Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

Infrastructure Réseau

TD n°2

Routage et « Policy-based Routing »

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

a. À quoi correspond la machine C ?

b. Quelles informations seront présentes dans les tables ARP de la machine A et de la machine B ?

c. Parmi les techniques suivantes lesquelles peuvent expliquer cette configuration ?

- « *Spoofing* » ;
- « *Proxy ARP* » ;
- « *load balancing* » ;
- « *NAT* »

d. Est-ce que chacune de ces adresses IP est attachée à un matériel spécifique et une seule interface réseau ?

2 – a. 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 » ?

b. Soient les 3 « scopes » suivants :

Adresse	Scope
10.1.1.1/8	Scope 1
172.16.1.1/16	Scope 2
192.168.1.1/24	Scope 3

À quel scope appartiennent les adresses suivantes :

Adresse	Scope
10.1.1.2/16	?
172.16.1.2/24	?
192.168.1.2/24	?

c. Chaque adresse appartenant à un scope différent est considérée comme « *primary* » et une nouvelle adresse appartenant à un scope déjà existant est considérée comme « *secondary* ».
Donnez les adresses considérées comme « *secondary* ».

d. Soit la configuration 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
    inet 192.168.127.201/24 brd 192.168.127.255 scope global secondary eth0
    inet6 fe80::20c:29ff:fea7:897/64 scope link valid_lft forever preferred_lft forever
```

Quelle commande a défini l'adresse considérée comme « *secondary* » ?
Si l'adresse « primary *» est supprimée avec la commande « `ip addr del xxxxx/yy dev ethx` » alors les adresses de même scope sont également supprimées.*

La notion de route

3 – Soit un réseau défini comme suit :

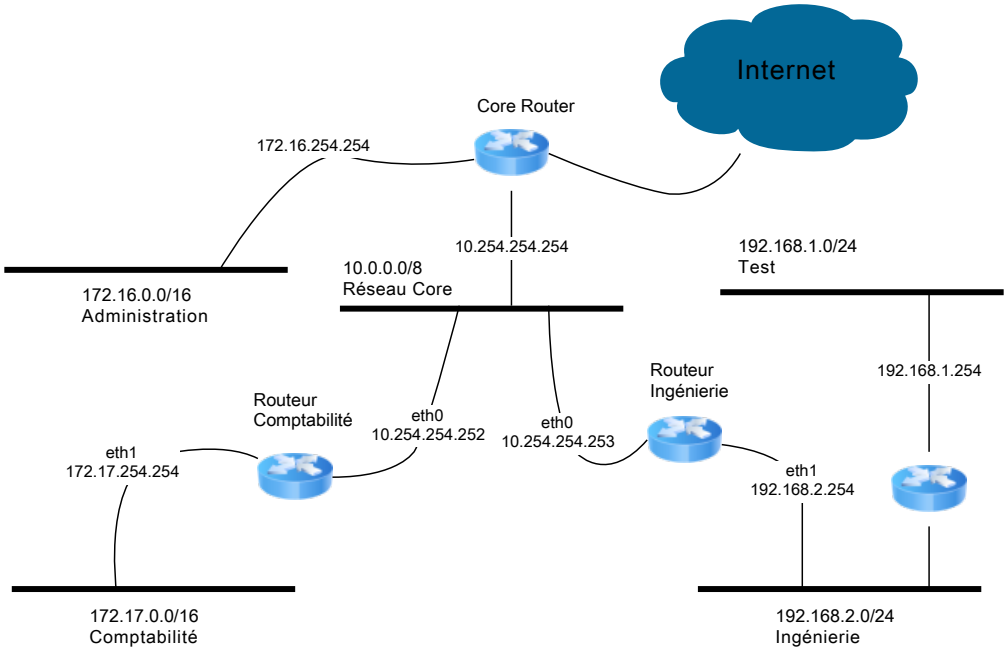
- la société utilise un réseau défini par un scope `10.0.0.0/8` ;
- l'Administration utilise le scope `172.16.0.0/16` ;
- l'Ingénierie utilise le scope `192.168.2.0/24`.
- la Comptabilité utilise le scope `172.17.0.0/16` ;
- le Testing Lab utilise le scope `192.168.1.0/24`.

Le « core router » de la société est connecté :

⋆ à Internet sur `10.254.254.254` (défini comme routeur « par défaut » pour l'accès à Internet) ;

⋆ à la partie administration en `172.16.254.254` (cette interface permet sa configuration) ;

Un second routeur est connecté en `192.168.1.254` à la partie Ingénierie.



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 ?

b. Soit la trace suivante, obtenue avec « `ip route list` » :

```
xterm
10.0.0.0/8 dev eth0 proto kernel scope link src 10.1.1.1
172.16.0.0/16 dev eth0 proto kernel scope link src 172.16.1.1
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.1
127.0.0.0/8 dev lo scope link
```

Depuis l'hôte il est possible de « *pinger* » l'adresse `172.16.254.254` et d'avoir une réponse. Pourquoi ?

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 ?

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

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

```
# 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) ?

e. L'administrateur rentre maintenant les commandes suivantes :

```
# 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 ?

f. 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` ?
Décrivez le chemin emprunté par les paquets.

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 :

▷ Depuis « Comptabilité » `172.17.0.0/16` :

Vers réseau	Réponse
10.2.3.32/27	*full route*
10.3.2.0/27	*full route*
10.0.0.0/8	***prohibit***
172.16.0.0/16	***prohibit***
192.168.2.0/24	***prohibit***

▷ Depuis « Ingénierie » `192.168.2.0/24` :

Vers réseau	Réponse
?	?
?	?
?	?
?	?

Questions :

a. Complétez la « Policy Routing » concernant le réseau « Ingénierie ».

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 # ip route add blackhole 10.0.0.0/8
4 # ip route add 10.10.0.0/16 scope link proto kernel dev eth0 src 10.254.254.253
5 # ip route add blackhole 172.17.0.0/16
6 # ip route add blackhole 172.16.0.0/16
```

b. À quoi correspond la notation « *blackhole* », en quoi est-elle différent de « *prohibit* » ?

c. Si on utilise les commandes $\{1, 2, 3\}$ sans les commandes $\{4, 5, 6\}$ que renvoie le routeur ?

d. Donnez la liste des commandes de configuration du routeur « Comptabilité ».

e. Où sont situées les machines qui seront impactées par ces définitions de route ?

f. Est-ce que la sécurité est « suffisante » ?

La notion de règle

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

- Vers « Comptabilité » `172.17.0.0/16` :

Depuis le réseau	Décision
10.2.3.32/27	allow
10.3.2.0/27	allow
0.0.0.0/0	prohibit

- Vers « Ingénierie » `192.168.2.0/24` :

Depuis le réseau	Décision
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 ?

- Du point de vue du routeur « Comptabilité » :

Depuis le réseau	Décision
10.2.3.32/27	allow
10.3.2.0/27	allow
0.0.0.0/0	blackhole

- Du point de vue du routeur « Ingénierie » :

Depuis le réseau	Décision
10.10.0.0/16	allow
0.0.0.0/0	blackhole

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

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` » ?

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

À quoi sert la ligne n°4 ?

Donnez les règles pour la partie « réseau Ingénierie ».

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

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

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

À quoi sert la règle n°3 ?

Donnez les règles sur le routeur « Ingénierie ».

Les tables de routage *multiples*

Par défaut, sous Linux, un système dispose des tables suivantes :

```
Table #253   =   DEFAULT (created by the default rule #32767)
Table #254   =   MAIN (default master route table)
Table #255   =   LOCAL (broadcast & local addresses)
```

La table `LOCAL` n'est pas à modifier, elle sert pour la diffusion, « *broadcast* », et le routage local.

Les nouvelles tables sont définies dans `/etc/iproute2/rt_tables` :

```
# reserved values
255   local
254   main
253   default
0  unspec
# local
#1 inr.ruhep
1 compta
2 ingenierie
```

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 table compta
4
5 # La table ingenierie
6 ip route add 192.168.2.0/24 table ingenierie via 10.254.254.253 proto sta
  tic
7 ip route add blackhole default table ingenierie
```

a. Est-ce que l'implémentation donnée est conforme à la « Security Policy » ?
Vous décrirez le chemin emprunté par les paquets de source autorisée et non autorisée.

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

b. Comment y remédier ?