QoS в безжични мрежи

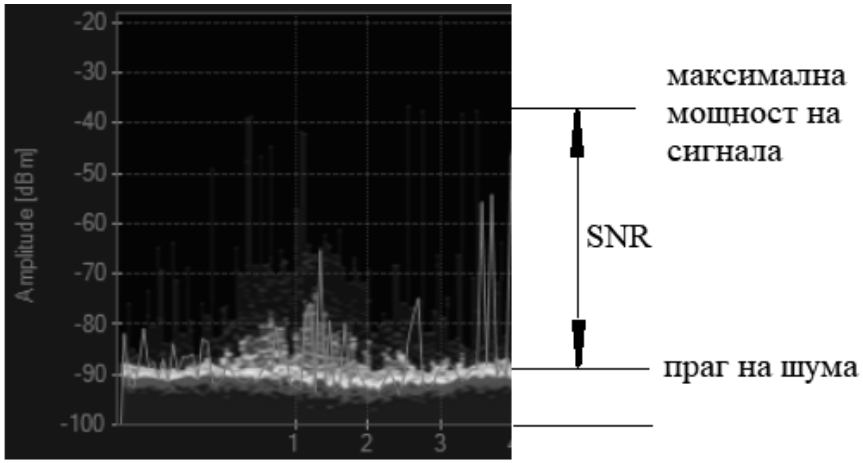
проф. д-р инж. Венета Алексиева

Основни моменти

- Качество при предаване на данни в мрежа
- Характеристики на трафика
- Алгоритми с опашки
- QoS модели
- Внедрени QoS техники

Цел на QoS

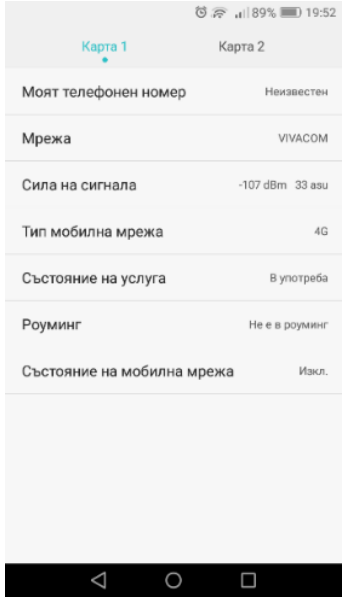
Сигнал и шум в Wi-Fi мрежа



- По време на комуникация в преносната среда възникват паразитни сигнали на същите честоти на предаване и те се наслагват с основния сигнал.
- Тези паразитни сигнали са в следствие на случайни процеси, при които се изменя концентрацията и /или скоростта на носещите честоти.
- Това поражда поява на шумов ток и напрежение и, следователно, на шумова мощност (P_n).
- Източници на шум са усилватели, смесители, антени и др.
- В безжичната преносна среда се проявява интерференция от други източници на сигнал, излъчващи в същия честотен спектър.
- .

В безжична мрежа

- На всяко мобилно устройство в Настройки / Всичко за телефона / Мрежа може да се наблюдава моментната стойност на мощността на сигнала за 4G мрежата, докато за моментната мощност на достъпните безжични мрежи до устройството, трябва да се ползва Wi-Fi анализатор.



SNR нива при Wi-Fi мрежа

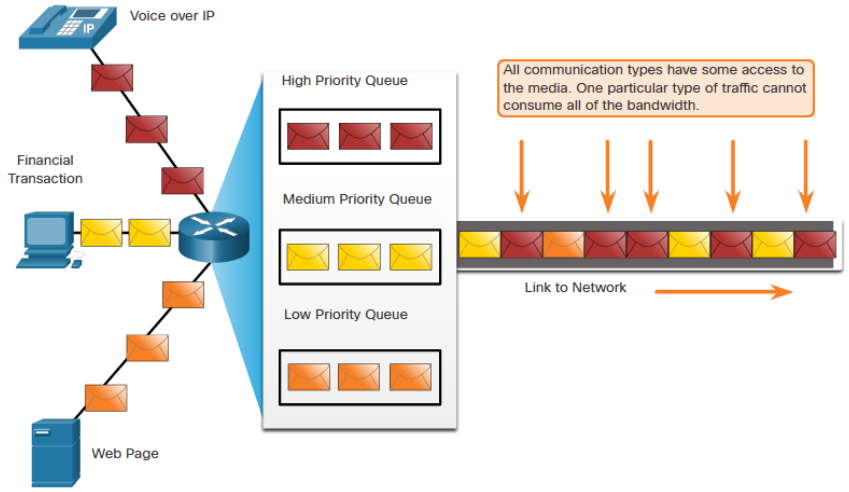
Ниво на SNR	Качество на сигнала	Статус	Скорост
> 40dB	Отличен сигнал	Винаги свързан	Максимална
25dB до 40dB	Много добър сигнал	Винаги свързан	Много висока
15dB до 25dB	Слаб сигнал	Винаги свързан	Обикновено висока
10dB до 15dB	Много слаб сигнал	В повечето случаи свързан	В повечето случаи бавна
5dB до 10dB	Няма сигнал	Несвързан	-

SNR нива при LTE модем

Ниво на SNR	Качество на сигнала	Статус	Скорост
>= 20dB	Отличен сигнал	Винаги свързан	Максимална
13dB до 20dB	Добър сигнал	Винаги свързан	Много висока
0dB до 13dB	Среден до слаб сигнал	Винаги свързан	Обикновено висока
<= 0	Няма сигнал	Несвързан	-

Приоритизация на трафика

Устройството прилага QoS само когато изпитва някакъв вид задръствания.



- Когато обемът на трафика е по-голям от този, който може да бъде транспортиран в мрежата, устройствата поставят на опашка пакетите в паметта, докато ресурсите не станат достъпни за предаването им.
- Подреждането на пакети в опашка причинява забавяне, тъй като новите пакети не могат да бъдат предадени, докато предишните пакети не бъдат обработени.
- Ако броят на пакетите в опашката продължава да се увеличава, паметта в устройството се запълва и пакетите се изгубват.
- Една QoS техника, която може да помогне с този проблем, е класифицирането на данни в множество опашки.

Приоритизация в различни технологии

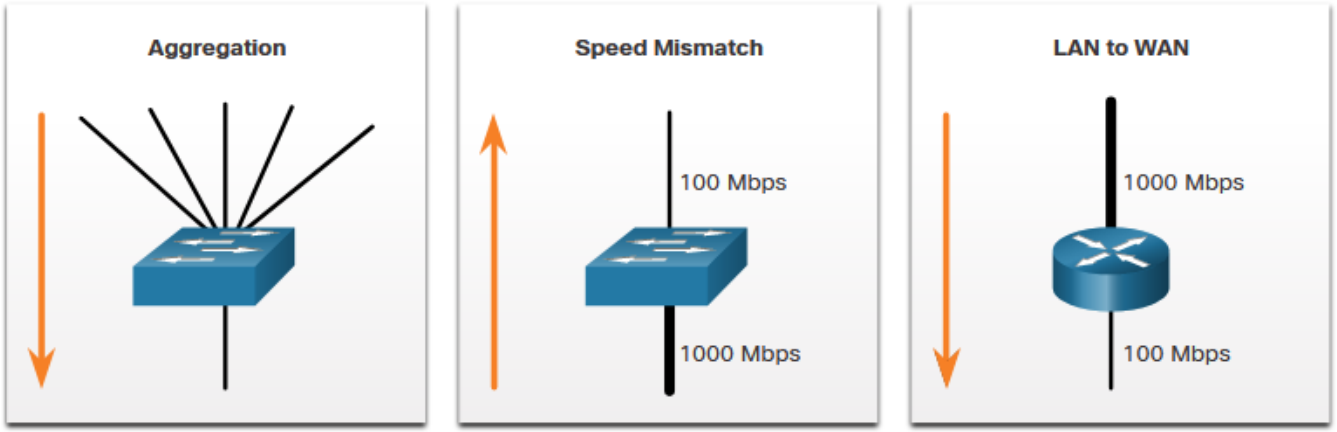
- Традиционно маршрутизиране – FIFO
- В MPLS – приоритети 0-7 (FEC класове трафик):
  - FEC с прецизна грануларност е на база 5 критерия:
    - source и destination IP адреси,
    - source и destination TCP и UDP портове,
    - и номер на протокол,
  - FEC със средна грануларност е според дестинацията на IP адресите,
  - FEC с груба грануларност е ако критерия е само egress LSR рутера.
- В LTE трафика се дели на:
  - Dedicated bearer
  - Default bearer
- В WiMAX трафика се дели на:
  - В реално време – UGS (напр. VoIP),rtPS (напр. MPEG),ertPS
  - Не в реално време – nrtPS (напр. FTP. TFTP,HTTP),
    BE(напр. Email, Web applications)

LTE QoS		
Dedicated Bearer		Default Bearer
Non-GBR	GBR	Non GBR
QCI 5-9 APN-AMBR UE-AMBR TFT ARP L-EBI	QCI 1-4 GBR MBR TFT ARP L-EBI	QCI 5-9 APN-AMBR UE-AMBR APN IP Address ARP

	В реално време			Не в реално време	
	UGS	ertPS	rtPS	nrtPS	BE
Приложения	VoIP		MPEG	FTP, TFTP, HTTP	Email Web applications

Пропускателна способност и претоварване

- Пропускателната способност на мрежата се измерва в броя битове, които могат да бъдат предадени за една секунда (bps).
- Претоварването на мрежата причинява забавяне. Интерфейсът изпитва задръствания, когато получава повече трафик, отколкото може да поеме.
- Точките за претоварване на мрежата са подходящи за QoS механизми.
- Такива са агрегиране, несъответствие на скоростта и LAN към WAN.

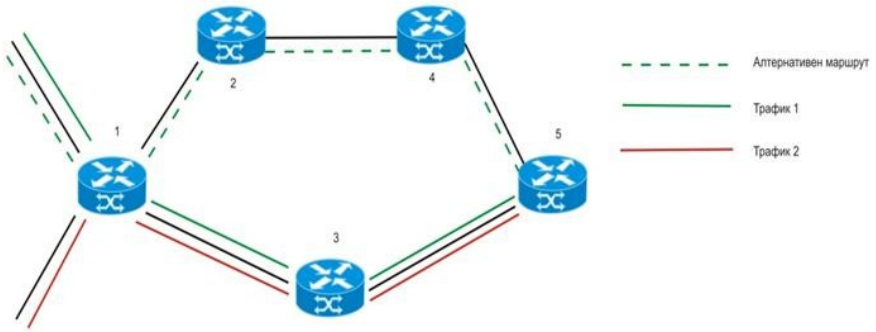


Закъснение и jitter

- Закъснение е времето, необходимо на пакета да пропътува от източника до дестинацията.
- Фиксирано закъснение е времето, което отнема определен процес, като например колко време е необходимо, за да се постави бит в предавателната среда.
- Променливото закъснение отнема неопределен период от време и се влияе от фактори като количеството трафик, който се обработва.
- Jitter (Трептене) е вариацията на забавянето на получените пакети.

Delay	Дефиниция
Code delay	Фиксираният период от време, необходимо за компресиране на данните в източника, преди да бъдат предадени към първото мрежово устройство, обикновено комутатор.
Packetization delay	Фиксираното време, необходимо за капсулиране на пакет с цялата необходима информация за заглавието.
Queuing delay	Променливият период от време, през който един кадър или пакет чака да бъде предаден по връзката.
Serialization delay	Фиксираният период от време, необходимо за предаване на кадър в проводника.
Propagation delay	Променливото време, необходимо на кадъра да пътува между източника и местоназначението.
De-jitter delay	Фиксираният период от време, необходимо за буфериране на поток от пакети и след това изпращането им на равномерно разпределени интервали.

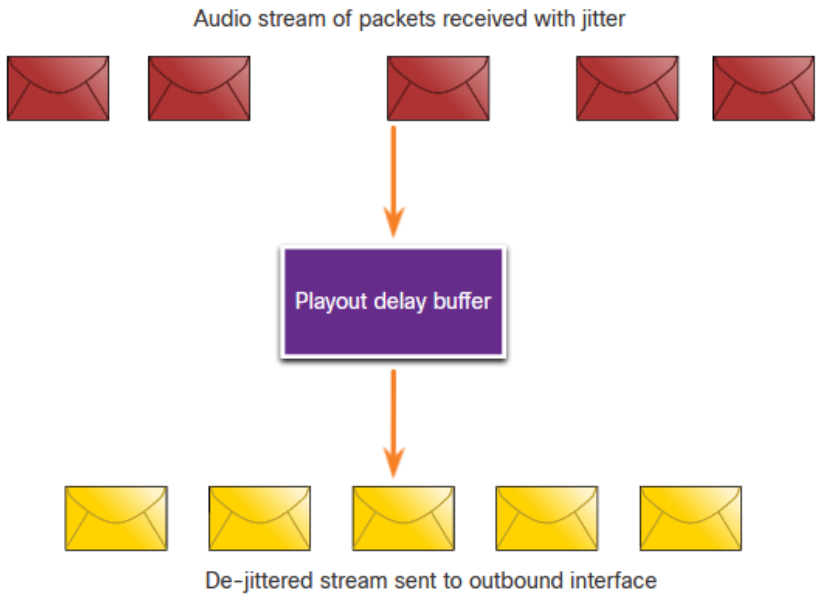
Трафик инженеринг



Трафик инженеринг

- Трафик инженерингът представлява процес на оптимизиране използването на мрежовите ресурси, с който се постига ефективно натоварване на мрежата.
- Основните проблеми, които ТЕ решава, са:
  - припокриването на маршрутите при наличие на множество източници с една дестинация
  - преминаване границата на капацитета на най-краткия маршрут, когато съществува алтернативен, по-слабо натоварен, но по-дълъг такъв.

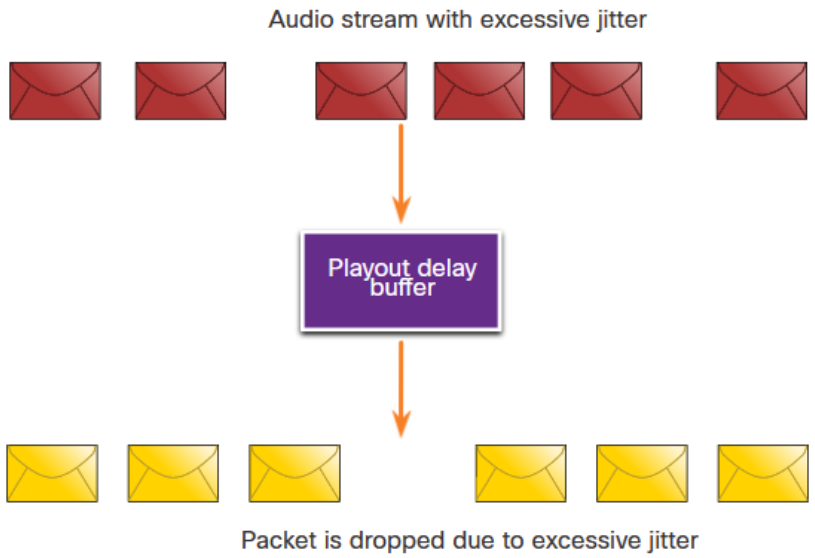
Загуба на пакети



- Без QoS механизми, чувствителните към забавяне пакети, като видео и глас в реално време, се отхвърлят със същата честота като данните, които не са чувствителни към времето.
- Когато рутерът получи цифров аудио поток по протокол в реално време (RTP) за VoIP, той компенсира jitter като използва буфер за забавяне на възпроизвеждането.
- Буферът за забавяне на възпроизвеждането буферира тези пакети и след това ги възпроизвежда в постоянен поток.

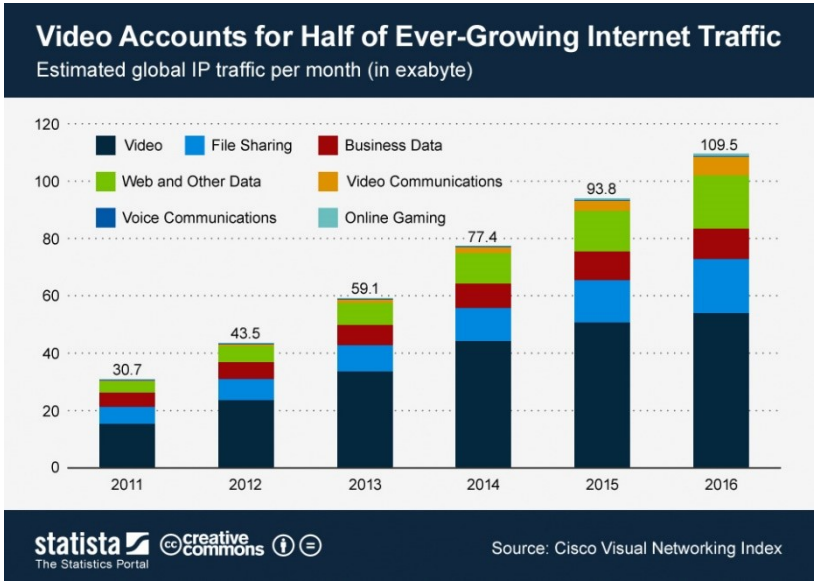
Загуба на пакети

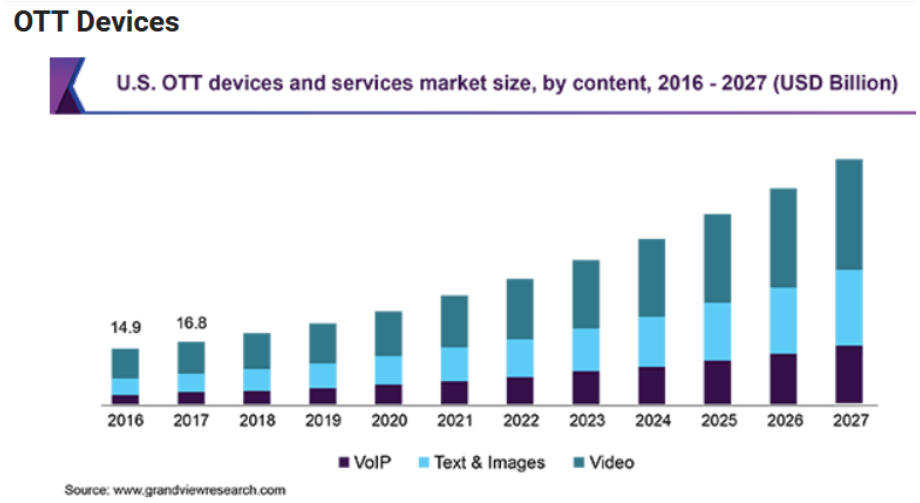
- В правилно проектирана мрежа загубата на пакети трябва да е близо до нула.
- Ако jitter е толкова голям, че води до получаване на пакети извън обхвата на буфера за възпроизвеждане, пакетите извън обхвата се изхвърлят и в аудиото се чуват прекъсвания.
- За загуби, малки като един пакет, цифровият сигнален процесор (DSP) интерполира това, което смята, че трябва да бъде аудиото и потребителят не чува никакъв проблем. Когато jitter надхвърля това, което DSP може да компенсира липсващите пакети, се чуват проблеми със звука.



Характеристики на трафика

- Типът изисквания, които глас, видео и данни поставят на мрежата, са много различни.
- Гласовият трафик има предвидима нужда от честотна лента и известни времена на пристигане на пакети.
- Трафикът на данни не е в реално време и има непредвидима нужда от честотна лента. Трафикът на данни може временно да нарасне, както при изтегляне на голям файл.
- Видео трафикът става все по-важен за бизнес комуникациите. Според индекса за визуални мрежи на Cisco (VNI), видео трафикът представлява 82% от целия трафик през 2022 г.





Характеристики на преноса на глас

- Гласовият трафик е предвидим и плавен и много чувствителен към закъснения и изпуснати пакети.
- Гласовите пакети трябва
- Продуктите на Cisco използват обхвата на RTP портове от 16384 до 32767, за да приоритизират гласовия трафик.
- Гласът може да толерира известно количество латентност, jitter и загуба без никакви забележими ефекти.
- Закъснението трябва да бъде не повече от 150 милисекунди (ms).
- Jitter трябва да бъде не повече от 30 ms.
- Загубата на пакети не повече от 1%. Гласовият трафик изисква поне 30 Kbps честотна лента.

Voice Traffic Characteristics	One-Way Requirements
• Smooth • Benign • Drop sensitive • Delay sensitive • UPD priority	• Latency ≤ 150ms • Jitter ≤ 30ms • Loss ≤ 1% Bandwidth (30-128 Kbps)

Характеристики на video трафика

- Видеотрафикът обикновено е непредсказуем, непоследователен и рязък.
- В сравнение с гласа, видеото е по-малко устойчиво на загуба и има по-голям обем данни на пакет.
- Броят и размерът на видео пакетите варират на всеки 33 ms в зависимост от съдържанието на видеото.
- UDP портове като 554 се използват за протокола за поточно предаване в реално време (RSTP) и трябва да им се даде приоритет пред друг, по-малко чувствителен към забавяне мрежов трафик.
- Закъснението трябва да бъде не повече от 400 ms.
- Jitter трябва да бъде не повече от 50 ms.
- Загубата на видео пакети трябва да бъде не повече от 1%.
- Видео трафикът изисква поне 384 Kbps честотна лента.

Video Traffic Characteristics	One-Way Requirements
• Bursty • Greedy • Drop sensitive • Delay sensitive • UPD priority	• Latency ≤ 200-400 ms • Jitter ≤ 30-50 ms • Loss ≤ 0.1 – 1% Bandwidth (384 Kbps - 20 Mbps)

Характеристика на трафика на данни

- Приложенията за данни, които нямат толерантност към загуба на данни, като имейл и уеб страници, използват TCP, за да гарантират, че ако пакетите бъдат загубени при предаване, те ще бъдат повторно изпратени.
- Трафикът на данни може да бъде гладък или разкъсан.
- Трафикът за управление на мрежата обикновено е гладък и предвидим.
- Някои TCP приложения могат да консумират голяма част от мрежовия капацитет.
- FTP ще консумира толкова честотна лента, колкото може да получи.
- Трафикът на данни е относително нечувствителен към спадове и закъснения в сравнение с гласа и видеото.
- Качеството на опита (QoE) е важно да се вземе предвид при трафика на данни:
  - Данните идват ли от интерактивно приложение?
  - Данните от критично важно приложение ли са?

Data Traffic Characteristics

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

Factor	Mission Critical	Not Mission Critical
Interactive	Дава приоритет на най-ниското забавяне от целия трафик на данни, като целта е време за реакция от 1 до 2 секунди.	Приложенията могат да се възползват от по-малко забавяне.
Not interactive	Закъснението може да варира значително, докато се доставя необходимата минимална честотна лента.	Получава останалата честотна лента, след като всички нужди на приложенията за глас, видео и други данни са изпълнени.

Опашки

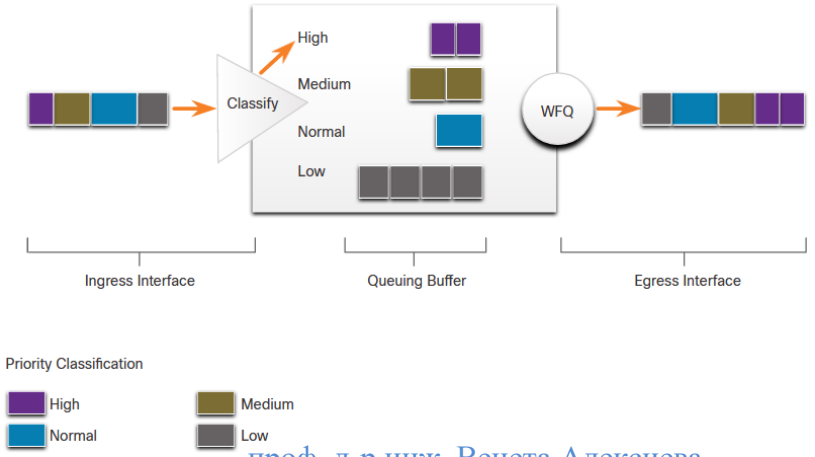
- Опашката е инструмент за управление на претоварване, който може да буферира, да приоритизира и, ако е необходимо, да пренареди пакети, преди да бъдат предадени до местоназначението.
- Налични са редица алгоритми за опашка:
  - Първи влязъл, първи излязъл (FIFO)
  - Претеглена справедлива опашка (WFQ)
  - Претеглена справедлива опашка, базирана на класове (CBWFQ)
  - Опашка с ниска латентност (LLQ)

First in First Out

- Първият дошъл, първият излязъл (FIFO) буферира и препраща пакети по реда на тяхното пристигане.
- FIFO няма концепция за приоритет или класове трафик и следователно не взема решение относно приоритета на пакетите.
- Има само една опашка и всички пакети се третират еднакво.
- Пакетите се изпращат по интерфейса в реда, в който пристигат.

Weighted Fair Queuing (WFQ)

- Претеглената справедлива опашка (WFQ) е автоматизиран метод за планиране, който осигурява справедливо разпределение на честотната лента за целия мрежов трафик.
- WFQ прилага приоритет или тегла към идентифицирания трафик, класифицира го в потоци и след това определя колко честотна лента е разрешена за всеки поток спрямо другите потоци.
- WFQ класифицира трафика в различни потоци въз основа на IP адреси на източник и местоназначение, MAC адреси, номера на портове, протокол и стойност на тип услуга (ToS).
- WFQ не се поддържа с тунелиране и криптиране, тъй като тези функции променят информацията за съдържанието на пакета, изисквана от WFQ за класификация.

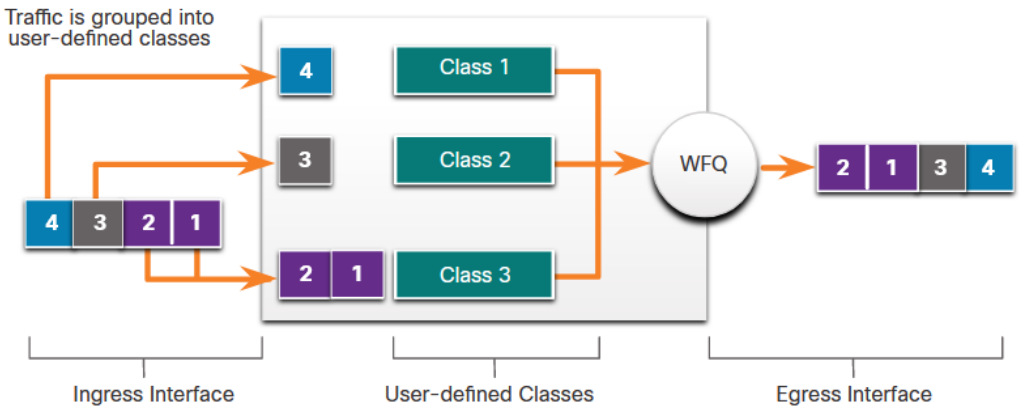


Class-Based Weighted Fair Queuing (CBWFQ)

- Претеглената справедлива опашка, базирана на класове (CBWFQ) разширява стандартната функционалност на WFQ, за да осигури поддръжка за дефинирани от потребителя класове трафик.
- Класовете трафик се дефинират въз основа на критерии за съвпадение, включително протоколи, списъци за контрол на достъп (ACL) и входящи интерфейси.
- Пакетите, отговарящи на критериите за съвпадение за даден клас, съставляват трафика за този клас.
- За всеки клас е запазена FIFO опашка и трафикът, принадлежащ към клас, се насочва към опашката за този клас.
- На клас могат да бъдат присвоени характеристики, като честотна лента, тегло и максимално ограничение на пакета. Пропускателната способност, присвоена на клас, е гарантираната честотна лента, предоставена по време на претоварване.
- Пакетите, принадлежащи към даден клас, подлежат на честотната лента и ограниченията на опашката, което е максималният брой пакети, разрешени да се натрупват в опашката, които характеризират класа.

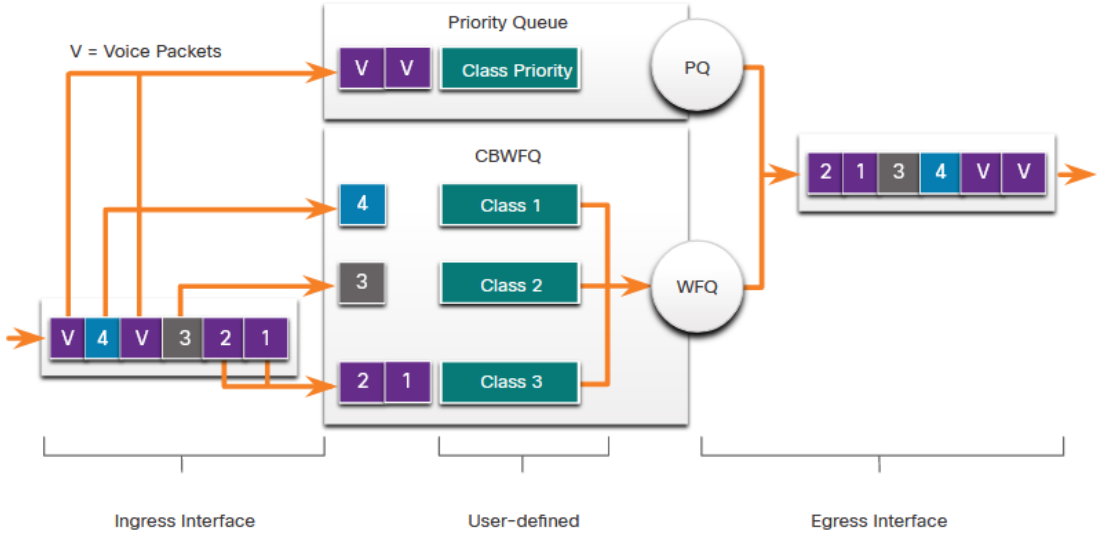
Class-Based Weighted Fair Queuing (CBWFQ)

- След като опашката достигне своето конфигурирано ограничение на опашката, добавянето на още пакети към класа води до действие на опашката или отхвърлянето на пакета, в зависимост от това как е конфигурирана политиката на класа.
- Tail drop изхвърля всеки пакет, който пристига в края на опашката, която е използвала напълно своите ресурси за задържане на пакети. Това е отговорът на опашката по подразбиране при претоварване.
- Tail drop третира целия трафик еднакво и не прави разлика между класовете услуги.



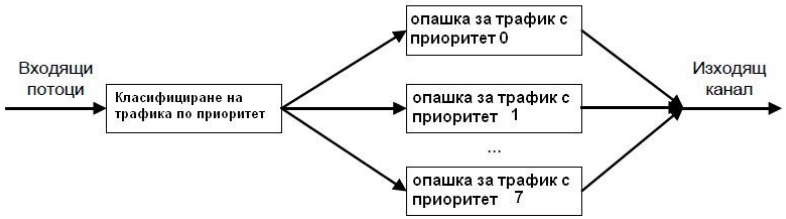
Low Latency Queuing (LLQ)

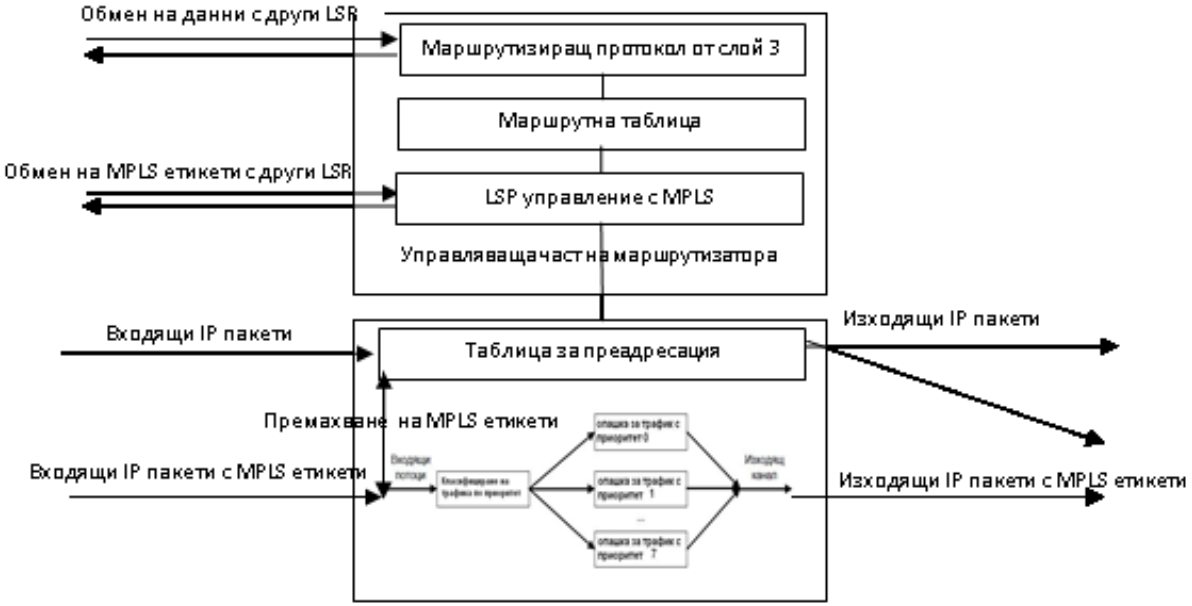
- Функцията за опашка с ниска латентност (LLQ) носи строг приоритет на опашка (PQ) към CBWFQ.
- Строгият PQ позволява чувствителни към забавяне пакети, като глас, да бъдат изпратени преди пакети в други опашки.
- LLQ дава преференциално третиране на чувствителните към забавяне пакети спрямо друг трафик.
- Например, Cisco препоръчва само гласовият трафик да се насочва към приоритетната опашка.



Пример: CBWFQ в MPLS

- В MPLS – 8 класа, но в рутера постъпва и не-MPLS трафик

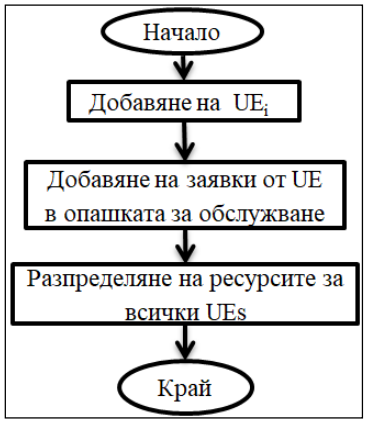




Пример: CBWFQ в LTE

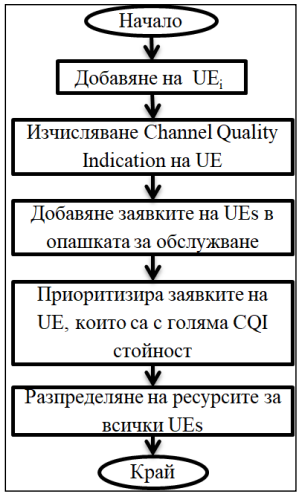
Dedicated Bearer		Default Bearer
Non-GBR	GBR	Non-GBR
QCI 5-9	QCI 1-4	QCI 5-9
APN-AMBR	GBR	APN-AMBR
UE-AMBR	MBR	UE-AMBR
TFT	TFT	APN
ARP	ARP	IP Address
L-EBI	L-EBI	ARP

QCI	Bearer Type	Priority	Delay of the Packet	Packet Loss	Example of Traffic Type
1	GBR	2	100ms	10^{-2}	VoIP
2		4	150ms	10^{-3}	Video call
3		3	50ms	10^{-3}	Real time games
4		5	300ms	10^{-6}	Video streaming
5	Non-GBR	1	100ms	10^{-6}	IMS Signaling
6, 8, 9		6, 8, 9	300ms	10^{-6}	TCP based services – chat, ftp
7		7	100ms	10^{-3}	Voice, video, interactive games

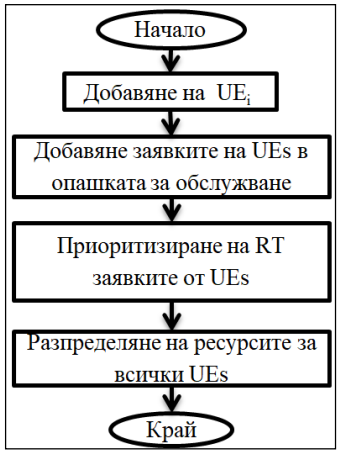


Алгоритми: RR

Max-rate

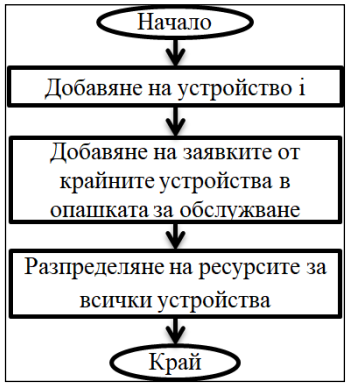


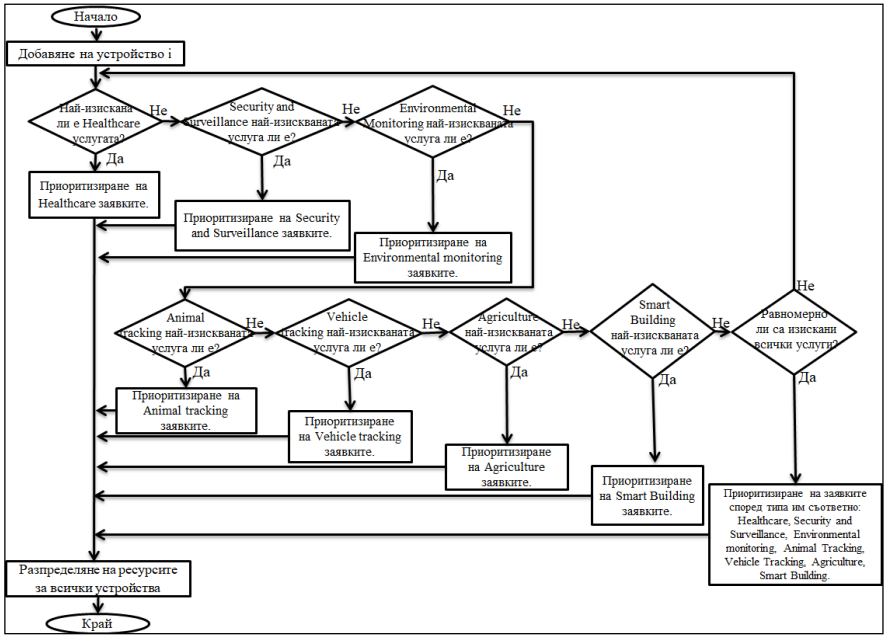
Proportional Fair

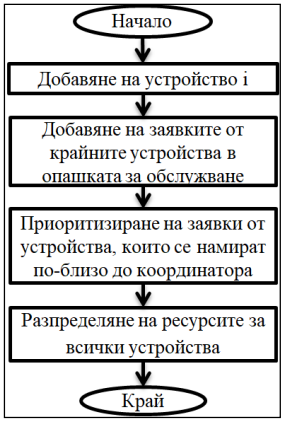


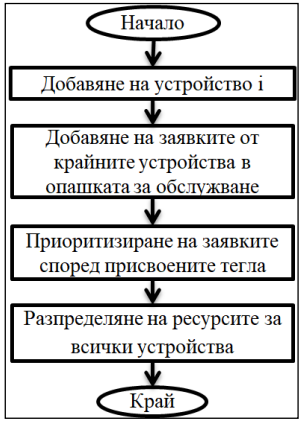
Exponential/Proportional Fair

Пример: CBWFQ в 6loWPAN









Алгоритми:

Knowledge Free -First Come First Served (FCFS)

Knowledge based

Knowledge of Network-Least Number of Hops First (LNHF) и
Least Weighted Farthest Number Distance Product First (LWFNDPF)

QoS модели

- Има три модела за внедряване на QoS.
- Понякога QoS се реализира в мрежа, използвайки IntServ или DiffServ съвместно.
  - Best-effort model
  - Integrated services (IntServ) - осигурява най-високата гаранция за QoS, той е много ресурсоемък и следователно не е лесно мащабируем.
  - Differentiated services (DiffServ) - е по-малко ресурсоемък и по-мащабируем.

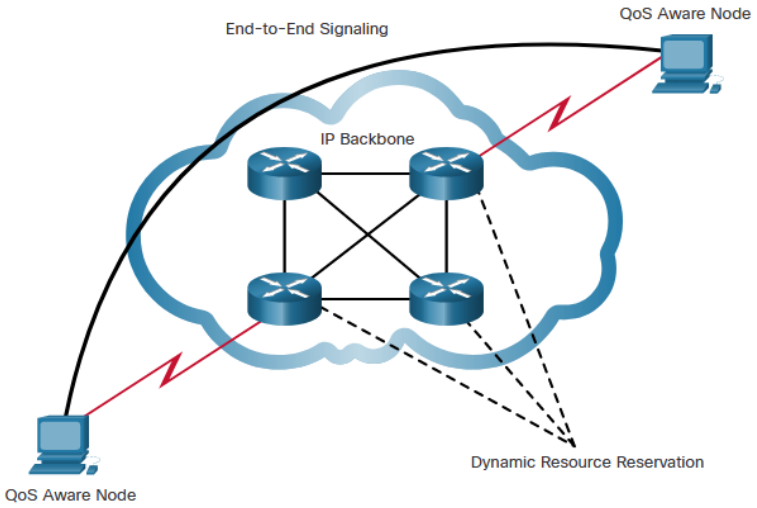
Модел	Характеристики
Best-effort model	• Не е реализация, тъй като QoS не е изрично конфигуриран. • Използва се когато QoS не се изисква.
Integrated services (IntServ)	• Осигурява много високо QoS към IP пакети с гарантирана доставка. • Дефинира процес на сигнализиране за приложения, които да сигнализират към мрежата, че изискват специално QoS за определен период и че честотната лента трябва да бъде запазена. • IntServ може сериозно да ограничи мащабируемостта на мрежата.
Differentiated services (DiffServ)	• Осигурява висока мащабируемост и гъвкавост при внедряване на QoS. • Мрежовите устройства разпознават класове трафик и предоставят различни нива на QoS за различните класове трафик.

Best Effort модел

- Основният дизайн на Интернет е доставка на пакети best effort и не предоставя никакви гаранции.
- Моделът best effort третира всички мрежови пакети по един и същ начин.

Предимства	Недостатъци
Моделът е най-мащабируемият.	Няма гаранции за доставка.
Мащабируемостта е ограничена само от наличната честотна лента, така целият трафик е еднакво засегнат.	Пакетите ще пристигнат винаги, когато могат и във всеки възможен ред, ако въобще пристигнат.
Не се изискват специални механизми за QoS.	Няма пакети с преференциално третиране.
Това е най-лесният и бърз модел за внедряване.	Критичните данни се третират по същия начин, както всички данни.

Модел Integrated Services



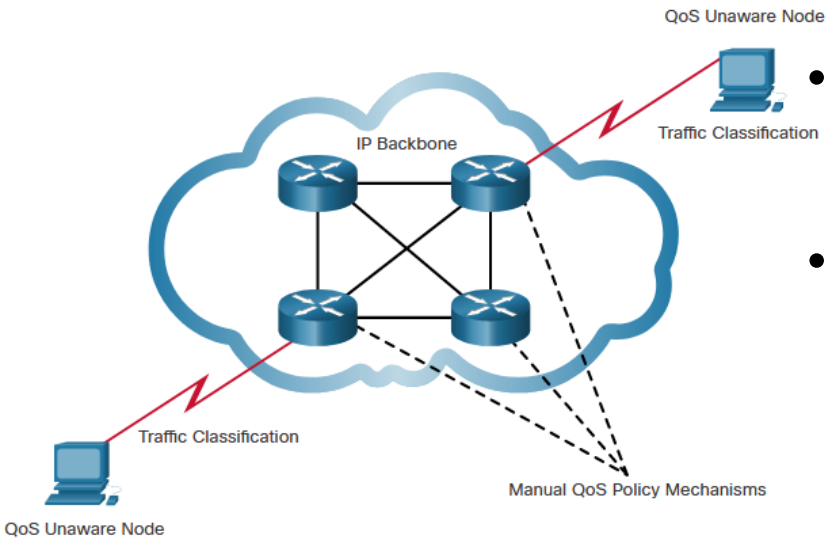
- IntServ предоставя QoS от край до край, което изискват приложенията в реално време.
- Управлява мрежовите ресурси, за да осигури QoS на отделни потоци, понякога наричани микропотоци.
- Използва механизми за резервиране на ресурси и контрол на достъпа като градивни елементи за установяване и поддържане на QoS.
- Използва подход, ориентиран към връзката.
- Всяка отделна комуникация трябва изрично да посочи своя дескриптор на трафика и исканите ресурси към мрежата.
- Крайният рутер извършва контрол на достъпа, за да гарантира, че наличните ресурси са достатъчни в мрежата.

Модел Integrated Services

- В модела IntServ приложението изисква специфичен вид услуга от мрежата, преди да изпрати данни.
- Приложението информира мрежата за своя профил на трафик и изисквания за честотна лента и забавяне.
- IntServ използва протокола за резервиране на ресурси Resource Reservation Protocol (RSVP), за да сигнализира за нуждите за QoS от устройствата по пътя от край до край през мрежата.
  - Ако мрежовите устройства по пътя могат да резервират необходимата честотна лента, приложението може да започне да предава.
  - Ако заявената резервация се провали по пътя, приложението не изпраща никакви данни.

Предимства	Недостатъци
• Изричен контрол за достъп до ресурси от край до край • Контрол на допускане на правила за заявка • Сигнализиране на динамични номера на портове	• Ресурно интензивен поради изискването за архитектура за непрекъснато сигнализиране. • Подход, базиран на поток, не може да се мащабира до големи реализации като Интернет.

Модел Differentiated Services



- Моделът за QoS на диференцирани услуги (DiffServ) определя прост и мащабируем механизъм за класифициране и управление на мрежовия трафик.
- Не е QoS стратегия от край до край, защото не може да наложи гаранции от край до край.
- Приема препращане на трафик към рутер, който класифицира потоците в агрегати (класове) и осигурява подходящата QoS политика за класовете.
- Налага и прилага QoS механизми на база хоп-по-хоп, като равномерно прилага глобалното значение към всеки клас трафик, за да осигури както гъвкавост, така и мащабируемост.

Модел Differentiated Services

- DiffServ разделя мрежовия трафик на класове въз основа на бизнес изискванията.
- След това на всеки от класовете може да бъде присвоено различно ниво на обслужване.
- Докато пакетите преминават през мрежата, всяко от мрежовите устройства идентифицира класа на пакета и обслужва пакета според този клас.
- Възможно е да се изберат много нива на обслужване с DiffServ.

Предимства	Недостатъци
• Силно мащабируем • Осигурява много различни нива на качество	• Няма абсолютна гаранция за качество на услугата • Изисква набор от сложни механизми за съвместна работа в цялата мрежа

Техники за внедряване на QoS - за избягване на загуба на пакети

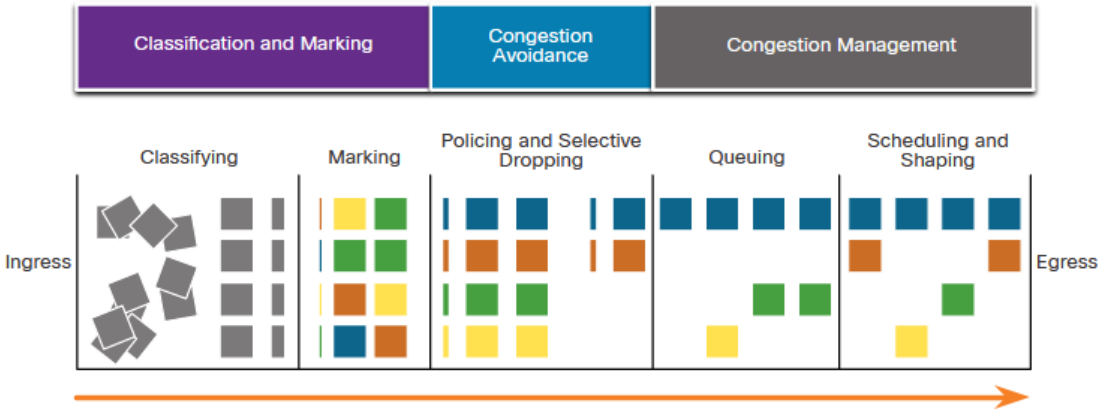
- Загубата на пакети обикновено е резултат от претоварване на интерфейс.
- Повечето приложения, които използват TCP имат забавяне, тъй като TCP автоматично се настройва към претоварването на мрежата. Изпуснатите TCP сегменти карат TCP сесиите да намалят размера на прозорците си.
- Някои приложения не използват TCP и не могат да се справят с отхвърлените пакети.
- Следните подходи могат да предотвратят спадове в чувствителни приложения:
  - Увеличаване капацитета на връзката.
  - Гарантиране на достатъчно честотна лента и увеличаване на буферното пространство, за да се поемат пиковете на трафик от чувствителните потоци.
  - Опашките WFQ, CBWFQ и LLQ могат да гарантират честотна лента и да осигурят приоритетно препращане към приложения, чувствителни към загуби.
  - Пуснете пакетите с по-нисък приоритет, преди да настъпи претоварване.
  - Например, Cisco IOS QoS предоставя механизми за опашка, като претеглено произволно ранно откриване (WRED), които започват да отхвърлят пакети с по-нисък приоритет, преди да настъпи претоварване.

Техники за внедряване на QoS - QoS Tools

QoS Tools	Характеристики
Инструменти за класификация и маркиране	• Сесиите или потоците се анализират, за да се определи към кой клас трафик принадлежат. • Когато се определи класът на трафика, пакетите се маркират.
Инструменти за избягване на задръствания	• За класовете трафик са разпределени части от мрежови ресурси, както е дефинирано от QoS политиката. • Политиката за QoS също така идентифицира как част от трафика може да бъде селективно пропусната, забавена или премаркирана, за да се избегнат задръстванията. • Основният инструмент за избягване на претоварване е WRED и се използва за регулиране на трафика на TCP данни по ефективен за честотната лента начин, преди да възникнат загуби, причинени от препълване на опашката.
Инструменти за управление на задръстванията	• Когато трафикът надвишава наличните мрежови ресурси, се поставя в опашка, за да изчака наличието на ресурси. • Например, Cisco IOS включва алгоритми CBWFQ и LLQ.

Техники за внедряване на QoS - QoS Tools

- Класификацията и маркирането могат да се извършват при влизане или излизане от устройството, докато опашки и шейпинг обикновено се извършват при излизане на трафика.
- Входящите пакети са класифицирани и съответното им IP заглавие е маркирано.
- За да се избегне претоварване, за пакетите след това се разпределят ресурси въз основа на определени политики.
- След това пакетите се поставят на опашка и се препращат през изходния интерфейс въз основа на тяхната дефинирана политика за оформяне и контрол на QoS.



Класификация и маркиране

- Преди пакетът да може да има QoS политика, приложена към него, пакетът трябва да бъде класифициран.
- Класификацията определя класа трафик, към който принадлежат пакетите или кадрите.
- Само след като трафикът е маркиран, към него могат да се прилагат правила. Как се класифицира пакетът зависи от изпълнението на QoS.
- Методите за класифициране на трафик потоци на слой 2 и слой 3 включват използване на интерфейси, ACL и класове.
- Трафикът може също да бъде класифициран на слоеве от 4 до 7 с помощта на мрежово разпознаване на приложения Network Based Application Recognition (NBAR).

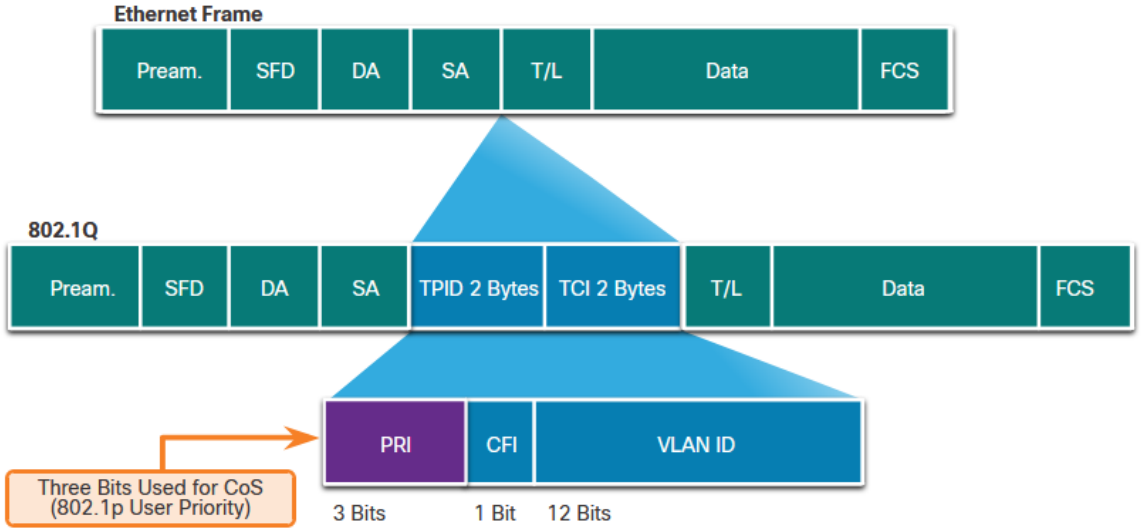
Класификация и маркиране

- Как се маркира трафикът обикновено зависи от технологията.
- Решението дали да се маркира трафик на слой 2 или слой 3 (или и двата) не е тривиално и трябва да се вземе така:
  - Маркирането на Слой 2 - маркиране на кадри може да се извърши за не-IP трафик. Това е единствената опция за QoS, налична за комутатори, които не са „наясно с IP“.
  - Маркирането на Слой 3 - ще носи QoS информацията от край до край.

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

Маркиране на Слой 2

- 802.1Q е стандартът IEEE, който поддържа VLAN маркиране на слой 2 в Ethernet мрежи. Когато се внедри 802.1Q, две полета се вмъкват в Ethernet рамката след полето за MAC адрес на източника.



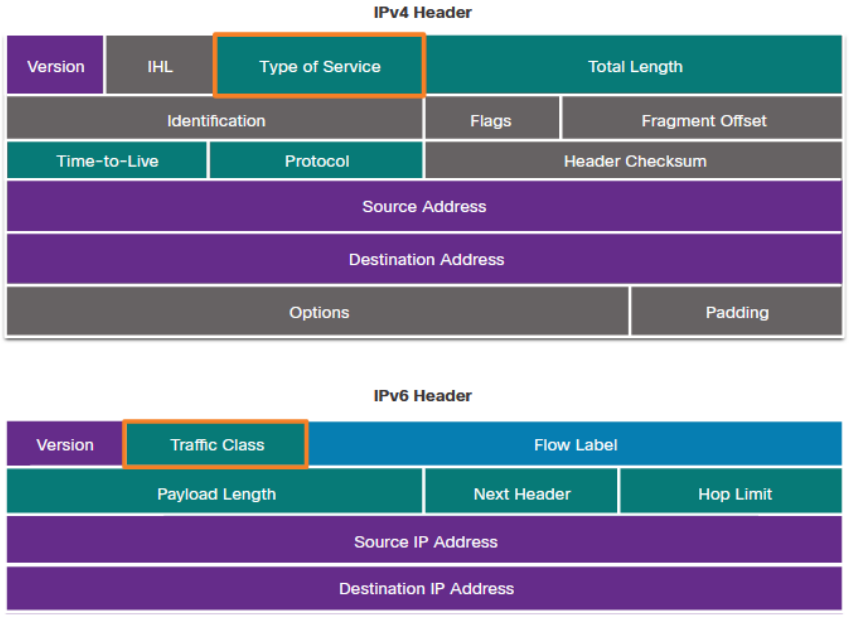
Маркиране на Слой 2

- Стандартът 802.1Q включва и схемата за приоритизиране на QoS, известна като IEEE 802.1p.
- Стандартът 802.1p използва първите три бита в полето Tag Control Information (TCI). Известно като поле за приоритет (PRI), това 3-битово поле идентифицира маркировките за клас на услугата (CoS). Три бита означават, че Ethernet кадъра от слой 2 може да бъде маркиран с едно от осемте нива на приоритет (стойности 0-7).

CoS Value	CoS Binary Value	Description
0	000	Best-Effort Data
1	001	Medium-Priority Data
2	010	High-Priority Data
3	011	Call Signaling
4	100	Videoconferencing
5	101	Voice bearer (voice traffic)
6	110	Reserved
7	111	Reserved

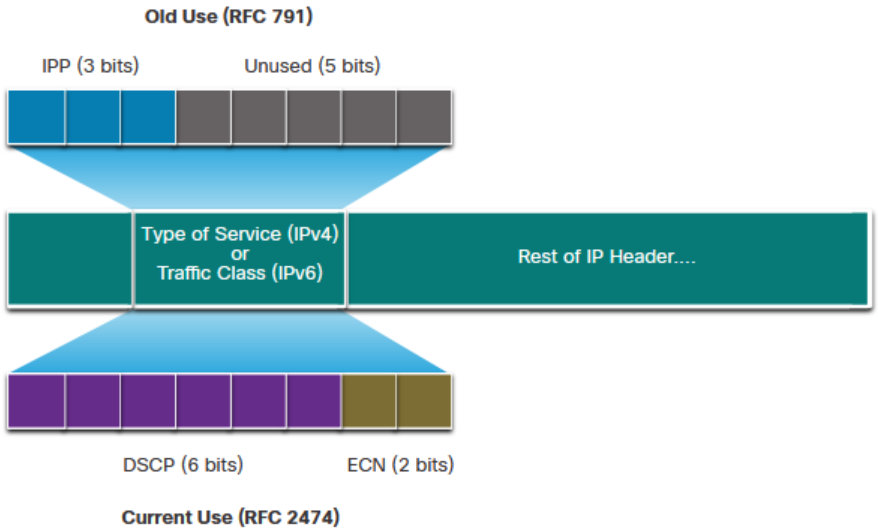
Маркиране на Слой 3

- IPv4 и IPv6 определят 8-битово поле в хедърите на своите пакети, за да маркират пакетите - полето Type of Service за IPv4 и полето Traffic Class за IPv6.



Полетата Type of Service и Traffic Class

- Типът на услугата (IPv4) и класът на трафика (IPv6) носят маркирането на пакета.
- RFC 791 посочи полето за 3-битов IP приоритет (IPP), което да се използва за QoS маркиране.
- RFC 2474 замества RFC 791 и предефинира полето на ToS чрез преименуване и разширяване на IPP полето до 6 бита- поле на кодова точка на диференцирани услуги (DSCP), тези шест бита предлагат максимум 64 възможни класа услуги. Останалите два бита за IP Extended Congestion Notification (ECN) могат да се използват от рутери за маркиране на пакети, вместо да ги отхвърлят.



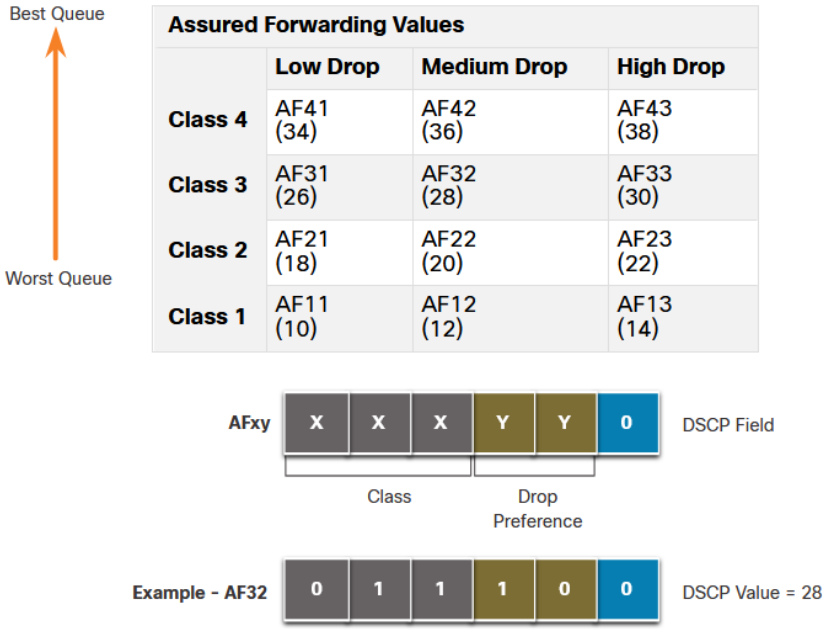
Полето DSCP

64-те възможни DSCP стойности са организирани в три категории:

- **Best-Effort (BE)** – Това е по подразбиране за всички IP пакети. DSCP = 0. Поведението е нормално маршрутизиране. При претоварване тези пакети ще бъдат отхвърлени от рутера. Не се прилага план за QoS.
- **Expedited Forwarding (EF)** – ускорено препращане- RFC 3246 дефинира EF като DSCP = 46 (двоично 101110). Първите 3 бита (101) се съпоставят директно със стойността на CoS на слой 2 – стойност 5, използвана за гласов трафик. На слой 3 EF се препоръчва да се използва само за маркиране на гласови пакети.
- **Assured Forwarding (AF)** - Осигурено препращане – RFC 2597 дефинира AF да използва 5-те най-младши DSCP бита за указване на опашки и предпочитание за отпадане.

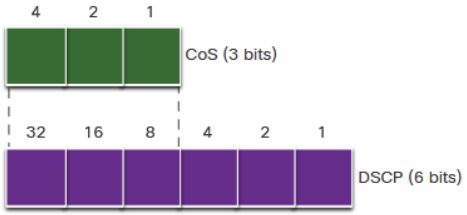
Полето DSCP

- Формулата AFxy е :
  - Първите 3 бита се използват за обозначаване на класа. Клас 4 е най-добрата опашка, а клас 1 е най-лошата опашка.
  - 4-ти и 5-ти битове се използват за обозначаване на предпочитанието за отхвърляне.
  - Шестият бит е нула.



Битове за избор на клас (CS)

- Първите 3 бита от полето DSCP и показват класа.
- Мапват се директно към 3-те бита на полето CoS и полето IPP, за да се поддържа съвместимост с 802.1p и RFC 791.

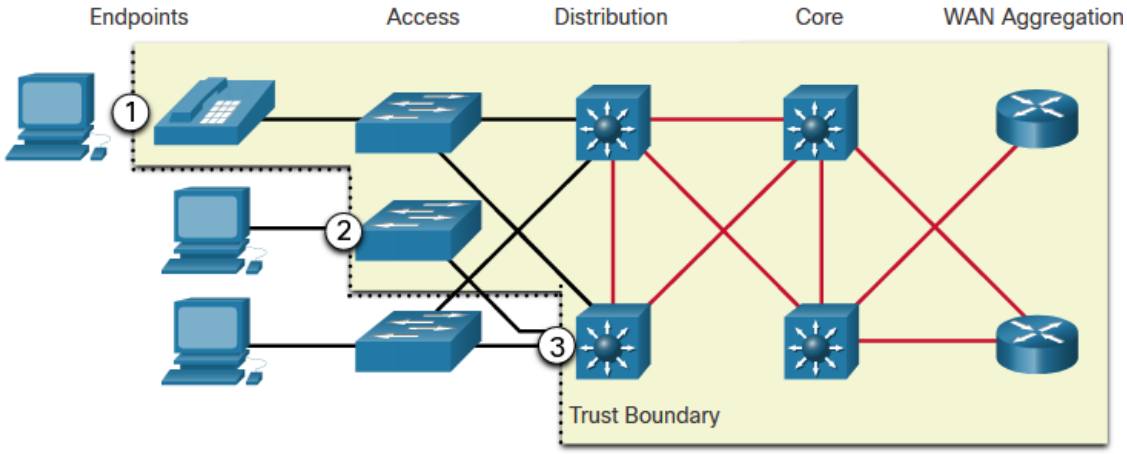


CoS values, Class Selectors, and corresponding DSCP 6-bit value

CoS Value	CoS Binary Value	Class Selector (CS)	CS Binary	DSCP Decimal Value
0	000	CS0*/DF	000 000	0
1	001	CS1	001 000	8
2	010	CS2	010 000	16
3	011	CS3	011 000	24
4	100	CS4	100 000	32
5	101	CS5	101 000	40
6	110	CS6	110 000	48
7	111	CS7	111 000	56

Граници на доверие

- Трафикът трябва да бъде класифициран и маркиран възможно най-близо до неговия източник, колкото е технически и административно осъществимо.
- Това определя границата на доверие.
- Доверените крайни точки имат възможностите и интелигентността да маркират трафика от приложенията към подходящите стойности на CoS на слой 2 и/или DSCP на слой 3.
- Сигурните крайни точки могат да имат маркиран трафик на суича на слой 2. Трафикът може да бъде маркиран и на комутатори/рутери на слой 3.

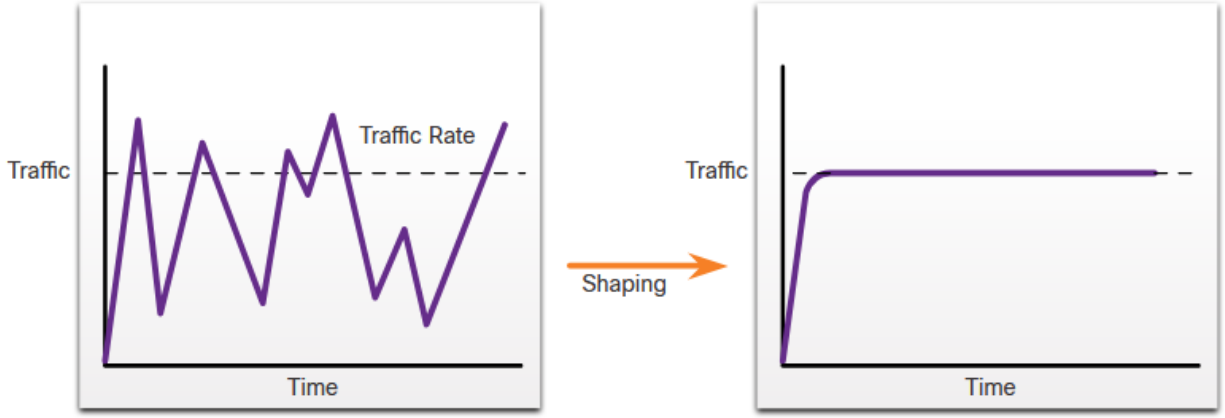


Избягване на задръствания

- Инструментите за избягване на задръстванията наблюдават натоварванията на мрежовия трафик в опит да предвидят и избегнат задръстванията в общите тесни места в мрежата преди претоварването да се превърне в проблем.
- Те следят средната дълбочина на опашката.
  - Когато опашката е под минималния праг, няма загуби.
  - Когато опашката се запълва до максималния праг, малък процент от пакетите отпадат.
  - Когато се премине максималният праг, всички пакети се отхвърлят.
- Някои техники за избягване на претоварване осигуряват преференциално третиране, за което пакетите се отхвърлят.
  - Претегленото произволно ранно откриване Weighted random early detection (WRED) позволява избягване на претоварване на мрежовите интерфейси, като осигурява управление на буфера и позволява на TCP трафика да се намали преди буферите да бъдат запълнени.

Shaping на изходящ трафик

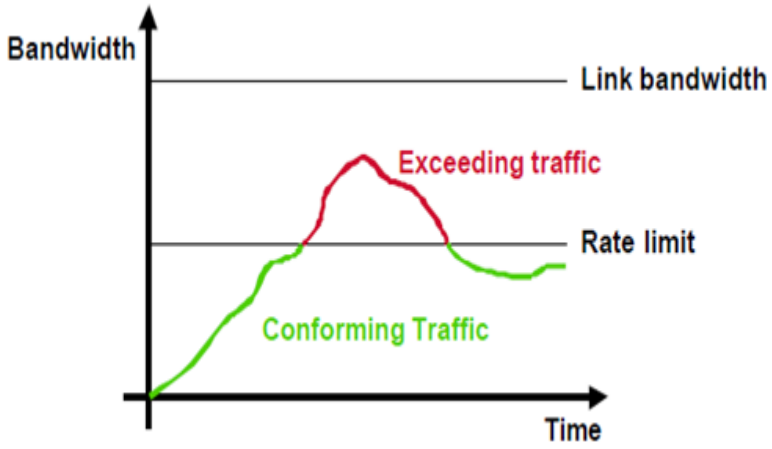
- Shaping- Оформянето на трафика е механизъм за предотвратяване на задръствания.
- Оформянето на трафика задържа излишните пакети в опашка и след това планира излишъка за по-късно предаване на стъпки от време.
- Оформянето на трафика води до равномерна изходяща скорост на пакетите.
- Оформянето е за изходящ трафик: пакетите, излизащи по интерфейса, се поставят в опашка и могат да бъдат оформени.

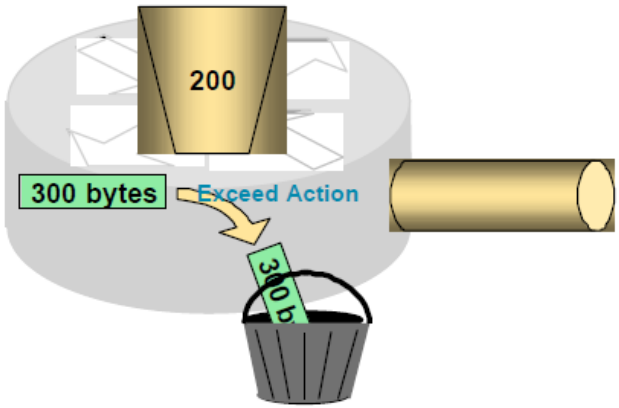


Policing на входящ трафик

- Уоравлението (Policing) се прилага към входящия трафик на интерфейса.
- Policing се прилага от доставчиците на услуги, за да се наложи договорен процент на информация за клиентите (CIR). Въпреки това, доставчикът на услуги може също да разреши надхвърляне на CIR, ако мрежата на доставчика на услуги в момента не изпитва задръствания.

Пример: Frame Relay – Token bucket





•Регулира данновия поток и има 2 компоненти:

- **n Tokens**: всеки token представя позволение за изпращане на фиксиран брой битове по мрежата
- **n The bucket**: има капацитет от няколко tokens

•Tokens се слагат в “кофата” от операционната система. Всеки влизащ пакет ако се препраща, взема tokens от “кофата”, в зависимост от размера на пакета:

- Ако “кофата” запълни капацитета си, новопристигналите токени се отхвърлят и са недостъпни за бъдещи пакети.
- Ако няма достатъчно токени в “кошницата”, за да изпратят пакетите, регулатора може да:
  - Изчака за достатъчно (traffic shaping)
  - Да отхвърли пакета (policing)

Правила за QoS

- QoS политиките трябва да вземат предвид пълния път от източника до дестинацията.
- Идеи:
  - Активира се опашката на всяко устройство по пътя между източника и дестинацията.
  - Класифицира се и се маркира трафика възможно най-близо до източника.
  - Shape и police на трафика се прилагат възможно най-близо до източника.

Въпроси ?

Благодаря за вниманието !