LES ACL

C'est quoi une ACL ?

Une ACL (Access Control List) est une liste de règles permettant de filtrer (autoriser ou bloquer) du trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole, etc.).

Donc, avec une ACL on peut soit autoriser du trafic (permit), soit le bloquer (deny).

Une ACL est appliquée à une interface. Le filtrage peut se faire en entrée de l'interface (Inbound traffic) ou en sortie de celle-ci (Outbound traffic).

Lorsque le routeur reçoit une trame, il la compare aux règles de l'ACL de manière séquentielle (dans l'ordre). Dès qu'une règle correspond à la trame, l'action définie est appliquée, le reste de l'ACL n'est pas analysé.

Toutes les trames ne correspondant à aucune règle d'une ACL sont rejetées.

Il existe plusieurs types d'ACL. Notamment les ACL simples (qui permettent de mettre en place des règles de filtrage en fonction des adresses IP sources) et les ACL étendues (qui permettent de mettre en place des règles de filtrage en fonction des adresses IP sources, des adresses IP de destination, des protocoles, des ports sources ou des ports de destinations).

ACL simple :

Avec les ACL simples, le routeur regarde les IP source des trames reçues et applique les règles qui ont été configurées.

Format d'une ACL simple :

Router(config) # access list [1-99] [permit ou deny] [source address] [source mask]

- **[1-99] : numéro de l'ACL entre 1 et 99 pour une ACL standard**
- **[permit ou deny] : autorise ou bloque la trame**
- **[source address] : IP source**
- **[source mask] : masque générique, c'est l'inverse d'un masque de sous-réseau habituel.**

On peut, dans l'ACL, utiliser le mot host pour désigner un hôte spécifique. Pour qu'une règle s'applique à toutes les IP, il est possible d'utiliser le mot any.

Dans une ACL standard Cisco, il existe également une règle implicite "deny any" par défaut. Cela signifie que si aucune règle permit explicite ne correspond au trafic, ce dernier sera automatiquement bloqué.

ACL étendue

Une ACL étendue s'intéresse à l'IP source mais aussi à l'IP de destination ainsi qu'aux ports (source et dest) et au protocole (TCP, UDP, ICMP).

Format d'une ACL étendue :

Router(config) # access-list [100-199] [permit ou deny] [protocol] [source address] [source mask][destination address]

[destination mask] [operator operand]

- **[100-199] : numéro de l'ACL entre 100 et 199 pour une ACL étendue**
- **[permit ou deny] : autorise ou bloque la trame**
- **[source address] : IP source**
- **[source mask] : masque générique, c'est l'inverse d'un masque de sous-réseau habituel.**
- **[destination address] : IP de destination**
- **[destination mask] : masque générique, c'est l'inverse d'un masque de sous-réseau habituel.**
- **[operator operand] : opérateur suivi (eq=equal, gt=greater than)**

Router(config) # access-list 101 deny icmp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 Router(config) # access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80 Router(config) # access-list 101 permit udp 192.168.1.0 0.0.0.255 any eq 53 Router(config) # access-list 101 deny ip any any	Liste de règles (ACL n°101)
Router(config) # interface Gi0/0 Router(config-if) #ip access-group 101 in	Application de l'ACL n°101 sur l'interface de sortie Gi0/0

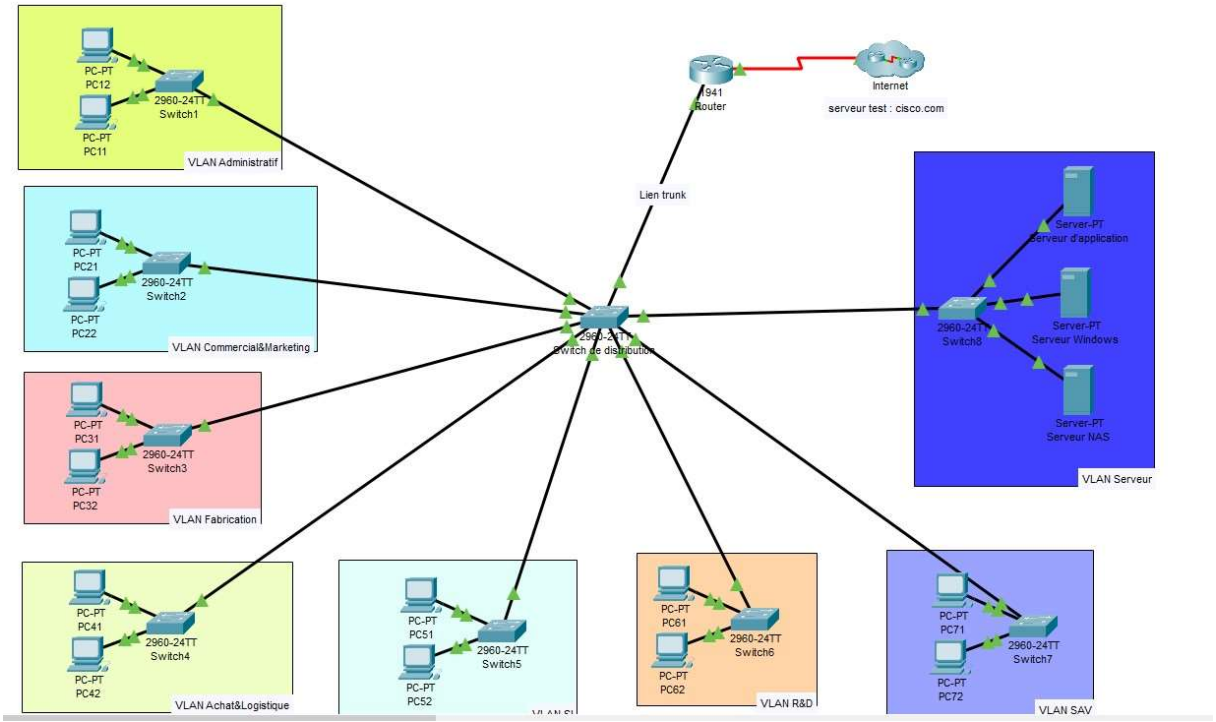
L'ACL n°101 interdit les requêtes ICMP (ping) allant du LAN1 au LAN2. Elle autorise les requêtes à destination du port 80 en TCP et les requêtes UDP avec le port de destination 53. Elle est appliquée à l'entrée de l'interface Gi0/0. La dernière règle interdit tout le trafic par défaut.

Dans une ACL étendue Cisco, tout le trafic est implicitement bloqué par défaut. Cela signifie que, si vous configurez une ACL étendue sans ajouter de règle explicite permit, tous les paquets non correspondants aux règles définies seront automatiquement refusés en fin de liste.

Il est possible de créer une ACL nommée, c'est-à-dire de lui donner un nom au lieu d'un numéro.

ACL standard	ACL étendue
Router(config)#ip access-list standard nomACLStd Router(config-std-nacl)#permit 192.168.0.0 0.0.0.255 Router(config-std-nacl)#exit	Router(config)#ip access-list extended nomACLextend Router(config-ext-nacl)#permit tcp any host 192.168.1.100 eq 80 Router(config-ext-nacl)#permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100 Router(config-ext-nacl)#exit

Exemples :



Consigne : Configurez les ACL permettant ainsi de filtrer les communications sur le routeur.

Vous devez configurer une ACL qui gère l'accès vers internet puis, vous devez la positionner sur l'interface de sortie du routeur.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny ip host 172.16.11.107 any
Router(config)#access-list 101 deny ip host 172.16.11.108 any
Router(config)#access-list 101 deny ip host 172.16.11.109 any
Router(config)#access-list 101 permit ip any any
Router(config)#interface Serial0/0/0
Router(config-if)#ip access-group 101 out
Router(config-if)#
```

Sur le routeur afin de filtrer les communications il faut intégrer cette suite de commande dans le CLI. Cette suite de commande intègre les 3 serveurs du VLAN Serveur dans l'ACL numéro 101 afin de leurs bloquer la communication en sortie avec Internet sur l'interface Serial0/0/0.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	Serve...	Server0	ICMP		0.000	N	0	(edit)	

Consigne : Configurez l'ACL permettant au PC-PT PC51 de communiquer :

- Avec le PC-PT PC61 du VLAN R&D et interdire le PC-PT PC62

- Avec le PC-PT PC71 du VLAN SAV et interdire le PC-PT PC72.

Voilà actuellement le statut de chaque communication :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC51	PC61	ICMP		0.000	N	0	(edit)	
	Failed	PC51	PC62	ICMP		0.000	N	1	(edit)	
	Failed	PC51	PC71	ICMP		0.000	N	2	(edit)	
	Failed	PC51	PC72	ICMP		0.000	N	3	(edit)	

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list 102 permit ip host 172.16.11.114 host 172.16.11.50
Switch(config)#access-list 102 deny ip host 172.16.11.114 host 172.16.11.51
Switch(config)#access-list 102 permit ip host 172.16.11.114 host 172.16.11.82
Switch(config)#access-list 102 deny ip host 172.16.11.114 host 172.16.11.83
Switch(config)#access-list 102 permit ip any any
Switch(config)#interface FastEthernet0/3
Switch(config-if)#ip access-group 102 in
                  ^
% Invalid input detected at '^' marker.

Switch(config-if)#
```

Ce que ça fait :

- On crée un ACL n°102 sur notre Switch qui autorise PC51 (172.16.11.114) à communiquer avec (172.16.11.50 (PC61) et 172.16.11.82 (PC71)). Bloque la communication avec (172.16.11.51 (PC62) et 172.16.11.83 (PC72)).

- Autorise tout le reste avec permit ip any any pour éviter de bloquer d'autres services.

- L'ACL est appliquée uniquement sur le port FastEthernet0/3, donc elle ne touche que PC51, pas PC52 ni le reste du VLAN.

Mais une erreur ce produit : % Invalid input detected at '^' marker.

Cela signifie que notre switch ne supporte pas la commande ip access-group sur une interface physique même avec un numéro d'ACL, cette commande ne passe pas sur ce modèle.

⚠ Les switchs Layer 2 (comme le 2960) ne supportent pas les ACL IP standard ou étendues sur les ports physiques — seulement sur les interfaces VLAN (SVI) pour l'administration, ou bien via des Port ACL avec une autre syntaxe.

La solution serait d'appliquer l'ACL sur tout le VLAN du PC51 (SVI) par exemple :

Switch(config)# interface vlan 50

Switch(config-if)# ip access-group 102 in

Switch(config-if)# exit

- Cela va filtrer tout le trafic entrant dans le VLAN 11 depuis l'extérieur.
- Cela filtrera donc tous les PC de ce VLAN, pas seulement PC51.
- C'est une solution globale par VLAN, pas ciblée.

Question/Réponse :

Question 1 :
Sur un switch 2960, peux-tu appliquer une ACL IP directement sur un port physique ? (oui / non)

Non

Question 2 :
Sur un switch 2960, où doit-on appliquer une ACL IP pour filtrer le trafic inter-VLAN ?

Sur un switch 2960 il n'est pas possible d'appliquer une ACL IP directement sur un port physique il faut l'appliquer sur l'interface VLAN.

Question 3 :
Si tu veux bloquer ce que PC1 envoie, tu appliques l'ACL sur l'interface VLAN 11 en in ou en out ?

Pour bloquer ce que PC1 envoie on applique l'ACL en in en out signifierait que les paquets sont déjà passer à l'extérieur du VLAN donc non filtré.

Question 4 :
Si tu veux bloquer ce que PC1 reçoit, tu appliques l'ACL sur l'interface VLAN 11 en in ou en out ?

Ici c'est out du coup le filtrage prendra effet avant d'entrer dans le VLAN (meme si le switch comprenant l'ACL se trouve dans le VLAN 11, les paquets n'atteindrons pas les appareils.

Question 5 :
Dans une ACL Cisco, s'il n'y a aucune ligne qui correspond au trafic, que se passe-t-il à la fin de la liste ?

S'il n'y a pas de correspondance, un deny implicite à la fin de l'ACL bloque tout le trafic par défaut.

Question 6 :
Quelle ligne est importante à mettre à la fin de ton ACL si tu veux autoriser tout ce qui n'est pas explicitement bloqué ?

access-list 102 permit ip any any

Question 7 :
Si tu veux bloquer le trafic de PC2 vers PC1, quelle IP doit être en source et quelle doit être en destination dans ta règle deny ?

L'ip du PC2 doit être la source et PC1, celle de la destination voici la syntaxe :
access-list 102 deny ip host <PC2> host <PC1>

Question 8 :
Si tu veux bloquer ce que PC1 reçoit de PC2, tu dois appliquer cette ACL sur l'interface VLAN 11 en in ou en out ?

Out

Question 9 :
Si tu veux bloquer ce que PC1 envoie vers PC2, tu dois appliquer l'ACL sur l'interface VLAN 11 en in ou en out ?

In

Question 10 :
Quelle commande permet de vérifier qu'une ACL est bien appliquée sur une interface VLAN et de voir si elle est en in ou out ?

La commande est :

show ip interface vlan 11

Elle affiche :

- **L'interface VLAN**
- **S'il y a une ACL appliquée**
- **Et dans quel sens (in ou out)**