

Routage et « Routing Policy »

■ ■ ■ La notion d'adresse

1 – Soient les informations de configuration suivantes :

Machine A - eth0:	MAC Address - 00:11:22:33:44:AA	IP Address - 192.168.1.1/24
Machine B - eth0:	MAC Address - 00:11:22:33:44:BB	IP Address - 10.1.1.1/8
Machine C - eth0:	MAC Address - 00:11:22:33:44:CC	IP address - 192.168.1.254/24 10.254.254.254/8

- À quoi correspond la machine C ?
La machine C dispose de deux interfaces munies de deux adresses : cela peut être un routeur ou bien un serveur (configuration utile lorsque l'on veut partager l'accès à serveur depuis deux VLANs par exemple). Ici, ce sera plutôt un routeur.
- Quelles informations seront présentes dans les tables ARP de la machine A et de la machine B ?
 - ◊ Pour A : 00:11:22:33:44:CC associé à 192.168.1.254 ;
 - ◊ Pour B : 00:11:22:33:44:CC associé à 10.254.254.254 ;
- Parmi les techniques suivantes lesquelles peuvent expliquer cette configuration ?
 - ◊ « Spoofing » ;
 - ◊ « Proxy ARP » ;
 - ◊ « load balancing » ;
 - ◊ « NAT »

Toutes
- Est-ce que chacune de ces adresses IP est attachée à un matériel spécifique et une seule interface réseau ?
Non, une adresse IP est indépendante d'un matériel spécifique et peut être attachée avec une ou d'autres adresses à la même interface réseau.

2 – Soient les commandes suivantes :

```
xterm
pef@cerberus:~$ sudo ip addr add 10.1.1.8/8 dev eth0 brd +
pef@cerberus:~$ sudo ip addr add 172.16.1.1/16 dev eth0 brd +
```

et la commande suivante :

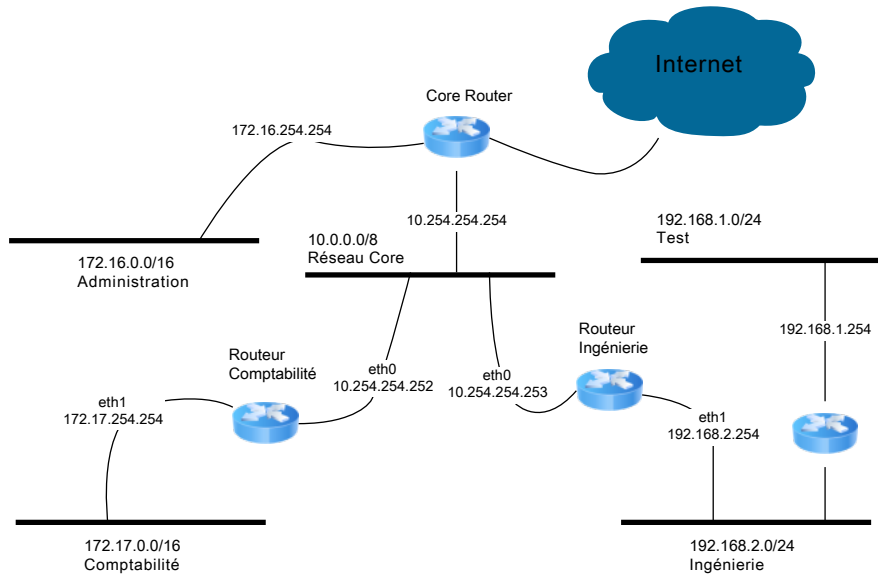
```
xterm
pef@cerberus:~$ ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:a7:08:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.127.131/24 brd 192.168.127.255 scope global eth0
    inet 10.1.1.8/8 brd 10.255.255.255 scope global eth0
    inet 172.16.1.1/16 brd 172.16.255.255 scope global eth0
    inet6 fe80::20c:29ff:fea7:897/64 scope link
    valid_lft forever preferred_lft forever
```

- À quoi correspond l'option « brd + » et la notion de « scope » ?
*Cette option permet de définir automatiquement l'adresse de « broadcast » par rapport à l'identifiant du réseau et la taille du préfixe.
Un nouveau « scope » est créé à chaque préfixe de longueur différente.*
- Donnez les adresses considérées comme « secondary ».
Dans la question précédente, la seule adresse « secondary » est 192.168.1.2/24.
- Quelle commande a défini l'adresse considérée comme « secondary » ?

```
xterm
pef@cerberus:~$ sudo ip address add 192.168.127.201/24 brd +
```

La notion de route

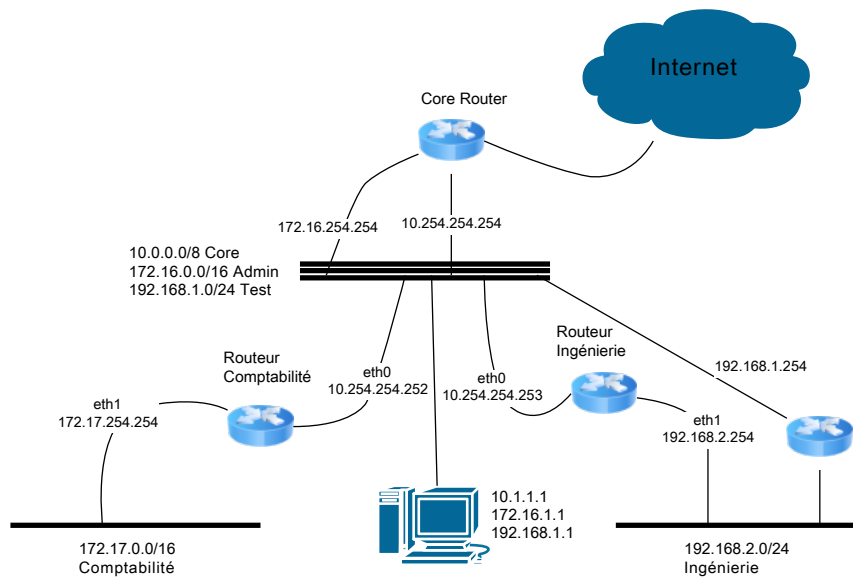
3 – Soit un réseau défini comme suit :



Un hôte possède sur son unique interface `eth0`, les adresses suivantes :

- 10.1.1.1/8 ;
 - 172.16.1.1/16 ;
 - 192.168.1.1/24.
- a. Comment évolue le synoptique réseau ?

Les réseaux 10.0.0.0/8, 172.16.0.0/16 et 192.168.1.0/24 sont physiquement identiques :



- b. Depuis l'hôte il est possible de « ping » l'adresse 172.16.254.254 et d'avoir une réponse. Pourquoi ?

Parce que l'hôte dispose d'une adresse 172.16.1.1 et d'un scope associé en /16: il peut donc envoyer son ping après avoir fait une requête ARP pour obtenir l'@MAC de 172.16.254.254. Le routeur 172.16.254.254 peut également lui répondre (configuration similaire).

- c. L'administrateur de l'hôte réalise le travail suivant :

```

1 # ip addr flush dev eth0
2 # ip addr add 10.1.1.1/32 dev eth0 brd 10.255.255.255
3 # ip addr add 172.16.1.1/32 dev eth0 brd 172.16.255.255
4 # ip addr add 192.168.1.1/32 dev eth0 brd 192.168.1.255
5 # ip route list
6 127.0.0.0/8 dev lo scope link
    
```

Expliquez le rôle de chaque ligne et le résultat obtenu ?

Chacune des lignes ajoute une adresse à l'interface `eth0` avec un scope vide (/32) et en donnant explicitement l'adresse de broadcast.

Quel lien existe entre « scope » et « route » ?

Si le scope est vide, il n'y a pas d'ajout **automatique** de route vers le scope auquel appartient l'adresse ajoutée.

d. Soit la commande suivante, entrée après les commandes de la question c) :

```
xterm
# ip route add 10.0.0.0/8 proto kernel scope link dev eth0 src 10.1.1.1
```

Quelles autres commandes doivent être entrées pour obtenir le résultat observé en b) ?

```
xterm
# ip route add 172.16.0.0/16 proto kernel scope link dev eth0 src 172.16.1.1
# ip route add 192.168.1.0/24 proto kernel scope link dev eth0 src 192.168.1.1
```

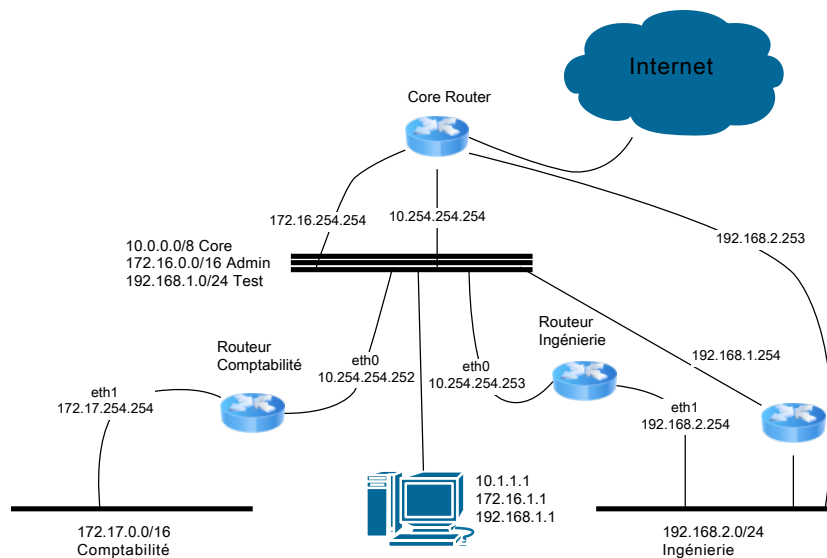
e. l'administrateur rentre maintenant les commandes suivantes :

```
xterm
# ip route del 172.16.0.0/16 proto kernel scope link dev eth0 src 172.16.1.1
# ip route add 172.16.0.0/16 proto kernel scope link dev eth0 src 192.168.1.1
```

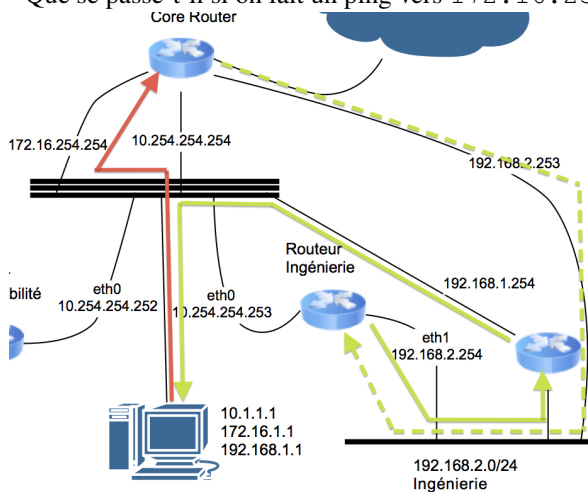
Quel est le résultat de ces commandes ?

Les deux commandes remplacent l'adresse source à employer pour aller vers le réseau 172.16.0.0/16 : on utilisera dorénavant l'adresse 192.168.1.1.

Maintenant, le « core router » dispose d'une connexion au réseau Ingénierie de scope 192.168.2.0/24 et dispose d'une route vers 192.168.1.0/24 par le routeur de l'Ingénierie.



Que se passe-t-il si on fait un ping vers 172.16.254.254 ?



Le message ICMP «echo-request» passe par le réseau 172.16.0.0/16 et atteint le routeur sur son interface 172.16.254.254.

Le message ICMP «echo-reply» passe par le réseau 192.168.2.0/24 du fait de :

- ♦ l'adresse d'émission du message ICMP «echo-request» appartenant au réseau 192.168.1.0/24 ;
- ♦ la route vers le réseau 192.168.1.0/24 par l'intermédiaire du routeur «Ingénierie» ;
- ♦ deux possibilités pour l'accès au routeur «Ingénierie» :

- * par la nouvelle connexion du «core router» vers le réseau 192.168.2.0/24 pour atteindre le routeur «Ingénierie» (tracé en pointillé) ;
- * par la connexion dans le réseau 10.0.0.0/8 (tracé non représenté sur le schéma).
- ♦ le message passe par le routeur «Ingénierie» qui l'envoie vers le routeur connecté au réseau «192.168.2.0/24».

4 – Soient :

- ▷ les réseaux suivants :
 - Comptabilité : 172.17.0.0/16 ;
 - Core/backbone : 10.0.0.0/8 ;
 - Ingénierie : 192.168.2.0/24 ;
- ▷ la « Security Policy » suivante :
 - ◊ la majorité du trafic en provenance du 10.0.0.0/8 est interdit dans les réseaux « Comptabilité » et « Ingénierie », avec les exceptions suivantes :
 - * « Comptabilité » est accessible depuis :
 - ▷ 10.2.3.32/27 ;
 - ▷ 10.3.2.0/27 ;
 - ▷ tout autre réseau doit être bloqué *administrativement*.
 - * « Ingénierie » est accessible depuis :
 - ▷ 10.10.0.0/16 ;
 - ▷ les autres réseaux ne doivent pas connaître son existence.

Soit la « Policy Routing » concernant les **messages** à faire retour à la machine d'origine :

- ▷ Paquets provenant de « Comptabilité » 172.17.0.0/16 :
- ▷ Paquets provenant de « Ingénierie » 192.168.2.0/24 :

À destination du réseau	Réponse du routeur
10.2.3.32/27	<i>full route</i>
10.3.2.0/27	<i>full route</i>
10.0.0.0/8	<i>prohibit</i>
172.16.0.0/16	<i>prohibit</i>
192.168.2.0/24	<i>prohibit</i>

À destination du réseau	Réponse du routeur
10.10.0.0/16	<i>full route</i>
10.0.0.0/8	<i>blackhole</i>
172.17.0.0/16	<i>blackhole</i>
172.16.0.0/16	<i>blackhole</i>

Questions :

- a. Complétez la « Policy Routing » concernant le réseau « Ingénierie » : *Voir table plus haut.*

Soit la liste des commandes de configuration du routeur « Ingénierie » :

```

1 # ip addr add 192.168.2.254/24 dev eth1 brd +
2 # ip addr add 10.254.254.253/32 dev eth0 brd 10.255.255.255
3 ...
6 # ip route add blackhole 172.16.0.0/16
    
```

- b. À quoi correspond la notation « blackhole », en quoi est-elle différent de « prohibit » ?
Dans le cas du « blackhole », le routeur ne renvoie aucun message ICMP d'erreur. Dans le cas du « prohibit », le routeur renvoie un message ICMP de type 3 code 13 « communication administratively prohibited ».
- c. Si on utilise les commandes {1, 2, 3} sans les commandes {4, 5, 6} que renvoie le routeur ? *Le routeur ne connaît pas la route et renvoi un message ICMP type 3 code 0 « Network unreachable »*
- d. Donnez la liste des commandes de configuration du routeur « Comptabilité ».

```

1 ip addr add 10.254.254.252/32 dev eth0 brd 10.255.255.255
2 ip addr add 172.17.254.254/16 dev eth1 brd +
3 ip route add 10.2.3.32/27 scope link proto kernel dev eth0 src 10.254.254.252
4 ip route add 10.3.2.0/27 scope link proto kernel dev eth0 src 10.254.254.252
5 ip route add prohibit 10.0.0.0/8
6 ip route add prohibit 172.16.0.0/16
7 ip route add prohibit 192.168.2.0/24
    
```

- e. Où sont situées les machines qui seront impactées par ces définitions de route ?
À l'intérieur des sous-réseaux « Comptabilité » et « Ingénierie ».
- f. Est-ce que la sécurité est « suffisante » ? *Elle bloque les datagrammes en retour, mais pas les datagrammes en entrée de ces réseaux : ce qui permet de faire des attaques :*
- ◊ pour des protocoles sans connexion (basés UDP par exemple) ;
 - ◊ pour des protocoles avec connexion basés le protocole TCP en combinant l'attaque avec une attaque sur la découverte de l'ISN, « Initial Sequence Number ».

La notion de règle

5 – Du point de vue du « core router » :

- o Vers « Comptabilité » 172.17.0.0/16 :

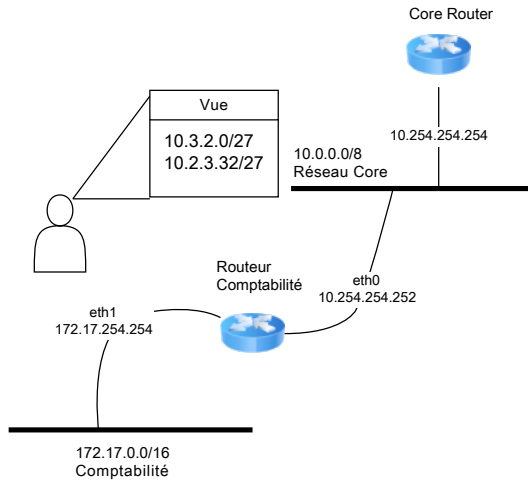
En provenance du réseau	Réponse du routeur
10.2.3.32/27	allow
10.3.2.0/27	allow
0.0.0.0/0	prohibit

- o Vers « Ingénierie » 192.168.2.0/24 :

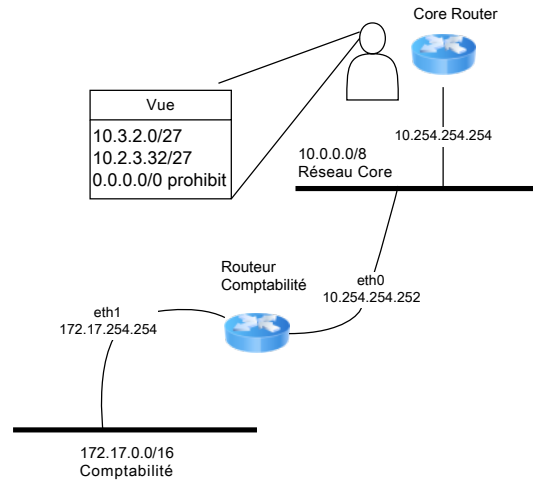
En provenance du réseau	Réponse du routeur
10.10.0.0/16	allow
0.0.0.0/0	blackhole

- a. Est-ce que la définition de la « vue » du réseau depuis le « core router » corrige les problèmes rencontrés dans l'exercice précédent ?

La vue depuis le routeur « comptabilité » :



La vue depuis le routeur « core router » :



À l'aide des règles basées sur l'adresse IP source, on bloque l'accès en entrée dans le réseau « Comptabilité » ce qui vient corriger les défauts énoncés dans l'exercice précédent.

- o Du point de vue du routeur « Comptabilité » :

En provenance du réseau	Réponse du routeur
10.2.3.32/27	allow
10.3.2.0/27	allow
0.0.0.0/0	blackhole

- o Du point de vue du routeur « Ingénierie » :

En provenance du réseau	Réponse du routeur
10.10.0.0/16	allow
0.0.0.0/0	blackhole

- b. Comparez ces définitions avec celles données dans l'exercice 4.

La configuration est plus réduite, puisqu'elle porte sur l'entrée du trafic dans le routeur alors que celle de l'exercice 4 portait sur le trafic en sortie (pas de trafic en entrée ⇒ pas de trafic en retour).

Le trafic est également déjà pris en charge par le « core router », ce qui diminue les besoins de configuration des autres routeurs. En effet, suivant la notion de route, le « core router » autorisait tout trafic à joindre les réseaux « Comptabilité » et « Ingénierie » et les deux autres routeurs bloquaient seulement les réponses.

Avec ces règles, le « core router » peut bloquer le trafic directement.

Soient les commandes implémentant la « vue » du « core router » :

1	# Pour le réseau Comptabilité :
2	ip rule add from 10.2.3.32/27 to 172.17.0.0/16 prio 16000
3	ip rule add from 10.3.2.0/27 to 172.17.0.0/16 prio 16010
4	ip rule add from 0.0.0.0/0 to 172.17.0.0/16 prio 16020 prohibit

- c. À quoi correspond la notation « prio xxxx » ?

À la notion de « priorité » : plus la valeur est petite plus la règle possède une priorité élevée : elle s'appliquera avant une règle de priorité inférieure.

On peut définir les priorités, par exemple, suivant la méthode «xxy00», où «xx» correspond à des règles s'associant à un même usage, le «y» permettant de les interclasser, et le «00» permettant d'insérer éventuellement de nouvelles règles au besoin.

Est-ce que l'ordre d'entrée des lignes est important ?

L'ordre des lignes n'est pas important, ce sont les priorités qui comptent.

À quoi sert la ligne n°4 ?

Cette ligne sert à bloquer tout trafic par défaut, c-à-d dont la source n'a pas été trouvée dans les règles des lignes 2 & 3.

Donnez les règles pour la partie «réseau Ingénierie».

1	ip rule add from 10.10.0.0/16 to 192.168.2/24 prio 17000
2	ip rule add from 0.0.0.0/0 to 192.168.2/24 prio 17010 blackhole

d. Soient les commandes implémentant les règles sur le routeur « Comptabilité » :

1	ip rule add from 10.2.3.32/27 dev eth0 prio 16000
2	ip rule add from 10.3.2.0/27 dev eth0 prio 16010
3	ip rule add from 0.0.0.0/0 dev eth0 prio 16020 blackhole

En quoi les règles définies ci-dessus permettent de mettre en œuvre la «vue» du routeur « Comptabilité » ?

Ici, les règles fonctionnent car elles s'appliquent directement sur l'interface d'entrée concernée «eth0», et car on est sur le routeur connecté au réseau « Comptabilité » (on peut imaginer que l'interface «eth0» est connectée au réseau du «core network»).

Une règle autorise le trafic s'il se présente sur la bonne interface et avec la bonne adresse source.

À quoi sert la règle n°3 ?

À établir une règle par défaut, c-à-d faire disparaître les datagrammes sans message ICMP d'erreur.

Donnez les règles sur le routeur « Ingénierie ».

1	ip rule add from 10.10.0.0/16 dev eth0 prio 17000
2	ip rule add from 192.168.2/24 dev eth1 prio 17010
3	ip rule add from 0.0.0.0/0 prio 17020 blackhole

■ ■ ■ Les tables de routage multiples

6 – Il est possible d'isoler le trafic en le redirigeant dans des tables de routage différentes :

```
1 # Pour le réseau Comptabilité
2 ip rule add from 10.2.3.32/27 to 172.17.0.0/16 prio 16000 table compta
3 ip rule add from 10.3.2.0/27 to 172.17.0.0/16 prio 16010 table compta
4
5 # Pour le réseau Ingénierie
6 ip rule add from 10.10.0.0/16 to 192.168.2.0/24 prio 17000 table ingenierie
```

Il est ensuite possible de remplir les tables de routages :

```
1 # La table compta
2 ip route add 172.17.0.0/16 table compta via 10.254.254.252 proto static
3 ip route add prohibit default
4
5 # La table ingenierie
6 ip route add 192.168.2.0/24 table compta via 10.254.254.253 proto static
7 ip route add blackhole default
```

a. Est-ce que l'implémentation donnée est conforme à la « Security Policy » ?

Oui.

- ◇ Pour un datagramme de source autorisé vers le réseau « Comptabilité », il va suivre la règle donnée à la ligne 2 ou 3, et ensuite aller dans la table « compta » qui le routera vers le réseau.
- ◇ Pour un paquet non autorisé, il n'ira pas dans les tables « compta » et « ingenierie » : il sera routé suivant le contenu de la table par défaut appelée « main » : il faudra vérifier le contenu de la table par défaut pour éviter les problèmes.

Que se passe-t-il si un trafic provenant de 10.0.0.0/8 interdit dans le réseau Ingénierie essaye d'accéder au réseau 192.168.2.0/24 ?

Le paquet sera routé par la table main, qui ne possède pas de route vers ce réseau : un ICMP « network unreachable » sera renvoyé alors que l'on voulait qu'il n'y ait rien en retour.

b. Comment y remédier ?

En ajoutant les règles suivantes :

```
1 # Pour le réseau Comptabilité
2 ip rule add from 0.0.0.0/0 to 172.17.0.0/16 prio 16050 prohibit
3
4 # Pour le réseau Ingénierie
5 ip rule add from 0.0.0.0/0 to 192.168.2.0/24 prio 17050 blackhole
```