

Configuration ACL



Ismaïl BOUSSAHA

BTS SIO SISR

AURLOM

Sommaire

1. Présentation ACL

A. C'est quoi une ACL ?

B. Dans quel contexte en utiliser

2. Prérequis

A. Matériels nécessaires

3. Installation

A. Configuration Switch

B. Configuration ROUTER

C. Adressage IP PC

D. Mise en place de l'ACL

4. Test

A. Conclusion

1. Présentation ACL

A. C'est quoi une ACL ?

Une **ACL (Access Control List)** est un ensemble de règles utilisées pour contrôler le trafic réseau. Elle permet de filtrer les paquets IP en fonction de critères tels que l'adresse IP source ou destination, le protocole, ou encore le port. Les ACL sont utilisées dans les équipements réseau comme les routeurs ou les commutateurs de niveau 3.

B. Dans quel contexte l'utiliser

Les ACL sont utilisées :

- Pour **limiter l'accès** entre des VLANs.
- Pour **sécuriser l'accès** à certains services.
- Pour **restreindre la communication** entre des hôtes selon des règles précises.
- Pour **contrôler la bande passante** dans certains cas.

2. Prérequis

A. Matériels nécessaires

Pour réaliser cette mise en œuvre, voici les éléments matériels et logiciels requis :

1. *Routeur*

- **Modèle recommandé** : Cisco 2811 (ou équivalent)
- **Rôle** : Fournit le routage inter-VLAN via des sous-interfaces configurées avec 802.1Q (encapsulation dot1Q).
- **Interface utilisée** : GigabitEthernet 0/0 (trunk entre le routeur et le switch).

2. *Commutateur (Switch)*

- **Modèle recommandé** : Cisco Catalyst 2950 / 2960
- **Rôle** : Création de VLANs et gestion du trafic réseau entre les postes de travail.
- **Ports utilisés** :
 - **Fa0/1** pour PC2 (VLAN 10)
 - **Fa0/2** pour PC3 (VLAN 20)

- **Fa0/24** pour la liaison trunk avec le routeur

3. Postes de travail (PC)

- **Nombre : 2**
- **Configuration :**
 - **PC2** : Assigné au VLAN 10, IP statique :
192.168.10.2 /24, passerelle :
192.168.10.1
 - **PC3** : Assigné au VLAN 20, IP statique :
192.168.20.2 /24, passerelle :
192.168.20.1

4. Logiciel de simulation

- **Cisco Packet Tracer** (version 8.0 ou supérieure recommandée)
- **Rôle** : Simulation du réseau et vérification du bon fonctionnement de l'ACL

3. Installation

A. Configuration Switch

Création VLAN 10 et 20 :

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
```

Affectation des ports aux VLANs :

```
Switch(config)#int fa0/1
Switch(config-if)#sw mode acc
Switch(config-if)#sw acc vlan 10
```

```
Switch(config)#int fa0/2
Switch(config-if)#sw mode acc
Switch(config-if)#sw acc vlan 20
```

Configuration du port en trunk vers le routeur :

```
Switch(config)#int fa0/24
Switch(config-if)#sw mode trunk
```

B. Configuration Router

Sous-interface pour inter-VLAN :

```
Router(config)#int gig0/0.10
Router(config-subif)#enc dot1q 10
Router(config-subif)#ip add 192.168.10.254 255.255.255.0
```

```
Router(config)#int gig0/0.20
Router(config-subif)#enc dot1q 20
Router(config-subif)#ip add 192.168.20.254 255.255.255.0
```

C. Adressage IP PC

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:BAFF:FE0C:C225
    IPv6 Address . . . . . : ::
    IPv4 Address . . . . . : 192.168.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : ::
                                192.168.10.254
```

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:97FF:FE59:276E
    IPv6 Address . . . . . : ::
    IPv4 Address . . . . . : 192.168.20.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : ::
                                192.168.20.254
```

D. Mise en place de l'ACL

Objectif : interdire l'accès de PC2 (VLAN 10) à PC3 (VLAN 20), mais autoriser l'inverse.

```
Router(config)#access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
```

Application de l'ACL sur l'interface de sortie :

```
Router(config)#int gig0/0.10
Router(config-subif)#ip access-group 100 out
```

4. Test

Test ping de PC2 vers PC3

```
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.10.254: Destination host unreachable.
Reply from 192.168.10.254: Destination host unreachable.
Reply from 192.168.10.254: Destination host unreachable.
Reply from 192.168.10.254: Destination host unreachable.

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Conclusion :

Cette mise en œuvre démontre comment une ACL permet de contrôler la communication entre différents VLANs.

L'utilisation des ACL est essentielle dans un environnement réseau pour des raisons de sécurité, de performance et de gestion du trafic. Dans cet exemple, nous avons mis en place une ACL qui bloque le trafic dans un sens tout en l'autorisant dans l'autre, illustrant la souplesse et la puissance des ACL dans un réseau bien segmenté.

