

TD 6

51

Multicast (IP)

Q1

- 1) En unicast, on multiplie beaucoup le nombre de paquets transmis sur le réseau.
- 2) La profondeur d'un arbre binaire = 2^n . Le nombre de liens = $\sum z^i$
Pour un arbre avec 32 récepteurs on a donc nb liens = $2+4+8+16+32 = 62$ (dans le cas multicast)
- Pour de l'unicast on a : $5 \times 32 = 160$ car pour rejoindre un récepteur un paquet doit traverser 5 liens et il y a 32 récepteurs donc on a bien 32×5 .
- b) On observe qu'en unicast on doit envoyer plus du double de paquet par rapport à Multicast.

Q2

- 1) Toutes les @IP multicast commencent par 1110, il reste donc 28 bits pour le groupe ID
Il y 2^{28} multicast différentes $\approx 268\ 000\ 000$. Il existe des sous parties dans les @multicast.
ex: 224.0.0.0 \rightarrow 224.0.0.255 sont des @ réservé pour un usage technique (OSPF, RIP)
239.0.0.0 \rightarrow 239.255.255.255 sont des @ privées non routées sur internet.
Toutes les @ entre ces 2 plages (224.0.0.255 et 239.0.0.0) sont aussi réservées pour certains usages.

A) les plages ne sont pas des subnets

- 2) Il n'y a pas de garantie de remise particulière. C'est la même chose qu'en unicast. Les paquets peuvent être perdus, dupliqués, etc...
Les machines en périphérie du réseau peuvent rejoindre et quitter un groupe multicast. N'importe qui peut recevoir un paquet multicast mais aussi envoyer un paquet multicast à destination d'un groupe multicast.
Il ne faut donc pas compter sur le multicast pour la sécurité...

PIM est le protocole utilisé pour le multicast

Q3

- 1) Pour chaque groupe de multicast il existe une @MAC propre.
Rappel: @MAC = 48 bit

AA:AA:AA:BB:BB:B
ID constructeur ID propre à la carte

En multicast: l'ID constructeur est toujours le même 01:00:5E + les 23 bit de fin de l'@IP

Pour l'@ 224.10.8.5 \rightarrow 01:00:5E:0A:08:05 A Le 24ème bit vaut 0

Pour l'@ 224.138.8.5 \rightarrow 01:00:5E:0A:08:05

224.10.8.5 0 000,1010:0000,1000:0000,0101

224.138.8.5 1 000,1010:0000,1000:0000,0101
 23 bits

- 2) Avantage : il est simple de passer de l'@IP Multicast à l'@MAC du groupe.

- 3) Non pas bijective car on peut avoir la même @MAC à partir de 2 IP différentes.

Avoir la même @MAC (multicast) est rare. En cas de très grave, on reçoit juste le flux de l'autre groupe en +.

Q3) 4) Probabilité d'une collision: $P = \frac{2^5}{2^{28}} = \boxed{2^{-23}}$

5) $N = \text{nb total @ multicast} = 2^{28}$, Prob. d'une @IP A = $P(A) = \frac{1}{N}$

Prob. de choisir une @IP identique à A = $P(A) \times P(A) = \frac{1}{N^2}$

Probabilité de collision: $N \times \frac{1}{N^2} = \boxed{\frac{1}{N}}$

Pour 1000 sessions au lieu de 2: Probabilité devrait être $\approx 1000 @$ différentes.

$$P = 1 - P(\text{tirer 1000 @ identiques}) = \frac{N \times (N-1) \times (N-2) \times \dots \times (N-999)}{N^{1000}}$$

6) Non on ne doit pas remplacer son @IP par l'@IP du groupe multicast.

Il va juste accepter et process des IP des groupes auxquels il est.

Q4)

1) IGMP = Internet Group Message Protocol

IGMP Snooping = option qui permet au switch d'écouter les messages IGMP pour ne pas flood tous le réseau.

Il est obligé de s'interroger les hôtes régulièrement car il ne peut pas savoir si un hôte n'est plus au groupe (ou inversement un nouvel hôte a rejoint le groupe)

2) Non cela ne sert à rien que les 2 routeurs envoient des Host Membership Queries.

On peut désigner un routeur qui s'occupe de faire les Membership Queries pour tout le réseau.
 ↳ DR (designated routeur)

3) L'envoie d'un "Report" est temporisé pour éviter que la bande passante soit saturée.

Le time doit être < à celui du routeur (le timer (max-time-response)).

Si un récepteur voit passer un "Report" concernant son groupe (duquel il est toujours abonné) il n'envoie pas de Report. Non en broadcast.

4) Il envoie le "Join" quand il en a besoin pour minimiser le temps d'attente.

5) Non, il maintient une liste d'interfaces (la OIL) et pas de hosts. Pour chaque groupe il maintient une OIL. Avec les différentes "Query" il peut mettre à jour la table.

6) En IGMPV2 il y a la notion de leave. Quand un hôte quitte le groupe il envoie une query pour le groupe pour savoir si il reste des membres dans le groupe. Ce qui permet de supprimer l'interface de la table OIL et d'arrêter le flood quand plus aucun host est abonné au groupe. (il peut flood du traffic multicast dans un groupe vide car la MAJ n'est pas instantanée...)

TD 6

f3

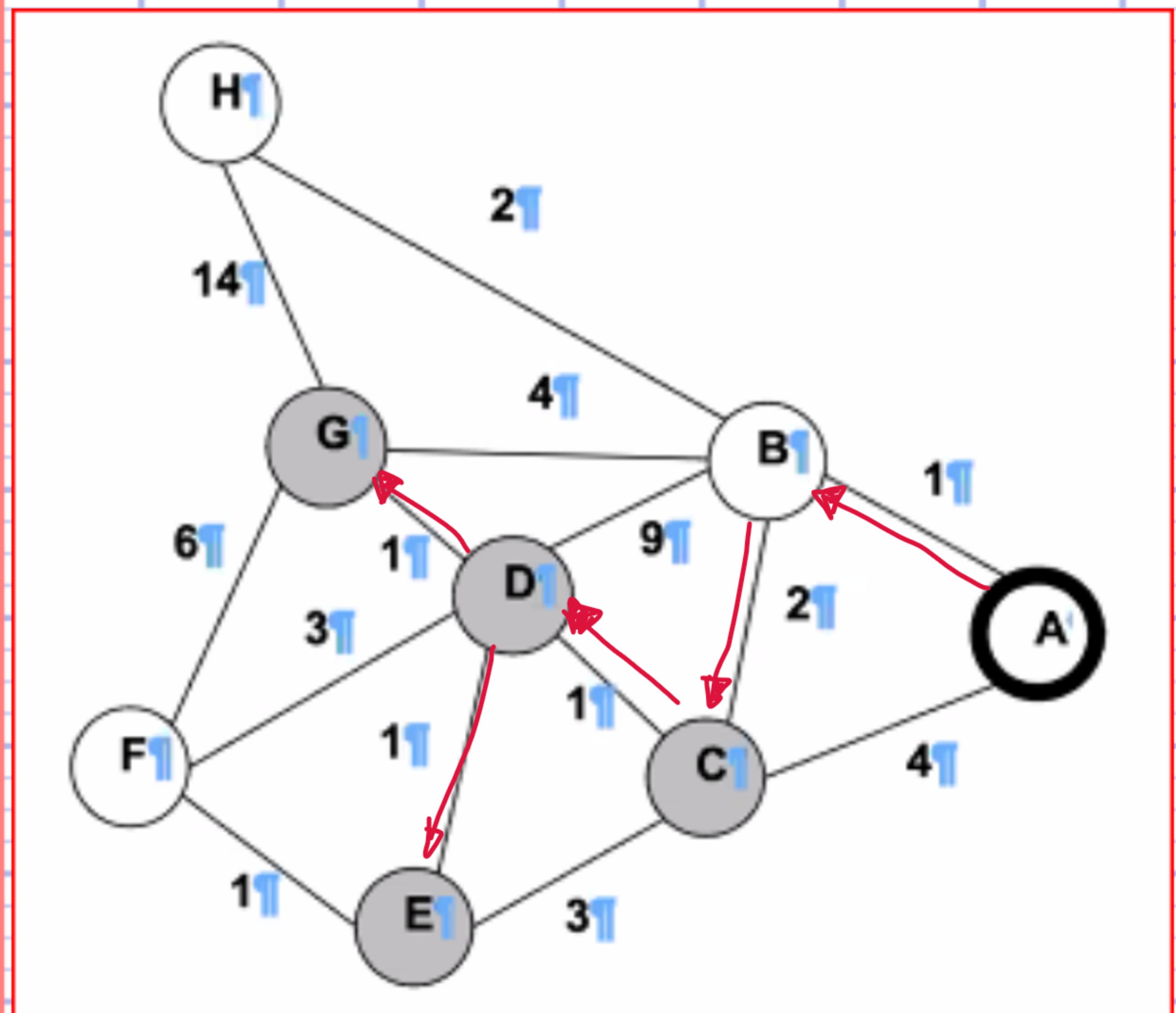
7) Ajout (à IGMP v3) de la notion d'abonnement à une source. Il peut même spécifier des sources auxquelles il ne veut pas s'abonner.

PIM: Il existe 2 mode pour paramétrer PIM.

- Dense mode: "Flood first, prune later", la première fois, la source envoie le paquets dans tous le réseau. Les routeurs qui n'ont pas besoin de ce paquet le signal à la source. À la prochaine émission la source n'envoie le paquet qu'aux routeurs qui sont abonnés.

- Sparse mode: Les hosts se mettent d'accord sur un routeur qui sera le point de rendez-vous (RP). Le RP sera alors le lien entre les 2 mondes (entre la source et l'arbre des hosts). La source envoie le multicast aux RP intéressé.

1) Arbre des + courts chemins reliant la racine (λ) à C, D, E et G



2)a) Il ne flodé pas sur l'interface d'entrée pour éviter les boucles de réseau.

b) floder sur un très grand réseau = saturation = KO.

3)a) ...

b) ...

c) Cela limite le Flooding

4) ...

prune = régulier
(n toutes les 3 min)
loop y a donc les 3 min...
s'abonne toutes les 3 min...