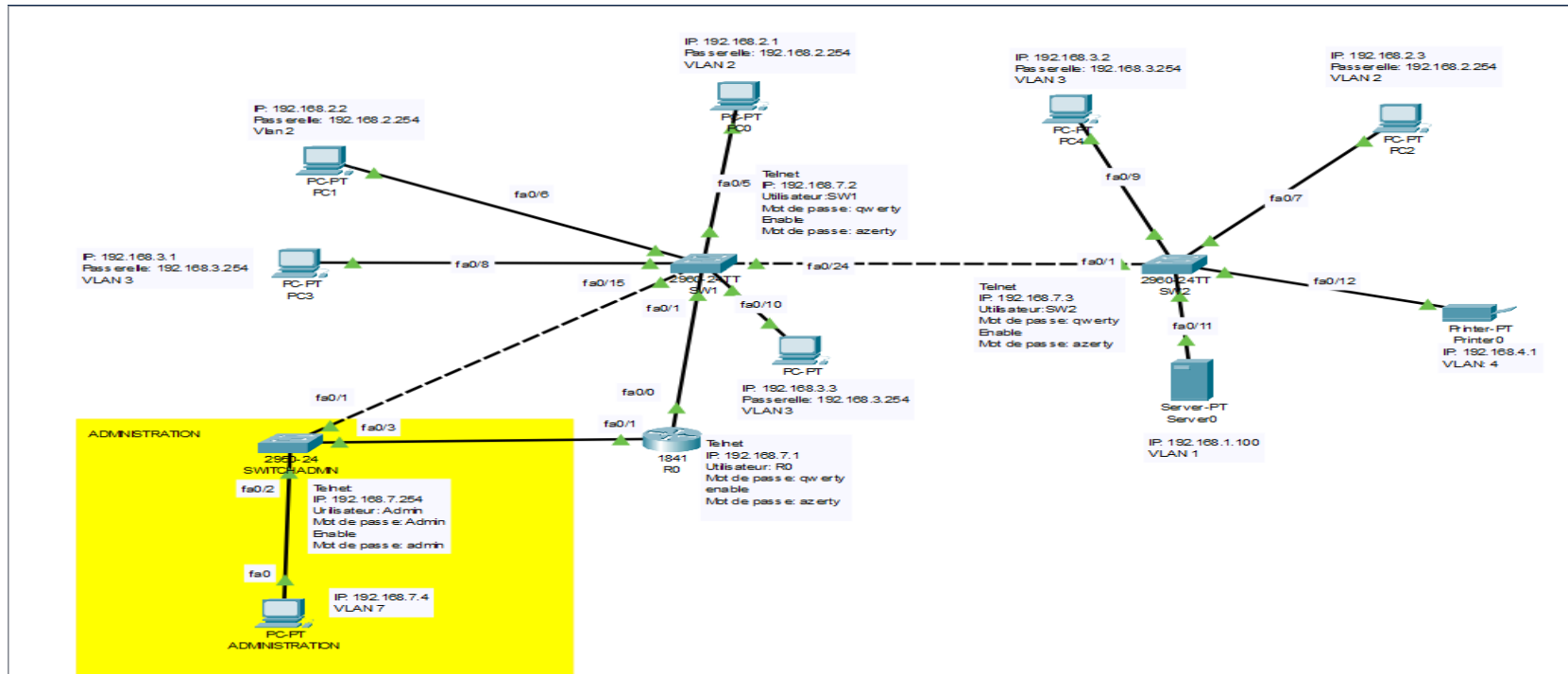


# TP- INTERVLAN

---

THOMAS GRZESINSKI

# Schéma réseau



# INTERVLAN ça sert à quoi ?

---

Le routage inter VLAN est le fait de permettre à des appareils contenus dans des VLANs différents de communiquer entre eux.

En effet si vous êtes un utilisateur raccordé au VLAN 2 mais que vous devez envoyer des données à un utilisateur qui est raccordé à un vlan 4 alors grâce à l'inter-vlan cela sera possible

# Configuration des SWITCHS

---

Tout d'abord nous allons devoir configurer nos switches:

Nous allons les nommer et leurs adresser un mot de passe et de clarté, on va aussi créer un utilisateur et attribuer un mot de passe sur chaque switches pour que l'on puisse y accéder à distance.

Il faudra appliquer ses commandes sur les deux switches

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#enable secret azerty
SW1(config)#line console 0
SW1(config-line)#password azerty
SW1(config-line)#login
SW1(config-line)#exit
SW1(config)#line vty 0 4
SW1(config-line)#password azerty
SW1(config-line)#login
SW1(config-line)#exit

SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#username SW1 password qwerty
SW1(config)#line vty 0 4
SW1(config-line)#login local
SW1(config-line)#exit
```

# Mise en place du protocole VTP

---

On va maintenant mettre en place le protocole VTP entre le switch 1 et le switch 2  
Pour que les VLANS créés sur le switch 1 soient directement mis sur le switch 2  
Il faut donc configurer le switch 1 en tant que serveur et le switch 2 en tant que client.

Il faut aussi que vous mettiez le port sur laquelle vous allez raccorder votre routeur en mode trunk pour qu'il puisse récupérer les VLANS et créer les sous-interfaces.

```
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vtp domain sio
Changing VTP domain name from NULL to sio
SW1(config)#vtp password sio24
Setting device VLAN database password to sio24
SW1(config)#vtp mode server
SW1(config)#interface fa0/24
SW1(config-if)#switchport mode trunk
```

```
SW2>enable
Password:
SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#vtp domain sio
Domain name already set to sio.
SW2(config)#vtp password sio2024
Setting device VLAN database password to sio2024
SW2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW2(config)#interface fa0/1
SW2(config-if)#switchport mode trunk
```

# Création des VLANS

Maintenant il vous faudra donc créer vos VLANS sur votre switch 1 et ensuite les nommer pour savoir à quelle interface et pour qui seront attribué ses VLANS.

Pour la création des VLANS, il vous faut entrer en mode configuration vlan + numéro du vlan et ensuite pour le nommer il faut tout simplement entrer la commande name + nom à donner à votre VLAN 2

```
SW1(config)#vlan 2
SW1(config-vlan)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
SW1(config-vlan)#name SISR
```

Vérifier ensuite la création de vos VLANS mais aussi de la mise en place de votre protocole VTP grâce à la commande sh vlan sur vos deux routeurs, si le switch 2 a exactement les mêmes VLANS alors le protocole fonctionne correctement

Switch 1

```
1    default                active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                           Fa0/9, Fa0/11, Fa0/12, Fa0/13
                                           Fa0/14, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Gig0/1, Gig0/2
2    SISR                   active    Fa0/5, Fa0/6
3    slam                   active    Fa0/8, Fa0/10
4    profs                  active
```

Switch 2

```
1    default                active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                           Fa0/6, Fa0/8, Fa0/10, Fa0/11
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2
2    SISR                   active    Fa0/7
3    slam                   active    Fa0/9
4    profs                  active    Fa0/12
```

# Raccorder un port a un VLAN

---

Pour que vos machines soit raccordé à un vlan vous devez donc faire en sorte que le port sortant du switch soit raccordé à un vlan

Suivre ces commandes et appliqué pour chaque VLAN que vous souhaitez intégré a X machines :

```
SW1(config)#interface fa0/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
SW1(config-if)#exit
SW1(config)#exit
```

# Intégration d'un routeur

---

Ici l'intégration d'un routeur permettra de procéder à la mise en place de l'inte-vlan, mais d'abord il vous faudra aussi lui configurer un nom et un mot de passe d'accès et un utilisateur et un mot de passe pour y accéder en telnet

```
Router(config)#hostname R0
R0(config)#enable secret azerty
R0(config)#line console 0
R0(config-line)#password azerty
R0(config-line)#login
R0(config-line)#exit
R0(config)#
R0(config)#line vty 0 4
R0(config-line)#password azerty
R0(config-line)#login
R0(config-line)#
R0(config-line)#
```

```
R0(config)#username R0 password qwerty
R0(config)#line vty 0 4
R0(config-line)#login local
```

# Intégration d'un router

---

Si vous souhaitez intégrer un message d'accueil à votre routeur, vous devez entrer la commande banner motd + un caractère que vous n'utiliserez pas dans votre message. Ecrivez votre message, et quand vous aurez fini remettez le caractère. Relancez votre switch et votre message d'accueil apparaîtra.

```
R0>enable
Password:
R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#banner motd (
Enter TEXT message.  End with the character '('.
Bienvenue sur le routeur SIO SAINT-LUC

(
Bienvenue sur le routeur SIO SAINT-LUC

User Access Verification
Password:
```

# Mise en place de l'inter-vlan

---

Maintenant nous procédons à la configuration de l'inter-VLAN:

Nous souhaitons faire communiquer le VLAN 2 avec le VLAN 4

Il vous faudra tout d'abord utiliser la commande interface (fast Ethernet ou gigabit-ethernet) + le port sortant + . le numéro du vlan

Ensuite utiliser la commande encapsulation dot1q + numéro du vlan (l'encapsulation permet avec un seul lien physique, le routage de plusieurs vlans)

Et ensuite entrer une adresse IP qui servira de passerelle

```
R0(config-if)#interface fa0/0.2
R0(config-subif)#encapsulation dot1q 2
R0(config-subif)#ip address 192.168.2.254 255.255.255.0
```

```
R0(config)#interface fa0/0.4
R0(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.4, changed state to up
R0(config-subif)#encapsulation dot1q 4
R0(config-subif)#ip address 192.168.4.254 255.255.255.0
```

# Mise en place du DHCP

---

Le protocole DHCP (Dynamic Host Configuration Protocol) est utilisé pour attribuer dynamiquement des adresses IP (Internet Protocol) à chaque hôte du réseau de votre organisation

Vous pouvez exclure des adresses IP d'abord en utilisant la commandes `ip dhcp excluded-address` (mettre votre adresse IP a autant d'adresses IP que vous souhaitez exclure)

```
R0(config)#ip dhcp excluded-address 192.168.1.2 192.168.1.254
R0(config)#ip dhcp excluded-address 192.168.2.10 192.168.2.254
R0(config)#ip dhcp excluded-address 192.168.3.10 192.168.3.254
R0(config)#ip dhcp excluded-address 192.168.4.10 192.168.4.254
```

Ensuite pour mettre en place le DHCP il vous suffit d'entrer la commande:

- ip dhcp pool VLAN + (numéro du vlan)
- Network (mettre l'adresses réseau de votre vlan)
- Mettre la passerelle du réseau (la passerelle est celle que l'on a mise dans la sous interface :

```
R0(config)#ip dhcp pool VLAN1
R0(dhcp-config)#network 192.168.1.0 255.255.255.0
R0(dhcp-config)#exit
R0(config)#ip dhcp pool VLAN2
R0(dhcp-config)#network 192.168.2.0 255.255.255.0
R0(dhcp-config)#default-router 192.168.2.254
R0(dhcp-config)#exit
R0(config)#ip dhcp pool VLAN3
R0(dhcp-config)#network 192.168.3.0 255.255.255.0
R0(dhcp-config)#default-router 192.168.3.254
R0(dhcp-config)#exit
R0(config)#ip dhcp pool VLAN4
R0(dhcp-config)#network 192.168.4.0 255.255.255.0
R0(dhcp-config)#default-router 192.168.4.254
```

# Test

---

Si tout se passe bien vos machines dans un VLAN 2 pourront pinguer les machines dans un vlan 4 et inversement

```
C:\>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 192.168.4.1: bytes=32 time<1ms TTL=127
Reply from 192.168.4.1: bytes=32 time<1ms TTL=127
Reply from 192.168.4.1: bytes=32 time<1ms TTL=127
Reply from 192.168.4.1: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

# ATTENTION!

---

Comme sur notre router nous avons mis en place une procédure d'un inter-VLAN notre router ne voudra plus distribuer les adresses IP sur le reste des VLANS. Pour régler ce problème vous pouvez utiliser une ACL (Access Control List), est un ensemble de règles qui permet de donner des droits d'accès à une personne ou à un groupe.

# ATTENTION !

---

Pour faire ceci vous devez donc quand même créer leurs sous interfaces sur le routeur comme on a vu précédemment.

```
R0(config)#interface fa0/0.1
R0(config-subif)#encapsulation dot1q 1
R0(config-subif)#ip address 192.168.1.254 255.255.255.0
R0(config-subif)#
R0(config-subif)#exit
R0(config)#
R0(config)#interface fa0/0.3
R0(config-subif)#encapsulation dot1q 3
R0(config-subif)#ip address 192.168.3.254 255.255.255.0
R0(config-subif)#end
```

Et seulement ensuite créer des listes différentes en disant avec qui l'adresse réseau doit

```
R0(config)#access-list 1 deny 192.168.2.0 0.0.0.255
R0(config)#access-list 1 deny 192.168.3.0 0.0.0.255
R0(config)#access-list 1 deny 192.168.4.0 0.0.0.255
R0(config)#access-list 1 permit any
R0(config)#access-list 2 deny 192.168.1.0 0.0.0.255
R0(config)#access-list 2 deny 192.168.2.0 0.0.0.255
R0(config)#access-list 2 deny 192.168.4.0 0.0.0.255
.....
R0(config)#access-list 2 permit any
```

Deny = refuser  
Any = n'importe qui  
In / out (port entrant ou sortant du router sur laquelle vous allez mettre la liste)

Et ensuite allez dans la sous-interface et intégrer y la liste avec la commande ip access-group 1 in ou out selon votre cas

# ATTENTION !

---

Vous pouvez donc retourner sur une machine en dehors du vlan 2 et 4 et vous verrez qu'ils pourront enfin avoir l'adresse IP qui a été mise en mode dhcp comme vous l'aviez souhaité mais ne pourront pas communiquer avec les autres VLANS

# Administration du réseau

---

Pour l'administration il est plus simple de raccorder un autre switch que l'on va se servir que pour l'administration du réseau, en effet votre router ne pourra jamais être raccorder en Telnet car chaque VLAN créer sur le Switch 1 va poser un problème lors de la création d'une adresse IP (overlaps) sur le router qui aura le même numéro que l'adresse réseau du switch 1. Et comme il n'y a pour l'instant qu'une sortie du router c'est ce qui créer notre problème.

La solution est donc:

Créer un nouveau Switch administrateur

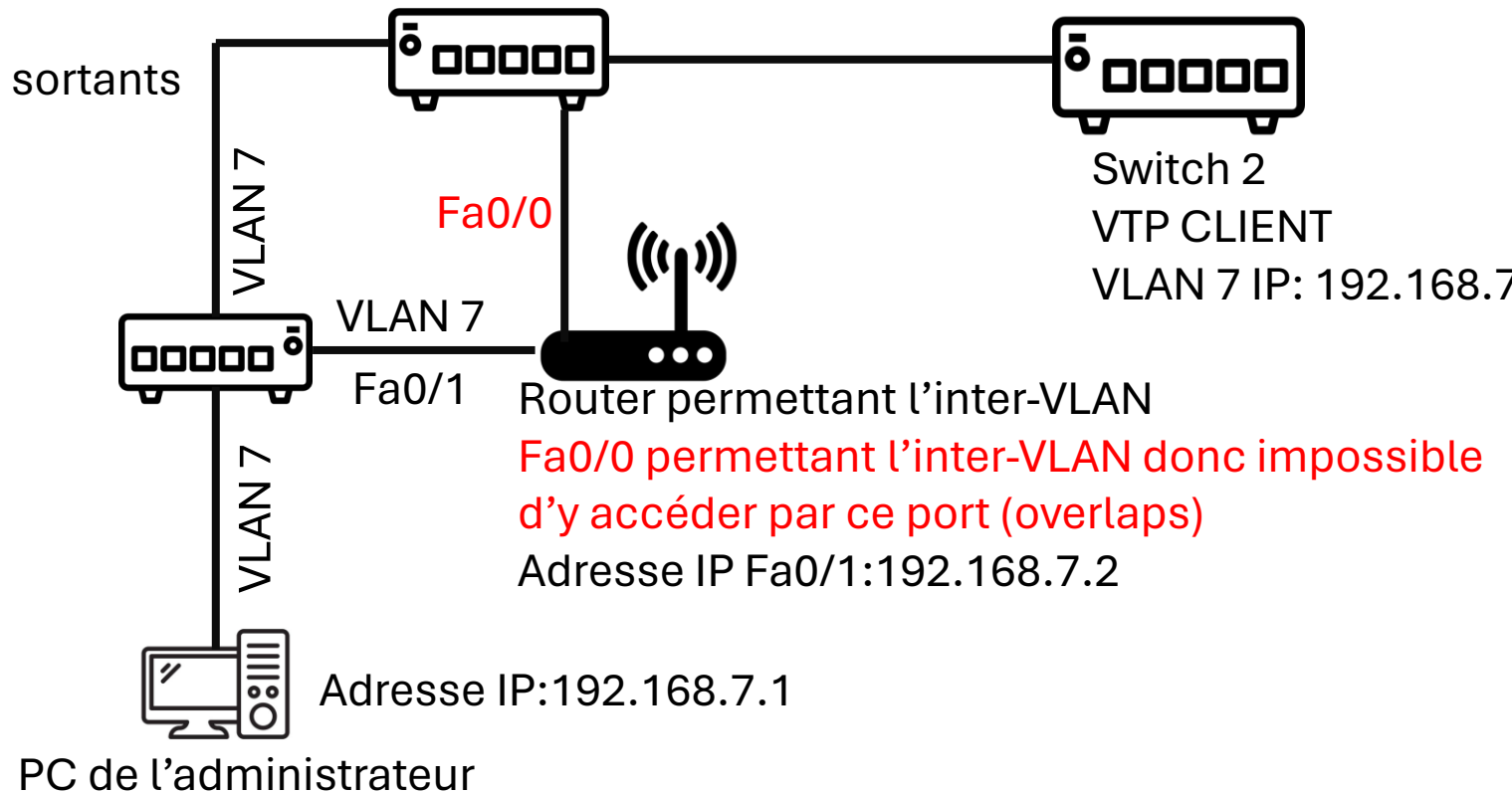
- Sur ce router créer un vlan et un accès telnet
- Mettre une adresse IP sur le VLAN créer
- Le raccorder a un port du router inter-vlan et le raccorder au switch 1 sur un port
- Raccorder un PC au Switch administrateur
- Mettre le Switch administrateur en mode VTP et client du switch 1
- Sur le switch 1 et 2 mettre sur le même VLAN que le switch admin une adresse IP logique de l'adresse réseau
- Sur le router la même chose sur le port relié à celui du switch administrateur mettre une adresse ip logique a celle de l'adresse ip réseau du vlan
- Mettre une adresse IP logique sur le pc à celle de l'adresse IP du switch
- Mettre les trois ports sortant du switch sur le VLAN

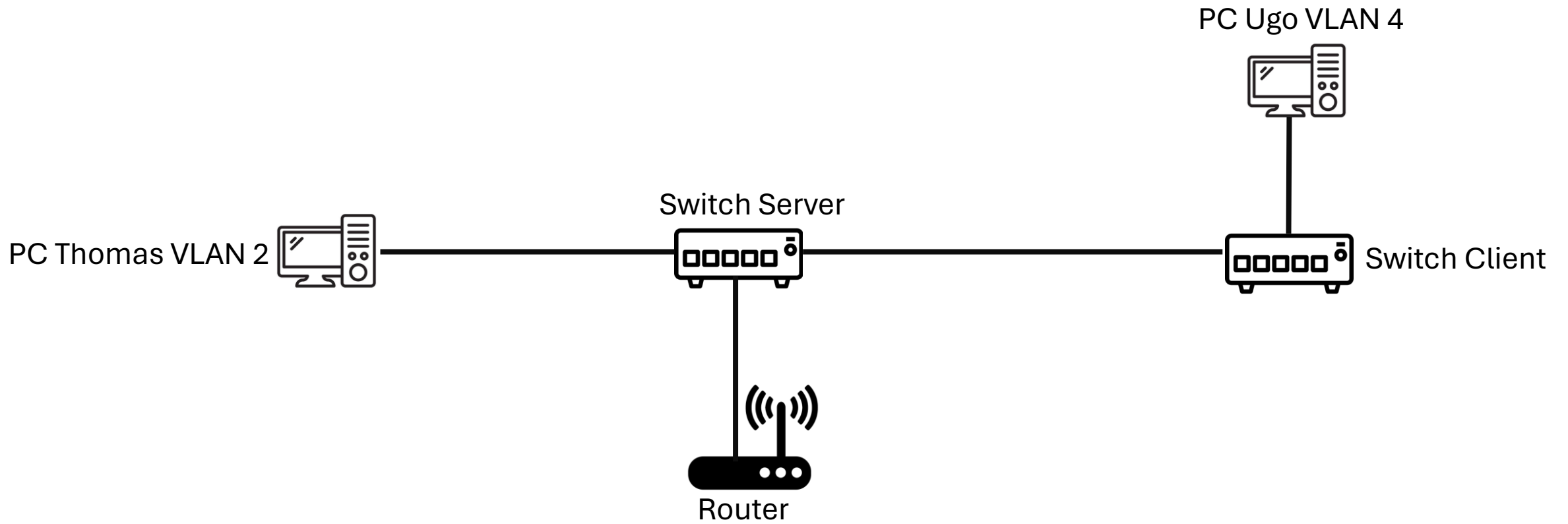
# Administration du réseau

Pour illustrer:

Switch 1  
VTP SERVER  
Mode trunk des trois ports sortants  
VLAN 7 IP: 192.168.7.3

Switch 2  
VTP CLIENT  
VLAN 7 IP: 192.168.7.4





---

TP-FAIT EN PHYSIQUE PAR THOMAS ET UGO ( A TERMINER)

# Partie Physique

---

Je suis le switch Server et Ugo et le switch client:

De mon côté j'ai donc configuré mon port 24 qui sera en mode Trunk, grâce a ce port Ugo va donc lui faire en sorte que son port 1 soit en mode client.

J'ai aussi fait en sorte en même temps que mon port soit en mode Trunk car le router sera relié a ce port.

```
thomasg#conf t
Enter configuration commands, one per line. End with CNTL/Z.
thomasg(config)#vtp mode server
Device mode already VTP Server for VLANS.
thomasg(config)#vtp domain SIO
Changing VTP domain name from NULL to SIO
thomasg(config)#vtp
Mar 30 01:37:23.336: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to S
thomasg(config)#vtp password sio2018
Setting device VTP password to sio2018

thomasg(config)#interface gil/0/24
thomasg(config-if)#switchport mode access
thomasg(config-if)#switchport mode trunk
```

```
thomasg(config)#interface gil/0/1
thomasg(config-if)#switchport mode access
thomasg(config-if)#switchport mode trunk
```

# Partie Physique

---

Par la suite on a donc créer un VLAN 2 nommer Thomas car il sera reliev directement a son PC, et le VLAN 4, on la donc reliev au PC de Ugo.

```
ADMINISTRATION(config-vlan)#name Thomasg  
ADMINISTRATION(config-vlan)#exit  
ADMINISTRATION(config)#Vlan 4  
ADMINISTRATION(config-vlan)#name UgoB
```

On a donc renommé les Vlan pour une meilleure clarté.

On a donc ensuite raccorder le VLAN 2 du PC de Thomas au port 2 et pareil pour Ugo sur son switch son port 2 permet d'y rattacher son VLAN 4

```
ADMINISTRATION(config)#interface f  
ADMINISTRATION(config)#interface gil/0/2  
ADMINISTRATION(config-if)#switchport mode access  
ADMINISTRATION(config-if)#switchport acces vlan 2
```

# Partie Physique

---

Maintenant sur le Router raccordé au Switch de Thomas on va y configurer l'inter-VLAN et le DHCP

On va donc faire la même chose que sur la simulation, on va aller dans les deux sous interfaces de notre réseau et mettre en place une adresse IP.

```
interface FastEthernet0.2
 encapsulation dot1Q 2
 ip address 192.168.2.254 255.255.255.0
!
interface FastEthernet0.4
 encapsulation dot1Q 4
 ip address 192.168.4.254 255.255.255.0
```

Par la suite on va donc configurer  
Notre DHCP, pareil on exclu les adresses IP non  
Voulus et on fait la sous-interface en tant que passerelle

```
Rthomasg(config)#ip dhcp excluded-address 192.168.2.10 192.168.2.254
Rthomasg(config)#ip dhcp excluded-address 192.168.4.10 192.168.4.254
Rthomasg(config)#ip dhcp pool VLAN2
Rthomasg(dhcp-config)#network 192.168.2.0 255.255.255.0
Rthomasg(dhcp-config)#default-router 192.168.2.254
Rthomasg(dhcp-config)#ip dhcp pool VLAN4
Rthomasg(dhcp-config)#network 192.168.4.0 255.255.255.0
Rthomasg(dhcp-config)#default-router 192.168.4.254
```