Administration de réseaux IP

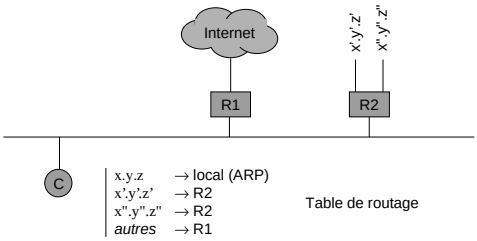
Roland Dirlewanger
CNRS - Délégation Aquitaine et Poitou Charentes
rd@dr15.cnrs.fr

Bibliographie *(1)*

- Christian Huitema, "Le routage dans l'Internet", Eyrolles, 1995.

  ISBN 2-212-08902-3

Routage IP : le cas du site feuille



Routage IP: l'acquisition des routes

- routage statique : par configuration de l'équipement
  - `route add` *destination relais distance*
- ICMP "redirect" : automatique
  - un routeur reçoit un paquet par une interface
  - il constate que pour l'acheminer, il doit le renvoyer par la même interface
  - il envoie un paquet "ICMP redirect" pour indiquer à l'émetteur qu'il peut atteindre le destinataire directement.

Routage IP: protocoles de routage *(1)*

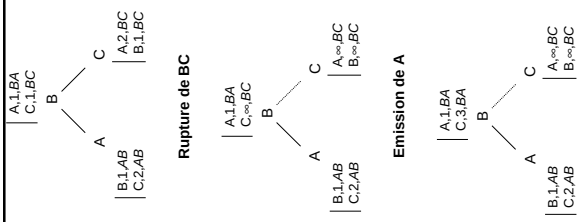
- Deux familles de protocoles
  - protocole de routage interne (*Internal Gateway Protocol*) : ex. RIP, OSPF, IGRP
  - protocole de routage externe (*External Gateway Protocol*) : ex. EGP, BGP
- Sytème autonome (AS, *Autonomous System*)
  - ensemble d'équipements sous une administration unique et obéissant à la même politique de routage

Protocoles à vecteurs de distance

Principe :

- distance ou métrique :
  - unité arbitraire liée soit au nombre de relais traversés, soit au coût de la liaison, soit à son débit, soit aux délais de transmission, pour atteindre la destination.
- émission :
  - diffusion du vecteur de distance (*destination, relais*)
- réception :
  - mise à jour de la table de routage ssi *distance + 1* pour *destination* est plus petite que la valeur actuelle
  - réarmement du temps d'expiration pour chaque destination telle que *distance + 1* = valeur actuelle

Boucles et comptage jusqu'à l'infini *(1)*



Boucles et comptage jusqu'à l'infini *(2)*

- *étape 3* :A a émis avant B=>
  - il y a une boucle entre A et B pour tout paquet émis vers C
- *étapes suivantes* :
  - A expire la route vers C, mais en reçoit une nouvelle de B avec une distance + 1
  - B expire la route vers C, mais en reçoit une nouvelle de A avec une distance + 1
  - cycle qui converge lentement (distance ← distance + 2) vers la distance maximale => comptage jusqu'à l'infini.

Boucles et comptage jusqu'à l'infini *(3)*

Améliorer la convergence

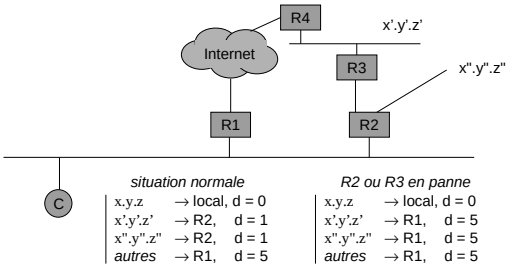
- Horizon partagé
  - A n'envoie pas vers B les routes reçues de B
  - plus efficace : A envoie vers B les routes reçues de B en indiquant une distance infinie
- Mise à jour déclenchées
  - envoi immédiat des modifications notables (rupture de connectivité, etc.)
  - en fait, chaque routeur envoie la mise à jour avec un délai aléatoire pour éviter les tempêtes de mises à jour.

Le protocole RIP

RIP (*Routing Information Protocol*)

- Version 1
  - utilise la diffusion sur Ethernet et l'émission sur liaison PàP
  - chaque nœud diffuse sa table toutes les 30 secondes et expire les routes non raffraîchies toutes les 3 minutes
  - utilise l'horizon partagé et les màj déclenchées
- Version 2
  - gère les subnets
  - implémente le multicast
  - authentification
  - notion de relais suivant

Exemple de liaison de secours



Protocoles à vecteurs d'états de liaisons

Principe :

- chaque nœud propage l'état de la liaison avec ses voisins par inondation
- chaque nœud maintient une carte complète du réseau :
  - il calcule le chemin le plus court pour atteindre une destination.

Avantages :

- routeurs en phase => pas de boucles
- convergence très rapide vers un état stable en cas de modification

Inconvénients :

- problème sur les gros réseaux (> 200 nœuds)

La carte du réseau

- l'élément d'information est un enregistrement
  - identificateur de la liaison
  - destination atteinte par cette liaison
  - information de distance
  - numéro de séquence
- rôle de chaque nœud
  - propager l'état de ses liaisons
  - propager les enregistrements reçus de ses voisins sur toutes les interfaces, sauf celle par laquelle l'enregistrement est arrivé
  - ignorer ses propres enregistrements

Plusieurs chemin vers la même destination

i.e distance (*dest* via *i*) = distance (*dest* via *j*)

Protocole à vecteur de distance :

- ne met pas à jour la table de routage => si on commence à router via *i*, on routera tous les paquets via *i*.
- si *i* tombe en panne, il faudra attendre la prochaine annonce de *dest* via *j*.

Protocole à vecteur d'état de liaisons :

- peut router via *i* ou via *j* ou les deux (équilibre de charge)
- si *i* tombe, le relais via *j* est immédiat

Le protocole OSPF

- OSPF (*Open Short Path First*) recommandé par l'IETF (*Internet Engineering Task Force*) comme protocole de routage interne (RIP = trop d'inconvénients, IGRP = propriétaire cisco).
- protocole à vecteur d'états de liaison, avec :
  - découpage en zones des gros réseaux
  - gestion des métriques multiples (débit, délai, coût, fiabilité)
  - gestion des routes externes
  - temporisation des enregistrements, acquittements, checksums, authentification

OSPF : démarrage

- démarrage d'un routeur :
  - numéro de séquence = valeur minimale, diffusion par inondation de l'état de liaison
  - s'il reçoit un état avec un numéro de séquence plus grand => numéro de séquence = ce numéro +1, diffusion par inondation de l'état de liaison
- rétablissement d'une liaison
  - échange avec ses voisins de l'état de ses liaisons
    - envoi de description (identifiant de la liaison, n° de séquence)
    - transmission uniquement des enregistrements de liaison différents

OSPF : les numéros de séquence

- éviter que le numéro de séquence déborde ($\geq 2^{32}$)
  - numéros de séquence évoluent selon l'algorithme suivant ($N = 2^{31} - 1$)
    - initialisation : $s = -N + 1$
    - progression : si $s < N - 2$ alors $s \leftarrow s + 1$; si $s = N - 2$ alors $s \leftarrow 0$
    - comparaison : si $s1 < 0$ ou $s2 < 0$, alors comparaison classique
      si $s1 \geq 0$ et $s2 \geq 0$. Supposons que $s1 < s2$ alors
      si $s2 - s1 > (N - 1)/2$ alors s2 plus récent
      sinon s1 plus récent

OSPF : les temporisations

- retransmission par inondation de toutes les liaisons toutes les 30 minutes
- éviter de conserver des routes anciennes
  - les enregistrements d'états de liaison ont un champ "âge" :
    - vaut 0 lorsque l'enregistrement est diffusé par le routeur responsable de la liaison
    - augmente d'un à chaque routeur traversé puis d'un toutes les secondes
  - si l'âge atteint 1 heure sur un routeur => envoi par inondation de la suppression de cet enregistrement
  - pour chaque enregistrement, on compare l'âge reçu avec l'âge actuel.
    - Si la différence est de quelques unités, c'est le cas normal
    - Si la différence dépasse 15 minutes, on met à jour l'enregistrement correspondant