

# Opravak 2010

Boli dve skupiny. V podstate obe boli rovnake az na jednu otazku a to c. 2

## 1. Seriove spojovanie

-typy zbernic a kratko vyzvetlit ako funguju

-rozdelenie zbernic na centralizovane a decentralizovane tie sa dalej delia na ....

## 2. Baseline, presne ta co chodi v minulorocnych a druha skupina mala Banyan

## 3. Aktivny manazment radu typu QMM (Queue Memory Managment) popisat

- popisat algoritmus Selective Discard

- porovnat ho s algoritmom Tail Drop ako sa odlišuje

## 4. MPLS popis

LER, LSR, LDP a FEC

-rozdiel medzi MPLS a GMPLS

## 5. Vlnovodne spinace popisat

Free - Space Opticke spinace

Vysvetlit princip S-SEED spinaca a nakreslit

Nebolo na opravaku NGN, Signalizacia a QoS

Moja rada, naučte sa na normalny, nebudete mať stresy.

Zaklad je NGN to je vzdy na normalnom, Opticke Spojovanie a tiež prve tri prednasky ked sa naucite, neni o com. Kebyze, tak pozriet si aj Signalizaciju a QoS to co je po ine roky.rovnat ho s algoritmom Tail Drop ako sa odlišuje

# Sériové spojovanie

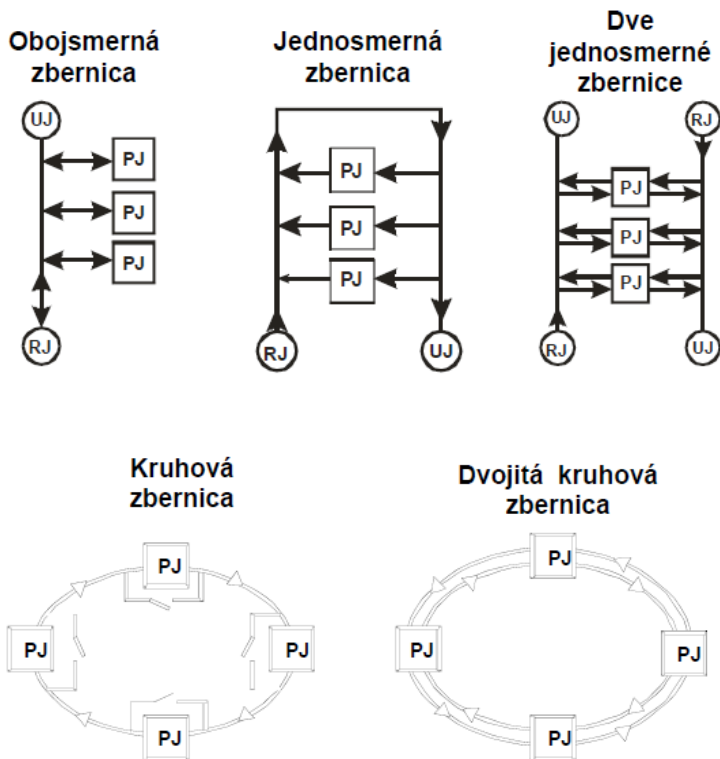
Charakteristika

- Vhodné pre paketové spojovanie
- Typické pre siete LAN a MAN
- Nevhodné pre izochrónne služby
- Dva spôsoby
  - spojovanie s pamäťou
  - spojovanie na zbernici
- Koncové terminály sú navzájom spojené zbernicou, ktorá tvorí spoločné transportné aj prepájacie médium pre všetky signály.

Klasifikácia:

- podľa typu zbernice,
- podľa procesu, ktorým jednotlivé terminály pristupujú na zbernicu

Typy zbernic



### Token

Single token passing - na zbernici môže byť iba jeden token

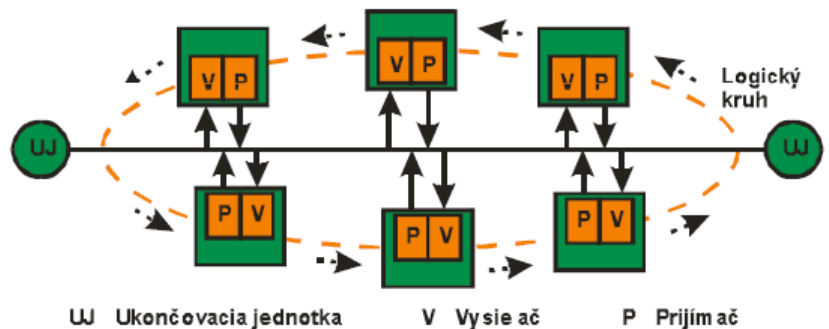
Multiple token passing - na zbernici môže byť niekoľko tokenov

Single frame - Token sa predáva k nasledujúcemu terminálu až keď vysielač stanica kompletne odstráni rámec zo zbernice

### Token Bus

Charakteristika

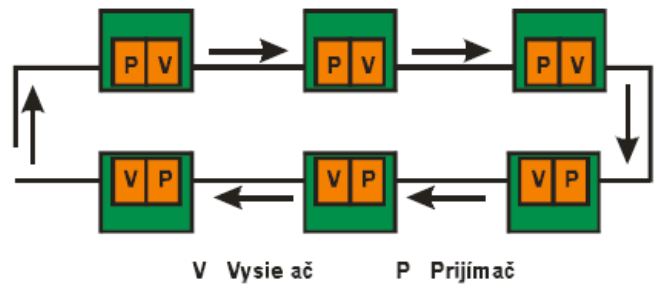
- 3 vrstvy: fyzická, MAC a LLC
- Fyzická vrstva:
  - umožňuje štyri rôzne prevádzky na zbernici
  - prenosové rýchlosti: 1, 5, 10 a 20 Mbit/s
  - médium: koaxiálny kábel (75 Ω), optické vlákno
- MAC podvrstva:
  - algoritmus: predávanie tokenov
  - 4 úrovne priority
- LLC podvrstva:
  - 8 druhov služieb



### Token Ring

### Charakteristika

- 3 vrstvy: fyzická, MAC a LLC
- Fyzická vrstva:
- prenosové rýchlosti: 4 / 16 Mb/s
- médium: UTP / STP
- max. počet opakovačov: 250
- max. vzdialenosť medzi opakovačmi: nešpecifikovaná
- MAC podvrstva:
- algoritmus: predávanie tokenov
- 8 úrovni priority
- LLC podvrstva:
- 8 druhov služieb



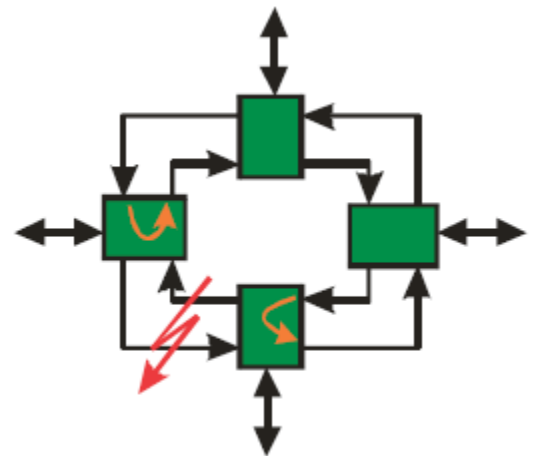
### FDDI - Fiber Distributed Data Interface

Zbernica: Dvojitá kruhová zbernica

MAC algoritmus: multiple token passing

Výhody:

- nekladie obmedzenie na:
  - dĺžku liniek,
  - počet staníc,
  - celkový dosah
- dobré alokačné vlastnosti, relatívna necitlivosť na nevyvážené záťaž
- pokračovanie v prevádzke v prípade poruchy



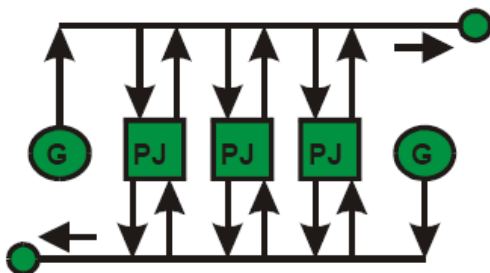
### FDDI - II

Charakteristika

- Spätná kompatibilita s FDDI
- Vhodné aj pre CBR služby
- FDDI - II
  - paketový mód (asynchrónne služby)
  - izochrónny mód (synchronne služby)

### DQDB

Topológia - Dve jednosmerné zbernice (34,368 / 155,520 Mbit/s)



G - generátor rámcov  
PJ - prístupová jednotka

Čítanie dát uzlami neovplyvňuje prechádzajúce dáta, zápis je realizovaný funkciou OR

MAC mechanizmus

- Sú definované dva prístupy na zbernicu:
  - QA (Queued Arbitrated) - prostredníctvom distribuovaného radu DQSM (Distributed Queue State Machine) - umožňuje 3 úrovne priority
  - PA (Pre-Arbitrated) - pre izochrónne služby

## Paralelné spojovanie s prepájaním paketov

Formy spojovania

- **Sériové spojovanie** - distribuované spojovanie na zdieľanom médiu (zbernica, kruh)
- **Paralelné spojovanie** - spojovacia sieť (maticové pole) s N vstupmi a M výstupmi
  - Použité v telefónnej sieti
    - Historický (technologický) dôvod
    - Kapacitný dôvod

Spojovacia sieť

- Transportná časť - fyzické médium, ktoré zabezpečuje prenos informácie z jednotlivých vstupov na jednotlivé výstupy
  - je daná svojou architektúrou
  - vykonáva funkcie dané v užívateľskej rovine protokolového modelu siete
- Riadiaca časť - riadi spojovací proces,
  - jej činnosť je závislá na signalizácií v sieti
  - vykonáva funkcie v riadiacej rovine protokolového modelu siete
- Základný spojovací prvok - spojovací element
  - veľkosť  $P \times Q$
  - limitovaná kapacita
- Väčšie polia - väčší počet spojovacích elementov kombinovaných do => viacstupňových spojovacích sietí (MIN - Multistage Interconnection Networks)

### Klasifikácia MIN

Podľa typu spojenia

- Unicast MIN (one-to-one, point-to-point)
- Multicast MIN
- Broadcast MIN

Podľa spôsobu transportu paketu v spojovacej sieti

- Jednocestná MIN
- Viaccestná MIN

Podľa riadenia spojovacej siete

- MIN s centralizovaným riadením
- MIN s decentralizovaným riadením

Podľa vnútorného blokovania

- Siete s blokovaním
- Siete bez vnútorného blokovania
- Siete bez vonkajšieho blokovania
- Rekonfigurovateľné siete bez blokovania

Podľa umiestnenia vyrovnávacej pamäte

- MIN s vonkajšou vyrovnávacou pamäťou
- MIN s vnútornou vyrovnávacou pamäťou
  - na vstupe elementu
  - na výstupe elementu
  - v strede elementu

Každá MIN má prvky priestorového aj časového prepojovania

- Priestorová zložitosť MIN - počet spojovacích elementov potrebných pre konštrukciu danej siete
- Časová zložitosť MIN - čas/oneskorenie paketu pri prechode sieťou

## Jednocestné unicast MIN s blokovaním

Unicast spojovacie siete - spájajú jeden vstup s jedným výstupom (v tom istom čase)

Jednocestné spojovacie siete - majú iba jednu cestu/možnosť spojenia medzi ľubovoľným vstupom a výstupom

Reprezentant: generalizovaná binárna sieť (GBN - Generalized Binary network)

## Generalizovaná binárna sieť

Veľkosť  $N \times N$  ( $2^n \times 2^n$ )

Vlastnosti:

- používa spojovacie elementy  $2 \times 2$ ,
- má  $n$  stupňov ( $0, 1, \dots, n-2, n-1$ )
- má  $2^{n-1}$  spojovacích elementov na stupeň
- pre funkciu spojenia medzi stupňami platí pravidlo susedstva
  - „Každý pár spojovacích elementov z  $i$ -teho stupňa je spojený len s jedným párom spojovacích elementov z  $(i+1)$  vého stupňa“

Označovanie

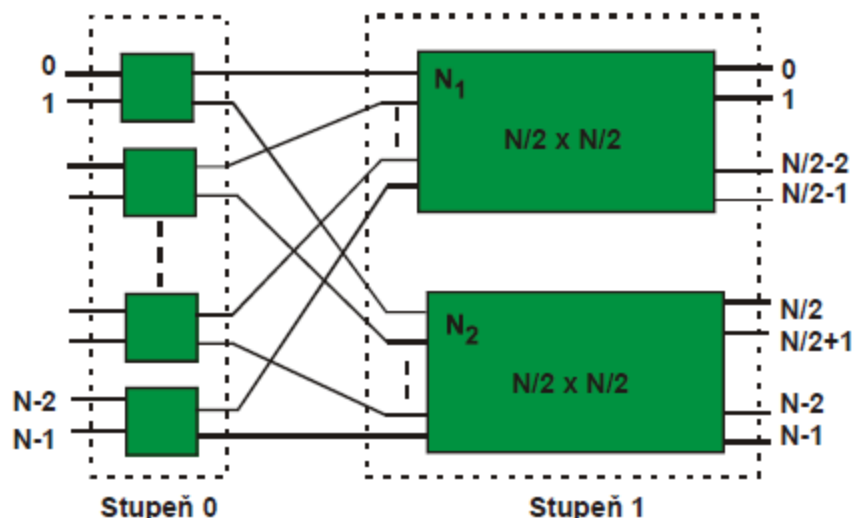
Každý vstup a výstup siete sú označené binárnym číslom (zhora nadol)

- vstup  $P = p_{n-1}p_{n-2} \dots p_1p_0$
- výstup  $D = d_{n-1}d_{n-2} \dots d_1d_0$

pre každý stupeň  $i$  v spojovacej sieti.

## Baseline sieť

Slúži ako referencia pre posúdenie iných GBN sietí  
Spojovacia funkcia medzi dvomi stupňami sa nazýva reverzné miešanie (Reverse Shuffle) a je definovaná:  $\text{reshuffle}(p_{n-1}p_{n-2} \dots p_1p_0) = p_0p_{n-1}p_{n-2} \dots p_2p_1$



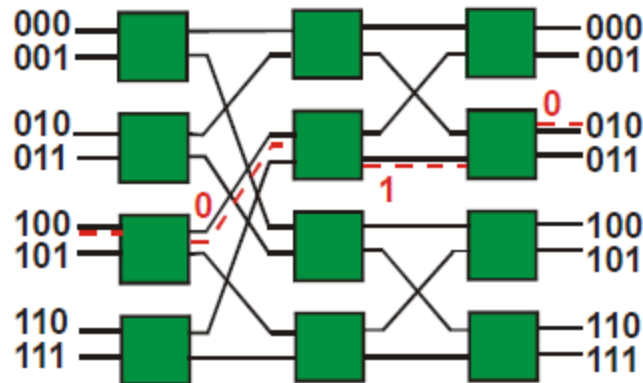
Výsledkom reverzného miešania je rotácia doprava

### Blokovanie

- Sieť má  $(N/2) \cdot \log_2 N$  spojovacích elementov
- Každý spojovací element má 2 stavy
- V sieti je možných  $2^{(N/2) \cdot \log_2 N} = N^{N/2}$  konfigurácií
- Ide o permutačnú sieť s množstvom permutácií  $N!$
- Pravdepodobnosť uskutočnenia spojenia/permutácie:  $P(N) = N^{(N/2)}/N!$
- Pravdepodobnosť vzniku blokády:  $B(N) = 1 - P(N)$

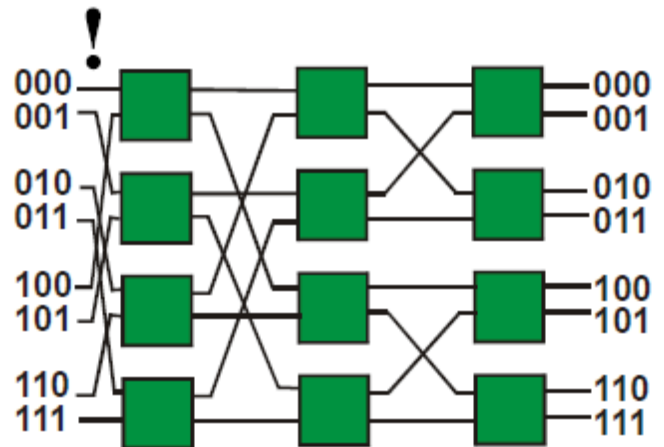
### Baseline sieť - samosmerovanie

- Smerovací tag = 010
- Smerovacia logika - 0 = horný výstup, 1 = dolný výstup



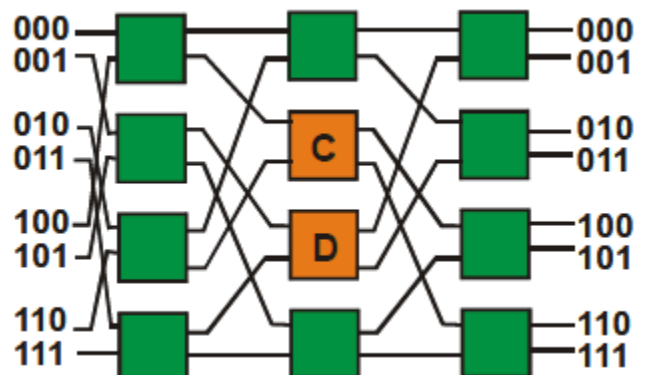
### Banyan sieť

- Nazýva sa aj generalizovaná kubická sieť
- Spojovacia funkcia medzi dvomi stupňami:  $cube_i(p_{n-1}p_{n-2} \dots p_1p_0) = p_{n-1}p_{n-2} \dots p_{i+1}p_i p_{i-1} \dots p_2p_1p_0$ , kde  $p$  označuje komplement  $p$
- Vzťah znamená, že na stupni  $i$  spojovacieho stupňa vstupujú do spojovacieho elementu linky s adresou, ktorá sa líši na mieste  $i$ .
- Pravdepodobnosť vzniku blokády:  $N = 8$ ,  $P(N) = 0,1$ ,  $B(N) = 0,9$



### Omega sieť

- Je charakterizovaná zmiešavacím (shuffle) algoritmom na každom stupni
- Spojovacia funkcia medzi dvomi stupňami:  $shuffle(p_{n-1}p_{n-2} \dots p_1p_0) = p_{n-2}p_{n-3} \dots p_1p_0p_{n-1}$



- Výsledkom dokonalého miešania je rotácia doľava
- Výmenou SE C a D dostaneme Banyan sieť
- Pravdepodobnosť vzniku blokády:  $N = 8$ ,  $P(N) = 0,1$ ,  $B(N) = 0,9$

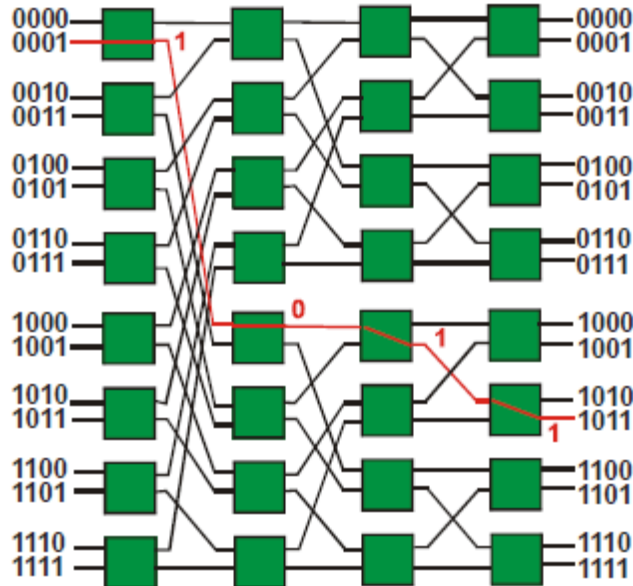
### Delta sieť

Definícia GBN predpokladá SE 2x2

Vo všeobecnosti počet vstupov a počet výstupov SE môže byť rôzny - (Irregular Networks)

Delta-b sieť:

- pravouhlá topológia  $N \times N$
- identické spojovacie elementy  $b \times b$
- počet stupňov je  $\log_b N = k$
- $N/b$  spojovacích elementov na stupeň
- $N = b^k$



### Viaccestné unicast MIN s blokovaním

- Zabezpečujú alternatívne cesty medzi vstupmi a výstupmi
- Zachovávajú samosmerovacie vlastnosti siete a len minimálne komplikujú časovú zložitosť
- Zlepšenie spoľahlivosti a priepustnosti siete

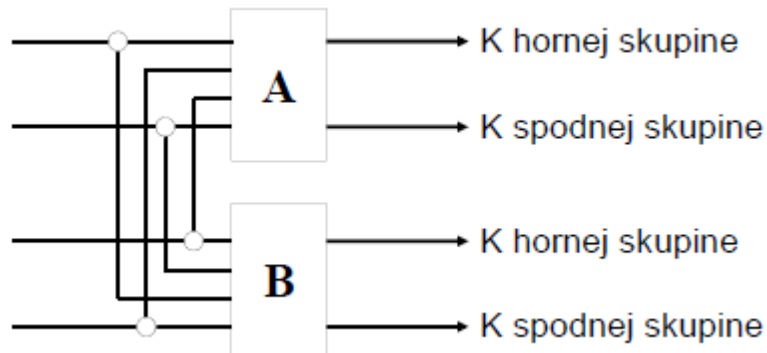
### Baseline sieť s delenou záťažou

Uvažujme:

- viacstupňovú Baseline sieť s  $n$  stupňami číslovanými od 0 po  $n-1$
- nech  $(s_{n-2} s_{n-3} \dots s_1 s_0)$  je binárne vyjadrenie polohy SE smerom zhora nadol v každom stupni  $\Rightarrow$  SE v  $i$ -tom stupni patria do tej istej skupiny, ak v ich binárnom vyjadrení je zľava  $i$  bitov totožných

Samosmerovanie:

- Paket môže byť poslaný do ktoréhokoľvek SE v jednej skupine a vždy dôjde na určený výstup bez zmeny smerovacej informácie (tag)
- Ak je niektorý SE blokovaný, ostatné SE v tej istej skupine spracujú prevádzku
- Podmienka dosiahnutia alternatívnej cesty
- z vyššie spomenutého vyplýva, že SE sa **musia párovať**
- Čím viac SE v jednom stupni sa podieľa na prevádzke, tým viac alternatívnych ciest sieť poskytuje



## Unicast MIN bez blokovania

Siete s blokovaniím - vyžadujú opatrenia na potlačenie blokovania

- najčastejšie - umiestnenie vyrovnávacích pamätí v sieti
- iné riešenie - siete bez blokovania

Siete bez blokovania:

- topologicky bez blokovania
- riadením bez blokovania

## Benešova sieť (Sériová baseline sieť)

- Využíva princíp viacnásobného radenia jednocestných GBN
- Topológia môže byť generovaná rekurzívnym spôsobom s využitím dokonalého a reverzného miešania

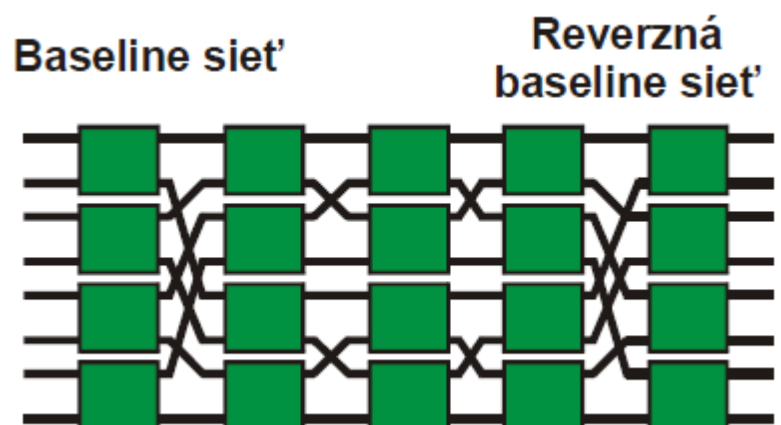
Sieť má:

- $(2\log_2 N - 1)$  stupňov
- v každom stupni  $N/2$  spojovacích elementov

Benešova sieť = rekonfigurovateľná sieť bez blokovania => vyžaduje algoritmus pre rekonfiguračný proces

Rekonfiguračný algoritmus pre:

- centralizované riadenie - existuje (napr. slučkový rekurzívny algoritmus)
- decentralizované riadenie - neexistuje (vhodnejšie pre FPS)



## Paralelná baseline sieť



Nevýhody sériovej baseline siete:

- obtiažne lokalizovanie chybných SE
- veľký počet stupňov

=> Paralelná baseline sieť

- Pozostáva z m baseline podsietí radených paralelne
- Na vstupe a výstupe siete je realizovaná funkcia expanzie a koncentrácie

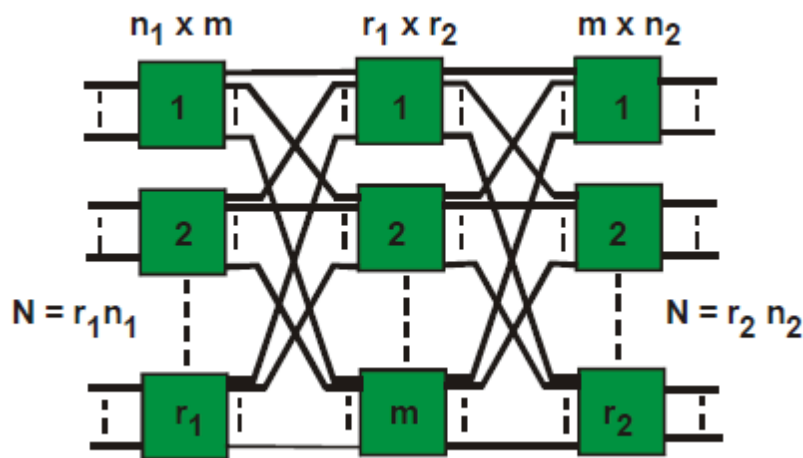
Počet stupňov (ak nerátame vstupné a výstupné stupne) = počet stupňov v baseline podsieti

Podmienka bezblokovosti pre rekonfigurovateľnú paralelnú sieť: ak  $n = \log_2 N$  je počet stupňov v baseline podsieti, tak počet paralelných podsietí  $N \times N$  musí byť  $m \geq 2^{(n/2)}$

### Closova sieť

Topologicky bez blokovania nevyžaduje algoritmus pre rekonfiguráciu siete

Podmienka bezblokovosti  $m \geq (n_1-1) + (n_2-1) + 1 \Rightarrow m \geq n_1 + n_2 - 1$



### Batcherova sieť

- Je určená pre prepájanie paketov s jednou, pevne stanovenou dĺžkou
- Nemá smerovacie vlastnosti
- Triedi vstupujúce pakety podľa ich adresy výstupu (od najmenších adres k najväčším)
- Použitý prvok - bitonický triedič 2x2

### Bitonický triedič

Dva druhy elementov - „+“ a „-“

Ak je na vstupe elementu len jeden paket - je smerovaný akoby mal nižšiu adresu



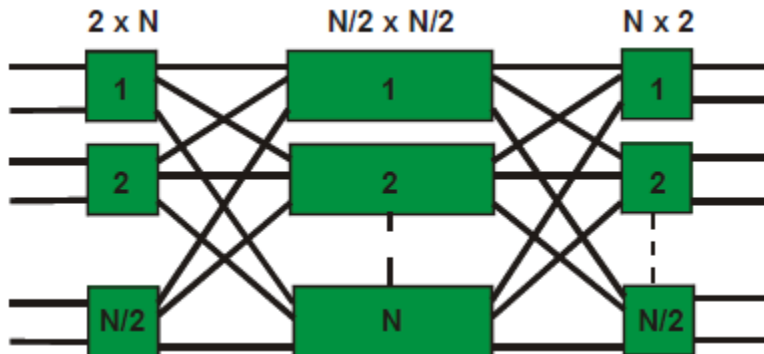
### Multicast siete

- Ľubovoľná skupina vstupov sa môže prepojiť s ľubovoľnou množinou výstupov
  - každý vstupný port môže byť spojený s viac ako jedným výstupným portom
  - každý výstupný port je zvyčajne spojený najviac s jedným vstupným portom
- Môžu uskutočniť NN rôznych spojení (unicast siete len N!)
- Ako multicast sieť môže fungovať každá unicast sieť ktorej spojovacie elementy dokážu

prepojiť svoje vstupy na viac výstupov

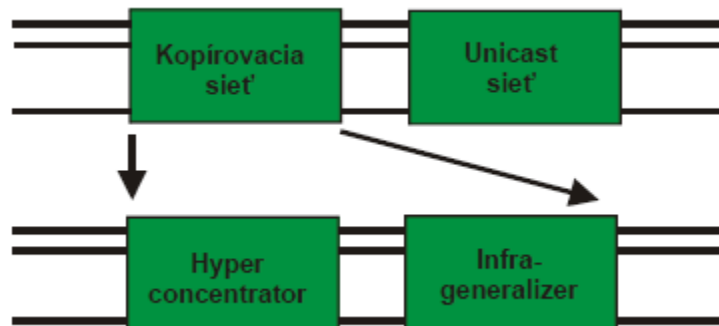
### Closova multicast sieť

- Trojstupňová sieť
- Vstupný a výstupný stupeň majú multicast vlastnosti
- Stredný stupeň nemá multicast vlastnosti



### Kaskádne siete

Kopírovacia sieť vytvorí viacnásobné kópie paketov, ktoré sú následne smerované v normálnej unicast sieti.



## Radenie paketov: QMM, QSD.

### Architektúra spojovacieho systému

Charakteristika

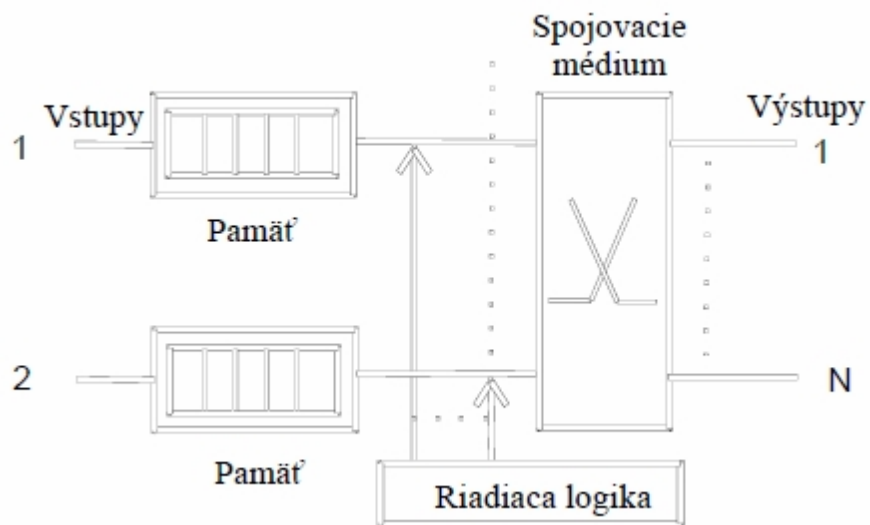
- Prepínač  $N \times N$
- Predpokladajme:
  - pakety konšt. dĺžky (ATM)
  - vstupy/výstupy prenášajú dáta rovnakou prenosovou rýchlosťou
- Spojovacia sieť (MIN) môže pracovať  $M$  krát rýchlejšie, ako je rýchlosť vstupných/výstupných liniek (počas trvania jedného paketu môže byť prenesených  $M$  paketov)
- Súčasne môže prísť na vstupy niekoľko paketov, ktoré majú byť smerované na rovnaký výstupný port => preťaženie
  - **Sieť musí byť schopná radiť pakety do radu**

MIN bez vyrovnávacích pamätí

- V prípade kolízie paketov sa prenáša iba jeden paket (ostatné sú zahodené).
- Výpočet priepustnosti prepínača

- Predpokladajme, že pakety prichádzajú v časových intervaloch (ATM bunky) s pravdepodobnosťou  $p$  (Bernoulliho rozdelenie)
- Pre  $N \rightarrow \infty$  platí pre priepustnosť prepínača vzťah  $(1 - e^{-p})$
- Maximálna priepustnosť ( $p=1$ ) je **0,632**
- Pravdepodobnosť, že paket bude zahodený je **0,368**

### Umiestnenie pamätí Riadenie na vstupe



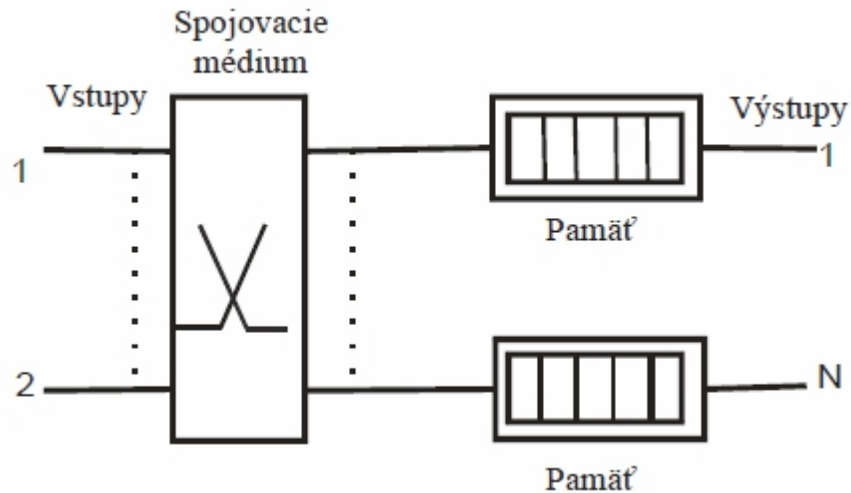
#### FIFO buffer

- Každý vstup obsahuje vyrovnávaciu pamäť typu FIFO
- Slabina – Head of line (HOL) blocking (blokovanie prvým v rade)
- Max. priepustnosť pre exponenciálne rozdelenie dĺžky paketu a Poissonove rozdelenie pravdepodobnosti príchodu paketov je okolo 0,5

#### Nie FIFO buffer

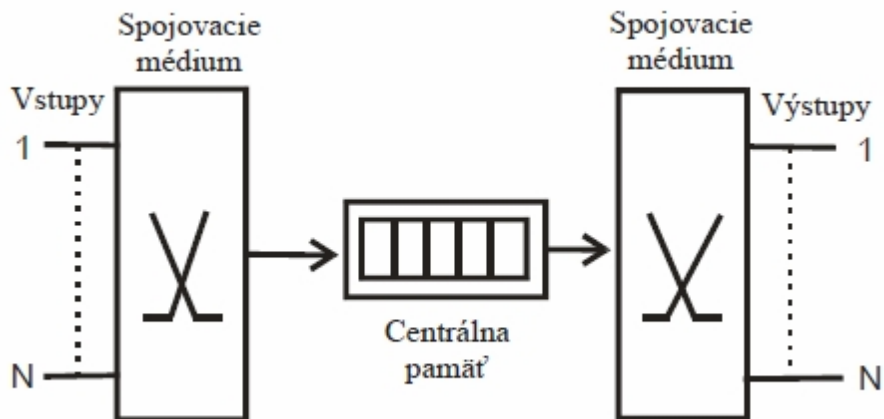
- Pre výber paketov sa využíva oknová metóda, alebo predpovedanie kolízie
- Ak nastane kolízia, na vyslanie sa vyberajú postupne pakety z prvých  $W$  paketov ( $W$  je veľkosť okna) v každom vstupnom rade.
- To sa opakuje dovtedy (max.  $W$  krát), kým sa nenájde paket, ktorý môže byť vyslaný → potláča sa HOL blocking.
- Dosahuje dobré výsledky (najmä pre malé  $N$  a veľké  $W$ )

### Riadenie na výstupe



- Vyrovnávacie pamäte sú umiestnené na výstupoch
- Spojovacia sieť pracuje M krát rýchlejšie, ako je rýchlosť vstupných liniek
- Dôsledok – sieťou môže prejsť M paketov určených pre jeden výstup, ktoré musia byť zapísané do výstupného radu.
- Nevyskytuje sa HOL blocking
- Nevýhoda – vyžaduje sa, aby interná rýchlosť spajovania bola vyššia -> má dopad na max. veľkosť prepínača

#### Centrálne zdieľaná pamäť



- Radenie sa uskutočňuje v centrálnej pamäti, ktorú zdieľajú všetky vstupné porty.
- Centrálne zdieľaná pamäť musí byť schopná uskutočniť N zápisov a N čítaní počas jedného cyklu
- Obmedzuje veľkosť prepínača.

#### Virtuálne radenie na výstupe

- Netrpí na HOL blocking
- Zachováva škálovateľnosť radenia na vstupe
- Potrebuje dobrý algoritmus na výber paketov, byť ktoré majú vyslané zo vstupných

portov na výstupné porty

- Umožňuje dosiahnuť až 99% priepustnosť

### **Aktívny manažment radu**

#### **Metódy manažmentu radu**

- **QMM** (Queue Memory Management)
  - Kontroluje počet paketov vo výstupnom rade.
  - Vykonáva sa pri operácii zaradenia prichádzajúceho paketu do radu.
- **QSD** (Queue Scheduling Disciplines)
  - Riadi veľkosť šírky prenosového pásma prideleného každej servisnej triede vo výstupnom rade.
  - Vykonáva sa pri výbere paketu z radu a jeho poslaní na výstupnú linku.

### **QMM**

Zabezpečuje:

- Pridávanie paketov do príslušného radu (napr. podľa ich klasifikácie a pod)
- Zahadzovanie paketov, ak je rad plný
- Vyberanie paketov vysielanie príkazov plánovača (scheduler)
- Voliteľne: monitorovanie zaplnenie radov a odstraňovanie paketov ešte pred zaplnením radu, alebo označovanie paketov pre neskoršie odstránenie

### **Radenie po skupinách**

- Pakety skupiny tokov/volaní patriacich k rovnakej kategórie služieb sú radené spoločne v jednom rade
- Garancie platia pre agregované toky, nie pre individuálne toky/volanía.
- Dobrá škálovateľnosť (relatívne malý počet kategórií)

### **Riadenie po tokoch**

- Pakety sú radené v individuálnych radoch pre každý tok.
- Garancie platia pre každý individuálny tok.
- Zlá škálovateľnosť (smerovač/prepínač si musí udržiavať stavové informácie o každom individuálnom toku)

### **Preťaženie siete**

- Krátkodobé – spôsobené krátkymi zhlukmi dát z niekoľkých tokov
- Dlhodobé – spôsobené dlhodobým pôsobením všetkých tokov využívajúcich príslušný rad

Reakcie QMM

- Označovanie paketov
- Zahadzovanie paketov
- Informovanie zdroja o preťažení

### **Výber paketu pre zahodenie**

Prichádzajúci paket

- Jednoduchá realizácia (paket sa nezarád do radu)
- Prichádzajúce pakety majú tendenciu mať väčšie oneskorenie a pre real time aplikácie sú „menej užitočné“

Paket na čele radu (DFF, Drop From Front)

- Náročnejšie na manipuláciu s radom,
- Pre niektorých službách (napr. TCP) – rýchlejšia reakcia na preťaženie siete

### **Algoritmy zahadzovania paketov**

#### **Tail Drop**

- Najjednoduchšia technika zahadzovania paketov
- Rad sa plní FIFO princípom, keď je plný, ďalšie prichádzajúce pakety sa automaticky zahadzujú
- Koncové uzly nie sú spravidla o zahadzovaní informované a musia stratu paketu detegovať samostatne
- Môže viesť k tzv. „globálnej synchronizácii“ (napr. pri TCP), kedy rýchlosť prevádzky osciluje medzi preplnenými a prázdny FIFO radmi

#### **Selective Discard**

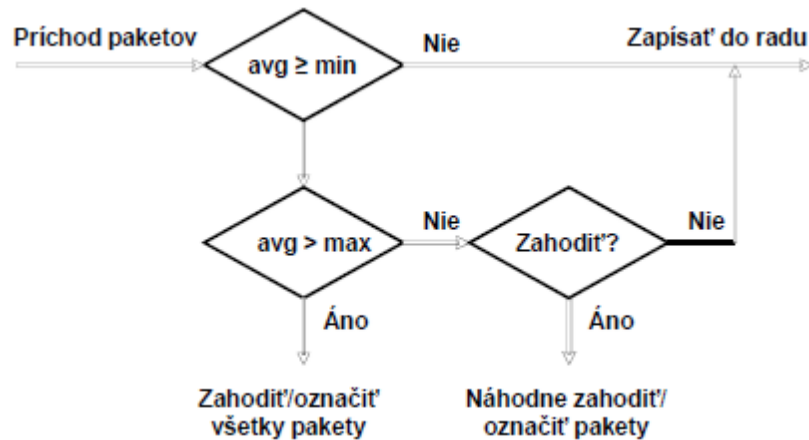
- Policing umožňuje, aby vstupný (ingress) sieťový uzol označoval pakety prekračujúce dohodnuté parametre za pekety s nižšou prioritou
- Možno implementovať v:
  - ATM - CLP bit
  - IP -Diffserv
  - MPLS -Exp bity
- Takto označené pakety sú zahadzované prednostne
- Pri extrémnom preťažení sú zahadzované aj pakety s vyššou prioritou --> potreba implementácie preventívnych mechanizmov

#### **Early/Partial Packet Discard**

- Vhodné špeciálne pre ATM
- Strata jednej bunky má za následok stratu celého paketu => Efektívnejšie je robiť zahadzovanie na úrovni rámcov ako na úrovni buniek.
- Na označenie poslednej bunky AAL5 PDU slúži PTI (Payload Type Indicator) v ATM bunke
- **Early Packet Discard (EPD)**
  - Zariadenie v stave preťaženia zahadzuje všetky bunky z AAL5 PDU
  - Ak bol povolený zápis paketu do pamäte rezervuje sa pamäťová kapacita pre všetky bunky z paketu.
- **Partial Packet Discard (PPD)**
  - Ak musí zariadenie zahodiť bunky zo stredu paketu, sú zahodené aj všetky nasledujúce bunky daného paketu.
  - Aplikuje sa, keď niektoré bunky z paketu už boli zapísané do pamäte.

#### **Random Early Detection (RED)**

- QMM technika často implementovaná na IP smerovačoch
- Predpokladá spoluprácu s algoritmi pre kontrolu toku technikou predchádzania zahltenia (obsahuje ju napr. TCP)
- RED používa tzv packet drop profil vyjadruje závislosť tzv. – medzi pravdepodobnosťou zahodenia prichádzajúceho paketu a zaplnením radu.



#### Výhody:

- Zavedenie RED nevyžaduje modifikáciu TCP protokolu
- Prístup k riešeniu zahltenia je proaktívny a nemalo by nikdy dôjsť k úplnému zaplneniu radu a následnému tail drop zahadzovaniu
- Zachováva sa podpora zhlukovej prevádzky, keďže ide o FIFO radenie. Pakety sú vysielané v tom poradí, v akom prišli. (Nevýhodou môže byť, že niektoré pakety zo zhlukovej prevádzky budú zahodené.)
- RED podporuje TCP, lebo nezahadzuje zhľuky paketov z jediného TCP toku v dôsledku preplnenia
- RED umožňuje držať naplnenosť radu pod určitou úrovňou a pomáha k lepšiemu využitiu prenosovej kapacity výstupnej linky. Množstvo paketov držaných v rade nie je ani príliš malé, čo by mohlo viesť k poddimenzovaniu výstupnej kapacity a ani sa neblíži k plnej kapacite, keď by sa museli zahodiť všetky prichádzajúce pakety z množstva TCP spojení, ktoré by následne znížili rýchlosť.
- RED podporuje teoreticky férové zahadzovanie paketov medzi jednotlivými TCP spojeniami – pričom si nemusia udržiavať stavovú informáciu pre každé spojenie.

#### Nevýhody:

- RED môže byť dosť ťažké nastaviť tak, aby dával očakávané výsledky
- RED pracuje dobre iba s TCP protokolom a s jeho algoritmi na predchádzanie zahlteniu.
- Zahadzovanie paketov nie je veľmi efektívny signál oznamujúci zahltenie. Plytvajú sa pri ňom sieťové prostriedky (paket musí byť znovu preposlaný).

### Weighted RED (WRED)

Rozširuje RED o možnosť priradiť rôzne drop profily rôznym typom prevádzky

#### Využitie:

- Viac rôznych profilov jedného radu v rámci radu.
- Rôzne profily pre jednotlivé rady (ak existuje viac radov, napr. existuje samostatný rad pre každú triedu služby)

### Adaptive Virtual Queue (AVQ)

- Nepočíta pravdepodobnosť zahodenia paketu, ale určuje kapacitu virtuálneho radu.
- Spravuje tzv. virtuálny rad, ktorého kapacita je nižšia ako skutočná kapacita výstupnej linky. Keď je paket zaradený do reálneho radu je aktualizovaný aj virtuálny rad.



- Keď virtuálny rad pretečie:
  - pakety sú zahodené alebo označené,
  - na každej linke je prepočítaná virtuálna kapacita, aby sa zabezpečilo, že celkový dátový tok smerovaný na linku dosahuje požadovanú úroveň využitia linky.
- AVQ rozhoduje o označení/zahodení na základe rýchlosti prichádzajúcich dát a nie na základe dĺžky radu -> zabezpečuje to rýchlu reakciu systému.
- Namiesto dĺžky radu reguluje využitie linky -> dosahuje vyššiu odolnosť a stabilitu pri extrémne výskyte krátkych tokov dát, alebo pri meniacom sa počte dlhých tokov.
- Dĺžka radu pri AVQ je v porovnaní s inými metódami pomerne nízka a výrazne sa nezvyšuje ani pri rastúcom zaťažení siete.
  - Využitie linky sa stabilne pohybuje okolo požadovanej úrovne (teda nie je maximálne)
  - Straty sú nižšie ako pri iných algoritmoch.

## Algoritmy QSD

### FIFO

Výhody:

- Oneskorenie závisí len od veľkosti radu
- Nízka výpočtová náročnosť
- Zachováva zhlukový charakter vstupnej premávky

Nevýhody:

- Neumožňuje diferencovaný prístup k paketom rôznych tried
- Nevhodný pre real-time a garantované služby
- Oneskorenie všetkých paketov rastie úmerne s nárastom zaťaženia siete
- Zvýhodňuje UDP toky pred TCP tokmi
- Nepriamo podporuje zhlukové toky - môžu pohltiť väčšinu kapacity FIFO radu

### Priority Queuing (PQ)

Rozoznávame dva modely implementácie PQ:

- PQ so striktnou prioritou (Strict PQ) - pakety s vyššou prioritou sú vždy odoslané pred paketmi s nižšou prioritou.
- PQ s nastaviteľnou šírkou pásma (Rate-controlled PQ) – pakety s vyššou prioritou sú uprednostnené pred paketmi s nižšou prioritou iba ak prevádzka vo vyššej prioritě nepresahuje stanovenú úroveň (napr. 20% výstupnej šírky pásma).

Výhody:

- Nízka výpočtová náročnosť - vhodné aj pre softvérové smerovače.
- PQ umožňuje zaviesť diferencovanie prevádzky. *Prevádzka s vyššou prioritou (napr. real-time prevádzka citlivá na oneskorenie) môže byť uprednostnená pred best-effort prevádzkou.*
- Vie zabezpečiť stabilitu siete počas zahltenia priradením najvyššej priority riadiacim signálom siete.

Nevýhody:

- Ak sa tok s vyššou prioritou približuje ku kapacite linky alebo ju presahuje, dochádza k výraznému oneskoreniu alebo až zastaveniu služby s nižšou prioritou.
- Triedy s rovnakou prioritou sú smerované rovnako, ako keby bolo použité FIFO radenie.

- Nerieši problém férovosti medzi TCP a UDP. Ak je TCP v triede s vyššou prioritou a neobmedzí sa, snaží sa využiť celú kapacitu linky na úkor UDP.

### Fair Queuing (FQ)

Výhody:

- Extrémne zhlukové toky, alebo toky ktoré sa chovajú zle, nemajú žiadny vplyv na QoS poskytovanú ostatným tokom, pretože toky sú navzájom izolované.

Nevýhody:

- Toky sú obsluhované rovnako -> nie je možné zvýhodniť jeden pred ostatnými a tak zabezpečiť QoS.
- Rovnaká obsluha je zachovaná iba pri paketoch presne rovnakej veľkosti -> toky s dlhšími paketmi dostanú väčšiu časť odchodzej kapacity ako toky s krátkymi paketmi.
- Je závislý na poradí príchodu paketov.
- Fair queuing nemá jednoduchý mechanizmus na podporu real-time služieb.
- Vo veľkých IP sieťach s desať tisícmi spojení by bolo potrebné obsluhovať pre každé spojenie samostatný FIFO rad -> neúnosné, spomaľujúce a ťažké na efektívnu implementáciu.
- FQ predpokladá, že vieme jednoducho a presne klasifikovať pakety do tokov -> možné zneužitie otvorením viacerých tokov

### Class-based Fair Queuing (FQ)

Vylepšenie - rozčlenenie kapacity linky podľa tried, napr.: 20 % kapacity linky pre toky so zárukou QoS (napr. pre VoIP toky), 80 % kapacity linky (pre ostatné dátové toky).

### Weighted Fair Queuing (WFQ)

Výhody:

- Každý rad má garantovanú minimálnu výstupnú kapacitu nezávisle na správaní ostatných radov.
- Pri kombinácii s riadením prevádzky na okraji siete WFQ zaručuje rovnomerné rozdelenie výstupnej kapacity, vzhľadom na váhu jednotlivých radov, s obmedzením oneskorením.

Nevýhody:

- Výpočet a zoradenie paketov podľa časov je výpočtovo náročné
- Silná zhluková prevádzka môže ovplyvniť ostatné toky v tom istom rade.
- Výpočtová zložitosť obmedzuje použitie WFQ v rýchlych zariadeniach s veľkým počtom tried.
- Aj napriek garantovanému oneskoreniu môžu byť iné algoritmy lepšie pre svoj jednoduchší výpočet.
- Pri N radoch s váhami  $w_1, w_2, \dots, w_N$  bude i-temu radu pridelená približne rýchlosť

$$R_i = \frac{R \cdot w_i}{\sum w_i}$$

Vylepšenia WFQ:

- **Class-based WFQ (CBWFQ):**
  - Používa užívateľom definované triedy na základe rôznych parametrov ako je

protokol, vstupné rozhranie, nastavenie prioritných bitov v IP protokole.

- Pre každú triedu je vyhradený rad s pridelenými parametrami ako šírka pásma, váha a maximálna veľkosť paketu a ich počet v rade.
- Pri prekročení tohto limitu dochádza k zahodeniu paketov.

- **Self-clocking Fair Queuing (SCFQ):**
  - Zjednodušuje výpočtovú náročnosť času, podľa ktorého sa pakety odosielajú, čo znižuje oneskorenie paketov.
- **Worst-case Fair Weighted Fair Queuing (WF2Q):**
  - Približuje sa viac ku GPS (General Processor Sharing).
  - Neuvažuje len čas za odoslal v GPS ale čas, ktorý by sa paket GPS, aj čas príchodu paketu.
- **Worst-case Fair Weighted Fair Queuing+ (WF2Q+):**
  - Implementuje novú funkciu virtuálnych hodín.
  - Je výpočtovo menej náročný a presnejší.

### **Weighted Round Robin (WRR)**

Výhody:

- WRR môže byť implementovaný hardvérovo, takže môže byť použitý na vysokorýchlostných zariadeniach chrbiticovej siete.
- WRR vykonáva hrubú reguláciu percenta výstupnej kapacity pridelenej jednotlivým službám.
- V každom kole sa z každého FIFO radu vyšle aspoň jeden paket, t.j. nemôže dôjsť k „vyhladovaniu“.

Nevýhody:

- Správne rozdelenie výstupnej kapacity dosiahneme len pri zachovaní rovnakej veľkosti paketov. (Vhodné pre siete s fixnou dĺžkou paketov ako je napr. ATM.)

### **Deficit Weighted Round Robin (DWRR)**

- Má odstrániť nedostatky WRR aj WFQ
- Definuje niekoľko tried služieb, ktoré majú vlastné FIFO rady.
- Pre každú triedu sú definované nasledovné parametre:
  - Váha [F] pre každú tried (defino ané Algoritmy QSD – triedu rad F) definované percento z výstupnej kapacity linky
  - DeficitCounter [F] – premenná, ktorá pre každú triedu udáva, koľko bajtov z nej bolo v jednom kole DWRR poslaných
  - Quantum [F] – max počet bajtov, ktoré môže daný FIFO rad vyslať v jenom kole DWRR. Kvantum je odvodené od váhy pridelenej triede.

Každý rad F je obslužený nasledovne:

1. nastaví sa DeficitCounter:  $\text{DeficitCounter}[F] = \text{DeficitCounter}[F] + \text{Quantum}[F]$
2. z danej triedy F sa pošle toľko paketov aby suma ich dĺžok bola nanajvýš  $\text{DeficitCounter}[F]$ . Nech je to B bajtov.
3.  $\text{DeficitCounter}[F] = \text{DeficitCounter}[F] - B$
4. Obsluži sa ďalší rad F

Výhody:

- Rady sa navzájom neovplyvňujú.
- Zaručuje presné pridelenie výstupnej kapacity aj pri paketoch rôznej dĺžky
- DWRR zaručuje, že každý rad má prístup k výstupnej kapacite. Nemôže dôjsť k „vyhladovaniu“.
- Jednoduchý a výpočtovo nenáročný algoritmus -> možno ho nasadiť na

vysokorychlostné linky

Nevýhody:

- Nevie presne garantovať oneskorenie.
- Pri odosielaní paketov kým DeficitCounter nie je menší ako veľkosť paketu na začiatku radu spôsobuje radu, kolísanie oneskorenia (jitter). To sťažuje implementáciu real-time prevádzky.
- Toky v rámci radu sa navzájom ovplyvňujú .

## Širokopásmové technológie: ATM, MPLS, MPLS-TP, GMPLS, PB, PBB, PBB-TE.

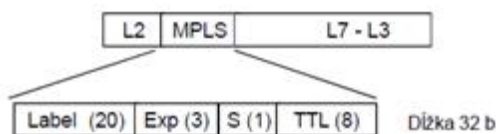
### Požiadavky na širokopásmové spojovacie prvky

- Veľký rozsah prepájaných prenosových rýchlostí
- Malé a konštantné oneskorenie signálu
- Bezchybný prenos informácie spojovacím poľom
- Spojovanie bez blokády
- Možnosť prepájať signály z jedného vstupu na viac, resp. všetky výstupy z poľa.

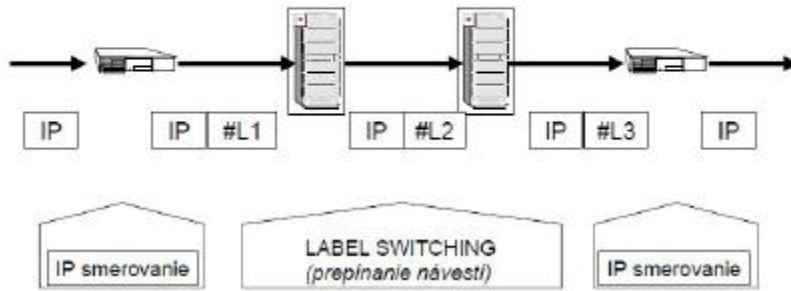
### MPLS Multiprotocol Label Switching

- Preferuje prepínanie paketov pred smerovaním. Pri vstupe IP paketu do siete MPLS je tomuto paketu priradená MPLS hlavička a ďalej je paket prepínaný na základe tejto hlavičky a nie je nutné vykonávať smerovanie (rozhodovanie kam poslať paket ďalej) v každom uzle, ktorým paket prechádza.
- Vhodný nielen pre IP
- Využitie:
  - VPN
  - Traffic Engineering (TE)
  - Quality of Service (QoS)
  - ATM over MPLS (AToM) ... tu je chyba v prednáške AToM znamená Any Transport over MPLS

MPLS - hlavička



## MPLS - princíp



- **Label** - návěstie (neštrukturované)
- **Exp** - *Experimental* – experimentálne použitie - v súčasnosti využívané ako pole Class of Service (CoS)
- **S** - *Bottom of Stack* (log.1 = spodok zásobníka)
- **TTL** - *Time to Live*

### LER Label Edge Router

Je to vstupný a výstupný bod siete MPLS, ktorý označí/odznačí (pridá/odoberie) MPLS hlavičku (značku) do paketu. V niektorých aplikáciách môže nastať, keď paket odovzdaný do LER už má MPLS hlavičku (label) a tento LER router mu pridá ďalšiu hlavičku.

### LSR Label Switching Router

Router, ktoré vykonávajú smerovanie na základe MPLS hlavičky

### LDP Label Distribution Protocol

Protokol na distribúciu MPLS hlavičiek (značiek) medzi jednotlivými LER a LSR

### LSP Label Switched Path

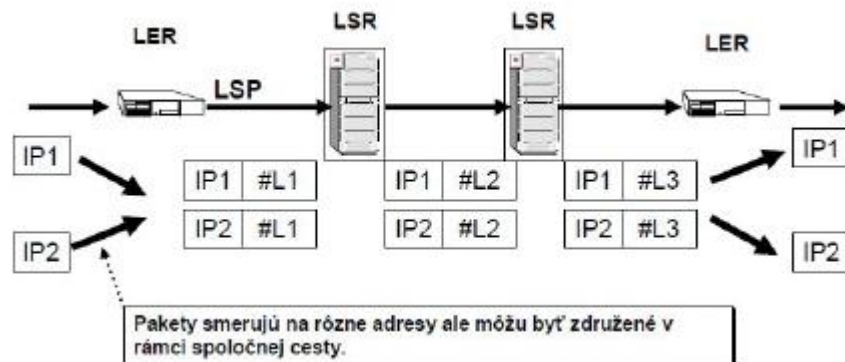
Cesta v sieti prepínaná na základe hlavičiek. Môže ju nastaviť operátor siete za rôznymi účelmi: vytvorenie VPN, na smerovanie prevádzky určitou cestou v sieti.

### FEC Forwarding Equivalence Class

FEC je skupina paketov, ktoré sú sieťou preposielané rovnakým spôsobom (po jednej ceste, s rovnakým pravidlom pre smerovanie atď.)

- Prevádzka v rámci FEC je v celej MPLS doméne prenášaná prostredníctvom konkrétnej LSP
- Vstupný LER priradzuje FEC pre pakety podľa:
  - IP adresy zdroja/cieľa
  - Čísla vstupného/výstupného portu
  - ID protokolu IP

*Príklad: Skupina paketov, ktoré majú adresu cieľa z určitého IP adresného priestoru a ktorých ToS (Type*



*of Service) bity sú identické*

- TTL chráni pakety pred nekonečným blúdením v sieti

- IPv4 aj IPv6 pakety majú pole špecifikujúce TTL
  - IPv4 paket = pole TTL
  - IPv6 paket = pole Hop Limit
- V IP sieťach každý smerovač dekrementuje TTL/Hop Limit (paket je zahodený, ak TTL=0)
- LSR neanalyzuje IP hlavičku => TTL je súčasťou MPLS hlavičky
- Vstupný LER nastaví pole TTL v MPLS hlavičke podľa aktuálnej hodnoty TTL/Hop Limit z IP paketu
- LSR :
  - dekrementuje o 1 TTL z MPLS hlavičky najvyššej úrovne.
  - ak:
    - hodnota TTL = 0, paket je zavrnutý
    - hodnota TTL > 0, LSR zapíše novú hodnotu TTL do MPLS hlavičky najvyššej úrovne
  - paket je vyslaný do nasledujúceho LSR
- Výstupný LER:
  - odstráni TTL z MPLS hlavičky
  - ak:
    - hodnota TTL = 0, IP paket je zavrnutý
    - hodnota TTL > 0, LSR zapíše novú hodnotu TTL do poľa TTL/Hop Limit IP paketu
  - paket je vyslaný do nasledujúceho uzla

## **GMPLS Generalized Multi-Protocol Label Switching**

Dopĺňa MPLS o schopnosť manažovať a riadiť zostavovanie a rušenie LSP cez niekoľko spojovacích technológií:

**PSC** (*packet switching*)

**L2SC** (*layer-two switching*)

**TDMSC** (*TDM switching*)

**LSC** (*wavelength switching*)

**FSC** (*fiber switching*)

- Sieť obsahujúca viac typov spojovacích technológií (napr. PSC a TDMSC), ktoré sú riadené jednou GMPLS riadiacou entitou sa nazýva **Multi Region Network (MRN)**
- Sieť obsahujúca uzly podporujúce viac spojovacích vrstiev (napr. LSC, TDM VC-11 a TDM VC-4-64c) riadené jednou GMPLS riadiacou entitou sa nazýva **Multi-Layer Network (MLN)**

### **Spoľahlivosť**

- Dôležitá vlastnosť GMPLS – automatizovaný manažment porúch.
- Porucha v jednom type siete môže byť izolovaná a odstránená bez negatívneho vplyvu na ostatné siete.
- GMPLS poskytuje ochranu pred poruchou kanálov (liniek):
- medzi dvomi susednými uzlami (span protection)
- v rozsahu koniec-koniec (path protection)

## **T-MPLS Transport-MPLS**

### **Charakteristika**

- Transportná technológia špecifikovaná ITU-T (G.8110.1/Y.1370.1) pre nasadenie v transportných sieťach telekomunikačných operátorov.
- Využíva podmnožinu funkcií MPLS

### **Rozdiely oproti MPLS:**

- používa obojsmerné cesty LSP (Label Switched Paths),
- nepodporuje PHP (Penultimate Hop Popping),
- nepodporuje spájanie LSP (tzv. *merging*),
- nepodporuje ECMP (Equal Cost Multiple Path).

## MPLS - TP (Transport Profile)

### Charakteristika

- Transportná technológia špecifikovaná IETF a ITU pre nasadenie v transportných sieťach telekomunikačných operátorov.
- Vychádza z pôvodnej IETF verzie MPLS
- Nahrádza T-MPLS
- Prináša výhody v oblasti:
- OAM (porovnateľné s SDH a OTH)
- Spolupráce s MPLS a PWE (Pseudowire Emulation) rovinnou riadenia a smerovania

**Ethernet** je založený na nápade, že počítače v sieti budú posilať správy spôsobom, ktorý pripomína rádio, ale prostredníctvom spoločného kábla alebo kanála, niekedy označovaného ako éter (ether). Každý počítač má globálne jedinečnú 48-bitovú MAC adresu, ktorú má každá karta pridelenú od výroby, aby bolo zabezpečené, že všetky systémy v spoločnom Ethernete majú rozdielne adresy. Kedyž stanice obdrží paket s jinou než vlastní adresou, zahodí jej. Pro prístup ke sdílenému přenosovému médiu (sběrnici) se používá metoda CSMA/CD (Carrier Sense with Multiple Access and Collision Detection), česky metoda mnohonásobného přístupu s nasloucháním nosné a detekcí kolizí. Prenosove media: koaxial, krutena dvojlinka, optika Verzie Ethernetu: Ethernet(10Mbits), FastETH(100), Giga a 10Gigabitovy

### Carrier Ethernet

??Carrier Ethernet je štandardizovaná carrier-štandardizovaná, carrier class služba a sieť definovaná piatimi tribútmi, ktoré ho odlišujú od LAN Ethernetu.

Sú to:

Štandardizované služby

Škálovateľnosť

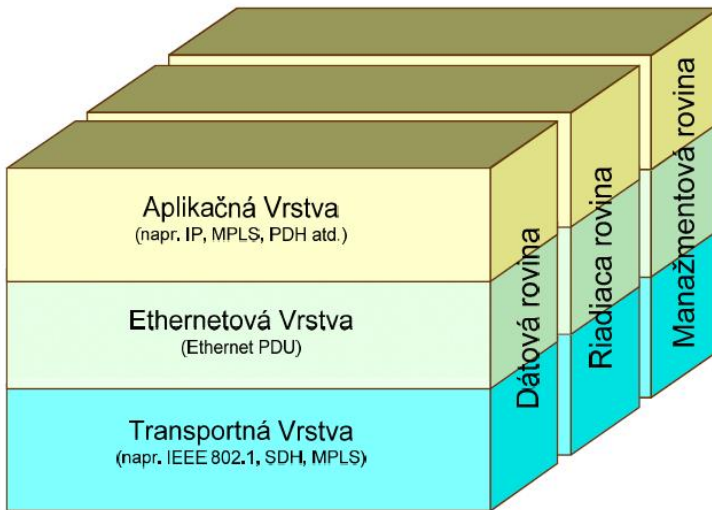
Spoľahlivosť

Kvalita služby

Manažment služby

### Vrstvový model CE



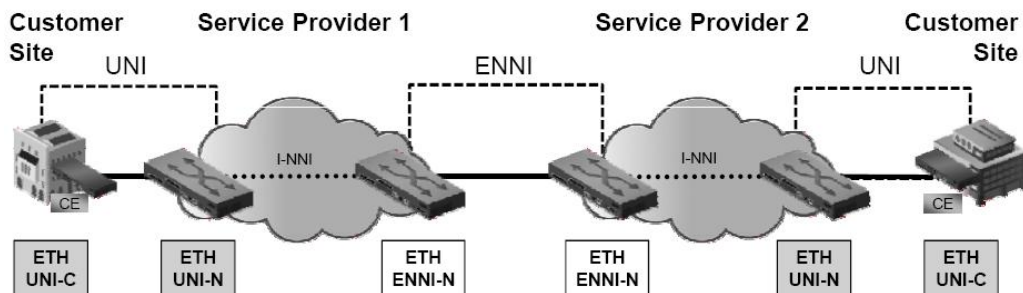


Dátová rovina - zabezpečuje prvky siete, ktoré smerujú ethernetové toky a podporuje prenos zákaznických datagramov sieťou.

Riadiaca rovina - ovláda funkčné prvky, ktoré riadia distribuované ethernetové toky v sieťových prvkoch dátovej roviny. Táto rovina tiež zabezpečuje signalizáciu potrebnú pre zostavenie, udržanie a ukončenie spojenia ako aj iné kontrolné funkcie.

Manažmentová rovina - zabezpečuje funkcie FCAPS a OAM.

## Architektúra CE



### UNI User Network Interface

UNI-C UNI-customer side

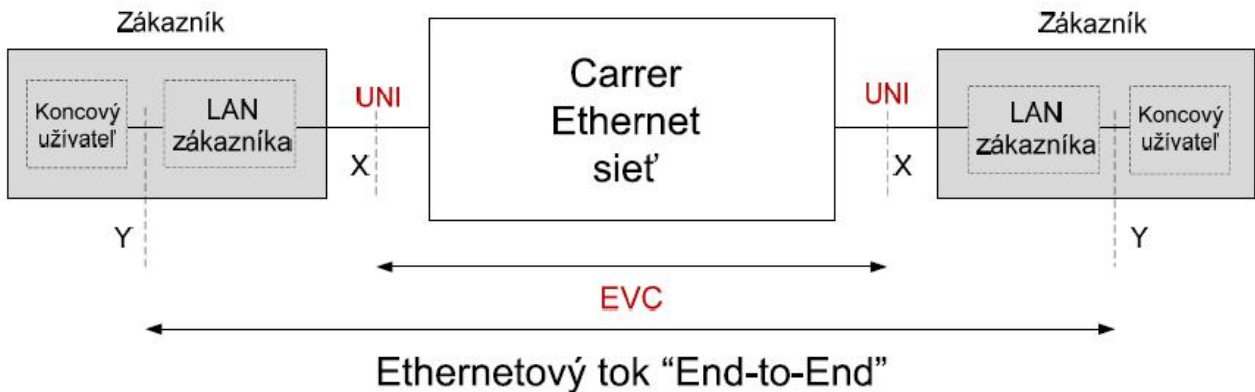
UNI-N UNI-network side

### NNI Network to Network Interface

ENNI External NNI

I-NNI Internal NNI

## Referenčný model CE siete



Požiadavky na UNI sú definuje MEF11 /Metro Ethernet Forum/  
 EVC (Ethernet Virtual Connection) je komunikačný vzťah medzi dvoma alebo viacerými UNI rozhraniami vytvorený za účelom prenosu ethernetových tokov po metropolitnej sieti operátora.

Do jedného EVC môže byť namapovaných viacero ethernetových tokov.

## CE služby

### E-Line (Ethernet Line)

služba na prepojenie dvoch UNI

Varianty:

**EPL** (Ethernet Private Line)

**EVPL** (Ethernet Virtual Private Line)

**E-LAN** (Ethernet Private LAN)

### EPL (Ethernet Private Line)

Služba typu bod-bod - vzájomne prepája pár UNI rozhraní

Na jeden fyzický port je vytvorené jedno EVC.

Nepovoľuje multiplexovanie služieb

Je to rámcovo a VLAN transparentná služba:

o Všetky rámce sú mapované do jedného EVC (tzv. all to one bundling).

o Rámce vstupujúce do zdrojového UNI sú identické s rámcami

vystupujúcimi z cieľového UNI.

### EVPL (Ethernet Virtual Private Line)

Nahrádza technológiu ako ATM multilexovaním služieb.

Pre jedno UNI je umožnený väčší počet virtuálnych spojení (jedným fyzickým portom môže byť prenášaný väčší počet EVC)

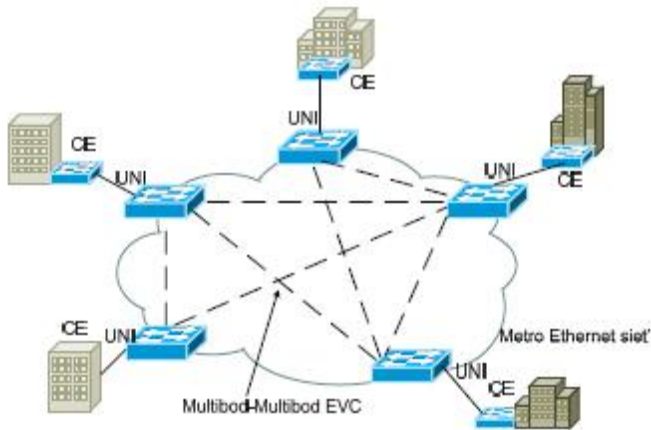
Od tejto služby nie je požadovaná úplná transparentnosť prenosu rámcov (rámce patriace rôznym VLAN môžu byť mapované do rôznych EVC)

### E-LAN (Ethernet Private LAN)

Služba na vytváranie multibodových L2 VPN spojení a transparentných LAN

služieb ako aj ich multiplexovanie,

Základ pre ethernetové multicast siete využívané pre broadcastové služby ako napr. IPTV

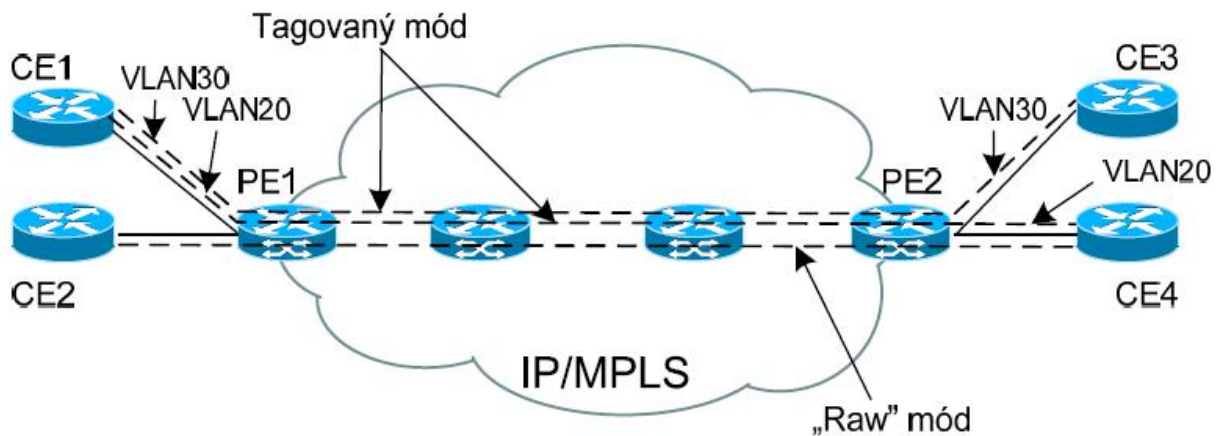


## Ethernet cez MPLS

Ethernetový rámec je prenášaný bez pridania akejkoľvek hlavičky a virtuálna cesta môže byť v dvoch módoch:

„Raw“ mód – reprezentuje virtuálny spoj medzi dvomi eth. portami. Môže ním prechádzať tagovaná alebo netagovaná prevádzka.

Tagovaný mód – reprezentuje spojenie medzi dvomi VLAN. Každá VLAN ide po inej virtuálnej ceste a je inak prepájaná sieťou.



## QoS v sieťach: Ethernet, FR, ATM, IP, MPLS. NGN.

### Definícia

služby = Kvalita spoločný vplyv jednotlivých parametrov služby, ktoré determinujú spokojnosť používateľa služby. [ITU-T E.800]

- Kvalita služby (Quality of Service - QoS) umožňuje posúdiť, ako sa poskytovaná služba približuje parametrom kontrahovanej služby.
- Na kvalitu služby poskytovanú zákazníčkovi majú vplyv:

- operačné kritéria,
- výkonnostné kritéria špecifické pre službu.

### **QoS pre prenos hlasu, požiadavky:**

- Oneskorenie (podľa G.114)
  - < 150 ms - jednosmerné oneskorenie
  - < 200 ms – neverejné siete max 250 ms
- Jitter
- Strata informácie

### **R - faktor** - „Hodnotiaci faktor“

Metrika na numerické vyjadrenie hlasovej kvality zohľadňujúca vnímanie účastníkom, ako aj celkový vplyv znehodnotenia zariadením.

### **QoS vo Frame Relay**

- Charakteristika FR
- QoS parametre
- CIR (Committed Information Rate)  $CIR = Bc/Tc$
- EIR (Excess Information Rate)  $EIR = Be/Tc$
- Mechanizmy na ochranu pred preťažením siete
- DE (Discard Eligibility)
- FECN (Forward Explicit Congestion Notification)
- BECN (Backward Explicit Congestion Notification)

### **Prostriedky na zabezpečenie QoS v ATM:**

- CAC (Connection Admission Control)
- UPC (Usage Parameter Control)
- Traffic shaping:
  - Implementovaný na vstupe do ATM siete
  - Zabezpečuje dodržiavanie prevádzkového kontraktu (napr. Leaky Bucket)
- Traffic policing:
  - Dohľad nad VC z pohľadu dodržiavania prevádzkového kontraktu
  - Pri prekročení prevádzkového kontraktu:
    - bunka bude zahodená
    - bunka bude označená (CLP - Cell Loss Priority)
  - Aplikovateľné na úrovni:
    - buniek (základné)
    - rámcov (napr. PPD /Partial Packet Discard/ a EPD /Early Packet Discard/ pre AAL5)

### **QoS v IP**

IPv4 - nemá implicitnú podporu QoS

- IPv6 – „predpripravené“ pre podporu QoS, v súčasnosti nie

je špecifikovaný žiadny špeciálny mechanizmus podpory QoS

- **Techniky na zabezpečenie QoS**

- Integrované služby (IntServ) **Nevýhody IntServ**

- Všetky zariadenia cez ktoré prechádzajú IP pakety dátových tokov, pre ktoré je potrebné zaručiť QoS musia podporovať RSVP.
- Každý smerovač v sieti musí udržiavať stavovú informáciu pre každú rezerváciu (dátový tok s požiadavkou na QoS).
- Vysoké nároky na implementáciu v rozsiahlych sieťach

- Diferencované služby (DiffServ)

**Využíva zlučovanie** (agregáciu) dátových tokov do tried:

- Okrajovésmerovače (resp. koncové zariadenia) zadeľujú a označujú pakety do jednotlivých tried
- Vnútorne smerovače spracovávajú pakety podľa ich označenia po skupinách tokov
- Definuje PHB (Per-Hop-Behavior) – chovanie uzla podľa vopred definovaných kritérií sieťovej politiky

**Nevýhody IntServ**

- Všetky zariadenia cez ktoré prechádzajú IP pakety dátových tokov, pre ktoré je potrebné zaručiť QoS musia podporovať RSVP.
- Každý smerovač v sieti musí udržiavať stavovú informáciu pre každú rezerváciu (dátový tok s požiadavkou na QoS).
- Vysoké nároky na implementáciu v rozsiahlych sieťach

## **QOS v MPLS**

Podpora QoS prostredníctvom MPLS–DiffServ (DiffServ-TE)(Max. 8 tried TE)

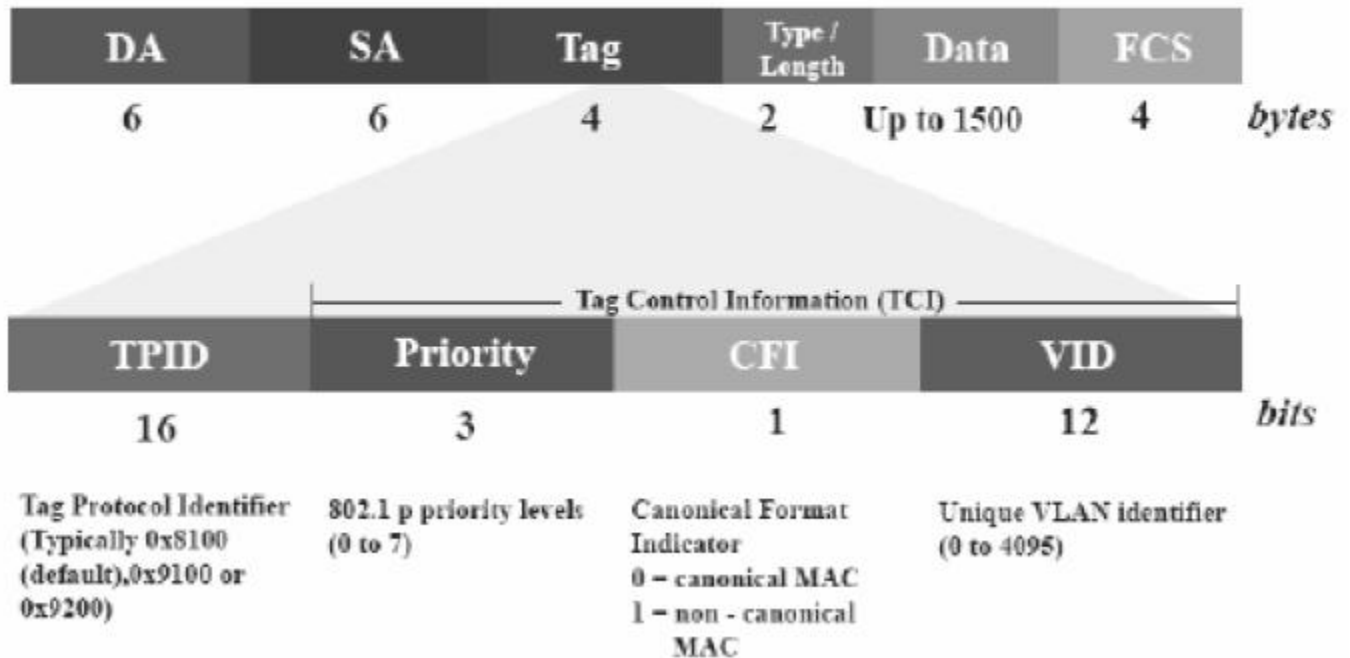
- Definované 3 BC (Bandwidth Constraint) Modely
- Maximum Allocation Model
- Maximum Allocation Model width Reservation
- Russian Dolls Model

MPLS-DiffServ

- Využíva kombináciu MPLS plánovania prevádzky a DiffServ pre zabezpečenie QoS (Quality of Service)
- MPLS-DiffServ (nazývaný tiež DiffServ-TE) definuje triedy riadenia prevádzky (**TE Classes**)

## **QOS Ethernet**

# IEEE 802.1Q rámeček



## Signalizácie: SIP, Megaco/H.248, SDP

### H.323 signalizácie

H.323 je množina štandardov ITU, ktoré definujú komponenty, protokoly a procedúry potrebné na prenos multimediálneho obsahu (hlasu, videa a dát) prostredníctvom IP sietí.

H.323 štandard špecifikuje štyri komponenty, ktoré umožňujú prenos multimediálnych dát:

- Terminál (koncové zariadenie)
- Brána (Gateway)
- Gatekeeper
- Multipoint Control Unit (MCU)

Medzi signalizačné protokoly patria:

- H.225 RAS (Registration, Admission, and Status) – protokol na komunikáciu medzi H.323 terminálmi, bránami a Gatekeeper-om.
- H.225 Call Signaling – zabezpečuje vytváranie a kontrolu spojení vrátane signalizácie potrebnej na vytvorenie spojenia medzi dvoma H.323 terminálmi.
- H.245 Control Signaling – používa sa na vytváranie logických komunikačných kanálov.

### Protokol H.225

- Kľúčový protokol v H.323 architektúre.
- Signalizačný protokol, ktorý slúži k vytvoreniu spojenia v
- paketových sieťach medzi H.323 koncovými bodmi.

- Vychádza z odporúčania Q.931.
- H.225 má dve hlavné časti:
  - RAS (Registration, Admission and Status).
  - Call signaling

### **Protokol H.225/RAS**

- H.225/RAS špecifikuje komunikáciu medzi koncovým bodom a Gatekeeperom.
- RAS je používaný na vykonanie registrácie, riadenie vstupu, zmenu šírky pásma, stavu a ukončenia procedúr medzi koncovými bodmi a Gatekeeperom.
- Správy RAS sú prenášané RAS kanálom.
- Správy H.225/RAS :
  - RegistrationRequest (RRQ) - žiadosť terminálu alebo brány o zaregistrovanie u Gatekeepera. Gatekeeper požiadavku buď potvrdí alebo odmietne (RCF alebo RRJ),
  - AdmissionRequest (ARQ) – žiadosť o prístup terminálu k paketovej sieti. Gatekeeper ju potvrdí alebo odmietne (ACF alebo ARJ),
  - BandwidthRequest (BRQ) – žiadosť o zmenu šírky pásma. Gatekeeper ju potvrdí alebo odmietne (BCF alebo BRJ).
  - InfoRequest (IRQ) – žiadosť o informáciu o stave terminálu ktorú posiela Gatekeeper,
  - InfoRequestResponse (IRR) – odpoveď na IRQ. Môže byť posiadaná v pravidelných intervaloch
  - DisengageRequest (DRQ) - žiadosť o odpojenie terminálu

### **Protokol H.225/Call signaling**

Signalizačné správy podľa H.225.0: Alerting, Call Proceeding, Connect, Connect Acknowledge, Disconnect, Information, Progress, Release, Release Complete, Setup, Setup Acknowledge, Status, Status Inquiry.

### **Protokol H.245**

- Protokol H.245 je riadiaci signalizačný protokol v H.323
- Slúži na výmenu H.245 správ medzi koncovými bodmi.
- H.245 správy sú prenášané cez riadiaci kanál. Riadiaci kanál je logický kanál 0 a je permanentne vytvorený.
- Jednotlivé správy slúžia pre nastavenie vlastností terminálov a nastavenie a zavretie logických kanálov.
- Správy H.245 protokolu sú definované pomocou ASN.1.
- Môžeme ich rozdeliť na žiadosti a odpovede.
- Správy H.245:
  - Master-Slave Determination – určuje, ktorý terminál je master a ktorý je slave. Možné odpovede sú: Acknowledge, Reject, Release,
  - Open Logical Channel - slúži na otvorenie logického kanála na prenos multimediálnych dát. Možné odpovede sú: Acknowledge, Reject, Release,
  - Close Logical Channel - slúži k zatvoreniu logického kanála medzi dvoma koncovými bodmi. Možné odpovede sú: Acknowledge,

- Request Mode – používa sa na nastavenie konkrétneho prenosového režimu terminálu. Jednotlivé typy režimov sú: VideoMode, AudioMode, DataMode a kódovaný mód. Možné odpovede sú: Acknowledge, Reject, Release
- Terminal Capability Set - obsahuje informácie o vlastnostiach terminálu prenášať a prijímať multimedialne toky. Možné odpovede sú: Acknowledge, Reject, Release,
- Send Terminal Capability Set – prikazuje vzdialenému koncovému terminálu aby poslal jednu alebo viac správ Terminal Capability Set.
- End Session Command - označuje koniec H.245 spojenia. Po príkaze už terminál ďalšie H.245 správy neposiela.

## SIP (Session Initiation Protocol)

- Textovo orientovaný signalizačný protokol aplikačnej vrstvy RM OSI štruktúrou podobný protokolu HTTP.
- Protokol typu klient-server.
- Používa sa pri IP telefónii, prezentáciách a videokonferenciách.
- Hlavné použitie:
  - Inicializuje vznik spojenia
  - Pre koncové body zaisťuje:
    - smerovanie dát,
    - autentifikáciu,
    - ďalšie potrebné funkcie.
- Rozšíriteľný pridaním nových hlavičiek, špecifikovaných ako samostatné RFC.
- SIP je určený pre zostavenie spojovania, zrušenie spojenia a správu spojení medzi dvoma alebo viacerými účastníkmi.
- Vnútri SIP správy je zapuzdrená správa, ktorá špecifikuje použité kódovanie pre multimedialne dáta, ich parametre a čísla portov, na ktorých majú byť dáta vysielané alebo prijímané.
- Najčastejšie sa používa protokol SDP (Session Description Protocol).
- SIP plní aj funkciu registrácie užívateľov – umožňuje používať pre identifikáciu užívateľa logické adresy nezávislé na fyzickom umiestnení užívateľa.

SIP správy sú dvoch druhov – žiadosti a odpovede.

Typy žiadostí:

- INVITE – žiadosť o nadviazanie spojenia alebo o zmenu parametrov už existujúceho spojenia,
- BYE – žiadosť o rozpojenie spojenia,
- ACK – žiadosť, ktorou klient potvrdzuje, že prijal odpoveď na žiadosť INVITE,
- REGISTER – žiadosť o registráciu klienta na registračnom serveri,
- CANCEL – žiadosť o zrušenie prebiehajúcej žiadosti
- INVITE,
- OPTIONS – žiadosť o poslanie podporovaných funkcií na serveri,
- INFO – prenos informácií počas hovoru.

Štruktúra odpovedí je podobná štruktúre žiadosti

Líši sa len v prvom riadku, ktorý obsahuje:



- verziu protokolu SIP
- návratový kód - trojmiestne číslo označujúce výsledok žiadosti
- návratový text - stručne popisuje výsledok žiadosti

#### Komunikácia

- SIP je protokol typu klient-server.
- Klient nadväzuje spojenie so serverom, pričom jedno zariadenie môže pracovať súčasne ako klient i server.
- Komunikácia môže byť:
  - Dvojbodová,
  - Viacbodová - multimedialne dáta sú prenášané:
    - naraz pre všetkých účastníkov spojením typu multicast,
    - spojením typu unicast od každého účastníka cez spojovaciu bránu,
    - spojením typu unicast medzi každou dvojicou účastníkov
    - kombináciou uvedených metód.
- Zariadenia podporujúce SIP môžu komunikovať so zariadením podporujúcim iný signalizačný protokol prostredníctvom brány
- Typy brán:
  - SIP/H.323
  - SIP/PSTN
  - SIP/ISDN
- SIP/H.323 brána
  - Prekladá signalizačné správy oboch protokolov.
  - Zariadenia používajúce protokol SIP alebo H.323 najčastejšie používajú na prenos multimedialnych dát protokol RTP => po nadviazaní spojenia pomocou SIP/H.323 brány môžu komunikovať priamo.

#### Transportný protokol

- Všetky SIP komponenty musia povinne podporovať transportné protokoly TCP a UDP
- SIP komponenty môžu podporovať aj iné transportné protokoly
- Najčastejšie sa využíva protokol UDP
- Datagram môže obsahovať iba jednu správu (žiadosť, alebo odpoveď)

#### Prenos dát

- Prenos multimedialnych dát prebieha po nadviazaní spojenia priamo medzi koncovými účastníkmi dohodnutým transportným protokolom, na dohodnutých adresách a portoch.
- Prenášané dáta nie sú prenášané cez SIP Proxy alebo redirect server.
- Najčastejšie používaným transportným protokolom pre prenos dát v IP sieťach so signalizáciou SIP je protokol RTP spolu s riadiacim protokolom RTCP

### **SDP (Session Description Protocol)**

- Textovo orientovaný protokol učený na špecifikáciu parametrov pri zostavovaní multimedialnych spojení
- Špecifikovaný v RFC 4566
- SDP správy môžu byť prenášané prostredníctvom rôznych protokolov (SIP, SAP, RTSP, email s MIME atď.)

## MGCP (Media Gateway Control Protocol)

- Signalizačný protokol slúžiaci na ovládanie mediálnych brán pre prenos audio dát.
- Definovaný IETF
- Založený na textovej architektúre.
- Jednotlivé správy sú tvorené z textových hlavičiek a postupnosťou parametrov. (Jednoduchšie vytvorenie a rozpoznávanie správ na strane odosielateľa resp. príjemcu ako v prípade binárnych správ. )
- Protokol typu Master/Slave
- Mediálne brány vykonávajú konverziu dát medzi jednotlivými typmi sietí.
- RFC 3435 rozlišuje nasledovné typy brán a zaradení:
  - Trunking gateway
  - Voice over ATM gateway
  - Residential gateway
  - Access gateway
  - Business gateway
  - Network Access Server
  - Circuit switch
  - Packet switch
- MGCP protokol je riadiaci protokol, ktorý definuje komunikáciu medzi MG (Media Gateway) a MGC (Media Gateway Controller).
- Mediálne brány (MG) sú riadené prostredníctvom MGC
- MGC obsahuje inteligenciu (Call Agent) pre riadenie mediálnych brán. (Samotné mediálne brány obsahujú minimálnu inteligenciu)
- Jeden MGC môže riadiť niekoľko mediálnych brán.
- Ak je počet mediálnych brán veľký, môžu sa rozdeliť na viac domén.
- MGCP je modulárny, ľahko rozšíriteľný protokol
- Rozširovanie je možné prostredníctvom tzv. balíkov (packages)
- MGCP rozlišuje dva typy logických zariadení:
  - Koncový bod
    - Fyzické alebo logické zariadenie ktoré vykonávajú konverziu dát medzi jednotlivými typmi sietí.
    - Najčastejšie sú to analógové alebo digitálne porty v smerovačoch ktoré slúžia ako brány.
  - Spojenie:
    - Dočasný logický tok ktorý slúži k zostaveniu, údržbe, a ukončeniu spojenia.
    - Ak je spojenie ukončené, zdroje ktoré boli pridelené tomuto spojeniu môžu byť opätovne použité pre ďalšie spojenie.
    - Spojenia typu bod-alebo viacbodové môžu byť bod bod viacbodové.
- MGCP protokol je typu master-slave. Protokol MGCP používa pre zostavenie spojenia príkazy a odpovede pričom master riadi slave
- Ak koncové body medzi ktorými má byť spojenie vytvorené sú ovládané rôznymi Call agentmi, tak signalizácia medzi nimi prebieha prostredníctvom SIP protokolu.

- MGCP protokol realizuje vzájomný vzťah medzi MGC a MG ako súbor správ.
- Správy sa skladajú z príkazu a požadovanej odozvy.
- Všetky príkazy sa skladajú z hlavičky príkazu po ktorom môže nasledovať telo správy.
- Hlavička a telo správy sú zakódované ako súbor textových riadkov, kde hlavička je od tela správy oddelená prázdny riadkom.
- Hlavička príkazu sa skladá z príkazového riadku a z riadkov obsahujúcich parametre
- Protokol SDP slúži k špecifikácii kódovania a ďalších parametrov prenosu audio dát počas komunikácie.
- Správa SDP je obsiahnutá v tele správy protokolu MGCP.
- Samotný prenos audio dát prebieha po nadviazaní spojenia priamo medzi koncovými bodmi prostredníctvom dohodnutých transportných protokolov.
- Používa sa transportný protokol RTP spolu s riadiacim protokolom RTCP.

## MEGACO/H.248

- Megaco je riadiaci protokol, ktorý definuje komunikáciu medzi MGC a MG.
- Definovaný v IETF (MEGACO) a ITU (H.248)
- Megaco je určený pre zostavovanie, rušenie a správu spojení medzi dvoma alebo viacerými koncovými bodmi.
- Vnútri správy protokolu Megaco je zapuzdrená správa, ktorá špecifikuje použité kódovanie pre multimediálne dáta, ich parametre a čísla portov, na ktorých majú byť dáta vysielané alebo prijímané.
- Protokol Megaco používa pri prenose správ cez IP transportný protokol UDP/ALF (Application Layer Framing) alebo TCP.
- Spojovací model popisuje logické entity, alebo objekty vo vnútri MG ktoré môžu byť riadené MGC.
- Pojmy používané v spojovacom modeli sú:
  - ukončenie - predstavuje zdroj alebo príjemcu mediálnych tokov.
  - kontext - predstavuje vzťah medzi jednotlivými ukončeniami.
- Existuje špeciálny typ kontextu nazývaný nulový kontext.
- Nulový kontext obsahuje ukončenia, ktoré nie sú priradené k iným ukončeniam
- Signalizácia umožňuje vytvorenie jednotlivých ukončení a kontextov v danej MG.
- Protokol Megaco je typu master-slave.
- Pomocou jednotlivých príkazov riadi zostavenie, údržbu a zrušenie spojenia v jednotlivých MG.

### Priebeh komunikácie

- Vzájomný vzťah medzi MGC a MG je realizovaný pomocou príkazov a požadovaných odpovedí.
- Príkaz a odpoveď obsahujú názov príkazu a povinné a nepovinné parametre.
- Jednotlivé príkazy sú zoskupené do transakcií ktoré sú určené prostredníctvom TransactionID, ktorý prideluje odosielateľ – je to jedinečné číslo.
- Transakcia sa skladá z jedného alebo viacerých činností (Action).
- Každá činnosť je tvorená postupnosťou príkazov ktoré sú určené pre dané ukončenie v danom kontexte.
- Každá činnosť špecifikovaná vlastným ContextID.

- ContextID prideli MG pri vytvorení kontextu a tento ContextID je používaný vo všetkých transakciách.
- Existujú dva prípady, kedy činnosť nešpecifikuje ContextID:
  - keď je modifikované ukončenie mimo kontextu,
  - keď je poslaná žiadosť o vytvorenie nového kontextu.
- Príkazy vo vnútri transakcie môžu byť vykonané v ľubovoľnom poradí.
- Dočasná odpoveď - posieľa ju príjemca a signalizuje ňou, že daná transakcia je aktívna a prebieha jej spracovanie.
  - Slúži na zamedzenie opätovného vyslania žiadosti pri dlhšom vykonávaní žiadosti na strane príjemcu. (Vysielač ktorý čaká na odpoveď v prípade, že odpoveď na žiadosť nepríde do definovaného času pošle opätovnú žiadosť.)
- Viacnásobné transakcie môžu byť zreťazené do správy.
- Jednotlivé transakcie v správe sú vykonávané nezávisle.
- Samotná správa nie je potvrdzovaná.
- Existuje niekoľko transportných protokolov na prenos správ medzi MGC a MG.
- Pre prenos Megaco signalizácie cez IP sa používajú TCP a/alebo UDP/ALF
- Samotný prenos multimediálnych dát prebieha po nadviazaní spojenia priamo medzi koncovými účastníkmi dohodnutým transportným protokolom, na dohodnutých adresách a portoch.
- Najčastejšie používaným transportným protokolom pre prenos dát v IP sieťach je protokol RTP spolu s riadiacim protokolom RTCP.

## Optické spínače (vlnovodné, free-space, digitálne).

### Dôvody zavedenia:

- Limitované kapacity súčasných spojovacích uzlov
- Elektronické komponenty:
  - elektromagnetické pole
  - RC konštanty
  - vysoká energetická spotreba
  - problémy s chladením

### Rozdelenie

- **Podľa transfér módu**
  - optické spínače s prepájaním okruhov
  - optické spínače s prepájaním paketov
- **Podľa technológie**
  - optické spínače na báze vlnovodov
  - free-space optické spínače
- **Podľa multiplexnej techniky**
  - optické spínače s priestorovým multiplexom
  - optické spínače s časovým multiplexom
  - optické spínače s vlnovým (frekvenčným) multiplexom
  - hybridné optické spínače

## Vlnovodné optické snímače

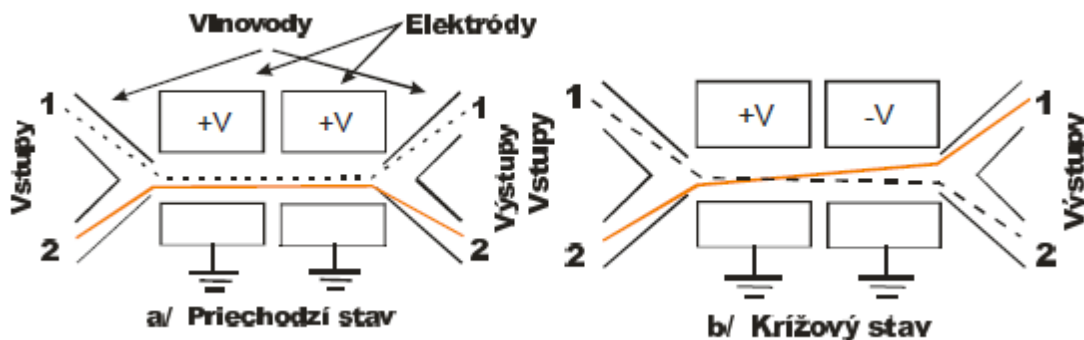
- Optický signál je vedený vo vlnovode
- Optické spojovacie polia sú tvorené kaskádou vlnovodných spínačov prepojených vlnovodmi (t.j. optickými vláknami)

### Výhody

- Prirodzená evolúcia z dnešnej elektronickej technológie použitej v komunikačných systémoch
- Budovanie na už existujúcej optike, ktorá je na podobnom princípe prítomná v komunikačných sieťach (prenosové linky)
- Veľké skúsenosti s optickou vlnovodnou technológiou
- Pokročilejšia technológia v porovnaní s dnešnou free-space technológiou

### Optické elementy s priestorovým delením

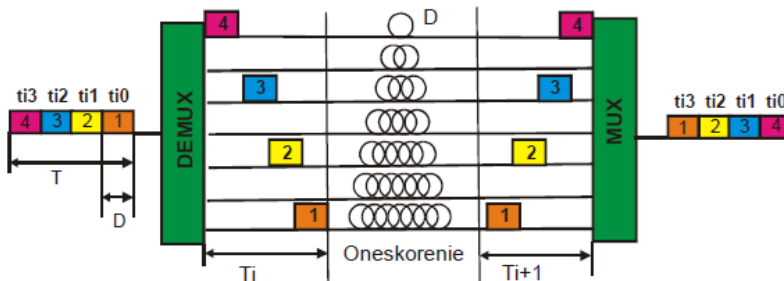
- smerovací väzobný člen



- Mach - Zehnder interferometer
- Spojovací element 2x2 (NTT)

### Optické elementy s časovým delením

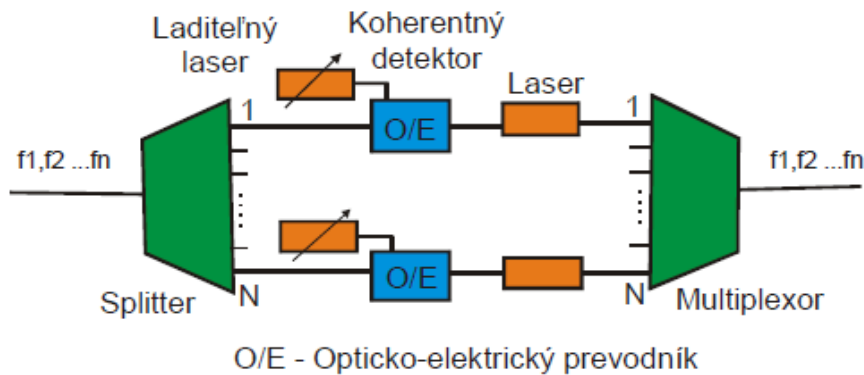
- Menič časovej polohy



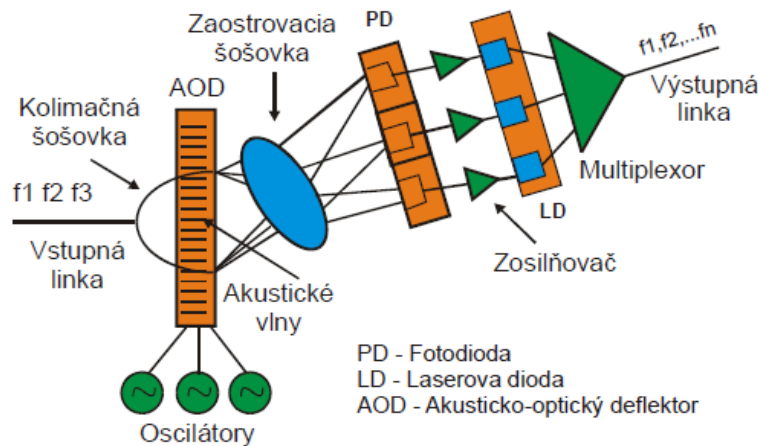
- Časové pole s viacnásobným prístupom
- Hviezdicový väzobný člen

### Optické elementy s vlnovým delením

- Menič vlnovej dĺžky



- Menič vlnovej dĺžky s akusticko-optickým deflektorom



- Vlnové pole s viacnásobným prístupom

## Free-space optické spínače

- Historicky prvé optické spínače
- Svetlo je transportované v spínači voľne v priestore

### Výhody

- umožňujú využiť ďalšiu dimenziu pri smerovaní signálov,
- umožňujú vyššiu integráciu elementov,
- umožňujú vnútornú paralelizáciu prenosového pásma a tým vyššiu výkonnosť,
- v dôsledku vysokej integrácie je vyššia pravdepodobnosť lacnejšej produkcie.

### Rozdelenie

- Podľa architektúry:
  - viacstupňové spojovacie štruktúry (napr. S-SEED spínač)
  - jednostupňové spínače (napr. holografický spínač)
- Podľa typu signálu:

- analógové spínače (transparentné vo formáte, bitovej rýchlosti a type modulácie; akumulujú energetické straty a presluchy)
- digitálne spínače (digitálny signál => nevykazujú útlm a presluchy)