# Les ACL

Les ACL (Access Control List) ont pour but de mettre ne place un filtrage sur un switch (3) ou sur un routeur. Une ACL est constituée de 1 ou plusieurs ACE (règles). Elles s'appliquent sur une interface particulière, et permettent de gérer le flux de trafic en entrée ou en sortie ainsi qu'en autorisation de transit ou en interdiction.

Une ACL est donc un ensemble séquentiel d'instructions d'autorisation ou de refus qui s'appliquent aux adresses IP ou aux protocoles supérieurs. Une ACL est une suite de commande iOS qui s'applique au routeur et qui indique si celui-ci va laisser passer ou non certains paquets (assimilable à iptables) en fonction des informations contenues dans l'en-tête de ces paquets.

Une ACL est donc constituée d'une ou plusieurs ACE. Une ACE est une commande iOS commençant par ***access-list*** ou ***ip access-list*** qui va définir les règles d'accès.


Tout comme iptables, le ACL vont pouvoir filtrer au niveau 3 : IP source, IP destination, Type de message (ICMP) mais aussi au niveau 4 : TCP ou UDP, port source et port de destination.

La dernière instruction d'une ACL est implicite et est automatiquement ajoutée : c'est une instruction DENY (on bloque tout). Une ACL ne contenant aucune ACE bloquerait donc tout le trafic.

Une ACL contenant plusieurs ACE se termine donc par « Tout le reste est bloqué ». L'ordre est donc important et on ira du plus ciblé au plus générique.

On distingue 2 types d'ACL :  ACL standard et ACL étendue

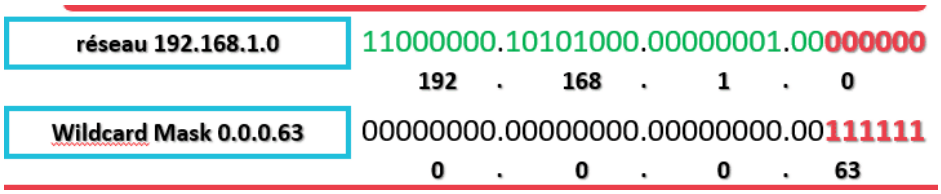
## Préambule

Pour utiliser certains protocoles ou bien certaines fonctionnalités du routeur, on fait parfois appel aux « wildcard masks », qui se traduit par « masques inversés ». Cela permet d'identifier un sous-réseau ou une plage d'adresses IP. Les masques inversés servent à identifier les adresses qui correspondent ou non à certains critères, c'est-à-dire en fonction d'un range d'IP.

Quand on doit appliquer un masque inversé, il faut garder à l'esprit que:

- Un bit avec une valeur de « 0 » vérifie la correspondance de l'adresse.
- Un bit avec une valeur de « 1 » ignore la valeur correspondante de l'adresse.

Par exemple :




Nous avons le réseau 192.168.1.0 avec un masque inversé en 3 fois « 0 ».63, ce qui correspond à un /26.

Pour calculer rapidement le masque inversé (Wildcard Mask), le plus simple est de faire une simple soustraction de 4 fois « 255 » par le masque normal qu'on souhaite convertir en inversé.

## Les ACL Standards

Une ACL Standard peut être utilisé uniquement pour autoriser ou bloquer le trafic des adresses IPv4 sources. La destination du paquet et les ports concernés ne sont pas évalués. C'est une ACL simple à mettre en place et qui s'appliquera de préférence en sortie d'interface.

Syntaxe : **(config)# access-list number {permit|deny} {host|source source-wildcard|any}**

Le numéro d'ACL pour une ACL standard sera compris entre 1 et 99 ou entre 1300 et 1999

Exemple 1 :

**access-list 10 permit 192.168.1.0 0.0.0.255**

On autorisera donc le trafic en provenance du réseau 192.168.1.0/24 et on interdit le reste (pensez à la dernière ACE implicite)

Exemple 2 :

access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 deny host 192.168.2.10
access-list 1 permit any

Ici on interdire l'accès seulement à tous les membres du réseau 192.168.1.0/24 ainsi qu'à l'hôte 192.168.2.10.

## Les ACL étendues

Grâce aux ACL étendues nous allons pouvoir créer des listes plus précises en fonction des adresses sources, des adresses de destination, des protocoles ou des numéros de port. Cisco préconise que les ACL étendues soient activées sur l'interface au plus près de la source.

Syntaxe :
**(config)# access-list number {deny|permit} protocole source masque-source [opérateur [port]] destination masque-destination [opérateur [port [established][log]]]**

- Le numéro d'ACL pour une ACL étendue sera compris entre 100 et 199 ou entre 2000 et 2699

- Les opérateurs sont : eq (égal) neq (différent) gt (+grand) lt (+petit)

Exemple 1 :

**access-list 101 deny ip any host 192.168.2.10**

Cette ACL interdit tout paquet à destination de l'hôte 192.168.2.10

Exemple 2 :

**access-list 101 deny tcp any gt 1023 host 192.168.2.10 eq 23**

Cette ACL interdit tout segment TCP de port source supérieur à 1023 et à destination du port 23 de l'hôte 192.168.2.10

Exemple 3 :

**access-list 101 deny tcp 192.168.10.0 0.0.0.255 any eq http**

Cette ACL interdit tout segment TCP à destination du port 80 et en provenance du réseau 192.168.10.0/24

**Les ACL nommées**

Il est possible de définir une description d'ACL pour plus de clarté :
**access-list 101 remark Description de l'ACL**

Les ACL numérotées sont complexes à administrer dès que leur nombre est important. De plus, il est impossible de modifier une ACE. Pour cela, il faudra complètement supprimer l'ACL et la recréer. Il existe un moyen d'éviter ceci c'est de nommer ses ACL :
**(config)# ip access-list extended nom**
**(config-ext-nacl)# {deny|permit} protocole source masque …**
Pour ajouter une règle, il suffit d'utiliser la même syntaxe que les ACL numérotée sans « access-list number »
La commande pour supprimer une ACL : no

**Appliquer une ACL à une interface**
Afin d'appliquer notre ACL (quel qu'elle soit) à une interface, il suffit de se mettre en mode configuration de cette interface et d'y appliquer l'ACL selon la syntaxe suivante :

**(config)# interface iface_name**
**(config-if)# ip access-group {number|name} {in|out}**

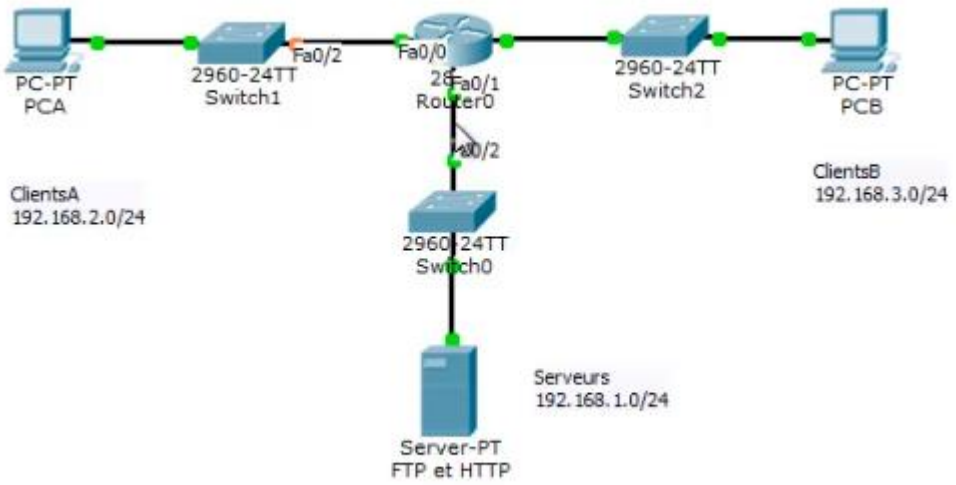
# Exercices

Que fait cette ACL ?

```
Switch# configure terminal
Switch(config)# access-list 1 deny 172.16.3.10 0.0.0.0
Switch(config)# access-list 1 permit 0.0.0.0 255.255.255.255
Switch(config)# interface fastethernet0
Switch(config-if)# ip address 172.16.1.1 255.255.255.0
Switch(config-if)# ip access-group 1 out
```

Même question

```
access-list 101 deny tcp 192.168.1.0 0.0.0.255 gt 1024 109.205.0.0
0.0.255.255 eq 443
```




On veut interdire les postes du réseau ClientsA de communiquer avec le réseau Serveurs.

- Quel type d'ACL va-t-on utiliser ?

- Ecrivez cette ACL

- Donnez les commandes qui permettent de l'appliquer au routeur

On veut interdire les postes du réseau ClientsB d'aller sur le serveur web.

- Quel type d'ACL va-t-on utiliser ?

- Ecrivez cette ACL

- Donnez les commandes qui permettent de l'appliquer au routeur

Exercice sur Packet Tracer :

1. A partir du fichier « ACL Standard Exo.pkt »

Mettez en place les ACL permettant le cahier des charges suivant :

- Le réseau des PC peut communiquer avec le réseau des serveurs.
- Le réseau des portables ne peut pas communiquer avec le réseau des serveurs sauf le poste 192.168.2.1.
- Le réseau des portables pourra communiquer avec le réseau des PC.
- Le réseau des PC pourra communiquer avec le réseau des portables.

Effectuez les tests de bon fonctionnement

2. A partir du fichier « ACL étendues Exo.pkt »

Mettes en place les ACL permettant le cahier des charges suivant :

- Le réseau des PC a accès en HTTPS seulement au site WEB 172.16.0.1 en tapant le nom www.tssr.com via un navigateur
- Le réseau des portables a accès au DNS et seulement en http au site
- Le portable 192.168.2.100 n'a pas accès au réseau 172.16.0.0/16
- Les portables ne peuvent pas effectuer un ping vers le réseau des PC
- Seul le PC 192.168.1.1 peut accéder à la configuration du routeur en SSH

Effectuez les tests de bon fonctionnement