

Cours 47 : Quality of Service (Partie 2)

Dans ce cours nous verrons la seconde partie de l'étude de la qualité de service, en Anglais Quality Of Service (QoS), dans la première partie nous avons vu la voix à travers les VLANs, le PoE, ainsi que l'intérêt d'utilisation du QoS qui est pour prioriser le trafic de la voix et la vidéo afin de réduire les délais, le jitter et les pertes. Dans ce cours détaillerons plus le fonctionnement de QoS. Nous verrons tout d'abord la classification et les classification et le marquage, nous verrons ensuite la gestion des queues et des congestions puis les politique de conception pour savoir quelle taux du trafic faire entrer ou sortir d'une interface.

L'intérêt de QoS est avant tout de pouvoir donner une priorité à certains types de trafic par rapport à d'autres lors des congestions. La classification organise le trafic réseau (les paquets) dans des classes de trafiques (avec des catégories).

La classification est fondamental à QoS, car pour donner une priorité à certains trafiques il faut identifier quelle type de trafic donner la priorité.

Il existe plusieurs méthode de classification du trafic, en voici plusieurs exemples :

- Une ACL permet à ce que le trafic soit permis par l'ACL pour lui donner un certain traitement par rapport à d'autre trafiques.
- NBAR (Network Based Application Recognition) fait fonctionner une inspection profonde des paquets, en regardant à travers les couches 3 et 4 jusqu'à la couche 7 pour identifier le type spécifique de trafic.
- Dans les couches 2 et 3 les entêtes ont une partie spécifique utilisé pour cela.

Le PCP (Priority Code Point) est une partie de la balise 802.1Q (dans l'entête Ethernet) et peut être utilisé pour identifier la priorité du trafic si haute ou basse. Cela ne fonctionne seulement lorsqu'il y a une balise dot1q.

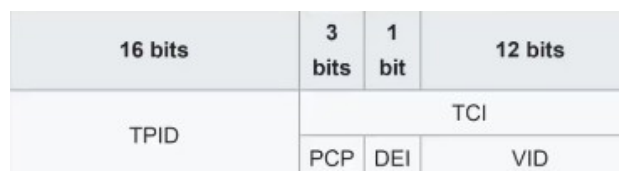
Le DSCP (Differentated Services Code Point) est une partie de l'entête IP qui peut aussi être utilisé pour identifier la priorité du trafic si elle est haute ou basse.

Voyons plus en détail ces méthodes de classifications :



Ci dessus l'entête Ethernet, pour PCP on peut voir qu'il y a la balise dot1q et une balise VLAN.

Le PCP est contenu dans cette partie 802.1Q, on peut voir ici les parties de la balise dot1q :



PCP est aussi connu comme CoS (Class of Service), son utilisation est défini par le standard IEEE 802.1p, on peut voir ci dessus qu'il y a 3 bits qui donnent 8 valeurs possibles (car $2^3 = 8$)

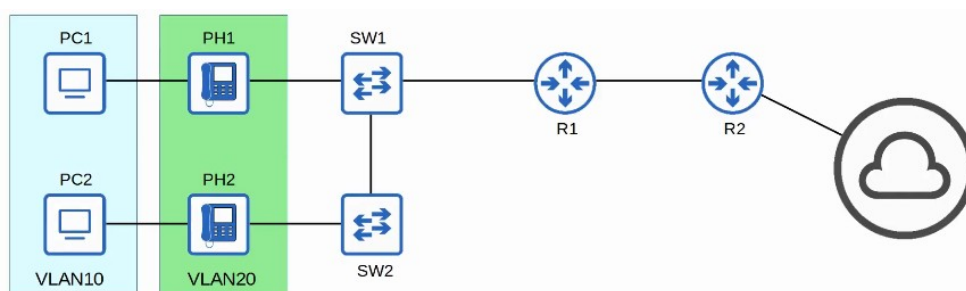
Ces valeurs sont définies en fonction du tableau suivant :

Valeur PCP	Type de trafic
0	Best Effort
1	Background
2	Excellent Effort
3	Critical Applications
4	Vidéo
5	Voice
7	Contrôle Réseau

« Best effort » signifie qu'il n'y a pas de garantie que la donnée est bien acheminée ou que cela correspond à un standard QoS. C'est un trafic régulier et non pas une haute priorité.

Les téléphones IP marquent les trafics appels signalés (utilisés pour établir des appels) comme PCP3. Ils marquent le trafic de voix actuel avec PCP5.

Voici un réseau dans lequel est réparti deux VLAN, une pour le trafic des données PC (VLAN 10) et une autre VLAN pour la voix (VLAN20)



Puisque le PCP est trouvé dans l'entête dot1q, il peut uniquement être utilisé avec les connexions suivantes :

- Les liens Trunk
- Les liens d'accès avec un VLAN de voix

Dans le diagramme ci dessus, le trafic entre R1 et R2 ou entre R2 et une destination externe ne sera pas balisé avec dot1q. Le trafic à travers ces liens PCP ne peuvent pas être marqués avec une valeur PCP.

Voyons à présent comment le marquage et la classification est faite dans la couche 3 :

Offsets	Octet	0	1	2	3
Octet	Bit	0	1	2	3
0	0	Version	IHL	DSCP	ECN
4	32	Identification			
8	64	Time To Live		Protocol	Header Checksum
12	96	Source IP Address			
16	128	Destination IP Address			
20	160	Options (if IHL > 5)			
24	192				
28	224				
32	256				

Le marquage est contenu dans les parties DSCP et ECN. Auparavant ces bits étaient organisés différemment avec ToS, 3 bits étaient utilisés pour le IPP (IP préférence) et 5 bits pour différents usages sans intérêt défini à présent c'est 5 bits pour DSCP et 2 bits pour ECN.

Voyons plus en détail IPP :

Le marquage avec le standard IPP est similaire à PCP :

- les bits 6 et 7 sont réservés pour le « contrôle trafic du réseau » (par exemple des messages OSPF entre des routeurs).
- Le bit 5 est pour la voix
- le bit 4 pour la video
- le bit 3 est pour le voice signaling
- le bit 0 est pour le best effort

Avec les bits 6 et 7 réservés, 6 valeurs possibles sont affichés.

Bien que 6 valeurs est suffisant pour plusieurs réseaux, les prérequis pour le QoS de certains réseaux demandent plus de flexibilité.

Voyons plus en détail DSCP :

Le RFC 2474 (1998) définit la partie du DSCP, et d'autres différents services que le RFC à élaborés sur son usage. Avec la mis à jour de IPP vers DSCP le nouveau marquage du standard à du être implémenté, le type de marquage a été changé car en ayant des marquages de différents standards pour différents types de trafic, l'implémentation QoS est simplifié, QoS fonctionne mieux entre les ISP et les entreprises avec d'autres bénéfices.

Différents marquages ont donc été créés et standardisés, en voici quelques uns :

- le Default Forwarding (DF) – Best effort trafic
- le Expedited Forwarding (EF) – bas trafic perte/latence/jitter (la voix)
- Assured Forwarding (AF) – un ensemble de 12 valeurs de standard
- Class Selector (CS) – un ensemble de 8 valeurs de standard, qui fournit une compatibilité avec IPP

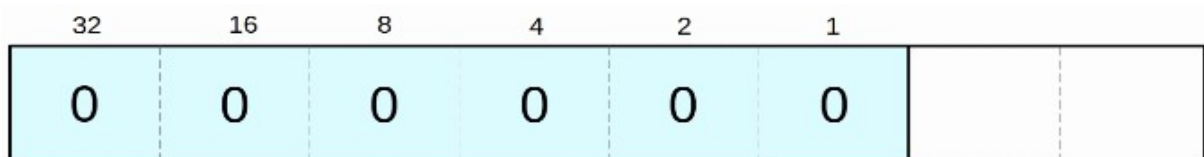
On configure un class-map appelé TEST avec la commande :

R1 (config) #class-map TEST

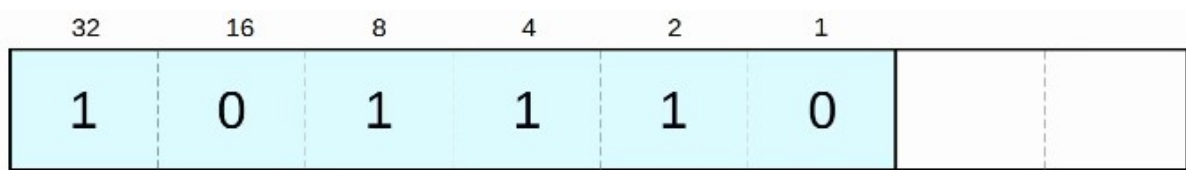
```
R1(config)#class-map TEST
R1(config-cmap)#match dscp ?
<0-63> Differentiated services codepoint value
af11 Match packets with AF11 dscp (001010)
af12 Match packets with AF12 dscp (001100)
af13 Match packets with AF13 dscp (001110)
af21 Match packets with AF21 dscp (010010)
af22 Match packets with AF22 dscp (010100)
af23 Match packets with AF23 dscp (010110)
af31 Match packets with AF31 dscp (011010)
af32 Match packets with AF32 dscp (011100)
af33 Match packets with AF33 dscp (011110)
af41 Match packets with AF41 dscp (100010)
af42 Match packets with AF42 dscp (100100)
af43 Match packets with AF43 dscp (100110)
cs1 Match packets with CS1(precedence 1) dscp (001000)
cs2 Match packets with CS2(precedence 2) dscp (010000)
cs3 Match packets with CS3(precedence 3) dscp (011000)
cs4 Match packets with CS4(precedence 4) dscp (100000)
cs5 Match packets with CS5(precedence 5) dscp (101000)
cs6 Match packets with CS6(precedence 6) dscp (110000)
cs7 Match packets with CS7(precedence 7) dscp (111000)
default Match packets with default dscp (000000)
ef Match packets with EF dscp (101110)
```

Voyons plus en détail chacune de ces parties.

DF (Default Forwarding) est utilisé pour le trafic best-effort, le marquage DSCP pour DF est 0

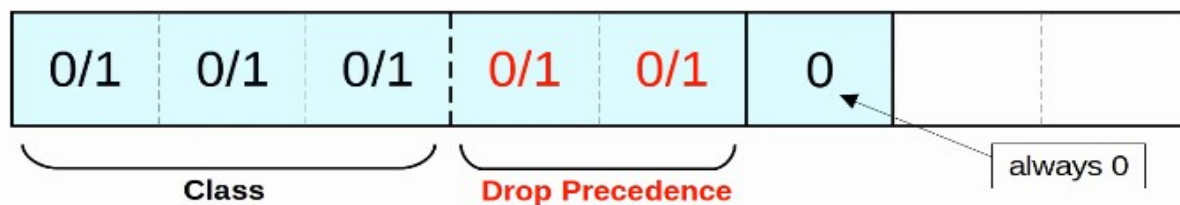


EF (Expedited Forwarding) est utilisé pour le trafic qui requière de basse perte/latence/jitter, le marquage DSCP pour EF est 46 comme suit :



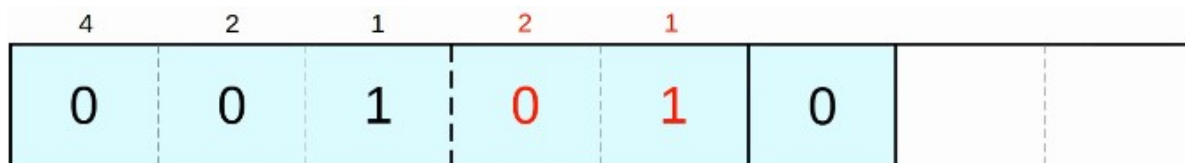
AF (Assured Forwarding) définit 4 classes de trafic. Tous les paquets dans une classe ont la même priorité. Pour chaque classe, il y a 3 niveau de perte précédente :

- Haute perte précédente = plus de chance de perte de paquet durant la congestion



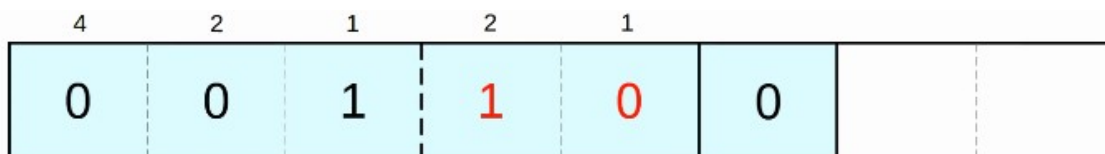
Lorsque l'on écrit la valeur de AF on note AF suivi du numéro décimal de la classe suivi du numéro décimal de la perte précédente.

Par exemple pour noter l'AF du nombre suivant :



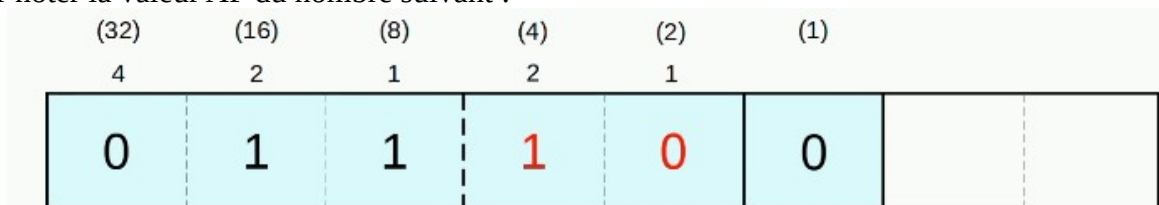
On écrira « AF11 », AF11 est aussi la même valeur de DSCP 10, pour calculer le DSCP on additionne les valeurs qui contiennent un bit à 1

Pour noter la valeur AF du nombre suivant :



On écrira « AF12 », AF12 est aussi la même valeur que DSCP 12

Pour noter la valeur AF du nombre suivant :



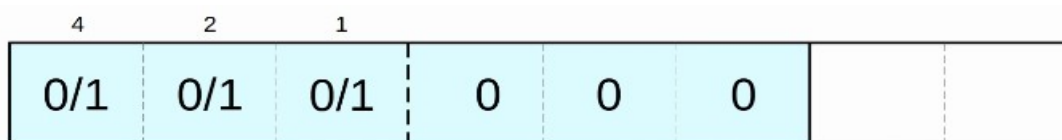
On écrira « AF32 », AF32 est aussi la même valeur de DSCP 28, pour calculer le DSCP on additionne les valeurs qui contiennent un bit à 1

La formule pour convertir de AF vers DSCP est $8X + 2Y$ où X est la valeur de la classe et Y la valeur de la perte précédente.

Voici un résumé des différentes valeurs à attribuer en fonction de la priorité, la valeur AF41 est la valeur la plus haute avec la plus grande priorité, AF13 est la valeur la plus basse avec la plus basse priorité

	Lowest drop precedence		Highest drop precedence
Highest priority ↑ Lowest priority	AF41 (34)	AF42 (36)	AF43 (38)
	AF31 (26)	AF32 (28)	AF33 (30)
	AF21 (18)	AF22 (20)	AF23 (22)
	AF11 (10)	AF12 (12)	AF13 (14)

CS (Class Selector) définit 8 valeurs DSCP pour la compatibilité arrière avec IPP
Les 3 bits ajoutés pour DSCP sont définis à 0, et le IPP originel est utilisé pour faire 8 valeurs.



Donc CS est similaire à IPP, la différence est dans le nom des valeurs, pour IPP il y a les valeurs 0, 1, 2, 3, 4, 5, 6, 7 pour CS il y a les valeurs : CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7

Le RFC 4954 a été développé avec l'aide de Cisco pour associer ces valeurs afin de standardiser leur utilisations.

Le RFC donne plusieurs recommandations, les plus importantes sont les suivantes :

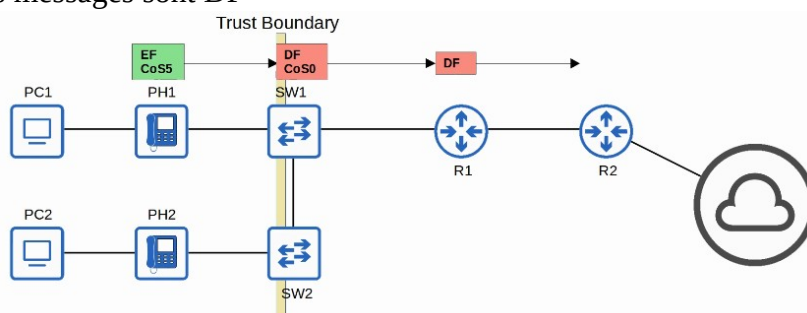
- trafic de voix : EF
- Video Interactive : AF4X
- Streaming Vidéo : AF3X
- Données de haute priorité : AF2X
- Best effort : DF

Le trust boundary d'un réseau définit où les appareils font confiance ou non au marquage QoS pour recevoir des messages.

Si le marquage est de confiance, l'appareil va transférer le message sans changer son marquage.

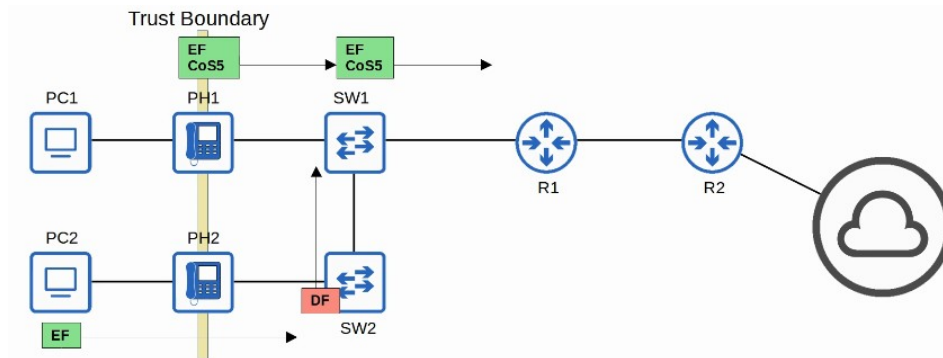
Si le marquage n'est pas de confiance, l'appareil va changer le marquage en accordement avec la politique de configuration.

Sur le réseau suivante le trust boundary est placé au niveau du switch, les messages avant le Switch sont de confiance donc le marquage est EF mais après le Switch le marquage n'est plus de confiance donc les messages sont DF



Si un téléphone IP est connecté au port Switch il est recommandé de bouger le trust boundary vers les téléphones IP. Cela se fait avec la configuration.

Si un utilisateur marque son PC avec une priorité haute, le marquage changera (en pas confiance) Donc sur le réseau suivant, le trust boundary est placé au niveau des téléphones et les messages des téléphones sont toujours de type EF et ne changent pas, par contre les messages des PC sont de type EF au départ et changent lorsqu'ils passent le trust boundary vers des messages de type DF.



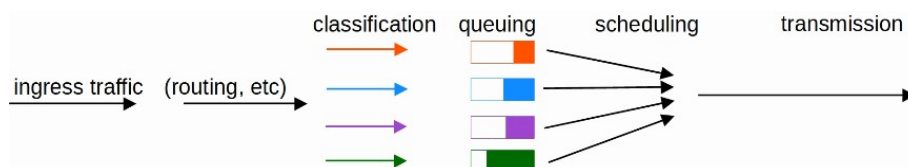
Voyons le concept de gestion des congestions et des fil d'attente.

Lorsque l'appareil d'un réseau reçoit un trafic plus rapidement qu'il ne peut le répartir vers l'interface appropriée, les paquets sont placés dans une file d'attente de l'interface et attendent d'être répartis. Lorsque la file d'attente est remplie, les paquets qui ne peuvent plus entrer dans la file d'attente sont bloqués (tail drop). RED et WRED lâche les paquets plus tôt afin d'éviter le tail drop. Une partie essentielle de QoS est qu'il peut utiliser plusieurs fil d'attente et non pas une seule. C'est à ce moment que la classification prend son sens. L'appareil qui correspond à certains facteurs (par exemple le marquage DSCP de l'entête IP) et le place dans la file d'attente appropriée.

L'appareil, est le seul capable de partager la trame en dehors d'une interface donc un planificateur est utilisé pour décider quelle file d'attente est partagée depuis le suivant.

La priorisation permet aux planificateurs de donner à certaines files d'attente une plus grande priorité par rapport à d'autres.

Voici un schéma pour simplifier cela :



Une méthode de planification commune est le weighted round-robin

- le round robin les paquets sont pris depuis chaque file d'attente dans l'ordre et de manière cyclique.
- weighted signifie que plus de données sont prises à partir de la plus haute priorité de file d'attente chaque fois que le planificateur atteint la file d'attente.

CBWFQ (Class-Based Weighted Fair Queuing) est une méthode populaire de planification qui utilise le planificateur weighted round-robin tant que la garantie de chaque file d'attente à un certain pourcentage de bande passante pour l'interface durant la congestion.

Le schéma est à présent le suivant :



Le round robin scheduling n'est pas idéal pour le trafic de voix et vidéo. Même si le trafic de voix et vidéo reçoit une garantie minimale du montant de la bande passante, round robin peut prendre un certain délai ainsi que du jitter puisque même avec une haute priorité la file d'attente doit attendre leur tour dans le planificateur.

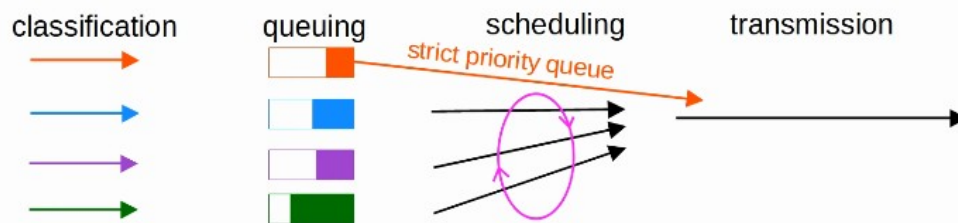
LLQ (Low Latency Queuing) désigne une (ou plus) de file d'attente comme file d'attente de priorité strict. Cela signifie que s'il y a un trafic dans la file d'attente, le planificateur attendra toujours de prendre le paquet suivant depuis la file d'attente jusqu'à ce qu'elle soit vide.

Cela est très efficace pour réduire le délai et jitter de la voix et du trafic vidéo.

Il y a tout de même l'inconvénient de laisser les autres files d'attente si le trafic est toujours désigné comme file d'attente de priorité strict.

La politique peut contrôler le montant du trafic permis dans la file d'attente de priorité strict donc cela peut prendre tous les liens de la bande passante.

Voici un schéma qui résume le fonctionnement :



Le shaping et policing (façonnage et politique en français) sont utilisés pour contrôler le taux du trafic.

Le shaping ajoute en mémoire de la file d'attente le trafic si le taux de trafic va au-dessus du trafic configuré.

Le policing bloque le trafic si le taux de trafic va au-dessus du taux configuré.

Le trafic « rafale » est permis pour une courte période de temps si le taux est au-dessus de celui configuré.

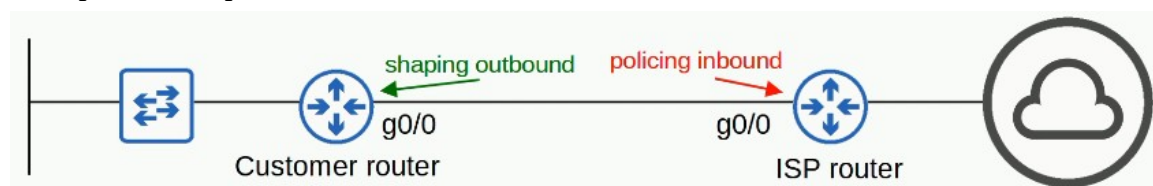
Cela est pratique aux données des applications qui sont en « rafale » de nature. Au lieu d'un débit constant de données, elles envoient des données en rafales.

Le montant du trafic en rafale permis est aussi configurable.

Dans les deux cas, la classification peut être utilisée pour permettre différents taux pour différents types de trafic.

Pourquoi limiter le trafic en fonction de l'envoi/Réception ?

Pour comprendre on peut utiliser le réseau suivant :



Si le routeur ISP reçoit et est limité à 300Mbps par la politique de l'ISP, le routeur du client va envoyer lui en rafale 300Mbps pour éviter que ses paquets ne soient perdus par le routeur de l'ISP.