

Sorbonne Université, Master 2^e informatique, spécialité réseaux

TME 5 : DiffServ Edge Configurations

(cf. Cours 9)

 [Compte rendu électronique \(pdf\)](#)

Rappel - DiffServ

Les services différenciés sont basés sur l'idée principale de discriminer entre les paquets au lieu des connexions. Le but est d'éviter de garder les états de chaque connexion dans les routeurs, notamment ceux du cœur du réseau, qui doivent traiter un nombre très élevé de connexions. Ainsi, en indiquant par *marquage* la qualité de service demandée par un paquet, le routeur applique le même traitement sur un ensemble de paquets pouvant appartenir à des connexions différentes d'où la notion d'*agrégation* de connexions.

Une architecture de services différenciés a été élaborée et retenue par le groupe de travail DiffServ au sein de l'IETF. Cette architecture représente un raffinement des méthodes proposées précédemment et qui sont basées sur le marquage des paquets et le contrôle de débit (*conditionnement de trafic*). DiffServ est une solution QoS flexible et facile à déployer dans les réseaux au sein desquels on souhaite *gérer efficacement le partage de la bande passante* dans l'objectif d'assurer des *qualités de service différentes* aux flots du réseau.

Le standard de l'IETF recommande l'utilisation d'un champ de 6 bits du paquet IP, nommé DSCP (Differentiated Services CodePoint) pour marquer les paquets. Le marquage et/ou le contrôle est souvent réalisé à travers des seuils à jetons au niveau des routeurs des bords (à l'entrée du réseau). Le seuil à jetons mesure les paramètres temporels du trafic et vérifie leur conformité avec un profil (**TCA**) déjà négocié entre le client et le FAI. Puis, il peut *marquer*, *retarder* ou *jeter* les paquets. Le TCA fait partie du **SLA** et peut refléter simplement les propriétés/besoins du trafic.

En plus du marquage, l'IETF a défini aussi la notion du **PHB** (Per-Hop Behavior). Selon la valeur du DSCP d'un paquet, un routeur effectue un traitement (comportement) spécifique pour expédier le paquet : c'est le PHB associé au DSCP en question. En associant à chaque valeur de DSCP un PHB distinct, on offre des services différents aux paquets. En plus du service BE (Best Effort ≡ PHB DF), d'autres services comme le service Expedited Forwarding (PHB EF) et le service Assured Forwarding (PHB AF) ont été ainsi définis.

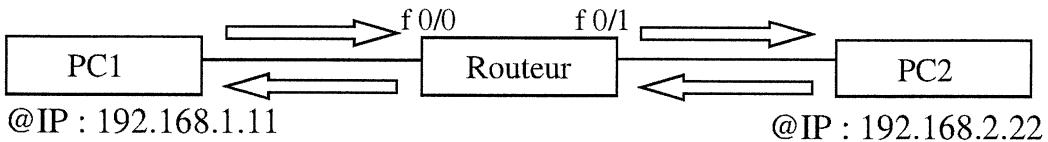
Pour implanter différents PHB dans un routeur, des mécanismes appropriés sont nécessaires. Ces mécanismes sont principalement l'*ordonnancement* et la *gestion de buffer* (files d'attentes). Les deux deviennent significatifs lorsque les routeurs sont sujets à des congestions persistantes. Le rôle de l'algorithme d'ordonnancement est de déterminer quel sera le paquet suivant à transmettre. Une ou plusieurs files d'attente peuvent être rattachées au port de sortie du routeur. Il faut noter que contrairement au modèle des services intégrés, le nombre de files d'attentes est limité et il ne correspond pas au nombre de connexions mais au nombre de *classes de service*. Cependant, on utilise souvent les mêmes algorithmes tels que **WFQ** (Weighted Fair Queuing) et **PQ** (Priority Queuing). *L'implantation exacte qui fournit un service donné est laissée au choix du constructeur et/ou du développeur*

Au niveau des routeurs, il est possible de configurer directement les mécanismes de contrôle de base tels que RED ou WFQ pour créer une architecture DiffServ quelconque, ou de *configurer des classes de services* en utilisant les mécanismes de contrôle sous-jacent définis par défaut avec ou sans paramètres (i.e. Il y a plusieurs granularités de configuration)

Préparation / Rappel

Avant de démarrer les tests de configuration vous effectuez ces différentes préparations dans le but d'obtenir un accès à 3 machines : une machine nommée PC1, une machine nommée PC2 et un routeur CISCO connectant les deux machines.

La topologie visée est la suivante :



D'abord, à partir d'un terminal, démarrez la machine virtuelle du TME qui est une machine virtuelle Scientific Linux 7 avec la commande :

Vbox ITQOS20_2016 Cette commande vous demandera le mot de passe de votre compte.

Le démarrage prendra plusieurs minutes. Si vous n'êtes pas automatiquement en mode plein écran, vous pouvez l'activer en tapant simultanément [Ctrl droite] [F].

Accédez à la machine virtuelle SL7 avec le compte **itqos**.

A l'intérieur de la machine virtuelle SL7 :

Tapez dans un terminal **telnet PC1** pour accéder à PC1. Ouvrez un autre terminal dans une autre fenêtre et non pas dans un autre onglet de la même fenêtre que PC1, et tapez **telnet PC2** pour accéder à PC2.

Afin de vérifier la topologie de la figure ci-dessus :

A partir du PC1, testez ping -R pc2 et/ou

A partir du PC2, testez ping -R pc1

Pour accéder au routeur, ouvrez un autre terminal dans une autre fenêtre et tapez **telnet router**. Ensuite, tapez [Entrée] pour obtenir le prompt Router>. Au prompt, tapez enable pour passer en mode privilégié et le nouveau prompt Router# s'affichera.

L'interface du routeur est du type vtysh (Virtual TeletYpe SHell) qui vous permet de passer des commandes de configuration au routeur CISCO.

Nous nous intéressons dans ce TME uniquement à l'architecture des services différenciés. Néanmoins, vous pouvez consulter tous les paramètres de configuration du routeur avec la commande show running-config ou encore l'abréviation sh run.

Pour connaître à tout moment la liste des commandes ou les suites possibles d'une commande vous tapez simplement ‘ ?’. Cette manœuvre est très recommandée voir même nécessaire quand vous tapez une commande quelconque et elle est à effectuer à chaque mot de la commande. La complétion par la touche Tabulation (↪) fonctionne aussi pour les commandes et leurs options. Exemple :

```
Router# configure [appuyer sur ' ?']  
Terminal Configuration terminal  
Router# configure term [appuyer sur ]  
Router# configure terminal
```

Vous pouvez ainsi consulter la liste de toutes les commandes disponibles et leur rôle en tapant immédiatement ‘?’.

La commande précédente vous permet de passer en **mode de configuration**. Vous pouvez aussi tapez simplement :

```
Router# conf t [appuyer sur 'Entrée']  
Router(config)#
```

Remarques importantes :

Pour effectuer une configuration quelconque, deux manuels de configuration sont à consulter et/ou à télécharger depuis le site de CISCO en cas de besoin. Le premier est le « **Cisco IOS Quality of Service Solutions Command Reference** », le deuxième est le « **Cisco IOS Quality of Service Solutions Configuration Guide** ». Le premier vous donne la liste complète des commandes QoS et leur descriptif détaillé. Le deuxième vous donne un aperçu des solutions et outils de qualité de service dans CISCO avec des exemples d'utilisation.

Méthodologie générale à suivre : D'abord, on essaye de trouver la ou les commandes avec l'aide de la commande elle-même en tapant à chaque mot ‘?’ . Si ce n'est pas suffisant, on consulte le “Command Reference” guide. Si pas de réussite, on consulte le “Configuration guide” pour mieux comprendre le mécanisme qu'on essaye de configurer. Si toujours pas de réussite, cela signifie que vous devez vous documenter beaucoup plus pour comprendre et maîtriser le mécanisme en question avant de pouvoir le configurer convenablement.

Attention : N'utilisez pas les moteurs de recherche sur Internet, pour chercher au hasard des exemples de configuration qui généralement peuvent être faux ou inadaptés aux scénarios de tests demandés. Les commandes du TME sont simples et les syntaxes peuvent être trouvées directement avec l'aide des commandes (en tapant à chaque mot ‘?’) et/ou le “Command Reference”.

Par la suite, vous effectuez une série de configurations qui sont souvent implantées dans les routeurs Diffserv du bord (« edge routers »). Il s'agit de la classification, marquage, mesure/rejet (« policing »), et remise en forme (« shaping »).

Classification et marquage (Class-based marking)

La procédure de marquage dans le routeur CISCO se fait en utilisant le processus de création de classes de paquets (classification), ensuite la création de politiques ou actions associées à ces classes, et enfin l'attachement de ces politiques à une interface afin d'activer les services qui sont directement créés avec ces politiques. Présentée de cette façon, cela semble compliqué mais une fois que les commandes sont tapées et exécutées ça devient d'un coup plus simple, et la correspondance avec l'architecture DiffServ devient claire.

Les trois commandes CISCO qui permettent de faire cela dans l'ordre sont :

class-map (après config terminal) et
match
policy-map (après config terminal) et
class
service-policy (à partir d'une interface)

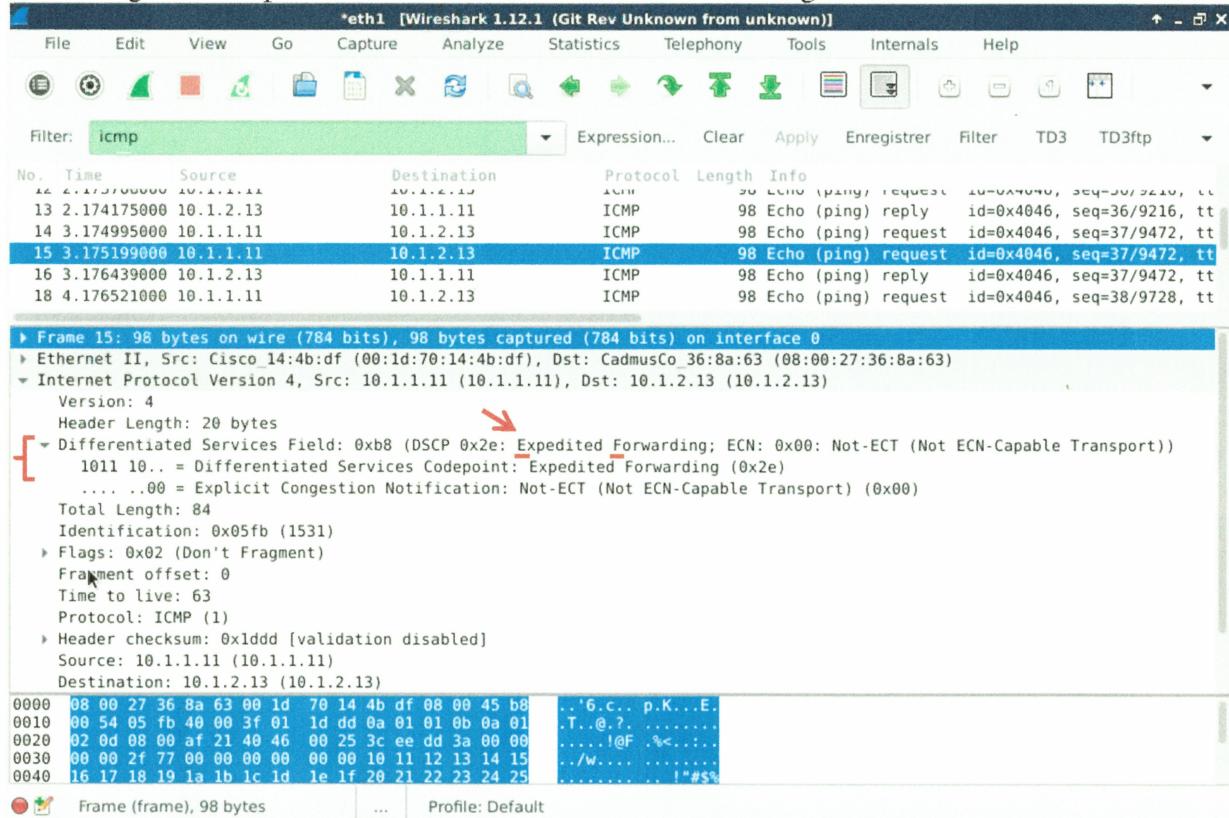
Pour annuler l'effet d'une commande ou pour supprimer une configuration, utilisez la négation de la même commande en ajoutant au début le mot clé no. Exemple :
R(config)# no class-map allpackets

Test 1

On souhaite effectuer un marquage de paquets à travers le routeur en utilisant le code DSCP de la classe Expedited Forwarding (EF) qui est 0x2e (correspondant à un TOS de 0xb8). Au niveau de l'interface qui connecte le routeur à PC1 (f 0/0), marquez avec le code EF tous les paquets IPv4 qui rentrent par cette interface, (et qui sortent donc par l'autre vers PC2.)

Vérifiez ce marquage en lançant wireshark et en observant l'interface fastethernet01, ou en lançant wireshark à partir de PC2.

L'affichage obtenu par wireshark est similaire à celui de la figure suivante :



Test 2

Enlevez le marquage précédent. Refaire l'expérience en marquant cette fois-ci uniquement les paquets du protocole HTTP avec le code DSCP AF22. Indication : match protocol ?.

Afin de tester ce marquage, utilisez le serveur HTTP (apache) installé et accessible depuis PC1 ou PC2. Pour le lancer :

`sudo httpd` depuis PC1 ou PC2. (Pour l'arrêter : `sudo killall httpd`).
Ensuite, lancez le navigateur `firefox` depuis PC1 ou PC2 et renseignez l'URL <http://pc1/> ou <http://pc2/>. Vous pouvez utiliser aussi la commande `wget`.

Si un client Web sur PC1 se connecte au serveur HTTP sur PC2, alors la requête HTTP doit être marquée. Si un client Web sur PC2 se connecte au serveur HTTP sur PC1, alors la réponse HTTP doit être marquée. Les autres paquets ICMP, UDP et TCP ne doivent pas être marqués

Test 3

Rajoutez le nécessaire afin de marquer en plus tous les paquets UDP avec le code AF43.
Indication : match access-group et access-list

Afin de générer des paquets UDP vous utilisez l'outil iperf. Les paquets ICMP et TCP ne doivent pas être marqués par le code AF43.

Test 4

Faites le nécessaire afin de marquer les paquets UDP destiné à une adresse IP et un numéro de port spécifiques (@IP : 192.168.2.22, #port : 12345) avec le code EF. Testez à nouveau.

Conditionnement de trafic (Class-based conditioning)

Test 5 - mesure/marquage (class-based policing)

Utilisez la commande police cir ... pir ... (depuis policy-map class) pour vérifier la conformité du débit d'une connexion UDP qui envoie ses données de PC1 à PC2 vers le port numéro 2979. Le TCA (« Traffic Conditioning Agreement ») est le suivant :

- Débit moyen = 1 Mbit/s avec une variabilité (tolérance) maximale de 120 kbit.
- Débit crête = 2 Mbit/s avec une variabilité (tolérance) maximale de 80 kbit.
- Si le débit des paquets est conforme aux deux débits mentionnés ci-dessus, alors les paquets sont marqués et transmis avec le DSCP AF31.
- Si le débit des paquets est conforme seulement au débit crête, alors les paquets sont marqués et transmis avec le DSCP AF32.
- Sinon, les paquets sont marqués et transmis avec le DSCP AF33.

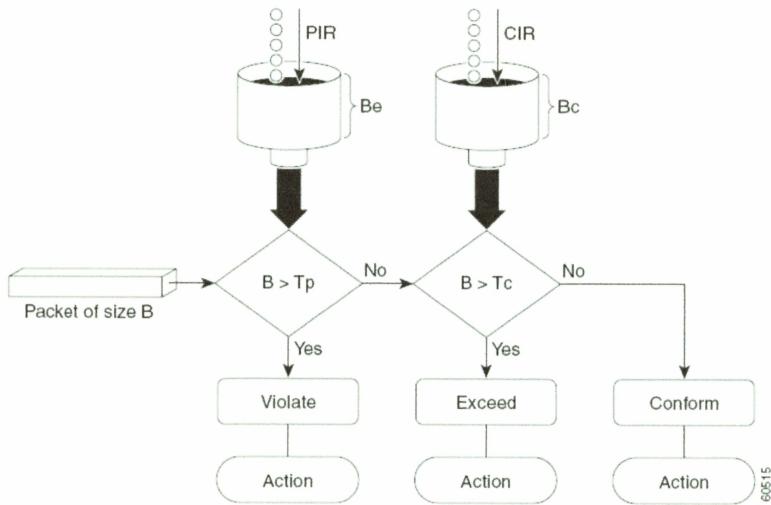
Ce ‘policing’ est effectuée à l’entrée de l’interface qui relie le routeur à PC1 (f 0/0).

Affichez et vérifiez l’état de votre configuration avec les commandes :

```
show policy-map NomPolicy et  
show policy-map interface NomInterface (affiche les statistiques en temps réel)
```

Aussi, avec iperf et l’option -b, vérifiez que les paquets sont marqués en les observant avec wireshark. Les statistiques affichées par iperf doivent montrer que le débit d’envoi est toujours le même que le débit reçu car il n’y a pas de remise en forme ni de rejet, uniquement du marquage avec envoi immédiat des paquets.

Enfin, pour vous aider à comprendre le fonctionnement de ce mesureur/marqueur et les résultats, voici le descriptif donné par la documentation CISCO (**two-rate three-color marker**) :



Updating Token Buckets

$$Tc(t) = \min(CIR * (t-t1) + Tc(t1), Bc)$$

$$Tp(t) = \min(PIR * (t-t1) + Tp(t1), Be)$$

Marking Traffic

- If $B > Tp(t)$, the packet is marked as violating the specified rate.
- If $B > Tc(t)$, the packet is marked as exceeding the specified rate, and the $Tp(t)$ token bucket is updated as $Tp(t) = Tp(t) - B$.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets— $Tc(t)$ and $Tp(t)$ —are updated as follows:

$$Tp(t) = Tp(t) - B$$

$$Tc(t) = Tc(t) - B$$

Question : Si le débit de transmission est de 3 Mbit/s, quelle est le pourcentage de paquets AF31 ? Même question pour AF32 et AF33. Ces résultats sont-ils cohérents avec le TCA ?

Test 6

Modifiez la configuration précédente afin de rejeter cette fois-ci les paquets non-conformes au lieu de les marquer avec le DSCP AF33. Testez avec un débit d'émission de 3Mbit/s.

Question : Quel est le taux de perte affiché par iperf ? Est-il cohérent avec le TCA ?

Question finale : Quelle est la différence entre les trois schémas de policing suivants :

- two-rate three-color marker
- one-rate two-color marker
- one-rate three-color marker

Test 7 - class-based shaping

a/ L'objectif ici est de forcer le trafic UDP sortant du routeur et allant à PC2 et vers le numéro de port 12345 à se conformer au TCA suivant : [débit crête (maximum) = 2 Mbit/s]. Pour ce faire, configurez une remise en forme de ce trafic en utilisant la commande `shape peak x`. Vous devez mentionner un seul paramètre de l'option `peak` qui est donc x. A vous de trouver une valeur adéquate. Testez et vérifiez le résultat avec iperf.

b/ Dans la commande précédente, remplacez l'option peak par l'option average sans changer x et testez à nouveau avec iperf.

Question finale : Quelle est la différence entre l'option average et peak ? Autrement dit, que fait exactement l'option average et que fait exactement l'option peak.

➔ Complétez le tableau suivant :

	Débit moyen	Débit crête	MBD
shape average x	x	...	$\frac{bc}{x}$
shape peak x	n/a

Avant de quittez la salle, éteignez la machine virtuelle avec le menu du bureau de la machine virtuelle et NON Virtual Box.