TD n°3
Les listes de contrôle d'accès

Exercice 1 *Masque générique*

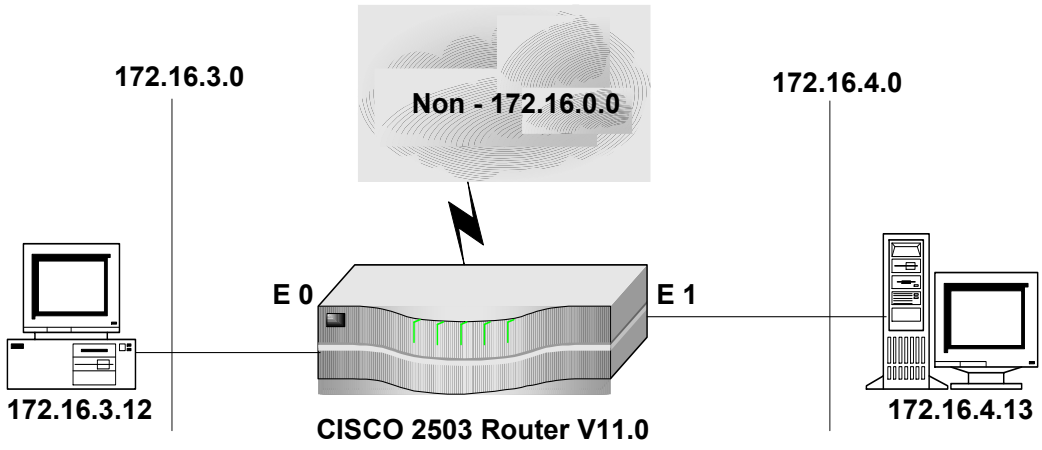
Donnez l'ensemble des adresses IP concernées par les notations suivantes :

1. 192.168.10.0 0.0.0.255
2. 172.16.0.0 0.0.255.255
3. 10.0.0.0 0.255.255.255
4. 192.168.50.1 0.0.0.254
5. 192.168.0.0 0.0.254.255
6. 192.168.10.61 0.0.0.95

Trouvez les notations « masque générique » qui correspondent aux réseaux suivants :

7. 10.250.50.112 255.255.255.224
8. 192.168.16.0 à 192.168.16.127
9. 172.250.16.32 à 172.250.31.63
10. 192.168.10.128 à 192.168.10.159 et 192.168.10.192 à 192.168.10.223

Exercice 2 *ACL standard et étendue*

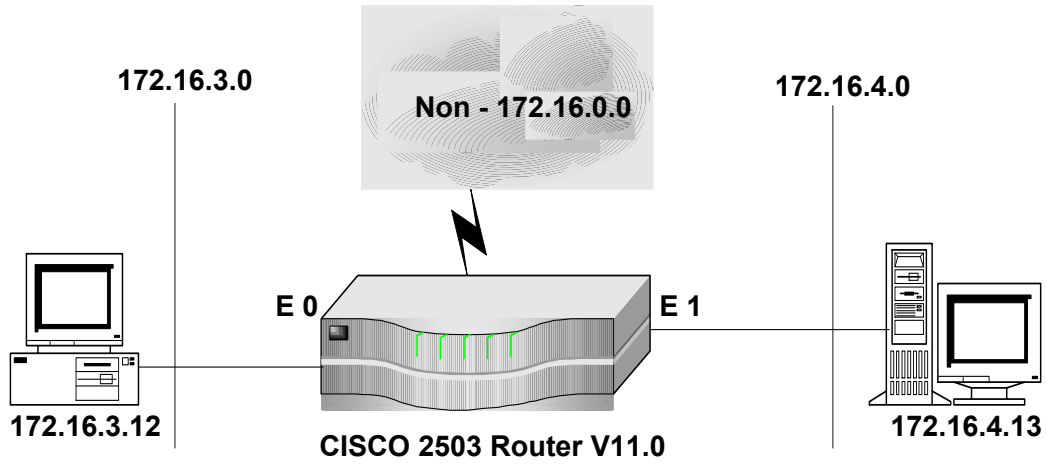



```
Router(config)#access-list 1 permit 172.16.0.0  0.0.255.255
Router(config)#interface Ethernet 0
Router(config-if)#ip access-group 1 out
Router(config)#interface ethernet 1
Router(config-if)#ip access group 1 out
```

1. Comment peut-on reconnaître qu'il s'agit d'une ACL standard ?
2. A quoi sert-elle ?
3. Est-il possible d'obtenir le même fonctionnement en plaçant la même ACL autrement ?

4. Est-il possible d'obtenir le même fonctionnement en plaçant une ACL standard différente sur une autre interface ?
5. Ecrivez une ACL étendue qui permette d'obtenir le même fonctionnement
6. Comment placez-vous cette ACL étendue ?
7. Quel avantage voyez-vous à cette solution ?

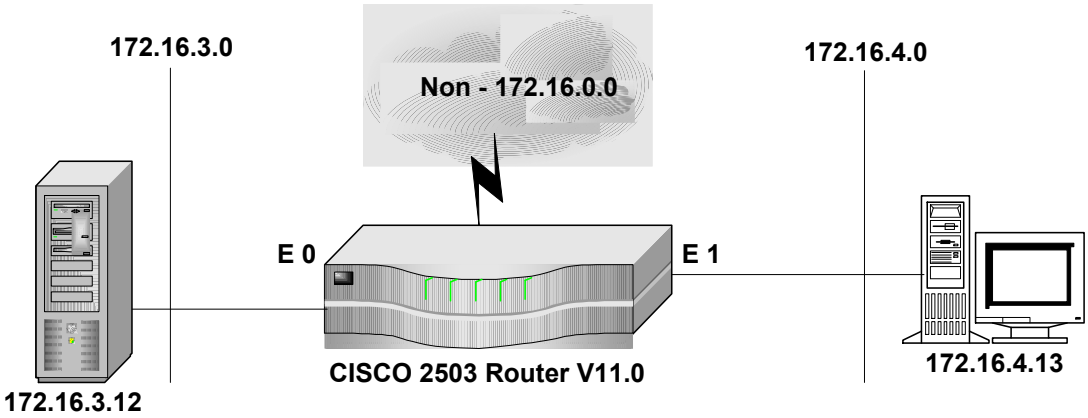
Exercice 3 *ACL standard*




```
Router(config)# access-list 1 deny 172.16.4.13 0.0.0.0
Router(config)# interface ethernet 0
Router(config)# ip access-group 1 out
```

1. A quoi sert cette ACL ?
2. Proposez une modification pour qu'elle produise effectivement l'effet attendu

Exercice 4 *ACL étendue*




```
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
Router(config)#access-list 101 permit ip any any
Router(config)#interface ethernet 0
Router(config-if)#access-group 101 out
```

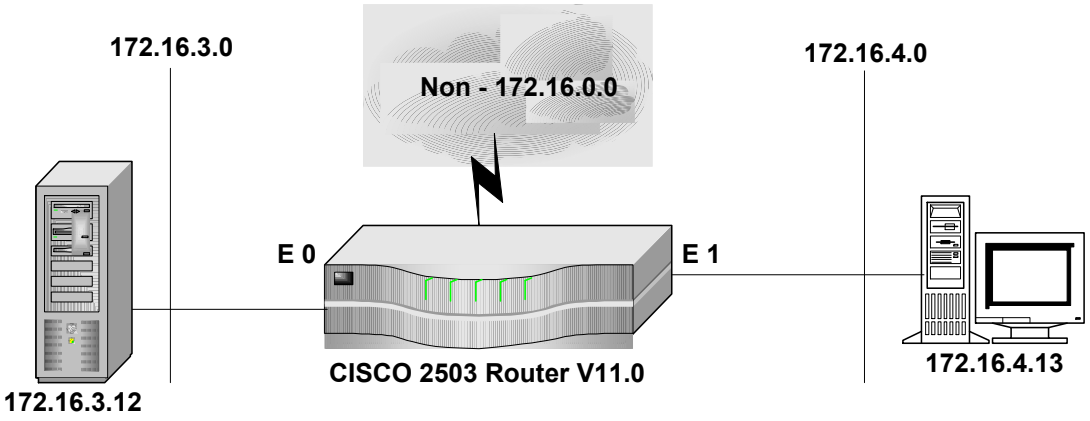
1. A quoi sert cette ACL ?
2. Pourquoi est-il utile de filtrer le port 21 et le port 20 ?
3. Trouvez une ACL standard qui produit le même effet

Exercice 5 *ACL étendue*

```
Router(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255 any neg 80
Router(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255 any neg 21
Router(config)#access-list 101 permit ip any any
Router(config)#interface ethernet 0
Router(config-if)#access-group 101 in
```

1. Quel est l'effet de cette ACL ?
2. En devinant l'intention de l'administrateur, proposez une ACL correcte

Exercice 6 *ACL étendue*



On souhaite empêcher les hôtes du réseau 172.16.4.0/24 de dialoguer avec le serveur web 172.16.3.12/24. Pour cela, l'administrateur réseau a choisi de ne pas bloquer les requêtes qui sortent du réseau 172.16.4.0/24, mais plutôt de bloquer les réponses du serveur.

1. Quelle syntaxe proposeriez vous ?
2. A quelle interface et dans quel sens appliquez-vous cette ACL ?
3. Que doit obligatoirement faire le routeur pour qu'une telle ACL puisse fonctionner ?
4. Que fait le routeur en réalité ?
5. Quelle est donc la seule manière de répondre au problème posé ?

Exercice 7 *ACL réflexives*

1. Quelle est l'utilité particulière des ACL réflexives ?
2. Est-il possible de faire la même chose avec des ACL étendues ?
3. Es-il possible de faire la même chose avec des ACL étendues, sans utiliser l'option « established » ?
4. Finalement, quelle est réellement la différence entre ACL étendue et ACL réflexive ?
5. Trouvez une situation où une ACL étendue serait mise en défaut, alors que son équivalent réflexive ne le serait pas
6. Pouvez-vous retrouver la particularité de la syntaxe d'une ACL réflexive ?

Réponses

Exercice 1

1. de 192.168.10.0 à 192.168.10.255
2. de 172.16.0.0 à 172.16.255.255
3. de 10.0.0.0 à 10.255.255.255
4. toutes les machines impaires du réseau 192.168.50.0/24
5. 192.168.0.0 à 192.168.0.255
   et 192.168.2.0 à 192.168.2.255
   et 192.168.4.0 à 192.168.4.255
   et … …
   et 192.168.250.0 à 192.168.250.255
   et 192.168.252.0 à 192.168.252.255
   et 192.168.254.0 à 192.168.254.255
6. 192.168.10.32 à 192.168.10.63
   et 192.168.10.96 à 192.168.10.127
7. 10.250.20.112 0.0.0.31
8. 192.168.16.32 0.0.0.127
9. 172.250.16.32 0.0.0.31
10. 192.168.10.128 0.0.0.95

Exercice 2

1. son numéro est compris entre 1 et 99 ; par ailleurs, seule l'adresse IP source est mentionnée
2. Elle oblige le réseau de droite à n'accepter que les paquets qui viennent du réseau de gauche et inversement
3. non
4. non
5. il suffit d'interdire tout le trafic entrant sur la liaison série :
   access-list 100 deny ip any any
6. dans le sens entrant :
   interface serial
   ip access-group 100 in
7. le routeur n'aura pas à traiter le trafic venant de l'extérieur avant de l'interdire

Exercice 3

1. cette ACL est fausse, elle interdit en fait tout le trafic sortant de E0 (c'est-à-dire vers le réseau 172.16.3.0/24. L'idée de l'administrateur était de n'interdire que le trafic qui vient du serveur 172.16.4.13
2. il faut ajouter : access-list 1 permit ip any any

Exercice 4

1. elle empêche les machines du réseau de droite d'utiliser ftp sur le réseau de gauche. Il faut remarquer que cette ACL aurait pu avantageusement être placée en entrée de l'interface E1.
2. il faut filtrer les deux ports car l'application ftp les utilise tous les deux (21 : contrôle ; 20 : données)
3. impossible, car les ACLs standards ne permettent pas de spécifier un numéro de port

Exercice 5

1. elle interdit tout car : si le paquet n'est pas à destination du port 21, il est refusé par la première ligne, si le paquet est à destination du port 80, il est refusé par la deuxième ligne
2. On devine que l'administrateur voulait interdire tout, sauf les ports 80 et 21. Il aurait dû écrire :

```
Router(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 80
Router(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 21
Router(config)#access-list 101 deny ip any any
Router(config)#interface ethernet 0
Router(config-if)#access-group 101 in
```

Exercice 6

1. access-list 100 deny tcp host 172.16.3.12 172.16.4.0 0.0.0.255 eq 80
access-list 100 permit ip any any

2. interface ethernet0
ip access-group 100 in

3. il faut que le routeur filter le port 80, mais attention, dans cette situation le port 80 apparaît dans le champ « port destination » de l'en-tête TCP !
4. en réalité, le routeur ne filtre que sur le port source !
5. la seule manière est de filtrer les requêtes et pas les réponses. La solution du 1. ne marche en fait pas du tout !

Exercice 7

1. elle permet de tenir compte des informations de connexion du protocole TCP, et pour ICMP et UDP, elles permettent de « pister » les connexions en observant la cohérence des identifiants de connexion (c'est-à-dire les couples @IP, n° de port)
2. oui, mais seulement evec TCP en utilisant l'option « established »
3. non
4. la vérification de UDP et ICMP, avec en plus une notion très importants : le temps. En effet, une ACL réflexive laissera passer le trafic motivé par une session en cours, mais seulement pendant un certain temps (programmable)
5. une ACL étendue (sans l'option established) acceptera un paquet entrant qui serait une « fausse réponse », c'est-à-dire un paquet non motivé par une session, alors qu'il est construit exactement comme si c'était le cas
6. il y a un lien entre le trafic inspecté en sortie et le trafic évalué en entrée