1. Définition

Une ACL (Access Control List) est un mécanisme de filtrage du trafic réseau sur un routeur (ou un switch de niveau 3).

Elle permet de définir qui a le droit ou non de communiquer sur le réseau en fonction de différents critères. L'objectif principal est de sécuriser et contrôler le trafic entre différentes machines ou réseaux.

- Une ACL est une liste de règles qui autorise (permit) ou interdit (deny) le trafic.
- Chaque règle est lue de haut en bas dans l'ordre où elle a été configurée.
- Dès qu'une règle correspond au paquet, elle est appliquée (les suivantes sont ignorées).
- À la fin de chaque ACL, il existe une règle implicite "deny all" : tout ce qui n'est pas autorisé est bloqué.

2. Les types d'ACL

Il existe deux grandes familles :

1. ACL standard
   - Filtrent uniquement en fonction de l'adresse IP source.
   - Numéros : 1–99 et 1300–1999.
   - S'appliquent au plus près de la destination pour éviter un filtrage trop global.
2. ACL étendues
   - Filtrent selon plusieurs critères :
     - IP source et destination
     - Protocole (TCP, UDP, ICMP, etc.)
     - Ports (HTTP, SSH, FTP, etc.)
   - Numéros : 100–199 et 2000–2699.
   - S'appliquent au plus près de la source pour optimiser le trafic.

3. La syntaxe générale

ACL Standard

access-list [numéro] {permit|deny} [adresse_source] [wildcard]

- wildcard : masque inversé (0 = bit exact, 1 = bit ignoré).
- Exemple :
- access-list 1 deny 192.168.1.2 0.0.0.0
- access-list 1 permit any

ACL Étendue

access-list [numéro] {permit|deny} [protocole] [adresse_source] [wildcard] [opérateur_port] [adresse_destination] [wildcard] [opérateur_port]

- Permet de filtrer en fonction du protocole et des ports.
- Exemple :
- access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 80
- access-list 100 permit ip any any

4. Application d'une ACL sur une interface

Inbound (in) : filtre les paquets entrant sur l'interface.

Outbound (out) : filtre les paquets sortant de l'interface.

Exemple :

interface GigabitEthernet0/1
ip access-group 1 out

5. Exemples d'ACL Standard

a) Bloquer un PC spécifique

access-list 10 deny 192.168.1.10 0.0.0.0
access-list 10 permit any
interface G0/1
ip access-group 10 out

PC1 (192.168.1.10) ne peut pas sortir du réseau.

b) Autoriser uniquement un serveur

access-list 20 permit 192.168.1.100 0.0.0.0
access-list 20 deny any
interface G0/1
ip access-group 20 out

Seul le serveur 192.168.1.100 a accès au réseau.

c) Bloquer plusieurs hôtes bruyants

access-list 40 deny 192.168.1.10 0.0.0.0
access-list 40 deny 192.168.1.11 0.0.0.0
access-list 40 permit any
interface G0/1
ip access-group 40 in

PC1 et PC2 sont bloqués pour libérer la bande passante.

d) Contrôler l'accès administratif

access-list 30 permit 192.168.1.50 0.0.0.0
access-list 30 permit 192.168.1.51 0.0.0.0
access-list 30 deny any
line vty 0 4
access-class 30 in

Seuls les administrateurs (50 et 51) peuvent gérer le routeur en SSH.

6. Exemples d'ACL Étendue

a) Bloquer l'accès web (HTTP)

access-list 101 deny tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 101 permit ip any any
interface G0/1
ip access-group 101 in

Les PC du réseau ne peuvent pas aller sur Internet en HTTP.

b) Autoriser un serveur vers une base MySQL

access-list 102 permit tcp 192.168.1.100 0.0.0.0 192.168.3.200 0.0.0.0 eq 3306
access-list 102 deny tcp any any eq 3306
access-list 102 permit ip any any

Seul 192.168.1.100 accède au serveur MySQL.

c) 7.3 Bloquer les pings

access-list 103 deny icmp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 echo
access-list 103 permit ip any any

Le réseau externe ne peut pas pinguer le VLAN interne.

d) Restreindre l'accès SSH

```
access-list 104 permit tcp 192.168.1.50 0.0.0.0 192.168.1.1 0.0.0.0 eq 22
access-list 104 permit tcp 192.168.1.51 0.0.0.0 192.168.1.1 0.0.0.0 eq 22
access-list 104 deny ip any any
line vty 0 4
 access-class 104 in
```

Seuls deux administrateurs ont accès SSH.

e) Autoriser les serveurs web de la DMZ

```
access-list 105 permit tcp any 192.168.3.0 0.0.0.255 eq 80
access-list 105 permit tcp any 192.168.3.0 0.0.0.255 eq 443
access-list 105 deny ip any 192.168.3.0 0.0.0.255
access-list 105 permit ip any any
```

Les serveurs web de la DMZ sont accessibles depuis l'extérieur, mais pas les autres services.

7. Les bonnes pratiques

Il faut :

- Placer les ACL standard près de la destination.
- Placer les ACL étendues près de la source.
- Toujours ajouter un permit any si nécessaire pour éviter un blocage complet.
- Rédiger les règles de la plus spécifique à la plus générale.
- Ne pas oublier que tout ce qui n'est pas explicitement autorisé est bloqué.

Les ACL sont un outil essentiel pour :

- Sécuriser le réseau (contrôle d'accès aux ressources).
- Optimiser le trafic (éviter le trafic inutile).
- Restreindre les services sensibles (SSH, bases de données, serveurs web).
  - Les ACL standard offrent un filtrage simple basé uniquement sur l'IP source.
  - Les ACL étendues permettent un contrôle avancé en fonction de la destination, du protocole et des ports.