

Administration Système et Réseaux, Sécurité

Routage IP

Philippe Harrand

¹ Département Informatique
Pôle Sciences et Technologie

² Direction Territoriale Sud Ouest
France Télécom

3 octobre 2007

Philippe Harrand (Université de La Rochelle)

3 octobre 2007 1 / 23

Routage

Routage

Routage Statique

Routage dynamique

Protocoles extérieurs

Protocoles intérieurs

Philippe Harrand (Université de La Rochelle)

3 octobre 2007 2 / 23

Principes

- ▶ Le routage permet de transmettre un datagramme d'une machine à une autre
 - ▶ situés sur le même réseau
 - ▶ situés sur 2 réseaux distincts
 - ▶ éventuellement en traversant d'autres réseaux
- ▶ Le routage fonctionne au niveau *réseau 3* du modèle TCP/IP
- ▶ Principe du *Best Effort*
- ▶ Principe du *Next Hop* (saut suivant)

Philippe Harrand (Université de La Rochelle)

3 octobre 2007 3 / 23

Routeurs

- ▶ Une machine capable de transférer (*forward*) des datagrammes d'un réseau à un autre est appelée **passerelle**
- ▶ Une machine dédiée au rôle de passerelle est nommée **routeur**
- ▶ Une passerelle efficace dispose d'au moins 2 interfaces réseau

Philippe Harrand (Université de La Rochelle)

3 octobre 2007 4 / 23

Table de routage

- ▶ Indique l'interface et le prochain routeur d'une destination
- ▶ Est située en RAM
- ▶ Se lit par :
 - ▶ Linux :
 - ▶ cat /proc/net/route
 - ▶ /sbin/route [-n]
 - ▶ netstat -r[n]
 - ▶ Windows : route print

Table de routage

Table de routage d'une station de travail

| Destination | Passerelle | Genmask | Indic | MSS | Fenêtre | irtt | Iface |
|-------------|---------------|---------------|-------|-----|---------|------|-------|
| 192.168.0.0 | * | 255.255.255.0 | U | 0 | 0 | 0 | eth0 |
| 127.0.0.0 | * | 255.0.0.0 | U | 0 | 0 | 0 | lo |
| 169.254.0.0 | * | 255.255.0.0 | U | 0 | 0 | 0 | eth0 |
| default | 192.168.0.254 | 0.0.0.0 | UG | 0 | 0 | 0 | eth0 |

Table de routage

Table de routage d'une autre station de travail

```

-
Liste d'Interfaces
0x1 ..... MS TCP Loopback interface
0x2 ...00 02 e3 47 41 63 ..... Atheros AR5005G Wireless Network Adapter - Miniport d'ordonnement de paquets
0x3 ...00 40 ca d9 a0 c9 ..... Broadcom 440x 10/100 Integrated Controller - Miniport d'ordonnement de paquets
-
Itinéraires actifs :
    
```

| Destination réseau | Masque réseau | Adr. passerelle | Adr. interface | Métrique |
|--------------------|-----------------|-----------------|----------------|----------|
| 0.0.0.0 | 0.0.0.0 | 192.168.0.254 | 192.168.0.107 | 20 |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 |
| 192.168.0.0 | 255.255.255.0 | 192.168.0.107 | 192.168.0.107 | 20 |
| 192.168.0.107 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 20 |
| 192.168.0.255 | 255.255.255.255 | 192.168.0.107 | 192.168.0.107 | 20 |
| 224.0.0.0 | 240.0.0.0 | 192.168.0.107 | 192.168.0.107 | 20 |
| 255.255.255.255 | 255.255.255.255 | 192.168.0.107 | 192.168.0.107 | 1 |
| 255.255.255.255 | 255.255.255.255 | 192.168.0.107 | 192.168.0.107 | 2 |
| | | | | 1 |

Passerelle par défaut : 192.168.0.254
Itinéraires persistants :

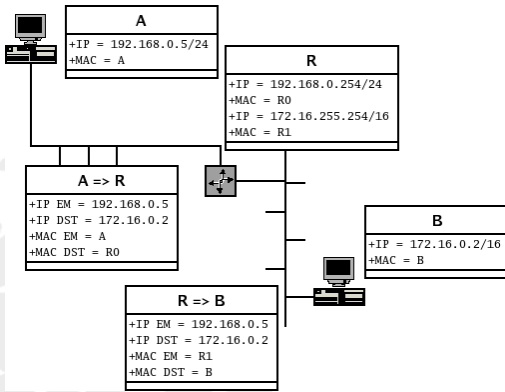
Table de routage

Table de routage

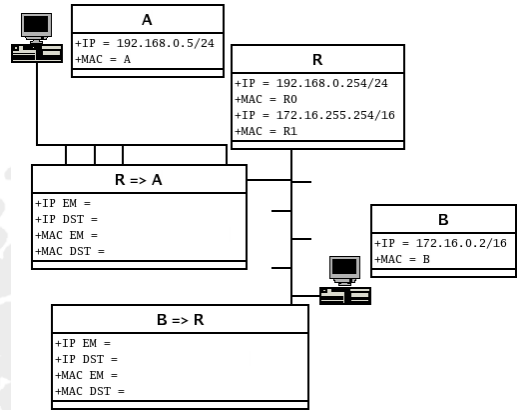
Table de routage d'un routeur

| Destination | Passerelle | Genmask | Indic | MSS | Fenêtre | irtt | Iface |
|-------------|---------------|---------------|-------|-----|---------|------|-------|
| 192.168.0.0 | * | 255.255.255.0 | U | 0 | 0 | 0 | eth0 |
| 192.168.1.0 | * | 255.255.0.0 | U | 0 | 0 | 0 | eth1 |
| 127.0.0.0 | * | 255.0.0.0 | U | 0 | 0 | 0 | lo |
| default | 192.168.0.254 | 0.0.0.0 | UG | 0 | 0 | 0 | eth0 |

Routage



Routage



Principes

- ▶ Chaque machine configure sa (ses) route(s) directement connectée(s)
- ▶ Les stations reçoivent la passerelle par défaut grâce à DHCP
- ▶ les routeurs sont configurés un par un grâce à SSH
- ▶ Ajout de route => nouvelle configuration de chaque routeur

Commandes

- ▶ Configuration des interfaces : `/sbin/ifconfig`
- ▶ Configuration des routes : `/sbin/route`
- ▶ Visualisations diverses : `/bin/netstat`

Systèmes Autonomes

- ▶ Ensemble de réseaux gérés par une seule entité administrative
- ▶ Sur Internet, chaque AS est identifié par un nombre de 16 bits
 - ▶ de 1 à 64511 => AS Internet
 - ▶ de 64512 à 65535 => AS privés

BGP

- ▶ BGP : Protocole Extérieur
- ▶ Border Gateway Protocol
 - ▶ Echange de routes entre AS
 - ▶ Seul protocole à supporter de très grands volumes de données
 - ▶ Fonctionne en mode connecté (TCP)
- ▶ Echange des réseaux (adresse IP + masque) avec ses voisins
- ▶ Problèmes de sécurité

RIP

- ▶ Vecteur de distance
- ▶ Métrique : nombre de sauts (hop)
- ▶ Nombre de sauts limités à 15
- ▶ Protocole le plus ancien et probablement le plus simple à utiliser, il ne nécessite (presque) pas de configuration

RIP

- ▶ Chaque routeur diffuse sur toutes ses interfaces des messages indiquant les réseaux qu'il peut joindre et leurs métriques
- ▶ diffusion toutes les 30 secondes
- ▶ RIP utilise UDP sur le port 520 en multicast (224.0.0.9)
- ▶ Actuellement version 2 (RIP2)
- ▶ voir la rfc2453 RIP2

EIGRP

- ▶ Enhanced Interior Gateway Routing Protocol
- ▶ Protocole de routage développé par Cisco
- ▶ ne fonctionne que sur des routeurs Cisco
- ▶ Métrique
 - ▶ Délai (D)
 - ▶ Bande passante Bp
 - ▶ Fiabilité (F)
 - ▶ Charge (C)

$$Métrique = (K1 * Bp) + \frac{(K2 * Bp)}{(256 - C) + (K3 * D)} * \frac{K5}{F + K4}$$

OSPF

- ▶ Open Short Path First
- ▶ Moins verbeux que RIP, économise la bande passante de l'internet
- ▶ mais demandant à être configuré
- ▶ et nécessite plus de ressources
- ▶ multicast 224.0.0.5 et 224.0.0.6
- ▶ utilise sa propre couche transport

OSPF

- ▶ Etat de lien
- ▶ Métrique
 - ▶ **Bande passante**
 - ▶ Nombre de sauts
 - ▶ Délai
 - ▶ Fiabilité
 - ▶ Coût financier

OSPF

- ▶ L'internet est divisé en zones (*area*)
- ▶ La zone 0 est le *backbone*
- ▶ Toutes les zones sont connectées au backbone
- ▶ Les routeurs d'une zone ne savent rien des autres zones
- ▶ Dans chaque zone un routeur est élu DR *Designated Routeur* (et un autre BDR)

OSPF

- ▶ Les routeurs envoient l'état de leurs liens dans des paquets échange (224.0.0.6)
- ▶ Les routeurs envoient périodiquement (10s) un paquet HELLO (224.0.0.5)
- ▶ En cas de changement de statut d'un lien, le routeur concerné envoie un message de mise à jour aux DR et BDR
- ▶ Le DR inonde tous les routeurs en cas de nécessité (224.0.0.5)
- ▶ Chaque routeur concerné recalcule la carte du réseau

Conclusion

| Nb routeurs | RIP | OSPF | Commentaire |
|-------------|-----|------|--|
| N<10 | OUI | OUI | OSPF converge plus vite que RIP qui marche tout seul |
| 10<N>30 | NON | OUI | Une seule zone |
| 30<N | NON | OUI | Plusieurs zones |

Quagga / Zebra

- ▶ Quagga/Zebra est un démon de routage modulaire GPL pour GnuLinux, *BSD, solaris, etc.
- ▶ Syntaxe Cisco IOS
- ▶ Zebra (2601)
 - ▶ routage statique
 - ▶ nécessaire aux autres modules
- ▶ ripd (2602)
- ▶ ospfd (2604)
- ▶ ospf6d (2606)
- ▶ ripngd (2603)
- ▶ bgpd (2605)
- ▶ isisd (2608)