Filtrage du trafic réseau : Les listes d'accès (ACL)

Objectifs	☑Comprendre le fonctionnement des listes d'accès Cisco, ☑Listes standards et listes étendues, ☑Mettre en place des listes d'accès.

1) Définition :

Une liste de contrôle d'accès (Access Control List) est une collection d'instructions permettant d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :

- L'adresse IP source,
- L'adresse IP destination,
- Le numéro de port source ou destination,
- Les protocoles de couches supérieures,

D'autres paramètres (horaires par exemple).

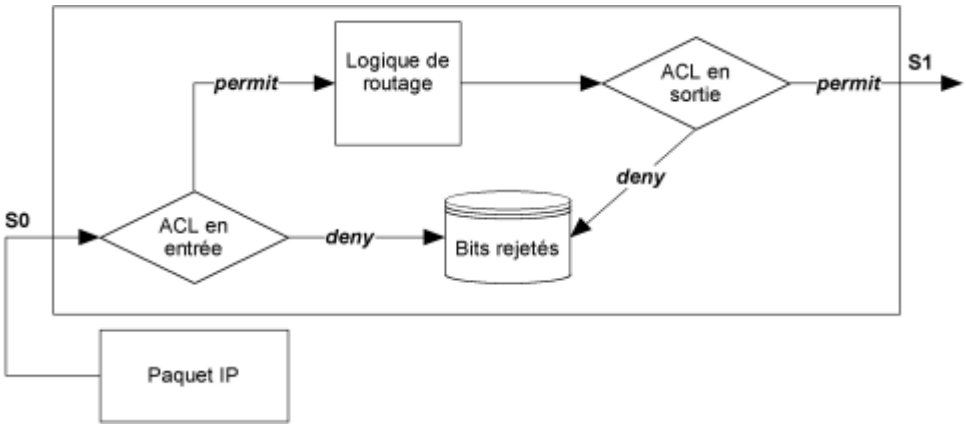
Les listes de contrôle d'accès permettent à un administrateur de mieux gérer le trafic et d'analyser des paquets particuliers.

Les ACLs sont appliquées à une interface du routeur.

2) Vérification des paquets :

Si le paquet arrivant à l'interface du routeur satisfait à une condition, il est autorisé ou refusé (suivant l'instruction) et les autres instructions ne sont pas vérifiés.

Si un paquet ne correspond à aucune instruction dans l'ACL, le paquet est jeté. Ceci est le résultat de l'instruction implicite « **deny any** » à la fin de chaque ACL.



➢ Les paquets peuvent être filtrés en entrée sur une interface avant la décision de routage.

➢ Les paquets peuvent être filtrés en sortie (avant de quitter une interface) après la décision de routage.

➢ Le mot clef « deny » permet de rejeter un paquet selon les critères précisés.

Le mot clef « permit » autorise un paquet selon les critères précisés.

Remarque : **Une instruction « deny » implicite rejette tout le trafic à la fin de chaque ACL.**

1) Création des ACL :

Pour mettre en place une liste de contrôle d'accès, il faut :

➢ Créer la liste de contrôle d'accès en mode de configuration globale,

➢ Assigner cette ACL à une interface en entrée ou en sortie,

a) Les différents types d'ACL

Il existe 3 types de liste de contrôle d'accès :

- **ACLs standards :** Les ACLs standards examinent seulement l'adresse IP source du paquet. Leurs numéros varient de 1 à 99.

- **ACLs étendues :** Les ACLs étendues permettent d'examiner les adresses IP et les ports aussi bien sources que destination, ainsi que le type de protocoles (TCP, UDP, HTTP, …). Leurs numéros varient de 100 à 199.

- **ACLs nommées :** Les ACLs étendues utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis. A la place du n° on utilise un **nom** pour identifier l'ACL.

a) Syntaxe des commandes

Listes standards :

Router(config)#**access-list** numéro-liste {**deny | permit**} adresse-source [**masque-générique**]

Listes étendues:

Access-list 100 permit IP 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 80

Router(config)#**access-list** numéro-liste {**deny | permit**} protocole adresse-source masque-source [opérateur **port**] adresse-destination masque-destination [opérateur **port**] [established]

Numéro_liste_accès : identifie la liste par un nombre compris entre 100 et 199.
Permit | deny : indique si cette entrée autorise ou refuse le trafic pour cette adresse.
Protocole : indique le type de protocole (IP, TCP, UDP, ICMP, GRP, IGRP, ...).
Source et destination : identifient l'adresse IP source et destination.
Masque_source et masque_destination : masque générique
Opérateur et opérande prennent les valeurs suivantes :

- **lt** (plus petit)
- **gt** (plus grand)
- **eq** (égal)
- **neq** (non égal)

established : autorise le trafic TCP si les paquets utilisent une connexion établie.

a) Assignation des ACLs aux interfaces

Les listes de contrôle d'accès sont affectées à une ou plusieurs interfaces et peuvent filtrer du trafic entrant ou sortant, selon la configuration. Nous verrons plus loin où placer les ACLs de façon optimale selon le type d'ACL créée.

```
Routeur(config)# int fa 0/0
Routeur(config-if)# ip access-group numéro-liste-accès { in | out }
Routeur(config-if)# end
```

b) Numéro des ACLs

Le numéro choisi pour identifier une liste de contrôle d'accès doit se trouver à l'intérieur d'une plage précise, valable pour le protocole.

Plage	Protocole
1-99 et 1300-1999	IP standard
100-199 et 2000-2699	IP étendue

Par exemple, si l'on affecte le numéro 30 à une ACL, cela induit que cette ACL sera de type standard et concernera le trafic IP.

c) Le masque générique

Un masque générique est jumelé à une adresse IP. C'est un masque de filtrage. Les bits 1 et 0 sont utilisés pour indiquer la façon de traiter les bits de l'adresse IP correspondante :

- 0 pour vérifier,
- 1 pour ne pas vérifier.

Exemple : Calculer le masque générique pour filtrer le réseau 172.16.0.0/17

Exercice 1 :

Calculer le masque générique permettant de filtrer les réseaux ou machines suivantes :

Adresse	Masque générique	Détail
192.168.0.0/24	0.0.0.255	1111 1111.1111 1111.1111 1111.0000 0000
192.168.0.0/20	0.0.15.255	1111 1111.1111 1111.1111 0000.0000 0000
10.1.0.0/16	0.0.255.255	1111 1111.1111 1111.0000 0000.0000 0000
10.0.0.0/30	0.0.0.3	1111 1111.1111 1111.1111 1111.1111 1100
172.16.0.0/15	0.1.255.255	1111 1111.1111 1110.0000 0000.0000 0000

Remarque :

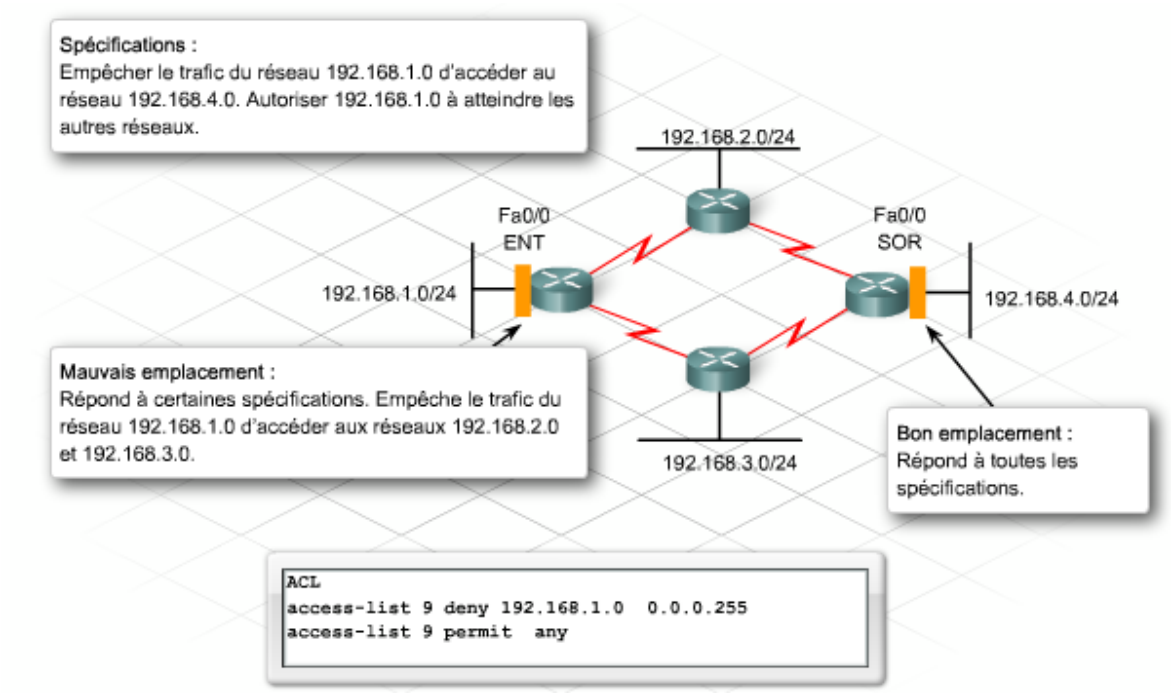
Exercice 2 :

Expliquer les commandes suivantes, en précisant le type d'ACL et la plage de machines concernées par le filtrage.

Commandes	Explications
access-list 51 permit 192.168.0.0 0.0.1.255	ACL standard n°51 qui autorise les adresses sources du réseau 192.168.0.0/23
access-list 101 permit ip 192.168.0.0 0.0.0.255 any	ACL étendue n°101 qui autorise le protocole ip pour les paquets provenant du réseau 192.168.0.0/24 vers toutes les destinations.
Access-list 107 deny ip 180.254.0.0 0.0.255.255 any	ACL étendue n°107 qui n'autorise pas le procotole ip pour les paquets provenant du réseau 180.254.0.0 0.0.0.255..255 vers toutes les destinations.
Access-list 77 deny 172.16.0.0 0.0.0.1	ACL standard n°77 qui n'autorise pas les paquets du réseau source 172.16.0.0 0.0.0.1
access-list 110 deny icmp any 192.168.1.254 0.0.0.0	ACL étendue n°110 qui n'autorise pas le protocole icmp vers toutes les adresses sources sur l'adresse 192.168.1.254 0.0.0.0
access-list 100 permit ip any host 10.0.0.1 eq 21	ACL étendue n°100 qui autorise le protocole ip de toutes les sources vers le poste 10.0.0.1 sur le port (ftp)
access-list 2000 permit ip 172.16.0.0 0.1.255.255 host 192.168.0.1 eq 80	ACL étendue n°2000 qui autorise les requêtes http provenant du réseau 172.16.0.0 0.1.255.255 vers le serveur 192.168.0.1

f) Où placer les ACL ?

ACL standard :



ACL étendue :