následné kolize se mohou opakovat libovolně dlouho, byť pravděpodobnost rychle klesá
- mohou být velmi efektivní
 - v případě nižší zátěže mají téměř nulovou režii
- při vyšší zátěži vykazují nestabilitu
 - zvyšování intenzity požadavků vede na horší chování metody
 - předpokládalo se, že budou využívány při nízké zátěži sítě
 - dnes nebývá vždy splněno!!
- Ethernet
 - používá přístupovou metodu CSMA/CD
 - 1-persistentní metodu (CSMA) s detekcí kolize (CD)
 - standard pro Ethernet vydala a udržuje IEEE a její pracovní skupina 802.3
 - místo "Ethernet" se říká "*sítě na bázi CSMA/CD*"
 - jméno Ethernet bylo původně chráněnou známkou firmy Xerox



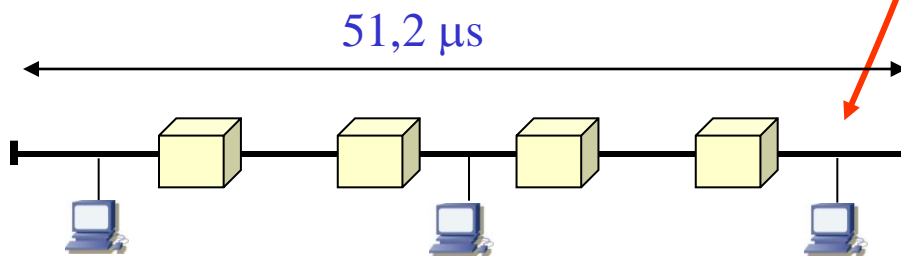
stavový diagram přístupové metody CSMA/CD v Ethernetu



vzdej to a ohlaš
neúspěch

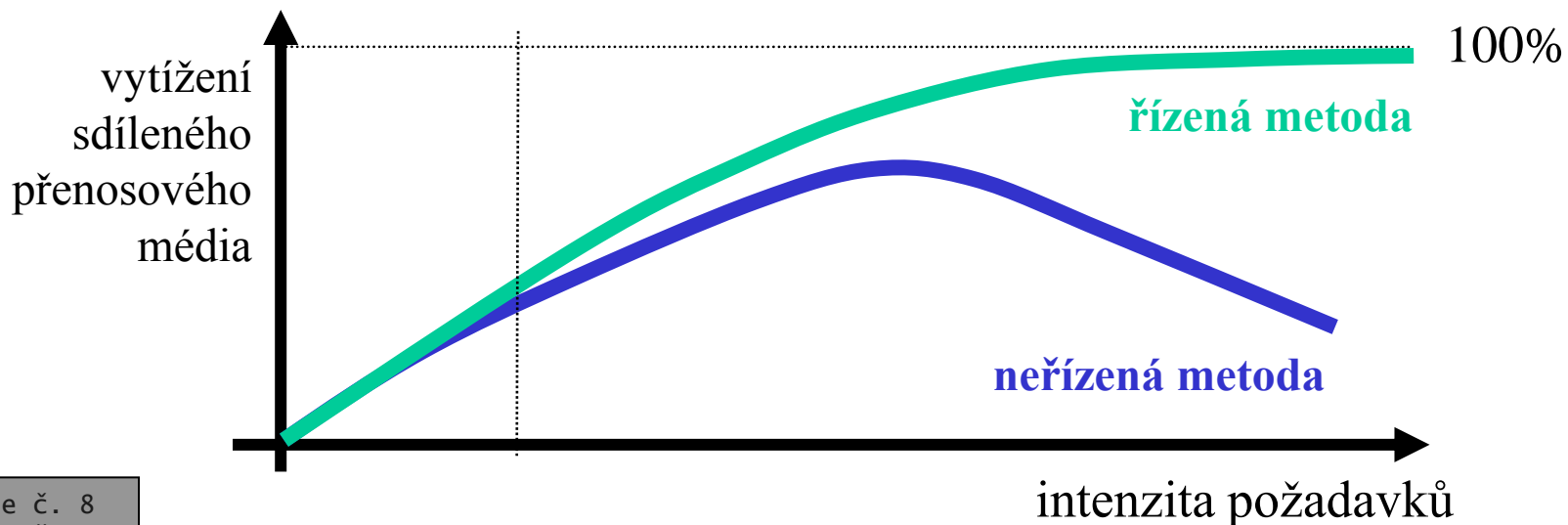
kolizní domény v (10 Mbit/s) Ethernetu

- kolize v Ethernetu se šíří přes tzv. opakovače (repeater-y)
 - "zastavují se" až na mostech, přepínačích, směrovačích atd.
- kabelové segmenty, spojené pomocí opakovačů, tvoří tzv. kolizní doménu
- fungování přístupové metody Ethernetu (CDMA/CD) vyžaduje, aby se "informace o kolizi" rozšířila po celé kolizní doméně v určitém maximálním čase
 - tento čas je definován standardem: 51,2 μ s
 - při přenosové rychlosti 10 Mbps to odpovídá 512 bitům, alias 64 bytům
- důsledky:
 - velikost kolizní domény je omezena
 - aby se "stihlo" 512 bitů (51,2 μ s)
 - omezen je počet opakovačů v kolizní doméně
 - pravidlo 5:4:3
 - max. 5 segmentů, max. 4 opakovače, max. 3 "obydlené segmenty"
 - uzel, který vysílá a dostane se do kolize, nesmí hned přestat vysílat
 - musí zajistit, aby se informace o kolizi dostala do všech "koutů" kolizní domény
 - pokračuje vysíláním speciálního "jam signálu", do konce intervalu 51,2 μ s od začátku vysílání
 - uzlu, který vysílá, stačí monitorovat dění na přenosovém médiu po dobu 51,2 μ s (prvních 512 bitů přenášeného rámce)
 - později už nemůže dojít ke kolizi



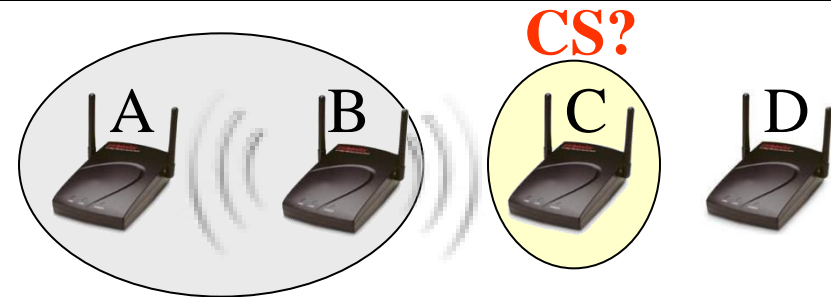
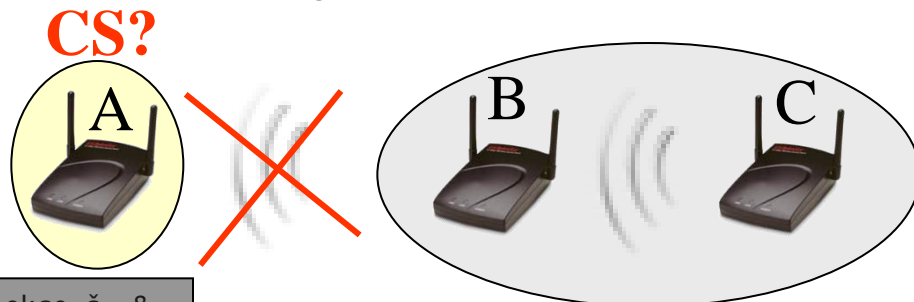
srovnání Ethernet vs. Token Ring

- jde hlavně o rozdíl mezi řízenou a neřízenou přístupovou metodou
 - neřízené přístupové metody (např. CSMA/CD) fungují lépe v menších sítích s nízkým využitím
 - malými objemy provozu
 - a jsou jednoduché
 - řízené metody (např. Token Passing) fungují lépe ve větších sítích s větším provozem
- jiné kritérium: doba odezvy
 - od požadavku na přenos do zahájení vysílání
- u řízených metod je doba odezvy méně závislá na intenzitě provozu
 - u neřízených se více mění v závislosti na provozu
 - při překročení určité limitní zátěže roste nade všechny meze



přístupové metody v bezdrátových sítích

- v čem jsou bezdrátové sítě specifické?
 - větší rušení/porychy/chybovost v přenosovém kanále ("éteru")
 - příposlech nosné (CS) nemusí být spolehlivý
 - na rozdíl od "drátových" sítí
- problém skryté stanice
 - médium je "obsazeno", ale uzel se to nedozví
 - příklad: A chce vysílat k B, ale "neslyší" že C právě vysílá k B
 - signál od C už nedosáhne k A



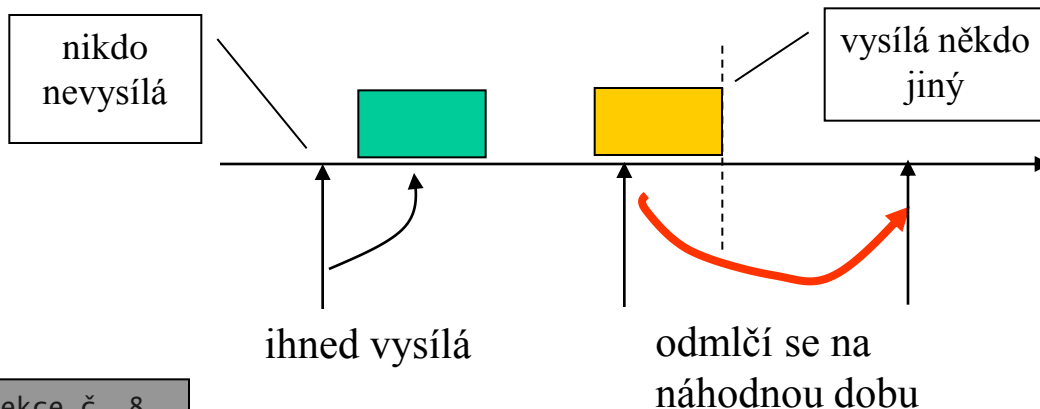
- problém předsunuté stanice
 - médium je fakticky volné, ale uzel se dozví, že je obsazeno
 - příklad: B vysílá k A, C by chtěl vysílat k D – ale zjistí, že B vysílá a domnívá se, že je médium obsazeno
- nelze detekovat kolize během vysílání
 - rádiová (RF) rozhraní jsou typicky pouze poloduplexní, a neumožňují proto současně přijímat i vysílat!!!
 - metody ..CD nepřípadají v úvahu

přístupové metody sítí Wi-Fi (802.11)

- není jedna, ale je jich několik
 - volitelných vs. povinných
 - centralizovaných vs. distribuovaných
- **DCF (Distributed Coordination Function)** – povinná varianta
 - nemá žádný centrální prvek/autoritu
 - varianta CSMA/CA
 - povinná
 - varianta CSMA/CA s výměnou RTS/CTS
 - volitelná, implementovaná v "lepších" produktech
- **PCF (Point Coordination Function)** – volitelná varianta
 - AP řídí veškerou komunikaci, ke kolizím vůbec nedochází
 - v praxi není (moc) implementováno
- používá se potvrzování
 - kvůli poloduplexního způsobu fungování rádiového rozhraní vysílající uzel nepozná, že došlo ke kolizi
 - nedozví se, že by měl přenos opakovat
 - rámec se odvysílá vždy celý
 - ale může se poškodit/ztratit i z jiných důvodů, než jen kvůli kolizi
 - např. kvůli rušení
 - řešení:
 - příjemce musí přijetí rámce explicitně potvrdit
 - posílá speciální potvrzovací rámec (ACK)

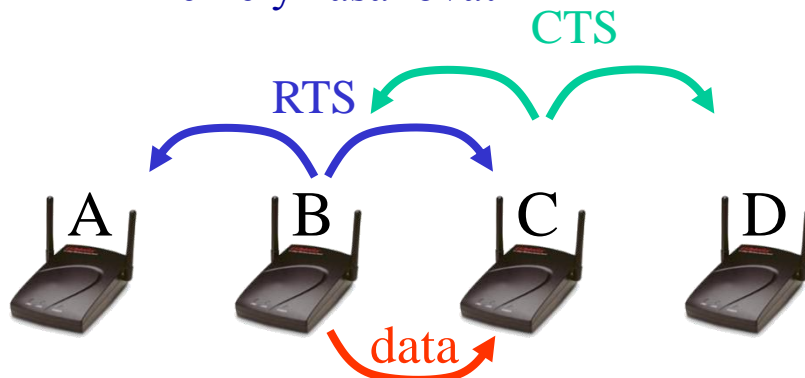
metoda DCF CSMA/CA (povinná)

- CS: zájemce o vysílání sleduje, zda právě probíhá nějaké vysílání
 - pokud ne, začne hned vysílat sám
 - odvysílá celá rámeček, aniž by monitoroval eventuelní kolize
 - jeho rádiové rozhraní je poloduplexní
 - čeká na potvrzení (ACK)
 - pokud právě probíhá nějaké vysílání, odmlčí se na náhodnou dobu
 - je to 0-persistence !!!!
 - pokud během čekání probíhá nějaké vysílání, odpočítávání doby čekání je pozastaveno!!
- používá se u všech Wi-Fi zařízení, včetně těch nejlacinějších
 - v režimu ad-hoc i v režimu infrastruktury
 - nedokáže garantovat výsledek
 - uzel se nemusí dostat "ke slovu"
 - nedokáže garantovat QoS
 - nedokáže vyhradit určitou část přenosové kapacity konkrétním uzlům
 - je to CA (Collision Avoidance)
 - ke kolizím může docházet
 - ale nevyhodnocují se
 - fungování je narušováno efektem "skryté stanice" a "předsunuté stanice"



metoda CDF CSMA/CA s RTS/CTS

- volitelná varianta
 - vyskytuje se u "lepších" (dražších) provedení Wi-Fi zařízení
- princip:
 - snaha eliminovat problémy skryté a předsunuté stanice
 - snaha upozornit "ostatní" uzly na to, že po určitou dobu bude probíhat přenos, a že by do něj neměly zasahovat

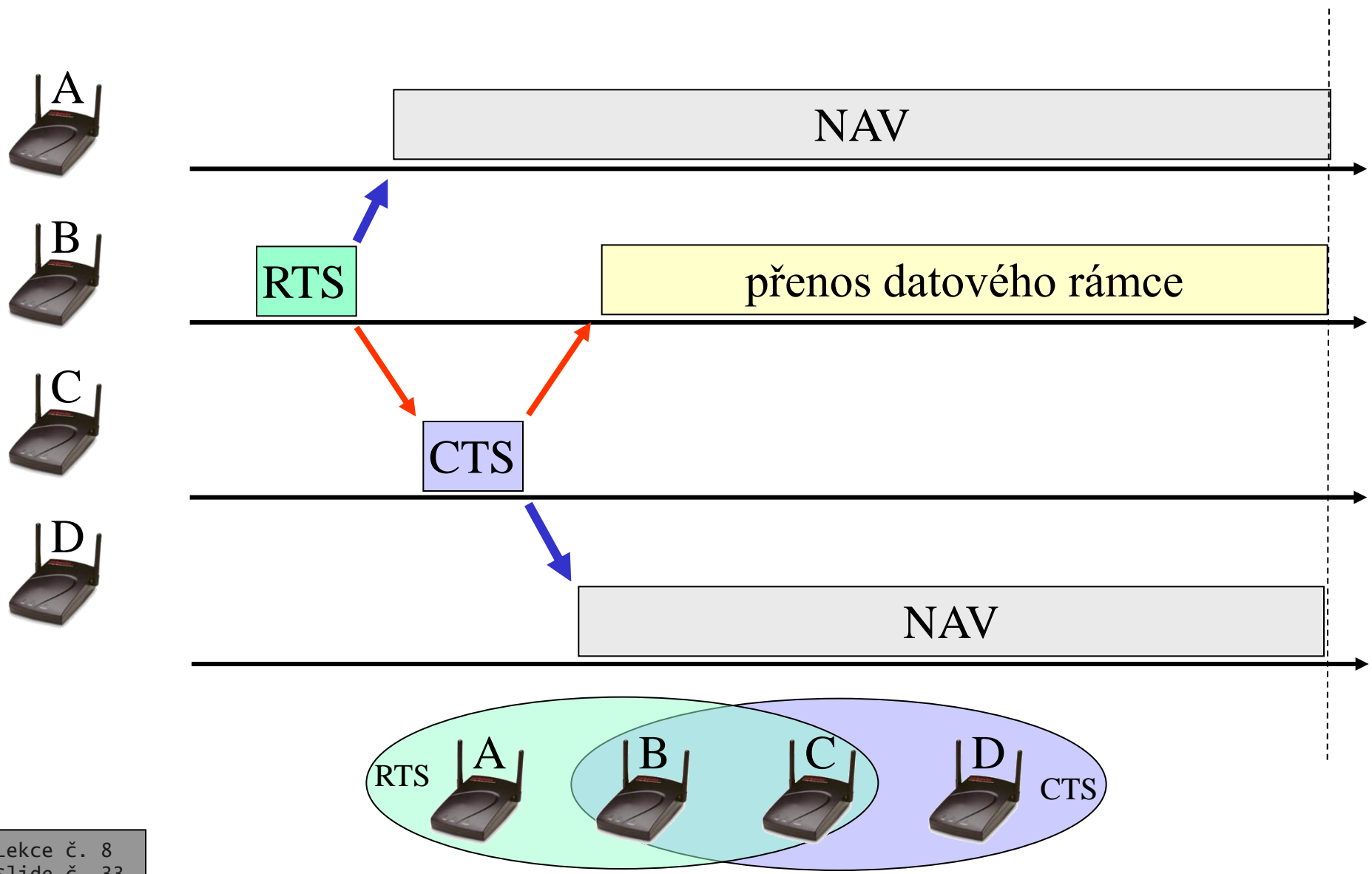


- B chce něco odvyšlat k C:
 - snaží se "vyřadit" A a D, aby do toho nevstupovali

- postup:

- B vyšle krátký rámec RTS, určený pro C
 - RTS – Request To Send
 - žádá jej o právo vysílat k uzlu C
 - říká jak dlouho bude vysílání trvat
- tento RTS rámec by měly zachytit ostatní uzly v okolí uzlu B (např. A)
 - měly by si z něj odvodit, jak dlouho bude B vysílat
 - nastaví si "stopky", v podobě vektoru NAV
 - Network Allocation Vector
- C odpoví krátkým rámcem CTS
 - CTS – Clear To Send
 - signalizuje připravenost k příjmu,
 - říká, jak dlouho bude přenos trvat
- tento CTS rámec by měly zachytit ostatní uzly v dosahu uzlu C (např. D)
 - nastaví si svůj NAV
- pak probíhá samotný datový přenos
 - ostatní uzly čekají na konec vysílání (podle "stopek" v podobě vektoru NAV)
 - během čekání se ostatní uzly nesnaží samy vysílat

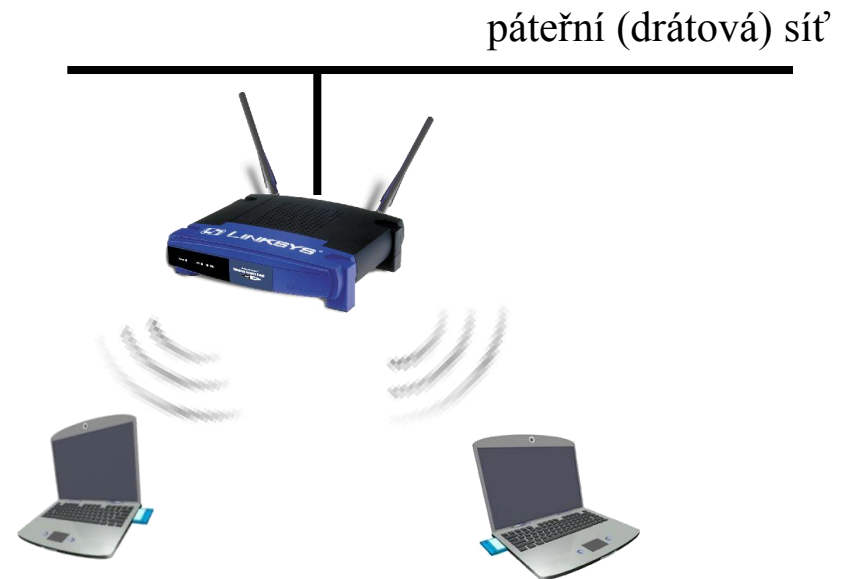
představa CSMA/CA RTS/CTS



varianta PCF (Point Coordination Function)

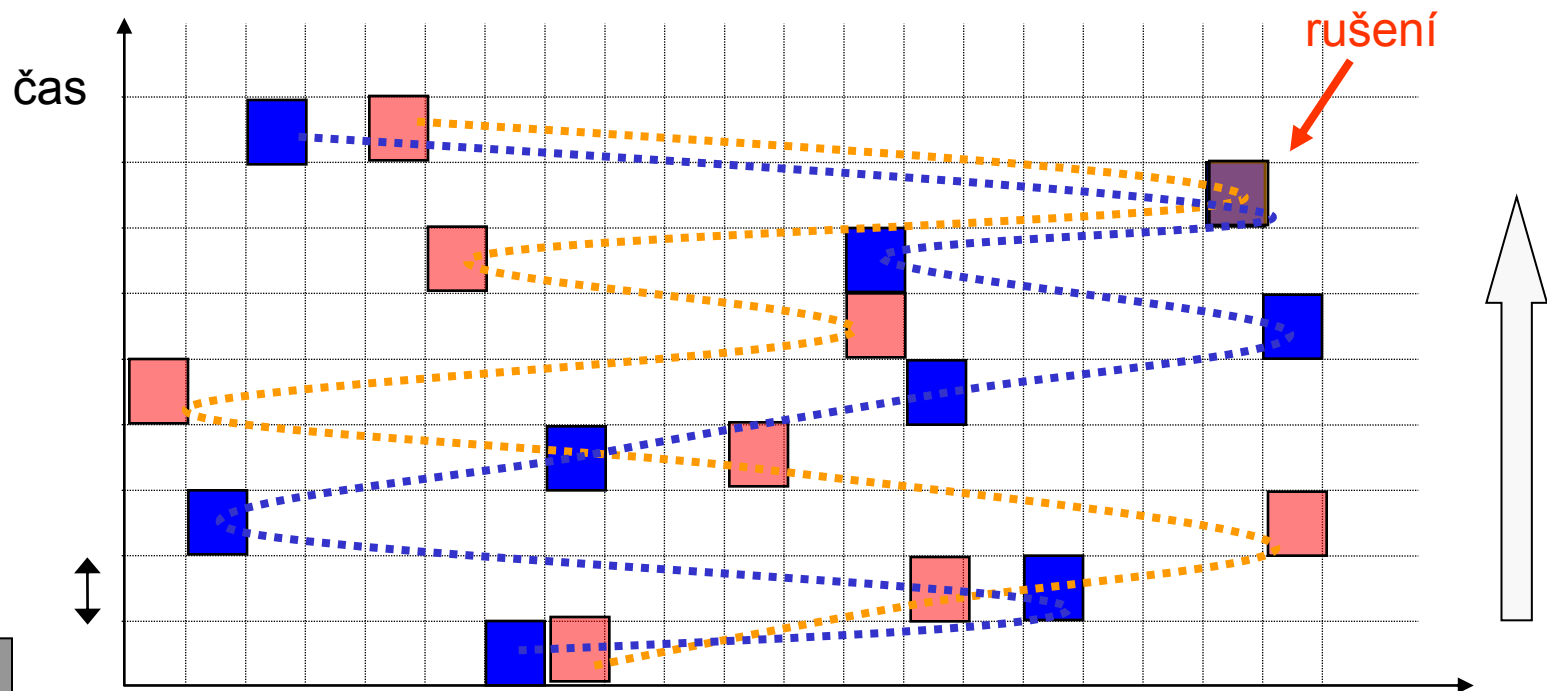
- je to volitelná varianta
 - není (dosud moc) implementována
- má centralizovaný charakter
 - veškerou komunikaci řídí Access Point
 - v režimu Infrastructure
 - přidělování přenosové kapacity probíhá na principu rezervace
 - AP pravidelně vysílá rezervační rámec, skrze který mohou uzly žádat o právo vysílat
 - lze tak realizovat i QoS
 - garantovat parametry, přidělovat přenosovou kapacitu

- varianty DCF a PCF mohou koexistovat vedle sebe!!!
 - dosahuje se toho vhodně volenými časovými odstupy mezi vysíláním rámců podle jednotlivých variant
 - tzv. InterFrame Spacing
 - "přednost" (kratší odstupy) mají rámce PCF



Bluetooth – řízení přístupu

- nemá klasickou přístupovou metodu
- místo ní používá velmi rychlé přeskokování mezi frekvencemi
 - 1600x za sekundu (každých 625 μ s)
 - spoléhá se na to, že případné kolize budou velmi krátké (625 μ s) a bude jich velmi málo
- návrh technologie Bluetooth byl přizpůsoben spíše potřebám přenosu hlasu
 - kde občasné velmi krátké výpadky (kvůli kolizím) nejsou znatelné
 - pro přenos dat je to větší problém, ale dá se řešit



řízení přístupu v kabelových sítích

- architektura kabelové sítě je sice stromovitá, ale chová se jako sběrnice!!

- má centrální prvek: CMTS

- Cable Modem Termination System
- dopředný kanál (downstream) se chová jako broadcastové médium
- vysílá pouze CMTS
- přijímají současně všechny kabelové modemy (ve skupině)

- zpětný kanál je sdílený

- a pro jeho využití je nutná přístupová metoda

- přenos dat je realizován podle standardu euroDOCSIS

- přístupová metoda je centralizovaná

- o všem rozhoduje CMTS

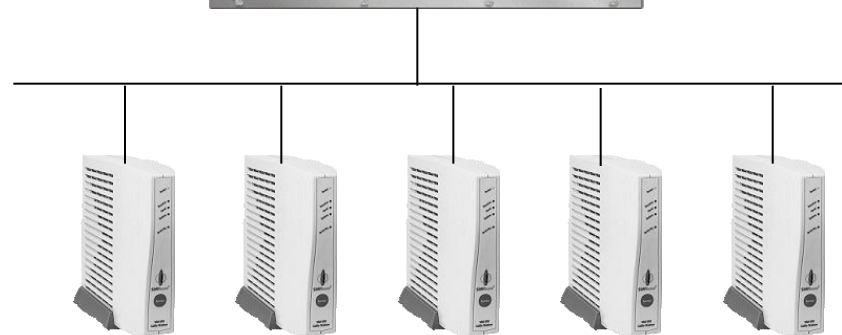
- na rezervačním principu

- vše funguje synchronně

- používají se časové (mini)sloty, vytvářené pomocí TDM



CMTS



- CMTS pravidelně vysílá "rámeček s výzvami"

- modem, který chce vysílat, vyznačí svůj požadavek do příslušného (mini)slotu
- CMTS mu odpoví a určí kdy bude moci vysílat na zpětném kanále

- rezervační (mini)slot je sdílen více modemy

- žádosti se mohou dostávat do kolize
- pokud modem nedostane odpověď od CMTS v obvyklém čase, odmlčí se na náhodně zvolenou dobu (při opakování ji prodlužuje na dvojnásobek)