Réseaux : TP 1

# Important :

Au cour de ce TP, la machine A est une machine windows ne pouvant que rpéondre au ping, suite à la panne d’une machine de TP

2 :

Le découpage a été fait de la manière suivante :

Mes adresses ont été répartie en 2 adresses /26 et une adresse /25

* 192.168.1.0 /25 => adresses machines entre 192.168.1.1 et 192.168.1.127
* 192.168.1.128 /26 => adresses machines entre 192.168.1.129 et 192.168.1.191
* 192.168.1.192/26=> adresses machines entre 192.168.1.193 et 192.168.1.254 (255 est l’adresse de broadcast)

Host A : 10.0.0.2

Routeur B (Side Net1) : 10.0.0.1

Routeur B (Side Net2) : 192.168.1.129/26

Routeur C (Side net2) : 192.168.1.130/26

Routeur C (side net 3) :192.168.1.193/26

Routeur Cisco (side net3) : 192.168.1.194/26

Routeur Cisco (side net4) : 192.168.1.1 /25

Host D (SIde net4) : 192.168.1.2/25

3 : Configuration :

(destination, gateway)

table de routage : hote D :

Destination Gateway

default 192.168.1.1

Routeur C :

Destination Gateway

10.0.0.0/8 192.168.1.129

192.168.1.0/25 192.168.1.194

Routeur B :

Destination Gateway

192.168.1.0/25 192.168.1.130

192.168.1.128/25 192.168.1.130

10.0.0.0/8 10.0.0.2

Hote A :

Destination Gateway

default 10.0.0.1

Routeur Cisco :

Destination Gateway

192.168.1.0/25 Ethernet 0/1

192.168.1.192 Ethernet 0/0

192.168.1.128/26 192.168.1.193

default 192.168.1.193

4 : Liste des paquet de D vers A (A ne peut pas ping, probleme Windows de sortie)

D (ARP cisco, ICMP D) -> Cisco(Arp resp D, ICMP receive D, arp request C, ICMP send C) -> C (ARP resp Cisco, ICMP receive Cisco, ARP B, ICMP B) -> B (ARP resp C, ICMP receive C, ARP A, ICMP A) -> A (ARP resp B, ICMP receive B, ICMP B) -> B (A,C) -> C (B,Cisco)-> Cisco (c,D) -> D(Cisco) => fin du ping

A chaque réception de paquet ICMP, la machine fait une requête ARP (ici, table ARP à vide) demandant qui est la machine possédant l’adresse trouvé dans la table de routage (en gateway). Une fois la requête répondue, la machine expédie un paquet ARP vers l’adresse gateway, et ainsi de suite.

5 :

Pas de traceroute sur A (commande tracert ne fonctionne pas, comme le ping)

Le principe de la mesure traceroute permet de calculer la distance en terme de routeur entre bous et le point recherché. La mesure augmente de 1 à chaque routeur traversé par le paquet.

6 : RIP

1. Les paquets RIP proviennent des machines routeurs et voisines, et donne les réseaux accessibles ainsi que la distance (métrique) du réseau depuis l’expéditeur du paquet. RIP implémente le split-Horizon en mentionnant des routes à 16 de métrique (infini pour le protocole RIP) sur l’interface par lequel il a reçu l’information de cette route. Cela évite donc les boucles.
2. On ne peut pas retrouver le netmask dans le paquet RIP. RIP déduis le netmask des adresses en prenant comme modèle le netmask de l’interface sur laquelle le paquet est reçu.
3. RIP ne tient aucun compte du routage statique ! Aucune information n’apparais sur l’adresse ajouté dans les paquets RIP
4. Un paquet IGMP a été communiqué sur le réseau indiquant qu’un membre (ne donne pas l’adresse du membre) a quitté le réseau. Le processus émet avant de mourir un paquet RIP qui met à jour la métrique des réseaux atteignable via l’ancien devenu inaccessible.
5. Le paquet ne s’envois plus, car le processus se tue instantanément.
   1. Rajout de l’accée directe à D, avec une métrique plus faible (1) sur RIP
   2. Rajout de l’accée à D en passant vers A (métrique plus faible que via C puis cisco, 2 contre 3)
   3. Inchangé (vers A la métrique est plus longue que via cisco, 2 contre 3)
   4. Ajout de la route directe vers A avec la métrique la plus faible (1)
6. Le mecanisme de route-poisonning peut être testé en faisant tomber en panne le net 3 et observer les paquets émis et reçu sur net 1. On observe que les notifications de route coupée sont émises directement. RIP v1 implémente bien le mécanisme.
7. Le trigger update est en place dans RIPv1, on observe que l’ajout d’une nouvelle route (entre a et d par exemple) déclenche automatiquement l’envois de paquet RIP avec l’update, sans tenir compte du timer.

RIPv2

L’avantage d’utiliser les adresse de multicast au lieux de broadcast permettent d’éviter de surcharger le réseau et réduit le cout réseau de update en sélectionnant plus finement les machines qui reçoivent l’update. De plus, RIPv2 n’est pas classful ce qui signifie qu’il transporte le netmask de chaque réseau, permettant donc d’éviter le problème qui étais survenu avec le routeur précédement sur RIPv1, lors de la transition entre deux réseau avec un netmask différent.

Traceroute :

On note que certain nœud sont particulièrement lent (comme le nœud en sortie du réseau renatter). On remarque que le débit entre certaine zone est bien plus fluide que sur d’autre.