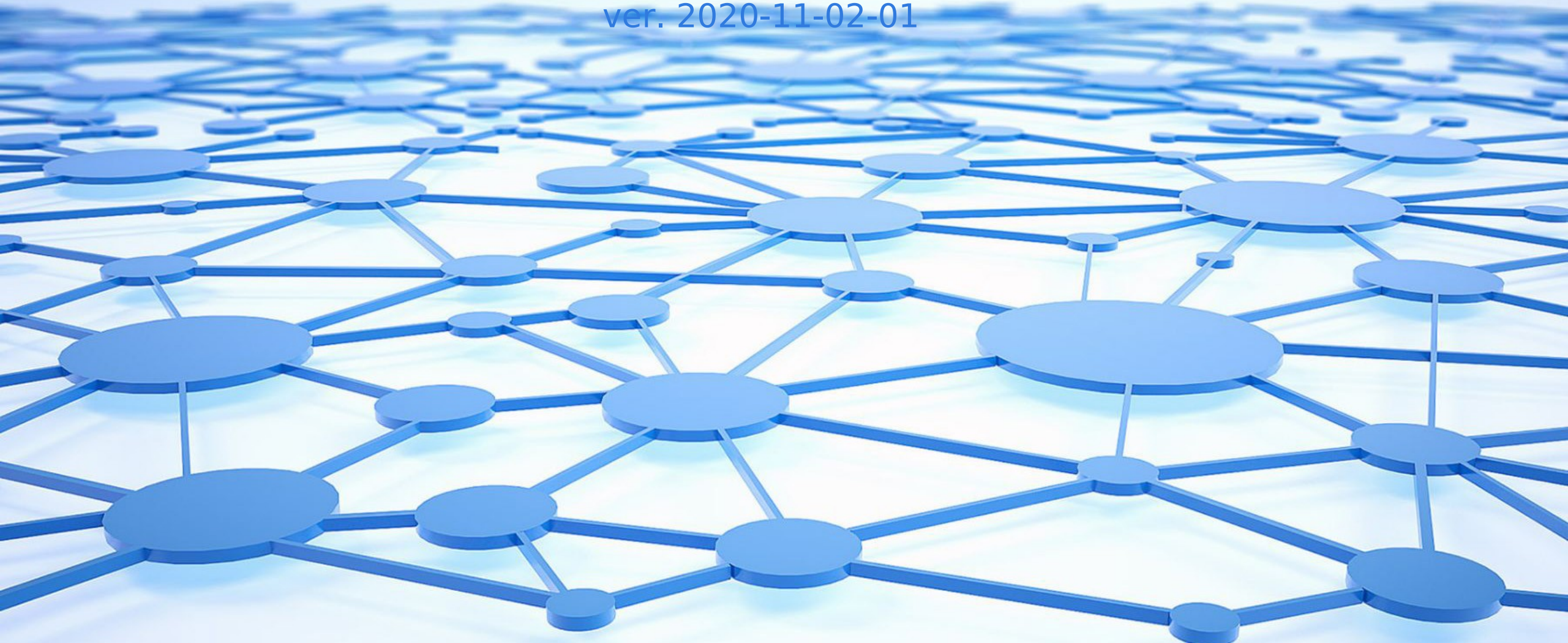
Úvod do počítačových sítí

Přednáška 7

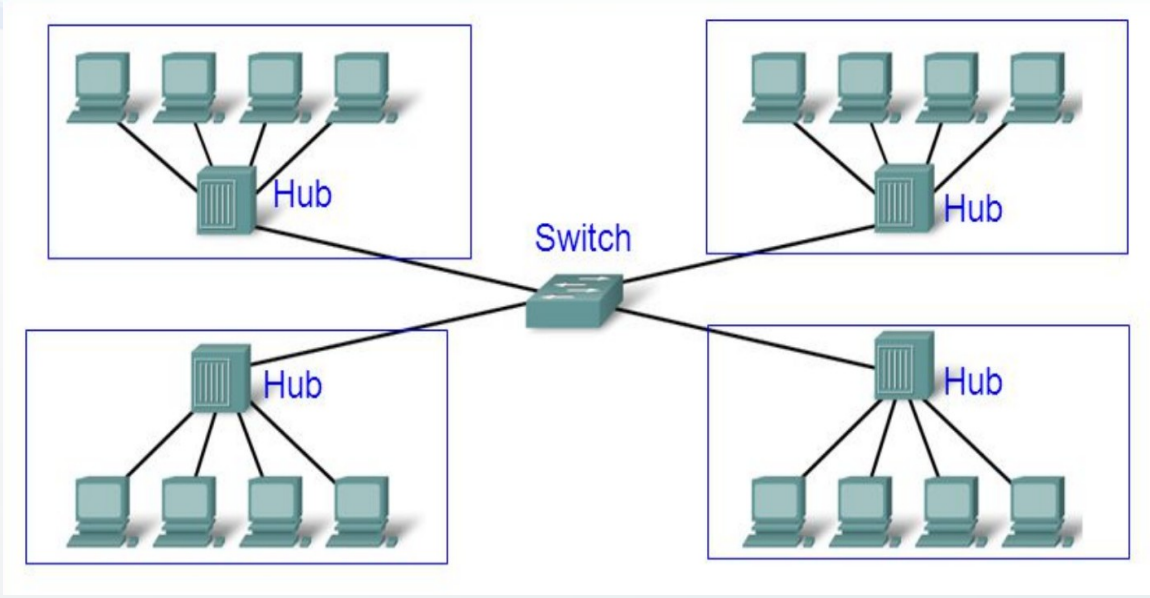
(2021/2022)

ver. 2020-11-02-01



Řízení přístupu

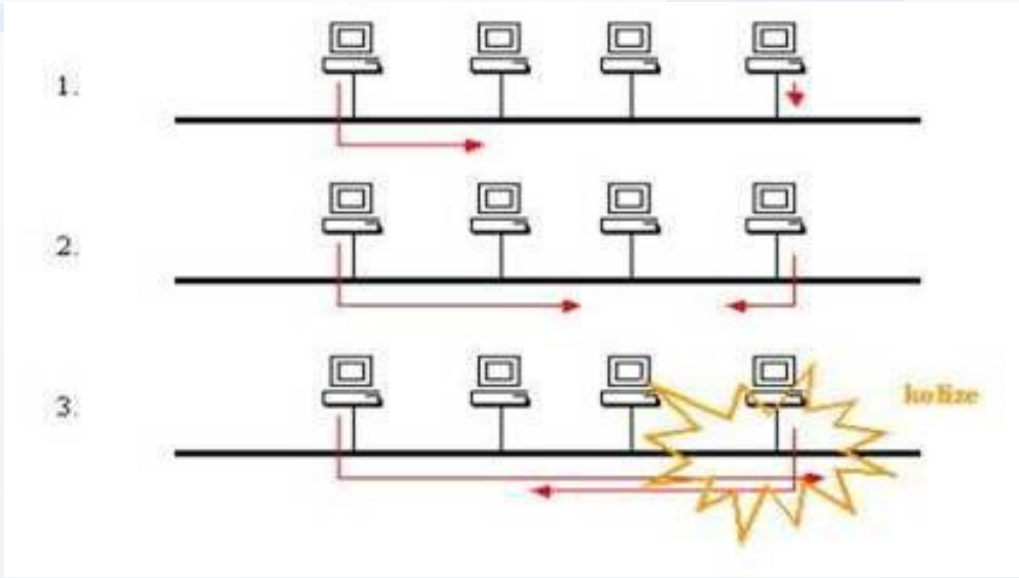
- MAC – Media Access Control
- Snažíme se vyřešit situaci, kdy N zařízení chce používat sdílený komunikační kanál
  - Bezdrátové sítě P-MP – Point to Multi-point
    - LAN: WiFi, Bluetooth
    - WAN: WiMAX, mobilní síť
  - Drátové sítě – bez ohledu na topologii či vodič
    - LAN: Ethernet, Token ring
    - WAN: DOCSIS
- Definujeme kolizní doménu – počet stanic, které mohou vzájemně kolidovat / oblast kde ke kolizi může dojít
  - HUB – všechny porty
    - Hub == více-portový opakovač
    - Vysílaná data vidí všichni, ale ne nutné ve stejný čas
  - Switch – vždy jen jeden port
    - Kolize může teoreticky nastat jen na jednom portu
    - Vysílání se nešíří na všechny porty
      - V rámci broadcastu ano, ale pak se jedná o kopii rámce na jednotlivé porty, ne o kopii signálu
- Na obrázku máme 4 kolizní domény
  - Každý port switche je jedna kolizní doména
  - Všechny porty každého hubu jsou v jedné kolizní doméně



zdroj: https://slideplayer.cz/slide/3101658/

Řízení přístupu: Kde je problém

- Problém je v „překrývání“ či „slučování“ signálů
  - Dva signály se potkají a z pohledu pozorovatele vznikne třetí - výsledný
- Pokud do společného kanálu začnou vysílat dvě stanice jejich vysílání se se vzájemně ovlivní a nebude možné je **zpětně oddělit**
- Vysílací stanice nemusí o kolizi ihned vědět
  - Signál není v jeden okamžik po celém komunikačním kanálu
    - Vliv zde hrají fyzikální vlastnosti, například rychlost šíření světla
  - Stanice odvysílá svá data a může mít „pocit“, že vše proběhlo správně, ale to nemusí být pravda



zdroj: http://pk-info.spsepn.edu.sk/studium/ucebtext/ele/siete/eth/ethernet.htm

Řízení přístupu versus multiplex

- Vypadá to podobně – více účastníků chce současně použít jeden komunikační kanál, ALE
  - Multiplex:
    - Je na fyzické vrstvě
    - Máme dva přístupové body a N účastníků
    - Účastníci jsou na jednom místě
    - Všichni se snaží přenést data z bodu A do bodu B stejným kanálem
  - Řízení přístupu:
    - Je na linkové vrstvě
    - Máme přenosový kanál – např sběrnici – a na ní N účastníků
    - Účastníci od sebe mohou být různě vzdáleni – signál k nim nedorazí ve stejný okamžik
    - Každý účastník může chtít přenášet data k různému cíli
      - A pro B, C pro D, D pro A

Řízení přístupu: Cíle

- Snažíme se o :
  - Předcházení kolizím
    - Předcházení problémům je téměř vždy „levnější“ než jejich následné řešení
  - Pokud už kolize nastane, potřebujeme to co nejdříve zjistit
    - Teprve když o problému víme, můžeme jej začít řešit
  - Pokud jsme zjistili, že nastala kolize je třeba zastavit vysílání a dát všem vědět o problému
    - Aby se minimalizoval čas, kdy se nepřenáší / přenáší již poškozená data
  - Snažíme se předcházet opakované kolizi
    - Pokud dvě stanice začnou vysílat v jeden okamžik dojde ke kolizi, pokud se následně vysílání přeruší – opět ve stejný okamžik - a znovu začne, situace se bude **pravděpodobně** opakovat

Typy přístupu k mediu: Nevýlučný

- Vysílací stanice nemá k mediu výlučný přístup – není sama kdo může vysílat
- Komunikační kanál sice sdílí s dalšími, ale má k němu trvalý přístup
- Metody nevýlučného přístupu jsou velice podobné metodám používaným v multiplexu či se dá říci, že z nich vycházejí
- Je možné garantovat přenosovou rychlost – logicky protože vím, kdy a jak budu přenášet
- Jde o princip přepojování okruhu, kdy „sestavím“ cestu a tou posílám data – proud bitů
  - Nejedná se z tohoto **pohledu** o strukturovaná data – rámce / pakety
- Příklady:
  - FDM (Frequency Division Multiplexing) => FDMA (Frequency Division Mutiple Access)
  - TDM(Time Division Multiplexing) => TDMA (Time Division Multiple Access)
  - CDM(Code Divison Multiplexing) => CDMA(Code Division Multiple Access)

Typy přístupu k mediu: Nevýlučný - příklady

- FDMA (Frequency Division Mutiple Access)
  - Dělí pásmu na jednotlivé kanály dle frekvencí - např po 22 MHz u WiFi
  - Zde je nevýlučný přístup – v rámci spektra
  - V rámci jednotlivých kanálů je ale přístup také třeba řešit -
    - CDMA / TDMA
- TDMA (Time Division Multiple Access)
  - Vytváří time sloty v rámci jednoho FDMA kanálu
- CDMA(Code Division Multiple Access)
  - Vysílá na stejném kanále, ale oddělitelnými „ortogonálními chipping“ kódy
    - Jak jsme si už říkali u CDM
- Frequency Hopping
  - Vysílání velice rychle mění frekvenční kanály
  - Změna je pseudonáhodná a je daná pro každou dvojici odesilatel/příjemce => šance, že dojde ke kolizi je velice malá
    - Pokud už k ní dojde, je opět třeba ji řešit, zde například až na vyšší vrstvě
  - Používá například Bluetooth

Typy přístupu k mediu: Výlučný

- Vysílací stanice **má** k mediu výlučný přístup – vysílám sám
  - Respektive by jej chtěl mít
- Mám k dispozici celý komunikační kanál, ale jen na omezenou dobu
  - Je třeba se „střídat“
- Jde o princip přepojování „paket“ (zde samozřejmě rámců)
  - Odesílám každý jeden ucelený blok strukturovaným dat a pak se řeší co dále
- S tímto typem přístupu není v ISO/OSI počítáno – proto se L2 „dělí“ na dvě
  - MAC a LLC
- Výlučné přístupy můžeme dělit dle:
  - „Předvídatelnosti“
    - Deterministické a nedeterministické
  - Dle způsobu řízení
    - Centralizované a distribuované
  - Ostatní
    - Dotazovací, předávací, rezervační, soutěžní a další

Typy přístupu k mediu: Výlučný přístup: Dělení dle převídatelnosti

- Deterministický – bez prvků náhody – předvídatelný
  - vždy vím přesně co se bude dít
  - Řídím se pravidly, která vždy vedou v konečném čase k cíli
  - Stejná posloupnost událostí skončí vždy stejným, výsledkem
  - Je garantováno, že každé stanice, která požaduje vysílat to bude v konečném čase umožněno
  - Nevýhodou je dražší implementace a v často i „dražší“ provoz z pohledu využití sítě, pokud se jedná o řídký provoz
  - Příkladem je např Token ring
- Nedeterministický – s prvků náhody – nepředvídatelný
  - Do řešení vstupuje náhoda – například v podobě náhodného odkladu dalšího vysílání
  - Není garantováno, že se každé stanici, která požaduje vysílat, to bude umožněno
    - S „téměř“ sto procentní jistotou ano, ale na sto procento říct nemůžeme - „blbá shoda náhod“
  - Stejná posloupnost událostí může dopadnout různě
    - Ale to může být právě výhoda – například při čekání na opakování vysílání
  - Příkladem je např Ethernet

Řízení přístupu: Výlučný: Dělené dle způsobu řízení: Centralizovaný

- Máme nějakého arbitra / moderátora – obecně stanici, která řídí provoz
- Jednoduché na realizaci
- Jednoduchá možnost změny přidělování práva vysílat – adaptivní vlastnosti
- Možnost zohledňovat priority
  - Jeden bod rozhoduje o tom kdo teď smí vysílat a některé stanice upřednostňovat – dávat jim více prostoru
- Problém při výpadku moderátora
  - Při jeho výpadku celá síť přestává fungovat
  - Je třeba detekovat výpadek a provést volbu/náhradu moderátora
- Může se stát, že moderátorů je více
  - To je chyba je třeba mít možnost tuto situaci detekovat a reagovat na ni
- Dokáže garantovat přístup pro stanici v konečném čase
  - Protože se typicky chová deterministicky, ale nutně nemusí
- Příkladem je např síť 100 VG Any-LAN

Řízení přístupu: Výlučný: Dělené dle způsobu řízení: Distribuovaný

- V síti nemáme žádnou řídící stanici, ale používáme společný algoritmus
- Zcela eliminujeme problém výpadku či volby moderátora – není třeba
- Všechny stanice musí algoritmus dodržovat, jinak to nemůže fungovat
  - Nedodržení může nastat například vinou chyby HW
  - Je třeba dodržování pravidel kontrolovat a na případné nedodržení reagovat
- Těžko se mění pravidla fungování sítě, protože je třeba novou informaci předat všem
  - Složité je to proto, že se často jedná o HW implementaci
- Může se chovat deterministicky i nedeterministicky
  - Ale jen jedním zvoleným způsobem v daném stavu
- Příkladem je Ethernet nebo Token ring

Řízení přístupu: Výlučný přístup: Další možnosti

- Dotazovací
  - Typicky, ale ne nutně, u centralizovaných řešení
    - Centrální stanice se ptá zda někdo nechce vysílat
    - Stanice, které chce vysílat se ptá centrální stanice nebo všech ostatních zda může vysílat
- Předávací
  - Jednotlivé stanice si „předávají pověření“ - právo vysílat – často označované jako „pešek“
  - Pokud mám právo vysílat mohu tak učinit, ale po pevně dané době musím „peška“ předat zas dále
    - Vzniká problém při ztrátě „peška“
- Rezervační
  - Sítí nejprve koluje „rezervační“ rámec, do kterého stanice provedou záznam, pokud budou chtít vysílat
  - Až rámec obejde celou síť, začnou vysílání dle rezervací
  - Opět problém při ztrátě rezervačního rámec
- Soutěžní
  - Stanice společně soupeří o přístup k médiu dle pevně daných pravidel

Řízení přístupu: Výlučný přístup: Příklady: „Čistá” Aloha

- Aloha je metoda řízení přístupu ke sdílenému mediu, která vznikla na Havajských ostrovech kolem roku 1970
  - Cílem bylo realizovat radiové spojení mezi jednotlivými ostrovy vzdálenými až 600km
- Princip byl velice jednoduchý
  - Kdo potřebuje vysílat tak to prostě udělá bez ohledu na cokoliv dalšího
  - Jelikož se na další neohlížím, může dojít ke kolizi – souběžnému a neoddělitelnému vysílání
    - Pokud se tak stane, operace musí být zrušeny, protože překrývající se vysílání nejdou oddělit
    - Nepoznám zda došlo ke kolizi nebo chybě – každopádně dle kontroly nejsou přenesená data správně a tedy neposílám potvrzení
  - Pokud ke kolizi nedošlo – tedy přenos proběhl správně – posílám kladné potvrzení
  - Pokud potvrzení nedojde v rámci timeoutu, přenos opakuji
    - Je jedno zda kvůli kolize či jiné chybě, prostě vysílám znovu – předtím ale náhodnou dobu počkám – abych riziko opakované kolize snížil
    - Pokud to udělá více stanic naráz, problém se bude velice pravděpodobně opakovat
- Reálně fungovalo jen díky řídkému provozu
  - I dnes se ještě používá tam, kde je velké zpoždění přenosu (vysoké RTT) - například satelitní přenos
- Díky velice častým kolizím má velice nízké využití kapacity přenosového kanálu – cca 18%
  - Logicky, čím více kolizí, tím častější potřeba přenos opakovat nebo čekat před začátkem dalšího přenosu a tím více „promrhaného“ času

Řízení přístupu: Výlučný přístup: Příklady: „Slotted” Aloha

- Slotted Aloha je také někdy označována jako synchronní Aloha
- Jak bylo řečeno, Aloha má velice špatné využití kapacity přenosové kanálu, což pochopitelně s nárůstem komunikace nevyhovovalo
- Důvodem bylo velké kolizní okénko
  - Tedy čas kdy může dojít k chybě
  - Rovnalo se dvojnásobku velikosti vysílaných dat
  - To bylo dáno tím, že stanice mohli vysílat úplně kdykoliv
- Řešením bylo sjednotit začátek vysílání – tedy minimalizovat čas souběhu
  - Centrální stanice vysílá všem info, kdy se může začít vysílat
  - Vysílají se pevně dané bloky – velikostně/časově
  - Ke kolizi tedy nedojde vůbec a pokud ano, tak se budou téměř 1 k 1 překrývat celé bloky
    - A tím bude velikost kolizního oken rovna MAX velikosti / délce vysílaných dat – tedy 1x lepší než u čisté Aloha
- Využití kapacity přenosového kanálu je zde až 36 % - tedy 1x více než u čisté Aloha

Řízení přístupu: Výlučný přístup: Příklady: CSMA

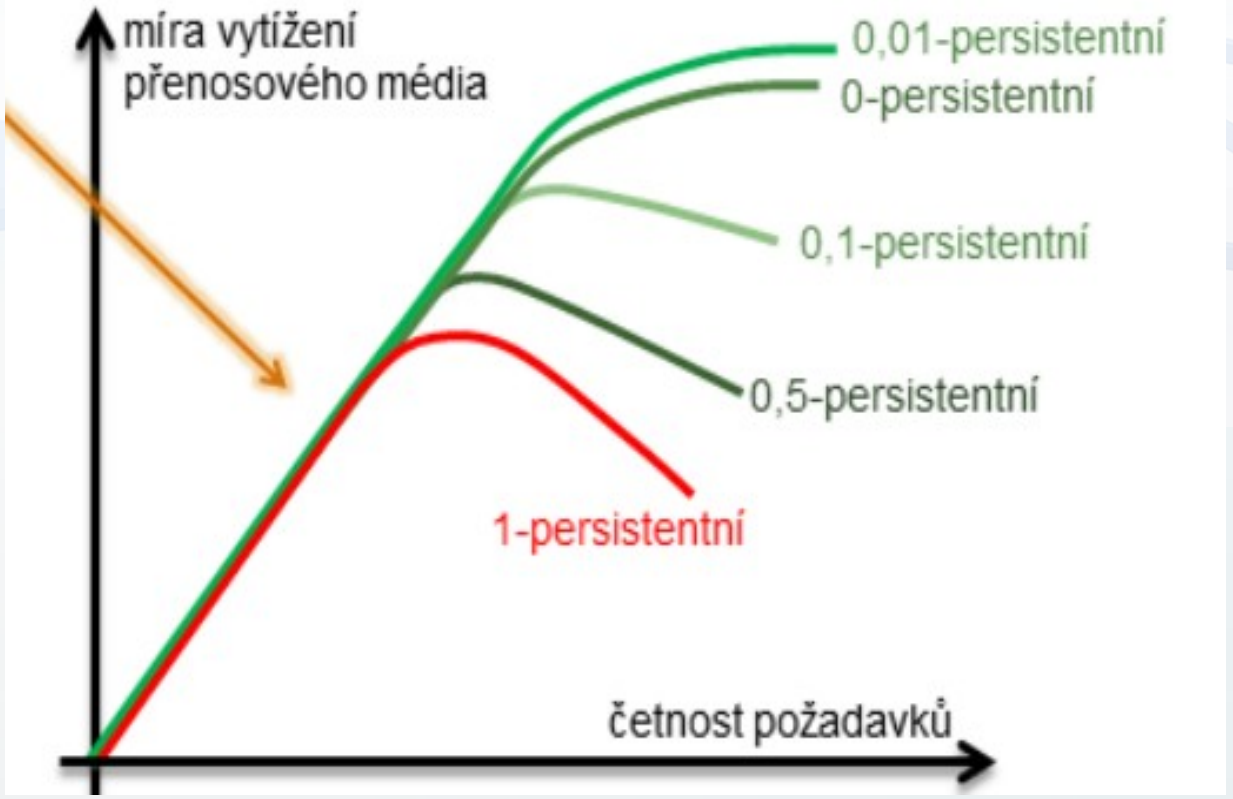
- CSMA - Carrier Sence Multiple Access
- Skupina přístupových metod, které se snaží minimalizovat možnost vzniku kolize „naslouchánim nosné“
  - Než začnu vysílat zkontroluji přenosový kanál, zda už náhodou neprobíhá vysílání
    - Pokud ne, mohu začít vysílat já
    - Pokud ano, vysílání musím odložit a zkusit po čase kontrolu znovu
- Samozřejmě zde může dojít ke kolizi
  - Dva se „rozhlédneme“ ve stejný čas a pokud je vše v pořádku začneme vysílat
  - Pokud ke kolizi dojde, zjistí se to až po dokončení celého přenosu a kontrole zabezpečení

Řízení přístupu: Výlučný přístup: Příklady: CSMA – naléhavost

- Pokud zjistím, že nějaký přenos probíhá počkám na jeho konec a pak pokračují podle jednoho ze tří možných scénářů
  - **Naléhající / vytrvalý / persistentní**
    - Nutně potřebuji vysílat, takže čekám na konec běžícího přenosu a jak je dokončen začnu sám vysílat
    - Zde už neprobíhá znova ověření, takže pokud se stejně chová více stanic, téměř jistě dojde ke kolizi
    - Výhodou je, že se „neztrácí“ čas a tím může docházet k lepšímu využití kapacity přenosového kanálu / nízká latence
    - Použito například u CSMA/CD v rámci Ethernetu
  - **Nenaléhající / „nevytrvalý“ / ne-persistentní**
    - Pokud poslechem nosné zjistím, že vysílat nemohu, vzdám to rovnou a na náhodně dlouhý čas se odmlčím
    - Pokud to udělají i další stanice, a čas čekání je náhodný, výrazně eliminuji pravděpodobnost kolize
    - Ale zhorší se využití kapacity přenosového kanálu(zvýší se latence), protože jistě vzniknou místa, kdy budou všichni náhodně dlouho čekat, ale linka už bude volná
    - Použito například i CSMA/CA v rámci WiFi
  - **P-Naléhající / „hodit si kostkou“ / p-persistentní**
    - Kombinace dvou předchozích – s pravděpodobnosti X se zachovám persistentně
    - Cílem je zvýšit využití kapacity přenosového kanálu, ale zároveň příliš nezvyšovat pravděpodobnost kolize okamžitým přenosem
    - Tedy ano, ke kolize může dojít, ale ne tak často a využití kanálu se zvýší, byť ne na maximum
      - Tedy kompromis

Řízení přístupu: Výlučný přístup: Příklady: CSMA – naléhavost - praxe

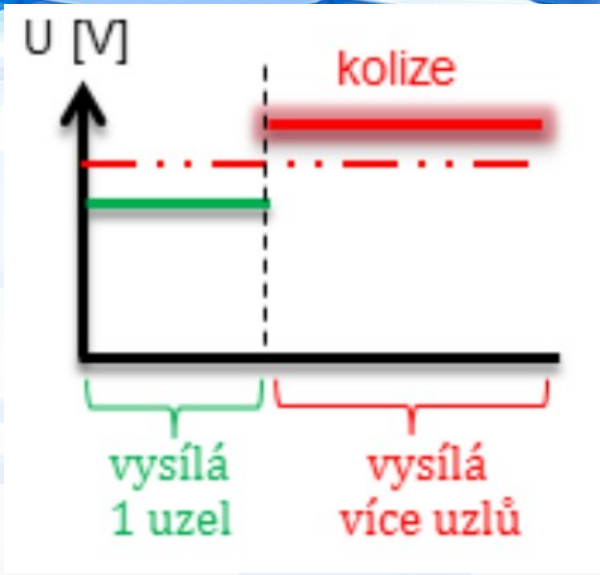
- Potřebujeme ideálně najít kompromis v naléhavosti
- Lze předpokládat, že čím více požadavků na vysílání a kolizí, tím hůře
  - Bude třeba více času k opakovaní přenosů
- Nejhůře se tedy budou chovat naléhající varianta
- Nejlépe pak vychází p-naléhající, kde p je rovna 0,01
- Při nízkých počet požadavků na přenos se všechny varianty chovají stejně
  - Protože je požadavků málo, je pravděpodobné, že budou rozprostřené v čase, kolize nebudou vnikat přirozeně



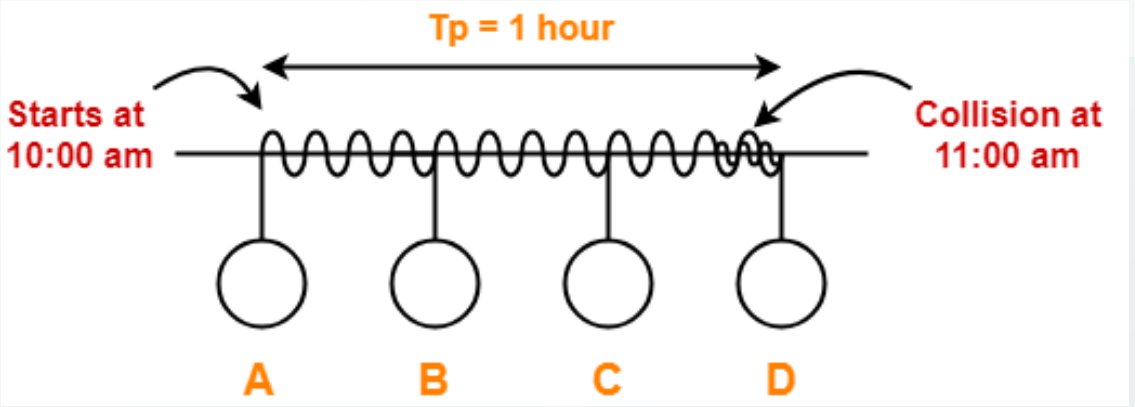
zdroj: https://www.earchiv.cz/l226/

Řízení přístupu: Výlučný přístup: Příklady: CSMA/CD

- Nevýhodou CSMA je fakt, že o kolize je odhalena až po dokončení vysílání
  - Dvě stanice ověří příposlechem nosné, že linka je volná a začnou vysílat
  - Obě – či více – začnou vysílat v téměř stejný okamžik a pokračují dokud neodvysílají celý blok
  - Po odvysílání je zkontrolováno zabezpečení rámce, zde je nalezena chyba a řeší se oprava
  - Je to zdlouhavé a nákladné na čas – kapacita využití přenosové kanálu klesá
- Řešením je snaha detekovat kolizi už v průběhu přenosu a tím minimalizovat čas násobného přenosu
  - Pokud dojde ke kolizi, nemá cenu pokračovat, stejně už to skončí s chybou, je třeba co nejdříve začít znovu - pokud možno lépe
  - CD – Collision Detect – společně s odesláním dat kontroluji, zda nepřichází data od jiné stanice
    - Signál, který se spojí z více stanice bude „nestandardní“ - tedy takový, který by se na lince neměl vyskytovat
    - Pokud ano, došlo ke kolizi



zdroj: https://www.earchiv.cz/l226



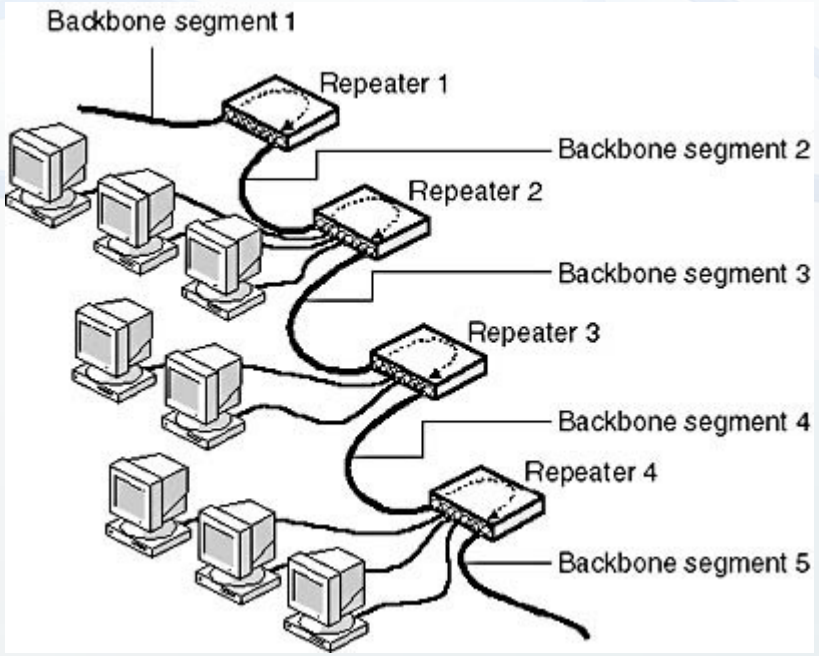
zdroj: https://www.gatevidyalay.com/csma-cd-access-control-in-networking/

Řízení přístupu: Výlučný přístup: Příklady: CSMA/CD : JAM

- Pokud v rámci CSMA/CD stanice zjistí, že došlo ke kolizi postupuje následovně:
  - Ukončí své vysílání
    - Proč by také pokračovala, už ví, že přenos dobře neskončí a tak může minimalizovat čas počátku obnovy
  - Rozešle do sítě JAM signál
    - Jednotlivé stanice nepřijmou data ve stejný okamžik
      - Kvůli vzdálenosti od vysílače a fyzikálním vlastnostem šíření signálu
    - Stanice, která pošle JAM tak pomáhá ostatním v co nejkratším čase detekovat problém
  - S opakovaným vysíláním počká náhodně dlouhou dobu
    - Princip náhodné „rozstřelu“ – aby nové vysílání nezačalo opakovaně u více stanic ve stejný čas
      - Samozřejmě při vyšším počtu stanic se to i tak může stát, ale pravděpodobnost je nižší
  - Pokud i opakovaný pokus, po náhodně dlouhém čekání, selže, čekám znovu, ale tentokrát už dvakrát tak dlouhý čas
    - První čekání nepomohlo, tak raději počkám déle, abych zvýšil šanci, že už linka bude volná
    - Samozřejmě může dojít ke snížení využití kapacity přenosového kanálu, ale to je menší zlo než nutnost opakovaného vysílání N stanic

Řízení přístupu: Výlučný přístup: Příklady: CSMA/CD : JAM : délka

- Pokud má JAM signál správně zafungovat, je třeba aby se s jistotou dostal „včas“ ke všem stanicím v rámci jedné kolizní domény
  - Pokud by byl kratší, došlo by k tomu, že část stanic by JAM neviděla mohla začít vysílat
- JAM signál je vlastně speciální rámec, který musí být minimálně tak dlouhý, aby v jeden okamžik obsáhl celou kolizní doménu
  - Tím pádem musí být omezena velikost kolizní domény
    - Nemohu ji pomocí opakovačů rozšiřovat neomezeně, protože tím by musel být delší JAM a tím by docházelo v případě kolize k větším latencím na lince
    - Uvádí se pravidlo 5:4:3
      - 5 segmentů – tedy spojů mezi opakovači
      - 4 opakovače – tedy maximálně 4 za sebou zapojené opakovače signálu
      - 3 sítě / obydlené segmenty – bloky mezi opakovači, kde je stanice
  - Např pro 10Mbps Ethernet je to 512bitů



zdroj: https://flylib.com/books/en/2.733.1.31/1/

Řízení přístupu: Výlučný přístup: Příklady: CSMA/CD : příklad Ethernet

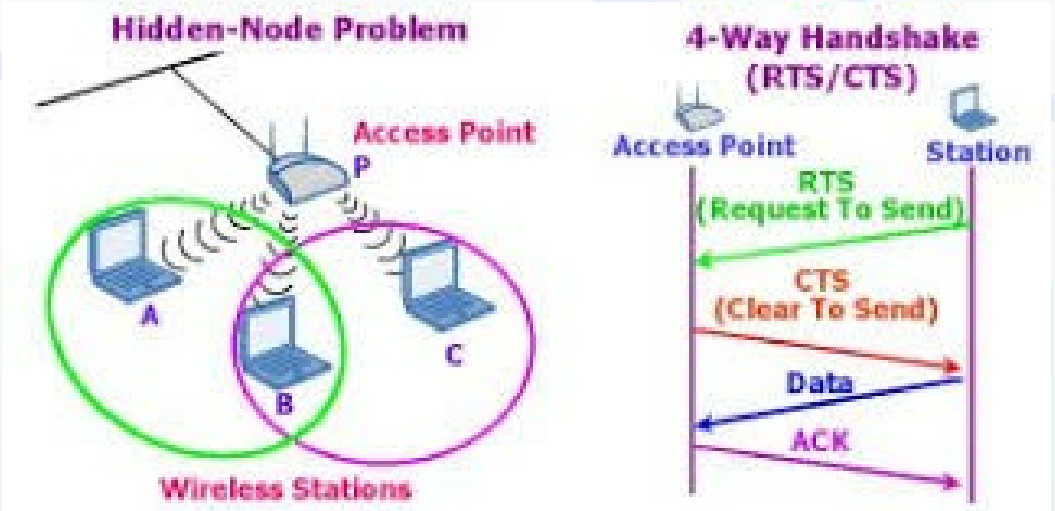
- Ethernet ve variantě half-duplex využívá CDMA/CD
  - Pro koaxiální kabel například
  - Pro full-duplex už není třeba, protože velikost kolizní domény je 1
- Rámec nesmí být kratší než 64B
  - Pokud by byl, docházelo by falešné identifikaci volné linky
- Používá se JAM o délce právě 64B, tedy 512 bitů
- Maximální přenosové rychlosti pro koaxiální kabel – do 10Mbps
  - Zde je vidět neefektivita tohoto řešení, protože obecně lze koaxiální kabel použít na výrazně vyšší rychlosti – viz přenos pomocí rozvodů kabelové televize

Řízení přístupu: Výlučný přístup: Příklady: CSMA/CA

- CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance
  - Collision Avoidance – vyhýbání se kolizím
- Používá se tam kde není možné použít CD – Collision Detect
  - Například bezdrátové sítě
- Princip chování se může dle implementací lišit, ale vždy se snaží kolizi předejít, protože ji nemůže v průběhu přenosu rozpoznat
- Příklad pro LocalTalk
  - Provedu kontrolu nosné a poté pošlu info ostatním stanicím, že chci vysílat
  - Žádost o vysílání je typicky násobně menší, než přenášená data, takže mohou nastat dvě situace:
    - Žádost projde v pořadu => Fajn, všichni ví, že já chci vysílat a tedy tedy by ke kolizi nemělo dojít
      - Samozřejmě ještě zde může být problém nové stanice, ale ta šance je výrazně nižší
    - Žádost neprojde v pořádku a je třeba ji opakovat => Ok, to je problém, ale ztratil jsem násobně méně času, než při vysílání reálných dat
- Příklad pro WiFi(IEEE 802.11)
  - Kontroluji, zda je linka volná
  - Pokud ano, počkám náhodně dlouhou dobu, pak zkontroluji zda je stále volná
    - Pokud ano, zkusím odeslat data a čekán na potvrzení doručení
  - Pokud ne, čekán dvojnásobnou dobu a pokus opakuji
  - Pokud odvysílám data a nepřijde včas potvrzení, opět čekám náhodně dlouhou dobu na opakování přenosu a pokud vysílat nemohou, zdvojnásobím čas čekání a zkusím znovu

Řízení přístupu: Výlučný přístup: Příklady: CSMA/CA s RTS/CTS

- Samotné čekání nemusí zajistit, že ke kolizi nedojde
- U CSMA/CA v rámci bezdrátových sítí se jako nepovinný prvek může ještě použít RTS/CTS
  - Vše předchozí, tedy příposlech nosné, čekání po zjištění volné linky atd zůstává platné
- Chceme ještě více snížit riziko kolize, takže provedeme „rezervaci“ kanálu
  - RTS – Request To Send – Dotaz na vysílání
    - Podobně jako u LocalTalk, než začnu vysílat, optám se, zda je mohu
    - Stanice, která chce vysílat, se zeptá přístupového bodu (například AP) zda může
  - CTS – Clear To Send – Volno k odeslání
    - Po přijetí odpovědi může začít vysílat, protože ví, že nikdo jiný právo vysílat v daný čas nemá
- Kromě jiného řeší problém skrytého uzlu
  - Typický problém v bezdrátových sítích, kdy se ne všechny uzly musí vidět navzájem
  - Snadno pak dojde k situaci, kdy stanici detekovala volný kanál, ale ono to tak nemusí být pro další stanice



zdroj: https://www.marigold.cz/wifi/doku.php/problem_skryteho_uzlu?rev=1154167313

Řízení přístupu: Výlučný přístup: Příklady: CSMA/BA

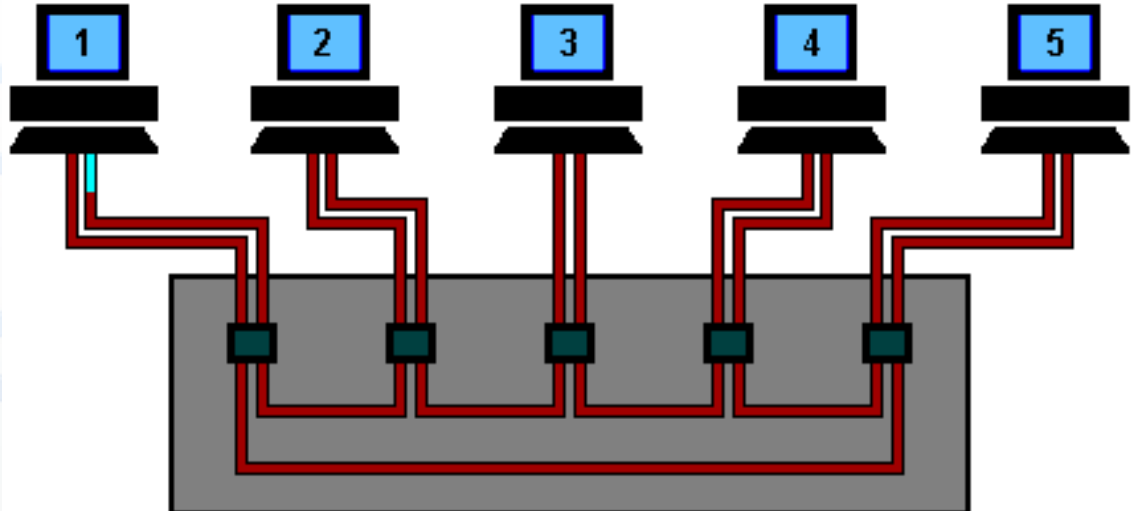
- Carrier Sense Multiple Access with Bitwise Arbitration
  - Bitwise Arbitration – bitová arbitráž / řešení priorit
- Opět řešíme příposlech nosné, ale v případě kolize nečekání náhodnou dobu jako v CSMA/CD
- Jednotlivé stanice mají přiřazen kód – prioritu
- Pokud dojde ke kolizi, je na základě „priority“ vybrána stanice, která smí vysílat
- Používání v průmyslu – CAN sítě
  - Například v autech na komunikaci řídících jednotek
- Výhodou je nižší prodleva po kolizi
- Navíc je možné upřednostňovat určité typy zpráv / rámců
  - Například info o nutnost zapnout ABS má jistě přednost před info o prasklé žárovce …
- Vzniká zde ale problém monopolizace
  - Pokud bude docházet ke kolizím často a u stejných stanic, nemusí se ty s nižší prioritou k vysílání vůbec dostat
  - Řešením je priorita složená z více prvků nebo proměnlivá v čase

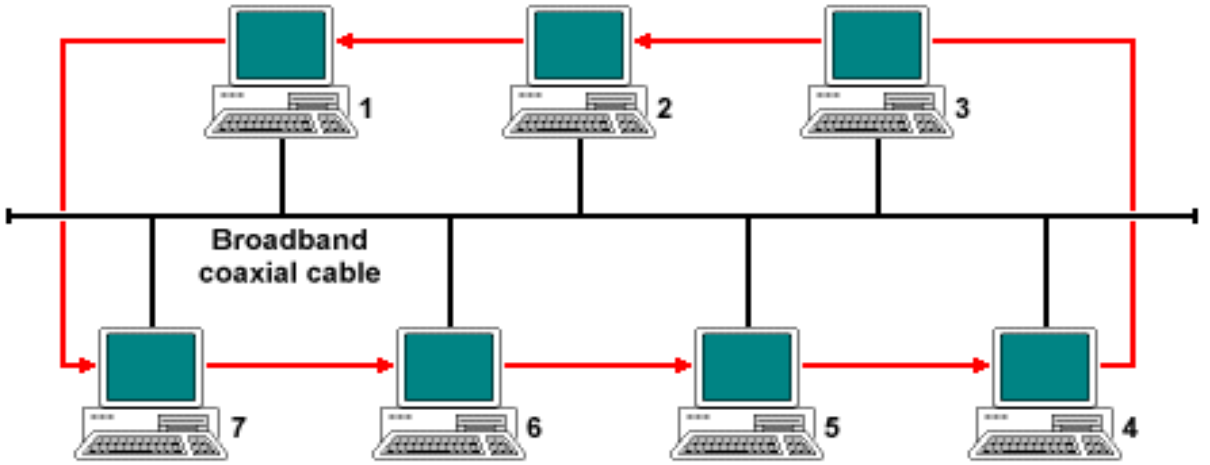
Metody řízení přístupu: Výlučný přístup: Token Passing

- Principem je předávání pověření / „peška“
  - Kdo má „peška“ může vysílat
- Jedná se deterministickou distribuovanou metodu
- Aby předávání fungovalo, je nutné aby bylo zapojení kruhové
  - Fyzicky – opravdu do kruhu zapojená síť
  - Logicky – zapojení je jiné než kruhové a „nějak jinak“ je zajištěn kruh
    - Pomocí MUA při zapojení do hvězdy
    - Pomocí pořadí ve sběrnicových sítích
      - Zde je třeba řešit výpadek stanice – protože pokud jedna vypadne, síť přestane fungovat
      - Stejně tak příchod nové stanice
- Problém nastává v případě, že
  - Pověření se ztratí
  - Pověřeních koluje více
- Obě situace řeší jeden vyčleněný prvek – aktivní monitor
  - Ten je typicky volen například na základě nejvyšší MAC
  - Při výpadku aktivního monitoru je zas nutné zvolit jiný

Metody řízení přístupu: Výlučný přístup: Token Passing : příklady

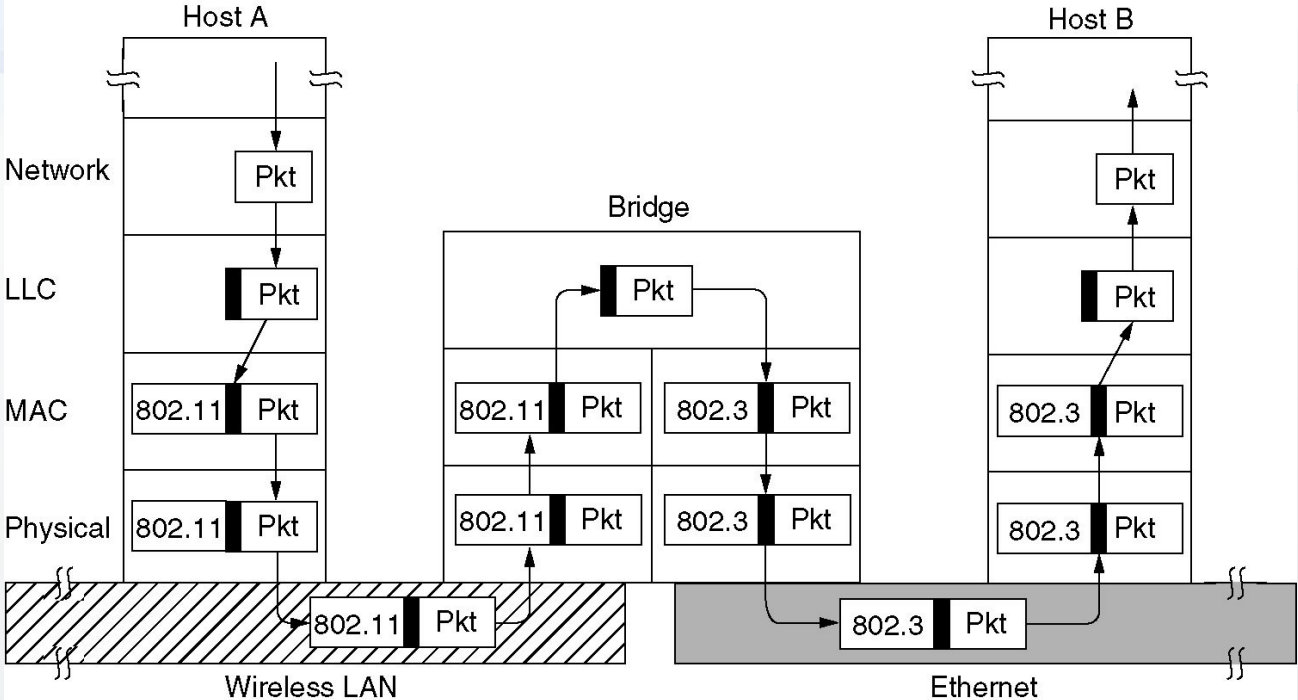
- Token Ring
  - Dvě varianty
    - IBM Token ring – zapojení do hvězdy, kroucená dvojlinka
    - IEEE 802.5 – nepředepisuje žádnou topologii ani medium
  - Používá logický kruh
  - Při větší síti a zatížení je efektivnější než Ethernet
  - Pokud nikdo nevysílá, koluje prázdné pověření
- Token Bus
  - Využívá sběrnicovou topologii
  - Kruh je opět pouze logický



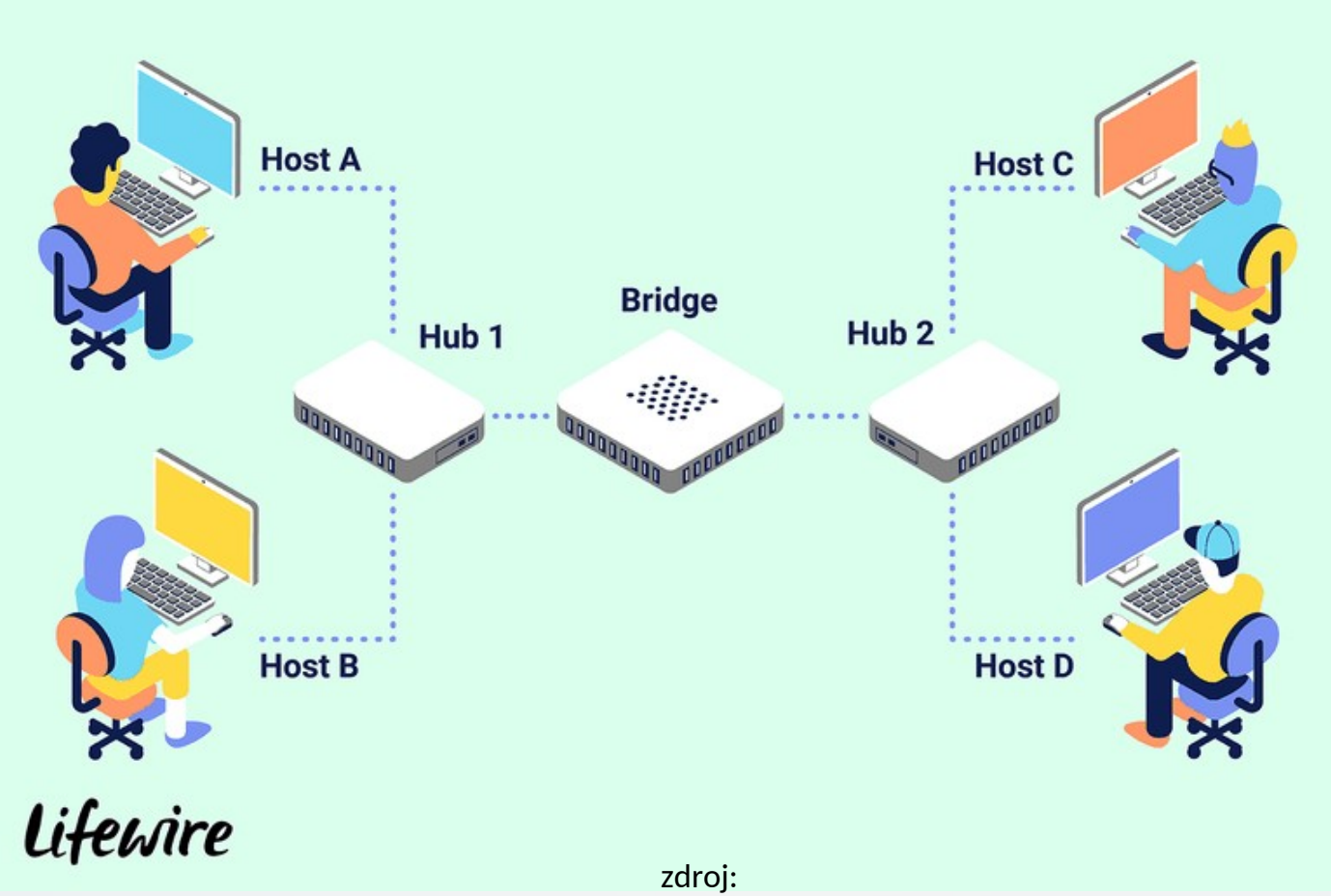


Mosty mezi 802.x a 802.y

- V rámci L2 se vyskytuje více protokolů
  - Mají své rámce, svůj přístup k mediu, své ověření …
- Jejich vzájemnou komunikaci zajišťují mosty / bridge mezi protokoly
  - Jedná se vlastně o zařízení, které umí oba protokolu
  - Dochází pak k transformaci jednoho rámce do rámce jiného
  - Například přechod Ethernet < = > WiFi
    - Zde je i jiné přenosové medium atd.
- Mosty mohou být:
  - Lokální
    - Propojení v rámci LAN
      - Např dva segmenty 802.3
  - Vzdálené
    - Propojení více LAN prostřednictvím WAN
      - Např Ethernet over PPP
- Existují dvě možné konfigurace
  - Transparentní – samoučící se
    - Na začátku nezná o sítí nic, ale postupně se učí
    - Pokud je zdroj i cíl ze stejné sítě nedělá nic
    - Pokud neví, pošle data dále
    - Zmenšuje kolizní doménu, ale nezmenšuje broadcastovou doménu
  - Se zdrojovým směrováním
    - Použití například v Token ring sitích
    - Kromě cílové adresy musí být uvedeno i to, přes jaké všechny mosty mají data projít

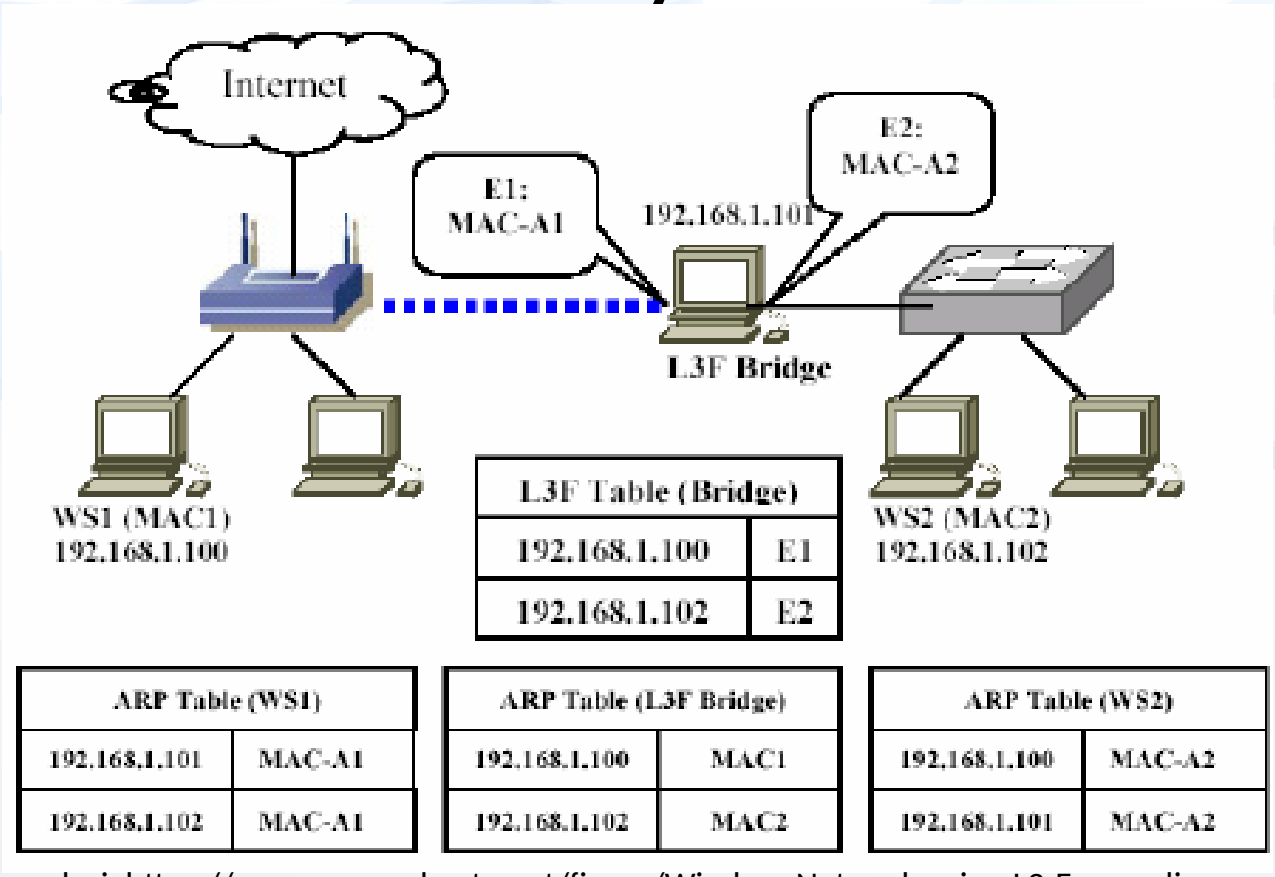


Mosty mezi 802.x a 802.y: příklad lokálních mostů



zdroj:
https://signup.fishedfun.com/en/html/sf/registration/eone_m3dsc.html#&sf=eone&lng=en&m=books&ref=5261516&prod=2&sub_id=explain-network-bridge-diagram&_sign=1a3ae649ec918155aa3976c2785a09ac&_signt=1606300992&utm_ex

Mosty mezi 802.x a 802.y: příklad vzdálených mostů



L3F Table (Bridge)	
192.168.1.100	E1
192.168.1.102	E2

ARP Table (WS1)	
192.168.1.101	MAC-A1
192.168.1.102	MAC-A1

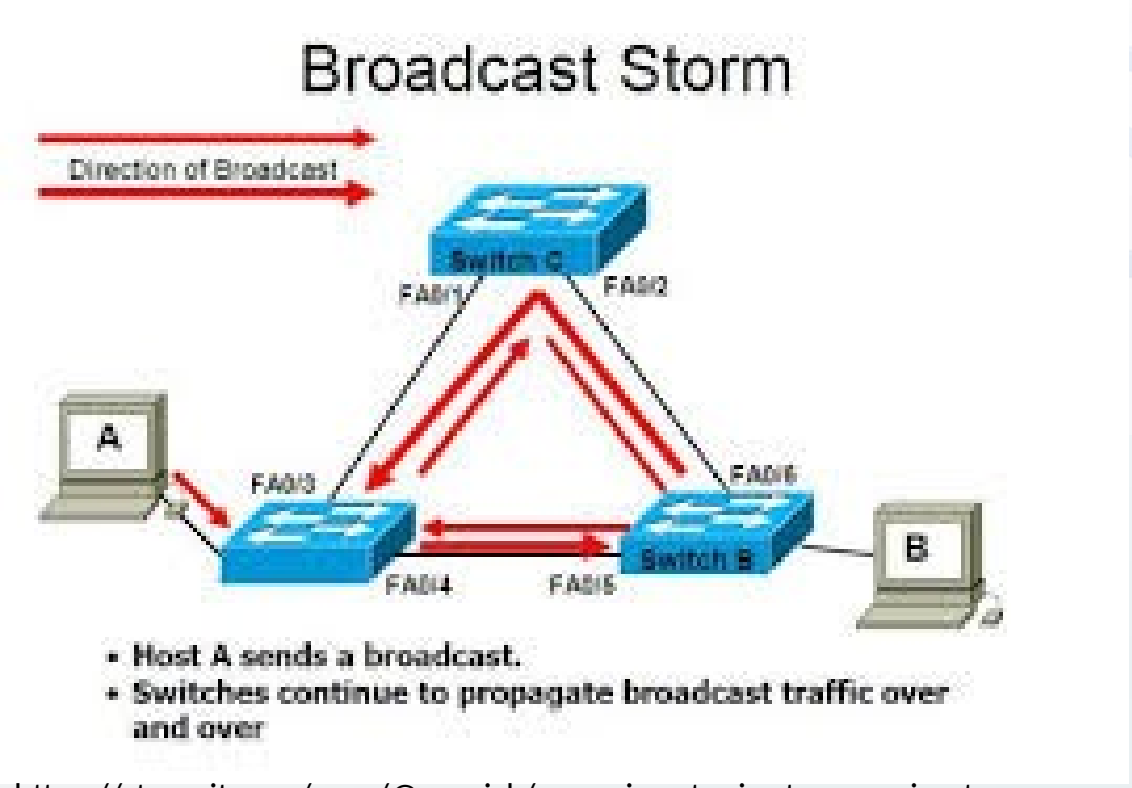
ARP Table (L3F Bridge)	
192.168.1.100	MAC1
192.168.1.102	MAC2

ARP Table (WS2)	
192.168.1.100	MAC-A2
192.168.1.101	MAC-A2

zdroj: https://www.researchgate.net/figure/Wireless-Network-using-L3-Forwarding-In-the-above-example-when-WS1-sends-a-packet-to_fig4_4226879

Spanning tree protokol

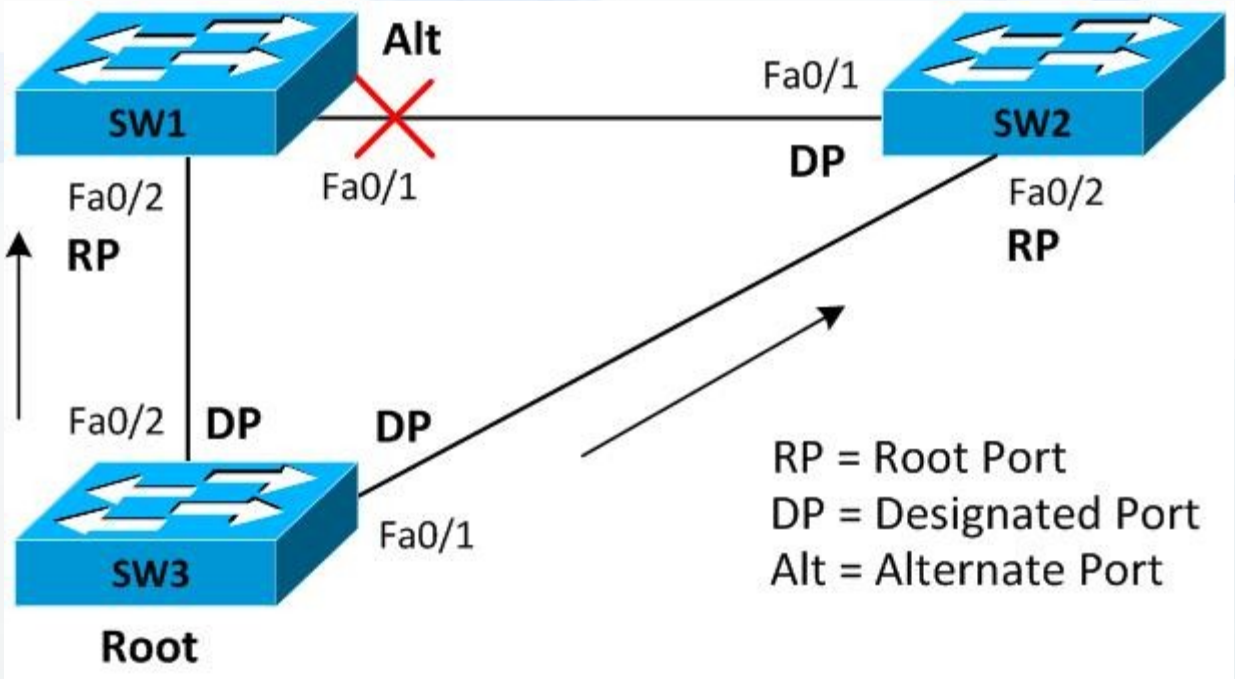
- STP – Spannig tree protocol
- Pokud propojíme více typu HUB / Bridge / Switch a nebo jen více portů jednoho zařízení, může dojít k zacyklení
- Typický problém u broadcastových vysílání
  - Ty jsou na všechny porty kromě příchozího
  - Vznikají broadcastové bouře
    - Přetížení zařízení díky násobnému doručování zpráv
- Cílem STP je hledat smyčky v síti a ty SW rozpojujeme
  - Samozřejmě pokud to zařízení umí
-
- Problém ve velkých sítích – konverze velice dlouho trvá
- Kromě prevence smyček může sloužit i jako fail-over řešení
  - Násobně zapojené linky jsou SW odpojené do výpadku aktivně používané
- Příklady:
  - Multiple Spanning Tree Protocol
  - Rapid Spanning Tree Protocol
  - Shortest Path Bridging



zdroj: https://steemit.com/ccna/@evesick/ccna-cisco-topic-stp-spanning-tree-protocol

Spanning tree protokol - fungování

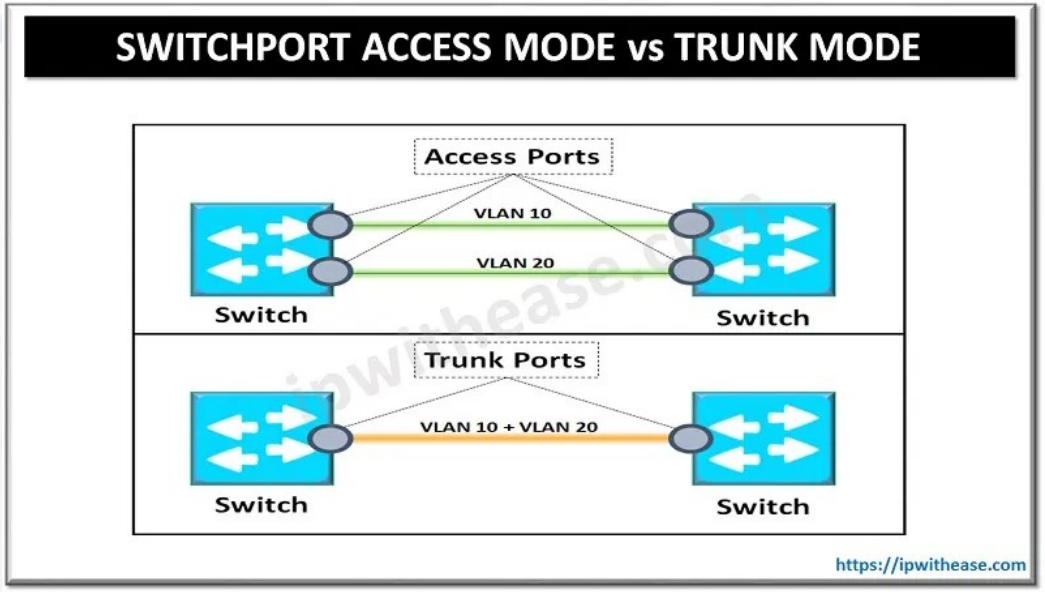
- Princip fungování
  - Zvolíme si kořen sítě Root Bridge – zařízení s nejnižší BID
    - BID = priorita + MAC
    - Root Bridge má všechny porty Designated a zároveň ve stavu Forwarding
    - Odešlu BPDU s vlastním BID
      - Pokud jsem nejnižší ostatní to akceptují
      - Pokud nejsem, stanice s nižším BID hodnotu změní a pošle dále
  - Dochází k rozpojení smyček – na základě rozeslaných a analyzovaných BPDU
  - Portům se nastaví jeden ze tří typů
    - Root port – port přímo spojený s Root switchem nebo s nejnižší cestou k němu, forwarduje data
    - Designated port – je členem STP, připojuje segment, forwardu
    - Non-designated port – blokovaný / alternativní port
- Porty prochází více stavy
  - Blocking
    - Blokován, neposílá nic
  - Listenig
    - Naslouchá a přijímá BPDU rámce
  - Learning
    - Učí se MAC adresy, předává BPDU rámce
  - Forwarding
    - Plnohodnotný provoz



zdroj: https://www.networkstraining.com/cisco-spanning-tree-protocol/

Virtual LAN - VLAN, Trunk
(opakování z první přednásky)

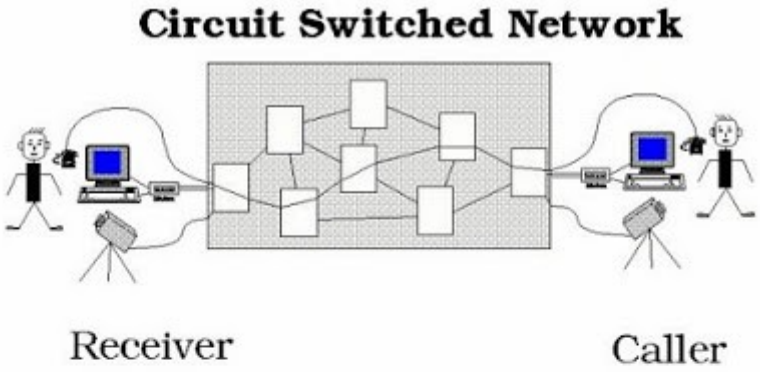
- VLAN – virtuální síť – virtuální rozdělení fyzického zařízení
- Dva typy portů:
  - VLAN virtuální LAN
    - „rozdělení“ jednoho fyzického zařízení na více virtuálních
    - Provoz v každé VLAN je isolované == nevidí data jiné VLAN
    - Identifikace VLAN pomocí VLAN ID, celé kladné číslo, výchozí je 1
    - V rámci jedná VLAN není nutné VLAN ID uvádět == „NETAGOVANÝ“ provoz
    - Porty v jedné VLAN se označují jako „access“ - „accessové“ porty
  - Trunk
    - Tím že se VLANy nevidí mezi sebou, musela by pro každou VLAN být samostatná cesta k dalšímu zařízení – switch / router
    - To je problém, protože pro 20 VLAN by se obsadilo 20 portů switche
    - Trunk je speciální port, kterým může procházet provoz více VLAN
    - Jednotlivé rámce se rozeznají pomocí VLAN ID v hlavičce rámce == „TAGOVANÝ“ provoz
    - Porty kde je povolen trunk jsou označované jako „trunkové“ porty

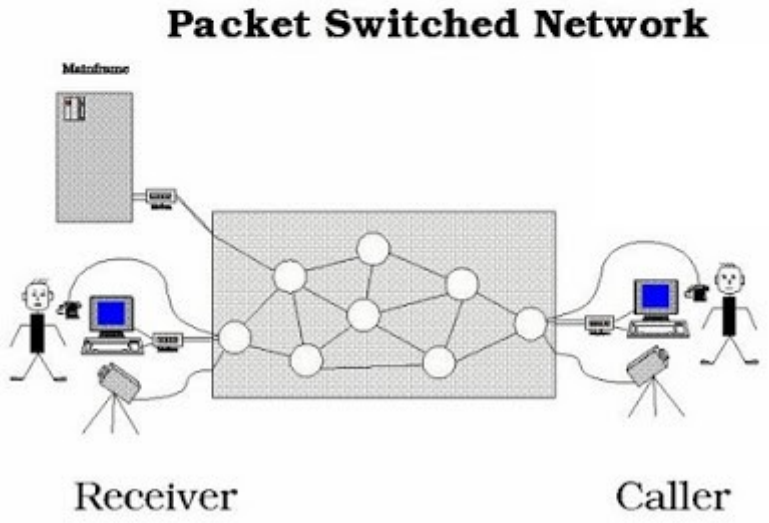


zdroj: https://ipwithease.com/switchport-trunk-mode-vs-access-mode/

Sítě dle typu přepínání

- Sítě může dělit dle toho jak jsou v nich data směrována
- Zda je směrování řešeno jako :
  - Posílání bloků
    - Řešíme každý blok dat „samostatně“
  - Posílání streamu data
    - Připravíme cestu a tou pak posíláme všechna data
- Základní možnosti
  - Sítě s přepínáním okruhů
    - Může se řešit i na L2
  - Sítě s přepínáním paketů / rámců
    - Může se řešit i na L2
  - Sítě s přepínáním zpráv

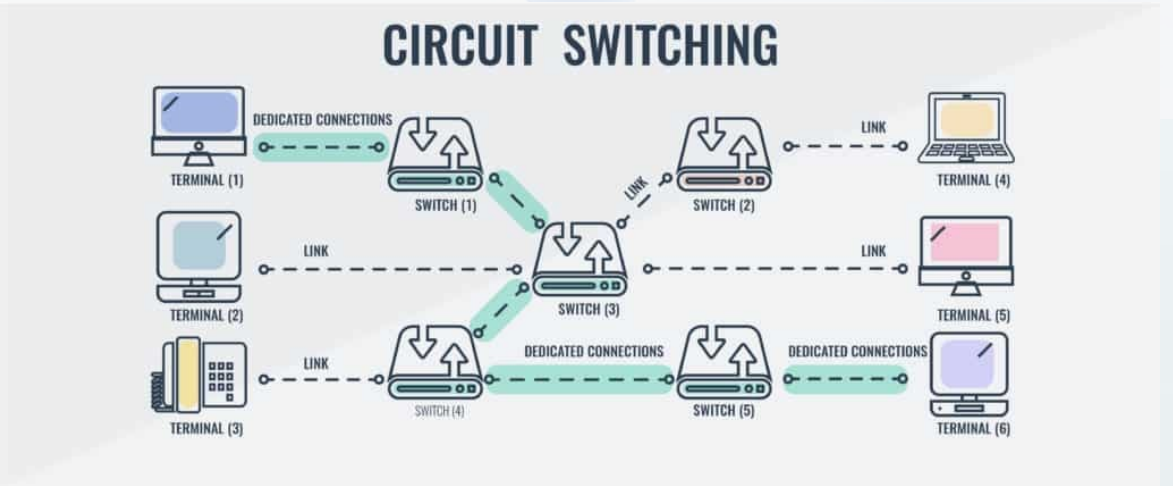




zdroj: http://http://www.differencebetween.net/technology/difference-between-circuit-switching-and-packet-switching/

Sítě dle typu přepínání: S přepínáním okruhů

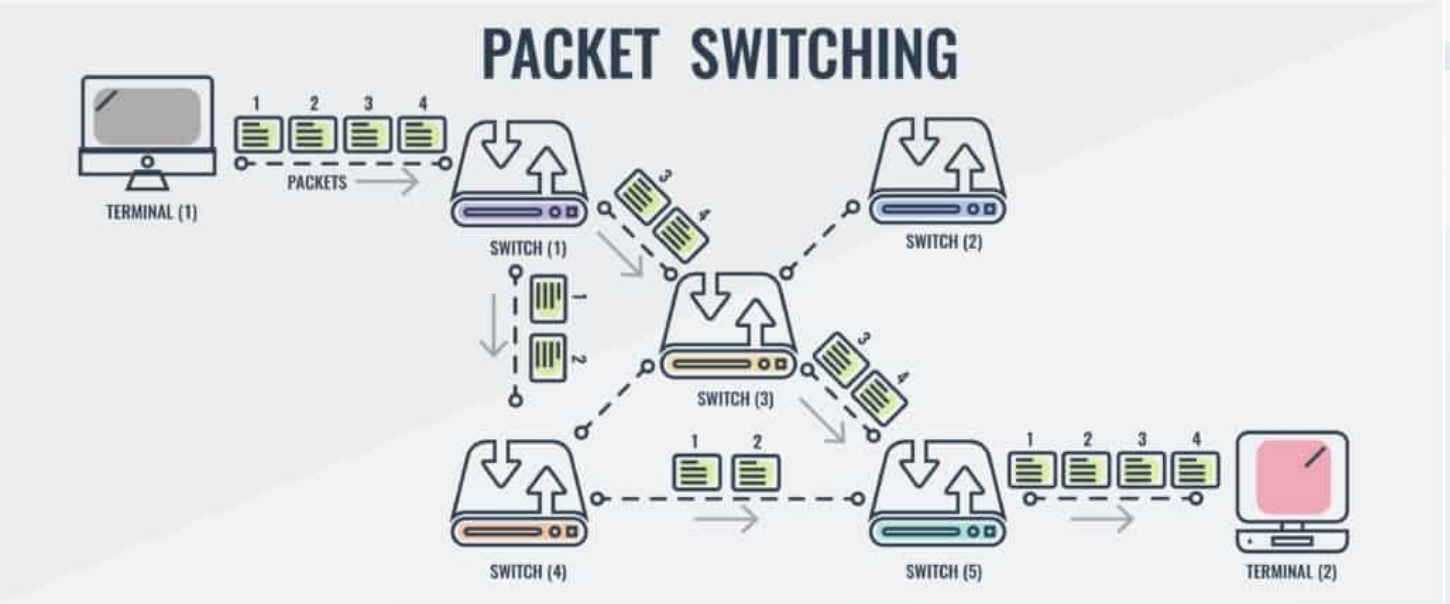
- Hledání cesty je realizováno na začátku vysílání
- Je sestavena virtuální cesta pro daný přenos a tou je přenos následně realizován
- Řešení je pomalejší na začátku – musí se počkat než se cesta najde
  - Hledání se realizuje na základě žádosti o vysílání
- Vzniká problém v případě výpadku či změny v sítí – je třeba virtuální cestu znovu sestavit
  - Čím více výpadků a přepočítávání tím hůře
- Velkou výhodou je pak ale rychlost následného zpracování
  - Data už se posílají po předem známé cestě a není nutné se v každém uzlu rozhodovat o cestě
  - Datová cesta je během přenosu vyhrazena pro daný přenos
- Jedná se o spojovaně orientovaný přenos
- Typicky se využívá v telefonní síti u hlasových služeb
  - Dříve i manuálně realizovaný přes spojovatelku



zdroj: https://www.comparitech.com/net-admin/circuit-switching-vs-packet-switching/

Sítě dle typu přepínání: S přepínáním paketů

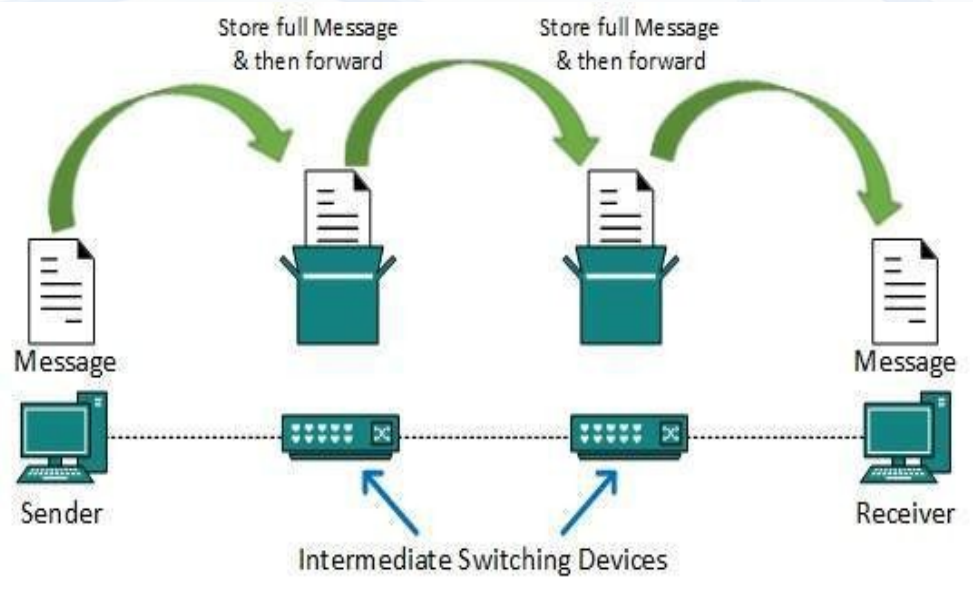
- Při realizaci přepínání okruhů je problém s časem nutným na přepočet při změně topologie či stavu sítě
  - Může dojít k odpojení linek nebo k jejich zahlcení
- Pokud ke změnám dochází často, bude sestavování cesty neefektivní
- Při přepínání paketů se rozhoduje na každém routeru
  - Rozhodování je samostatné
  - Nezáleží na předchozích odeslaných datech
  - Data mohou jít vždy různou cestou
  - V rámci dat musí být celá adresa příjemce
- Při intenzivním přenosu dat na stabilní síti bude mít vyšší řeži než sítě s přepínáním okruhů
- Dokáže se vypořádat s častými změnami v síti
- Dokáže optimalizovat přenos
  - Rozklad po více cestách



zdroj: https://www.comparitech.com/net-admin/circuit-switching-vs-packet-switching/

Sítě dle typu přepínání: S přepínáním zpráv

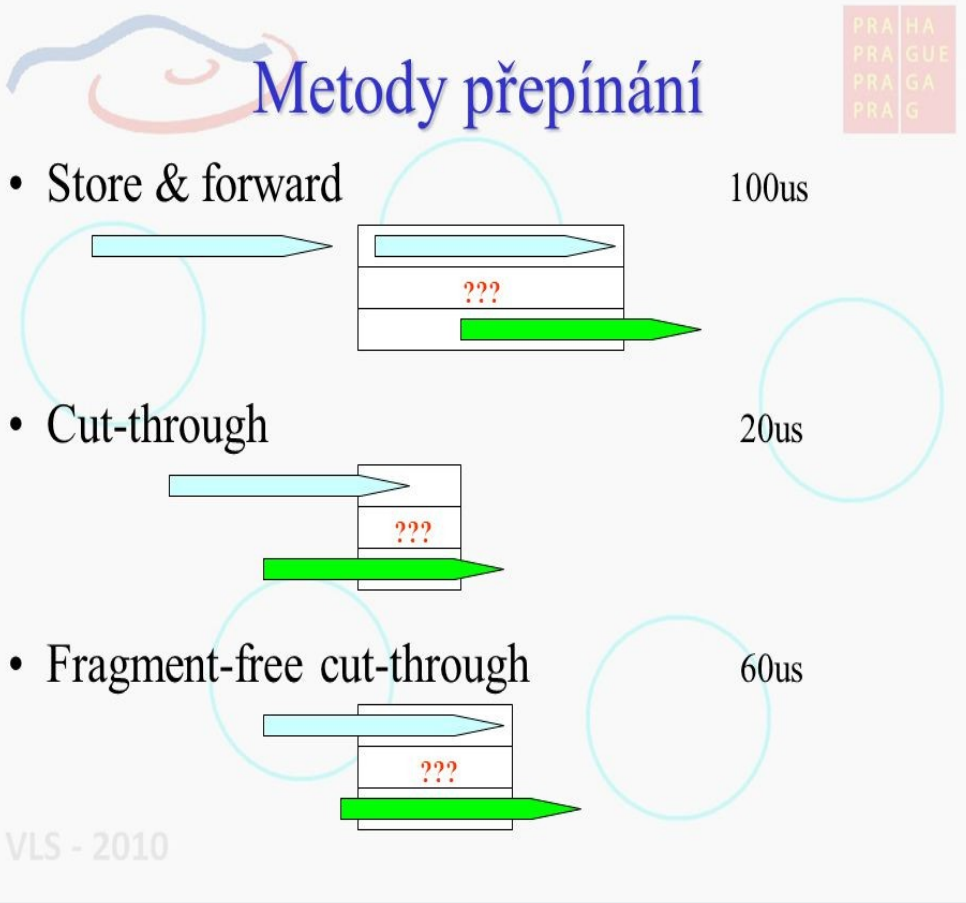
- Jedná se o „speciální“ případ sítí s přepínáním paketů
- Přenášenou jednotkou není paket, ale zpráva
  - Například email pro L7
- Princip přenosu je ale stejný jako u paketů, jen s jinou jednotkou
- Zpráva je přenesena na další uzel - celá – tam zkontrolována a pokud je v pořádku je přeposlána dále
- Pokud v pořádku není, je tato informace zachycena na prvním směrovači kde došlo k chybě
  - Šetříme tím čas přenosu, protože v co nejkratší době reagujeme na problém
  - Typicky řešeno na vyšších vrstvách
    - Viz email, který prochází jednotlivými SMTP servery a na každém je jako celek - email – zpracován, doplněn o další data a poslán dále



zdroj: https://www.tutorialspoint.com/data_communication_computer_network/physical_layer_switching.htm

Metod posílání dat

- Store & Forward
  - Přijme celý rámec / paket a teprve po jeho přijetí jej jako celek zpracovává
  - Může vyvažovat výkyvy v síti pomocí cache
  - Dochází k prodlevám, protože musí přijmout celý rámec / paket
- Fast forward / Cut-through
  - Začne odesílat data ihned po obdržení celé adresy příjemce
    - Adresa příjemce je na začátku data
    - Snižuje latenci
- Fragment-free
  - Kombinace obou předchozích
  - Nejprve přijme přijme data po adresu odesílatele, ověří že nenastal problém a pak posílá data dále



zdroj: https://slideplayer.cz/slide/3327168/