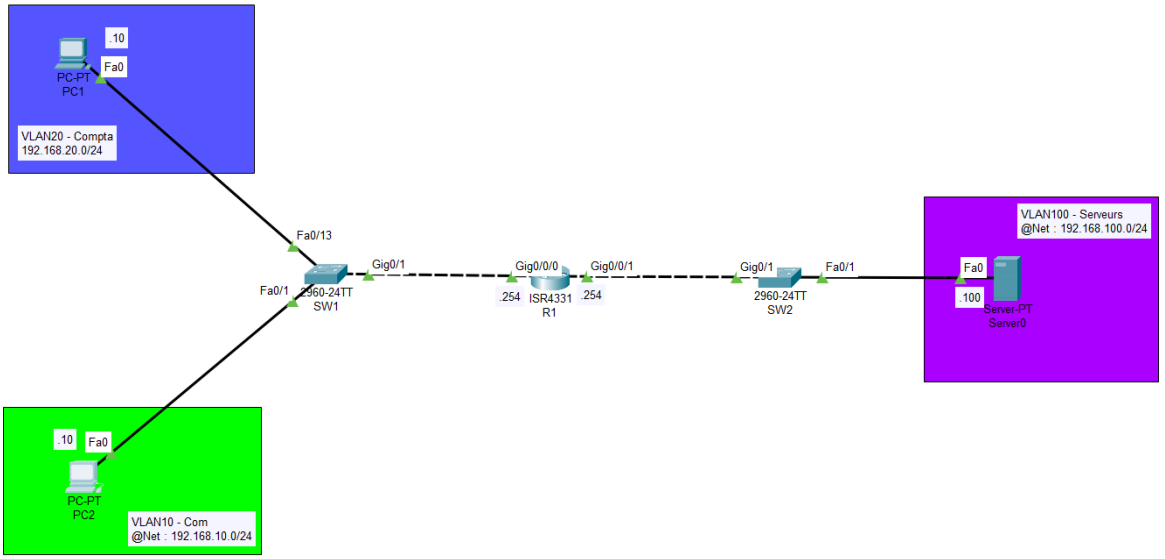
Routage Inter-VLANs & ACL

Auteur : Jules QUENTIN
Date et version : 10/02/2025 v1



Machine	@IP/Netmask	VLAN
PC1	192.168.20.10/24	20
PC2	192.168.10.10/24	10
Server	192.168.100.100/24	100
R1	.254 (de chaque réseau)	

Introduction :

Le principe de la segmentation par VLAN est de renforcer l'étanchéité de notre réseau en nécessitant l'utilisation d'une passerelle pour communiquer entre deux VLAN différents.
A cela nous rajoutons le principe des ACL (Access Control List) qui permettent d'ériger des règles au sein de notre système (autorisation/refus d'accès à un réseau, un hôte, un protocole…)

Configuration des interfaces & VLAN

On commence par configurer les interfaces sur notre routeur qui serviront de passerelle pour nos VLAN ainsi que créer nos VLAN sur nos commutateurs

Sur R1 :

```
int gi0/0/0.10
encapsulation dot1Q 10
ip address 192.168.10.254 255.255.255.0

int gi0/0/0.20
encapsulation dot1Q 20
ip address 192.168.20.254 255.255.255.0

int gi0/0/1.100
encapsulation dot1Q 100
ip address 192.168.100.254 255.255.255.0
```

Sur SW1 :

```
int range fa0/1-12
      switchport mode access
      switchport access vlan 10

int range fa0/13-24
      switchport mode access
      switchport access vlan 20
```

Sur SW2 :

```
int fa0/1
      switchport mode access
      switchport access vlan 100
```

Les VLANs sont automatiquement créés s' ils sont inexistants lors de l'attribution sur un port. On peut accéder à la configuration de celui-ci pour changer son nom par exemple via :

```
vlan [VLANID]
      name [TEXT]
```

Configuration des ACL

Maintenant que la communication Inter-VLANs est fonctionnelle on peut instaurer des règles de circulation sur notre système via les Access Control List.

Celles-ci peuvent être soit “standard” correspondant à une ACL numérotée de 1 à 99, elles permettent d’autoriser ou refuser qu’un réseau ou un hôte ne puisse passer le routeur sur lequel l’ACL est instaurée.
Ou bien les ACL peuvent être “étendues” et dans ce cas là correspondent soit à un n° à partir de 100 ou bien à un nom défini libre de notre choix.
Les ACL étendues permettent un filtrage plus précis avec une source, une destination, un port, une connexion potentiellement déjà établie…

Pour configurer une ACL cela se passe sur un routeur :

```
ip access-list extended [N° ou TEXT]
[permit | deny] [ip | icmp | tcp | ...] [@Source] [Wildcard source]
[@Destination] [Wildcard destination] ([eq www | ftp | pop3 | ...]
[established | echo-reply | ...])
```

Par exemple si on souhaite permettre au réseau du VLAN 20 d’accéder au réseau du VLAN 10 par ICMP (ping) :

Sur R1 :

```
ip access-list extended 100
      permit icmp 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
      permit icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
echo-reply
```

Ainsi dans la première ligne le réseau VLAN20 est autorisé à ping le réseau VLAN10 et le réseau VLAN10 possède en deuxième ligne le droit de répondre à un echo-request émis par le réseau VLAN20.

Une fois l’ACL créée il faut l’attribuer au port où le filtrage sera effectué en “in” ou en “out” qui correspond au sens du flux.

Sur R1 :

```
int gi0/0/0
      ip access-group 100 in
```

Ainsi le filtrage se fera à l’entrée des trames dans R1.

Il est aussi possible de filtrer selon le port du protocole correspondant à la trame, si il s'agit d'un hôte spécifique d'un réseau…

/!\ Il est important de savoir qu'à la fin de chaque ACL il est automatiquement introduit un refus de toutes autres passages de trames (exemple sur une ACL étendue à la fin le routeur instaurera automatiquement deny ip any any) /!