RT2 – Modules M3102 et M3103

Travaux Dirigés

Plan :

TD1 : Architecture des ISP et fonctionnement de BGP

TD2 : Occupation de ressource et TCP

TD3 : Qualité de service

TD4 : MPLS, LDP et L3-VPN

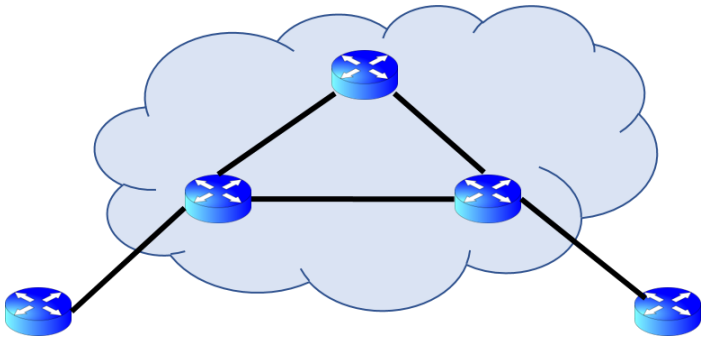
TD1 : Architecture des ISP et routage BGP

Exercice 1 : Architecture de ISP et bases de BGP

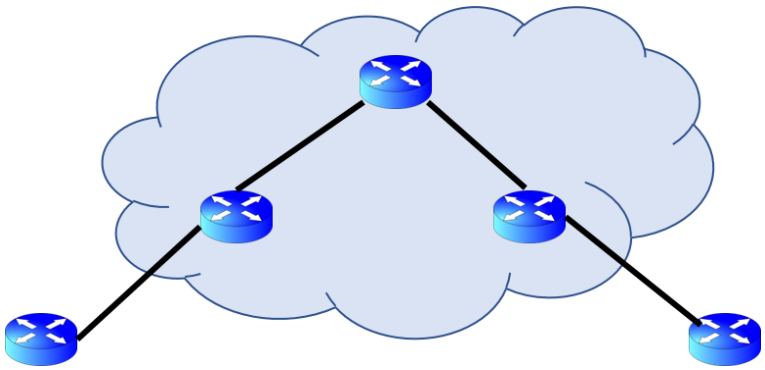
1. Définir les termes transit et peering et donner leur caractéristiques respectives.
2. A quel endroit physique une relation de peering est-elle établie ?
3. Quels sont les équipements qui y sont mis en jeu (dans la version simple) ?
4. Y a-t-il uniquement des opérateurs (ISP) à ces points ?
5. Définir *Autonomous System* (AS).
6. Quel est le terme générique désignant les protocoles de routage limité à un AS ?
7. Quel est le seul protocole de routage autorisé pour l'échange de routes entre AS ?
8. Quelles sont ces 2 versions et à quoi correspondent-elles ?
9. Quelle est sa caractéristique de fonctionnement principale ?

Exercice 2 : Fonctionnement de BGP

1. A quoi correspond la règle de découpage d'horizon ?

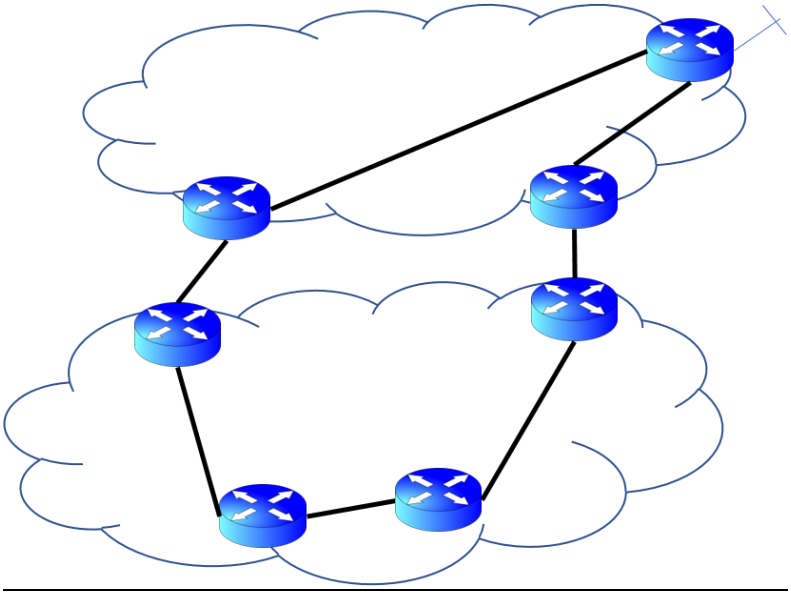


2. A quoi correspond la règle de synchronisation ?



3. Comment BGP sélectionne, parmi plusieurs routes menant au même réseau, celle à introduire dans la table de routage générale du routeur ?

4. Expliquez sur l'exemple vu en cours ce que permet l'attribut MED.



TD2 : Occupation de ressource et TCP

Exercice 1 : Utilisation (occupation) du réseau et congestion

1. Donner la définition de congestion dans les réseaux.
2. En quoi la congestion nuit-elle à la QoS ?
3. Quels sont les 2 buts d'un ISP ?
4. Quels sont les 4 buts de TCP ?
5. Quels sont les paramètres à prendre en compte pour réaliser ces objectifs ?
6. Décrire le fonctionnement de TCP Tahoe (3 ou 4 phrases).

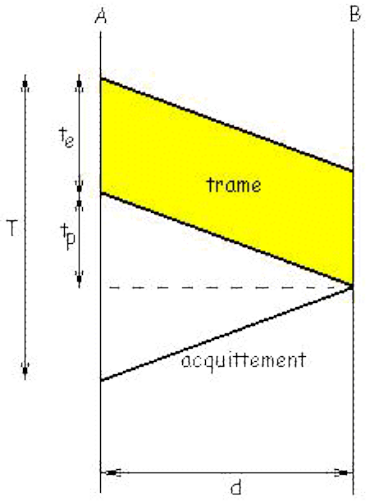
Exercice 2 : Gestion simpliste du débit injecté dans le réseau

Dans le but d'éviter la congestion du réseau sans connaître la bande passante (débit) disponible, on peut utiliser un protocole fonctionnant avec accusé de réception (*acknowledgement*, noté ACK). L'ACK permet d'assurer la source que le réseau n'est pas congestionné. S'il l'était, le paquet aurait été abandonné par un équipement intermédiaire et l'ACK n'aurait pas été reçu. Il existe de nombreux types de protocoles avec accusés de réception. On va en voir 3 différents dans les 3 exercices suivants.

On imagine un protocole avec ACK le plus simple possible, obéissant aux règles suivantes :

- le débit maximum est D
- à la suite de l'envoi d'une paquet par la station A, un ACK est renvoyé à A par la station B destinataire de la paquet. On considérera que cet ACK peut être réduit à 1 bit.
- la longueur L de la paquet est fixe

On désigne par d la distance entre les stations A et B et par v la vitesse de propagation d'un signal (correspondant ici à un bit) dans la voie reliant A et B.



1. Exprimer le temps total de transmission d'une paquet T (depuis l'émission du premier bit jusqu'à la réception de l'ACK) en fonction de L, D, d, v.
   NB1 : cette question nécessite de bien faire la distinction entre vitesse de propagation et débit de données
   NB2 : dans le cas général (réseaux réels), on ne peut pas connaître v et d pour les raisons mentionnées en réponse à la question 5 de l'exercice 2 précédent.
2. L'efficacité Θ du protocole est définie comme le débit moyen obtenu par la destination, divisé par le débit maximum disponible. Exprimer Θ en fonction du rapport $a = t_p/t_e$.
3. Application numérique : Calculer θ pour L=1024 bits ; D = 64 Kbits/s ; d = 1000 m ; v = 2.10^8 m/s
4. Application numérique : Calculer θ pour L = 53 octets ; D = 155 Mbits/s ; d = 1000 m ; v = 2.10^8 m/s (situation présentant des analogies avec l'ATM).
5. A partir des résultats des deux applications numériques précédentes, quelles conclusions pouvez-vous en tirer ?

Exercice 3 : Gestion évoluée du débit injecté dans le réseau pour maximisation de l'occupation sans congestion – Le cas idéal

On utilise dans la transmission de paquets d'un émetteur A vers un récepteur B un protocole défini de la manière suivante :

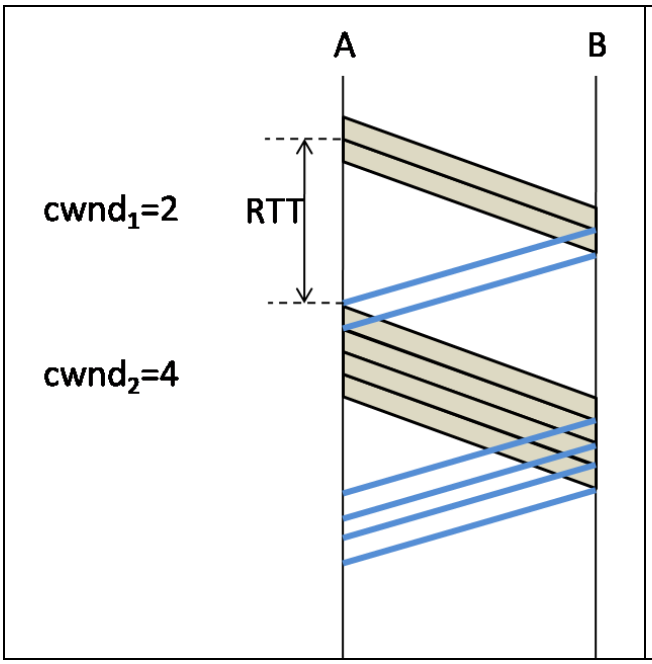
- L'émetteur envoie successivement N=3 paquets puis attend leur acquittement de la part de B.
- Quand cet acquittement arrive, l'émetteur envoie les N paquets suivantes et attend un nouvel acquittement.
- Les paquets sont composés de B_{tot}=1024 bits dont B_c=80 bits de contrôle.
- Les acquittements sont composés de B_{ack}= 64 bits.
- La bande passante disponible est de D_n=2 Mbits/s et la vitesse de propagation des ondes électromagnétiques est de v=3.10^8 m/s sur la voie de d=10 km reliant A et B.

1. Quelle est la durée T nécessaire à l'expédition confirmée d'un paquet ? On décomposera T en T_e (temps d'émission d'un paquet), T_p (temps de propagation) et T_a (temps d'émission de l'ACK).
2. Exprimer l'efficacité Θ du protocole en fonction des paramètres de l'énoncé.
3. Trouver N permettant de maximiser le taux d'utilisation.
4. De quoi dépend N ?
5. Un message de 1 Mo est envoyé de A vers B par utilisation du protocole précédent. Quelle est la durée totale de la transmission de ce message ?

Exercice 4 : TCP en slow start – se rapprocher du cas idéal quand les paramètres du réseau ne sont pas connus

Pour transmettre des messages entre deux stations A et B. Nous sommes dans le cas général (NB1 de question 1 de exercice 2 précédent), dans lequel doit fonctionner le protocole TCP. Ce protocole est capable uniquement de mesurer le temps écoulé entre l'émission d'un paquet et la réception de l'ACK correspondant, appelé *Round-Trip Time* (RTT, ou temps d'aller-retour).
On suppose que les paquets générés au niveau de la couche transport ont tous une taille de ***m*** bits. Un segment est émis à un débit ***r*** bps. Le débit maximum possible sur cette liaison est de ***C*** bps. On négligera la taille d'un ACK.

On rappelle que la fenêtre de congestion est l'ensemble des paquets envoyés dont les ACKs n'ont pas encore été reçus. Pour cette transmission, on utilise une version de TCP qui rajoute un paquet à la fenêtre de congestion à chaque ACK reçu : la taille ***cwnd*** de la fenêtre est donc doublée à chaque **RTT** (round-trip time, ou temps d'aller-retour). Voir figure ci-après.
Tous les résultats doivent être donnés sous forme littérale uniquement.



1. Quel est la valeur du RTT en fonction de T_e , le temps d'émission d'un segment, et T_p le délai de propagation.

2. On définit un cycle comme un aller-retour. Deux cycles sont représentés sur la figure : cycle *i* où la taille de la fenêtre est $cwnd_i$, pour i=1 et i=2.
   Exprimer le débit D_i appliqué en entrée du réseau par A au cycle *i* en fonction de $cwnd_i$ et des autres paramètres (quelque soit ***i*** entier positif).

3. Exprimer le nombre *N* de cycles et le temps correspondant *L* pour que le débit appliqué par A en entrée du réseau atteigne *C*. Dans ce cas-là, quel est le taux d'utilisation du lien ?

TD3 : Qualité de service

Exercice 1 : Bases de la QoS

1. Donner la définition de congestion dans les réseaux.
2. En quoi la congestion nuit-elle à la QoS ?
3. Pourquoi le traitement de la QoS est-il indispensable, même dans un réseau surdimensionné par rapport aux besoins des utilisateurs ?
4. Avec quels paramètres peut-on mesurer la QoS ?
5. Quelles applications nécessitent de la QoS ?
6. Quelles sont les 3 grandes stratégies de traitement de la QoS ?
7. Quand un client achète un certain niveau de QoS, quels traitements sont réalisés dans l'équipement de bord de l'opérateur ?
8. Avec quels types de techniques l'opérateur traite-t-il la QoS dans le cœur du réseau ?
9. Mentionner et définir les techniques qui vous semblent représentatives, au sein de ces 2 types.
10. Quelle architecture de service (ou nom de champ dans l'entête IP) est actuellement utilisée dans les réseaux cœur pour spécifier le niveau de qualité de service requis par un paquet IP ? Décrivez son principe en une phrase.
11. Les token buckets et les leaky buckets sont deux manières de limiter le débit des données. Expliquer en quoi ils sont différents en termes de capacité à accepter les rafales dans le réseau, et garantir un débit de données moyen ou pic.

Exercice 2 : Limiter le débit pic ou le débit moyen : sceau percé et sceau à jeton

Dans cet exercice, aucune valeur numérique ne doit apparaître, toutes les réponses seront données uniquement sous forme littérale. N'hésitez pas à faire des schémas pour vous aider.

1. On suppose un leaky bucket de débit **r** et taille de buffer **b**.
   On observe le comportement suivant en sortie du leaky bucket (Figure 1). Exprimez la condition pour qu'aucun paquet ne soit abandonné à cause de la rafale. Cette condition sera exprimée sous la forme d'une inégalité reliant le débit $\mathbf{d_{burst}}$ de la rafale, sa durée $\mathbf{t_{burst}}$, **r** et **b**.

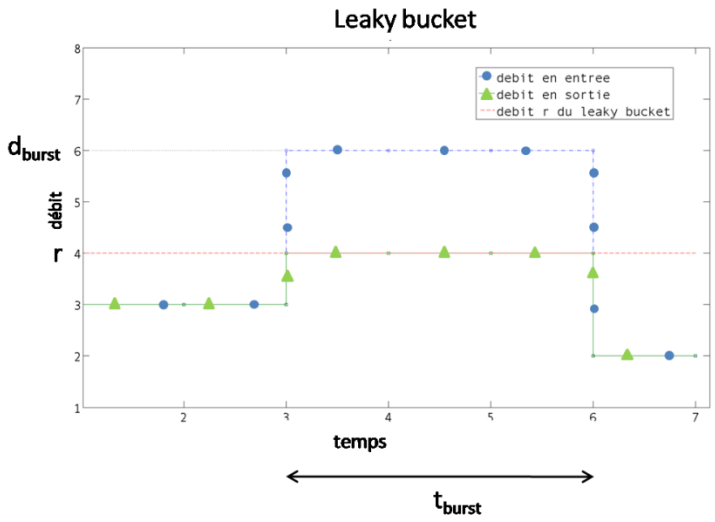


Figure 1

2. On suppose un token bucket de débit **r** et de taille **b**.
   La Figure 2 représente le débit en sortie et le débit en entrée du seau. Donner la condition pour que le phénomène apparaissant sur la figure ne se produise pas, c'est-à-dire la condition pour que le débit de sortie soit constamment le même que celui d'entrée. Cette condition sera exprimée en fonction du débit $\mathbf{d_{burst}}$ de la rafale, sa durée $\mathbf{t_{burst}}$, **r** et **b**.

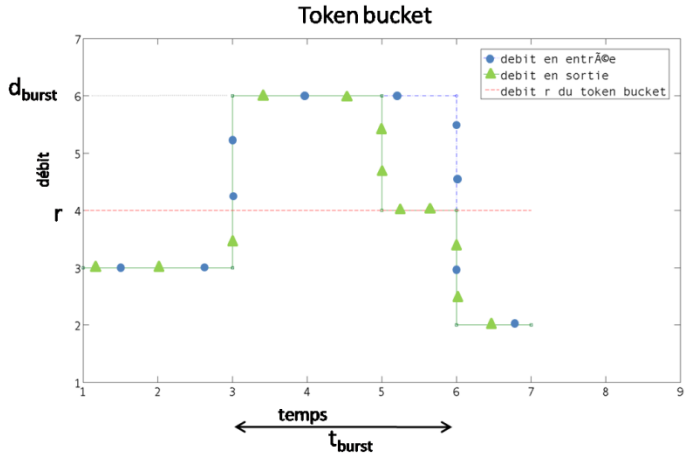


Figure 2

3. On considère un token bucket de débit **r** et de taille **b**.
   La Figure 3 représente une première rafale (de l'instant 3 à l'instant 5 sur la figure). En supposant que le seau a été vidé par cette rafale, donnez la condition sur le débit $\mathbf{d_f}$ du trafic en entrée pendant une durée $\mathbf{t_f}$, **r** et **b** pour que le seau soit à nouveau plein quand la deuxième rafale débute.

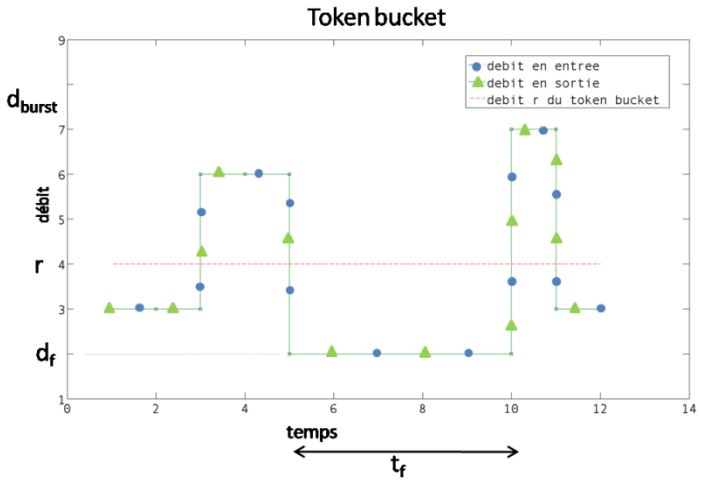


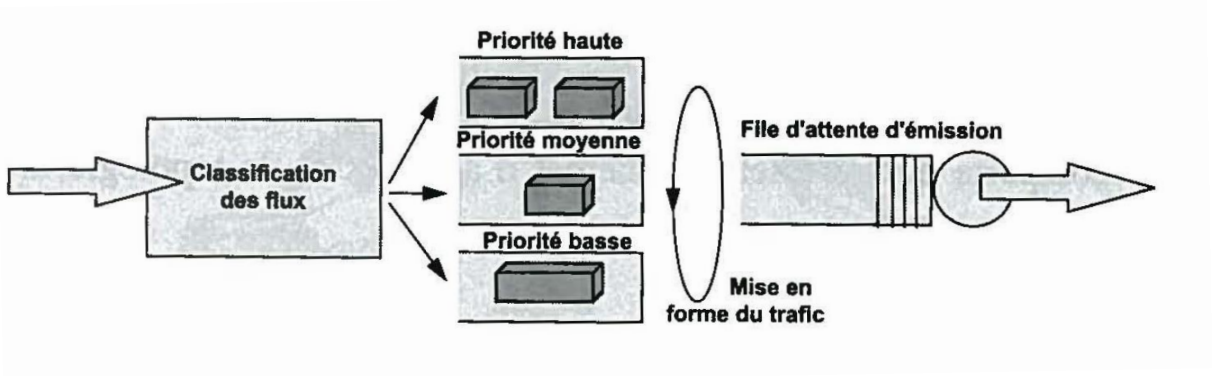
Figure 3

Exercice 3 : Abandonner des paquets en situation de congestion ou à l'approche : gestion de buffer

1. Donner la définition de la politique de gestion de file « DropTail ».
2. En supposant 3 connexions TCP partageant un lien goulot d'étranglement (*bottleneck*) entre 2 routeurs, que va avoir comme effet l'usage de DropTail au routeur d'entrée du goulot d'étranglement sur : le débit d'une part, et le délai d'autre part.
3. Donner la définition de la politique de gestion de file « Random Early Detection » (RED).
4. Dans la configuration de la question 2, quel impact a l'usage de RED sur le débit et le délai ?

Exercice 4 : Faire passer les paquets prioritaires d'abord : ordonnancement de files d'attente

La méthode la plus utilisée aujourd'hui pour garantir aux applications une certaine qualité de service consiste à assurer à chaque type de flux un service différencié. La figure en illustre le principe :



Selon des critères définis par l'administrat·eur·rice du réseau (@IP, Port, champ DS, Tag 802.1p, etc) les données sont placées dans un file d'attente spécifique. Les différents systèmes se différencient selon la manière dont sont lues les données (mise en forme et/ou ordonnancement), avant d'être émises.

Dans le système représenté précédemment, la bande passante est affectée aux files d'attente selon une pondération définie par l'administrat·eur·rice réseau (WRR, *Weighted Round Robin).* Par exemple
si la file d'attente de haute priorité a un poids de 5, celle de moyenne priorité 3 et celle de basse priorité 2, le système lira 5 blocs de données de la file 1, puis 3 blocs de la file 2 et enfin 2 de la file 3. Si une file d'attente est vide, le système passe immédiatement à la suivante.

Votre système informatique met en oeuvre trois types d'application:
- Voix sur IP.
- Clients/serveur.
- Transfert de fichiers.

Votre administrat·eur·rice réseau décide d'affecter respectivement la moitié de la bande passante aux applications voix, 30 % aux applications clients/serveur et seulement 20 % aux applications de transfert de fichiers, pour cela il affecte aux files d'attente les poids de 5, 3 et 2.

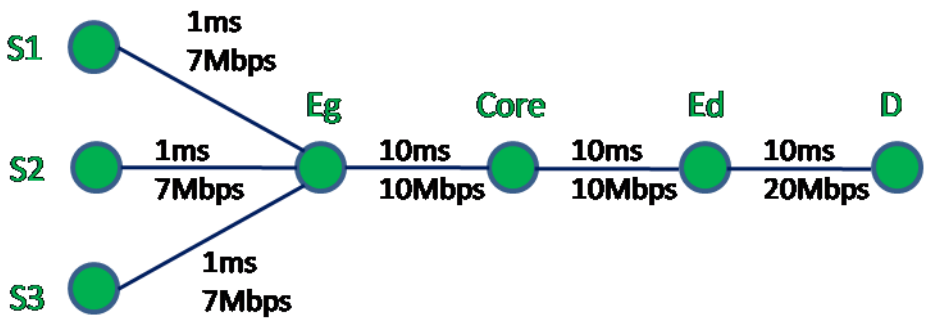
1. Dans ces conditions, si le débit du lien est 2 Mbit/s, calculez quelle est, *a priori,* la bande passante maximale et minimale susceptible d'être allouée à chacun des flux.

2. En admettant que chacun des flux soit caractérisé par une taille moyenne de blocs de données de 40 octets pour la voix, 256 pour les applications clients/serveur et 1 500 octets pour les applications de transfert de fichiers (pour simplification on négligera les données protocolaires) :
   a. Calculez la bande passante maximale et minimale réellement affectée à chaque type de flux. Que pensez-vous de votre réponse à la première question?

   b. Déterminez les poids qui assureraient le respect de la bande minimale allouée à chaque flux.

<u>Exercice 5 : Marquer l'entête IP des paquets pour indiquer leur priorité : DiffServ</u>

Nous considérons l'utilisation de DiffServ. Nous allons considérer une certaine topologie de réseau avec du trafic prédéfini. La figure ci-après représente la topologie. Trois flux UDP portant une application CBR de débit 10Mbps, sont générés à S1, S2 et S3, à destination de D.
Les paquets IP générés à S1, S2 et S3 vont d'abord arriver au routeur Eg, routeur de bord de l'opérateur, où ils vont être marqués avec des priorités différentes, et traités en conséquence dans les routeurs Eg, Core et Ed. Ed fait de même avec le trafic dans l'autre sens venant de D (seulement les ACKs de possibles connexions TCP dans notre cas).



1- Regarder le fichier diffserv.tcl du sujet de TP2, et joint en annexe en fin de fascicule. Lisez et analysez ce fichier, et répondez aux questions suivantes:
   a. Sur quel critère les 3 flows sont-ils différenciés ? (type d'application ? ou paire source-destination ? ou protocole de transport ?...)
   b. Quelle est la différence entre files physiques et virtuelles ?
   c. Quels sont les critères avec lesquels les paquets sont mis dans chaque file physique et dans chaque file virtuelle ?
   d. Décrivez le type de buffer management associé à chaque file physique.
   e. Quels sont les choix possibles, dans le code tel qu'il vous est fourni, pour l'ordonnancement entre les différentes files physiques ?
   f. D'après vous, à quoi sert la variable *meanPktSize*, et à quoi correspondent les valeurs qu'elle prend ?

2- Décrire la politique d'ordonnancement « Strict Priority » de plusieurs files d'attente.
3- Si les poids weightWRR1, weightWRR2 et weightWRR3 sont respectivement à 10, 5 et 2, quels seront les débits obtenus par chaque connexion ? Une formule littérale directe application de la définition de la politique d'ordonnancement « Weighted Round Robin » permettra de répondre facilement.
4- D'après vous, quels sera l'ordre des délais obtenus par les paquets de chaque connexion ?

TD4 : MPLS, LDP et L3-VPN

Exercice 1 : Notions fondamentales sur MPLS

1- Sur quel grand principe de transfert de l'information Frame Relay, ATM et MPLS reposent-ils ?
2- A la suite de quelle autre norme MPLS a t-il été introduit, et pour quelles raisons ?
3- Décrire comment un paquet IP est pris en charge par un réseau utilisant MPLS.
4- Donner la définition de l'ingénierie de trafic.
5- Comment fonctionne l'ingénierie de trafic avec MPLS ? (en 5 lignes max)
6- Qu'est-ce qu'un IP-VPN et un VPLS ?
7- Quel est l'intérêt de ces 2 types de VPN basés sur MPLS en termes de gestion d'adresses pour les clients?

Exercice 2 : Utilisation de la FLIB (manipulation de labels MPLS)

Une table regroupant la table de routage et les actions à effectuer en fonction et sur les labels MPLS s'appelle une FLIB (Forwarding Label Information Base). Pour plus de commodité, on peut la voir comme 3 sous-tables (ce qui peut aussi être un type d'implémentation de la FLIB) :

- **ILM** : Correspondance entre label d'entrée et numéro de l'action à faire.
- **FTN** : Correspondance entre une FEC (classe d'équivalence) d'entrée et numéro de l'action.
- **NHLFE**: Correspondance entre numéro et action.

Soient les tables suivantes :

FTN

FEC	NHLFE
132.12.17.0/25	(3)
123.1.4.192/26	(5)
129.175.32.0/24	(7)
129.175.23.0/25 TOS=184(10111000)	(11)
129.175.23.0/25	(8)
147.193.160.0/19	(17)
0.0.0.0/0	(20)

ILM

Label	NHLFE
15	(1)
22	(4)
145	(6)
234	(12)
456	(4)
989	(19)
1087	(2)

NHFLE

Entry	Operation	Label	Next Hop	Interface
(1)	swap	311	131.1.2.1	eth0
(2)	swap+push	786 555	131.2.3.4	eth1
(3)	push	561	131.1.2.1	eth0
(4)	pop	-	-	eth0
(5)	push	234	131.2.3.4	eth1
(6)	swap	561	131.1.2.1	eth0
(7)	push	89	131.1.2.1	eth0
(8)	push	77	131.2.3.4	eth1
(11)	push	90	131.1.2.1	eth0
(12)	pop	-	-	eth1
(17)	push	178	131.1.2.1	eth0
(19)	swap	234	131.2.3.4	eth1
(20)	push	1111	131.2.3.4	eth1
(21)	swap	14	131.2.3.4	eth1

Questions :

Indiquez l'en-tête MPLS en sortie pour les paquets suivants :

1. Paquet sans étiquette avec pour adresse destination 132.12.17.129.

2. Paquet avec étiquette 145.
3. Paquet sans étiquette avec pour adresse destination 129.175.23.72 et le champ TOS = 184.
4. Paquet avec étiquette 456.
5. Paquet sans étiquette avec pour adresse destination 129.175.32.15.
6. Paquet sans étiquette avec pour adresse destination 129.175.23.11 et le champ TOS = 189.
7. Paquet avec étiquette 15.
8. Paquet sans étiquette avec pour adresse destination 147.193.175.234.
9. Paquet avec étiquette 234.
10. Paquet sans étiquette avec pour adresse destination 123.1.4.195.
11. Paquet avec étiquette 1087.
12. Paquet sans étiquette avec pour adresse destination 132.12.17.126

Exercice 3 : Création de la FLIB

Soit la table de routage unicast suivante :

Préfixes	Prochain saut	Interface
15.1.3.224/27	-	eth0
15.1.3.192/27	-	eth1
15.1.3.0/27	-	eth2
134.1.3.0/24	15.1.3.2	eth2
129.175.0.0/16	15.1.3.194	eth1
132.4.5.0/23	15.1.3.194	eth1
131.3.4.128/25	15.1.3.2	eth2
0.0.0.0/0	15.1.3.227	eth0

Le routeur reçoit les « mappings » LDP suivant

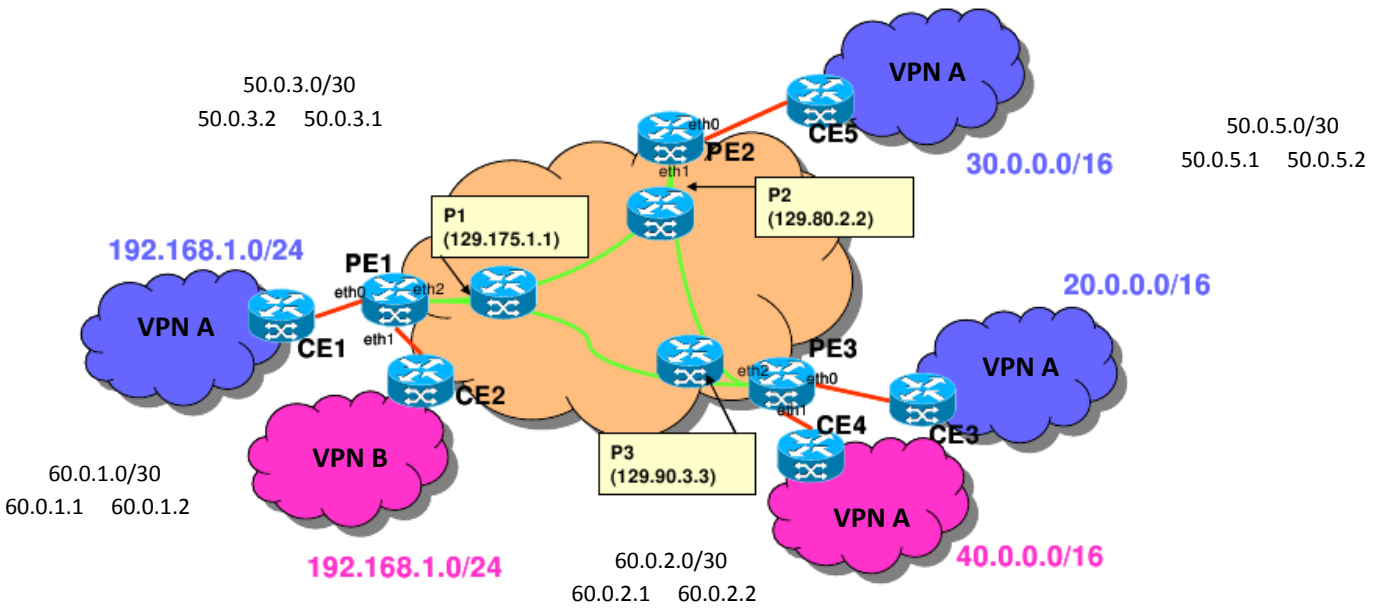
1. mapping 56 prefix 132.4.5.0/23 provenant de 15.1.3.227
2. mapping 20 prefix 134.1.3.0/24 provenant de 15.1.3.2
3. mapping 22 prefix 131.3.4.128/25 provenant de 15.1.3.2
4. mapping 144 prefix 132.4.5.0/23 provenant de 15.1.3.194
5. mapping 321 prefix 129.175.0.0/16 provenant de 15.1.3.2
6. mapping 1234 prefix 111.1.1.192/26 provenant de 15.1.3.227
7. mapping 675 prefix 129.175.0.0/16 provenant de 15.1.3.194

Question : Sur la table de routage on voit que le routeur a trois sous-réseaux directement connectés, donnez les tables MPLS en conséquence.

Exercice 4 : Création d'un IP-VPN

50.0.4.0/30

50.0.4.1 50.0.4.2



On considère que l'opérateur possède un réseau dans le cœur (entre les routeurs PE de bord de l'opérateur) duquel le transfert des paquets se fait par commutation MPLS. Les LSP établis entre PE1, PE2 et PE3 sont tels que le labels de départ pour aller de PE1 vers PE2 est label 12, de PE1 vers PE3 label 13, de PE2 vers PE1 label 21, de PE2 vers PE3 label 23, de PE3 vers PE1 label 31, de PE3 vers PE2 label 32.
Les adresses de bouclage du routeur PEx est x.x.x.x.

Cet opérateur a 2 clients avec un VPN pour chacun entre leurs sous-réseaux respectifs. Remplir les tables nécessaires à PE1 pour gérer ces 2 VPNs : la ***MPLS forwarding table*** et les 2 tables **VRF** (les tables privées de routage).

PE1

MPLS forwarding table

Label tag	Outgoing tag	Prefix	Outgoing interface	Next hop
	12	2.2.2.2/32	eth2	129.175.1.1
	Untag			

VRF A : VRF (ou VPN) label 128 attachée à l'interface _ _ _ _ _ _ _

Prefix	Next hop	Outgoing interface	Outgoing label

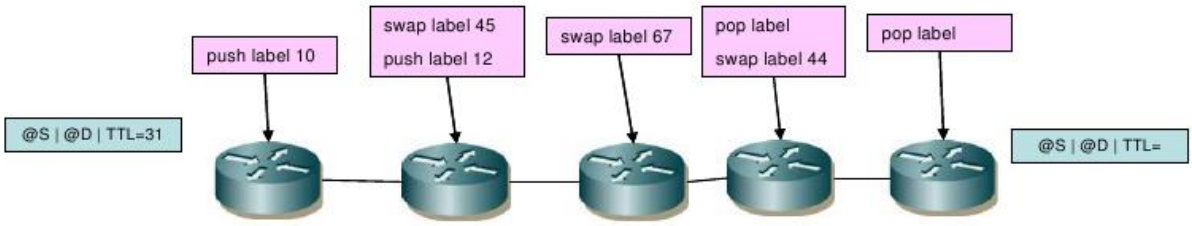
VRF B : VRF (ou VPN) label 64 attachée à l'interface _ _ _ _ _ _ _

Prefix	Next hop	Outgoing interface	Outgoing label

Exercice 5 : Gestion du TTL dans un réseau MPLS

Pour répondre aux questions suivantes, consulter d'abord l'annexe en fin de ce sujet.

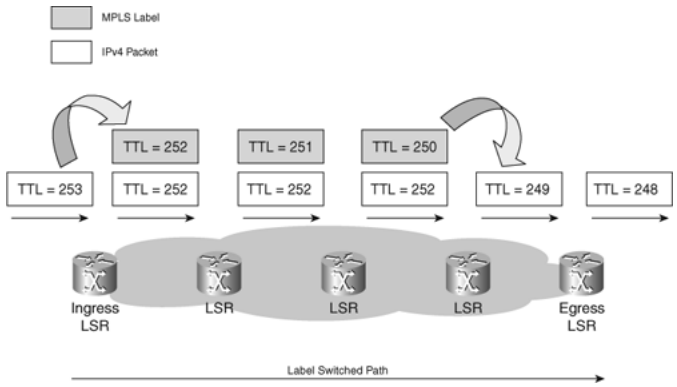
1. On considère le paquet de la figure ci-dessous et les routeurs ci-dessous. Le paquet traverse les 5 routeurs MPLS. Les « push/pop/swap » pour ce paquet sont indiqués au dessus de chaque routeur. Le paquet arrive sans étiquette sur le premier routeur. Indiquez la valeur des TTLs tout au long de ce chemin.



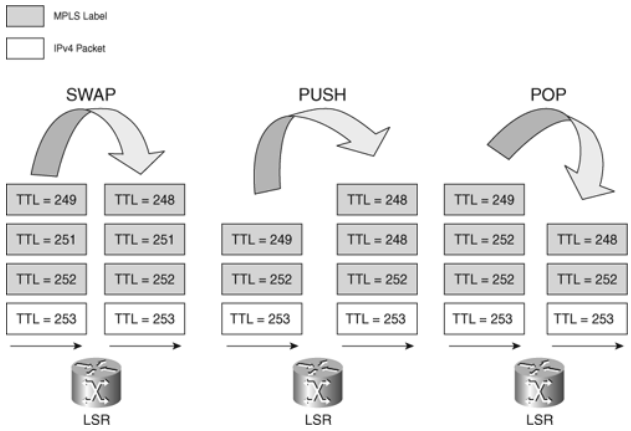
2. Que se passe-t-il si le TTL d'un paquet expire dans le domaine MPLS ?

Annexe :

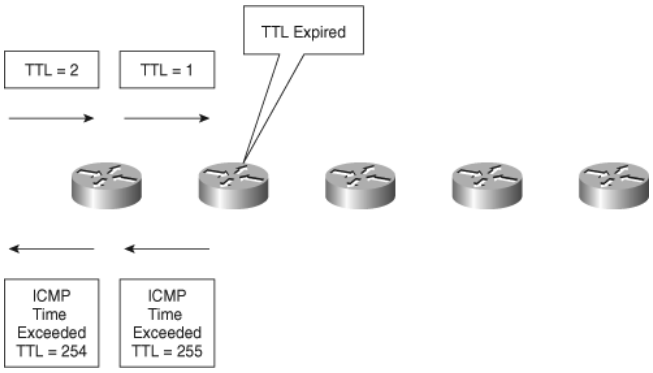
TTL Behavior in the Case of IP-to-Label or Label-to-IP:



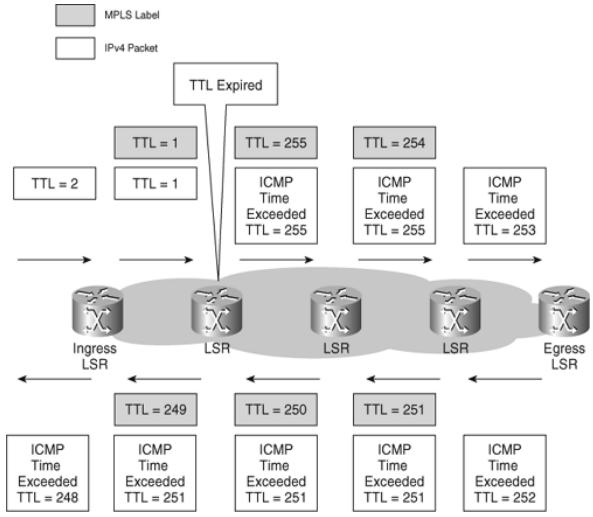
TTL Behavior in the Case of Label-to-Label:



TTL Expiration in an IP network:

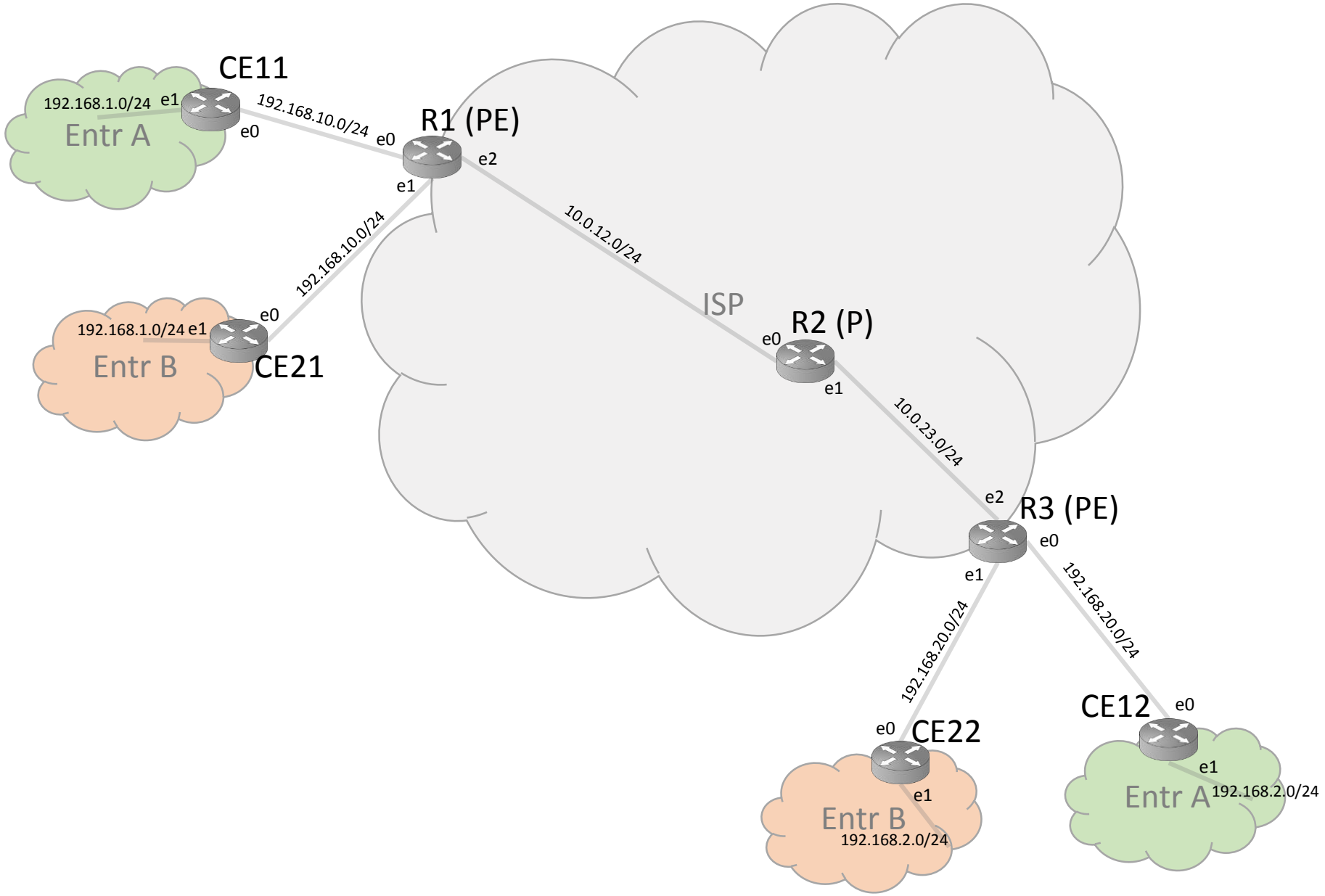


TTL expiration in an MPLS network:



Sources :

- Anthony Busson
- www.ciscopress.com


CE11
192.168.1.0/24
e1
Entr A
e0
192.168.10.0/24
e0
R1 (PE)
e2
e1
192.168.10.0/24
10.0.12.0/24
ISP
192.168.1.0/24
e1
e0
Entr B
CE21
e0
R2 (P)
e1
10.0.23.0/24
e2
R3 (PE)
e0
e1
192.168.20.0/24
192.168.20.0/24
CE12
e0
e0
CE22
e1
Entr B
192.168.2.0/24
e1
Entr A
192.168.2.0/24

CE11

Network	Next hop	Intf

R1 (PE)

Local tag	Outg tag	Network	Nxt hop	Intf

Network	Nxt hop	Int	Outg VPN label

Network	Nxt hop	Int	Outg VPN label

R2 (P)

Local tag	Outg tag	Network	Nxt hop	Intf

R3 (PE)

Local tag	Outg tag	Network	Nxt hop	Intf

Network	Nxt hop	Int	Outg VPN label

Network	Nxt hop	Int	Outg VPN label

CE12

Network	Next hop	Intf