

Cours Théorique – Séance : Introduction aux ACL et restriction SSH

1. Qu'est-ce qu'une ACL ?

- Une Access Control List (ACL) est un ensemble de règles permettant de filtrer le trafic réseau.
- Fonctionne en lisant les paquets de haut en bas → ordre important.
- Chaque paquet est comparé aux règles, si aucune règle ne correspond → deny implicite (bloqué).

👉 Utilisation principale :

- Restreindre l'accès à des ressources (SSH, Telnet, HTTP).
 - Filtrer des flux IP (trafic entrant/sortant).
-

2. Types d'ACL

- ACL standard : filtre uniquement selon l'adresse source IP.
- ACL étendue : filtre selon l'IP source/destination, protocole, ports.

👉 Dans notre cas (SSH autorisé seulement pour une IP), une ACL standard suffit.

3. Commandes de base

Créer une ACL standard :

```
access-list <numéro> permit <ip_source> <wildcard>
```

```
access-list <numéro> deny any
```

Exemple :

```
access-list 10 permit 192.168.1.10
```

👉 Autorise uniquement l'hôte 192.168.1.10.

Tous les autres sont implicitement refusés.

4. Application d'une ACL aux lignes VTY (SSH)

Une fois l'ACL créée, on l'applique aux accès distants (VTY) :

```
line vty 0 4
```

```
access-class 10 in
```

👉 Cela signifie que seule l'IP autorisée dans l'ACL peut établir une connexion SSH.

5. Exemple de configuration complète

1. Créer une ACL pour n'autoriser que le PC d'admin (192.168.1.10) :

```
Switch(config)# access-list 10 permit 192.168.1.10
```

2. Appliquer l'ACL aux lignes VTY :

```
Switch(config)# line vty 0 4
```

```
Switch(config-line)# access-class 10 in
```

3. Vérifier :

```
Switch# show access-lists
```

```
Switch# show users
```

6. Cas pratique (Packet Tracer)

- PC1 (192.168.1.10) → doit accéder en SSH au switch.
 - PC2 (192.168.1.20) → ne doit pas pouvoir se connecter en SSH.
 - Tester avec :
 - `ssh -l admin 192.168.1.1`
 - Observer que PC2 est bloqué.
-

7. Texte à trous

1. Une ACL standard filtre uniquement sur _____.
 2. La commande pour créer une ACL standard est _____.
 3. Pour restreindre l'accès SSH à une IP, on applique l'ACL sur _____.
 4. Si aucune règle ne correspond, le trafic est _____.
-

8. Tableau de configuration à compléter

Objectif

Commande Cisco

Créer une ACL autorisant 192.168.1.10

Appliquer l'ACL aux lignes VTY

Vérifier l'ACL

Tester SSH depuis PC autorisé

9. Questions de révision

- 1. Quelle est la différence entre une ACL standard et étendue ?**
 - 2. Quelle est la règle implicite à la fin d'une ACL ?**
 - 3. Quelle commande permet d'appliquer une ACL sur l'accès SSH d'un switch ?**
 - 4. Pourquoi est-il important de restreindre l'accès SSH ?**
 - 5. Peut-on utiliser une ACL pour bloquer uniquement Telnet mais pas SSH ? Comment ?**
- ➔ **Access-list 101 deny tcp any any eq 23**
- ➔ **Access-list 101 permit ip any any**