Routage inter-vlan et Filtrage

Chapitre 6

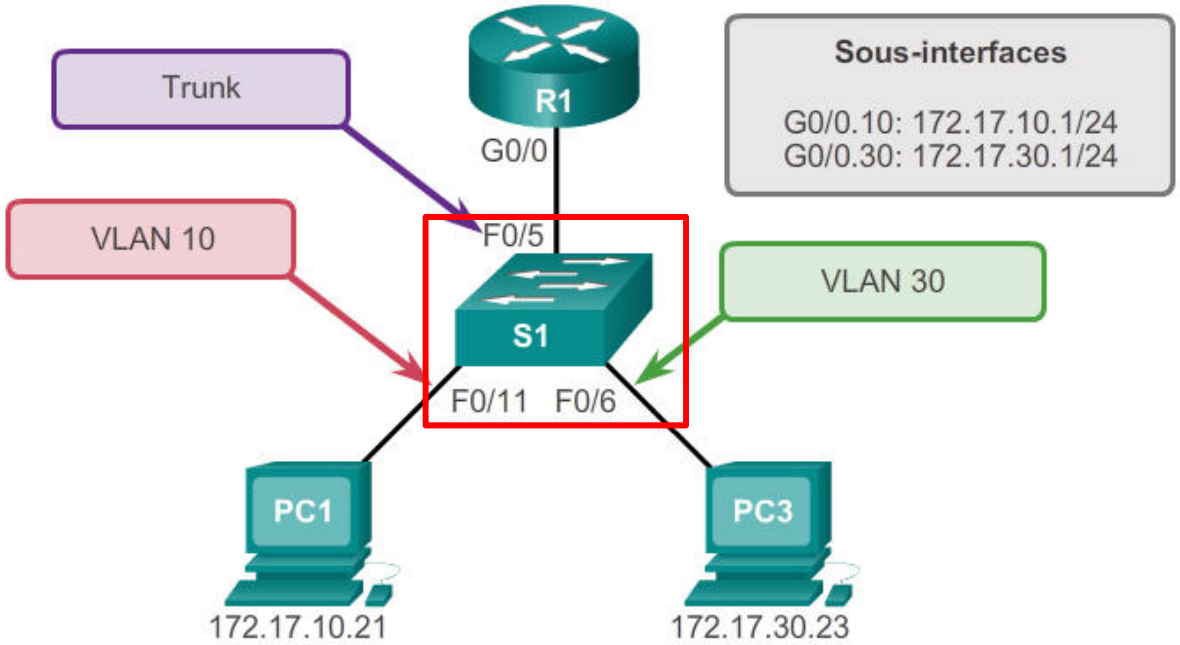
Plan

1. Routage inter-Vlan:
    1. configuration de commutateur
    2. configuration du routeur
2. Filtrage avec ACL
    1. les ACL
    2. filtrage à base d'adresses IP
    3. filtrage à base de numéro de port

Routage inter-vlan et Filtrage

1. Routage inter-Vlan

1.1. configuration de commutateur



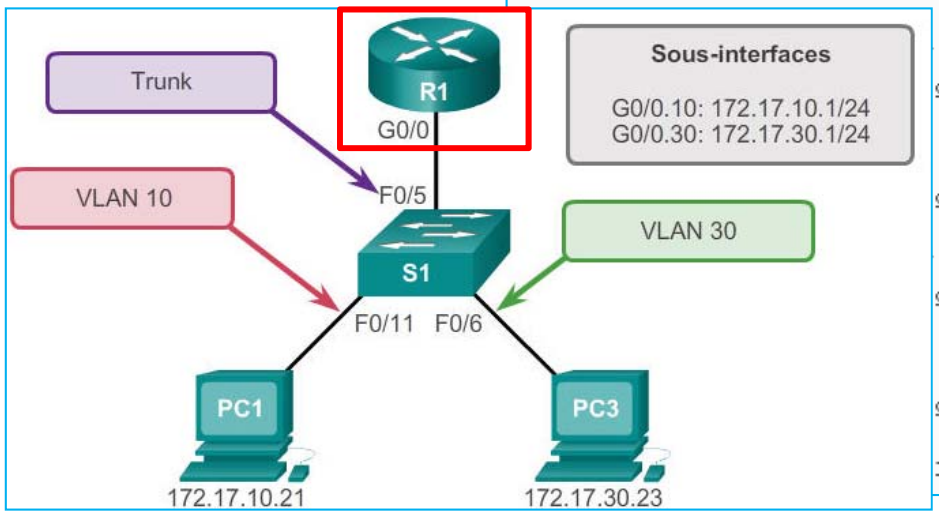

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

Routage inter-vlan et Filtrage

1. Routage inter-Vlan

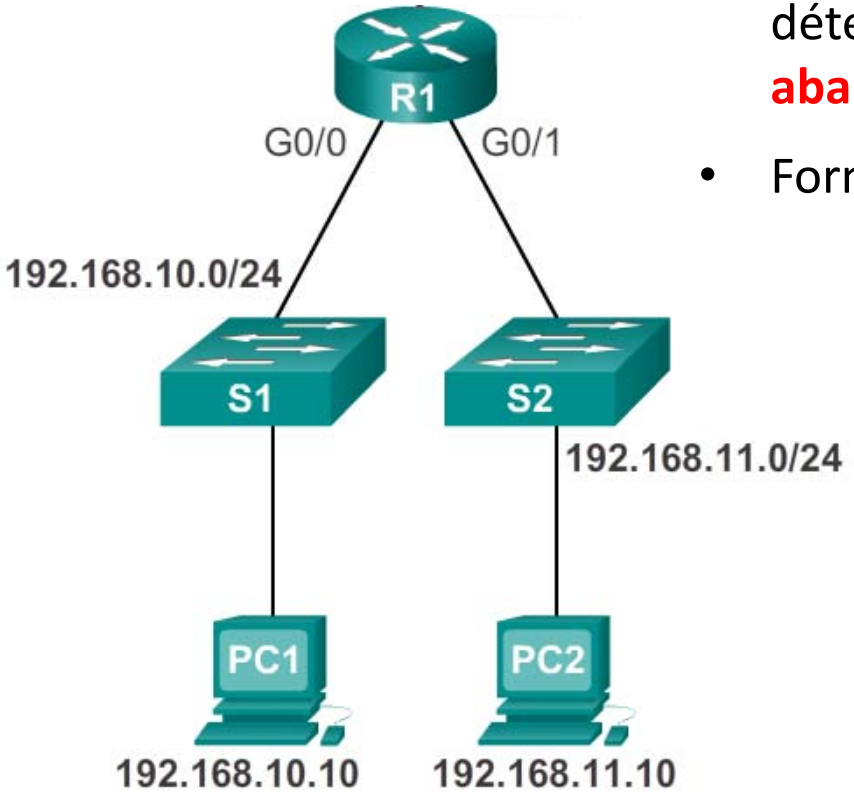
1.1. configuration du routeur

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,

%LINK-3-UPDOWN: Interface GigabitEthernet0/0,

%LINEPROTO-5-UPDOWN: Line protocol on

%LINK-3-UPDOWN: Interface GigabitEthernet0/0,

%LINEPROTO-5-UPDOWN: Line protocol on
rnet0/0, changed state to up
```



2. Filtrage avec ACL

2.1. les ACL



- Une ACL est une série de commandes qui déterminent si un routeur **achemine** ou **abandonne** les paquets **entrants** ou **sortants**
- Format générale d'une entrée ACL:

  REGLE PROTOCOLE CORRESPONDANCE

  REGLE :
  PERMIT: autoriser le trafic
  DENY: refuser le trafic

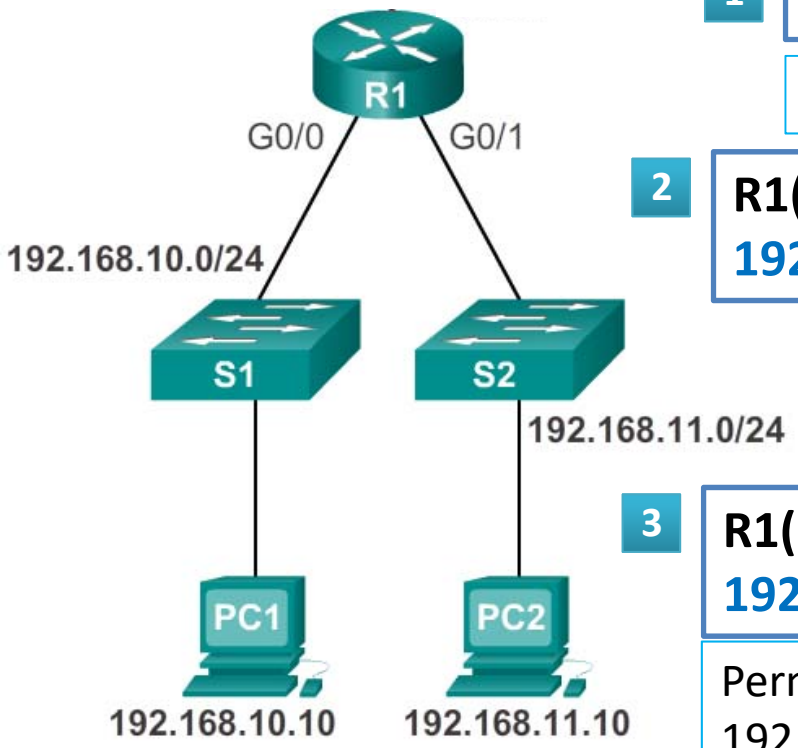
  PROTOCOLE: IP, ICMP, TCP, UDP

  CORRESPONDANCE: comparer les adresses IP source et adresses IP de destination
- Une ACL est appliquée au niveau **des ports**

2. Filtrage avec ACL

2.2. filtrage à base d'adresses IP

Exemple1: Empêcher les éléments du réseau 192.168.10.0/ d'accéder au réseau 192.168.11.0/24



1 **R1(config)# ip access-list extended NO-ACCESS**

Crée une ACL étendu nommée NO-ACCESS

2 **R1(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 192.168.11.0 0.0.0.255**

Empêcher les éléments du réseau 192.168.10.0/24 d'accéder au réseau 192.168.11.0/24

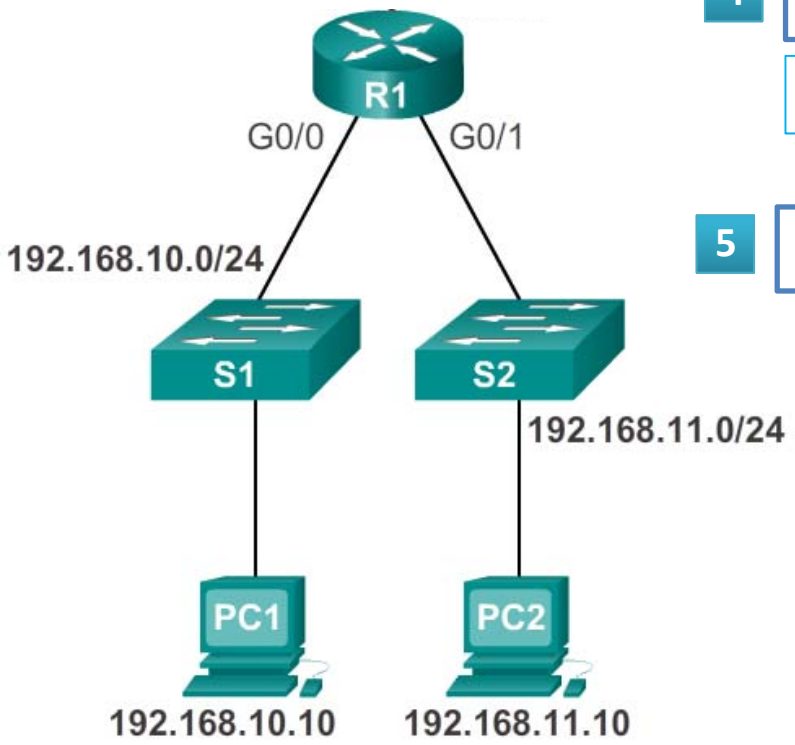
3 **R1(config-ext-nacl)# permit ip any 192.168.11.0 0.0.0.255**

Permettre les autres réseaux d'accéder au réseau 192.168.11.0/24. any remplace 0.0.0.0 255.255.255.0

2. Filtrage avec ACL

2.2. filtrage à base d'adresses IP

Exemple1: Empêcher les éléments du réseau 192.168.10.0/ d'accéder au réseau 192.168.11.0/24



4 **R1(config)# interface g0/1**

L'ACL NO-ACCESS sera appliquée à l'interface g0/1

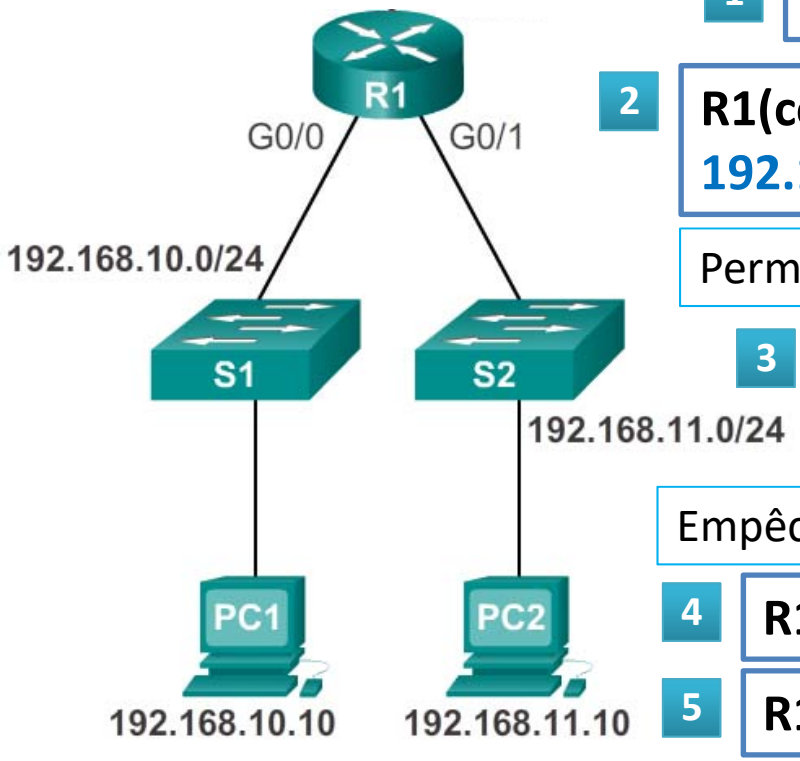
5 **R1(config-if)# ip access-group NO-ACCESS out**

Appliquer l'ACL NO-ACCESS sur le trafic sortant du routeur R1 via le port g0/1 vers la destination 192.168.11.0/24

2. Filtrage avec ACL

2.2. filtrage à base d'adresses IP

Exemple2: Empêcher tout le monde d'accéder au réseau 192.168.11.0/24 à l'exception de l'hôte 209.115.30.1



1 **R1(config)# ip access-list extended NO-ACCESS**

2 **R1(config-ext-nacl)# permit ip host 209.115.30.1 192.168.11.0 0.0.0.255**

Permettre l'hôte 209.115.30.1 d'avoir un accès

3 **R1(config-ext-nacl)# deny ip any 192.168.11.0 0.0.0.255**

Empêcher le reste d'accéder au réseau 192.168.11.0/24

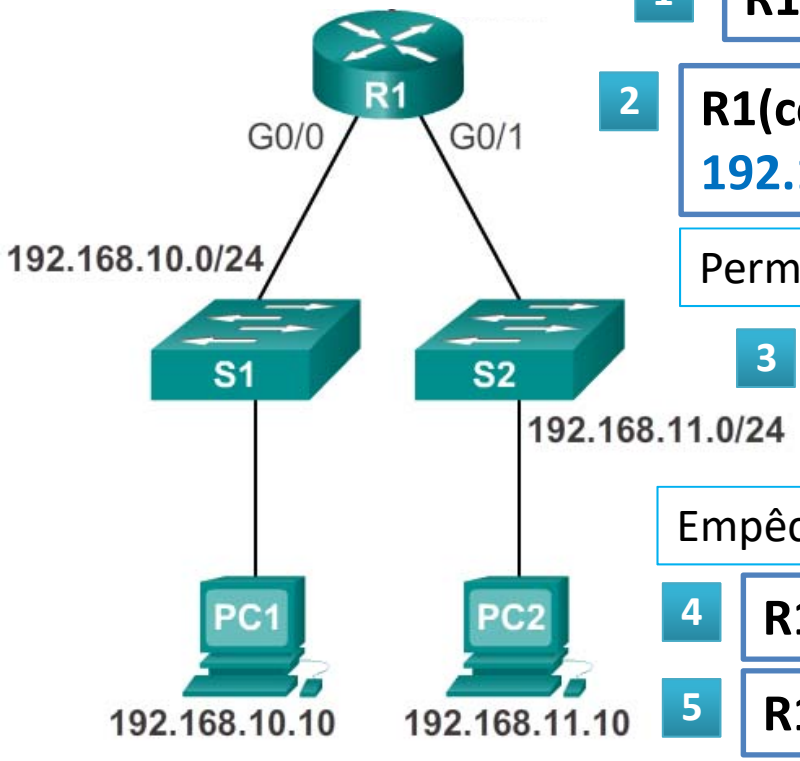
4 **R1(config)# interface g0/1**

5 **R1(config-if)# ip access-group NO-ACCESS out**

2. Filtrage avec ACL

2.3. filtrage à base de numéro de port

Exemple3: ne permettre que l'accès au service web (port 80) de l'hôte 192.168.11.10



1 **R1(config)# ip access-list extended WEB-ACCESS**

2 **R1(config-ext-nacl)# permit tcp any host 192.168.11.10 eq 80**

Permettre l'accès au service web de l'hôte 192.168.11.10

3 **R1(config-ext-nacl)# deny ip any host 192.168.11.10**

Empêcher l'accès à tout autre service

4 **R1(config)# interface g0/1**

5 **R1(config-if)# ip access-group WEB-ACCESS out**

Fin