



Durée : 1h30 — Documents autorisés

■■■■ Routage dynamique & « Routing Protocol » — 8 points

1 – Dans un réseau d’interconnexion on a capturé le trafic suivant :

3pts

```
03:43:03.387182 00:10:7b:35:f5:b5 > 01:00:5e:00:00:05, ethertype IPv4 (0x0800), length 78: (tos 0xc0, ttl 1, id 2, offset 0, flags [none], proto OSPF (89), length 64)
  192.168.23.2 > 224.0.0.5: OSPFv2, Hello, length 44
  Router-ID 10.3.3.3, Area 0.0.0.1, Authentication Type: none (0)
  Options [External]
  Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1

03:44:03.385637 00:10:7b:35:f5:b5 > 00:00:0c:07:ac:01, ethertype IPv4 (0x0800), length 206: (tos 0xc0, ttl 1, id 142, offset 0, flags [none], proto OSPF (89), length 192)
  192.168.23.2 > 192.168.23.1: OSPFv2, Database Description, length 172
  Router-ID 10.3.3.3, Area 0.0.0.1, Authentication Type: none (0)
  Options [External], DD Flags [More], MTU: 1500, Sequence: 0x000000ce1
  Advertising Router 10.1.1.1, seq 0x80000002, age 18s, length 76
  Router LSA (1), LSA-ID: 10.1.1.1
  Options: [External, Demand Circuit]
  Advertising Router 10.2.2.2, seq 0x80000006, age 19s, length 76
  Router LSA (1), LSA-ID: 10.2.2.2
  Options: [External, Demand Circuit]
  Advertising Router 10.3.3.3, seq 0x80000005, age 18s, length 88
  Router LSA (1), LSA-ID: 10.3.3.3
  Options: [External, Demand Circuit]
  Advertising Router 10.4.4.4, seq 0x80000002, age 15s, length 64
  Router LSA (1), LSA-ID: 10.4.4.4
  Options: [External, Demand Circuit]
  Advertising Router 10.1.1.1, seq 0x80000001, age 19s, length 8
  Summary LSA (3), LSA-ID: 10.0.252.1
  Options: [External, Demand Circuit]
  Advertising Router 10.1.1.1, seq 0x80000001, age 19s, length 8
  Summary LSA (3), LSA-ID: 192.168.4.0
  Options: [External, Demand Circuit]
```

Questions :

- a. À quel « area » appartient ce routeur ?
Quel pourrait être le « type » de ce routeur suivant les appellations d’OSPF ?
b. À quel matériel correspond l’adresse de destination « 192.168.23.1 » ?
c. À quoi sert l’adresse « 224.0.0.5 » ? Que permet-elle par rapport au protocole OSPF ?
d. À quoi correspond la valeur « age » ?

2 – Dans un réseau d’interconnexion on a capturé le trafic suivant :

3pts

```
02:12:26.504157 IP (tos 0xc0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 92)
  10.0.0.253.520 > 224.0.0.9.520:
  RIPv2, Response, length: 64, routes: 3
  AFI IPv4, 0.0.0.0/0, tag 0x0000, metric: 16, next-hop: self
  AFI IPv4, 164.81.10.0/24, tag 0x0000, metric: 16, next-hop: self
  AFI IPv4, 193.50.1.0/24, tag 0x0000, metric: 16, next-hop: self
0x0000: 45c0 005c 0000 4000 0111 8dcb 0a00 00fd E..\.@.....
0x0010: e000 0009 0208 0208 0048 3e54 0202 0000 .....H>T....
0x0020: 0002 0000 0000 0000 0000 0000 0000 0000 .....
0x0030: 0000 0010 0002 0000 ac10 0100 ffff ff00 .....
0x0040: 0000 0000 0000 0010 0002 0000 c0a8 6400 .....d.
0x0050: ffff ff00 0000 0000 0000 0010 .....
```

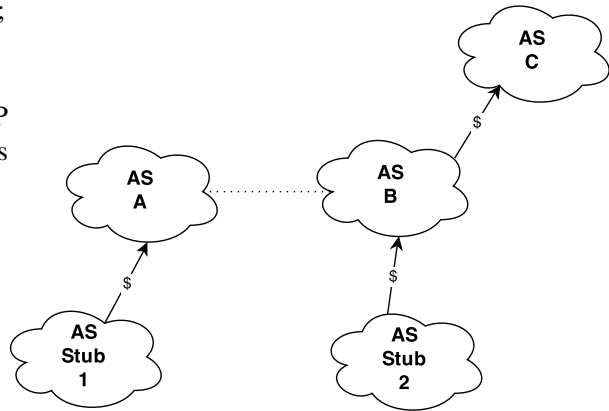
Questions :

- a. À quoi sert l’adresse « 224.0.0.9 » et à quoi correspond la valeur « 520 » ?
b. À quoi sert ce paquet ?
c. Qu’est-ce que cela veut dire pour les réseaux dont l’adresse est indiquée dans le corps du paquet ?

3- BGP

- 2pts
- * l'AS_A et l'AS_B ont un accord de « peering » ;
 - * l'AS₁ est cliente de l'AS_A ;
 - * l'AS₂ est cliente de l'AS_B ;
 - * l'AS_C reçoit les informations de routage BGP de la part de l'AS_B permettant d'atteindre les réseaux suivants :

164.81.10.0/24	AS _B
193.18.32.192/26	AS _B



Vous justifierez vos réponses.

- a. Indiquez pour chacun des réseaux suivants à quel AS « Stub », il appartient :

Réseaux	AS ₁	AS ₂
87.34.123.0/24		
164.81.10.0/24		
193.18.32.192/26		
211.89.42.128/25		

- b. Comment sont appelées les deux AS, AS_A et AS_B ?

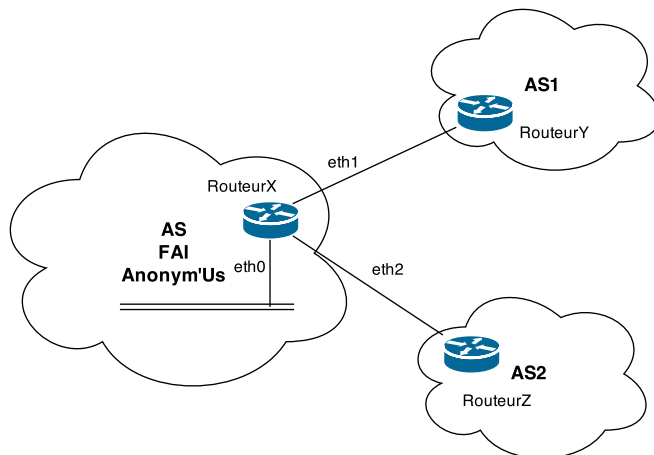
Policy Routing & Firewall- 9 points

- 4- Le FAI « Anonym'Us » veut offrir un service d'anonymisation pour ses clients entreprises lorsqu'ils utilisent le protocole de chat « IRC », « Internet Relay Chat », basé sur le protocole TCP et le port serveur 6667.

6pts

Le fonctionnement de l'anonymisation est le suivant :

- ▷ les clients du FAI « Anonym'Us » :
 - ◇ obtiennent une adresse globale de sous-réseau au choix parmi les réseaux : 143.56.17.0/24, 43.12.66.0/23 et 111.27.12.0/22 (la configuration du réseau d'interconnexion permettant à ces différents sous-réseaux d'atteindre RouteurX n'est pas donnée) ;
 - ◇ utilisent RouteurX comme route par défaut pour leur routeur de sortie ;
- ▷ le FAI « Anonym'Us » utilise :
 - ◇ l'AS1 pour tout son trafic, en utilisant la route par défaut désignant « RouteurY » ;
 - ◇ l'AS2 pour le trafic devant bénéficier de l'anonymat ;
 - ◇ vu de l'extérieur le trafic concernant le protocole IRC doit apparaître comme provenant du réseau « 156.32.45.17/16 ».



Soit la configuration des routeurs suivante :

RouteurX	156.32.45.17/16
RouteurY	118.65.23.11/22
RouteurZ	201.18.32.100/23

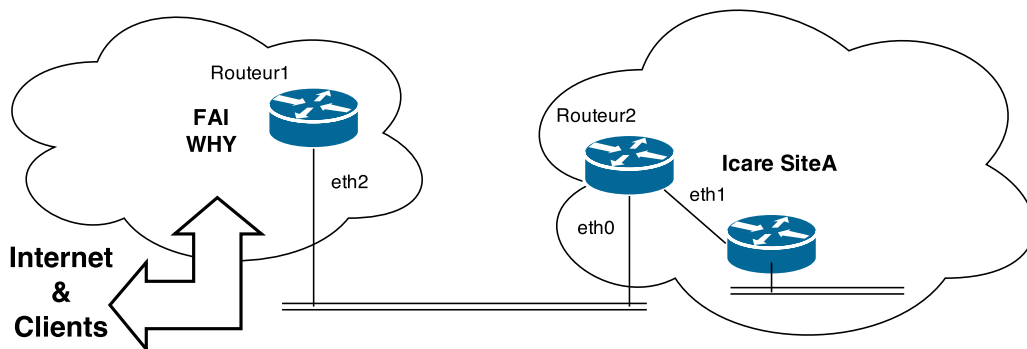
Questions :

- a. Expliquez par quel(s) moyen(s) vous allez utiliser :
 - ◇ le « Policy Routing »
 - ◇ le firewall « NetFilter »pour réaliser le travail d'anonymisation.
Vous justifierez votre réponse.
- b. Donnez les ordres de configuration de la « Policy Routing » et du firewall « NetFilter » sur le RouteurX réalisant l'anonymisation du trafic IRC.
- c. Vérifiez que le trafic IRC circule bien du client vers le serveur et vice-versa.
Justifiez votre réponse par un exemple de traitement de datagramme.

5 – 6pts En tant que responsable du réseau d'interconnexion du FAI « WHY », vous devez travailler en collaboration avec l'ingénieur Réseaux d'une entreprise Icare qui est en train de mettre à jour son système d'information.

L'entreprise Icare :

- ★ passe par le FAI « WHY » pour accéder à Internet. Les clients de l'entreprise passe également par le FAI pour accéder au « SiteA » ;
- ★ fournit de l'hébergement d'applications métiers accessibles en TCP sur le port 548 ;
- ★ répartit les connexions entrantes de ses clients entre deux sites distincts « SiteA », 136.18.24.224/27 et « SiteB », 200.32.45.16/28 suivant leur proximité géographique avec l'un ou l'autre de ces sites ;
- ★ réalise des opérations de synchronisation à l'aide de protocoles sécurisés basés sur le port 22 et le protocole TCP entre les sites « SiteA » et « SiteB » ;



Questions :

- a. En tant que responsable du réseau d'interconnexion du FAI « WHY », comment pouvez vous permettre au trafic provenant du « SiteB » d'être **mieux géré** par le « SiteA », par rapport à celui provenant des clients de l'entreprise ?

Que faut-il utiliser : de la « Policy Routing » et/ou du « firewall » ?

Vous justifierez votre réponse.

Vous donnerez la configuration à employer sur Routeur1 pour réaliser ce travail.

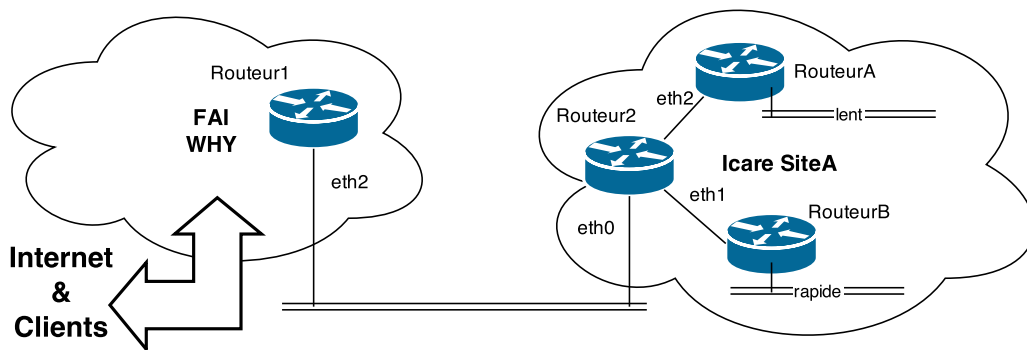
Indications :

- ◇ les adresses des clients de l'entreprise ne proviennent pas de « SiteB » ;
- ◇ vous ne vous intéressez pas à la configuration de Routeur2.
- ◇ la configuration des routeurs est la suivante :

Routeur1	eth2	192.168.1.254/24
Routeur2	eth0	192.168.1.253/24
	eth1	136.18.24.254/27

Le « SiteA » vient d'investir dans du nouveau matériel pour son « SiteA » : switch gigabits utilisant la fibre optique, serveurs de données/traitement utilisant de la virtualisation dynamique. Ce réseau est accessible par le « RouteurA ».

L'ancien matériel réseau utilisant des serveurs de données/traitements sans virtualisation et des liaisons en 100Mbits est accessible par le « RouteurB ».



Dans une phase de transition, le nouveau réseau « rapide » du « SiteA » est un « miroir » de l'ancien réseau « lent » du « SiteA » :

- ▷ les serveurs fournissent les mêmes services et exploitent les mêmes données qui sont automatiquement synchronisées entre les deux (le mécanisme de synchronisation utilise un réseau privé et des cartes réseaux supplémentaires sur les serveurs d'application) ;
- ▷ la configuration IP du réseau « lent » est **la même** que celle du réseau « rapide » ;
- ▷ un client peut accéder, sans faire la différence, aux machines accessibles par le RouteurA ou par le RouteurB ;
- ▷ par défaut les clients accèdent à la version lente et les connexions du « SiteB » accèdent à la version « rapide ».

Questions :

- b. Si les réseaux « lent » et « rapide » sont configurés de la même manière, est-ce que les interfaces eth1 et eth2 de Routeur2 peuvent :
- ◇ avoir la même adresse ?
 - ◇ permettre d'accéder à un réseau configuré de la même manière ?

Donnez les commandes de configuration à utiliser pour configurer ces interfaces sur Routeur2.

- c. En tant qu'ingénieur Réseaux du « SiteA », comment pouvez vous exploiter la solution utilisée par le FAI pour distinguer le trafic et permettre soit d'utiliser réseau « rapide », soit le réseau « lent » ?

Vous donnerez les commandes à utiliser pour faire la configuration de Routeur2.

■■■■ Rappels & Compléments d'information

Les instructions du « Policy Routing » sont : « ip rule », « ip route », « ip address » et la création de table dans « /etc/iproute2/rt_tables ».

Dans la saisie d'une commande « ip rule », si l'option « table » ou « lookup » n'est pas utilisée, la commande affecte la table « main ».

Quelques exemples de règles de firewall :

```
iptables -t nat -A POSTROUTING -p tcp --dst 164.81.10.60 --dport 80 -j SNAT --to-source 164.81.10.45
iptables -t nat -A POSTROUTING -s 10.10.10.0/8 -j MASQUERADE
iptables -t nat -A PREROUTING -p tcp -d 15.45.23.67 --dport 80 -j DNAT --to-destination 192.168.1.1-192.168.1.10
iptables -t mangle -A FORWARD -p tcp --dport 80 -j DSCP --set-dscp 1
iptables -t mangle -A POSTROUTING -p tcp --dport 80 -j DSCP --set-dscp-class EF
iptables -A INPUT -i eth0 -p udp --dport 67:68 --sport 67:68 -j ACCEPT
```