QoS Concepts

# Network transmission quality

Om de optimalisattie van het netwrk van lethas te kunnen doen, is er een onderzoek nodig met als resultaat een stapenplan en strategie. Om dit mogelijk te maken heeft een professional toegang tot informatiebronnen om best practises te bestuderen[[1]](#footnote-1).

## Verkeer Prioriteiten geven

Qos zorgt ervoor dat we voorrang geven aan verschillende verkeersoorten. QoS wordt steeds belangrijker door de nieuwe voice en videoapplicaties. Voice- en videogebruikers verwachten en steeds hoger kwaliteit.

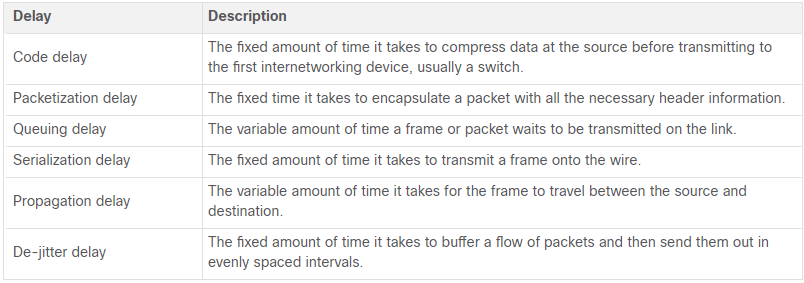
Qos is nodig op plaatsen in het netwerk waar opstopping kan plaats vinden.

* Aggregation : Wanneer verkeer van meerder kabels informatie moeten vervoeren door een router of switch, en uitkomen in een kabel. Waardoor er een opstopping gebeurt.
* Speed Mismatch: wanner een informatie vervoerd wordt vanuit een hoge snelheid link en aan de andere kant van de routers is een trage link. Bv: van 1000Mbps naar 100Mbps
* Lan-To-Wan: Wanneer verkeer van een gateway router van het ene netwerk naar het andere netwerk gaat.

Wanneer de verkeer groter is dan wat er beschikbaar is in het netwerk dan houdt de toestel de pakketten in geheugen tot ze verstuurd kunne worden. De pakketten worden dan in een wachtrij  
(queuing) gezet, dit zorgt voor vertraging(delay) omdat nieuwe pakketten pas kunnen gaan wanner de wachtrij leeg is. Wanneer het geheugen van het toestel vol is dan worden pakketjes gedropt. Een QoS oplossing hiervoor is de verschillende data classificeren in meerdere wachtrijen.

## Delay and Jitter

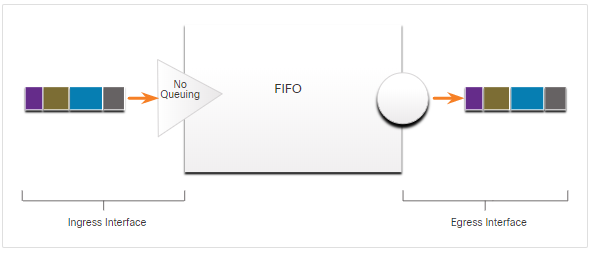
Tijd die een pakket neemt van om van de verstuurder maar de ontvanger te gaan heet Delay of Jitter. Er zijn twee soorten delay’s, vaste delay en wisselend delay. Een vaste delay is een specifieke hoeveelheid tijd die een proces in beslag neemt. Een wisselend delay duurt een onbepaalde tijd en wordt beïnvloed door factoren zoals hoeveel verkeer wordt verwerkt.



# Queuing Algoritme

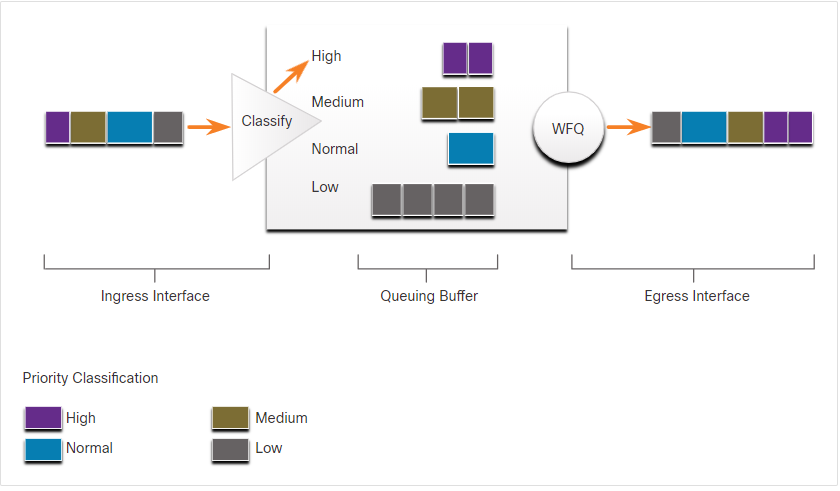
## First in First out (FIFO)

Dit is de eenvoudigste form van queuing. De pakketten worden in hetzelfde volgorde naar buiten gestuurd. Bij FIFO kan belangrijk en tijdsgevoelige verkeer gedropt worden bij een opstopping van de interface. FIFO is de snelste methode van queuing en wordt best gebruikt bij een grote link of een link met zeer weinig opstoppingen.



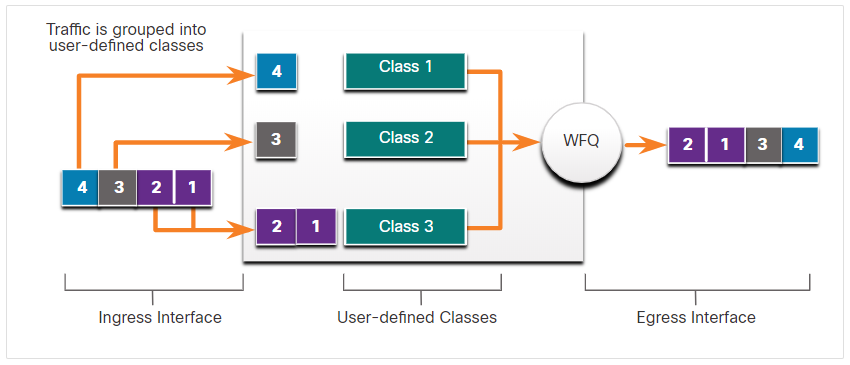
## Weighted Fair Queuing (WFQ)

In komende verkeer wordt geclassificeerd en afhankelijk van de classificatie krijgen ze een prioriteitsniveau. Het verkeer met hoogste prioriteit mag eerst door. Elke inkomende pakket krijgt een prioriteit. Dit zorgt ervoor dat de volledige bandbreedte eerlijk verdeeld wordt tussen het verschillende verkeer in het netwerk. WFQ zet het verkeer in verschillend soort afhankelijke van de Type of Service (TOS). De ToS gegevens in de IP-header wordt gebruikt om deze classificaties te maken. WFQ zorgt ervoor dat kleine interactieve verkeer zoals Telnet sessie en voice een hogere prioriteit krijgen dan grote verkeer zoals een ftp-sessie.



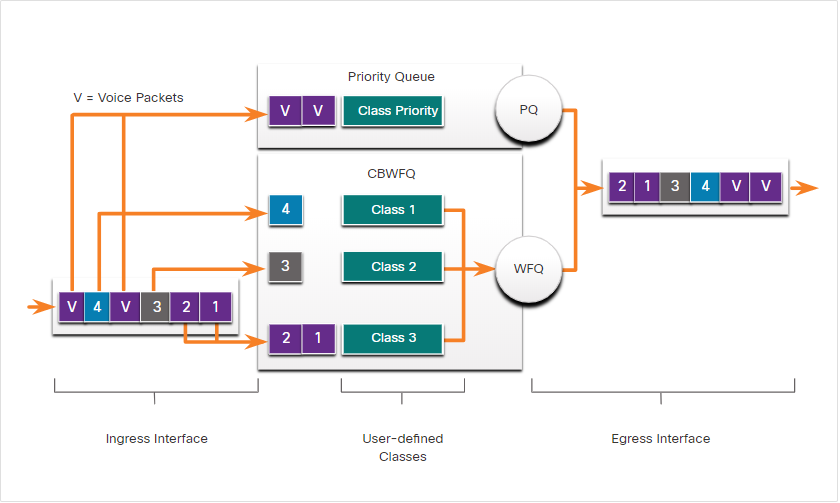
## Class-Based Weighted Fair Queuing

Dit is een verlenging van de WFQ. Hier moet gebruiker de verschillende klassen van het netwerkverkeer definiëren, doormidden van protocollen, Access control lists (ACLs)en de input interface. Elke class heeft zijn eigen FIFO-wachtrij. Elk class heeft zijn een paar karaktereigenschappen die geconfigureerd moeten worden. De karaktereigenschappen bandbreedte, weight en max pakketten in de wachtrij.



## Low Latency Queuing (LLQ)

LLQ zorgt ervoor dat er een extra priority Queuing bij de CBWFQ. Hiermee kunnen we specifieke ervoor zorgen dat belangrijke en tijdgevoelige verkeer zoals Voice eerst gestuurd wordt.



# Qos Models

## Best-Effort Model

Het internet gaat zijn best doen om het pakket te versturen, maar er zijn geen garanties. Dit behandelt alle pakketten in het verkeer hetzelfde. Zonder Qos kan het netwerk de verschillende pakketten niet uit elkaar halen.

### Voordelen

* Model kan vergroot worden.
* Scalability is beperkt door de beschikbare bandbreedte.
* Geen speciale QoS mechanismen nodig
* Het is de gemakkelijkste en de snelste die ingezet kunnen worden.

### Nadelen

* Geen garantie voor de levering
* Levering van de pakketten zullen gebeuren wanneer het mogelijk is.
* Pakketten hebben geen preferentieel behandeling.
* Gevoelig en tijdsgevoelige data zullen hetzelfde behandeld worden als een afbeelding

## Integrated Services (IntServ)

Deze model is specifiek gemaakt voor de behoeften van de Real-Time Applicaties. Een applicatie stuurt een request van het netwerk voor een speciefiek service. De applicatie informeert het netwerk over zijn verkeersprofiel en vraagt om een bepaalde service die de vereisten bandbreedte en delay heeft. IntServ stuurd Resource Reservation Protocol (RSVP) naar de toestellen in het netwerk. Wanneer zij de nodige bandbreedte en delay kunnen reserveren, dan kan de applicatie beginnen te versturen.

### Voordelen

* Controle of er genoeg Resource zijn om de taak van begin tot eind af ter werken
* Er wordt altijd een request gestuurd voor een taak.
* Betere Qos voor Real-Time verkeer
* Classificatie voor pakketten
* Queuing

### Nadelen

* Veel middelen nodig, doordat er continue signalen gestuurd wordt.
* Geen grote uitbreidingen mogelijkheden.

## Differentiated Services (DiffServ)

Elke pakket wordt gemarkeerd voordat ze het netwerk binnen komen, deze markering wordt gedaan op basis van verkeerstype. Het netwerk gebruikt die markering om te weten hoe het pakket behandeld moet worden. Dit betekent ook dat elke netwerk device de nodige vereisten aan, Dit is geen end-to-end Qos Strategie.

### Voordelen

* Veel mogelijkheden voor uitbreiding
* Bied verschillende QoS aan

### Nadelen

* Geen Garantie voor de QoS.
* Heeft complexe mechanismen nodig om te functioneren in het netwerk

# Qos implemtation techniques

## Packet loss

Dit gebeurt meestal omdat er een opstopping is bij de interface. Om ervoor te zorgen dat pakketten niet gedropt worden kunnen de volgende oplossingen toegepast worden.

* Verhoog de capaciteiten van de link, om opstopping te verminderen of te vermijden.
* Zorg ervoor dat er genoeg bandbreedte en buffer om de plotselinge verhogingen, die veroorzaak worden door bepaalde gevoelige verkeer. WFQ, CBWFQ en LLQ kan helpen bij het reserveren van bandbreedte en prioriteiten geven aan bepaalde verkeerstypes.
* Het droppen van pakketten met lage prioriteit voordat er een opstopping gebeurt. Cisco IOS QoS heeft een queuing mechanisme die zulke handelingen doen. Bv: Weightrd Random Early Detection (WRED)

## QoS Tools

### Tool For implementing

#### Classification and marking tools

* Sessies en datestromen worden geanalyseerd om te bepalen tot welke verkeersklasse ze behoren
* Wanner de klasse bepaald is worden ze gemarkeerd.

#### Congestion avoidance tools

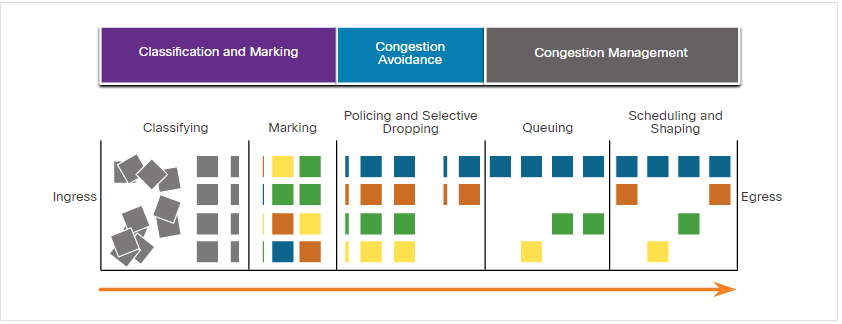
* Verkeersklassen krijgen netwerkbronnen toegewezen.
* Sommige verkeer worden gedropt, vertraagt of opnieuw gemarkeerd on opstopping te vermijden.
* WRED regelt zo efficiënt mogelijk de TCP-verkeer om drops te vermijden

#### Congestion management tools

* Wanneer de beschikbare netwerkbronnen overschreden worden, word het netwerkverkeer in een wachtrij gezet totdat er bronnen vrijkomen.
* Congestion-management tools bevatten CBWFQ en LLQ-algoritmes

### SoQ Sequence

Pakketten die binnenkomen worden geclassificeerd en hun IP-headers gemarkeerd. Dit zorgt ervoor dat ze in een bepaalde verkeersklasse gezet worden. Bij de 2de sectie krijgen pakketten verkeersbronnen gebaseerd op hun verkeersklassen. Pakketten met lage prioriteiten worden gedropt om opstopping te vermijden. Bij de laatste deel worden pakketten in wachtrij gezet en verstuurd via de exit interface.

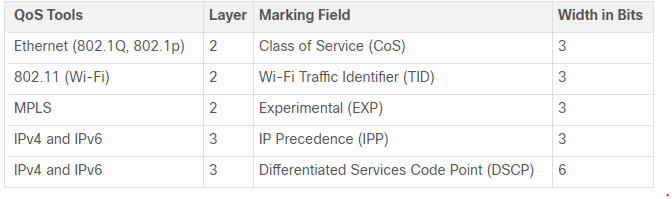


## Classification and marking

Classificatie en markering zorgt ervoor dat de pakketten in klassen gezet worden en dan gemarkeerd worden. Hierdoor kunne de pakketten geïdentificeerd worden en ze onderscheiden tussen de verschillende verkeerstypes. Hierna kunne de verschillende polities toegepast worden. Bij de

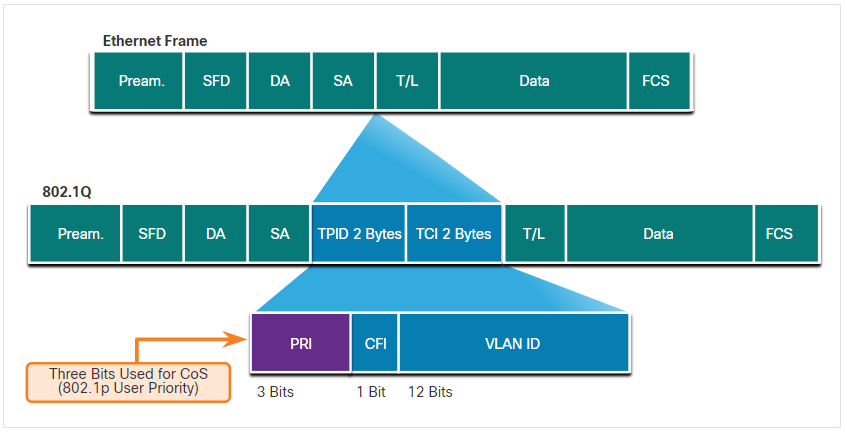
De classificatie methode is afhankelijk van de QoS implementatie. Op de Layer 2 en 3 niveau via Interface, ACL en Class-Maps. Op Layer 4 tot 7 Via Network Based Application Recognition(NBAR)

Markering van pakketten worden extra waardes toegevoegd aan de IP-Header.

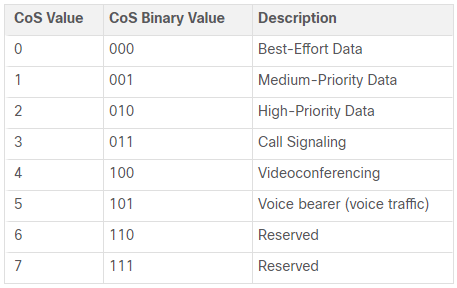


## Marking at Layer 2

802.1q is de IEEE-standard voor VLAN tagging op de Layer 2. De 802.1q heeft een QoS prioriteit schema genaamd 802.1P. 802.1p gebruikt de eerste 3 bits in de Tag Controle Information (TCI), deze heten Priority (PRI) field.

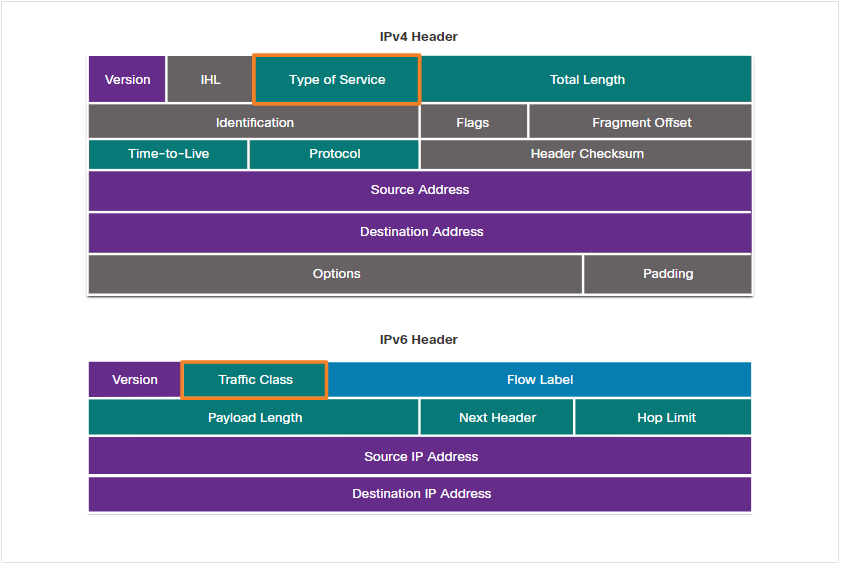


De 3 bits in de PRI kunne gebruikt worden voor Class Of Service (COS) markeringen. De 3 bits waarden komt gelijk aan een van de acht niveau prioriteiten.



## Marking at Layer 3

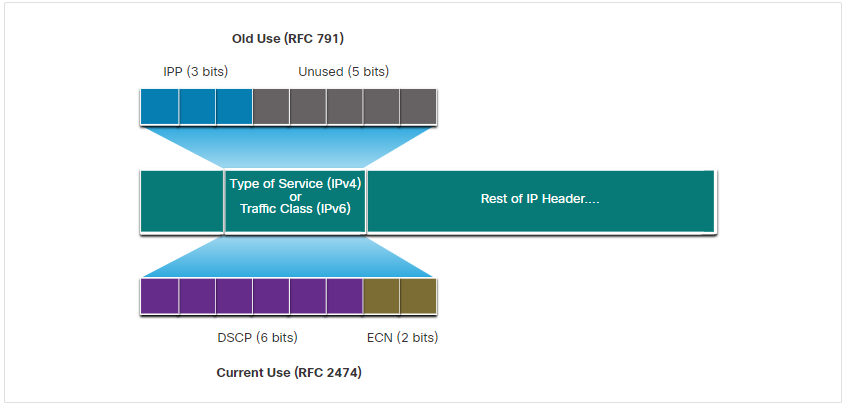
In de ipv4 en ipv6 pakket header is er een 8-bits field die gebruikt wordt om pakketten te markeren. Dat zijn de Type os Service (ToS) en Traffic Class.



## Type of Service and Traffic Class Field

De Tos en TC hebben de pakket markeringen, die bestaan uit 8 bits. De eerste 3-bits daarvan heet de IP Precedent maar, dit werd eerst gebuikt op de priotiy value te geven. O tot 7 maar 6 en 7 mag niet gebuikt worden. om gedetaileerderr te zijn gebruiken we de 6 eerste bits(Differentiated Services Code Point **DSCP**), nu hebben we 64 mogelijke class services.

Per-Hub Behavior(**PHB** ) zijn de waardes die de IETF gegeven heeft aan de gekozen 21 van de 64 service classes. De PHB worden verdeeld in 4 delen. Default, Expedited Forwoarding(EF), Class Selector (CS), Assured Fowarding(AF)

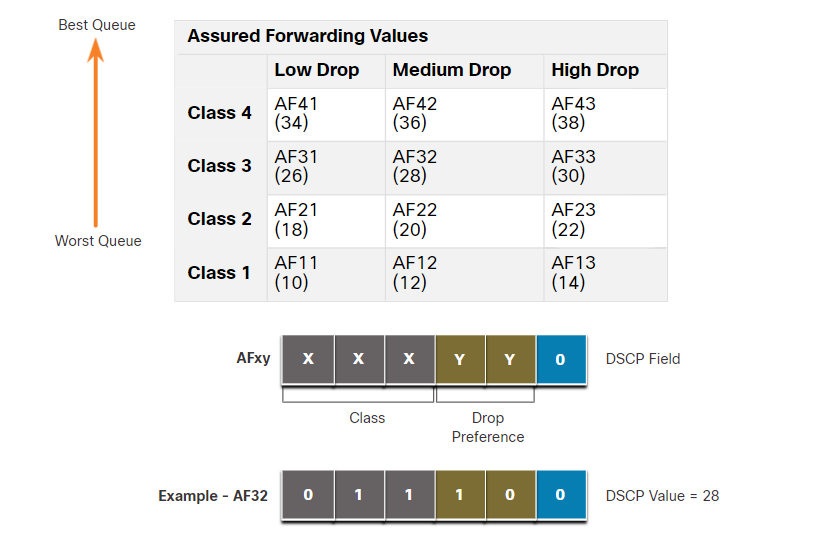


DSCP Values

**Best-Effort (BE)**: Dit is de default. De DSCP-waarden is 0, hier wordt geen QoS gedaan. Pakketten met deze waarden worden direct gedropt.

**Expedited Forwarding** (EF): EF heeft een waarden van 0, Ef wordt alleen gebruikt voor voice pakketten.

**Assured Forwarding(AF):**gebruikt de 5 eerste bits voor wachtrij en drop preference aan te duiden**.**

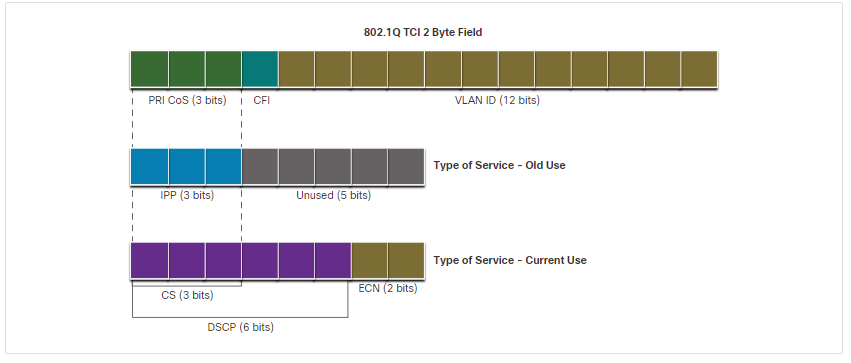


* De eerste 3 bits wordt gebruikt om de class aan te geven. Class 4 is de beste wachtrij en class 1 is het ergste.
* Bits 4 en 5 worden gebruik om de *drop preference* aan te geven.
* Bit 6 is altijd 0

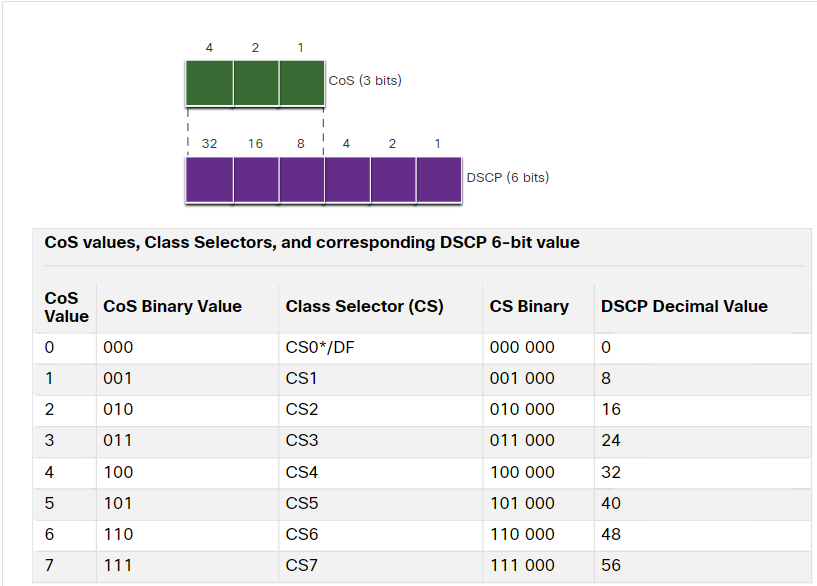
Bv: AF32🡪 hoort in class 3(binair 011) en zijn drop preference is op Meduim(binair 10)de volledige DSCP waarde is 28(binair 011 10 0).

## Class Selector Bits

De 3 eerste bits van de DSCP-veld de class aanduiden worden ze Class Selector(CS) genoemd. De 3 bits van DSCP komen direct overeen met de 3 bits van IPP-veld en COS veld om compatible te blijven met 802.1p.

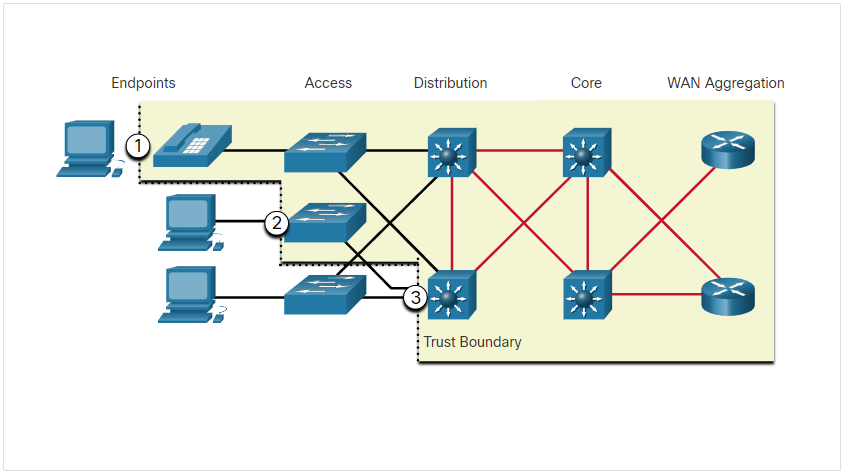


We kunne nu de CoS in kaart brengen met de overeenkomstige Class selector.



## Trust Boundaries

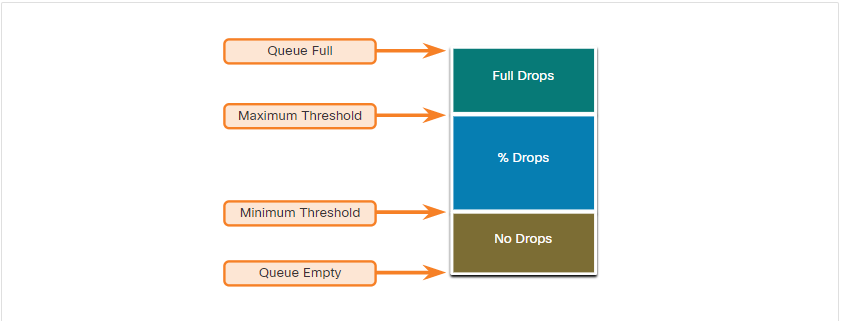
Wanner het het verkeer ge markeerd wodt moet dit zo dicht mogelijk bij de verzender. Een afstand die zo dicht mogelijk van de verzender is en nog steeds administratief en technische haalbaar is. dit heet Trust Boundaries.



1. Trusted endpoint kunnen het verkeer met Layer 2 CoS of Layer 3 DSCP waaren maarkeren bv : Ip Telephone, Wireless Access Point, Ip Conference Statiojn …
2. Veilige endpoint kunnen op de Layer 2 switch markering toepassen.
3. Verkeer kan ook gemarkeerd worden op Layer 3 switch of router

## Congestion Avoidance

Congestion management bevat wachtrij en planning methodes om de overvloed van verkeer te bufferen of wachtrijen. Congestion avoidance tool monitoren netwerk en internetwerk bottlenecks voordat er een opstopping is. Wanneer de rij onder de *Minimum Treshhold* is zij´n er geen drops. Maar hoe meer pakketten in de wachtrij komen, hoe hoger dichterbij het bij de *maximum Threshold* komen. Wanneer de aantal pakketten over de *maximum Threshold* is dan wordt alles gedropt.

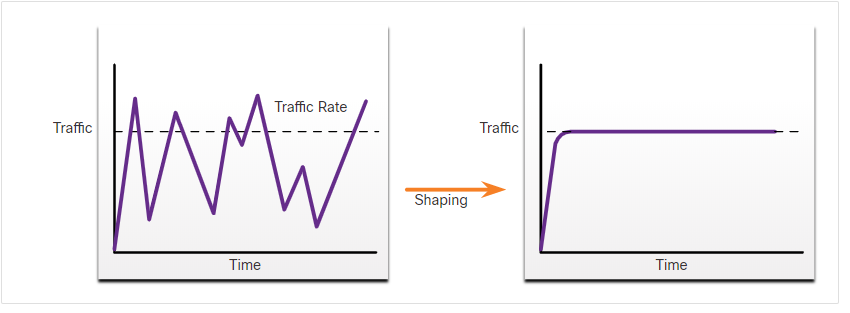


De WRED-algoritme is een oplossing die gebruikt wordt bij Congestion avoidance

## Shaping and Policing

Dit zijn twee mechanismes van Cisco QoS Software om opstopping tegen te houden.

Shaping is een concept voor verkeer die naar buiten(outbound) gaan Shaping neemt het overschot van pakketten en zet ze in een wachtrij. Deze pakketten worden dan geplant om later te versturen over een bepaalde periode. De planning aspect van shaping zorgt ervoor dat pakketten die vertraging hebben, in een wachtrij gaan en wachten om later opnieuw opgestuurd te worden. Voorbeeld van planning functies voor shaping zijn CBWFQ en LLQ.



Policing is voor het verkeer die binnen(inbound) de interface komt. Wanneer het netwerkverkeer de maximun rate behaald, dan worden het overbodige verkeer gedropt. Policing wordt gebruikt door ISP.



1. [qos1] p.1 – 13. [↑](#footnote-ref-1)