MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Kvalita služby v IP sieťach

PS2 – prednáška 8

Katedra informačných sietí
FRI, UNIZA

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

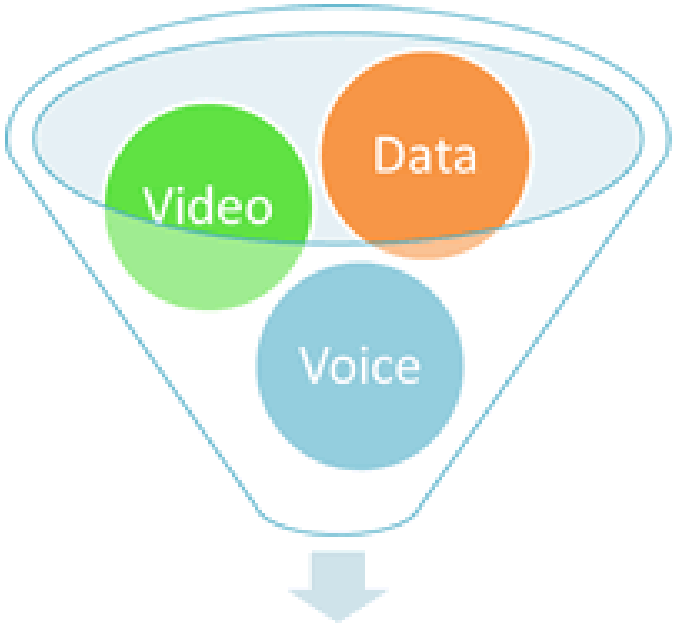
Čo nás dnes čaká

- Aké faktory ovplyvňujú kvalitu služieb v IP sieti
- Aké sú minimálne požiadavky na sieť pre prenos hlasu, videa a údajov
- Aké frontovacie algoritmy sú používaných sieťovými zariadeniami
- Aké sú rôzne modely QoS
  - Best-effort
  - Integrated Services
  - Differenciated Services
- Ako QoS používa mechanizmy na zabezpečenie kvality prenosu


MEASURE
ERROR
ROUGHPUT
NETWORK
MECHANISM
REQUIREMENTS
TRAFFIC
QUALITY
APPLICATIONS
OF
SLA
BANDWIDTH
SERVICE
DELAY
RATES
TELEPHONY
JIT
LATENCY
PERFORMANCE
COMPUTER
QoS
STANDARD
AVAILABILITY
© Can Stock Photo - csp19010668

Úvod do QoS

Prostriedky pre kvalitu služby

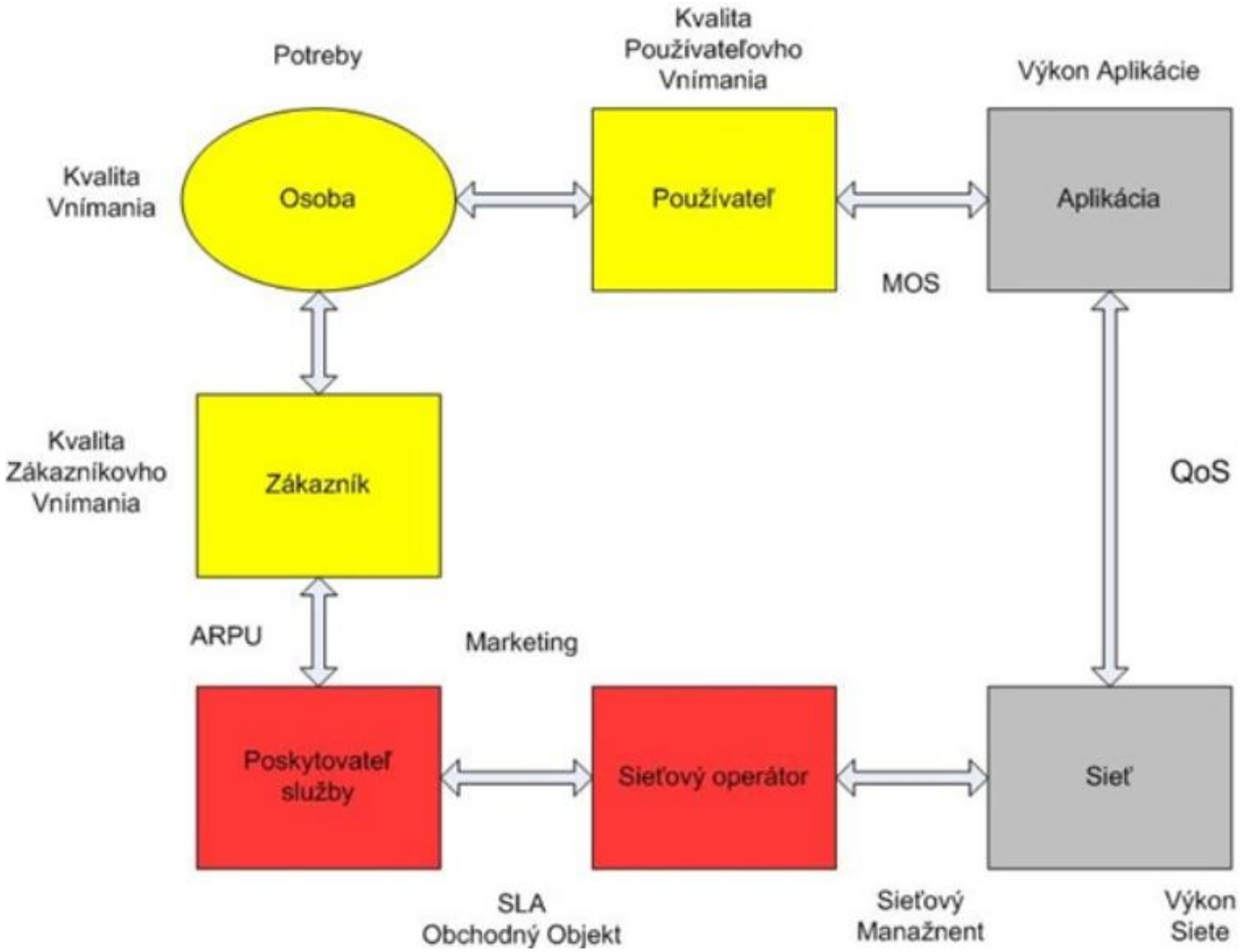


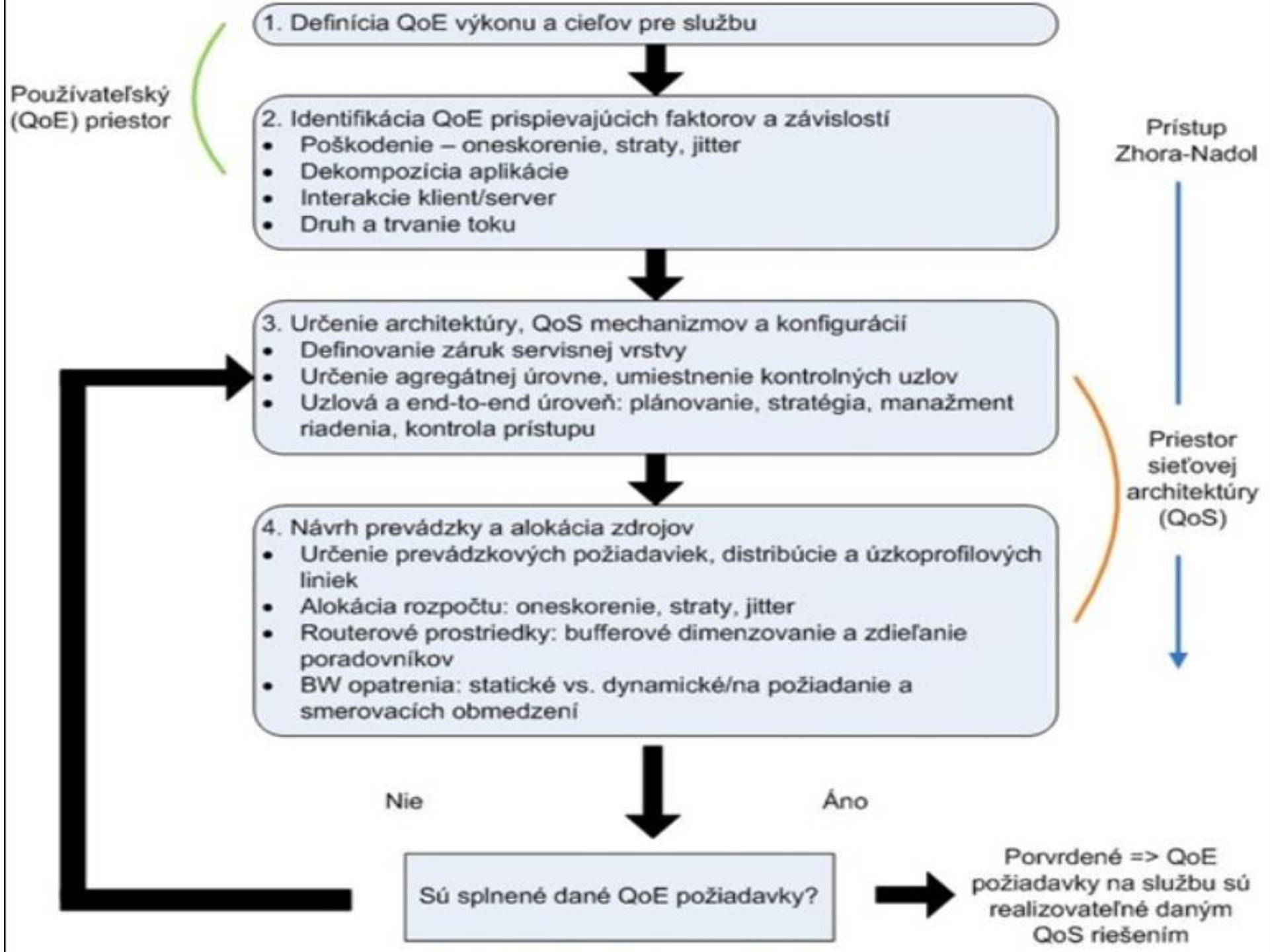
- Čo je to kvalita služby?
  - Miera uspokojenia používateľa tejto služby s jej úrovňou
  - Veľmi subjektívny pojem
  - Silne závislý na povahe služby
- Prečo potrebujeme riešiť kvalitu služby?
  - Pretože IP siete, s ktorými pracujeme, sa ku každému toku dát zvyknú chovať rovnako
  - Toky dát ale nie sú rovnocenné
  - Bezuzdné zvyšovanie kapacity liniek nie je ani ekonomické, ani dostupné

QoS – merateľné parametre siete, QoE – vnímaná kvalita

- QoS (kvalita služby)
- QoS riešenie – zabezpečí „sieťové parametre“, tie sú merateľné (napr. oneskorenie paketu pri prechode sieťou, ...)
- QoE (kvalita vnímania) - Ako vníma kvalitu služby človek
- Parametre QoS prepočíta na hodnotu QoE (MOS)
- QoE študujú viac na – KT EF
- My „robíme“ QoS – ako konfigurovať zariadenia, aby sme dosiahli určité hodnoty sieťových parametrov
- http://www.posterus.sk/?p=11948

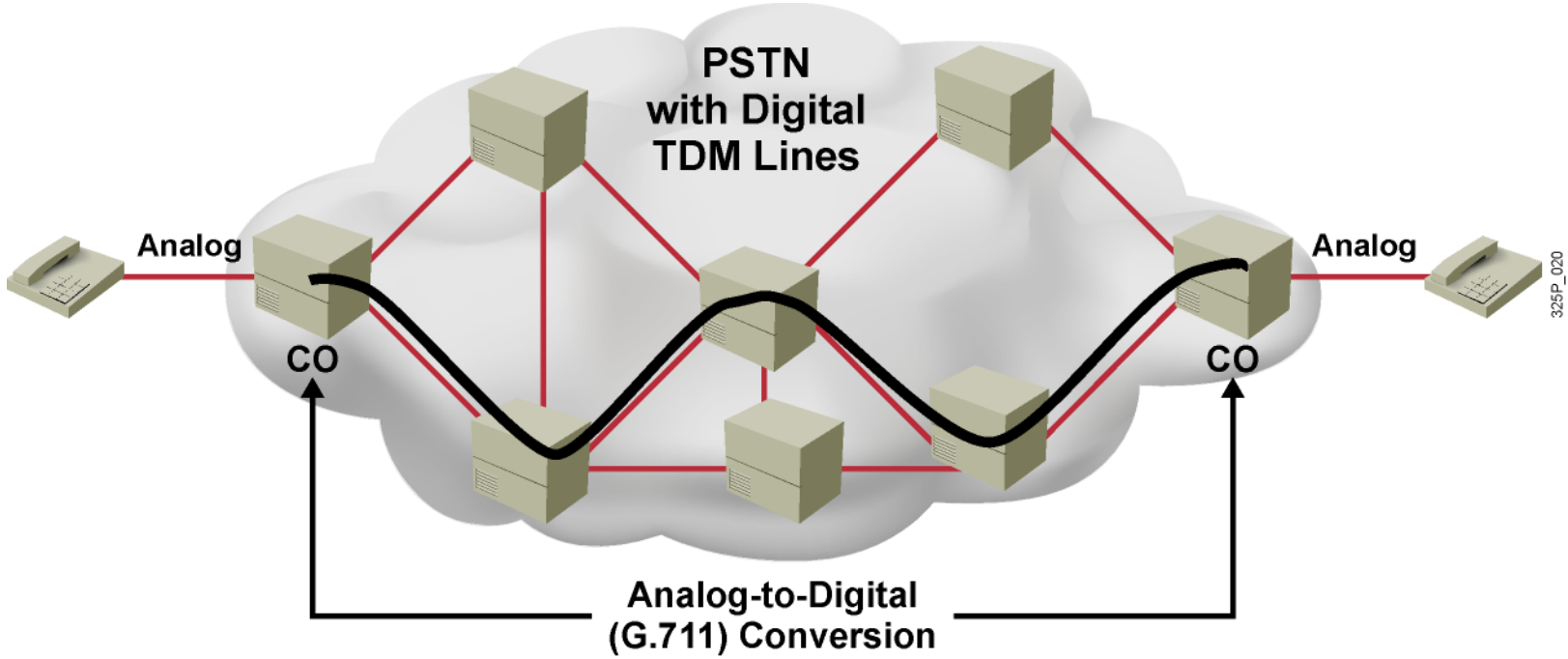
QoE (kvalita vnímania), QoS (sieťové par.)




1. Definícia QoE výkonu a cieľov pre službu
Používateľský (QoE) priestor
2. Identifikácia QoE prispievajúcich faktorov a závislostí
• Poškodenie – oneskorenie, straty, jitter
• Dekompozícia aplikácie
• Interakcie klient/server
• Druh a trvanie toku
Prístup Zhora-Nadol
3. Určenie architektúry, QoS mechanizmov a konfigurácií
• Definovanie záruk servisnej vrstvy
• Určenie agregátnej úrovne, umiestnenie kontrolných uzlov
• Uzlová a end-to-end úroveň: plánovanie, stratégia, manažment riadenia, kontrola prístupu
Priestor sieťovej architektúry (QoS)
4. Návrh prevádzky a alokácia zdrojov
• Určenie prevádzkových požiadaviek, distribúcie a úzkoprofilových liniek
• Alokácia rozpočtu: oneskorenie, straty, jitter
• Routerové prostriedky: bufferové dimenzovanie a zdieľanie poradovníkov
• BW opatrenia: statické vs. dynamické/na požiadanie a smerovacích obmedzení
Nie
Áno
Sú splnené dané QoE požiadavky?
Porvrdené => QoE požiadavky na službu sú realizovateľné daným QoS riešením

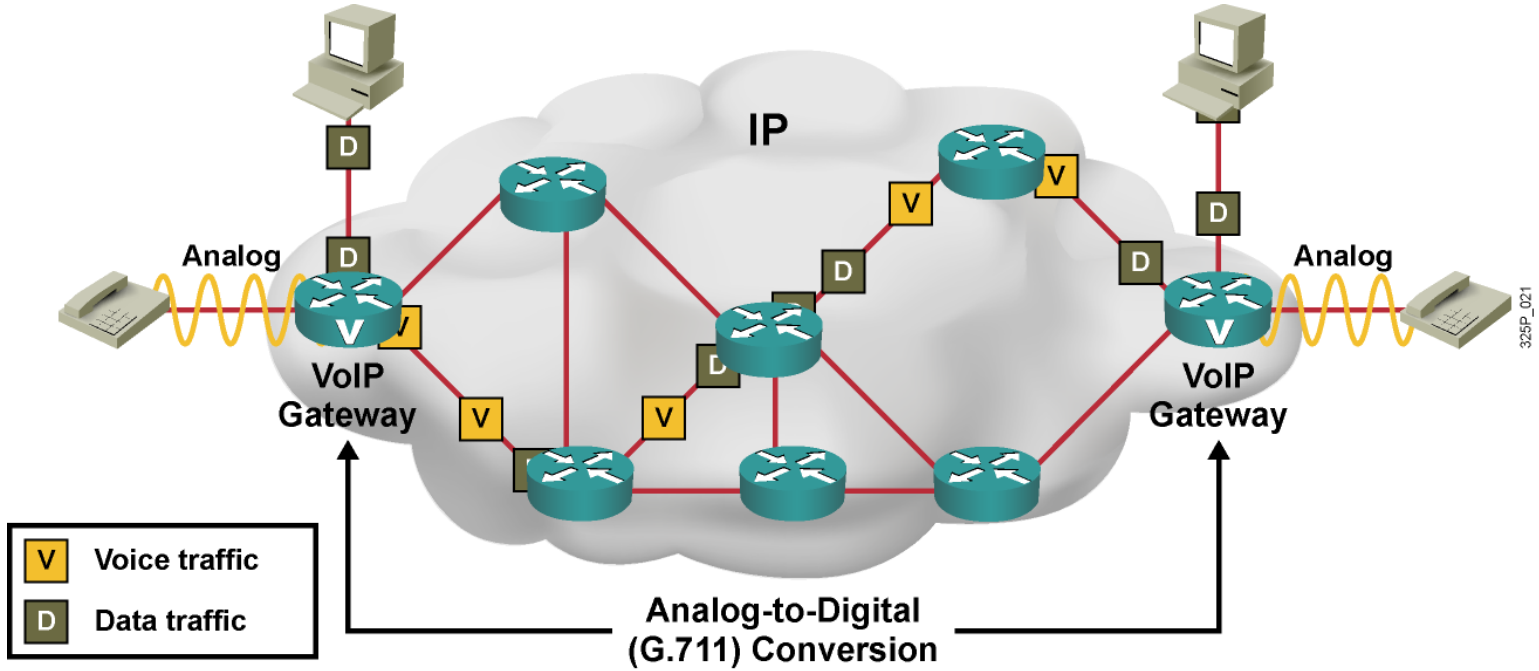
Prenos hlasu v sieťach s prepínaním okruhov

- Analógové telefóny sa pripájajú k telefónnym ústredniam
- Telefónne ústredne realizujú konverziu medzi analógovým a digitálnym signálom
- Po zostavení hovoru sa telefónna sieť stará o to, aby hovor mal
  - Svoj vlastný vyhradený prenosový okruh
  - Synchrónny prenos s fixnou šírkou pásma a veľmi malým, konštantným oneskorením



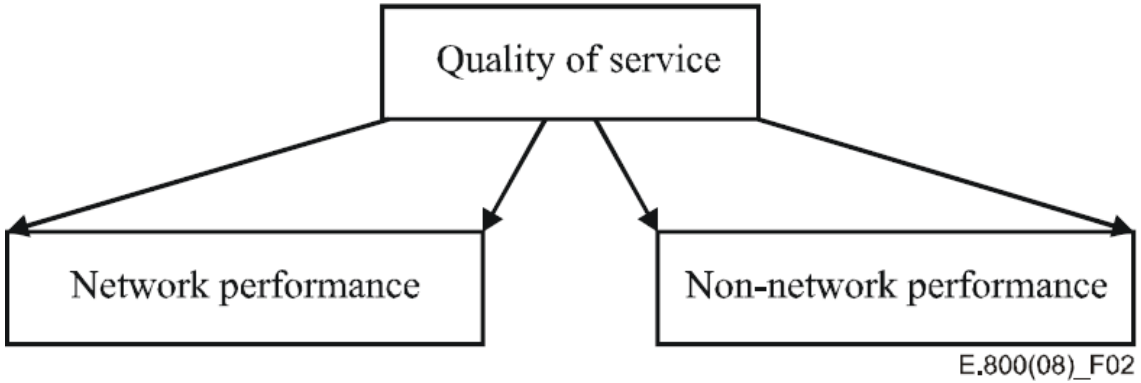
Prenos hlasu vo VoIP sieťach

- Analógové telefóny sa pripájajú k hlasovým bránam
- Hlasové brány realizujú konverziu medzi analógovým a digitálnym signálom
- Po zostavení hovoru IP sieť poskytuje
  - Prenos individuálnych paketov sieťou nezávisle
  - Zdieľanú šírku pásma, vyššie a premenlivejšie oneskorenie



ITU-T Odporúčanie E.800

- Kvalite služby sa venuje široká pozornosť aj zo strany normotvorných organizácií
- ITU-T má rad odporúčaní, ktoré sa dotýkajú otázok kvality služby, SLA, jej hodnotenia atď.
- E.800: Definitions of terms related to quality of service

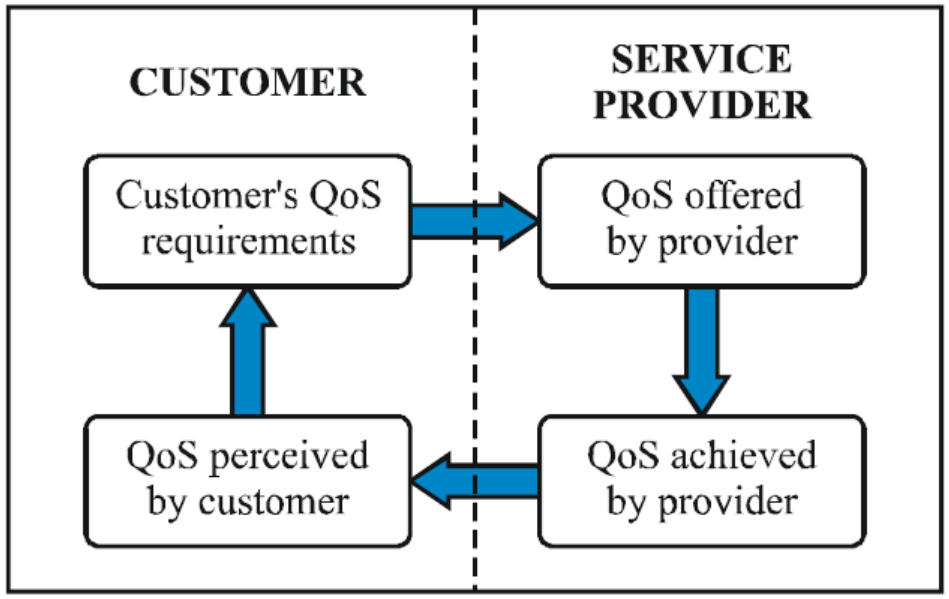


  - NP: Prenosová rýchlosť, oneskorenie, jitter, stratovosť, ...
  - NNP: Čas zriadenia služby, trvanie odstránenia výpadku, tarify, ...

●Picture retaken from ITU-T E.800 (09/2008), https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809-I!!PDF-E&type=items

ITU-T Odporúčanie E.800

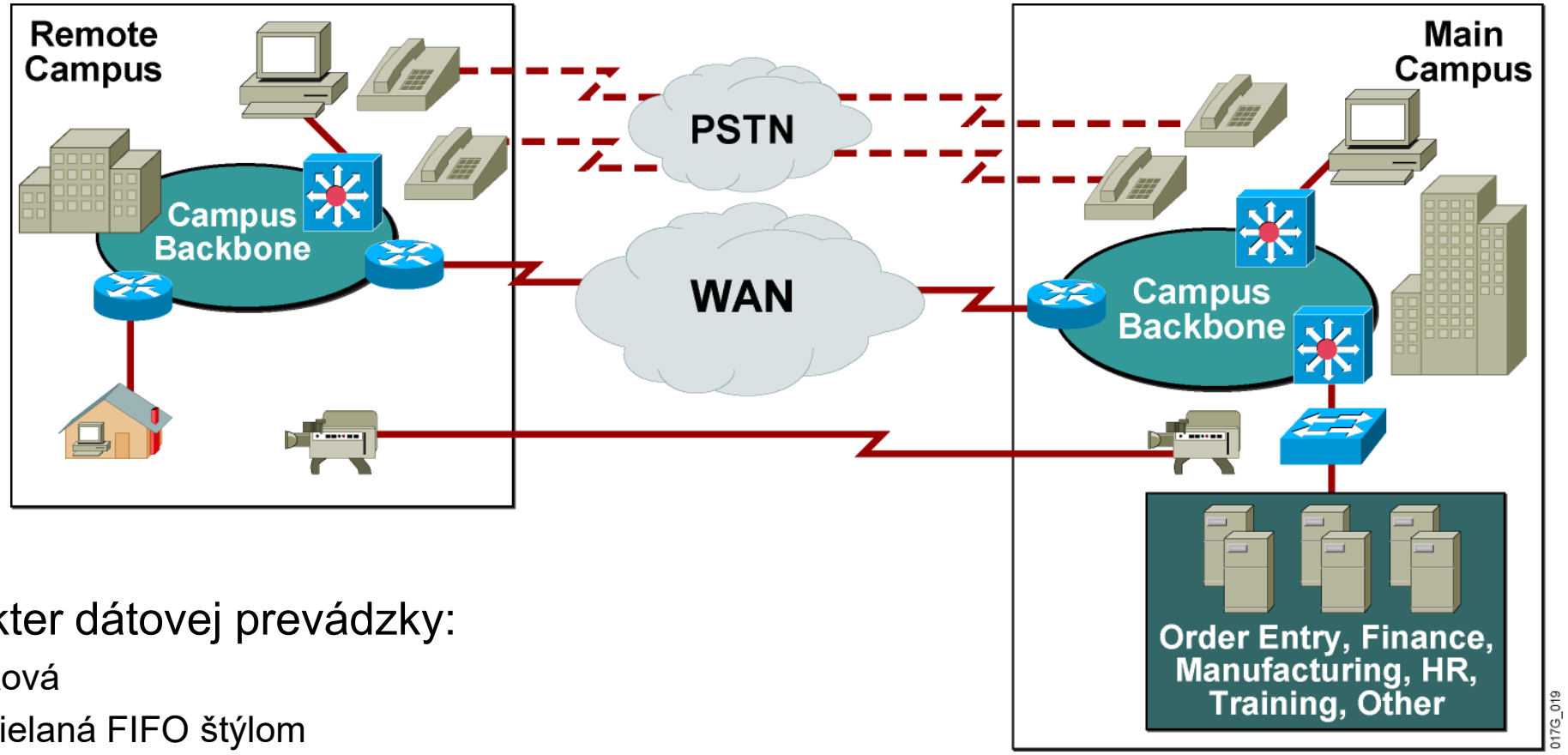
- Podľa E.800:
  - **Quality**: The totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs.
  - **Service**: A set of functions offered to a user by an organization.
  - **Quality of Service**: Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service.
- Zákazníkovo vnímanie poskytovanej QoS sa môže líšiť od úrovne QoS, o ktorej sa operátor domnieva, že ju ponúka



Picture retaken from ITU-T E.800 (09/2008), https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809-I!!PDF-E&type=items

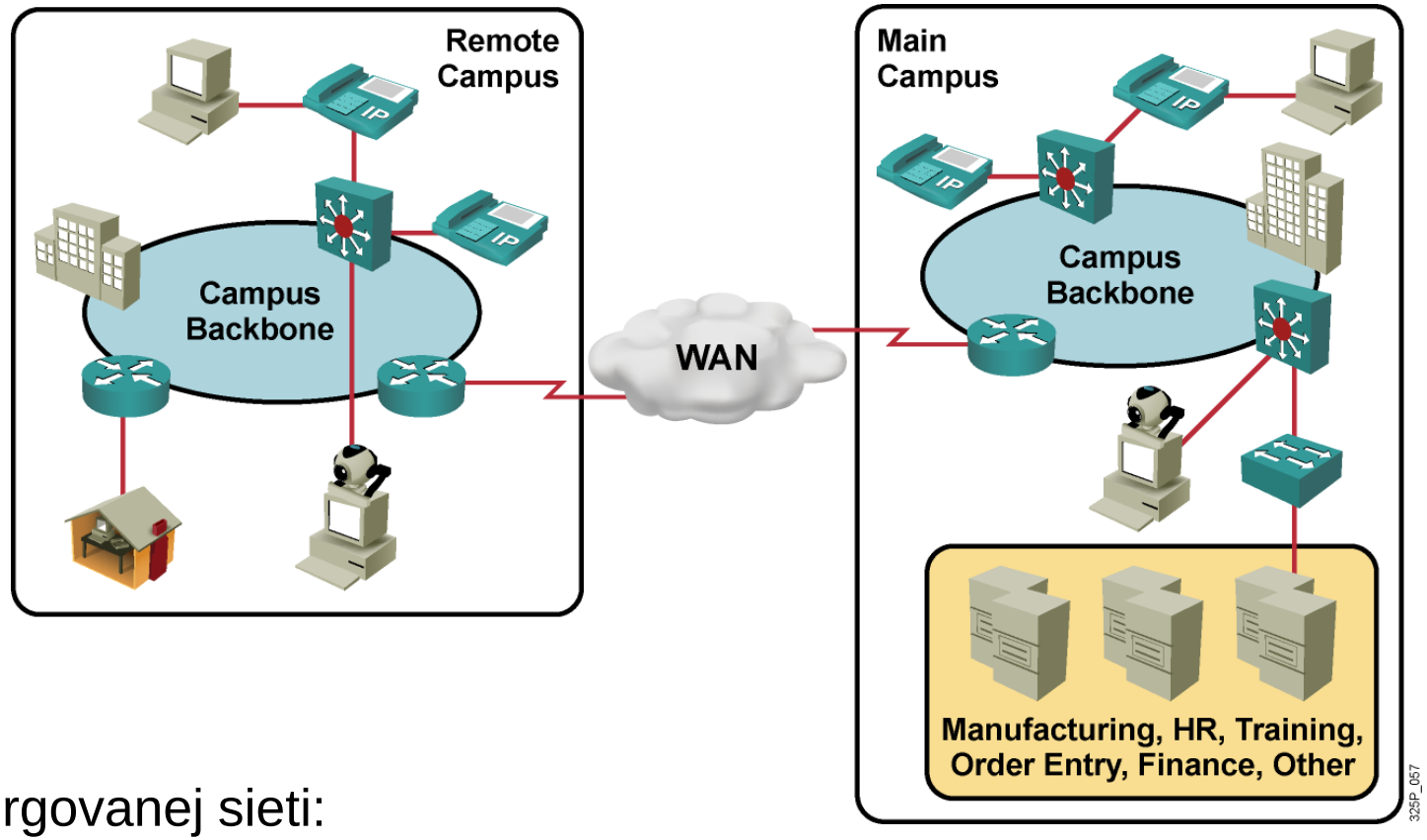
Faktory ovplyvňujúce kvalitu služby

Tradičná nekonvergovaná sieť



- Charakter dátovej prevádzky:
  - Zhluková
  - Odosielaná FIFO štýlom
  - Nenáročná na včasnosť doručenia
  - Krátke výpadky sú tolerovateľné

Problémy v konvergovanej sieti



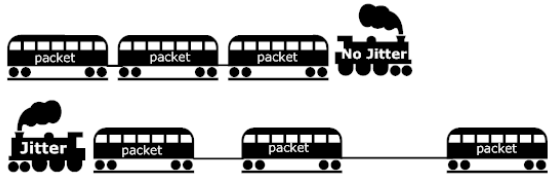
- Toky v konvergovanej sieti:
  - Pravidelné hlasové toky malých paketov súperia so zhlukovou dátovou prevádzkou
  - Časovo kritická prevádzka musí mať prioritu
    - Hlas, video, real-time aplikácie
  - Nemožno tolerovať ani krátke výpadky

Faktory vplývajúce na kvalitu služby v paketovej sieti

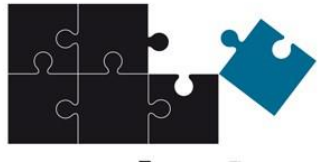
- **Prenosová kapacita**
  - Mnohé toky súperia o obmedzené množstvo prenosovej kapacity prepínačov, smerovačov a rozhraní medzi nimi

- **Celkové oneskorenie (pevná aj variabilná zložka)**
  - Pakety musia prejsť cez početné sieťové zariadenia a prepoje, z ktorých každé vnáša svoju časť oneskorenia

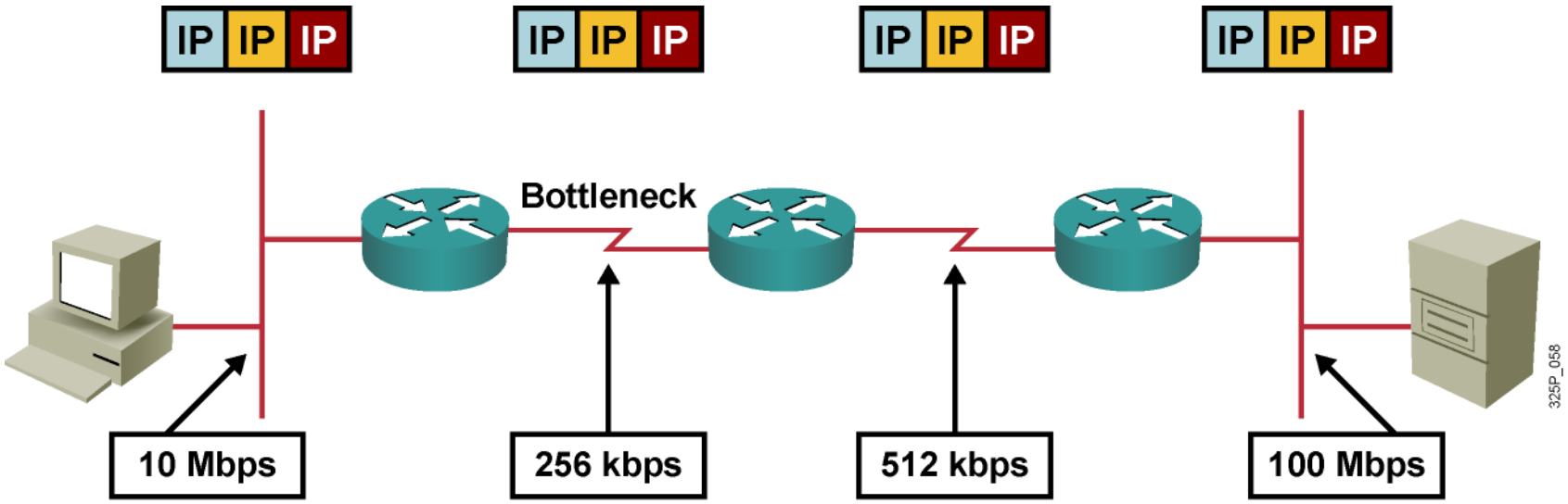
- **Kolísanie oneskorenia (jitter)**
  - Tok inej prevádzky popri hlasovej prevádzke vnáša náhodné zmeny v oneskorení



- **Straty paketov**
  - Pri zahltení rozhrania sa pakety môžu zahadzovať



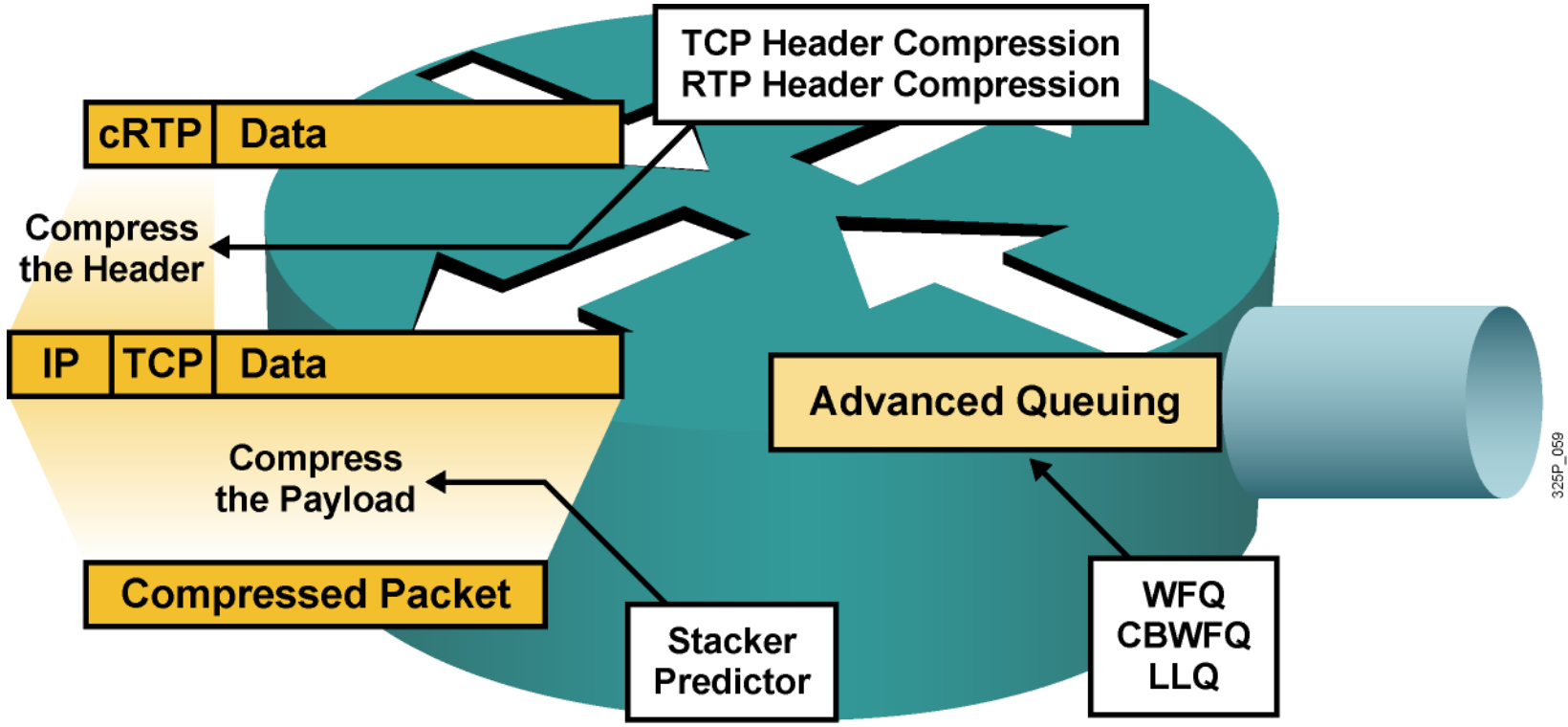
Disponibilná prenosová kapacita



$Bandwidth_{max}$ = min (10 Mbps, 256 kbps, 512 kbps, 100 Mbps) = 256 kbps
$Bandwidth_{avail}$ = $Bandwidth_{max}$ / flows

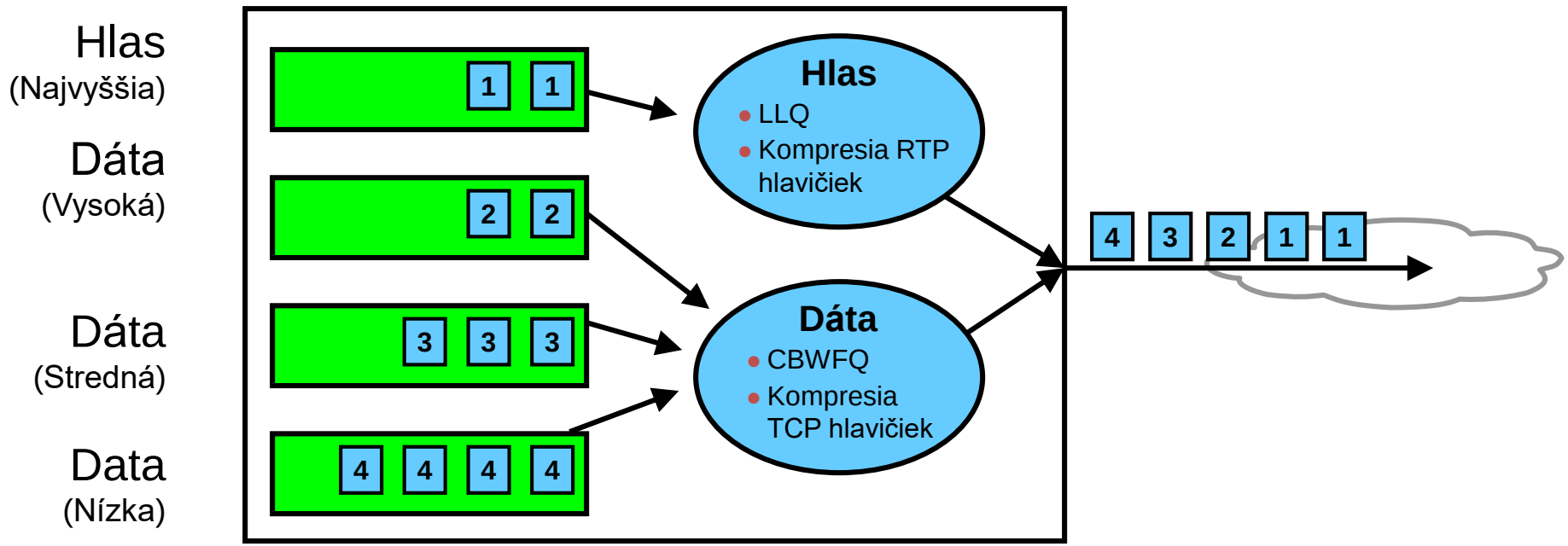
- Maximálna dostupná prenosová kapacita je kapacita najpomalšej linky
- O túto prenosovú kapacitu sa uchádzajú mnohé toky, čím môžu znížiť jej dostupnosť pre ktorúkoľvek individuálnu aplikáciu
- Prirodzene, nedostatok prenosovej kapacity má negatívny vplyv na aplikácie

Ako získať disponibilnú prenosovú kapacitu



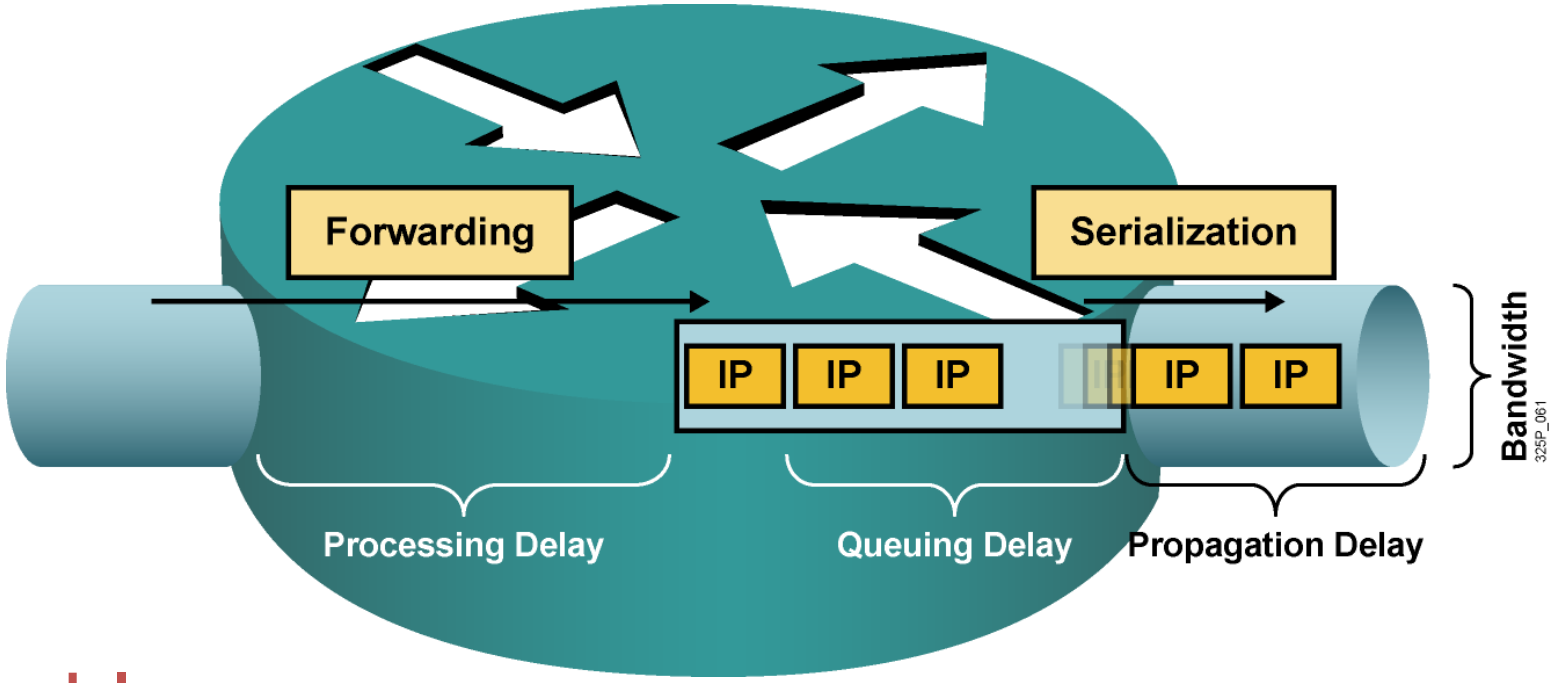
- Zrýchliť linku (najlepšie, ale aj najdrahšie riešenie)
- Využiť QoS prostriedky a dať prioritu dôležitým paketom (na úkor iných tokov)
- Komprimovať obsah rámcov (to však trvá istý čas)
- Komprimovať IP hlavičky (detto)

Efektívne využívanie prenosovej kapacity



- Pomocou frontových a kompresných mechanizmov je možné efektívejšie využívať dostupnú prenosovú kapacitu
  - Hlas: LLQ a kompresia RTP hlavičiek
  - Interaktívne toky: CBWFQ a kompresia TCP hlavičiek

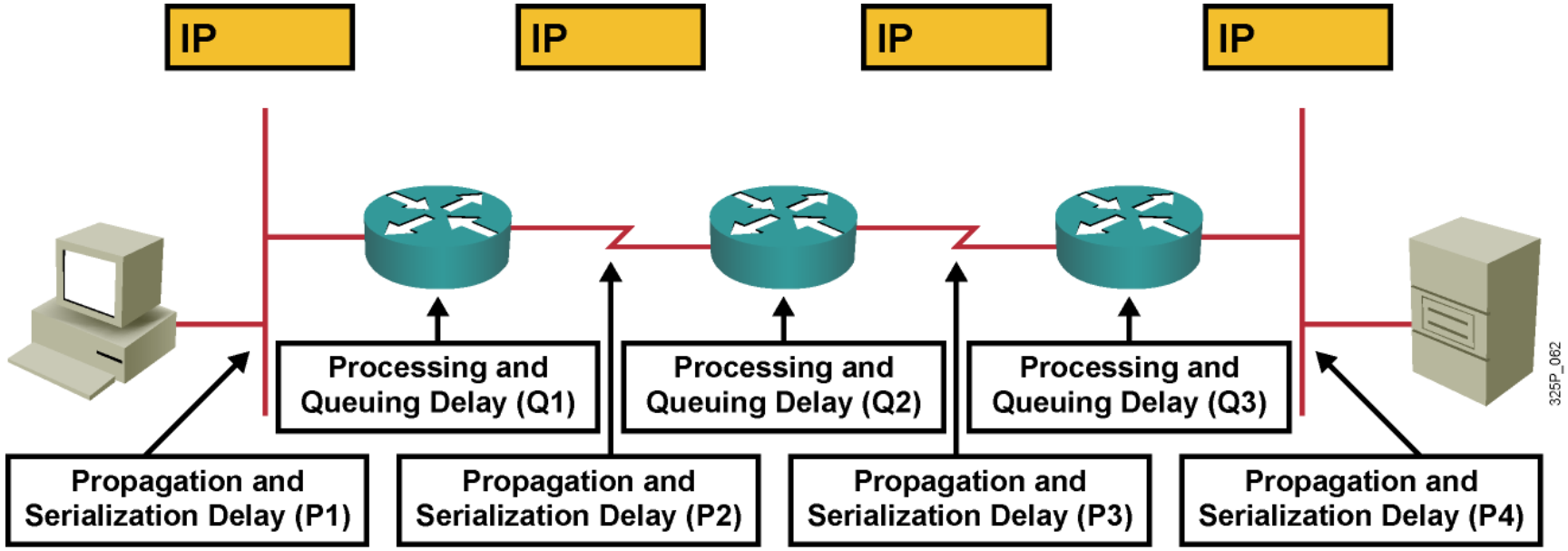
Druhy oneskorenia



- **Processing delay** (oneskorenie pri spracovaní):
  - Čas od prevzatia paketu zo vstupného rozhrania, jeho analýzy, cez smerovacie rozhodnutie až po jeho uloženie do výstupného frontu na výstupnom rozhraní
- **Queuing delay** (oneskorenie vo fronte):
  - Čas, ktorý paket strávi vo výstupnom fronte rozhrania
- **Serialization delay** (serializačné oneskorenie):
  - Čas, ktorý je potrebný na odoslanie paketu rozhraním danej prenosovej rýchlosti
- **Propagation delay** (oneskorenie pri šírení):
  - Čas, ktorý je potrebný na prechod signálu po danom fyzickom médiu

Od čoho závisia?

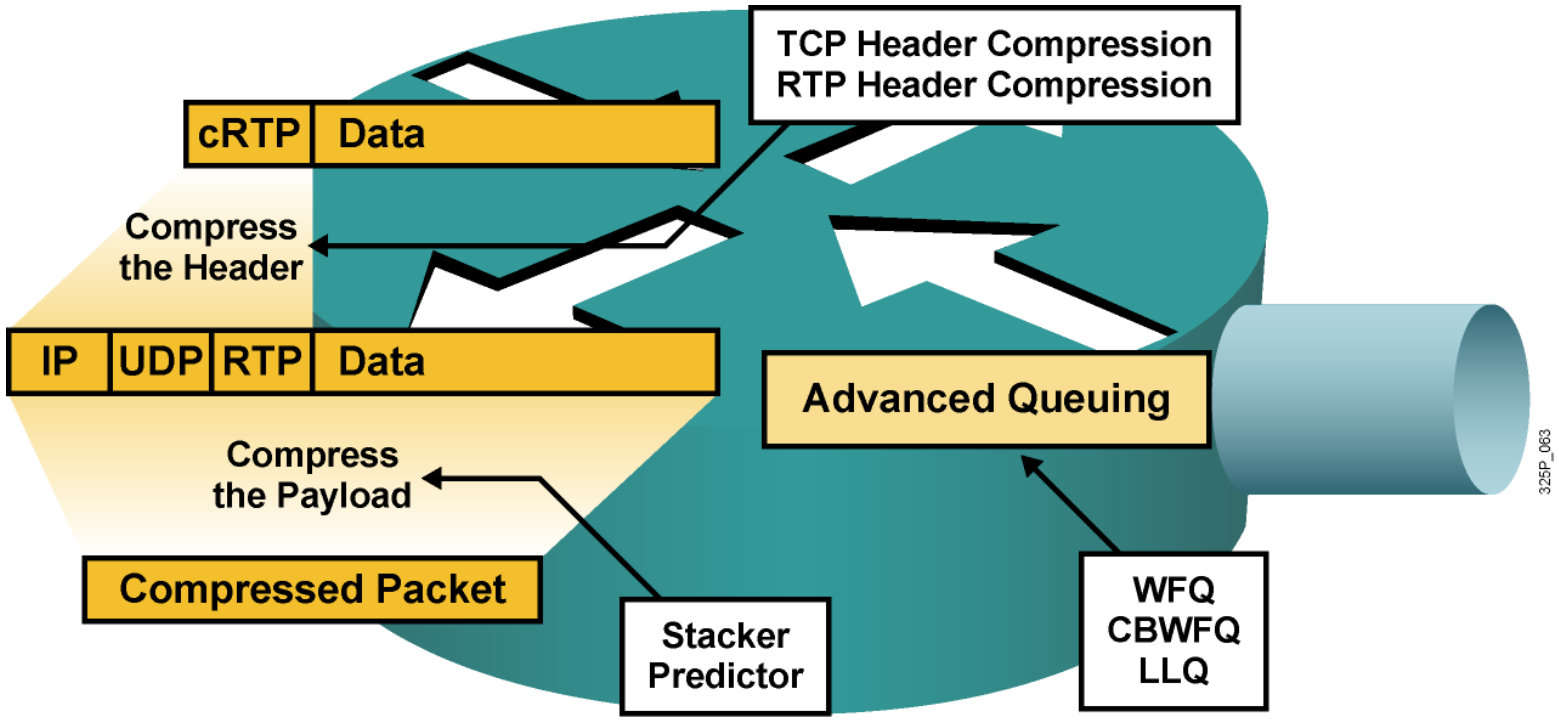
Dopad oneskorenia a jeho kolísania na kvalitu



Delay = P1 + Q1 + P2 + Q2 + P3 + Q3 + P4 = *x* ms

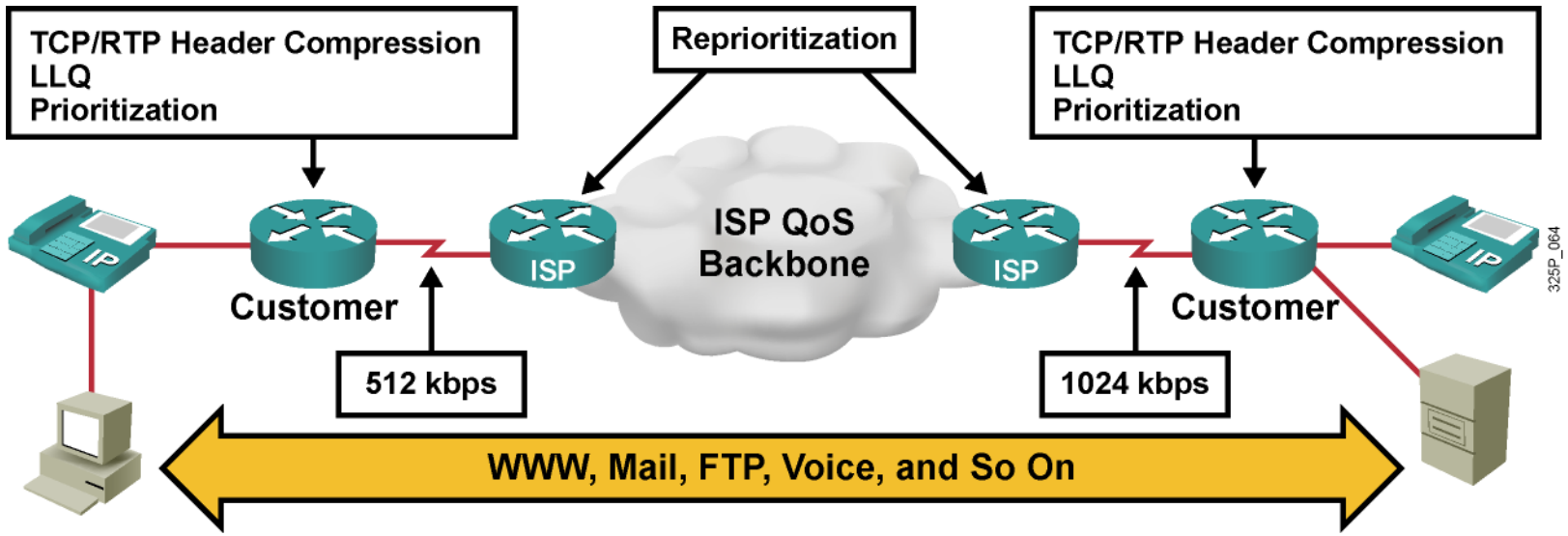
- Celkové oneskorenie: Súčet všetkých propagačných, procesných, serializačných a frontových oneskorení pozdĺž prenosovej trasy
- Ktoré oneskorenia sú v best-effort sieťach pevné a ktoré sú náhodné?
  - Pevné: propagačné a serializačné
  - Náhodné: procesné a frontové

Ako znížiť oneskorenie



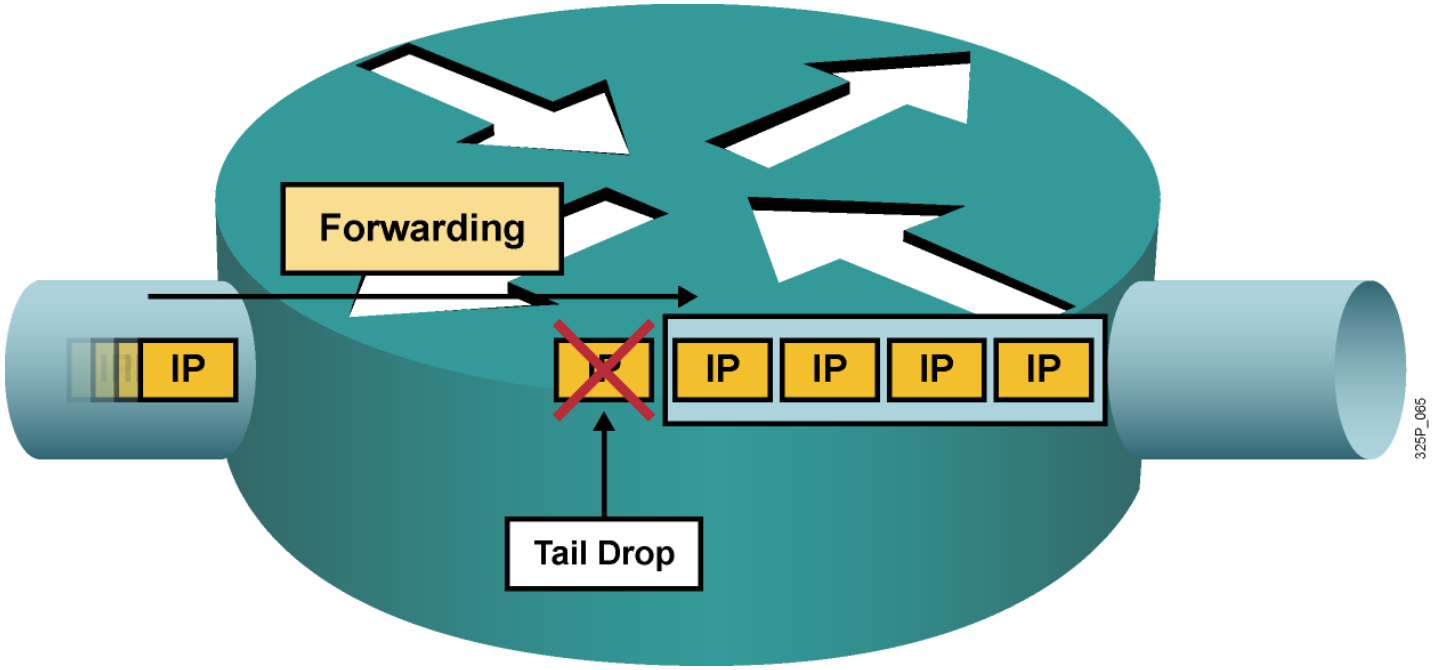
- Zrýchliť linku (najlepšie, ale aj najdrahšie riešenie)
- Dať prioritu dôležitým paketom
- Umožniť úpravu priority dôležitých paketov (reprioritizáciu)
- Komprimovať obsah rámcov (to však trvá istý čas)
- Komprimovať IP hlavičky (detto)

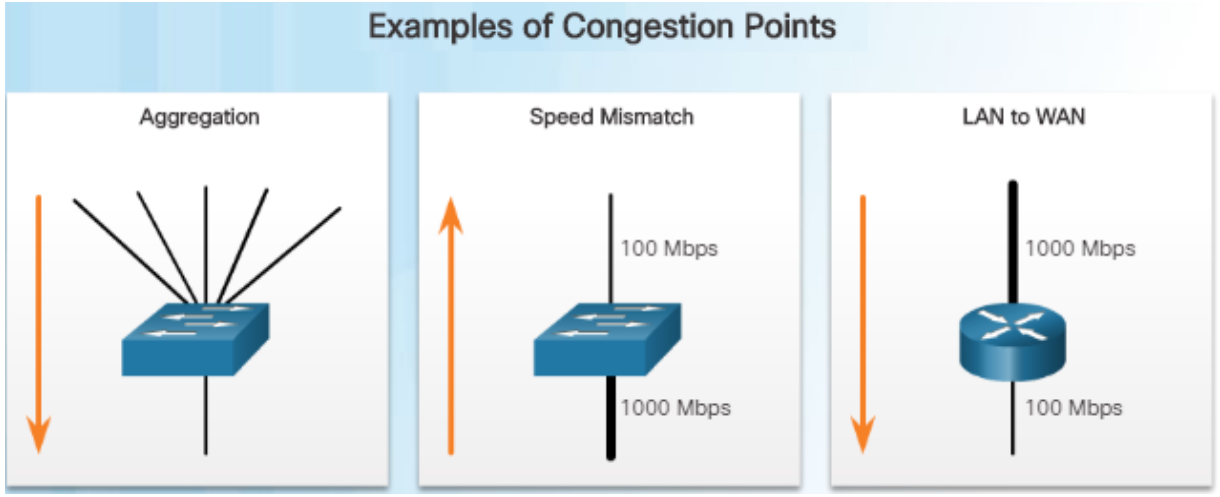
Znižovanie oneskorenia



- Zákaznícke smerovače realizujú:
  - Kompresiu TCP/RTP hlavičiek
  - LLQ (Low Latency Queueing)
  - Prioritizáciu
- Smerovače ISP realizujú:
  - Reprioritizáciu na základe dohodnutých QoS pravidiel

Druhy strát paketov



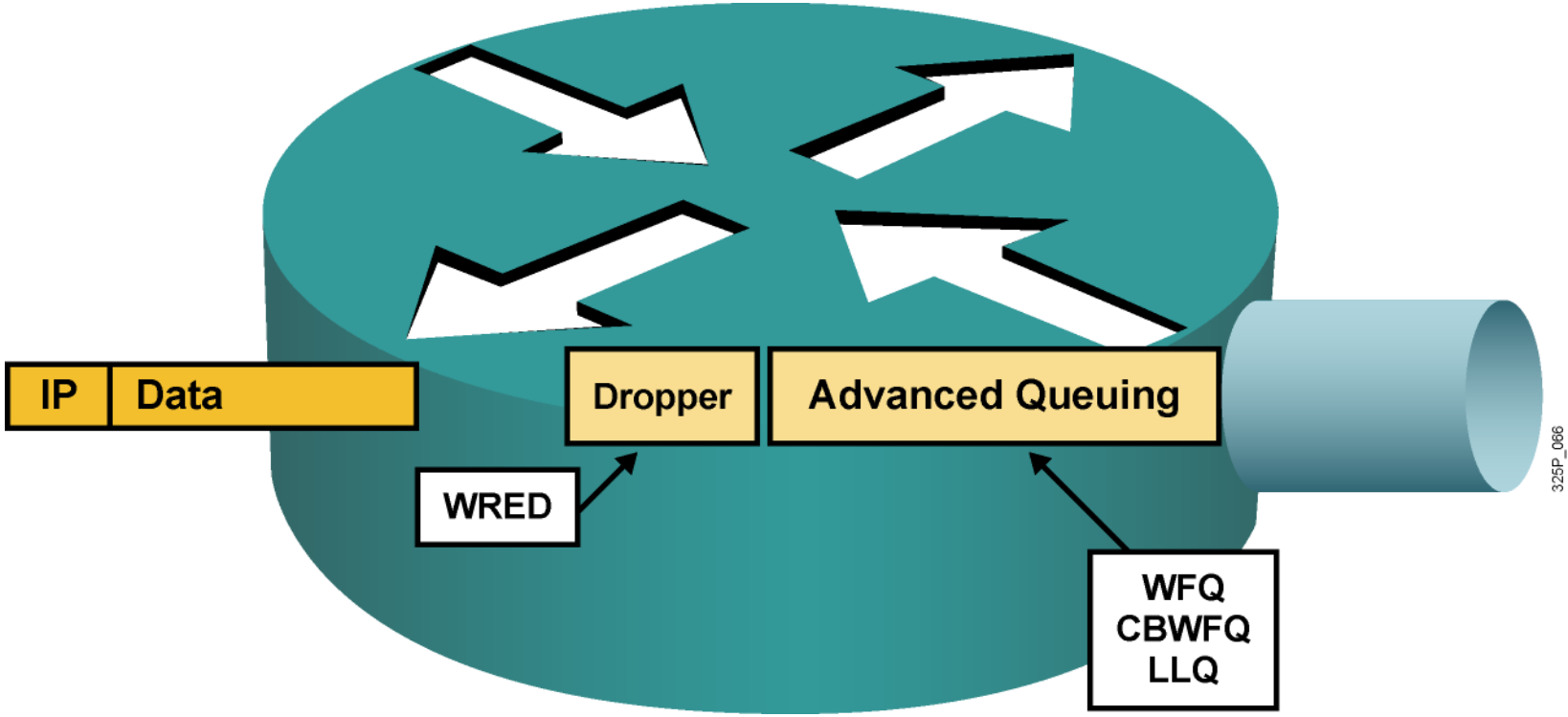


- Straty typu „tail drop“ nastávajú, keď je výstupný front plný.
  - bežné a nastávajú pri zahltení výstupného rozhrania
- Iné druhy strát sú obvykle spôsobené:
  - zahltením na vstupnom rozhraní
  - pomalým procesorom
  - chybami pri prenose.

Ktoré z nich sa dajú odstrániť upgradom hardvéru?

- Tie iné..

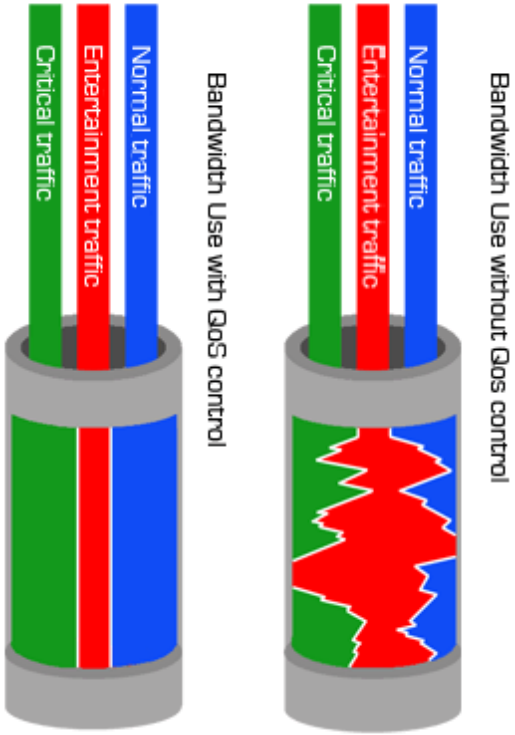
Predchádzanie stratám



- Zrýchliť linku (najlepšie, ale aj najdrahšie riešenie)
- Garantovať dostatočné pásmo pre citlivé pakety
- Predchádzať zahlteniu náhodným zahadzovaním menej dôležitých paketov ešte skôr, než dôjde k zahlteniu

Nástroje pre poskytovanie QoS

- Klasifikácia
  - Identifikácia toku alebo triedy prevádzky
- Značkovanie (Marking)
  - Vyznačenie identifikovaného toku alebo triedy prevádzky
- Predchádzanie zahlteniu (Congestion Avoidance)
  - Tail Drop, Random Early Detection, Weighted RED
- Riešenie zahltenia (Congestion Management)
  - Plánovacie mechanizmy pre obsluhu frontov
- Tvarovanie a obmedzovanie prevádzky (Shaping, Policing)
- Mechanizmy efektívnosti linky (Link Efficiency Mechanisms)
  - Link Fragmentation and Interleaving
  - On-the-fly kompresia hlavičiek alebo tiel paketov



Ako QoS nástroje pracujú?

Klasifikácia a značkovanie

Ukladanie do frontov (Selektívne) zahadzovanie

Činnosti po uložení do frontu

IDENTIFY & PRIORITIZE

MANAGE & SORT

PROCESS & SEND

Modely poskytovania QoS

Modely poskytovania kvality služby

Model	Popis
Best effort	Bez riadenia kvality služby. Vhodné, ak nie je dôležité, kedy alebo v akom poradí budú pakety doručené.
Integrated Services (IntServ)	Aplikácie oznamujú sieti, aké QoS parametre požadujú pre ich správnu činnosť.
Differentiated Services (DiffServ)	Sieť rozoznáva triedy prevádzky, ktoré vyžadujú osobitné QoS parametre.

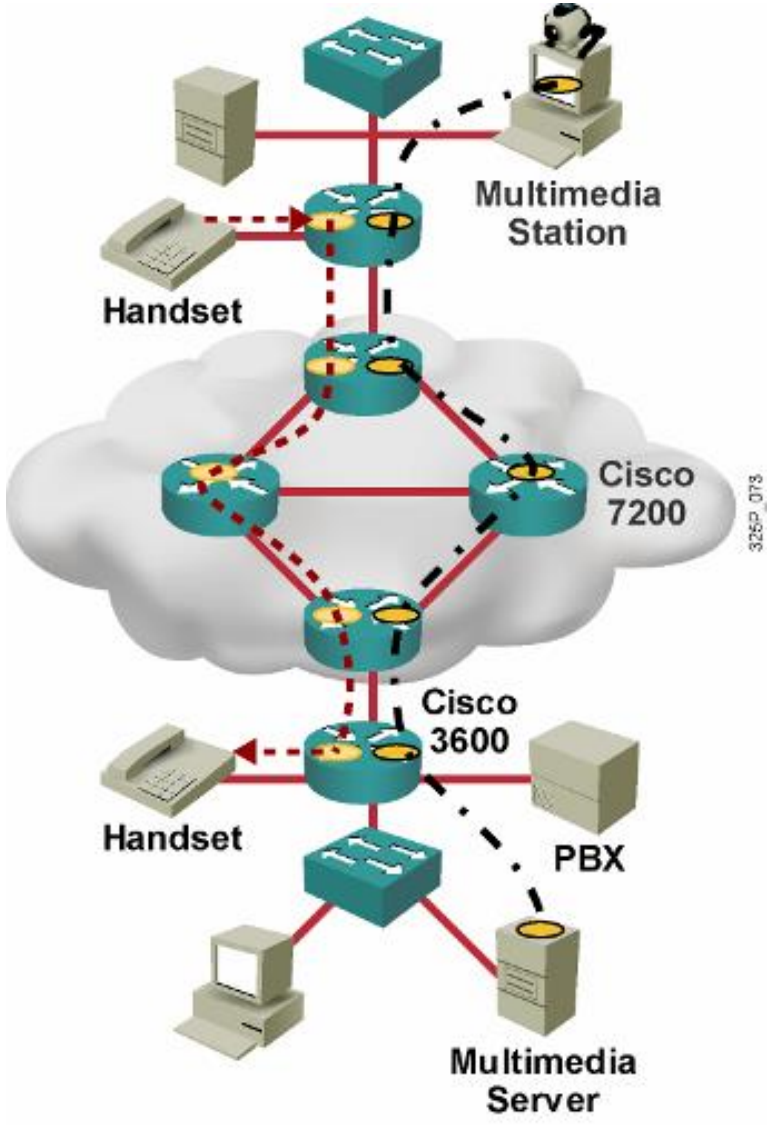
Model Best-Effort

- Model best-effort je pôvodným modelom, na ktorom bol Internet založený
- Medzi tokmi dát nie je nijaká diferenciácia
  - Doručovanie sa podobá obyčajnej poštovej zásielke
  - Paket „príde vtedy, keď príde“

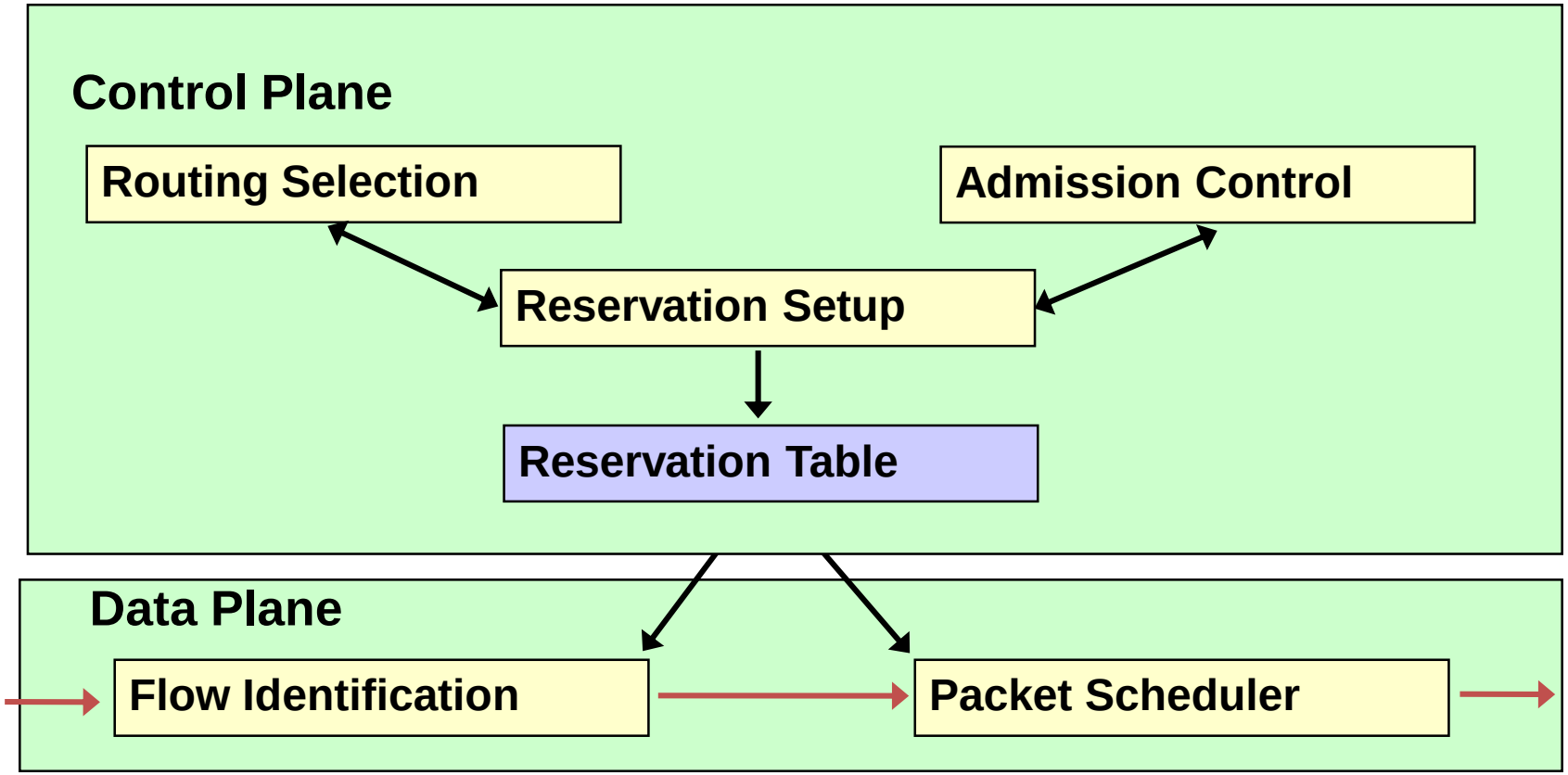
- Výhody:
  - Vynikajúca škálovateľnosť
  - Nie je potrebný nijaký osobitný mechanizmus
- Nevýhody:
  - Neposkytuje garancie služby
  - Nediferencuje medzi službami

Model Integrated Services (IntServ)

- Poskytuje garantované doručenie a predikovateľné správanie sa siete voči aplikáciám
- Poskytuje viaceré úrovne služieb
- Kľúčovým podporným protokolom je RSVP na signalizáciu QoS požiadaviek pre jednotlivé toky
- QoS parametre sa vzťahujú na jednotlivé toky medzi jednotlivými uzlami a aplikáciami
- Ak sieť nie je schopná splniť požiadavku aplikácie na QoS parametre, bude o tom aplikáciu informovať
- Potrebné sú inteligentné frontové mechamizmy na poskytovanie rezervácie zdrojov:
  - Garantovaná rýchlosť
  - Riadená záťaž (nízke oneskorenie, vysoká priepustnosť)



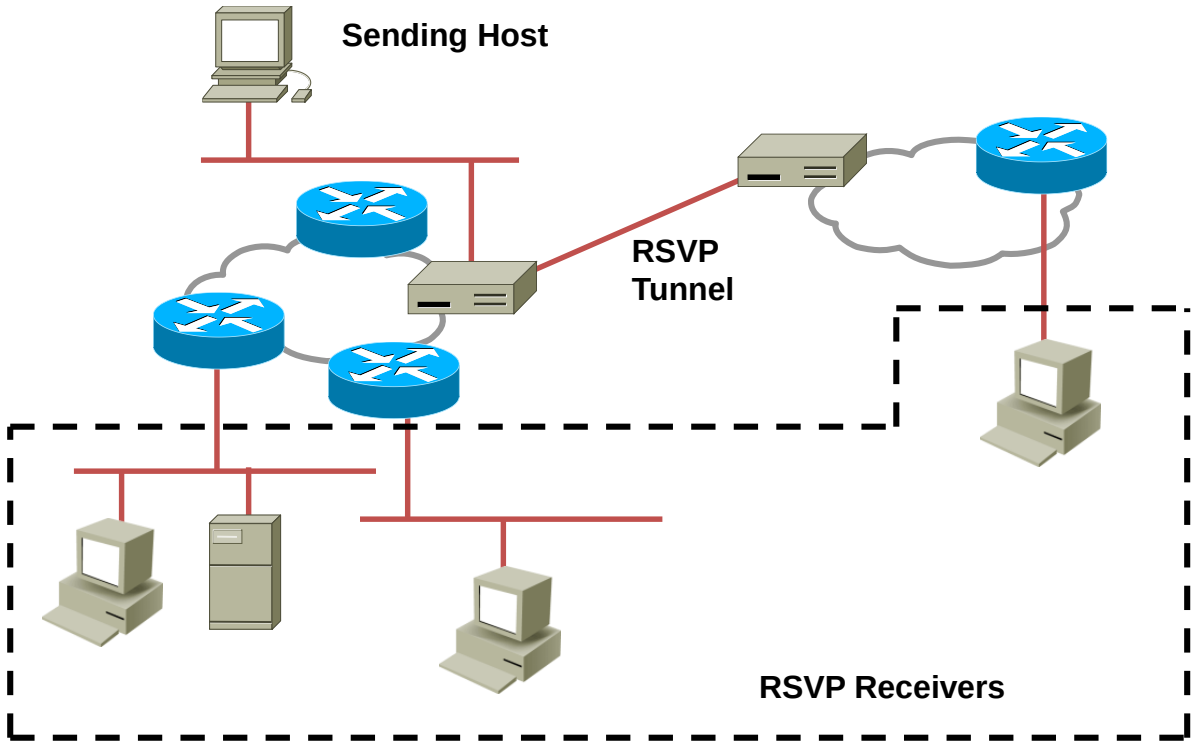
Procesy a architektúra smerovača v IntServ



Resource Reservation Protocol (RSVP)

- Prenáša sa v IP – číslo protokolu 46
- Môže využiť aj TCP/UDP port 3455
- Jedná sa o signalizačný protokol
  a spolupracuje so smerovacími protokolmi
- Slúži na rezerváciu QoS prostriedkov na všetkých zariadeniach medzi odosielateľom a príjemcom

- Zabezpečuje prostriedky pre rôznorodé multimediálne aplikácie
  - Premávka citlivá na prenosové pásmo
  - Premávka citlivá na oneskorenie



Výhody a nevýhody modelu IntServ

Výhody:

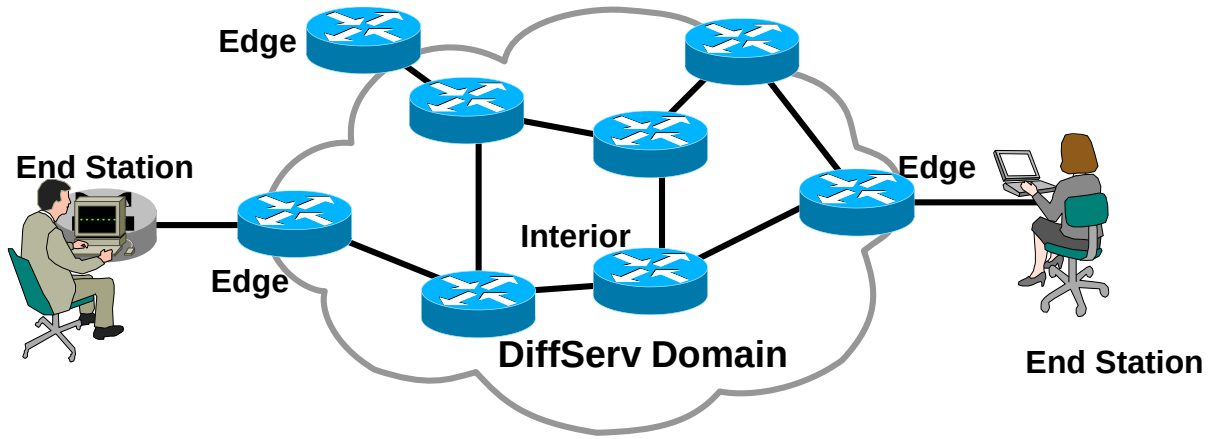
- Explicitné riadenie prístupu k zdrojom (end to end)
- Veľmi vysoká granularita prideľovania QoS prostriedkov
- Riadenie prístupu k prostriedkom na každú žiadosť individuálne
- Signalizácia dynamických čísel portov (napr pre H.323)

Nevýhody:

- Potreba trvalej signalizácie vzhľadom na stavovú architektúru
- Tokovo orientovaný prístup nie je škálovateľné na siete veľkého rozsahu, ako napr. Internet

Model Differentiated Services

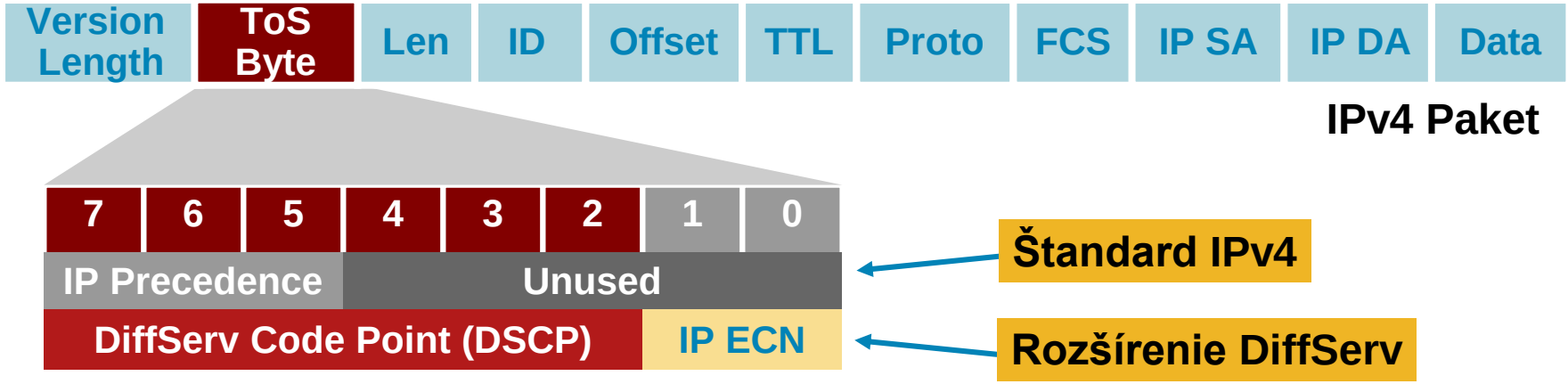
- Za cenu istých kompromisov rieši mnohé obmedzenia modelov Best-Effort a IntServ
- Na rozdiel od signalizovaných tvrdých požiadaviek na QoS využíva **dopredu pripravené QoS** prostriedky a politiky
- Toky triedi do tzv. agregátov (**tried**) a poskytuje QoS prostriedky celým triedam
- Minimalizuje signalizáciu (žiadna) a stavovú informáciu (minimálna) na sieťových uzloch
- QoS parametre charakterizuje popisom tzv. Per-Hop Behavior (**PHB**)
- Úroveň služby sa stanovuje na triedu prevádzky, nie na individuálne toky



Model Differentiated Services (DiffServ)

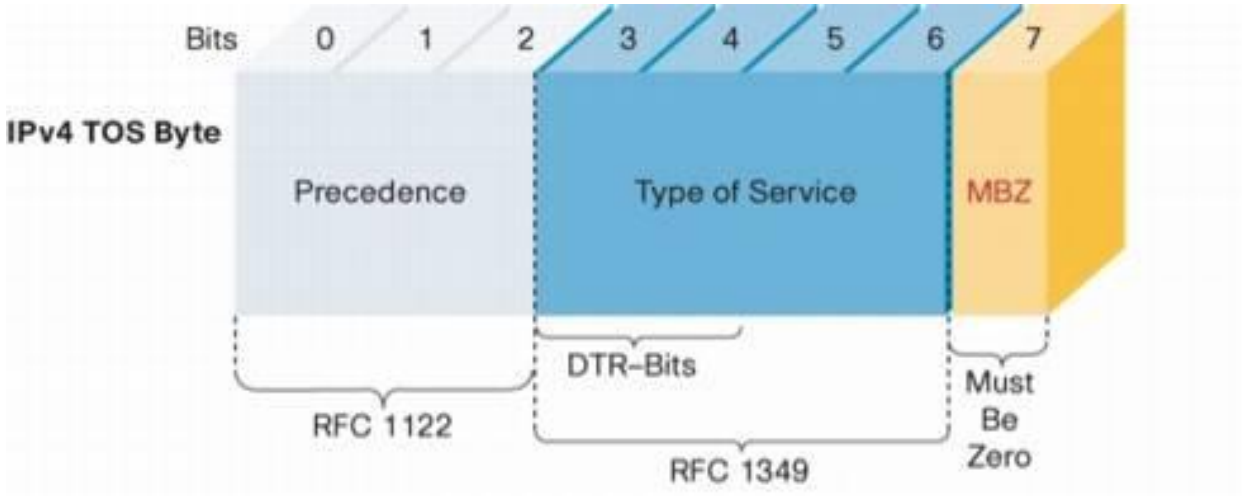
- Model DiffServ sa zaoberá poskytovaním QoS nad **triedami** prevádzky, nie nad jednotlivými tokmi
- Komplexná klasifikácia, značkovanie a vstupné úpravy prevádzky sa realizujú na **okraji** siete
  - Vo vnútri siete sa QoS pravidlá riadia už iba pridelenými značkami
- Vo vnútri siete sa neudržiavajú informácie o jednotlivých tokoch, udržiavajú sa len informácie o **spôsobe obsluhy** jednotlivých tried prevádzky
- **Cieľom** DiffServ je
  - Škálovateľnosť
  - Spolupráca s uzlami, ktoré ešte nepodporujú DiffServ
  - Možnosť postupného nasadzovania

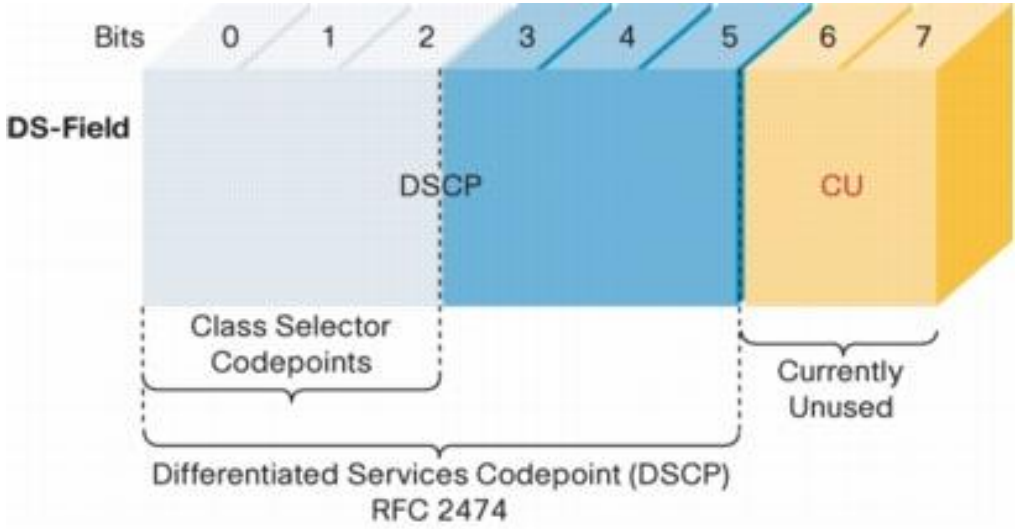
Klasifikačné nástroje IP Precedence a DiffServ Code Point



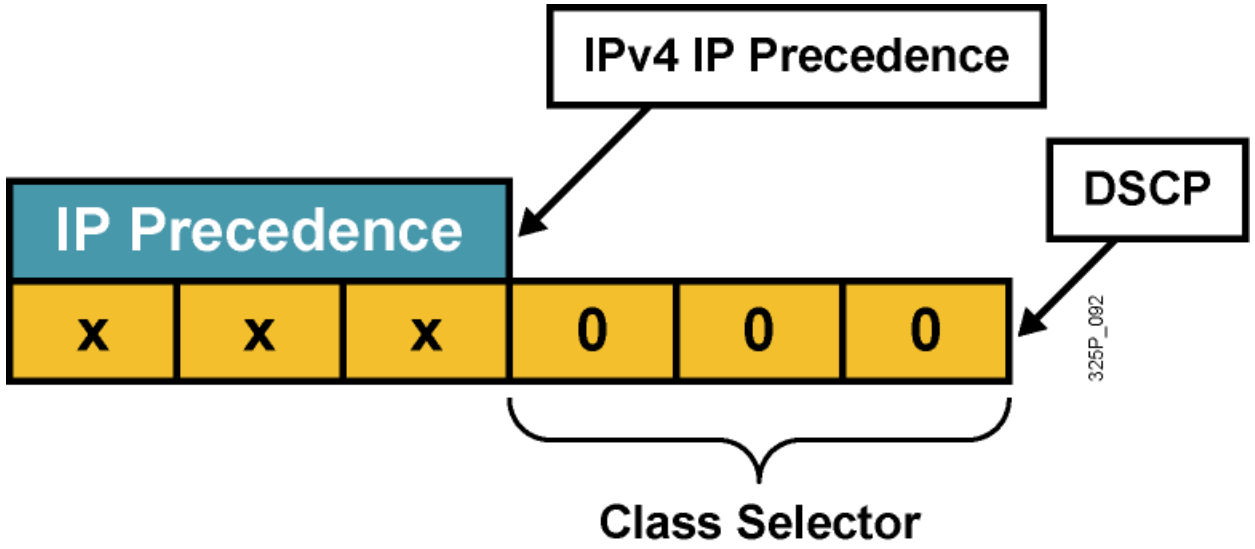
- IPv4: tri najvyššie bity ToS bajtu sa nazývajú **IP Precedence** (IPP). Ostatné bity boli niekoľkokrát predefinované (Delay, Throughput, Reliability, Monetary cost)
- DiffServ: šesť najvyšších bitov ToS bajtu sa nazývajú DiffServ Code Point (DSCP). Zvyšné dva bity sa využívajú na explicitnú informáciu o zahltení (ECN). Hodnota DSCP poľa sa nazýva **codepoint**
- Hodnoty DSCP sú spätne **kompatibilné** s hodnotami IP Precedence

IP ToS a DS pole v IP hlavičke



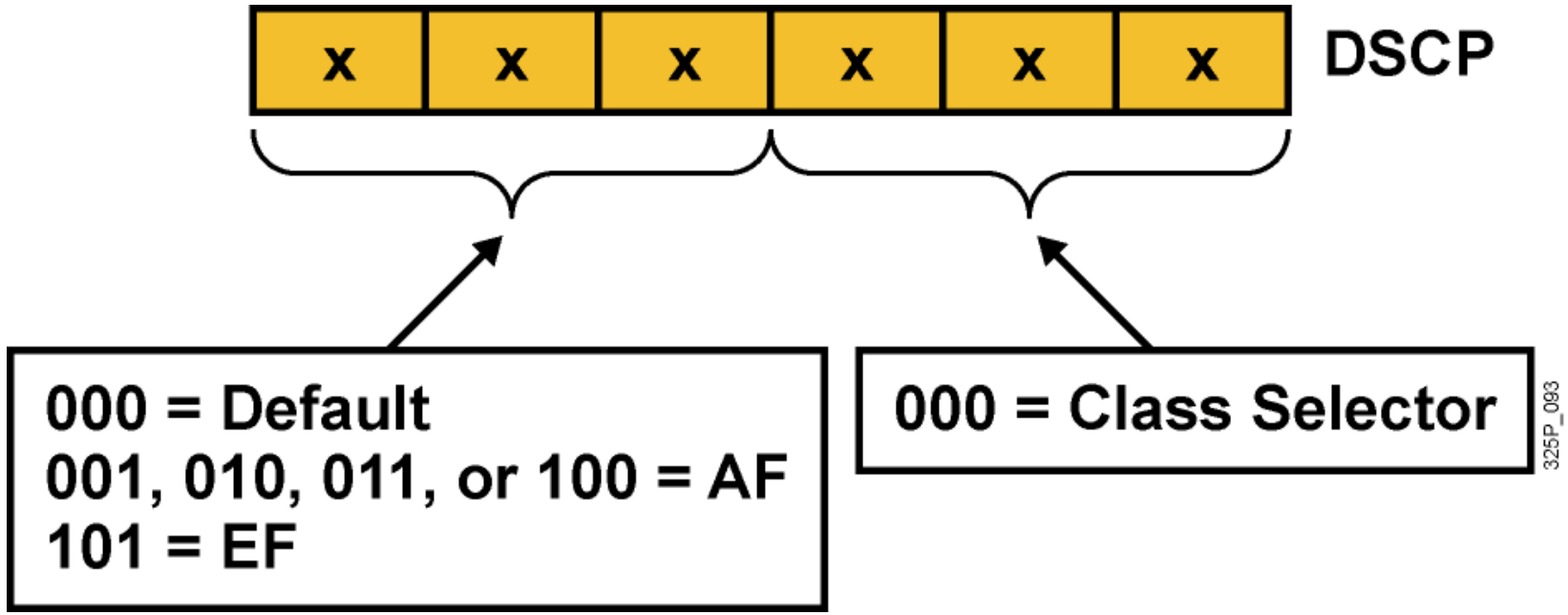


Kompatibilita IP Precedence a DSCP



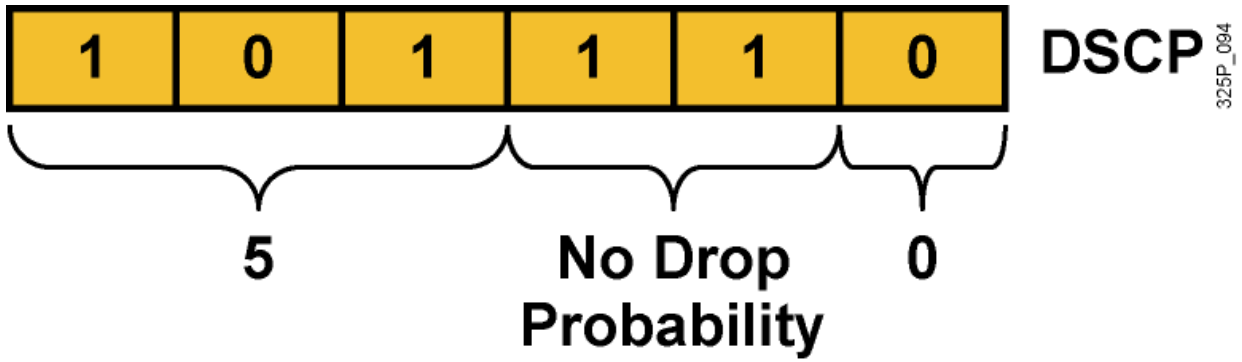
- Pre zachovanie kompatibility s IP Precedence (RFC 1812) boli zavedené tzv. **Class Selector codepoints** v tvare xyz000 s názvom **CS0** až **CS7**
- Odlišuje pravdepodobnosť včasného vybavenia paketu:
  - P(xyz000) >= P(abc000), ak xyz >= abc
- Napríklad, ak má paket DSCP codepoint 011000 (CS3), má väčšiu pravdepodobnosť včasného odoslania než paket s DSCP 001000 (CS1)

Per-Hop Behavior – PHB



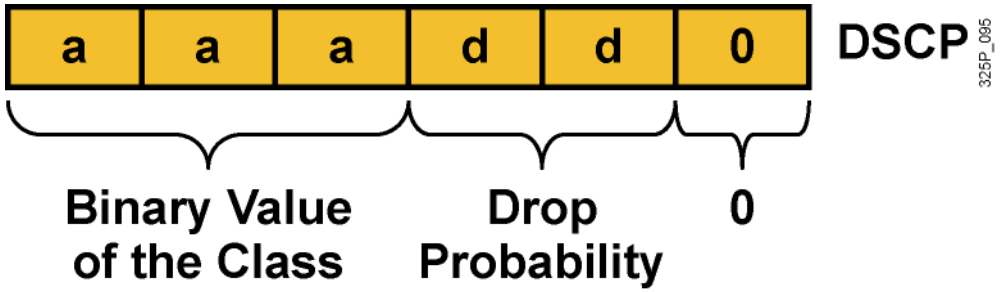
- PHB je spôsob obsluhy konkrétnej triedy prevádzky na danom uzle
- DSCP vlastne vyberá PHB pozdĺž siete
  - Default PHB (FIFO, tail drop)
  - Class-selector PHB (IP precedence)
  - EF PHB (Expedited Forwarding)
  - AF PHB (Assured Forwarding)

Expedited Forwarding (EF) PHB



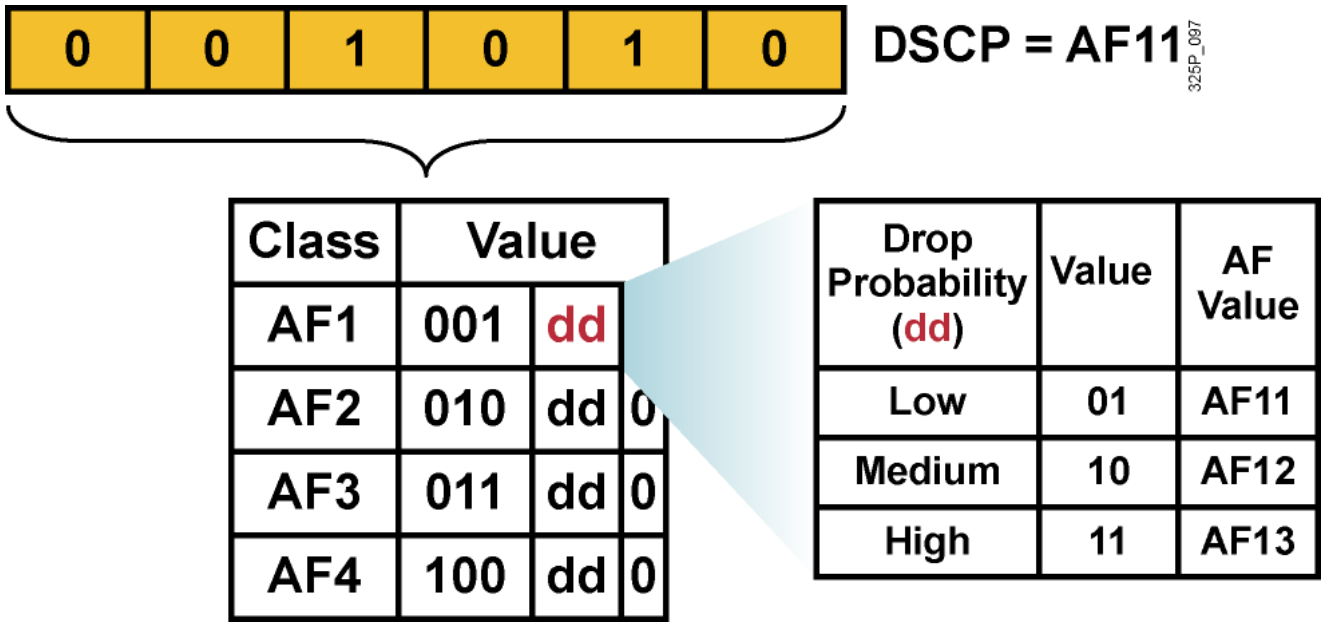
- EF PHB:
  - Garantuje tzv. minimum departure rate – právo prednostného odoslania
  - Garantuje prenosové pásmo vyhradené pre triedu prevádzky s EF
  - Limituje pásmo pomocou policingu – trieda s EF nemôže prekročiť garantované pridelené pásmo
- DSCP codepoint 101110 (46): Pre zariadenia podporujúce len IPprecedence je to precedencia 5:
  - Bity 5 až 7: 101 = 5 (rovnaké 3 bity použité pre IP Precedence)
  - Bity 3 a 4: 11 = Bez strát (low delay, high throughput)
  - Bit 2: Nastavený na 0

Assured Forwarding (AF) PHB



- AF PHB:
  - Garantuje isté minimálne prenosové pásmo
  - Umožňuje využiť aj väčie pásmo, ak je momentálne k dispozícii
- Štyri základné kategórie: AF1, AF2, AF3 a AF4
- DSCP codepoint má tvar aaadd0:
  - aaa je binárne číslo triedy (1, 2, 3 alebo 4)
  - dd je pravdepodobnosť zahodenia

Hodnoty AF PHB

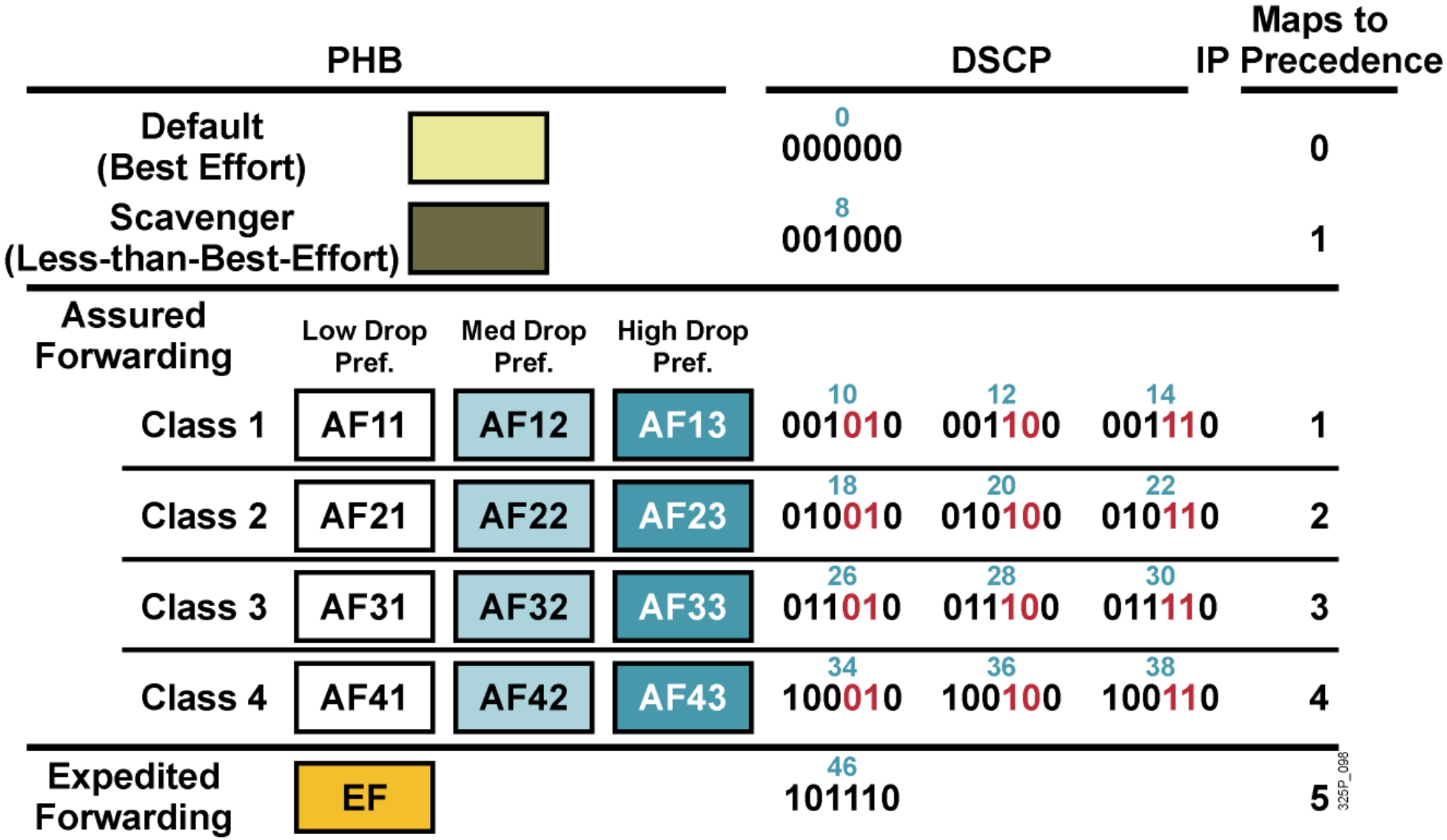


- Každá AF trieda využíva **3** DSCP hodnoty
- Každá AF trieda sa preposiela **nezávisle** od ostatných so svojou garantovanou šírkou pásma

- Aby sa predišlo zahlteniu, v každej triede sa používajú techniky predchádzania zahlteniu – Weighted RED (WRED)
- Ak je daná trieda AFxy, dekadickú hodnotu DSCP vypočítame ako?

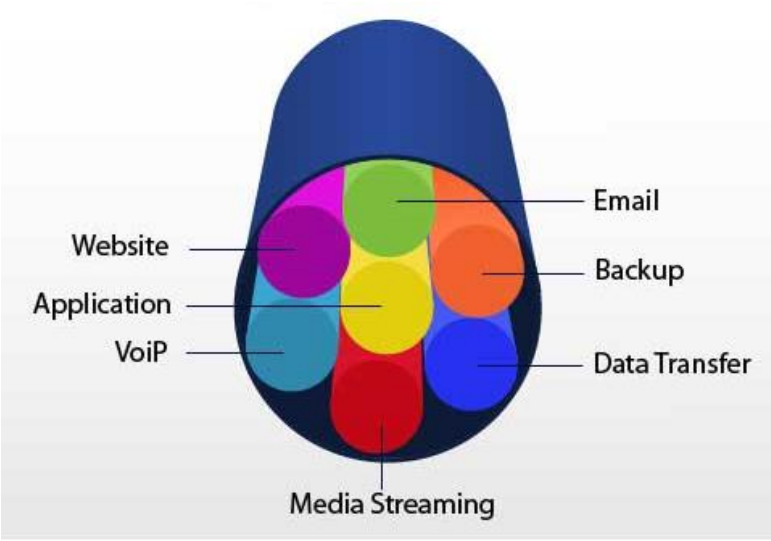
8x+2y

Štandardné PHB skupiny (definované v RFCs)

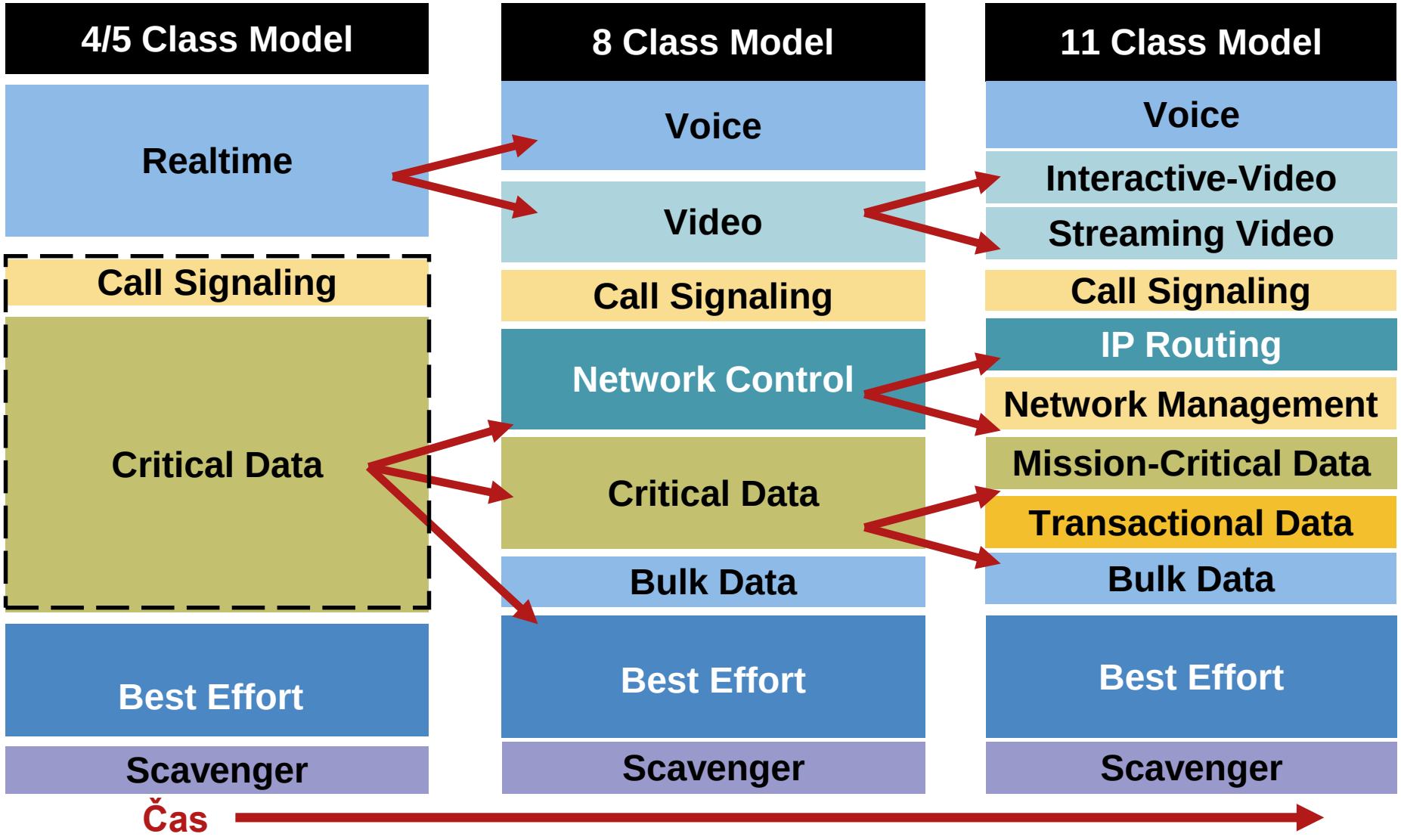


Vytváranie obslužných tried

- Obslužné triedy sú typy prevádzky, ktoré budú vybavované rovnakým spôsobom (dostanú rovnakú QoS obsluhu)
- Nie je vhodné vytvárať priveľa tried. Pre dátovú prevádzku obvykle stačí najviac 4-5 tried:
  - Hlasové aplikácie: VoIP
  - Mission-critical aplikácie: Oracle, SAP, SNA
  - Interaktívne aplikácie: Telnet, TN3270
  - Veľkoobjemové aplikácie: FTP, TFTP
  - Best-effort aplikácie: E-mail, web
  - Ostatné „smeti“: Kazaa, Yahoo, RapidShare
- Do mission-critical a transakčných tried nezaraďovať viac ako tri aplikácie
- Uprednostniť proaktívne pravidlá (WRED) pred reaktívnymi (policing)
- Pred nasadením QoS pravidiel si nechať odsúhlasiť rozdelenie prevádzky na jednotlivé priority a ich pomery od vedenia spoločnosti



Koľko tried treba?

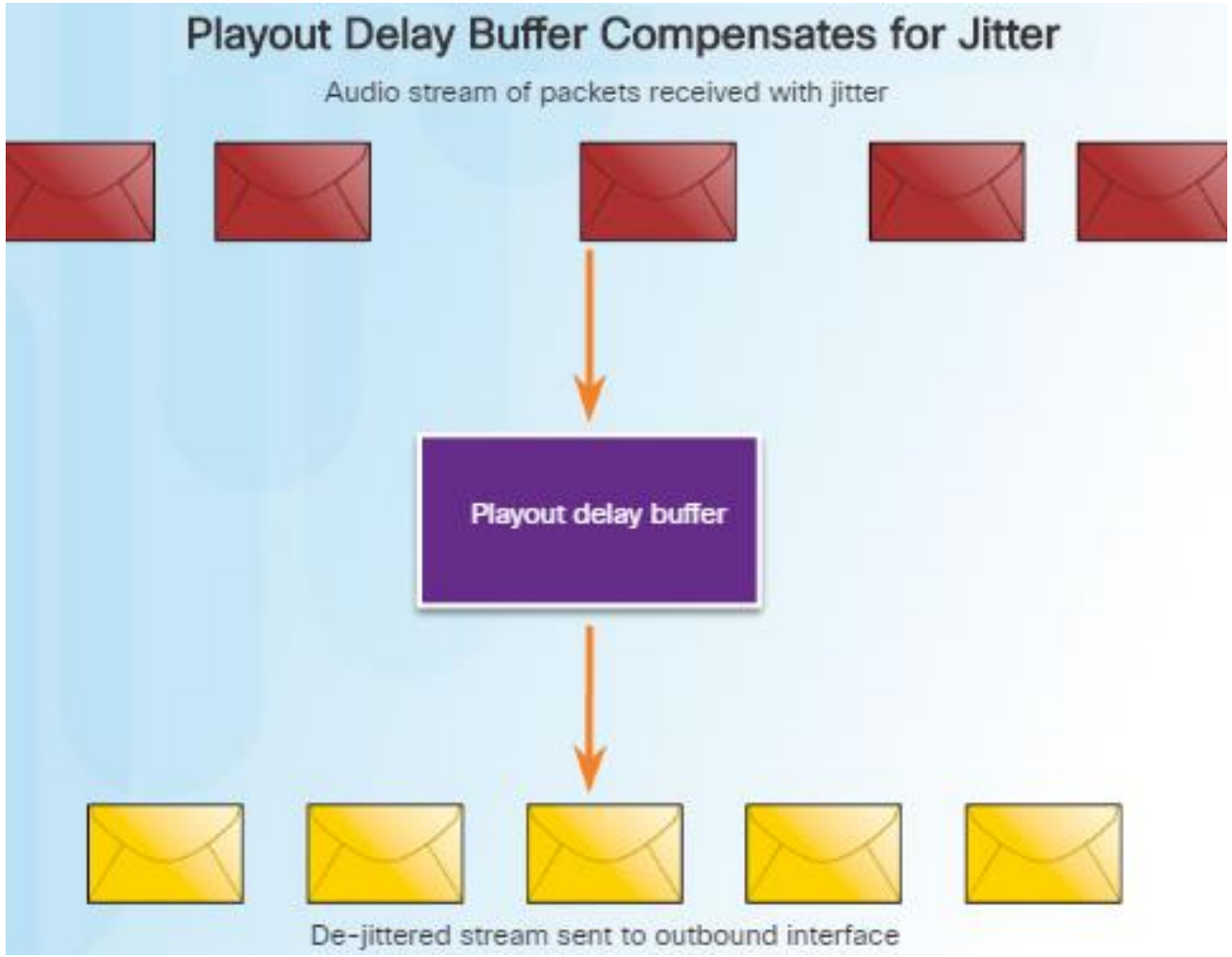


Odporúčania pre QoS Baseline Marking

Application	L3 Classification			L2
	IPP	PHB	DSCP	CoS
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31*	26	3
Call Signaling	3	CS3*	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Best Effort	0	0	0	0
Scavenger	1	CS1	8	1

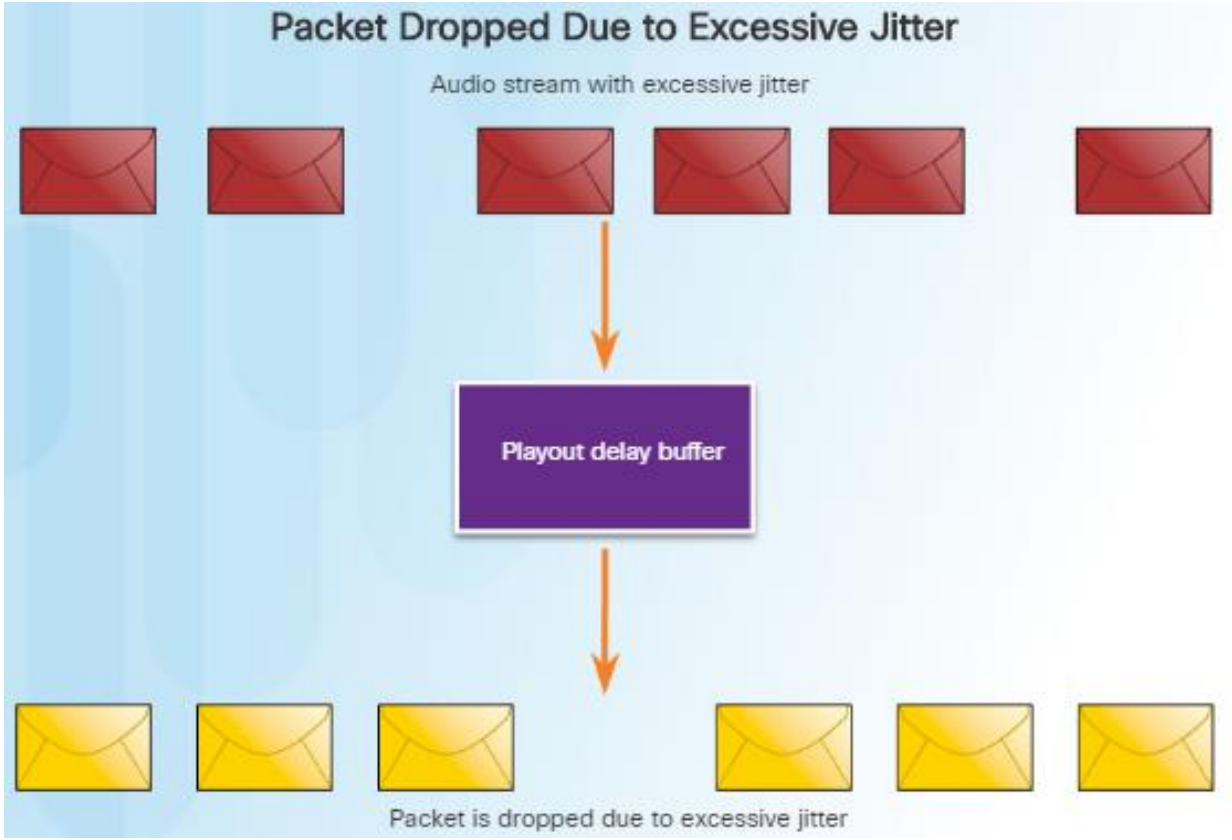
Packet Loss

- Čo bez QoS mechanizmov
  - Pakety sa spracujú ako prídu
  - Pri zahltení -> straty paketov
    - Problém pre video a audio pakety citlivé na oneskorenie
  - Napr. na smerovač príde VoIP tok, musí kompenzovať jitter
    - Použije „playout delay buffer„
      - Odkladá ich do buffra, a následne posiela s konštatnými medzerami



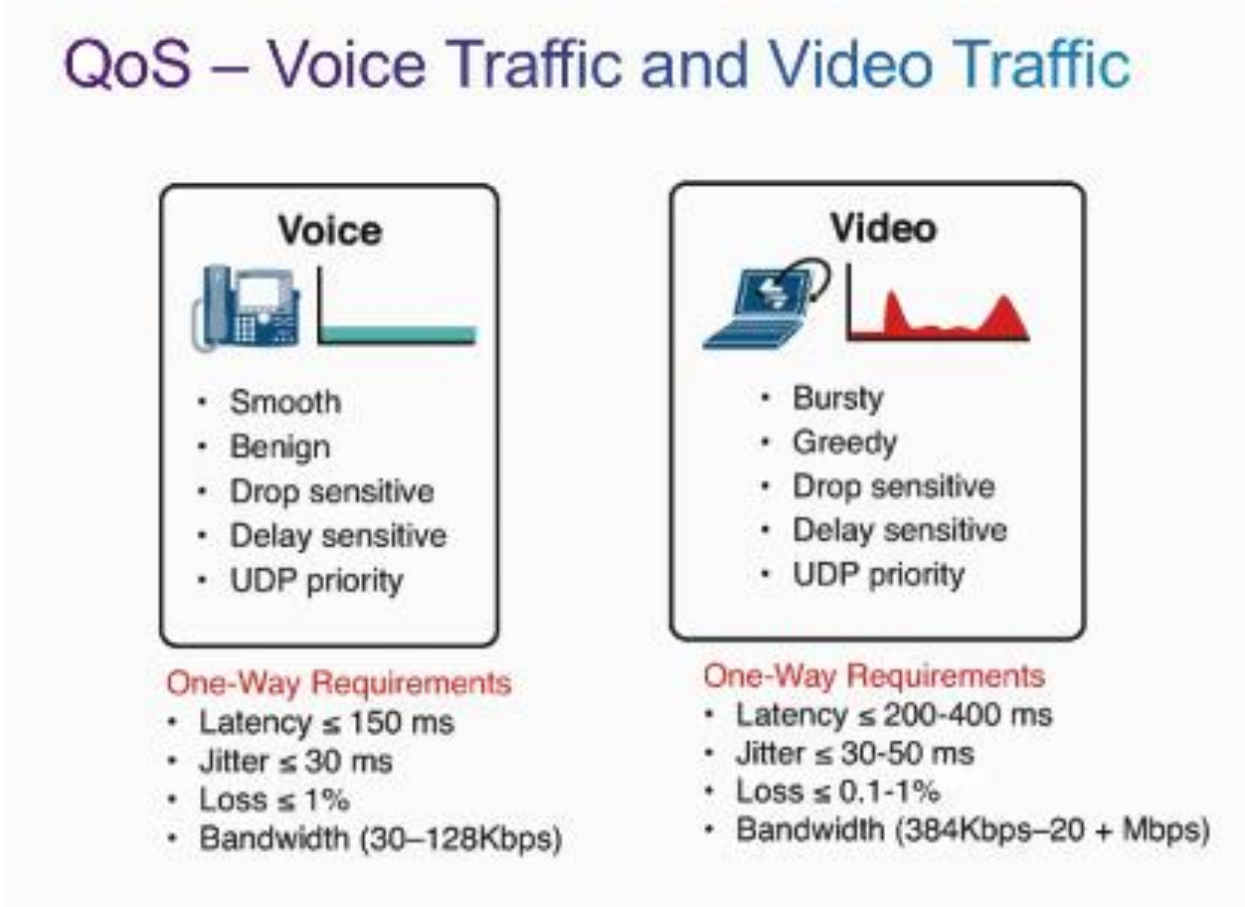
Packet Loss

- If the jitter is so large that it causes packets to be received out of the range of this buffer, the out-of-range packets are discarded and dropouts are heard in the audio.
- For losses as small as one packet, the digital signal processor (DSP) interpolates what it thinks the audio should be and no problem is audible to the user.
- However, when jitter exceeds what the DSP can handle, audio problems are heard.
- In a properly designed network, voice packet loss should be zero
- Network engineers use QoS mechanisms to classify voice packets for zero packet loss.



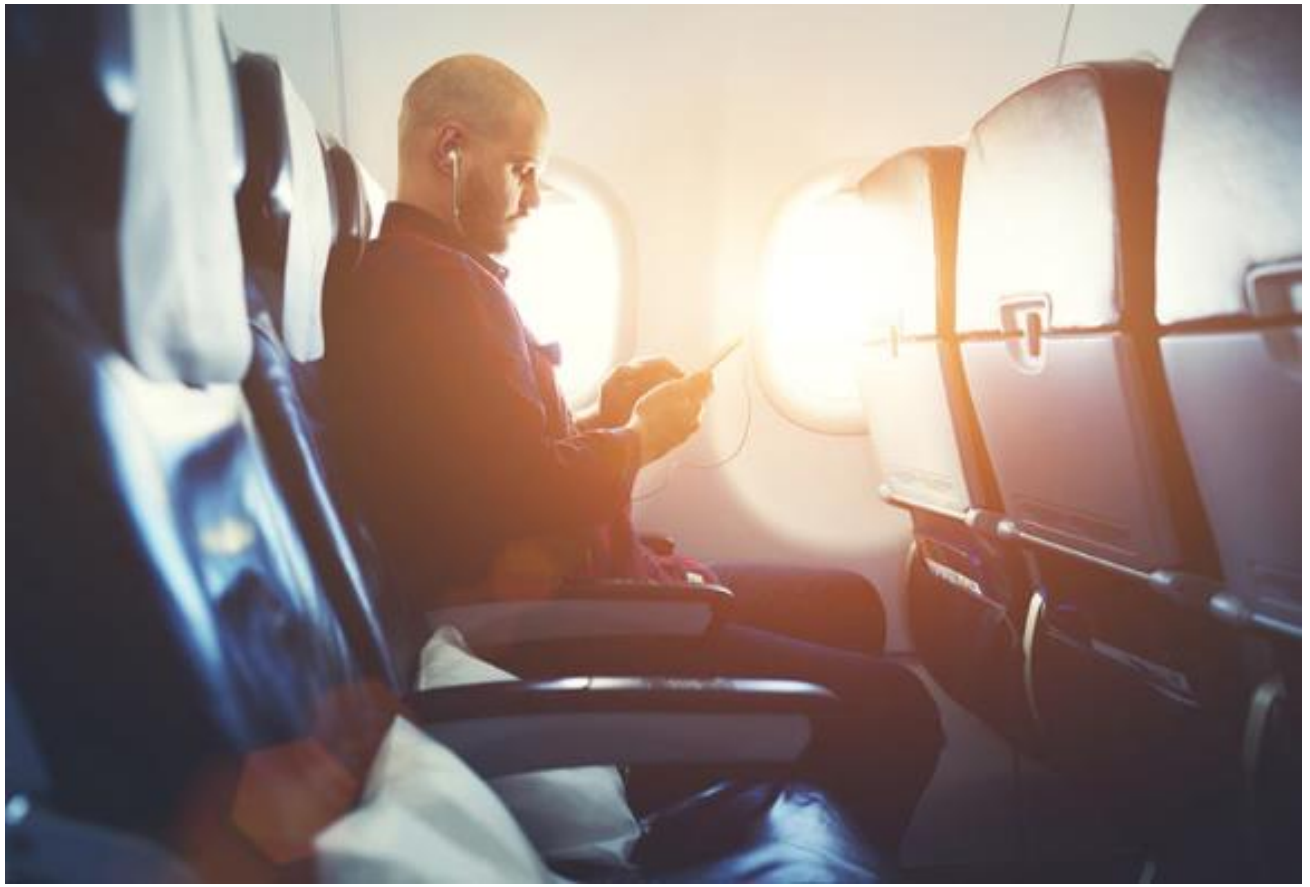
Video Tutorial – Traffic Characteristics

- Voice and video traffic place a greater demand on the network and are two of the main reasons for QoS.
- There are some differences between voice and video:
  - Voice packets do not consume a lot of resources because they are not very large and they are fairly steady. Voice traffic requires at least 30 kilobits per second of bandwidth with no more than 1% packet loss.
  - Video traffic is more demanding. The packets are more bursty and greedy. It consumes a lot more resources. Video traffic requires at least 384 kilobits per second in bandwidth with no more than 0.1 to 1% packet loss.



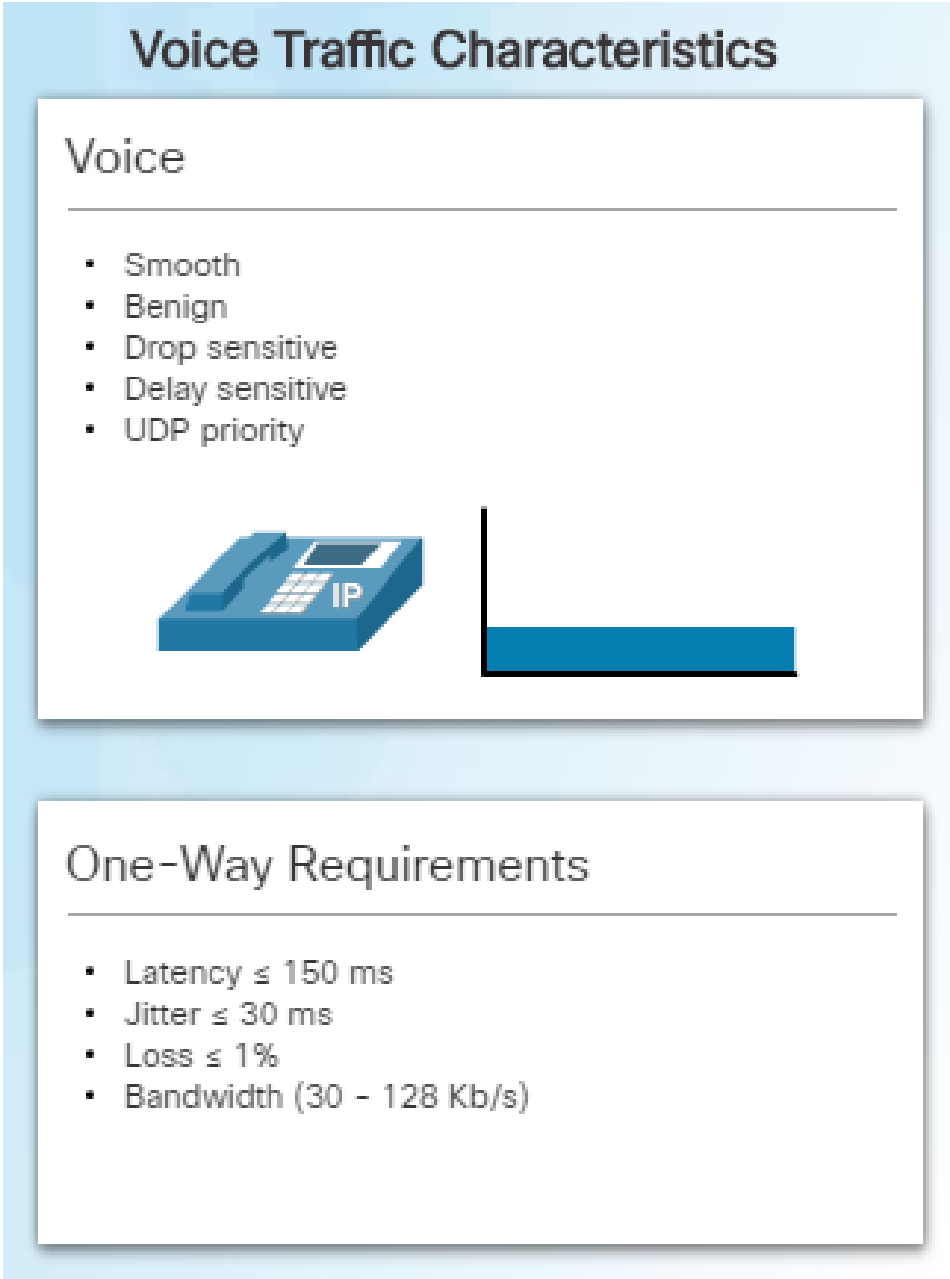
Network Traffic Trends

- In the early 2000s, the predominant types of IP traffic were voice and data.
- Voice traffic has a predictable bandwidth need and known packet arrival times.
- Data traffic is not real-time and has an unpredictable bandwidth need.
- More recently, video traffic has become increasingly important to business communications and operations.
- According to the Cisco Visual Networking Index (VNI), video traffic represented 67% of all traffic in 2014. By 2019, video will represent 80% of all traffic.
- The type of demands that voice, video, and data traffic place on the network are very different.



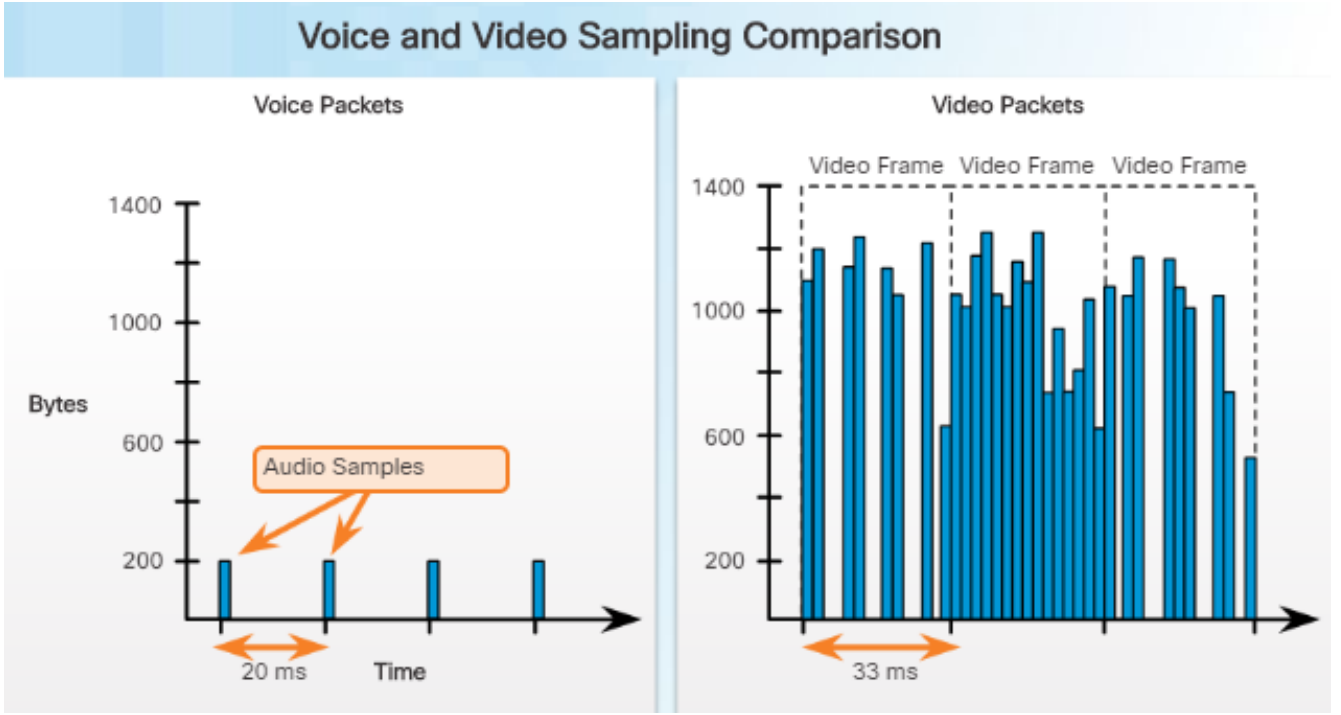
Voice

- Voice traffic is predictable and smooth.
- However, voice traffic is very sensitive to delay and dropped packets; there is no reason to retransmit voice if packets are lost.
- Voice packets must receive a higher priority than other types of traffic.
- Cisco products use the RTP port range 16384 to 32767 to prioritize voice traffic.
- Voice can tolerate a certain amount of latency, jitter, and loss without any noticeable effects.
- Latency should be no more than 150 ms.
- Jitter should be no more than 30 ms.
- Voice packet loss should not exceed 1%.



Video

- Without QoS and a significant amount of extra bandwidth capacity, video quality typically degrades.
- The picture appears blurry, jagged, or in slow motion. The audio portion may become unsynchronized with the video.
- Video Traffic Characteristics:
  - Video – Bursty, greedy, drop sensitive, delay sensitive, UDP priority
  - One-Way Requirements:
    - Latency <= 200 - 400 ms
    - Jitter <= 30 – 50ms
    - Loss <= 0.1 – 1%
    - Bandwidth (384 Kb/s – 20+ Mb/s)



- Compared to voice, video is less resilient to loss and has a higher volume of data per packet as shown above.
  - Notice how voice packets arrive every 20 ms and are 200 bytes.
  - In contrast, the number and size of video packets varies every 33 ms based on the content of the video.

Data

- Most applications use either TCP or UDP. Unlike UDP, TCP performs error recovery.
- Data applications that have no tolerance for data loss, such as email and web pages, use TCP to ensure packets will be resent in the event they are lost.
- Some TCP applications, such as FTP, can be very greedy, consuming a large portion of network capacity.
- Although data traffic is relatively insensitive to drops and delays compared to voice and video, a network administrator still needs to consider the quality of the user experience.

Data Traffic Characteristics

Data

- Smooth/bursty
- Benign/greedy
- Drop insensitive
- Delay insensitive
- TCP retransmits

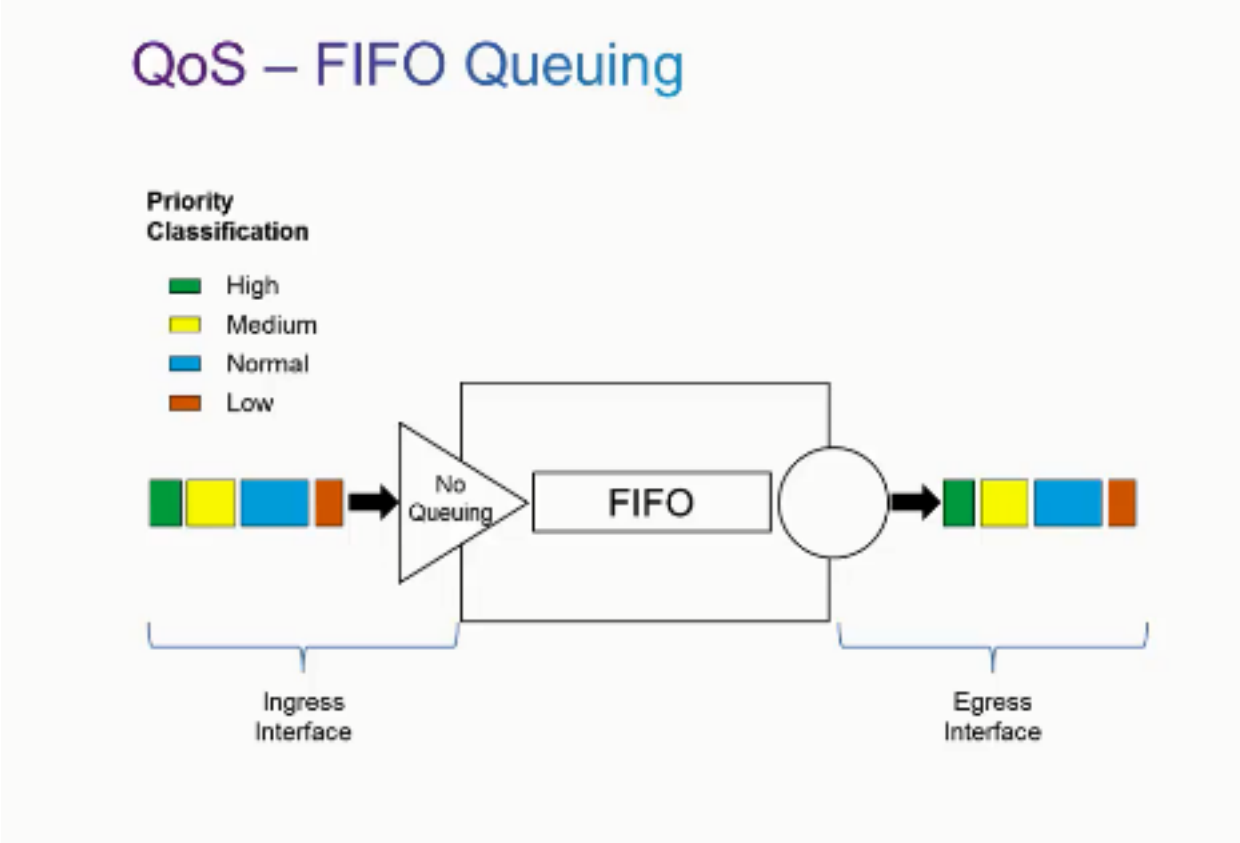
Factors to Consider for Data Delay

Factor	Mission Critical	Not Mission Critical
Interactive	Prioritize for the lowest delay of all data traffic and strive for a 1 to 2 seconds response time.	Applications could benefit from lower delay.
Not interactive	Delay can vary greatly as long as the necessary minimum bandwidth is supplied.	Gets any leftover bandwidth after all voice, video, and other data application needs are met.

- Two factors that need to be determined:
  - Does the data come from an interactive application?
  - Is the data mission critical?

QoS Algorithms

- If we look at the queuing strategies for QoS, FIFO Queuing or First in First Out Queuing, is basically the absence of QoS.
- Packets that enter the router will leave the router in the same order.
- Compare this with Weighted Fair Queuing or WFQ and packets that come into a router are then classified and prioritized based on the classification.
- A newer form of Weighted Fair Queuing is Class Based Weighted Fair Queuing.
- In order to guarantee that voice traffic is prioritized to the point there are no drops, Low-Latency Queuing can be used with CBWFQ to prioritize voice packets above all else.

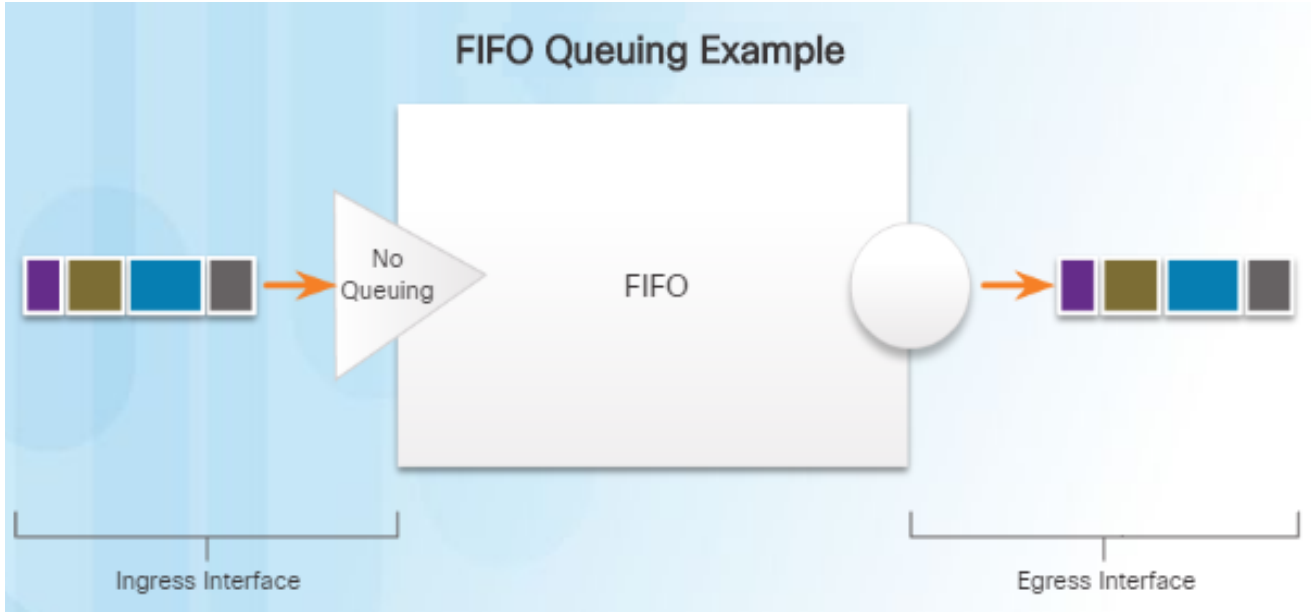


Queuing Overview

- The QoS policy implemented by the network administrator becomes active **when congestion occurs** on the link.
- Queuing is a congestion management tool that can buffer, prioritize, and if required, reorder packets before being transmitted to the destination.
- This course will focus on the following queuing algorithms:
  - First-In, First-Out (FIFO)
  - Weighted Fair Queuing (WFQ)
  - Class-Based Weighted Fair Queuing (CBWFQ)
  - Low Latency Queuing (LLQ)

First In First Out (FIFO)

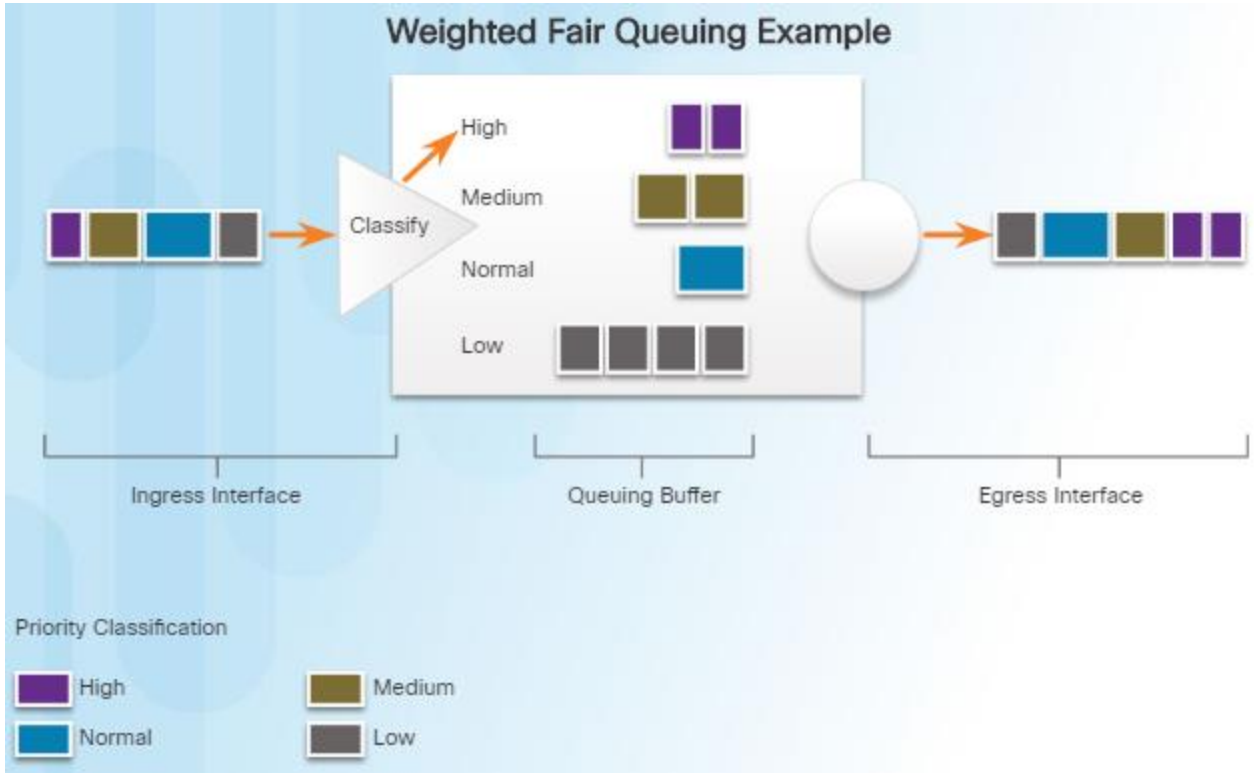
- FIFO queuing, also known as first-come, first-served queuing, involves buffering and forwarding of packets in the order of arrival.
- FIFO has no concept of priority or classes of traffic and consequently, makes no decision about packet priority.
- There is one queue and all packets are treated equally.
- When FIFO is used, important or time-sensitive traffic can be dropped when congestion occurs on the router or switch interface.
- When no other queuing strategies are configured, FIFO is used on serial interfaces at E1 (2.048 Mbps) and below.



- FIFO is effective for large links that have little delay and minimal congestion
- If your link has very little congestion, FIFO queuing may be the only queuing you need to use.

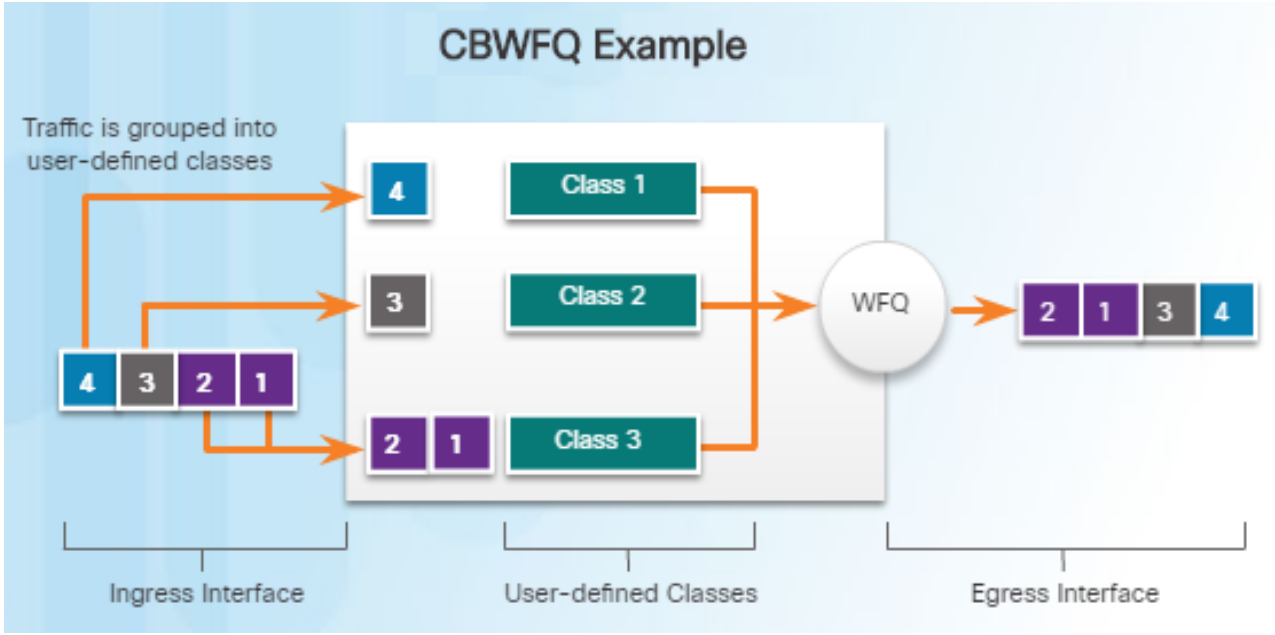
Weighted Fair Queuing (WFQ)

- WFQ is an automated scheduling method that provides fair bandwidth allocation to all network traffic.
- WFQ applies priority, or weights, to identified traffic and classifies it into conversations or flows.
- WFQ then determines how much bandwidth each flow is allowed relative to other flows.
- WFQ schedules interactive traffic to the front of a queue to reduce response time. It then shares the remaining bandwidth among high-bandwidth flows.
- WFQ classifies traffic into different flows based on packet header addressing, including source/destination IP addresses, MAC addresses, port numbers, protocols, and type of service (ToS) values.



Class-Based Weighted Fair Queuing (WFQ)

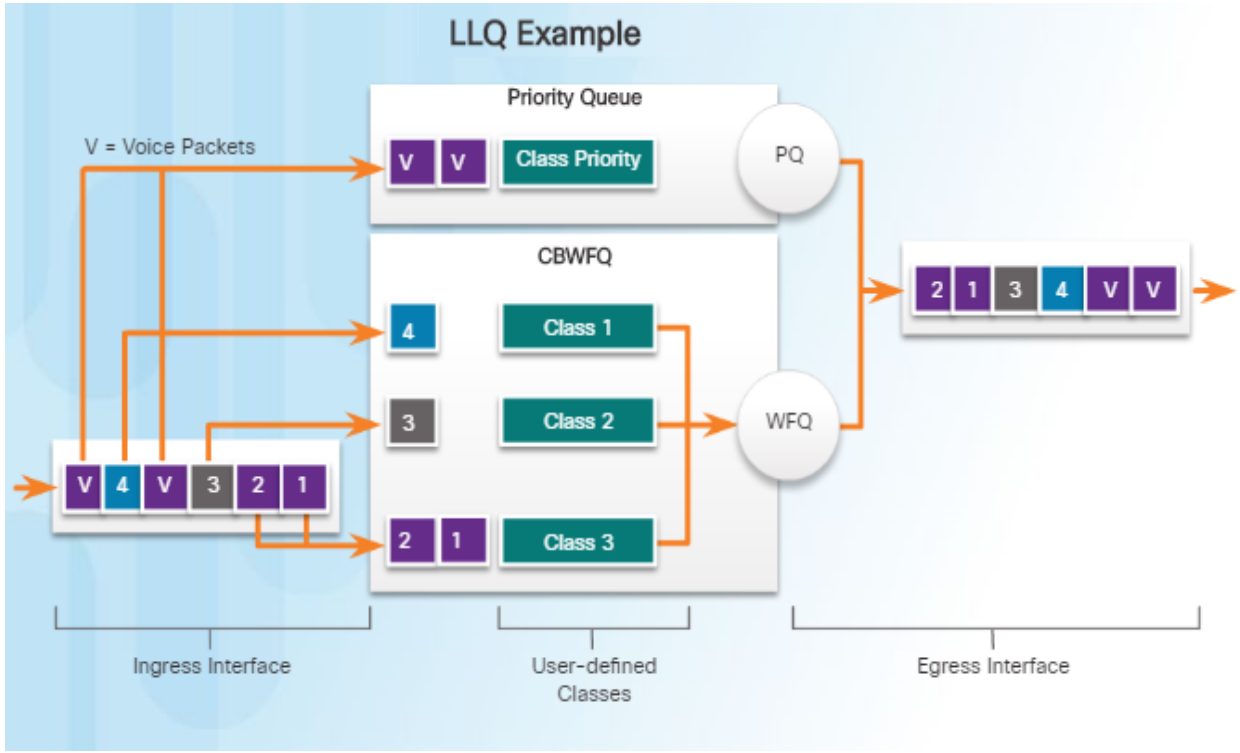
- CBWFQ extends the standard WFQ functionality to provide support for user-defined traffic classes.
- You define traffic classes based on match criteria including protocols, ACLs, and input interfaces.
- When a class has been defined according to its match criteria, you can assign it characteristics.
  - To characterize a class, you assign it bandwidth, weight, and maximum packet limit.
  - The bandwidth assigned to a class is the guaranteed bandwidth delivered to the class during congestion.



- Packets that match the criteria for a class constitute the traffic for that class. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue.

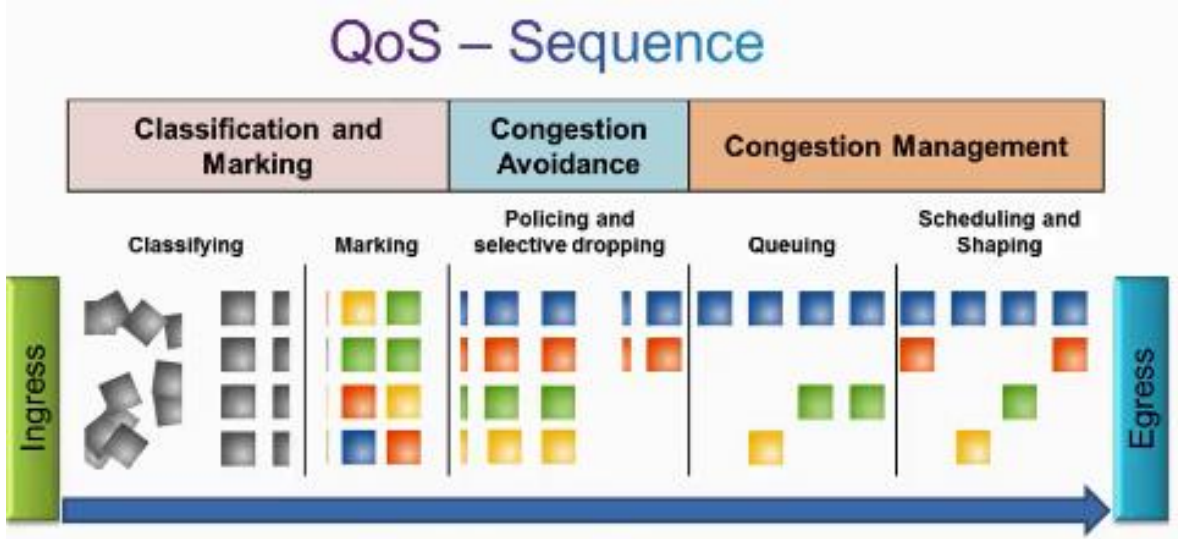
Low Latency Queuing (LLQ)

- The LLQ feature brings strict priority queuing (PQ) to CBWFQ which reduces jitter in voice conversations. See the figure to the left.
- Strict PQ allows delay-sensitive data such as voice to be sent before packets in other queues.
- Without LLQ, CBWFQ provides WFQ based on defined classes with no strict priority queue available for real-time traffic.
  - All packets are serviced fairly based on weight.
  - This scheme poses problems for voice traffic that is largely intolerant of delay.
- With LLQ, delay-sensitive data is sent first, before packets in other queues are treated.
- LLQ allows delay-sensitive data such as voice to be sent first giving it preferential treatment.



Video Tutorial – QoS Implementation Techniques

- QoS implementation tools can be categorized into three main categories:
  - Classification and marking tools – Session traffic is classified into different priority groupings and packets are marked.
  - Congestion avoidance tools – Traffic classes are allotted network resources and some traffic may be selectively dropped, delayed or remarked to avoid congestion.
  - Congestion management tools – During congestion, traffic is queued to await the availability of those resources; tools include class based weighted fair queuing, and low latency queuing.



QoS – Traffic Marking

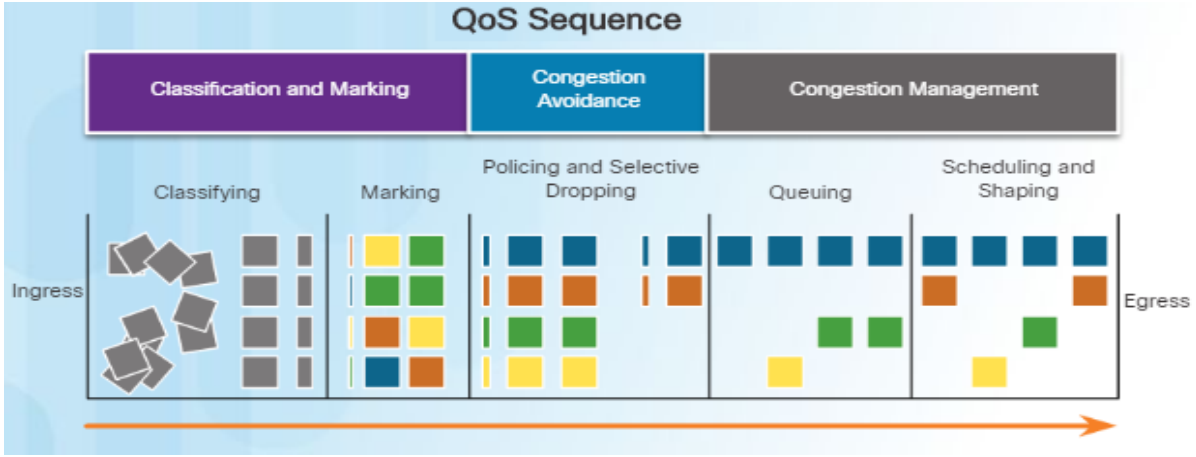
QoS Tools	Layer	Marking Field	Width in Bits
Ethernet (802.1Q, 802.1p)	2	Class of Service (CoS)	3
802.11 (Wi-Fi)	2	Wi-Fi Traffic Identifier (TID)	3
MPLS	2	Experimental (EXP)	3
IPv4 and IPv6	3	IP Precedence	3
IPv4 and IPv6	3	Differentiated Services Code Point (DSCP)	6

Avoiding Packet Loss

- Packet loss is usually the result of congestion on an interface.
- Most TCP applications experience slowdown because TCP automatically adjusts to network congestion.
  - Some applications do not use TCP and cannot handle drops (fragile flows).
- The following approaches can prevent drops in sensitive applications:
  - Increase link capacity to ease or prevent congestion.
  - Guarantee enough bandwidth and increase buffer space to accommodate bursts of traffic from fragile flows – WFQ, CBWFQ and LLQ.
  - Prevent congestion by dropping lower-priority packets before congestion occurs – weighted random early detection (WRED).

QoS Tools

- There are three categories of QoS tools:
  - Classification and marking tools
  - Congestion avoidance tools
  - Congestion management tools
- Ingress packets (gray squares) are classified and their respective IP header is marked (colored squares). To avoid congestion, packets are then allocated resources based on defined policies.
- Packets are then queued and forwarded out the egress interface based on their defined QoS shaping and policing policy.
- Classification and marking can be done on ingress or egress, whereas other QoS actions such as queuing and shaping are usually done on egress.



Tools for Implementing QoS

QoS Tools	Description
Classification and marking tools	• Sessions, or flows, are analyzed to determine what traffic class they belong to. • Once determined, the packets are marked.
Congestion avoidance tools	• Traffic classes are allotted portions of network resources as defined by the QoS policy. • The QoS policy also identifies how some traffic may be selectively dropped, delayed, or re-marked to avoid congestion. • The primary congestion avoidance tool is WRED and is used to regulate TCP data traffic in a bandwidth-efficient manner before tail drops caused by queue overflows occur.
Congestion management tools	• When traffic exceeds available network resources, traffic is queued to await availability of resources. • Common Cisco IOS-based congestion management tools include CBWFQ and LLQ algorithms.

Classification and Marking

- A packet has to be classified before it can have a QoS policy applied to it.
- Classification and marking allows us to identify, or “mark” types of packets.
- Classification determines the class of traffic to which packets or frames belong. Policies can not be applied unless the traffic is marked.
- Methods of classifying traffic flows at Layer 2 and 3 include using interfaces, ACLs, and class maps.
- Marking requires the addition of a value to the packet header and devices that receive the packet look at this field to see if it matches a defined policy.
- Marking should be done as close to the source as possible and this establishes the trust boundary.

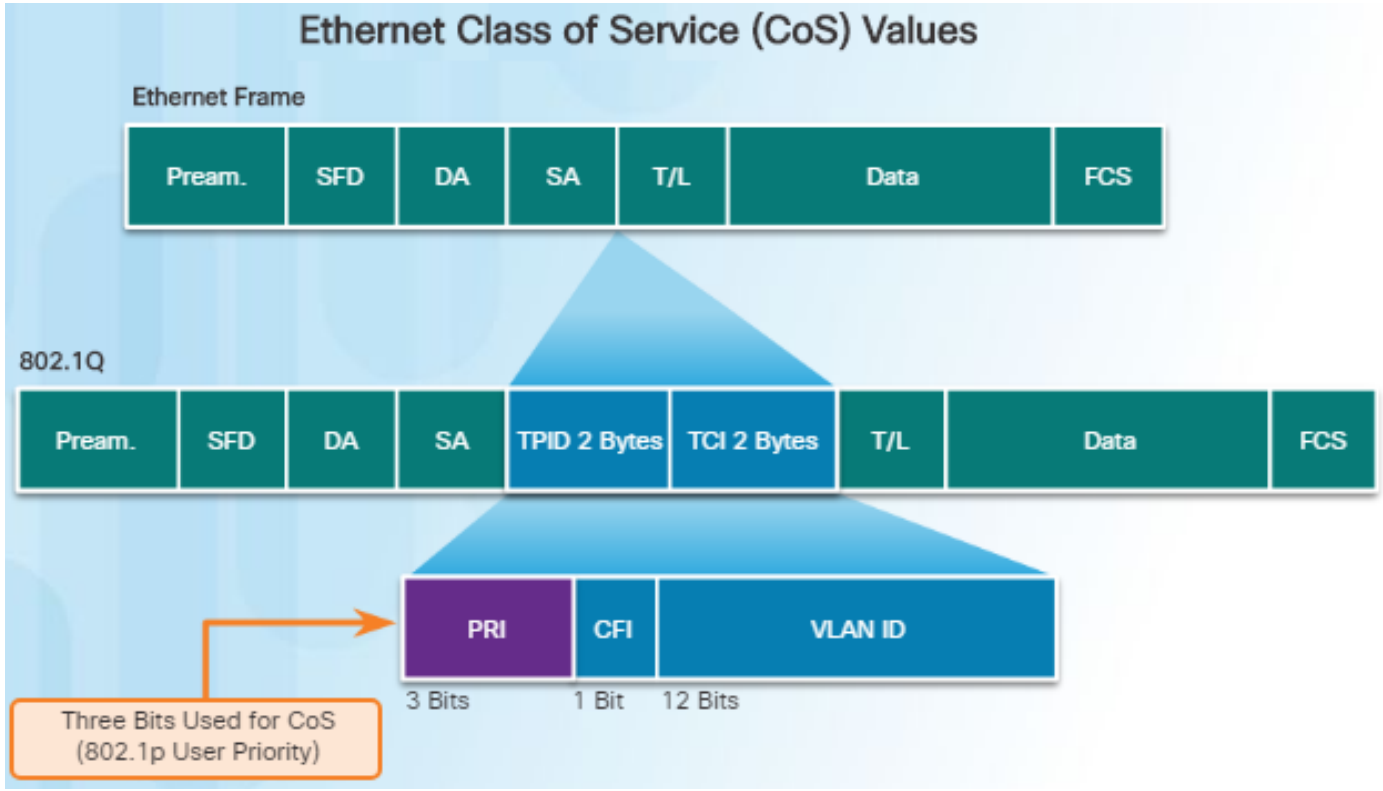
Traffic Marking for QoS

QoS Tools	Layer	Marking Field	Width in Bits
Ethernet (802.1Q, 802.1p)	2	Class of Service (CoS)	3
802.11 (Wi-Fi)	2	Wi-Fi Traffic Identifier (TID)	3
MPLS	2	Experimental (EXP)	3
IPv4 and IPv6	3	IP Precedence (IPP)	3
IPv4 and IPv6	3	Differentiated Services Code Point (DSCP)	6

- The table in the figure describes some of the marking fields used in various technologies. Consider the following points when deciding to mark traffic at Layers 2 or 3:
  - Layer 2 marking of frames can be performed for non-IP traffic.
  - Layer 2 marking of frames is the only QoS option available for switches that are not “IP aware”.
  - Layer 3 marking will carry the QoS information end-to-end.

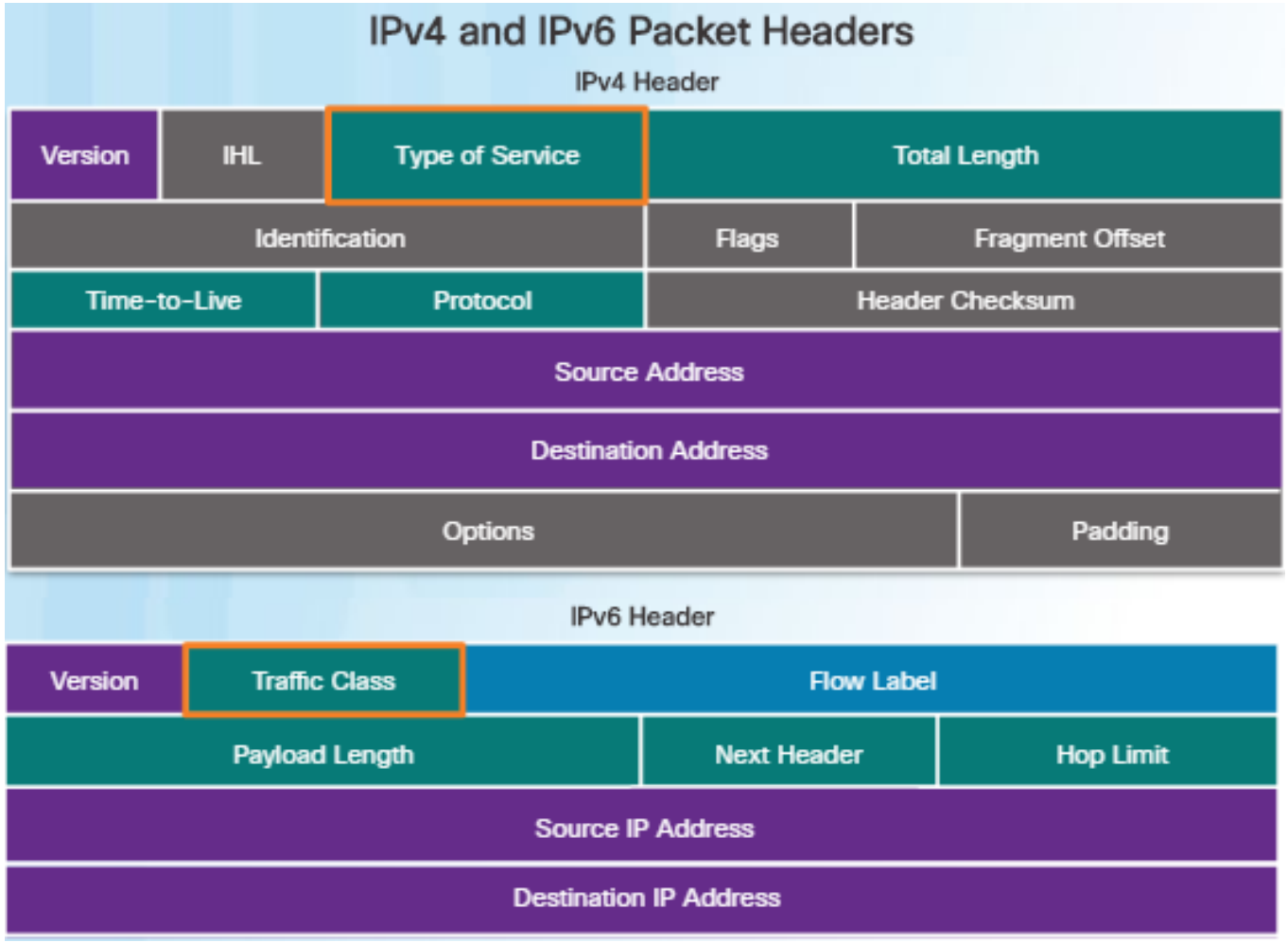
Marking at Layer 2

- 802.1Q is the IEEE standard that supports VLAN tagging at Layer 2 on Ethernet networks.
- When 802.1Q is implemented, two fields are added to the Ethernet Frame and are inserted following the source MAC address field as shown in the figure to the left.
- The 802.1Q standard includes the QoS prioritization scheme known as IEEE 802.1p. The standard uses the first three bits in the Tag Control Information (TCI) field and identifies the CoS markings.
- These three bits allow eight levels of priority (0-7).



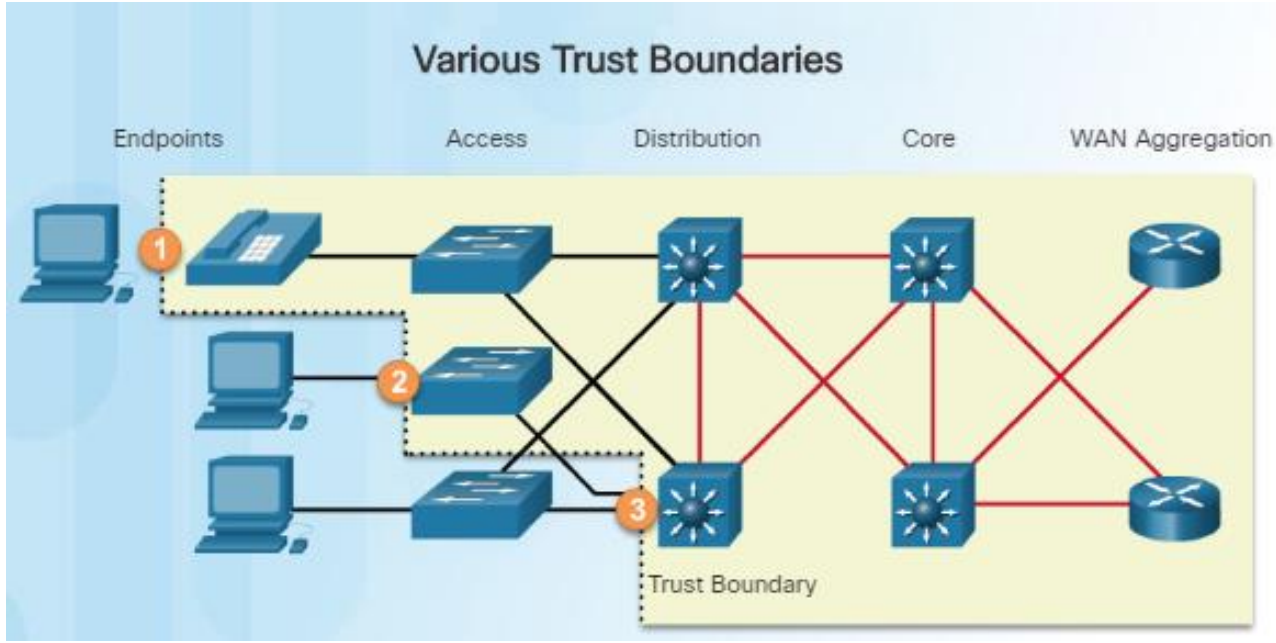
Marking at Layer 3

- IPv4 and IPv6 specify an 8-bit field in their packet headers to mark packets.
  - IPv4 – Type of Service (ToS) field
  - IPv6 – Traffic Class field
- These fields are used to carry the packet marking assigned by the QoS classification tools. Forwarding devices refer to this field and forward the packets based on the QoS policy.
- RFC 2474 redefines the ToS field by renaming and extending the IPP field. The new filed has 6-bits allocated for QoS called the differentiated services code point (DSCP) field.
- These six bits offer a maximum of 64 possible classes of service.



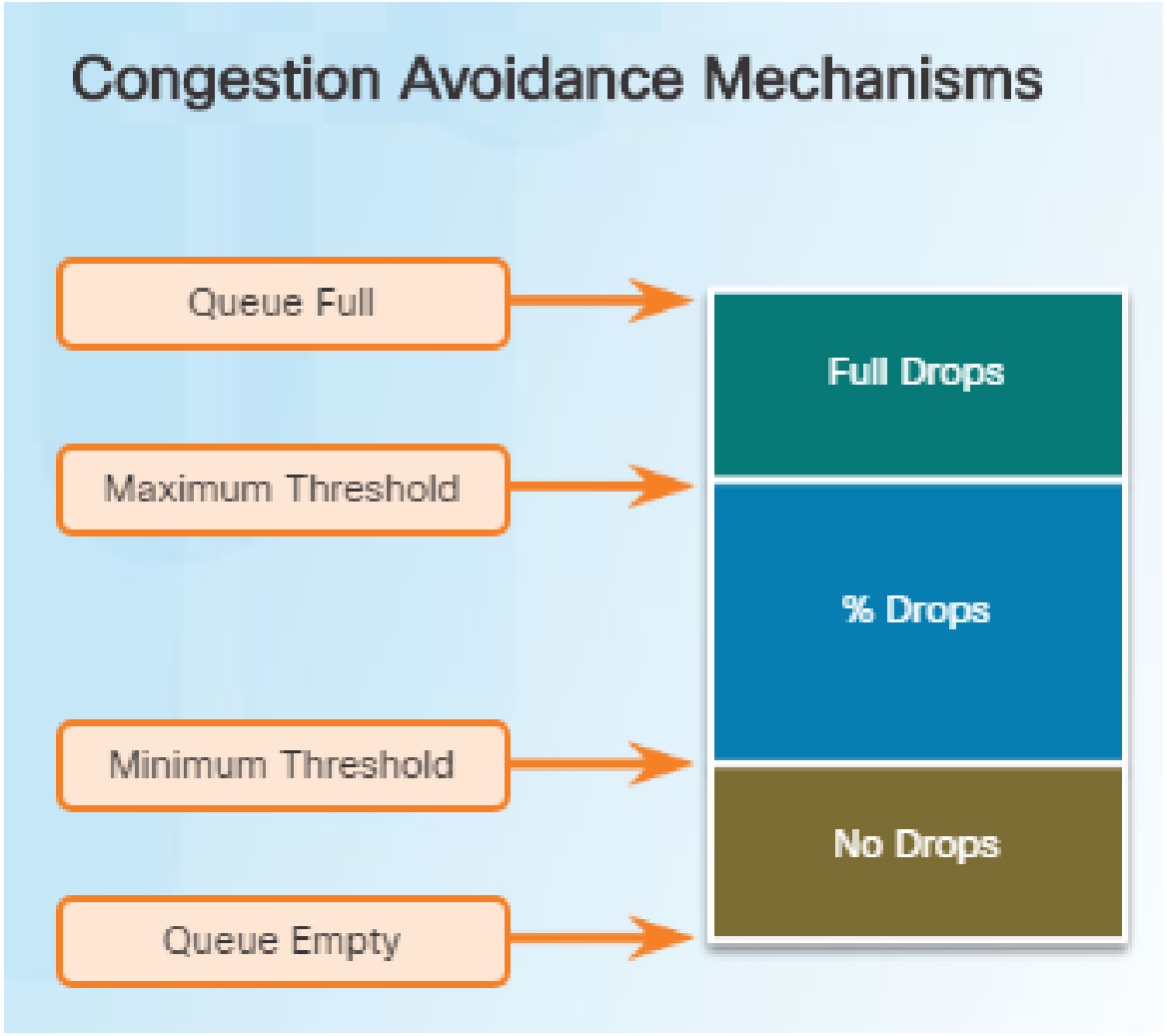
Trust Boundaries

- Where should markings occur?
- Traffic should be classified and marked as close to its source as possible.
- This defines the trust boundary as shown in the figure.
  - Trusted endpoints have the capabilities and intelligence to mark application traffic to the appropriate Layer 2 CoS or Layer 3 DSCP values. Examples of trust endpoints include IP phones, wireless access points, and videoconferencing systems.
  - Secure endpoints can have traffic marked at the Layer 2 switch.
  - Traffic can also be marked at Layer 3 switches and routers.
- Re-marking of traffic is typically necessary.



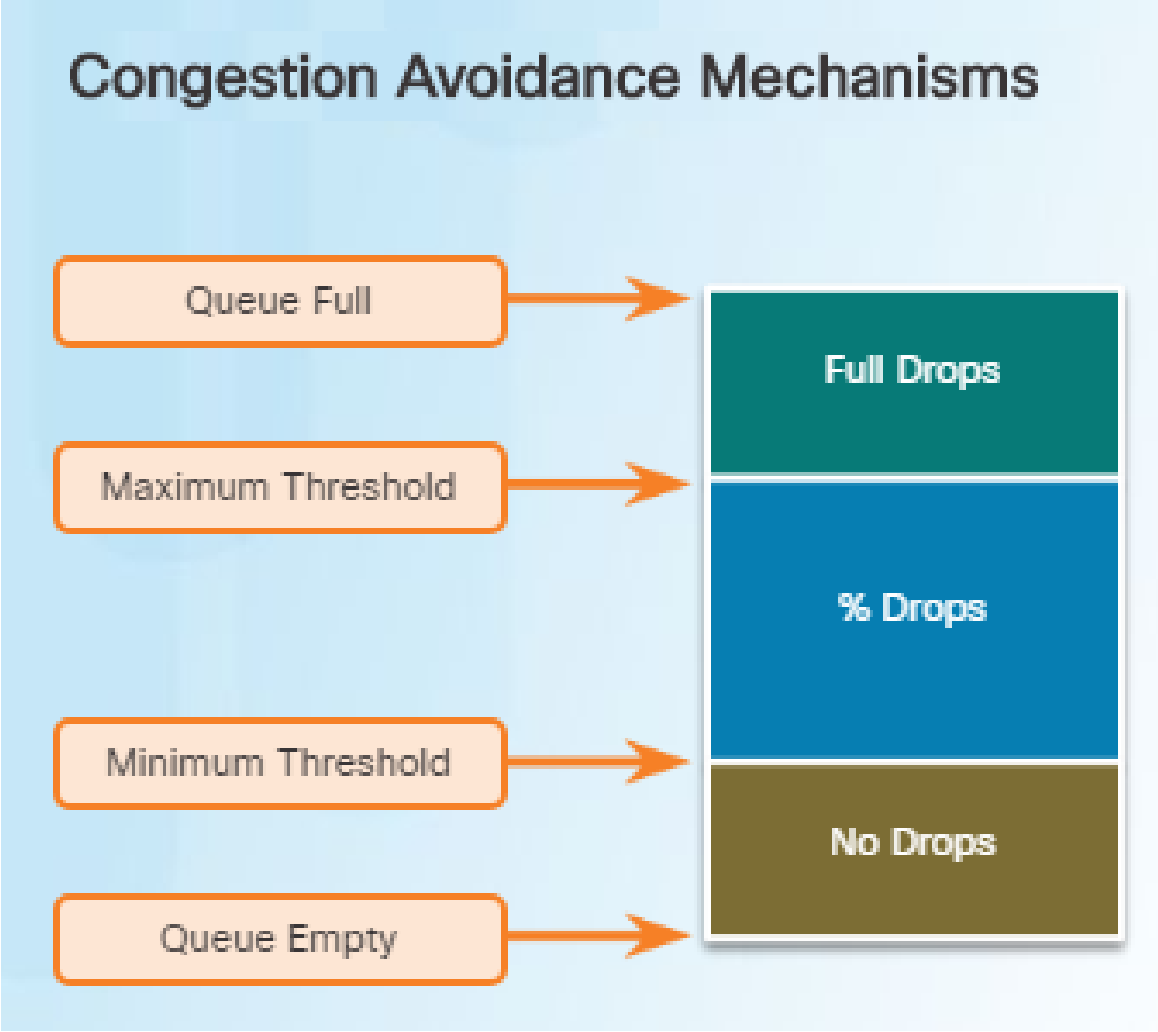
Congestion Avoidance

- Congestion avoidance tools monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks before congestion becomes a problem.
- Congestion avoidance is achieved through packet dropping.
- These tools monitor the average depth of the queue.
  - For example, when the queue fills up to the maximum threshold, a small percentage of packets are dropped.
  - When the maximum threshold is passed, all packets are dropped.



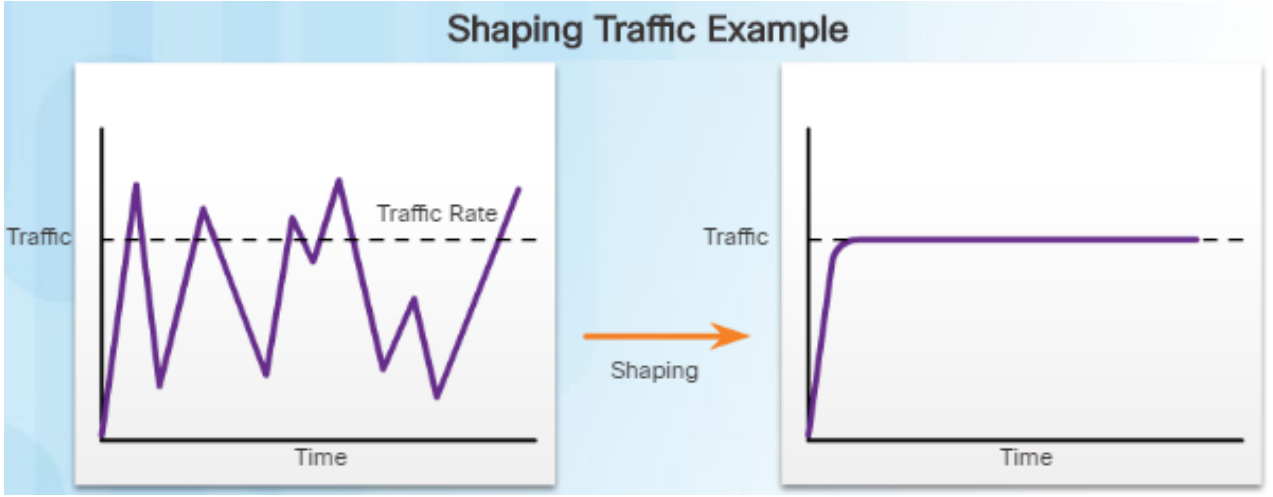
Congestion Avoidance (Cont.)

- The Cisco IOS includes weighted random early detection (WRED) as a possible congestion avoidance solution.
  - WRED is a congestion avoidance technique that allows for preferential treatment of which packets will get dropped.
  - The WRED algorithm allows for congestion avoidance on network interfaces by providing buffer management and allowing TCP traffic to decrease, or throttle back, before buffers are exhausted.
  - Using WRED helps avoid tail drops and maximizes network use and TCP-application performance.
- There is no congestion avoidance for UDP traffic – such as voice traffic.



Shaping and Policing

- Traffic shaping and policing are two mechanisms provided by the Cisco IOS QoS software to prevent congestion.
- Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time.
  - The result of traffic shaping is a smoothed packet output rate as shown in the figure.
  - Shaping requires sufficient memory.
- Shaping is used on outbound traffic.
- Policing is commonly implemented by service providers to enforce a contracted customer information rate (CIR).
- Policing either drops or remarks excess traffic.
- Policing is often applied to inbound traffic.



MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť!

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7

Vytvorené v rámci projektu KEGA 011STU - 4/2017.