

TP10 - VLANs et ACLs

I/5 Configuration du VLAN 10

1. Sur S2 et S3, configurer les noms d'hôte adaptés
2. Créer et nommer le VLAN 10 sur S2 et S3 du tableau I/3
3. Question : Quelles commandes avez-vous tapé? Vous indiquerez les équipements sur lesquels ces commandes ont été tapées

```
#Sur S2
en
conf t
hostname S2
vlan 10
name IT
end
```

```
#Sur S3
en
conf t
hostname S3
vlan 10
name IT
end
```

4. Configurer et activer l'interface de gestion sur S2 et S3 en utilisant les informations relatives à l'adresse IP dans le tableau d'adressage
5. Question : Quelles commandes avez-vous tapé? Vous indiquerez les équipements sur lesquels ces commandes ont été tapées

```
#Sur S2
en
conf t
interface vlan 10
ip address 192.168.1.1 255.255.255.0
no shutdown
end
```

```
#Sur S3
en
conf t
interface vlan 10
ip address 192.168.1.2 255.255.255.0
no shutdown
end
```

6. Sur S2 et S3, affecter l'interface Fa0/1 au VLAN 10

7. Question : Indiquer les commandes tapées

```
#Sur S2 et S3
en
conf t
interface Fa0/1
switchport mode access
switchport access vlan 10
```

8. Question : Bien que PC1 et PC3 soient dans le même VLAN, la communication n'est pas possible (voir ci-dessous), expliquer pourquoi.

- Pour le moment nous n'avons pas autorisé les paquets de la vlan 10 à transiter entre les deux commutateurs donc les paquets ne dépassent pas les commutateurs lors d'un ping.

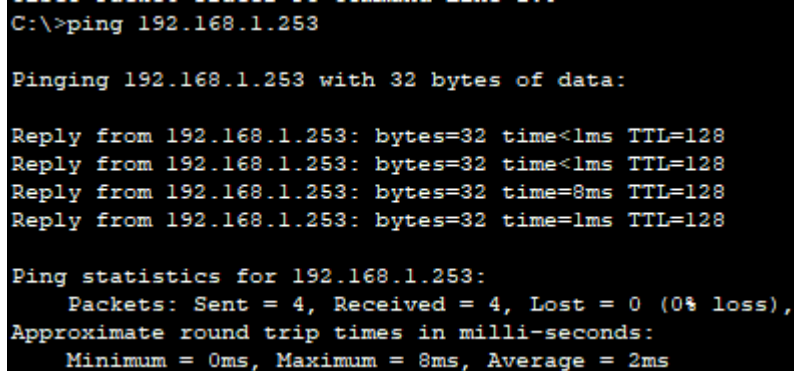
9. Sans utilisation du mode trunk, régler le problème

10. Question : Expliquer comment le problème a été réglé ainsi que les commandes tapées. Vous justifierez également la résolution du problème (une capture de la communication effective est attendue).

- Pour régler le problème, il faut autoriser les paquets à transiter entre les switches de cette manière :

```
#Sur S2 et S3
en
conf t
interface Fa2/1
switchport mode access
switchport access vlan 10
end
```

ping de PC1 à PC3:



```
C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Reply from 192.168.1.253: bytes=32 time<1ms TTL=128
Reply from 192.168.1.253: bytes=32 time<1ms TTL=128
Reply from 192.168.1.253: bytes=32 time=8ms TTL=128
Reply from 192.168.1.253: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

II/5 Configuration du VLAN 20

1. Ø Faire la configuration totale du VLAN 20. Le mode trunk n'est toujours autorisé. (conseil : il peut être judicieux d'adapter ce qui a été fait lors de la partie précédente)
2. Question : Indiquer les commandes tapées sur S2

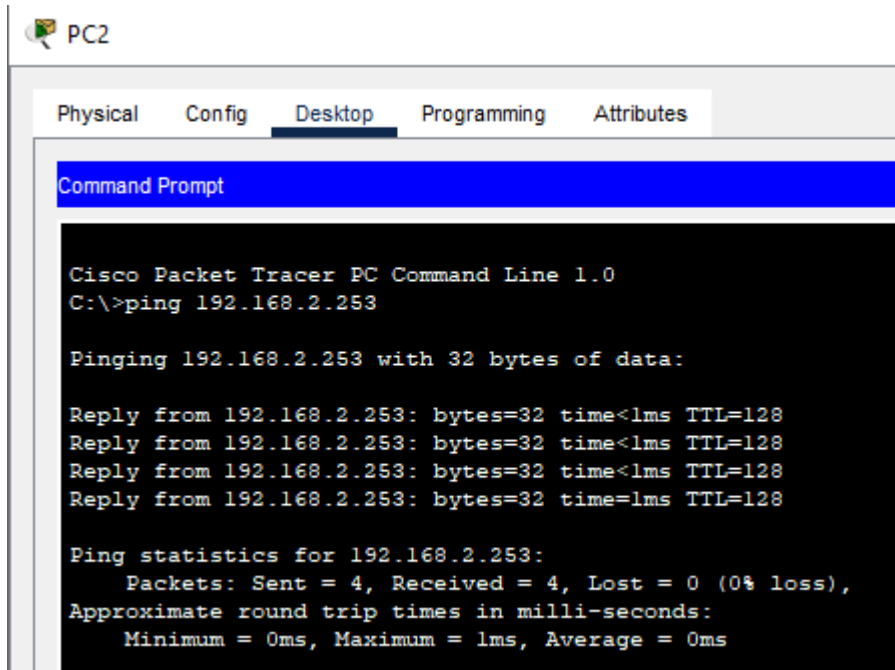
```
en
conf t
vlan 20
name RH
exit
interface vlan 20
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
interface Fa1/1
switchport mode access
switchport access vlan 20
exit
interface Fa3/1
switchport mode access
switchport access vlan 20
```

3. Question : Indiquer les commandes tapées sur S3

```
en
conf t
vlan 20
name RH
exit
interface vlan 20
ip address 192.168.2.2 255.255.255.0
no shutdown
exit
interface Fa1/1
switchport mode access
switchport access vlan 20
exit
interface Fa3/1
switchport mode access
switchport access vlan 20
```

4. Question : Indiquer si la structure du réseau a été modifiée (rajout/suppression de câble/machine). Si oui, indiquer pourquoi.
 - La structure du réseau a été modifiée, il a fallu ajouter un nouveau lien entre S2 et S3 afin de pouvoir supporter le trafic du vlan 20 pour pouvoir faire communiquer PC2 et PC4.
5. Question : Montrer que PC2 communique avec PC4

Ping de PC2 à PC4:



III/4 Configuration des équipements

1. Ø Sur R1, configurer le nom d'hôte adapté
2. Ø Définir les adresses IPs des interfaces de R1 en vous aidant de la table d'adressage
3. Question : Quelles commandes avez-vous tapé ?

```
#Sur R1
en
conf t
hostname R1
interface fa0/0
ip address 172.16.1.1 255.255.255.0
no shutdown
exit
interface fa1/0
ip address 192.168.1.3 255.255.255.0
no shutdown
exit
interface fa2/0
ip address 192.168.2.3 255.255.255.0
no shutdown
exit
```

4. Ø Affecter les ports voulus aux VLANs sur S2
5. Question : Indiquer les commandes tapées

```
#Sur S2
en
conf t
interface fa4/1
switchport mode access
switchport access vlan 10
exit
interface fa5/1
switchport mode access
switchport access vlan 20
```

6. Question : PC1 peut-il communiquer avec Server1 (capture du ping à l'appui)?

- PC1 peut communiquer avec Server1 grâce à la mise en place du routeur.

```
C:\>ping 172.16.1.254

Pinging 172.16.1.254 with 32 bytes of data:

Request timed out.
Reply from 172.16.1.254: bytes=32 time<1ms TTL=127
Reply from 172.16.1.254: bytes=32 time=1ms TTL=127
Reply from 172.16.1.254: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

7. Question : Quel « problème » cette mise en place a-t-elle introduite ?

- Le problème vient du fait que maintenant que le routeur a été mis en place, on a perdu la notion de "cloisonnement" des Vlan, il faudra donc mettre en place des ACLs pour restreindre les communications.

IV/ Partie 4 : Mise en place d'ACLs

1. Question : Compléter le tableau suivant :

Interfaces de R1 (sortie)	Numéro de la règle à appliquer
Fa0/0	Règles 2, 3 et 4
Fa1/0	Règle 5
Fa2/0	Règle 1

2. Créer l'ACL 1 avec les règles adéquates. Cette ACL sera associée à l'interface Fa0/0 de R1

3. Question : Indiquer les commandes tapées

```
#Sur R1
en
conf t
access-list 1 deny 192.168.2.254 0.0.0.0
```

```
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.1.0 0.0.0.255
```

4. Ø Appliquer la règle à la bonne interface

5. Question : Indiquer les commandes tapées

```
interface fa0/0
ip access-group 1 out
exit
```

6. Ø Question : Mettre en avant la création de l'ACL

```
sh access-list
Standard IP access list 1
 10 deny host 192.168.2.254
 20 permit 192.168.2.0 0.0.0.255
 30 permit 192.168.1.0 0.0.0.255
```

7. Ø Créer l'ACL 2 avec les règles adéquates. Cette ACL sera associée à l'interface Fa1/0 de R1

8. Question : Indiquer les commandes tapées

```
access-list 2 deny 192.168.2.0 0.0.0.255
access-list 2 permit 172.16.1.0 0.0.0.255
```

9. Ø Appliquer la règle à la bonne interface

10. Question : Indiquer les commandes tapées

```
interface fa1/0
ip access-group 2 out
```

11. Ø Question : Mettre en avant la création de l'ACL

```
sh access-list
Standard IP access list 1
 10 deny host 192.168.2.254 (8 match(es))
 20 permit 192.168.2.0 0.0.0.255 (3 match(es))
 30 permit 192.168.1.0 0.0.0.255 (8 match(es))
Standard IP access list 2
 10 deny 192.168.2.0 0.0.0.255 (4 match(es))
```

12. Question : Doit-on créer une ACL pour bloquer la communication entre le VLAN IT et RH (règle 1)

- Pour des questions de sécurité il est conseillé de créer une telle ACL même si dans la situation actuelle, RH ne peut pas communiquer avec IT, le trafic est possible dans un sens mais pas dans un autre.

13. Ø Créer l'ACL 3 avec les règles adéquates. Cette ACL sera associée à l'interface Fa2/0 de R1

14. Question : Indiquer les commandes tapées

```
access-list 3 deny 192.168.1.0 0.0.0.255
access-list 3 permit 172.16.1.0 0.0.0.255
```

15. Ø Appliquer la règle à la bonne interface

16. Question : Indiquer les commandes tapées

```
interface fa2/0
ip access-group 3 out
```

17. Ø Question : Mettre en avant la création de l'ACL

```
R1#sh access-list
Standard IP access list 1
 10 deny host 192.168.2.254 (8 match(es))
 20 permit 192.168.2.0 0.0.0.255 (3 match(es))
 30 permit 192.168.1.0 0.0.0.255 (8 match(es))
Standard IP access list 2
 10 deny 192.168.2.0 0.0.0.255 (12 match(es))
Standard IP access list 3
 10 deny 192.168.1.0 0.0.0.255
```

18. Ø Il vous est fortement conseillé de vérifier toutes les règles et les communications possibles (ou non)

V/2 Un peu de pratique

1. Question : Sur quelle interface de R1 cette ACL doit-elle se mettre ?

- Etant donné que les ACLs étendues doivent être appliquées le plus proche possible de la source, cette ACL pour bloquer le trafic HTTP doit être appliquée sur l'interface Fa2/0 de R1.

2. Ø Créer l'ACL HTTP-RH sur R1 permettant de bloquer le trafic HTTP du département RH aux serveurs

3. Question : Indiquer les commandes tapées

```
en
conf t
access-list 100 deny tcp 192.168.2.0 0.0.0.255 any eq 80
```

4. Ø Attribuer l'ACL à la bonne interface

5. Question : Indiquer les commandes tapées

```
interface fa2/0
ip access-group 100 in
```

6. Ø Depuis PC4, tenter un ping vers Server1

7. Question : Indiquer le problème et sa cause.

- PC4 ne peut plus communiquer avec les serveurs car suite à l'ajout des acl étendues, il n'y a aucune acl qui autorise tout autre trafic (en dehors du http), il se passe alors le phénomène de refus implicite bloquant aussi le trafic icmp.

8. Ø Permettre à toutes les machines du département RH de ping les serveurs (sauf PC2 cf. partie précédente)

9. Question : Indiquer les commandes tapées

```
access-list 100 permit ip any any
```

10. Ø Vérifier si le ping est maintenant réalisable

```
C:\>ping 172.16.1.254

Pinging 172.16.1.254 with 32 bytes of data:

Reply from 172.16.1.254: bytes=32 time=7ms TTL=127
Reply from 172.16.1.254: bytes=32 time<1ms TTL=127
Reply from 172.16.1.254: bytes=32 time<1ms TTL=127
Reply from 172.16.1.254: bytes=32 time=4ms TTL=127

Ping statistics for 172.16.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\>ping 172.16.1.253

Pinging 172.16.1.253 with 32 bytes of data:

Request timed out.
Reply from 172.16.1.253: bytes=32 time<1ms TTL=127
Reply from 172.16.1.253: bytes=32 time=5ms TTL=127
Reply from 172.16.1.253: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.253:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms
```