TP – Qualité de Services IP avec Cisco

Important : Un rapport électronique doit être envoyé au plus tard 15 jours après le TP à l'adresse : rachedi@univ-mlv.fr.

Objectif :

- ☐ Etudier le mécanisme de qualité de services (QoS) et en particulier le mécanisme DiffServ
- ☐ Comprendre les mécanismes de filtrage, classification des flux réseau
- ☐ Création de politique de services
- ☐ Connaître les principales commandes « Cisco » pour configurer les routeurs afin qu'ils supportent la QoS

Pré-requis :

- ☐ Protocole IP et adressage
- ☐ Routage statique

Le TP doit se dérouler en deux phases : simulation par « Packet Tracer » et réalisation par des vrais routeurs et câbles.

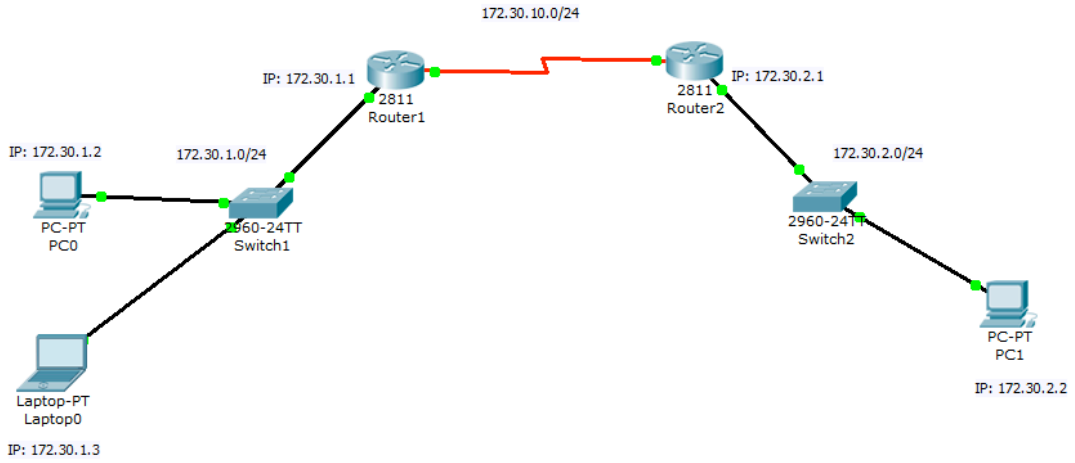


Figure 1. Topologie réseau

I. Configuration de base

Tâche 1 : configuration des informations IP sur les interfaces Ethernet d'un réseau

Étape 1 : configurez les informations IP sur les ordinateurs.
Configurez les informations IP suivantes sur les trois ordinateurs du réseau :

- *PC0 - Adresse IP : 172.30.1.2, masque de sous-réseau : 255.255.255.0, passerelle :172.30.1.1*
- *Laptop0 - Adresse IP : 172.30.1.3, masque de sous-réseau : 255.255.255.0, passerelle :172.30.1.1*
- *PC1 - Adresse IP : 172.30.2.2, masque de sous-réseau : 255.255.255.0, passerelle :172.30.2.1*

Étape 2 : configurez les informations IP sur les interfaces Ethernet et Série des routeurs 1 et 2.
Accédez au routeur R1. Sous l'onglet ILC, saisissez le mode d'exécution privilégié en entrant la commande **enable**. Saisissez le mode de configuration globale en entrant la commande **config t**. Saisissez le mode de configuration pour la première **interface FastEthernet** en entrant la commande **interface fa0/0**. Configurez l'adresse IP en entrant la commande **ip address 172.30.1.1 255.255.255.0**. Activez l'interface en entrant la commande **no shutdown**. Quittez le mode de configuration en utilisant le raccourci clavier **Ctrl+z**. Enregistrez la

configuration en lançant la commande **copy run start**. Répétez ces étapes pour l'interface FastEthernet 1/0 (**ip address 172.30.1.1 255.255.255.0**).
Configurez les interfaces séries des deux routeurs R1 et R2. N'oubliez pas la commande "**clock rate 64000**" pour synchroniser le lien entre les deux routeurs.

Tâche 2 : vérification du bon fonctionnement

Étape 1 : vérifiez l'état des interfaces sur les routeurs.
Vérifiez l'état des interfaces FastEthernet en entrant la commande **show ip interface brief.**

Étape 2 : vérifiez la connectivité entre les hôtes et les routeurs.
Entrez la commande **arp -a** depuis l'invite de commandes PC1. Entrez la commande **show arp** sur le routeur R1. Notez le résultat. Entrez la commande **ping 172.30.1.1** depuis l'invite de commandes PC1. Entrez la commande **arp -a** depuis l'invite de commandes PC1. Entrez la commande **show arp** sur le routeur R1. Notez le résultat : Chacun des deux périphériques a désormais une entrée de l'autre périphérique dans sa table ARP.

II. Génération et mesure du trafic réseau

Nous considérons la concurrence entre deux trafics : UDP entre PC1 et PC2 et TCP entre Laptop0 et PC2.

- Le cas de « *Packet Tracer* » : vous pouvez utiliser l'outil « Traffic Generator » qui se trouve dans le bureau des PC/Laptop.
- Le cas des vrai routeurs/PC : vous pouvez générer et mesurer le trafic réseau de deux manières : l'utilisation des outils MGEN/TRPR ou les outils UDPMT/UDPTARGET pour le trafic UDP et TCPMT/TCPTARGET pour le trafic TCP.

III. Identification et filtrage de flux

Pour établir une qualité de service il faut tout d'abord identifier et sélectionner les flux qu'on veut différencier. Nous disposons de deux techniques de filtrage dans l'IOS du routeur qui sont basées sur l'utilisation d'ACLs (**Access Control List**) ou bien de **class-map**.

Access Control List : Une liste de contrôles d'accès est une collection d'instructions permettant d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :
-L'adresse d'origine, L'adresse de destination, Le numéro de port, Les protocoles de couches supérieures

Il existe 3 types de listes de contrôles d'accès : les ACLs standards, les ACLs étendues et les ACLs nommées.
Les **ACLs standards** utilisent des spécifications d'adresses simplifiées et autorisent ou refusent un ensemble de protocoles. C'est-à-dire en d'autres termes que l'on peut interdire par exemple à une machine l'accès à une autre machine ou à un autre réseau.
Les **ACLs étendues** utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis. Ce type d'ACL utilise un filtrage bien plus spécifique - on peut selon nos besoins, interdire (ou permettre) des flux depuis et vers une autre machine (ou réseaux) suivant des critères tels que :
- Le type de protocole de niveau 4 (en l'occurrence TCP ou UDP).
- Le numéro de port utilisé.
- Ou même le type de l'application (ftp, telnet .....).

Les **ACLs nommées** peuvent être soit standards, soit étendues; elles n'ont pour but que de faciliter la compréhension et de connaître la finalité de l'ACL.

Paramètres d'une ACL :

Routeur# access-list *numéro { **permit** ou **deny** } protocole source destination opérateur (numéro de port)*

numéro : <1-99> : IP standard, <***100-199***> : IP étendu (des paquets IP qui transitent le routeur), …
protocole : IP, TCP, UDP, ICMP, GRE, IGRP
source : adresse source
destination : adresse destination
opérateur : lt *less than* (plus petit que), gt *greater than* (plus grand que), eq *equal (*egal à), neq *not equal (*différent

de)
numéro de port : le numéro de port de l'application

Exemple : Pour filtrer les paquets TCP à destination du PC1 *172.30.2.2*, port 80, et quel que soit l'émetteur. Nous pouvons utiliser la commande suivante :
access-list 101 permit tcp 0.0.0.0 255.255.255.255 172.30.2.2 255.255.255.0 eq 80

1. Dans le but de protéger le flux TCP, limiter le débit du trafic UDP avec l'utilisation de la commande Cisco « *rate-limit* ». Cette méthode appelée CAR (Committed Access Rate) permet de limiter la bande passante sur l'interface de sortie d'un trafic particulier.
   La syntaxe de la cmd :
   ***rate-limit {input | output} [dscp* dscp-value*] [access-group [rate-limit]* acl-index*] bps burst-normal burst-max conform-action* conform-action *exceed-action* exceed-action
   Exemple : ***rate-limit output access-group 101 80000 8000 8000 conform-action transmit exceed-action drop***
2. Analyser le trafic réseau.
3. Quelle est la limite de cette méthode?

IV. Création d'une politique de qualité de service avec DiffServ

a) DiffServ (Differentiated Services)

Permet de marquer le trafic selon sa classe de priorité en utilisant le champ ToS (Type of Service) de 6 bit dans l'entête du paquet IP. Les valeurs de ce champ définissent un code pour classer les priorités appelé DSCP (Differentiated Services Code Point) autorisant **64** niveaux différents. Deux Classes de DSCP existent EF (Expedited Forwarding) et AF (Assured Forwarding) : EF définie un service premium alors que AF est constitué de quatre classes indépendantes, chacune comportant trois niveaux de priorités de rejet des paquets.

Type of Service (TOS)	X	X	X	X	X	X	X	0
	7	6	5	4	3	2	1	0
Differentiated Services (DS)	X	X	X	X	X	X	X	X

Figure 2. Le champ ToS dans l'entête IP

La notion **IP Precedence** est la technique de QoS la plus utilisée à cause de sa simplicité et de son interopérabilité avec les éléments du réseau. Elle utilise les **3 bits de poids fort du DSCP** ce qui assure la compatibilité avec la technique précédente, mais n'offre, par conséquent, que **8 niveaux de classifications**. Les valeurs **6 et 7** sont réservées pour **le contrôle du réseau et les protocoles de routage**. Il reste 6 niveaux de priorités. L'implémentation utilise généralement une priorité 5 pour la voix sur IP, 4 pour la vidéo et la visioconférence en général, 0 pour le trafic Best effort. Selon les RFC791/RFC1349 l'interprétation des valeurs attribuées au champ Tos et les recommandations en fonction de type de trafic réseau sont données dans les 2 tableaux suivants :

Bits	Meaning
7-5	IP Precedence: 111 Network Control 110 Internetwork Control 101 Critic/ECP 100 Flash Override 011 Flash 010 Immediate 001 Priority 000 Routine
4	1 = Low Delay; 0 = Normal Delay
3	1 = High Throughput; 0 = Normal Throughput
2	1 = High Reliability; 0 = Normal Reliability
1	1 = Minimise monetary cost (RFC 1349)
0	Must be 0

Trafic réseau	DSCP PHB	DSCP Décimale	IP Precedence
Voix (Voice)	EF	46	5
Vidéo	AF41	34	4
Contrôle voix	AF31	26	3
Données- High Priority1	AF21	18	2
Données- High Priority2	AF22	20	2
Données- High Priority3	AF23	22	2
Données – Medium Priority 1	AF11	10	1
Données – Medium Priority 2	AF12	12	1
Données – Medium Priority 3	AF13	14	1
Données – Best Effort	BE	0	0

Figure 3. Interprétation des valeurs du champ ToS et recommandation d'utilisation

AFxy Assured Forwarding (x=class, y=drop precedence) (RFC2597)
EF Expedited Forwarding (RFC 3246)

La table de conversion entre DSCP et IP Precedence est la suivante :

DSCP Name	DS Field Value		IP Precedence
	Binary	Decimal	
CS0	000 000	0	0
CS1	001 000	8	1
AF11	001 010	10	1
AF12	001 100	12	1
AF13	001 110	14	1
CS2	010 000	16	2
AF21	010 010	18	2
AF22	010 100	20	2
AF23	010 110	22	2
CS3	011 000	24	3
AF31	011 010	26	3
AF32	011 100	28	3
AF33	011 110	30	3
CS4	100 000	32	4
AF41	100 010	34	4
AF42	100 100	36	4
AF43	100 110	38	4
CS5	101 000	40	5
EF	101 110	46	5
CS6	110 000	48	6
CS7	111 000	56	7

Classification du trafic réseau

L'utilisation du Modular QoS CLI (MQC) permet de réduire la complexité de configuration afin de créer des classes de services avec des politiques différentes. Une classe de trafic contient trois éléments essentiels : le nom de la classe, une série de commandes **match,** et comment évaluer ces commandes match.
Les commandes match sont utilisées pour spécifier divers critères de classification des paquets. Les paquets sont vérifiés pour déterminer s'ils appartiennent ou non à ces critères spécifiés par la commande match.
En utilisant la classification des paquets on peut par la suite partitionner notre réseau en plusieurs niveaux de priorités ou en classes de services (**class-map**).

Paramètres des class-map

routeur(config)#class-map *nom-de-la-classe*

On associe un nom à une class-map pour mieux la désigner par la suite

routeur(config)#class-map match-all *nom-de-la-classe*

On spécifie que TOUS les critères doivent être vérifiés pour que le paquet appartienne à la classe.

routeur(config)#class-map match-any *nom-de-la-classe*

On spécifie qu'AU MOINS un des critères doit être vérifié pour que le paquet appartienne à la classe.

routeur(config-cmap)#match access-group *numéro-de-l'ACL*

On spécifie que le paquet doit vérifier l'ACL correspondante pour qu'il appartienne à la classe.

routeur(config-cmap)#match any

On spécifie que tous les paquets seront dans cette classe.

routeur(config-cmap)#match {destination ou source}-address mac *adresse*

On spécifie que le paquet doit vérifier l'adresse MAC source ou destination pour qu'il appartienne à cette classe.

routeur(config-cmap)#match input-interface *nom-de-l'interface*

On spécifie que le paquet doit vérifier l'interface d'entrée indiquée pour qu'il appartienne à la classe.

routeur(config-cmap)#match ip dscp *valeur-du-ip-dscp*

Pour l'utilisation de DiffServ on a la possibilité de spécifier la valeur du **ip dscp** entre **0 et 63** pour que le paquet appartienne à la classe.

routeur(config-cmap)#match ip precedence *valeur-de-champs-TOS*

3 bits du champ TOS dans l'entête ip forment *l'IP precedence* utilisée pour la qualité de service. Dans un paquet reçu, si la valeur de ce champ est égale à la valeur indiquée ici alors le paquet appartient à cette classe.

routeur(config-cmap)#match protocol *protocole*

On spécifie le protocole suivant lequel les paquets appartiennent à la classe

Exemples :
Nous pouvons aussi assurer le filtrage et la classification des flux en fonction du protocole avec l'utilisation de la commande **class-map** et **match protocol** comme l'exemple suivant :

```
class-map match-any web-traffic
match protocol http
match protocol secure-http
match protocol ipsec
match protocol dns
```

A l'entrée du routeur, une vérification sur le type de trafic est effectuée pour établir une classification en fonction du protocole utilisé. Nous pouvons aussi établir une classification du trafic en fonction de l'URL avec la même commande voir l'exemple suivant :

```
class-map match-any scum
match protocol http url "*youtube*"
match protocol http url "*video.google*"
match protocol http url "*myspace*"
```

En outre, la commande **class-map** permet aussi de vérifier si les paquets entrant sont déjà marqués ou pas

afin respecter la politique de QoS. L'exemple suivant, nous montre l'utilisation de la commande **class-map** avec la spécification **« *ip dscp* »** dans le but de détecter les paquets déjà marqués avec un dscp = af31 :

```
class-map match-all VOIP
match ip dscp af31
```

b) Création d'une politique de service

Maintenant qu'on a différencié le trafic on doit partager la bande passante de notre routeur. C'est pourquoi on doit utiliser des politiques de priorités (**policy-map**). C'est à partir du moment où on utilise les **policy-map**, qu'effectivement on met en place la Qualité de Service voulue.
Une policy-map contient trois éléments : le nom de la politique, les classes associées et les commandes de qualité de service.

Paramètres des Policy-map

routeur(config)#policy-map *nom-de-la-policy-map ;* On spécifie un nom pour la policy-map

routeur(config-pmap)#class *nom-de-la-classe*

On spécifie le nom de la classe sur laquelle on veut appliquer la politique de qualité de service

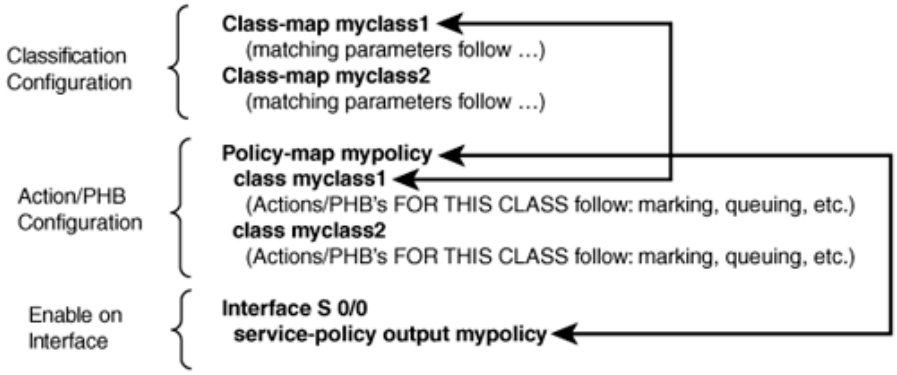
routeur(config-pmap-cmap)#bandwidth *debit en kbps ou pourcentage*

On spécifie la bande passante du routeur qu'on veut allouer à cette classe

routeur(config-pmap-cmap)#pritority *en kbps ou en percentage*

On spécifie pour la classe une bande passante avec un niveau de priorité élevé. Cette commande est en général utilisée pour le trafic temps réel.

Les commandes MQC et leurs corrélations sont montrées dans la figure suivante :



Exemple : Dans l'exemple suivant, une politique de QoS est crée pour attribuer 35% du débit sortant au trafic web.

```
policy-map inbound-internet
class web-traffic
bandwidth percent 35
```

Pour afficher la configuration actuelle du routeur il suffit d'utiliser les commandes suivantes :

```
show policy-map <policy-map-name>
show class-map <class-map-name>
show policy-map interface <interface>
show interface <interface>
```

Cas pratique 1 :

Nous allons configurer le routeur **R1** afin de différencier le trafic **FTP** des autres trafics réseau.

Etape 1 : Création de la classe de service

Créer une **class-map** pour marquer tous les paquets FTP comme « critical »

```
Router(config)#class-map match-all critical
Router(config-cmap)#match protocol ftp
```

Etape 2 : Création de politique de service

La politique de service nommée «**markingpolicy**» appliquée au paquet FTP est fixée à 2 comme **IP precedence**

```
Router(config)#policy-map markingpolicy
Router(config-pmap)#class critical
Router(config-pmap-c)#set precedence 2
```

Etape 3 : Attachement de la politique à une interface

Après avoir créé une politique de service il faut l'appliquer sur une (ou les deux) interface(s) du routeur. Suivant le flux du trafic il est possible de l'attacher soit à l'interface entrante soit à l'interface sortante. Par exemple pour limiter les paquets arrivant de l'extérieur afin d'éviter la congestion du réseau internet on l'applique sur l'interface entrante.

```
Router(config)#interface Serial 0/0/0
Router(config-if)#service-policy output markingpolicy
```

Il faut vérifier que le routeur (R1) est bien configuré ; il suffit d'utiliser la commande suivante :

```
Router#show policy-map interface Serial 0/0/0
FastEthernet0/0
  Service-policy output: markingpolicy
    Class-map: critical (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ftp
      QoS Set
        precedence 2
          Packets marked 0
      Queueing
        Output Queue: Conversation 265
        Bandwidth 0 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Etape 4 : Tester la configuration du routeur R1
Le PC0 génère un trafic FTP pour le PC1 et le Laptop0 génère des requêtes ICMP pour la même destination PC1. .
La génération de trafic réseau est assurée par l'application « Traffic Generator » dans le cas de « Packet Tracer ».

Si vous travaillez avec Packet Tracer, il faut passer au mode simulation et activer les trafics FTP et ICMP de manière périodique chaque 4 secondes. Lancer des captures avec un filtre sur les protocoles TCP et ICMP. Analyser les en-têtes des paquets reçus au niveau du PC1.

Questions :

1) Est-il possible de filtrer les paquets avec la commande « **access-lists** » on se basant sur le champ DSCP? Si oui donner la commande qui permet de filtrer les paquets dont le DSCP est marqué "EF" (Expedited Forwarding).
2) Sur un routeur donné R1, comment peut-on marquer les paquets "telnet" destinés ou originaire du routeur R1 pour leur attribuer un niveau de Precedence IP 6?

Remarque : Afin de convertir la notation de la classe AFxy en valeur décimale, vous pouvez utiliser la formule suivante **: « 8x + 2y = valeur décimale».**
Exemple pour la classe AF41 : (8*4)+(2*1) = 34