

# Master d'Informatique – E-Secure

## Réseaux

### Adressage - Routage

Bureau S3-354

Jean.Saquet@unicaen.fr

[http : saquet.users.greyc.fr/M2/rezo](http://saquet.users.greyc.fr/M2/rezo)

# Espace IPv4

Rappel : 4 octets donc 2 puissance 32 adresses en théorie (environ 4 milliards).

Place perdue à cause des classes (A, B, C ) distribuées, ou même des /n, n entre 8 et 30.

Quelques classes réservées (privé, autoconf, local).

Notation en décimal (hélas?!).

Masque de sous-réseau encore souvent écrit « à l'ancienne » (avant CIDR).

# Attribution des adresses IPv4

International : ICANN. Plus d'adresses disponibles  
« Régional » (4 grandes régions du monde).

RIPE : Europe, Asie Centrale et Moyen Orient, Afrique du Nord. A commencé à distribuer son dernier /8.

Sous délégations pour les pays ou groupes de pays.

# Adresses IPv4 des machines

Une adresse par interface, sauf exception.

Les adresses faisant partie d'un même réseau local ou VLAN sont regroupées en une suite d'adresses contigües (là encore sauf exception), donc :

- partie « réseau » de l'adresse ( $n$  bits)
- partie « machine » ( $32 - n$  bits)

Où  $n$  est le masque de sous réseau écrit à la mode CIDR. Voir correspondance avec l'ancienne écriture.

# Espace IPv6

128 bits (8 mots de 16 bits écrits en hexadécimal), soit environ 64 milliards de milliards de milliards de milliards d'adresses ...

Espace réellement utilisé pour les adresses « agrégées globales » : le 1/8 de cet espace pour lequel les trois premiers bits sont 001. (de 2000::1 à 3FFF:FF...FE). Quelques autres plages d'adresses pour certaines utilisations.

# Attribution des adresses IPv6

Ce sont les mêmes organismes qu'en v4, mais il y en a pour tout le monde.

Selon l'importance de l'utilisateur final, il obtiendra un préfixe allant du /48 au /64 en général. Notons qu'un /64 permet encore des milliards de milliards d'adresses ...

Cet espace bien trop grand permet de mapper une adresse physique dans une adresse IP.

# Adresses IPv6 des machines

Par interface, toujours une adresse « lien-local », dans l'espace FE80 ::/64.

La partie machine peut être calculée à partir de l'adresse physique, ou choisie aléatoirement, ou par un mécanisme cryptographique ...

Si connectivité au réseau Internet, adresse globale comme indiquée précédemment, configurée manuellement ou par un procédé automatique.

Possibilité de plusieurs adresses globales par interface.

# IPv4 ou IPv6 : sous-adressage

Si on dispose d'un « /n », on peut toujours (sauf si  $n=30$ ) le découper en 2 ou plusieurs parties pour en attribuer une à chacun de ses sous-réseaux, physiques ou virtuels.

Exemple = un « /n » peut être découpé en 2 « /(n+1) », ou 4 « /(n+2) », ou un « /(n+1) » et 2 « /(n+2) », ...

Inversement, on peut regrouper, notamment dans une table de routage, voir plus loin.



# IPv4 ou IPv6 : écriture des adresses

Une adresse machine comporte 32 ou 128 bits (4 octets ou 8 mots de 16 bits).

Une adresse réseau comporte  $n$  bits utile, où  $n$  est le masque. Cependant, il faut toujours écrire l'adresse en entier (en complétant par des 0 de préférence). Ex :

192.168.128.0/24

2001:660:7101:1a:8000 ::/65

# Politique d'adressage

Déterminer l'architecture du réseau : VLANs éventuels, sous-réseaux, estimation des tailles de chacun, ...

Positionnement des routeurs les interconnectant.

Découpage de son préfixe en fonction de cette architecture.

Attribution d'une adresse à chaque interface de chaque routeur.

Détermination du mode de distribution des adresses des autres machines.

# Positionnement des routeurs

Ils peuvent se contenter de joindre deux sous-réseaux. On risque alors d'obtenir des chemins assez long pour certaines communications.

Inversement, tout ou partie des routeurs peuvent être regroupés dans un « réseau d'interconnexion », qui peut presque ne contenir que des routeurs. On peut alors utiliser pour ce sous-réseau des adresses privées v4 ou des lien-local v6.

Penser aussi à l'accès des switchs administrables à partir du poste de l'administrateur.

# Routage : principes

Les routeurs ont pour rôle de forwarder les datagrammes IP. Ils sont en effet susceptibles de recevoir des DG qui ne leur sont pas destinés, et donc pour lesquels ils doivent trouver un chemin.

Les tables de routage de ces appareils sont plus complexes à configurer que celles des machines « ordinaires ».

# Routeurs : table de routage(1)

Toutes les interfaces étant munies d'une adresse IP, avec masque de sous-réseau indiqué, le routeur peut calculer automatiquement les lignes de la table de routage concernant les réseaux auxquels ils sont directement connectés :

Adresse réseau / masque, accès direct via interface xx  
Il faut par contre lui apprendre le reste.

# Routeurs : table de routage(2)

Pour apprendre aux routeurs les chemins vers les réseaux « lointains », solution manuelle ou protocole d'échange d'informations de routage.

Manuelle : cf. exemples déjà vus au Tps 1 et 1b.  
Penser éventuellement à la route par défaut.

# Protocoles de routage

Les routeurs s'échangent de l'information au moyen de protocoles appropriés. Exemples : RIP, OSPF, ISIS, BGP.

Les échanges ont lieu en général entre les routeurs situés sur un même réseau local (sinon, il faut déjà une partie du routage opérationnel pour échanger l'info!). Les infos ainsi apprises par un routeur sont ensuite répercutées sur les autres réseaux auxquels est connecté ce routeur.

# Le protocole RIP

Basé sur le principe du vecteur de distance : les réseaux directement accessibles sont à une distance 0, n s'il faut traverser n routeurs.

Les routeurs munis d'un logiciel compatible RIP envoient régulièrement leurs informations aux routeurs voisins.

Ces derniers ajustent éventuellement leurs tables de routage en fonction des informations apprises : nouvelles routes, changement de chemin dû à une amélioration ou une détérioration de la distance.



# RIP : principes de configuration

Le protocole RIP étant supposé activé (mode actif = envoi et écoute des infos, mode passif = seulement écoute des infos reçues), chaque routeur décide :

- de quelles infos il envoie précisément
- du ou des réseaux sur le(s)quel(s) il les envoie.

Ce peut être tout, partout ou plus sélectif. En général, il y a des réseaux sur lesquels il est inutile d'envoyer les infos.

# RIP : infos apprises

Si un routeur A reçoit une info concernant le réseau X venant d'un routeur voisin B, X la distance à B étant  $d$  :

- Si cette info n'améliore pas la distance de A à X, on ne change rien.
- Si cette info améliore la distance de A à X (ou si X n'était pas encore connu), alors on modifie ou on ajoute la ligne de la table de routage concernant X :  
X est à une distance  $d+1$ , via le routeur B (et via l'interface par laquelle on a reçu l'information)

# Routeurs

Les routeurs peuvent être des matériels spécialisés (indispensable si la charge est importante).

On peut aussi utiliser des routeurs logiciels sur des machines « ordinaires » munies de deux ou plusieurs cartes réseau (Ethernet, Wi-Fi, ...).

Il faut alors choisir ce routeur logiciel, le configurer et penser à activer le forwarding.

# Configuration des routeurs

Elle se fait souvent à distance, avec donc la nécessité qu'un routage minimum soit déjà activé !

La première configuration se fera donc le plus souvent soit avec une liaison série entre le routeur et le terminal, soit avec un mini-réseau à deux postes (le routeur et une machine) configurés en fonction de la « configuration d'usine » du routeur.

L'interface de configuration est le plus souvent rudimentaire au niveau confort (commandes ligne) mais complète au niveau des commandes disponibles.

# Routeur logiciel Quagga

Routeur logiciel libre pour le monde Unix, Quagga (successeur de Zebra) peut utiliser plusieurs protocoles de routage et comporte plusieurs démons :

- Zebra
- Un démon par protocole : bgp, isis, ospf, ospf6, rip, ripng.

Il faut activer Zebra et au moins un des autres.

# Configuration Quagga

Elle peut s'effectuer à distance au moyen de l'accès au(x) démon(s) concerné(s), ou bien en local si la machine supportant Quagga possède une interface utilisateur, ou est accessible par ssh.

Si on accède à distance, il faudra employer les commandes disponibles ; si on accède en local, on pourra éditer les fichiers de configuration et relancer le routeur.

# Quagga : fichiers de config

Configurer daemons en fonction des protocoles choisis  
Configurer l'accès au démon à distance et les logs :

```
! Zebra configuration file
!  
hostname Router  
password zebra  
enable password zebra  
!  
log stdout  
!
```

# Quagga : config RIP(ng)

Exemple :

```
router ripng
! Activation sur eth0 :
network eth0
! Distribution via eth0 :
distribute-list local-only out eth0
! Annoncer les réseaux directement connectés :
redistribute connected
! Annoncer les routes configurées manuellement :
redistribute static
```



# Compléments

Le « redistribute » ci-dessus permet d'annoncer des routes obtenues autrement que par RIP (directes, statiques comme ci-dessus mais aussi apprises par OSPF, par BGP, ...)

Tutorial sur Quagga :

<http://www.nongnu.org/quagga/docs.html>

Configuration plus complexes de routeurs :  
cf. unité optionnelle : compléments routage et DNS  
(UMIS1J)