10. přednáška

Kvalita služby v IP telefonii

Co byste měli být schopni

- Vysvětlit, proč je QoS pro sítě VoIP zásadní
- Rozlišit řízení zabezpečení od předcházení zahlcení
- Popsat, jak omezit šířku pásma používanou určitými typy provozu
- Určit strategii pro maximalizaci dostupné šířky pásma sítě WAN pro provoz VoIP

Obsah

1. Diferencované a integrované služby
2. Klasifikace a značkování
3. Metody řazení do fronty

1. Diferencované a integrované služby

K čemu vede nedostatek šířky pásma

- Zpoždění
- Časová nestabilita, kolísání velikosti zpoždění paketů při průchodu sítí (angl. jitter) způsobující zrychlování a zpožďování v hovoru, případně mezery v hovoru
- Zahazování paketů v důsledku zahlcení vyrovnávacích pamětí

Tři základní kroky

Krok 1. Stanovení požadavků na výkonnost sítě pro různé typy provozu
Příklad: Hlas zpoždění do 150 ms, jiter do 30 ms, ztrátovost do 1%
Video zpoždění do 150 ms, jiter do 30 ms, ztrátovost do 1%

Krok 2: Roztřídění do tříd provozu
Příklad: Nízké zpoždění, nízká priorita…

Krok 3: Zdokumentování politiky QoS

Klasifikaci QoS dle doporučení ITU Y.1541

Třída QoS	Charakteristika	IPTD	IPDV	IPLR	IPER
0	Přenos v reálném čase, citlivé na rozptyl zpoždění, vysoká interaktivita	100 ms	50 ms	$1x10^{-3}$	$1x10^{-4}$
1	Přenos v reálném čase, citlivé na rozptyl zpoždění, interaktivita	400 ms	50 ms	$1x10^{-3}$	$1x10^{-4}$
2	Transakční data, vysoká interaktivita	100 ms	bez limitu	$1x10^{-3}$	$1x10^{-4}$
3	Transakční data, interaktivita	400 ms	bez limitu	$1x10^{-3}$	$1x10^{-4}$
4	Citlivé na ztrátu paketů (krátké transakce, videořetězce, důležitá data)	1 s	bez limitu	$1x10^{-3}$	$1x10^{-4}$
5	Ostatní aplikace v IP sítích se základním nastavením	bez limitu	bez limitu	bez limitu	bez limitu

IPTD – IP Packet Transfer Delay
IPDV – IP Packet Delay Variation
IPLR – IP Packet Loss Ratio
IPER – IP Packet Error Ratio

Přístup ke QoS

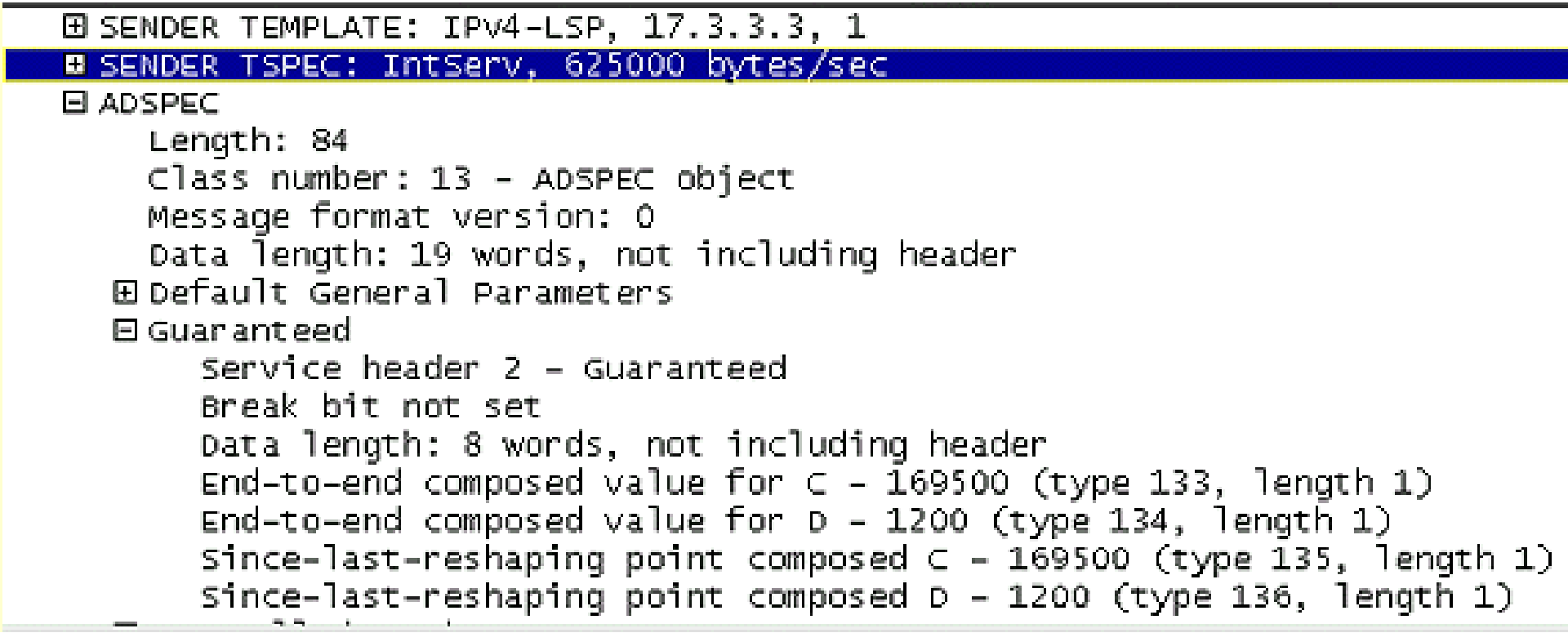
- Best-Efford
- Integrované služby (hard QoS)
  provádí rezervaci
- Diferencované služby (Soft QoS)
  značkování paketů

IntServ

Rozlišuje dvě třídy služeb:

- GS (Guaranteed Service) [RFC 2212]
  GS zajistí, že IP pakety budou doručeny v limitu, který nepřesáhne maximální hranici nadefinovaného času pro doručení, a že nebudou zahozeny z důvodu přetečení zásobníků na rozhraní směrovačů.
- CLS (Controlled–Load Service) [RFC 2211]
  CLS je obdoba služby „Best–Effort“ v lehce namáhaných sítích. K zajištění využívá nástroje pro kontrolu a alokaci šíře pásma při přetížení sítě. Lehce namáhaná síť je taková síť, která garantuje vysokou pravděpodobnost doručení přenášených paketů a naměřené zpoždění při přenosu mezi koncovými uzly pro vysoké procento paketů nepřekročí jejích minimální hranici zpoždění skládající se ze součtu přenosového zpoždění a procesního zpoždění způsobené na přenosových zařízeních v síti.

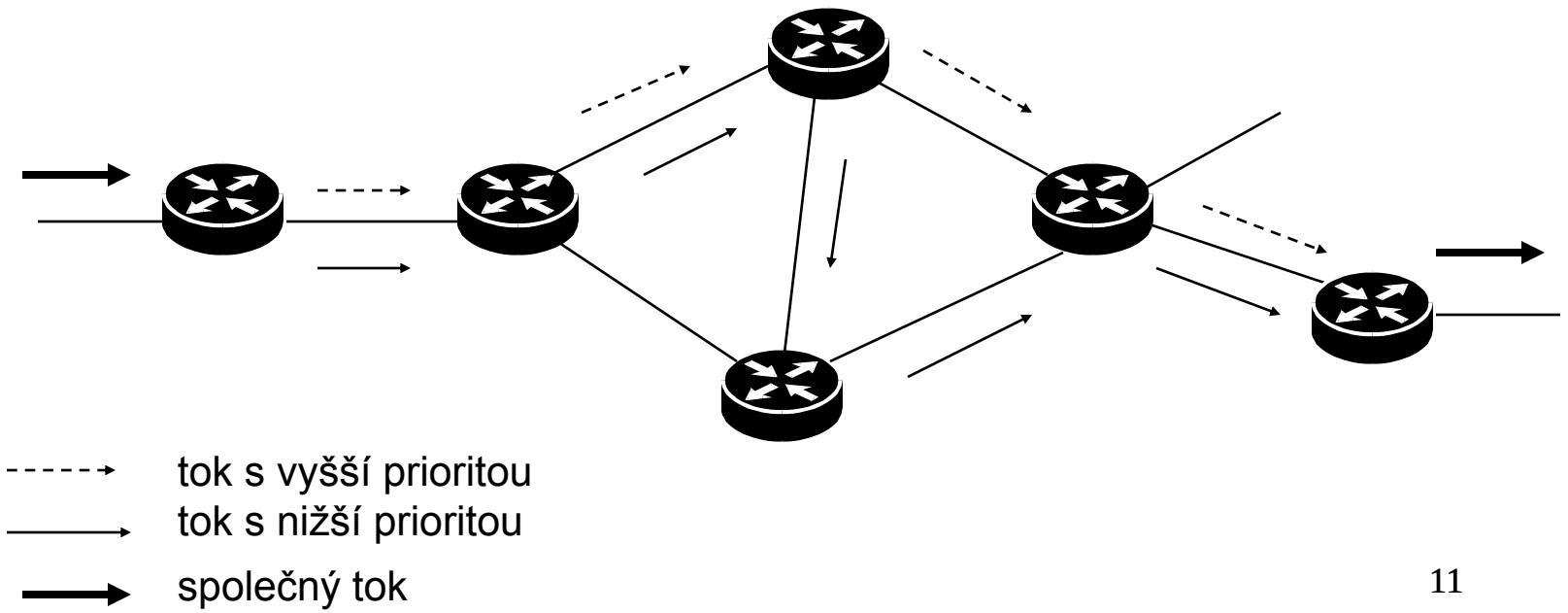
Pro hlas je důležitý traffic engineering, zde RSVP-TE



Ukázka odchyceného paketu, který specifikuje požadavek na provoz.
Hodnota požadavku (TSPEC - traffic specification) je zde 625 kb/s.
Použit byl protokolový analyzátor Etheral (*www.etheral.com*).

Příklad MPLS

Pakety v okrajovém uzlu dostávají návěští v závislosti na poli PHB; čím vyšší priorita, tím je přidělena efektivnější cesta.Další směrovače hodnotu PHB však již nezkoumají.



Problém dodržení QoS v MPLS síti

Pro jednotlivé cesty v MPLS sítích lze definovat potřebnou kvalitu služby (QoS – Quality of Service). Problémem je, jak tuto kvalitu dodržet v případě, kdy jsou na cestu posílány přesměrované pakety.

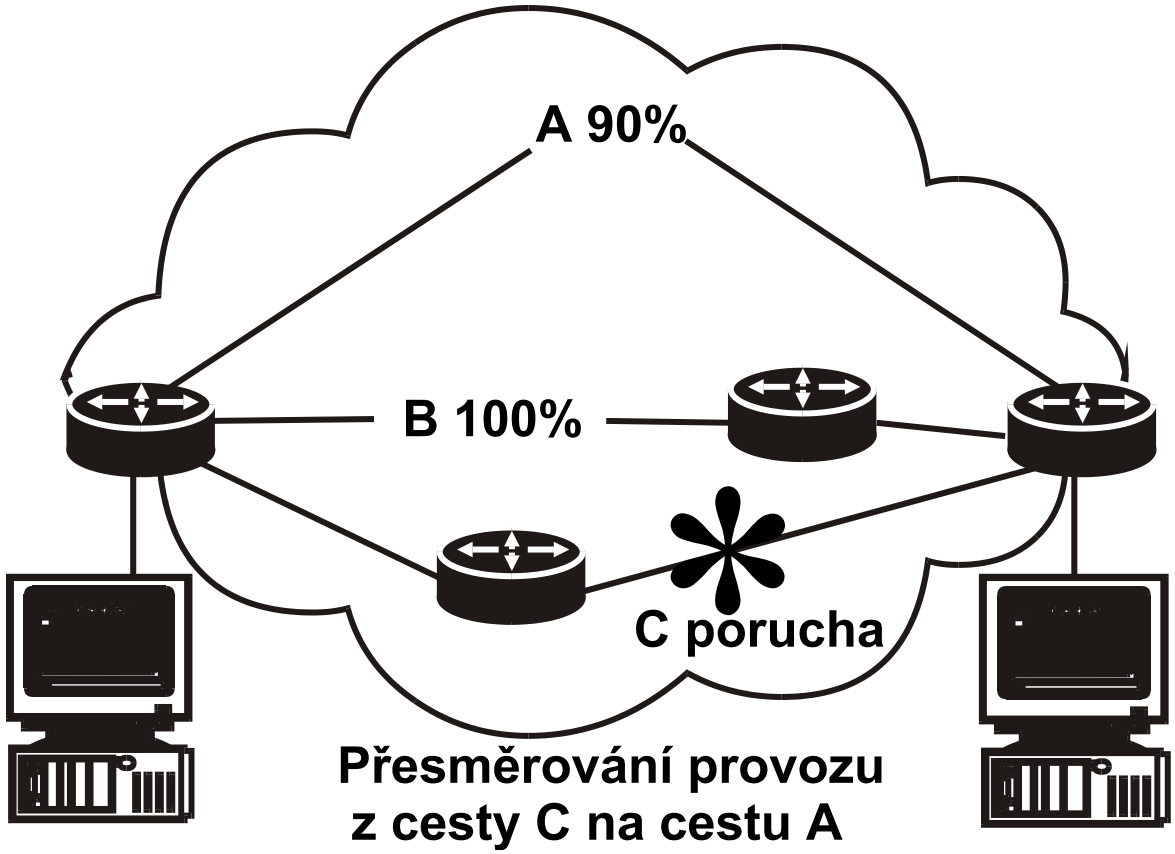
Na obrázku na následujícím slajdu jsou zobrazeny tři různé cesty sítí WAN:

- cesta A je nastavena na 90 % šířky pásma v hodinách špičkové zátěže,
- cesta B je v hodinách špičkové zátěže nastavena na 100 % a nakonec
- cesta C je obdobně nastavena na 125 %.

Pakety, které budou přenášeny po cestě A se nikdy nesetkají se zahlcením, cesta poskytuje pro případ výpadků dostatečnou rezervu zátěže. V případě zahlcení na cestě C mohou být pakety přesměrovány na cestu A a pak na cestě A není možné dodržet parametry kvality služby.

K překonání problému přesměrování pracovní skupiny IETF navrhly některá možná řešení. Především platí, že pro zajištění plnohodnotné QoS musí být systém schopen označovat, klasifikovat a dohlížet na provoz. Označování a klasifikace provozu je zajišťována návěštími MPLS, ale není zde zajištěn dohled nad stanoveným provozem.

Problém dodržení QoS v MPLS síti



Nevýhody IntServ

- není dostatečně škálovatelná
  - několik požadavků je schopno zabrat dostupné pásmo
  - pásmo je rezervováno i v okamžiku, kdy není příslušným procesem plně využito
- není plně podporována aplikacemi a operačními systémy
  - rezervaci pásma si zajišťuje aplikace;
- nezajišťuje správu priorit;
- zavádí do paketově orientovaného modelu okruhově orientovaný model;
- poměrně náročná signalizace mezi sousedními uzly zvyšující režii;

DiffServ

DiffServ [RFC 2475] nezajišťuje přímou rezervaci pásma, ale zajišťuje dynamické rozlišení úrovně služeb požadované datovým tokem na základě informace v záhlaví paketu.
Je proto podstatně vhodnější pro implementaci, neboť staticky nezabírá pásmo po dobu, kdy jej proces nevyužívá. K rozlišení úrovně služeb se používá ToS pole v záhlaví IP paketu. To je v tomto případě rozděleno na dvě části:

- DSCP (Differentiated Services Code Point)
  bit 0 až 5 definují PHB (Per Hop Behavior) index;
- CU (Currently Unused);
  bit 6 a 7 (rezervovány pro budoucí použití);

Na základě hodnoty indexu PHB rozhoduje směrovač v příslušné doméně, jak se bude nakládat s konkrétním paketem. Stejná hodnota indexu RHB může mít odlišný význam pro různé domény. IETF definuje 3 typy PHB:

- EF (Expedited Forwarding);
  nejvyšší typ služby, zajistí služby virtuální pronajaté linky;
- AF (Assured Forwarding);
  zajišťuje rozlišení úrovně služeb pro různé uživatele a procesy;
- DF (Default);
  standardní služba typu „Best Effort“, nezajišťuje žádnou úroveň kvality služeb ani garanci výkonu

Implementace PHB u DiffServ

	vstupní IP plánování	**výstupní IP plánování**	**ochrana před zahlcením**
BE	nic	nejnižší priorita	pakety se prioritně vyhazují
AF	hlídání průměrné hodnoty dávky, pakety dávky a mimo kontrakt se značkují	vyšší priorita	co je v souladu s kontraktem nemůže být vyhozeno, je-li třeba, vyhazují se pakety mimo kontrakt
EF	hlídání průměrné hodnoty, pakety mimo kontrakt jsou vyhazovány	nejvyšší priorita (odstraňování provozních špiček)	žádné prioritní pakety nelze vyhodit

Použití DiffServ v MPLS

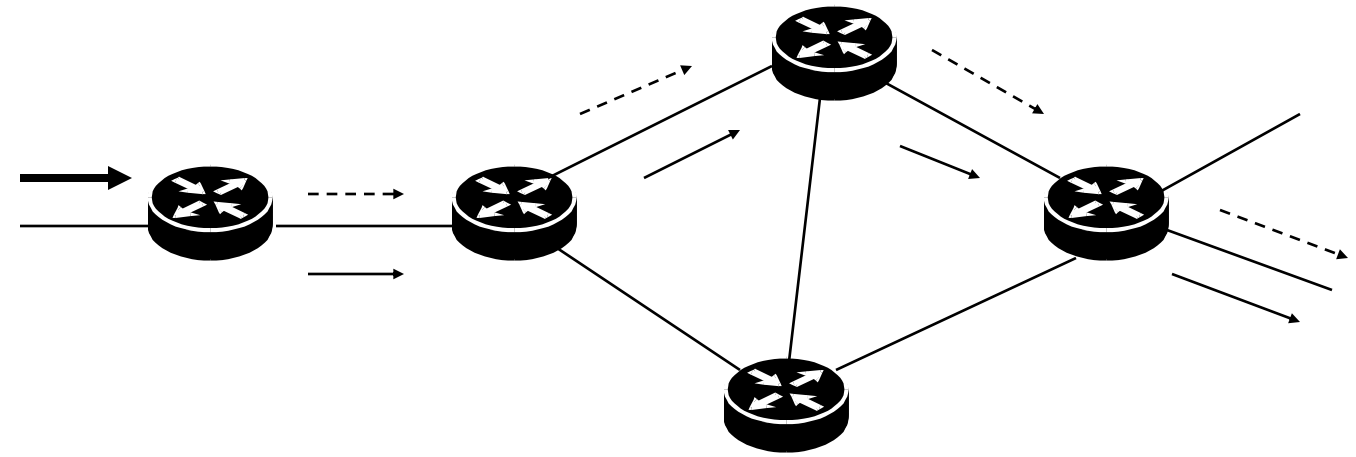
Pokud je datový tok přenášen po stejné trase, je v MPLS nazývána jako Label Switched Patch (LPS). Ty pakety, které požadují stejné Diffserv chování, se nazývají Behaviour Aggregate (BA). Toto řešení umožňuje síťovému MPLS administrátorovi pružně definovat, jak jsou BA mapovány do LPS. Například toto řešení umožňuje síťovému administrátorovi, zda různé sady BA mapovat na stejnou nebo odlišné LPS.

Ve vstupním bodě do Diffserv domény jsou pakety klasifikovány a značeny v Diffserv Code Point (DSCP), který odpovídá jejich BA. V každém tranzitním uzlu je DSCP použito k výběru hodnoty PHB, které určuje způsob plánování a (v některých případech) pravděpodobnost vyřazení paketu.

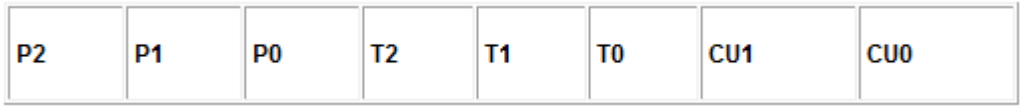
Pro uložení hodnoty PHB bylo vybráno 5 bitů z 8 bitů pole ToS (Type of Service) záhlaví IP. Význam prvních tří bitů zůstal pro kompatibilitu zachován (zpoždění, spolehlivost, průchodnost). Doplněn byl např. *expedited forwarding* (EF). Šestý bit označuje tzv. „in or out profile“ (IN), tj. zda paket respektuje daný profil (například tak lze označit pakety s vyššími požadavky na spolehlivost doručení). Poslední dva bity v současnosti nejsou využity.
Předpokládá se jejich budoucí použití pro uložení hodnot o zahlcení sítě (ECN - explicit congestion notification). Problémy přináší kombinace bitu IN a hodnoty EF, protože bit IN je pro pakety EF nevhodné používat.

Příklad DiffServ

Vstupující paket je v rámci Diffserv provozu v okrajovém směrovači sítě označen prioritní informací, podle které ho pak další směrovače směrují.



Bity ToS A pole DiffServ



- IP precedence – 3 bity (P2 až P0)
- Zpoždění průchodnost, spolehlivost – 3 bity (T2 až T0)
- CU (Currently Unused) – 2 bity(CU1-CU0)

- DSCP – 6 bitů (DS5-DS0)
- ECN (Explicit Congestion Notification) – 2 bity

Default: 000000

DSCP

V IP sítích uplatňujících technologii DiffServ je kvalita služby určena významem hodnot tvořících DSCP.
Hodnota DSCP identifikuje specifickou třídu datového provozu a udává, jak by se mělo s pakety zacházet. Důležité ovšem je, jak budou pravidla implementována.

DSCP je tvořeno šesti bity umožňujících vytvořit 64 kombinací, viz RFC 2474:
1–32 jsou určeny pro standardní akce (tzv. Pool 1);
33–48 jsou určeny pro experimentální a lokální užití (tzv. Pool 2);
49–64 jsou určeny pro standardní aplikace (tzv. Pool 3), používaný pokud nevystačuje Pool 1.

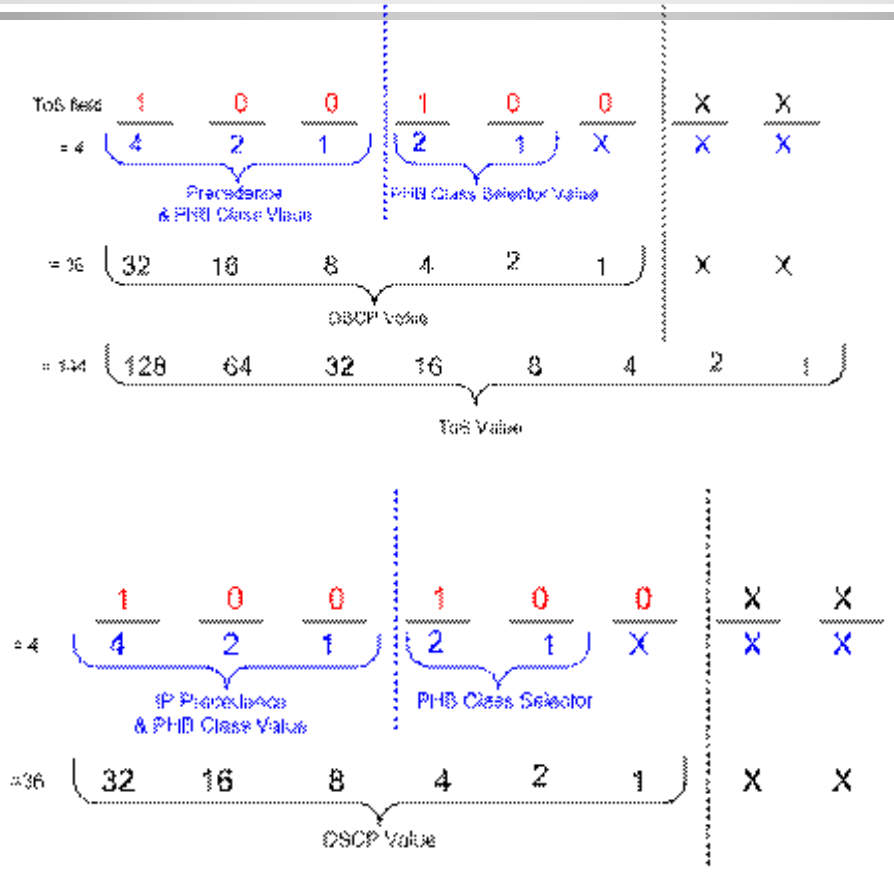
Hodnota DSCP se dále dělí na dvě tříbitové hodnoty.
První tři bity určují třídu CS (Class Selector), další trojice bitů pak označují prioritu P (Precedence).
V RFC 4594 jsou uvedena doporučení pro značení DSCP hodnot pro různé druhy datových přenosů.

Urychlené předávání (Expedited Forwarding), selektor třídy (Class Selector)

DSCP 46 = 101110 – PHB EF dostane hlas, zatímco provoz pro inicializaci telefonního hovoru používá hodnotu CS3, Interaktivní video hodnotu AF41.
Kategorie CS chování PHB zajišťují kompletní zpětnou kompatibilitu s hodnotami IP precedence, protože stejně jako IP precedence mají CS nuly ve 4., 5., a 6. bytu v bajtu ToS.
Např. směrovač používá značení DSCP, ale posílá pakety na směrovač, který rozumí pouze značení IP precedence My pošleme paket s DSCP 40 (101000), tak se na druhém směrovači DSCP transformuje na IP precedenci 5 (berou se v úvahu pouze první tři bity zleva).

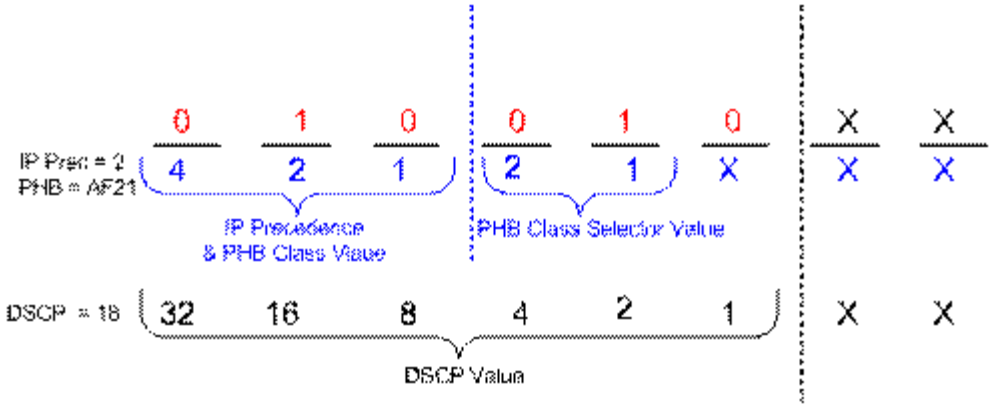
PHB	Decimal Value	Binary Value	IP Precedence Value
CS0	0	**000**000	0
CS1	8	**001**000	1
CS2	16	**010**000	2
CS3	24	**011**000	3
CS4	32	**100**000	4
CS5	40	**101**000	5
CS6	48	**110**000	6
CS7	56	**111**000	7

Příklad



Hodnota DSCP je 36, Precedence je 4, ToS je 144, AF je 42

Příklad



Hodnota DSCP je 18, Precedence je 2, ToS je 72, AF je 21

Zajištěné předávání (Assured Forwarding)

Nejširší kategorie

Drop	Class 1	Class 2	Class 3	Class 4
Low	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Medium	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
High	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Zařízení, které podporuje IP precedenci, prověřuje jen tři bit nalevo
Každá třída obsahuje tři priority vyřazení paketu.
Např. paket AF13 bude pravděpodobněji zahozen, než paket AF11.
AF41 je zde nejlepší číslo a AF13 nejhorší.

Značení DSCP hodnot dle RFC 4594

Služba	Typ třídy	Hodnota DSCP	Hodnoty CS–P–DSCP	Použité značení pro PHB	Příklady aplikací
Administrative	CS7	111000	7–0–56	RFC 2474	Informace pro směrování a kontrolu
Network Control	CS6	110000	6–0–48	RFC 2474	Informace pro směrování a kontrolu
Telephony	EF	101110	5–6–46	RFC 3246	IP Telefonie – přenos
Signaling	CS5	101000	5–0–40	RCF 2474	IP Telefonie – signály
Multimedia Conferencing	AF41 AF42 AF43	100010 100100 100110	2–4–34 4–4–36 4–6–38	RFC 2597	H.323/V2 video konference
Real–Time Interactive	CS4	100000	4–0–32	RFC 2474	Video konference a interaktivní hry
Miltimedia Streaming	AF31 AF32 AF33	011010 011100 011110	3–2–26 3–4–28 3–6–30	RFC 2597	Přenos video a audio signálu
Broadcast Video	CS3	011000	3–0–24	RFC 2474	TV a živé přenosy
Low–Latency Data	AF21 AF22 AF23	010010 010100 010110	2–2–18 2–4–20 2–6–22	RFC 2597	Webové klient/servet transakce
Operation and Management	CS2	010000	2–0–16	RFC 2474	OAM
High–Throughput Data	AF11 AF12 AF13	001010 001100 001110	1–2–10 1–4–12 1–6–14	RFC 2597	Ukládání a odesílání dat pro aplikace
Standard	DF (CS0)	000000	0–0–0	RFC 2474	Pro nespecifikované aplikace
Low–Priority Data	CS1	001000	1–0–8	RFC 3662	Ostatní operace ("Best–Effort")

Obecné hodnoty metrik tříd

Služba	Typ třídy	Hodnota DSCP	IPTD	IPDV	IPLR
Administrative	CS7	111000	0,05–1s	0 s	0 – 10^{-3}
Network Control	CS6	110000	1–10 s	0 s	10^{-2} – 10^{-3}
Telephony	EF	101110	100–400 ms	30–50 ms	10^{-2} – 10^{-3}
Signaling	CS5	101000	100–400 ms	30–50 ms	10^{-2} – 10^{-3}
Multimedia Conferencing	AF41 AF42 AF43	100010 100100 100110	100–400 ms	30–50 ms	10^{-2} – 10^{-3}
Real–Time Interactive	CS4	100000	100–400 ms	30–50 ms	10^{-2} – 10^{-3}
Miltimedia Streaming	AF31 AF32 AF33	011010 011100 011110	5–10 ms	0 s	10^{-2} – 10^{-3}
Broadcast Video	CS3	011000	nespecifikováno	nespecifikováno	nespecifikováno
Low–Latency Data	AF21 AF22 AF23	010010 010100 010110	20–100 ms	1–50 ms	0
Operation and Management	CS2	010000	nespecifikováno	nespecifikováno	nespecifikováno
High–Throughput Data	AF11 AF12 AF13	001010 001100 001110	1–50 ms	0 ms	0 – 10^{-3}
Standard	DF (CS0)	000000	nespecifikováno	nespecifikováno	nespecifikováno
Low–Priority Data	CS1	001000	nespecifikováno	nespecifikováno	nespecifikováno

Jak nastavujeme DSCP ?

```
Router(config)# class-map match-all VOIP
 1751-uut1(config-cmap)# match ip dscp ?
   <0-63>   Differentiated services codepoint value
   af11     Match packets with AF11 dscp (001010)
   af12     Match packets with AF12 dscp (001100)
   af13     Match packets with AF13 dscp (001110)
   af21     Match packets with AF21 dscp (010010)
   af22     Match packets with AF22 dscp (010100)
   af23     Match packets with AF23 dscp (010110)
   af31     Match packets with AF31 dscp (011010)
   af32     Match packets with AF32 dscp (011100)
   af33     Match packets with AF33 dscp (011110)
   af41     Match packets with AF41 dscp (100010)
   af42     Match packets with AF42 dscp (100100)
   af43     Match packets with AF43 dscp (100110)
   cs1      Match packets with CS1(precedence 1) dscp (001000)
   cs2      Match packets with CS2(precedence 2) dscp (010000)
   cs3      Match packets with CS3(precedence 3) dscp (011000)
   cs4      Match packets with CS4(precedence 4) dscp (100000)
   cs5      Match packets with CS5(precedence 5) dscp (101000)
   cs6      Match packets with CS6(precedence 6) dscp (110000)
   cs7      Match packets with CS7(precedence 7) dscp (111000)
   default  Match packets with default dscp (000000)
   ef       Match packets with EF dscp (101110)
 Router1(config-cmap)# match ip dscp af31
```

Podle preference lze i vybírat pakety

```
Router1(config)# access-list 101 permit ip any any ?
dscp        Match packets with given dscp value
fragments   Check non-initial fragments
log         Log matches against this entry
log-input   Log matches against this entry, including input interface
precedence  Match packets with given precedence value
time-range  Specify a time-range
tos         Match packets with given TOS value
```

QoS v sítích IPv6

V záhlaví paketu protokolu IPv6 jsou vyčleněny dvě pole sloužící k úpravě kvality služby:

- pole pro identifikaci datového toku, tzv. značka toku (Flow Lable) o velikosti 20 bitů – novinka;
  - identifikuje pakety určitého datového toku;
  -označení provedené zdrojem dat se během přenosu nemění
  -fragmentace ani šifrování nepředstavuje problém jako v IPv4
  Dává možnosti (zatím nevyužité) řízení toku jako ATM mechanismem VC/VP
  Do RFC 3697 se nevědělo, co s tím
- pole tzv. třída provozu (Traffic Class) o velikosti 8 bitů;
  - funkčně ekvivalentní poli ToS v IPv4;

RFC 3697 - IPv6 Flow Label Specification

Toky jsou rozlišovány podle **trojice údajů**: IP adresa odesílatele, IP adresa příjemce a značka toku. Shodují-li se všechny tři, patří datagramy ke stejnému toku.

Pole Flow Label pomáhá identifikovat pakety téhož datového toku, s nimiž mohou směrovače na cestě zacházet jistým jednotným způsobem. Konkrétní mechanismy jsou však dosud pouze ve stádiu návrhů.

Díky údaji v poli Flow Label směrovač provádí vyhledání ve směrovací tabulce pouze jedenkrát a výsledek vloží pro další použití do paměti cache. Záznamy v cache paměti tak budou mít tvar n-tic

<zdrojová adresa, flow label, next_hop_IP, výstupní_rozhraní, záhlaví_2.vrstvy>

Předpřipravení záhlaví 2. vrstvy pro výstupní rozhraní má za úkol urychlit přepnutí, protože odpadá potřeba opakovaného prohledávání ARP tabulky výstupního rozhraní.

Dokument nenařizuje žádný specifický způsob, jak značky toků přiřazovat.

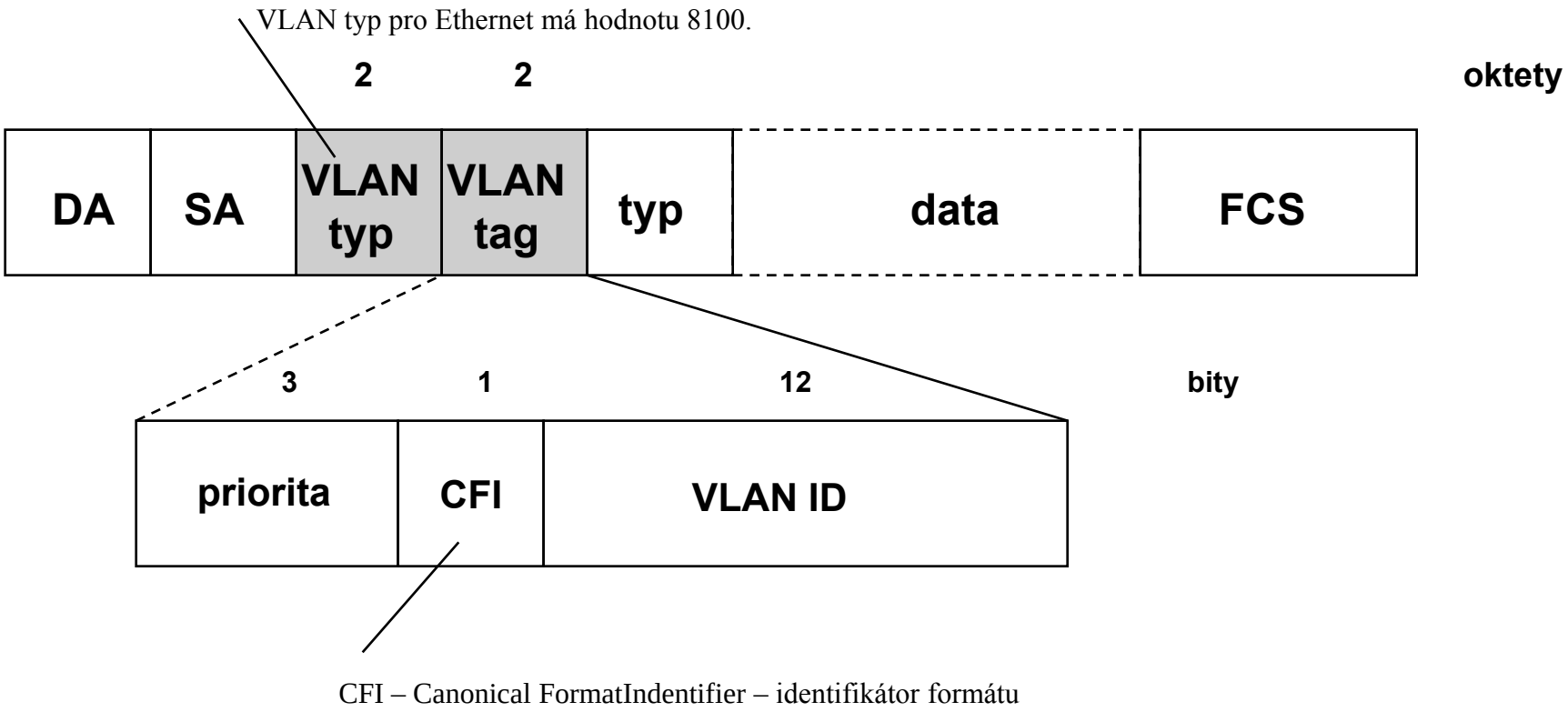
Značná pozornost je v dokumentu věnována otázkám **bezpečnosti**, řeší se především otázky možného zcizení provozu změnou značky toku. Tato problematika a její dopady se dost podobají falšování IP adres, ovšem s určitými rozdíly: značka toku není chráněna mechanismy IPsec. S toky prostě ještě neumíme ani pracovat, ani je chránit.

Závěr k zajištění QoS v sítích IPv6

Architektura s implementaci IPv6 může uplatňovat zabezpečení kvality služeb dvěma hlavními způsoby.

- První způsob je orientován na poskytovanou třídu služeb v síti, obdobně jako u DiffServ technologie. Ale na rozdíl od DiffServ technologie, která má limitované množství tříd služeb definované v poli ToS, má IPv6 mnohem větší rozsah pro tvorbu tříd. Neprobíhá zde žádná identifikace jednotlivého uživatelského datového toku a vzniklý provoz je přepínán na základě DSCP hodnoty. Tento způsob je znám jako tzv. „Class of Service Full IPv6 Network“.
- Druhý způsob je orientován na podporu služeb jednotlivým uživatelů, obdobně jako u ATM technologie nebo MPLS, kde každý tok může mít nadefinovány specifické kvalitativní požadavky pro přenos. Na základě hodnoty v poli Flow Label jsou IPv6 pakety v IPv6 směrovači, tzv. „IPv6 Label Switch Router“, přepínány a směrovány k cíli. Tento způsob je znám jako tzv. „Full IPv6 Switched Network“.

Priority ve VLAN



CFI – Canonical FormatIndentifier – identifikátor formátu

Standardy 802.1p, 802.1Q

VLAN tag má tři části: prioritu (3 bity), identifikátor formátu (1 bit) a identifikátor VLAN sítě (12 bitů).
Pole priority není definováno pomocí VLAN standardu, nýbrž pomocí vlastního standardu IEEE 802.1p. Protokol 802.1p je zde jistý vedlejší produkt protokolu 802.1Q a byl zahrnut jako doplněk do protokolu 802.1D.

Bylo stanoveno osm prioritních úrovní:

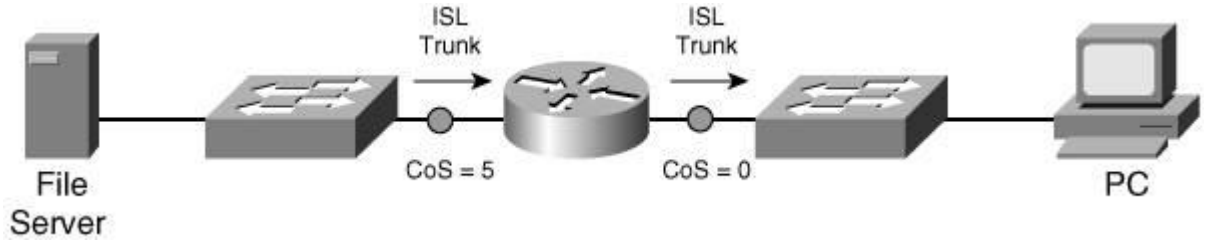
0 … „best effort“ (defaultní hodnota);
1 … pozadí;
2 … standard;
3 ... pro kritické obchodní aplikace;
4 …pro multimédia;
5 …video se zpožděním < 100 ms;
6 …hlas se zpožděním < 10 ms;
7 …řízení sítě.

Problém je zde s prodloužením rámce (1522 oktetů místo 1518), to řeší standard 802.3ac. Pokud není rámec typu VLAN, má v poli VLAN typ standardní hodnotu.

Příklad

Ve Frame relay máme bit DE (značkování zahoditelných rámců při přetížení),
v ATM máme obdobný bit CLP.

Před průchodem směrovačem musí být značka CoS přeznačena na DSCP nebo ToS,
neboli značka 2. vrstvy na značku 3. vrstvy, jinak by provoz ze směrovače odcházel
s hodnotou CoS 0:



I když se doporučuje značkovat provoz co neblíže u zdroje, nechceme, aby si priority nastavovali koncoví uživatelé. Proto se na přepínačích vytváří tzv. **trust boundary** (hranice důvěry), kdy nedůvěřujeme příchozím značkám od koncových uživatelů. Výjimkou jsou IP telefony, které značkují pakety a lze rozšířit hranici důvěry až k nim.

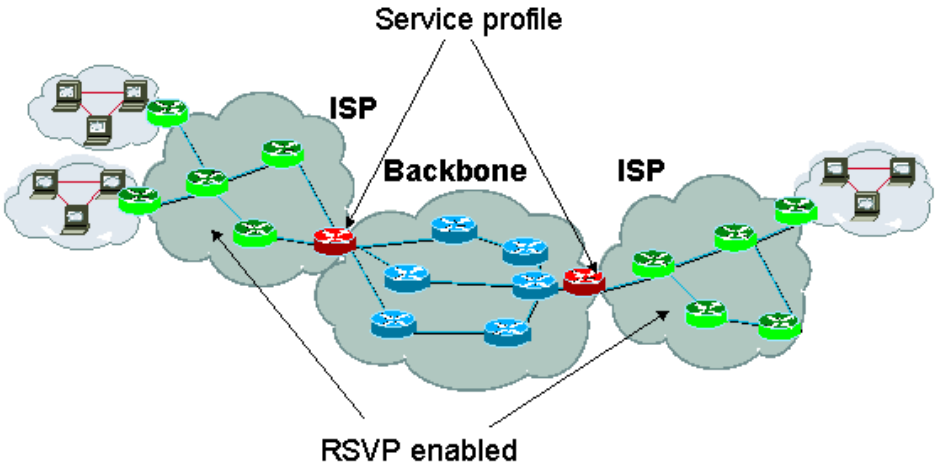
Rozdíl mezi službami IntServ a DiffServ

Porovnávací kritéria/Technologie	IntServ	DiffServ
Zajištění kvality přenosu	na jednotlivý tok	na všechny toky
Rozsah zajištění kvality přenosu	na úrovni aplikace	na úrovni domény
Zdroj rezervace	provádí aplikace	provádí hraniční směrovač na základě SLA
Správa řízení	distribuovaná	centrálně v doméně
Signalizace	RSVP	DSCP
Škálovatelnost	limitována počtem datových toků	limitována počtem tříd
Typ kvality služby	GS, CLS, "Best–effort"	EF, AF, "Best–effort"
Složitost uplatnění	vysoká	nízká

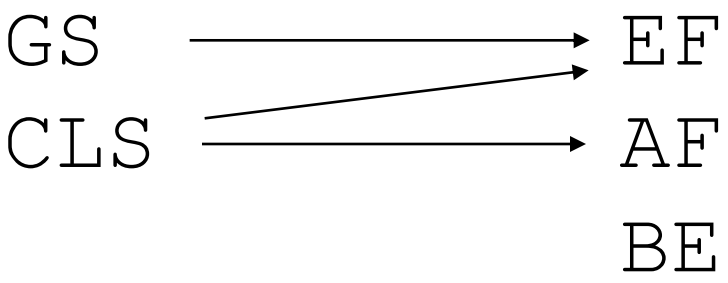
Dá se říci, že architektura Intserv je komplementární k architektuře Diffserv.
Tyto architektury lze kombinovat tak, že se budou mapovat požadavky Intserv do požadavků Diffserv. Diffserv v porovnání s Intserv eliminuje práci s datovými toky a tím přispívá ke škálovatelnosti velkých sítí. Na druhé straně ovšem negarantuje koncovou kvalitu služby.

Kombinované systémy

Problém je předmětem výzkumu, např. na Carnegie Mellon University v Pittsburgu (USA), viz obrázek z http://www.ncne.nlanr.net/news/workshop/vbns-techs2/Talks/huiqos/sld013.htm,
kde okrajové sítě podporují RSVP/Intserv a páteřní Diffserv.



Mapování z Intserv do Diffserv lze provést nejlépe takto:



2. Klasifikace a značkování

Kategorie mechanismů QoS

- Klasifikace
- Značkování
- Řízení zahlcení
- Předcházení zahlcení
- Omezení rychlosti (policing a sharping)
- Výkonnostní linky

Mechanismy pro klasifikaci na směrovačích

- ACL (Access Control List)
- NBAR (Network Based Application Recognition)

NBAR

```
Pepa(config)#interface fastethernet 0/0
Pepa(config-if)#ip nbar protocol-discovery
Pepa#show ip nbar protocol-discovery
FastEthernet0/0
                         Input                     Output
                         -----                     ------
   Protocol              Packet Count              Packet Count
                         Byte Count                Byte Count
                         5min Bit Rate (bps)       5min Bit Rate (bps)
                         5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
   ---------------------- ------------------------ ------------------------
   ftp                   4317                      10757
                         279012                    14127498
                         0                         62000
                         15000                     363000
   dhcp                  134                       0
                         82812                     0
                         1000                      0
                         1000                      0
   pop3                  70                        59
                         4356                      7487
                         0                         0
                         0                         1000
   smtp                  65                        67
                         6298                      5142
                         0                         0
                         0                         0
   http                  3                         2
```

Kde všude lze použít priority?

```
config)#priority-list 1 ?

default      Set priority queue for unspecified datagrams
interface    Set priorities for packets from a named interface
protocol     priority queueing by protocol
queue-limit  Set queue limits for
```

Výběr podle protokolu

```
F(config)#priority-list 1 protocol ?
arp             IP ARP
bridge          Bridging
cdp             Cisco Discovery Protocol
http            HTTP
ip              IP
llc2            llc2
pad             PAD links
pppoe           PPP over Ethernet
snapshot        Snapshot routing support
……              ……
```

Výběr z protokolu IP

```
FC-CPE-1(config)#priority-list 1 protocol ip ?

high
medium
normal
low
```

Jak zpřesnit IP pakety vysoké priority

```
FC-CPE-1(config)#priority-list 1 protocol ip high ?

fragments  Prioritize fragmented IP packets
gt         Prioritize packets greater than a specified size
list       To specify an access list
lt         Prioritize packets less than a specified size
tcp        Prioritize TCP packets 'to' or 'from' the specified port
udp        Prioritize UDP packets 'to' or 'from' the specified port
```

Jak zpřesnit segmenty TCP?

```
FC-CPE-1(config)#priority-list 1 protocol ip high tcp ?
<0-65535>  Port number
domain     Domain Name Service (53)
echo       Echo (7)
ftp        File Transfer Protocol (21)
ftp-data   FTP data connections (20)
irc        Internet Relay Chat (194)
nntp       Network News Transport Protocol (119)
pop3       Post Office Protocol v3 (110)
smtp       Simple Mail Transport Protocol (25)
telnet     Telnet (23)
www        World Wide Web (HTTP, 80)
……
```

Konfigurace prioritních front

F (config)#**priority-list *1* protocol http high**
F (config)#**priority-list *1* protocol ip normal tcp ftp**
F (config)#**priority-list *1* protocol ip medium tcp telnet**
!
F(config)#**int s0/1/0**
F(config-if)#**priority-group 1**
!
FC-CPE-1**#show queueing priority**
Current DLCI priority queue configuration:
Current priority queue configuration:

List Queue Args
1 high protocol http
1 normal protocol ip tcp port ftp
1 medium protocol ip tcp port telnet

Kontrola toků na vstupu a výstupu

```
F(config)#interface fastethernet 0/0
F(config-if)#ip flow egress
F(config-if)#ip flow ingress
F(config-if)#interface fastethernet 0/1
F(config-if)#ip flow ingress
F(config-if)#ip flow egress
!
F#show ip flow interface
FastEthernet0/0
  ip flow ingress
  ip flow egress
FastEthernet0/1
  ip flow ingress
  ip flow egress
!
F#clear ip flow stats
```

Výstup statistik

```
F#show ip cache flow
IP packet size distribution (3969 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .351 .395 .004 .011 .001 .005 .009 .001 .002 .005 .001 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .013 .000 .195 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 1368 added
  22316 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17416 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 02:50:15
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           9      0.0        13    47      0.0       5.2      10.8
TCP-FTP             28      0.0         7    62      0.0       0.8      10.4
TCP-WWW             64      0.0         7   138      0.0       0.3       2.1
TCP-other           16      0.0        75   840      0.1       0.0       4.1
UDP-DNS            878      0.0         1    72      0.0       0.0      15.4
UDP-other          347      0.0         3    88      0.1       4.5      15.5
ICMP                26      0.0         1    70      0.0       0.8      15.4
Total:            1368      0.1         2   318      0.3       1.2      14.6
```

Jiná varianta výstupu

```
F#show ip cache verbose flow
IP packet size distribution (5223 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .303 .030 .142 .031 .034 .001 .002 .001 .000 .000 .004 .000 .075 .000
……….

IP Flow Switching Cache, 278544 bytes
  9 active, 4087 inactive, 62 added
……….
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          18      0.0         3    45      0.2       3.6      10.9
……….
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Fa0/1          0.0.0.0         Null           255.255.255.255 11 00  10     222
0044 /0  0                     0043 /0  0     0.0.0.0                604  1356.9
Fa0/1          10.0.0.200      Se0/1/0        10.20.0.200     06 00  18    1368
01BD /0  0                     06AA /0  0     0.0.0.0                970   184.9
Fa0/1          10.0.0.200      Se0/1/0*       10.20.0.200     06 00  18    1368
01BD /0  0                     06AA /0  0     0.0.0.0                970   184.9
FFlags: 01
Se0/1/0        10.20.0.200     Fa0/0          172.17.1.1      11 00  10       5
0404 /0  0                     0035 /0  0     0.0.0.0                62     4.3
Se0/1/0        10.20.0.200     Fa0/0*         172.17.1.1      11 00  10       5
0404 /0  0                     0035 /0  0     0.0.0.0                62     4.3
FFlags: 01
Fa0/0          172.17.1.1      Se0/1/0*       10.20.0.200     11 00  10       5
0035 /0  0                     0404 /0  0     0.0.0.0                62     4.3
FFlags: 01
Fa0/0          172.17.1.1      Se0/1/0        10.20.0.200     11 00  10       5
0035 /0  0                     0404 /0  0     0.0.0.0                62     4.3
Se0/1/0        10.20.0.200     Fa0/1          10.0.0.200      06 00  18    1152
```

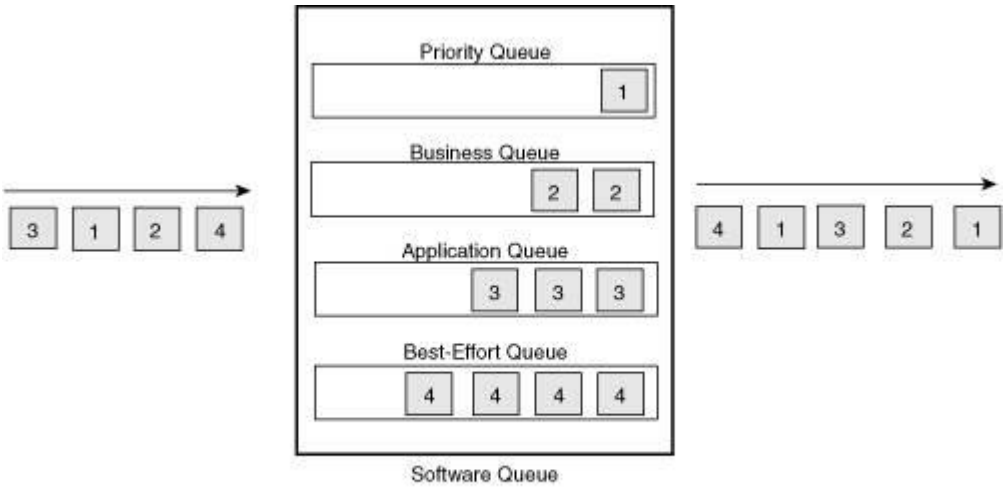
Dílčí závěr

Klasifikace a značkování slouží jako prvotní kroky k zajištění kvality hlasu, samy o sobě však nemění chování provozu.

3. Metody řazení do fronty

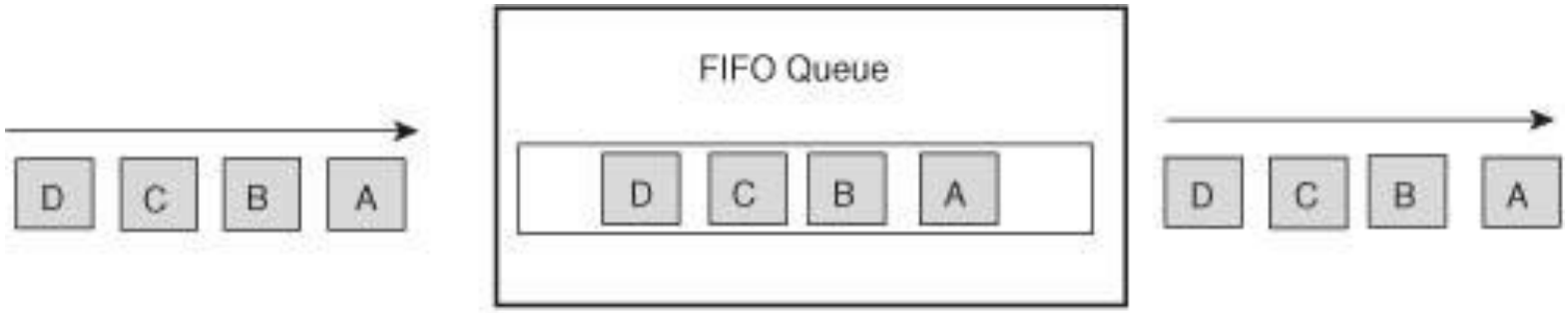
Necítíte se přetížení?

Neobsloužené požadavky ukládáme do vyrovnávací paměti.
Směrovače obsahují hardwarové i softwarové fronty.
Hardwarové fronty pracují metodou FIFO.
Při zaplnění její kapacity se pakety ukládají do softwarových front, u kterých lze použít různé mechanismy řazení do fronty



A software queuing mechanism is only invoked after an interface hardware queue overflows.

Metoda řazení FIFO

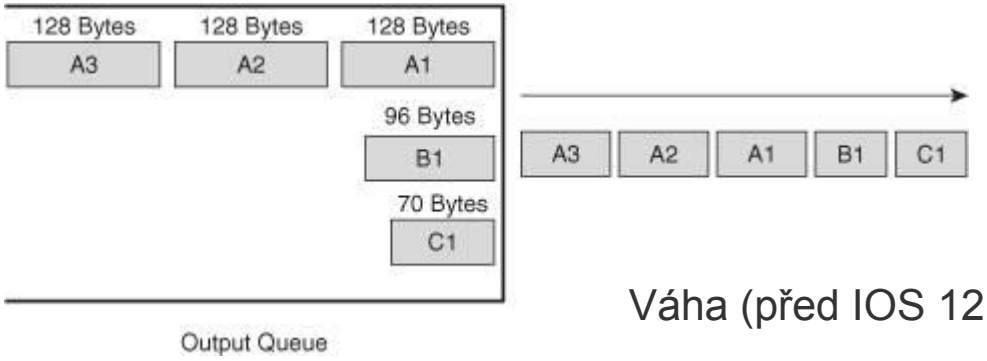


FIFO queuing does not perform any packet reordering.

Hlasové pakety mohou být trhány velkými např. FTP pakety,
což může vést k vyhladovění provozu a k značným pauzám ve hlasu.

Metoda WFQ (Weighted Fair Queuing)

Určena pro rozhraní s nízkými přenosovými rychlostmi (do 2 Mb/s).
IP precedence slouží jako váha, ukazatel se posunuje byte po byte.



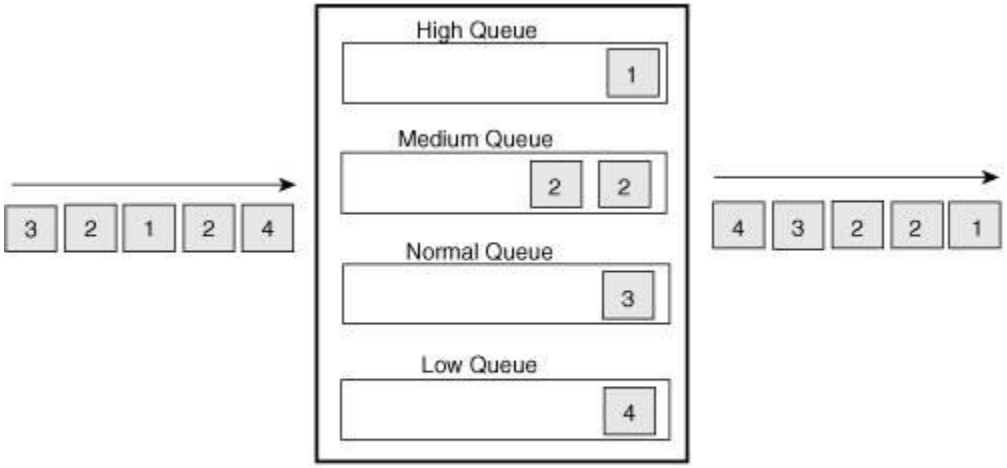
Váha (před IOS 12.0(5)T) = 4096 / (IP Prec. + 1)

Novější verze IOS (od 12.0(5)T)

Váha (novější IOS) = 32768 / (IP Prec. + 1)

Před verzí12.0(5)T
A1 = 4096 / (5 + 1) * 128 = 87,381
A2 = 4096 / (5 + 1) * 128 + 87381 = 174,762
A3 = 4096 / (5 + 1) * 128 + 174762 = 262,144
B1 = 4096 / (0 + 1) * 96 = 393,216
C1 = 4096 / (0 + 1) * 70 = 286,720

Řazení PQ (priority Queuing)



Priority queuing completely empties higher-priority queues before emptying lower-priority queues.

Režim dokáže vyhladovět provoz s nízkou prioritou.

Řazení CB-WFQ (Class-Based Weighted Fair Queuing)

Mechanismus WFO na rozdíl od PQ zajišťuje, že žádný provoz nevyhladoví, čili není opomíjen. Ani jeden však nezajistí dostupnost pásma pro definované typy provozu. Pomocí mechanismu CB-WFQ lze naopak určit minimální šířku pásma a to pro 64 tříd provozu.

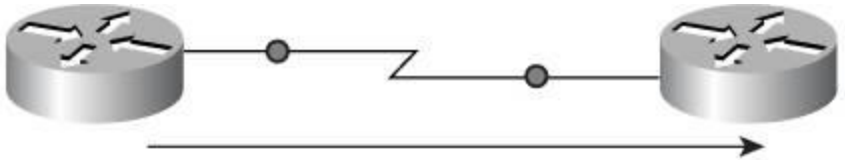
Nevyhladoví ani provoz s nižší prioritou, jako ´je tomu u PQ.

Jediná nevýhoda: nedostatek mechanismů pro prioritní řízení, to řeší drobná úprava řazení CB-WFO, která se nazývá LLQ.

LLQ může jedné nebo více třídám provozu nařídit provoz směrovat do prioritní fronty.

Je si ale třeba uvědomit, že umístěním paketu do prioritní fronty nepřidělujeme tomuto provozu pouze šířku pásma, ale také policing (omezení dostupné šířky pásma), aby provoz s nižší prioritou nevyhladověl.
LLQ je typ řazení preferovaný pro provoz, citlivý na zpoždění.

Řazení LLQ (Low Latency Queuing)

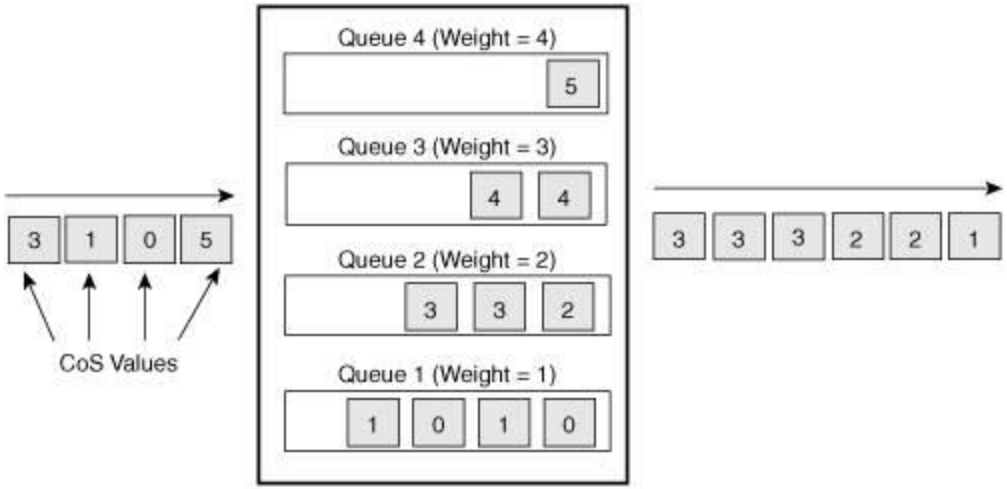


Web ⇒ Allocate at least 128 kbps of bandwidth if needed.

Voice ⇒ Allocate up to 256 kbps of *priority* bandwidth.

While CB-WFQ allocates a specific bandwidth amount, LLQ can allocate *priority* bandwidth amounts for specified traffic classes.

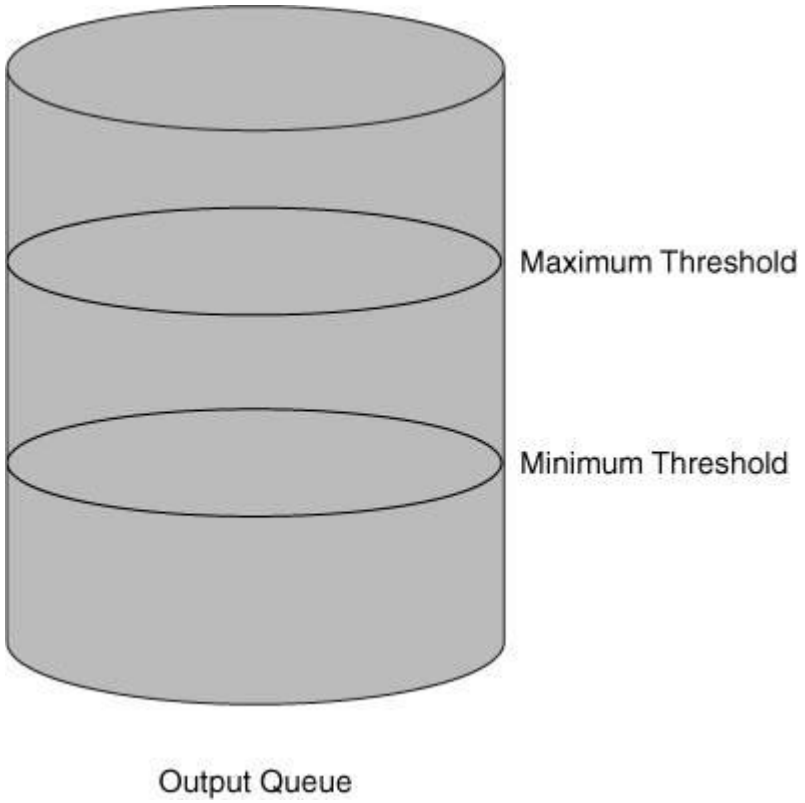
Řazení WRR (Weighted Roud Robin) používané u přepínačů Catalyst



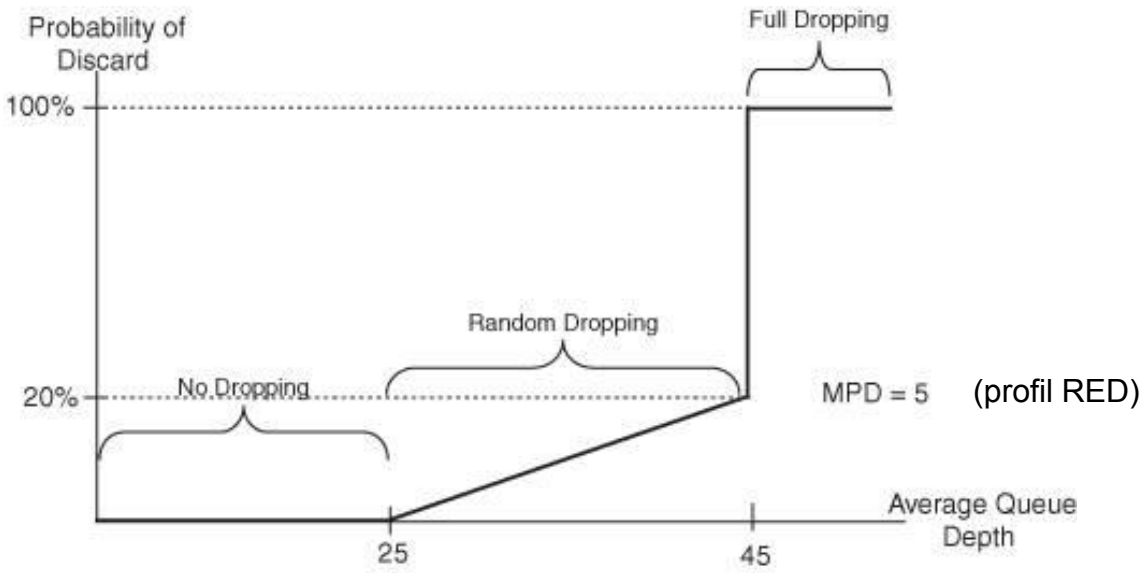
WRR *weights* queues to determine the relative amount of bandwidth available to each queue. In this example, Queue 4 has twice the available bandwidth of Queue 2.

Priority a cyklická obsluha

Mechanismus RED
(Random Early Detection)



Rozsahy zahazování RED



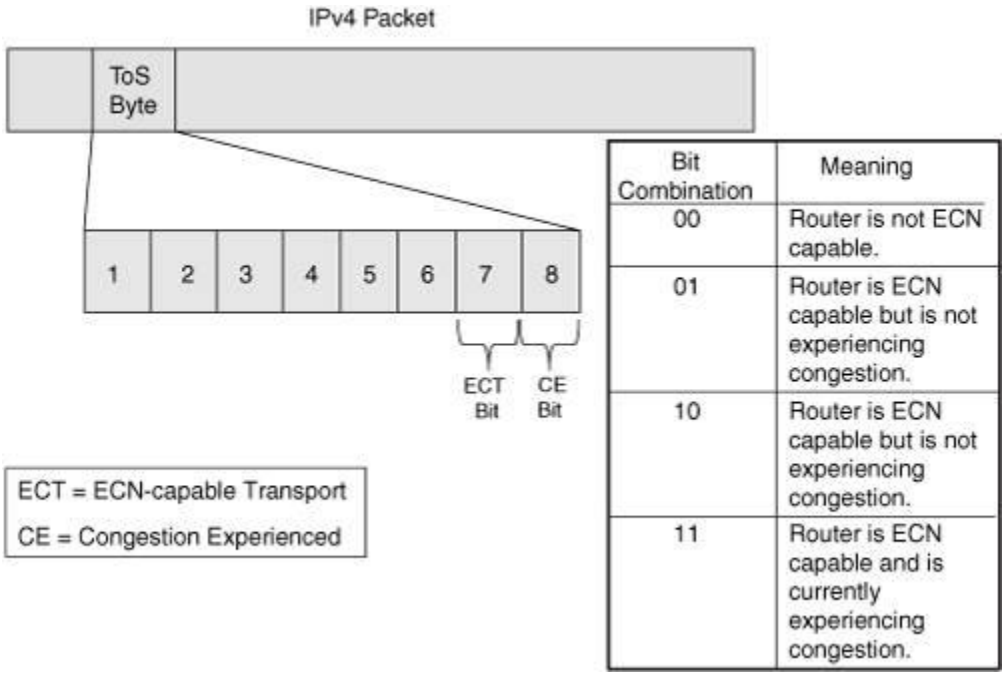
Pravděpodobnost zahození: 1/5 = 0,2 = 20 %

WRED (Weighted RED)

Na rozdíl od RED WRED vytváří profil pro každé značení priority.

Příklad:
Paket s precedencí 0 má minimální limit 20 paketů (začnou se zahazovat v případě přetížení dříve).
Paket s precedencí 1 má minimální limit 25 paketů.

WRED (Weighted RED) a oznámení ECN (Explicit Congestion Notification)



Bit Combination	Meaning
00	Router is not ECN capable.
01	Router is ECN capable but is not experiencing congestion.
10	Router is ECN capable but is not experiencing congestion.
11	Router is ECN capable and is currently experiencing congestion.

ECN (Explicit Congestion Notification) je používáno směrovači jako nástavba WRED: signalizuje, že je třeba snížit rychlost.

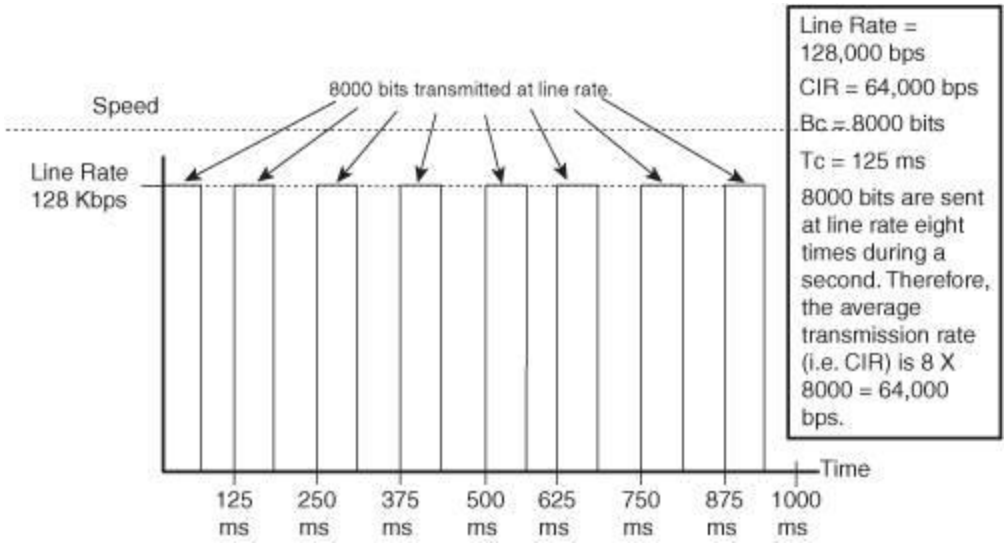
Usměrňovače provozu

Jsou to mechanismy QoS, které limitují šířku pásma:

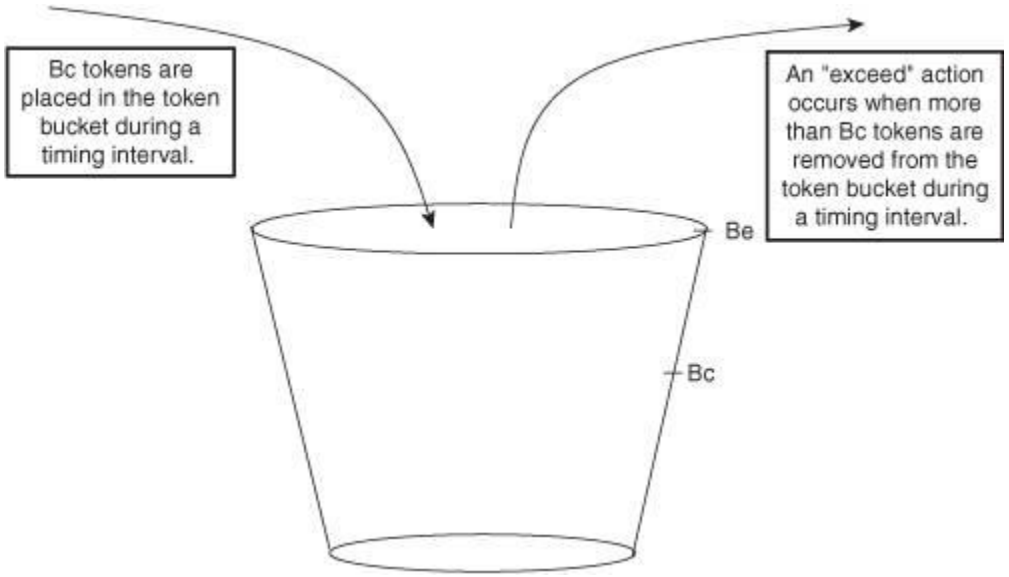
Policing: zahazuje – mechanismus lze uplatnit v příchozím i odchozím směru

Sharping: ukládá do vyrovnávací paměti
- může vést ke zpoždění, proto je určeno pro rozhraní s nižšími přenosovými rychlostmi

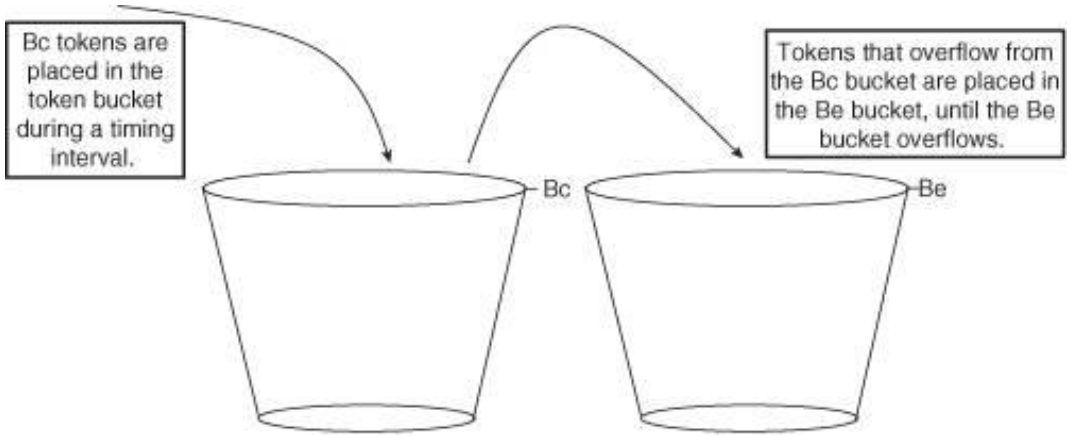
Příklad metody sharping
(přenos 64kb/s přes linku 128 kb/s)



Token Bucket

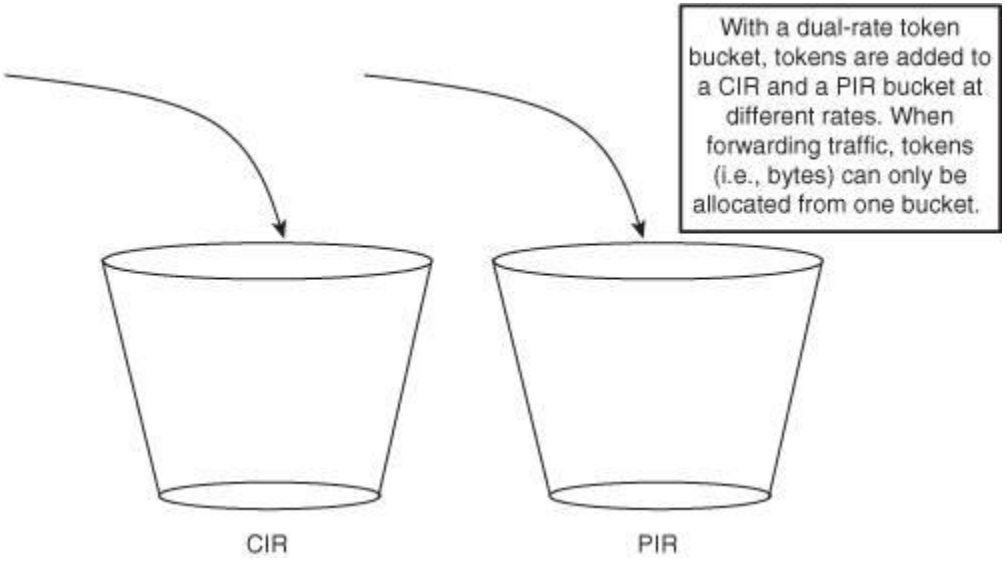


Dvojitá nádoba s pověřeními



Lze-li paket přesměrovat pomocí bajtů z první nádoby, je vyhovující.
Pokud je nutná i druhá nádoba, jde o nadměrný provoz.
Pokud ani to, jde o porušující (vioalating) provoz

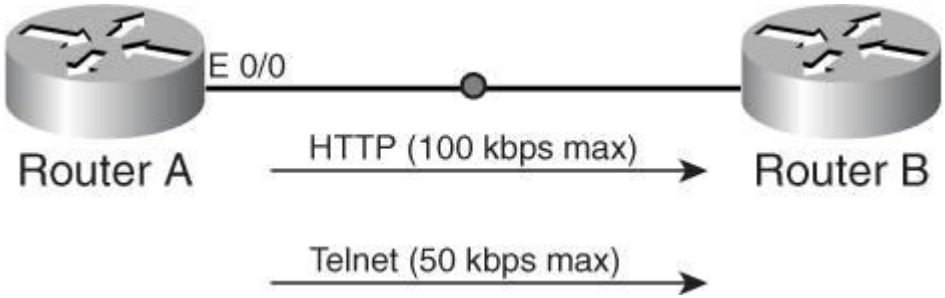
Dvě nádoby pro dvourychlostní policing



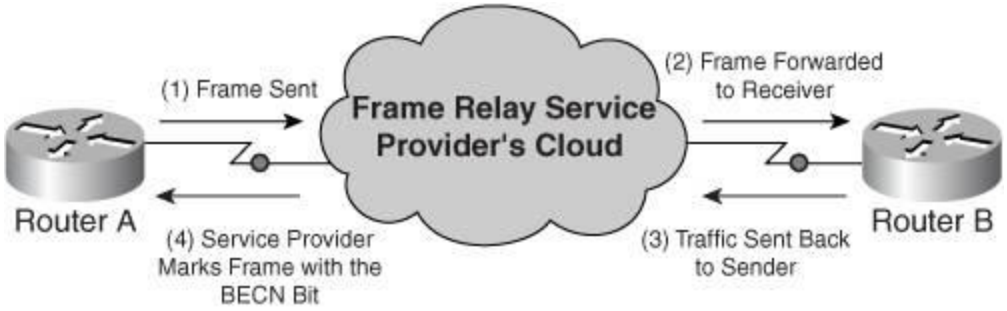
PIR (Peak Information Rate) se naplňuje vyšší rychlostí
S nadměrnými pakety se dělá akce překročení (např. se paket přenese s DSCP AF11)

Mechanismus policing

Omezení pro zajištění přenosu hlasu.



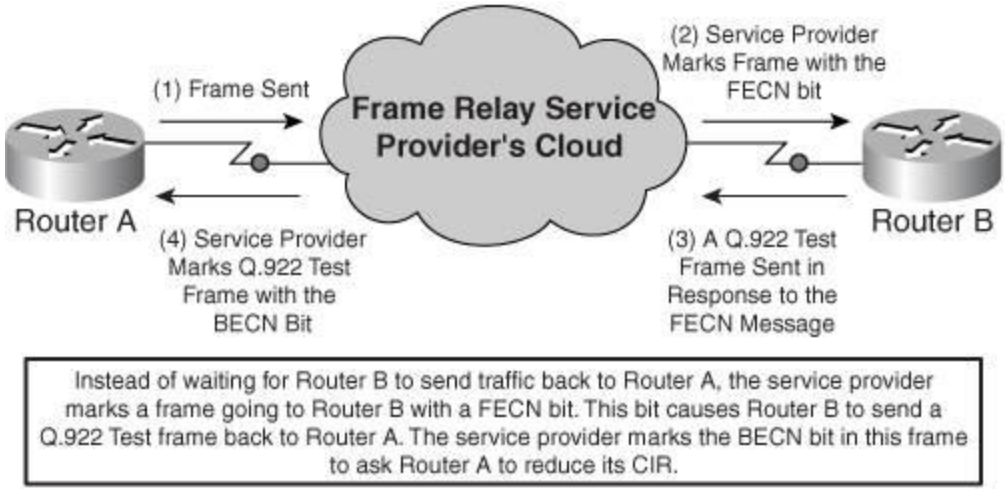
Sharping na sítích Frame Relay
Oznámení BECN



When Router A receives a frame marked with a BECN bit, it reduces its CIR by 25 percent.

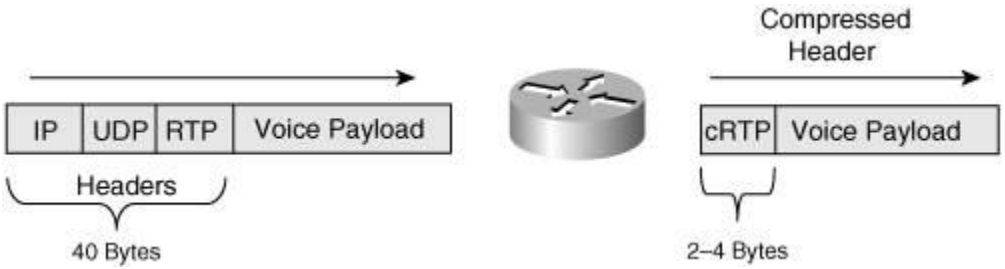
Výchozí směrovač musí být nakonfigurován tak, aby reagoval na BECN.

Sharping na sítích Frame Relay
Oznámení BECN



Cílový směrovač musí být nakonfigurován tak, aby reagoval na FECN:
Pošle bezvýznamný rámec (testovací rámec Q.922).
Zvýšení rychlosti je už opatrné: (Be + Bc)/16 bitů za časový interval.

Komprimace záhlaví



Fragmentace a prokládání
(LFI - Link Frgmentation and Interleaving)

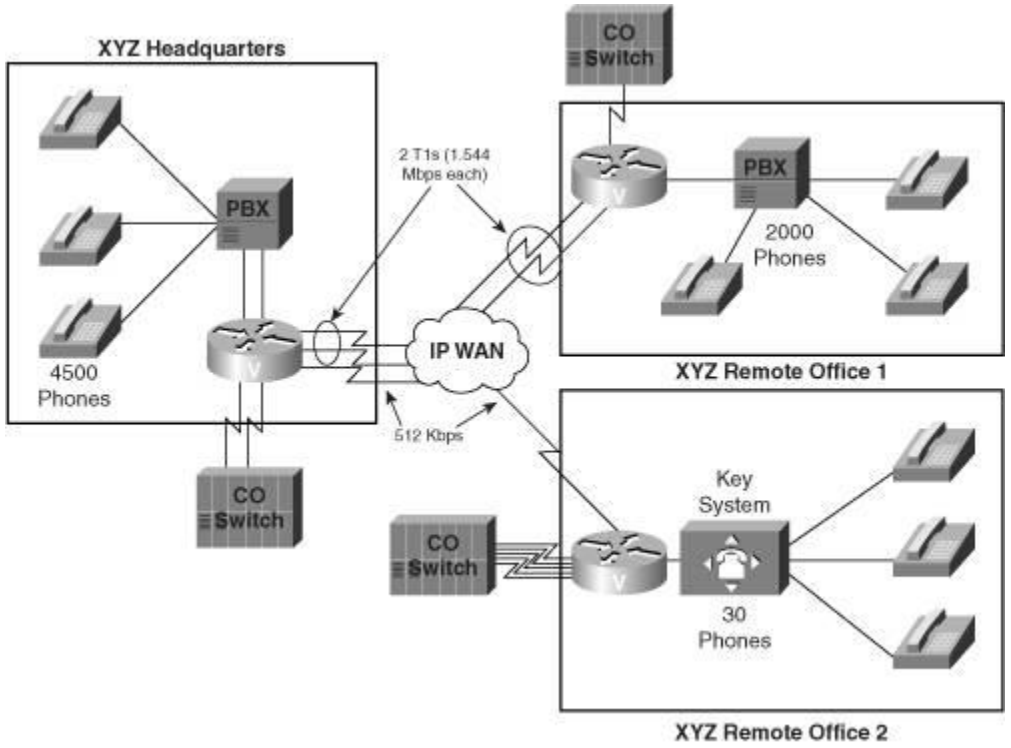
Tři mechanismy LFI:

- MLPP (také označení MP, MPL, MPPP či Multilink)
- FRF.12 - VoIPoFR
- FRF.11 Annex C – u linek VoFR

Při konfiguraci mechanismu LFI musí být zpoždění serializace v rozsahu od 10 do 35 ms

Příklad: Rámec 512 B na lince o 128 kb/s má zpoždění serializace
(512 *8)/128 = 32 ms, neboli nevyhovuje požadavku

Příklad: Navrhované řešení pro firmu XYZ



Doporučení: Ústředí společnosti XYZ – vzdálená pobočka 1: LLQ nebo WRED
Ústředí společnosti XYZ – vzdálená pobočka 2: LLQ, WRED, c RTP, MLP