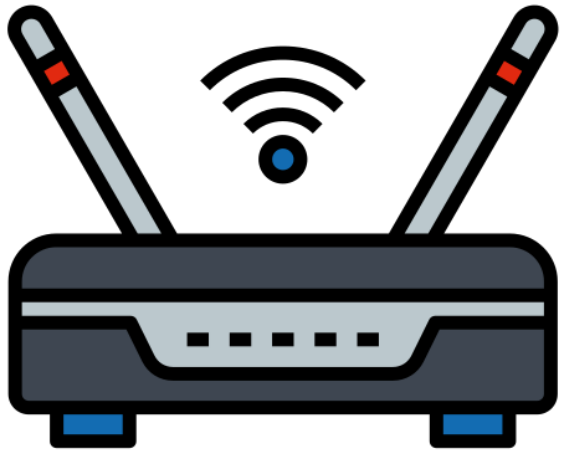
TRIOUX Jimmy
BTS SIO1 SISR

TP – InterVLAN



Sommaire

Contexte du TP

L’objectif est de segmenter le réseau en plusieurs VLANs afin de séparer les flux entre les différents groupes d’utilisateurs (SISR, SLAM et PROFS).

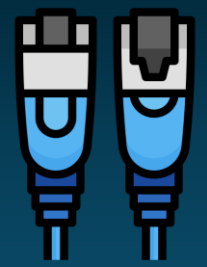
- Création des VLANs
- Attribution des noms
- Affectation des ports aux VLANs correspondant
- Configuration du mode VTP

Par défaut, les VLANs ne peuvent pas communiquer entre eux.
Pour permettre l’échange d’informations entre eux, il faut utiliser un routeur qui joue le rôle d’intermédiaire.

- Création des sous-interfaces sur le routeur
- Utilisation du protocole dot1Q
- Attribution des adresses IP correspondant aux passerelles pour chaque VLAN
- Mode trunk entre le routeur et les switchs

Le VLAN 2 doit pouvoir communiquer uniquement avec le VLAN 4. Tous les autres échanges doivent être bloqués.

- Création d’une ACL
- Ajout d’un deny ip any any pour bloquer le reste des autres adresses.
- Application de l’ACL sur la bonne sous-interface



Pour simplifier la configuration des équipements utilisateurs, nous mettrons en place un serveur DHCP sur le routeur qui attribue automatiquement une adresse IP à chaque PC selon son VLAN.

- Définir les plages d’adresses par VLAN
- Exclure les adresses réservées
- Définir le réseau, le masque et la passerelle par défaut pour chaque pool

Dictionnaire des commandes

Commandes	
switchport mode trunk	Permet de transporter plusieurs VLANs simultanément en configurant un port de switch ou de routeur pour qu'il accepte des trames étiquetées à l'aide du protocole 802.1Q.
encapsulation dot1Q [n° vlan]	Permet de configurer une sous-interface sur le routeur pour utiliser le protocole 802.1Q afin de permettre le routage interVLAN.
ip dhcp excluded-address x x	Empêche le serveur DHCP d'attribuer automatiquement certaines adresses IP spécifiques.
ip dhcp pool [n° vlan]	Permet de créer un pool DHCP, souvent par un numéro de VLAN, duquel le routeur pourra attribuer automatiquement des adresses IP aux hôtes du VLAN concerné.

Qu’est-ce qu’un InterVLAN ?

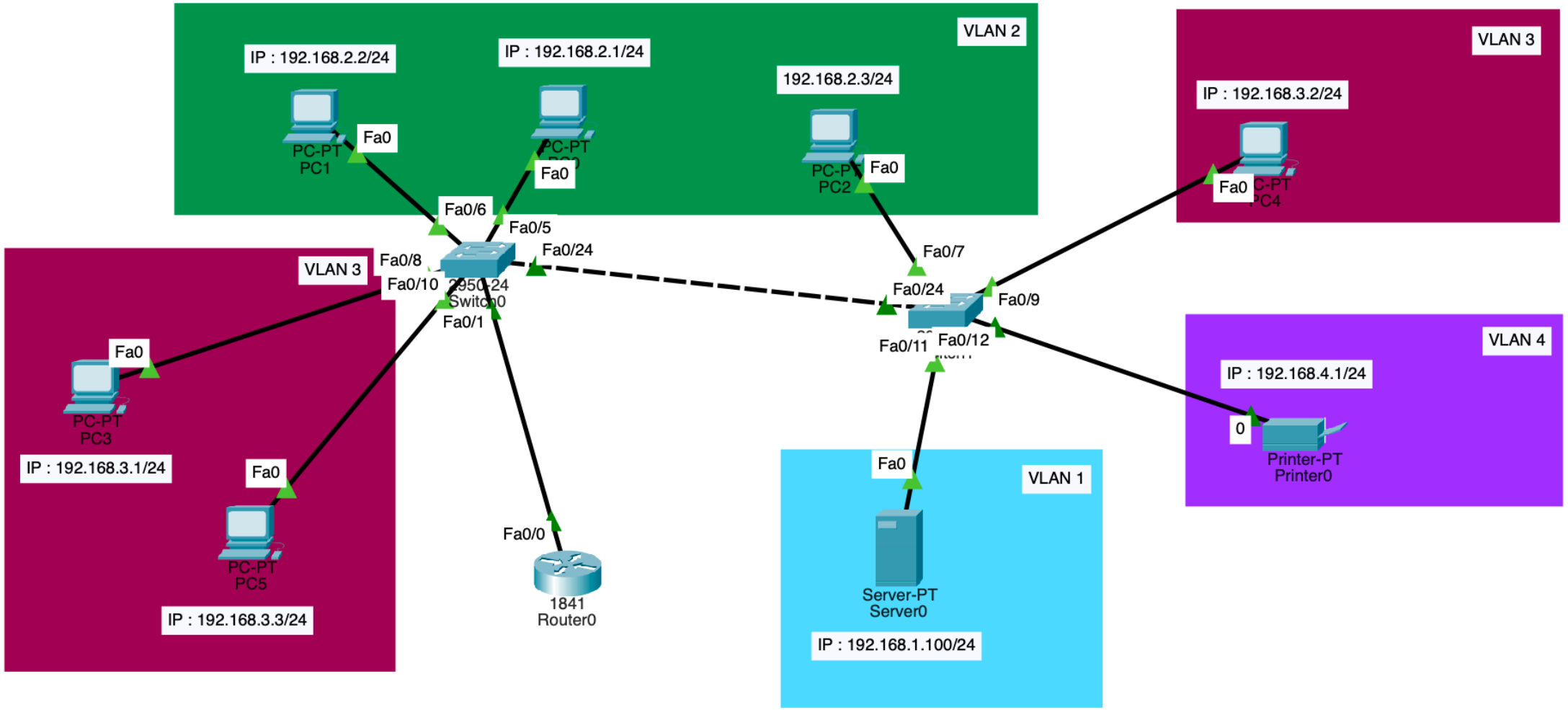
Un interVLAN (ou routage interVLAN) permet la communication entre plusieurs VLANs qui sont normalement isolés les uns des autres.

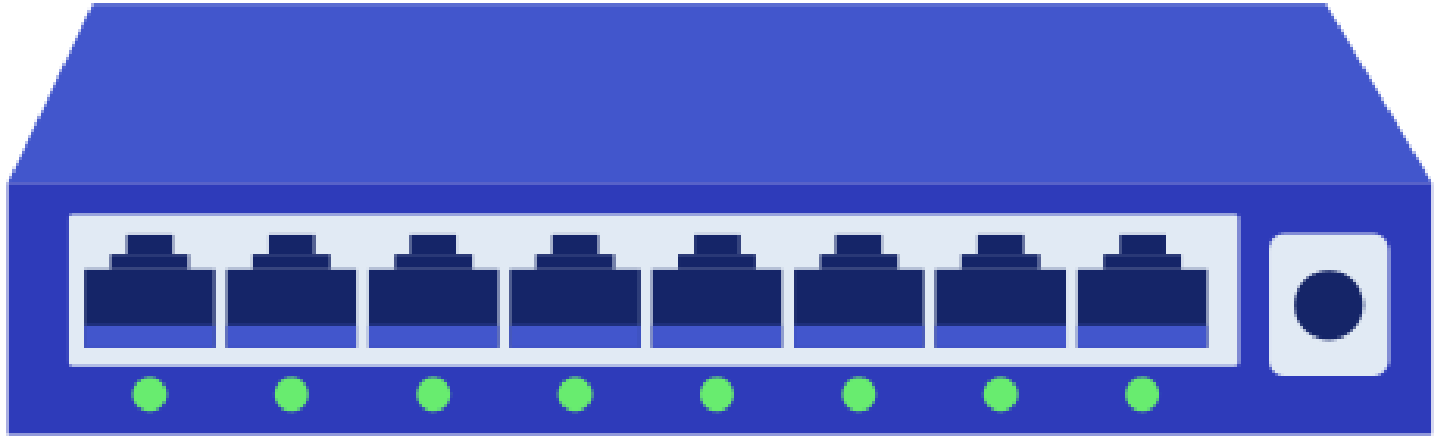
Chaque VLAN correspond à un sous-réseau différent, et comme les appareils dans les VLANs différents ne peuvent pas s’échanger de données directement, un **routeur** ou un **commutateur de niveau 3** (Cisco 3560, 3750, 3850, …) est utilisé pour faire passer les informations d’un VLAN à un autre.

C’est essentiel dans les réseaux d’entreprises, car il permet de segmenter le réseau pour des raisons de sécurité ou d’organisation, tout en s’assurant que l’interconnexion entre les différents services soient contrôlé.

En somme, le routage interVLAN permet d’isoler et de faire communiquer des services selon les besoins.

Topologie du réseau





Sur le commutateur

Configuration basique des deux commutateurs

SW1

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

SW2

```
Switch>en
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#hostname SW2
SW2(config)#
SW2(config)#enable secret azerty
SW2(config)#
SW2(config)#line vty 0 4
SW2(config-line)#
SW2(config-line)#password qwerty
SW2(config-line)#
SW2(config-line)#login
SW2(config-line)#
SW2(config-line)#exit
```

Dans un premier temps, nous ferons deux configurations simples sur les commutateurs.

On affecte un nom d'hôte à chacun puis on active les lignes vty afin de pouvoir s'y connecter à distance.

Création du protocole VTP

SW1

```
SW1(config)#vtp mode server
Device mode already VTP SERVER.
SW1(config)#vtp domain TRIOUX
Changing VTP domain name from NULL to TRIOUX
SW1(config)#vtp password azerty
Setting device VLAN database password to azerty
```

Ensuite en restant dans le mode de configuration terminal, passons le switch 1 en mode serveur pour le VTP et donnons-lui un nom de domaine.

SW2

```
SW2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW2(config)#
SW2(config)#vtp password azerty
Setting device VLAN database password to azerty
```

Sur le switch 2, faisons-le basculer vers le mode client.

Création des VLANs

```
SW1(config)#vlan 2
SW1(config-vlan)#
SW1(config-vlan)#name SISR
SW1(config-vlan)#
SW1(config-vlan)#exit
SW1(config)#
SW1(config)#vlan 3
SW1(config-vlan)#
SW1(config-vlan)#name SLAM
SW1(config-vlan)#
SW1(config-vlan)#exit
SW1(config)#
SW1(config)#vlan 4
SW1(config-vlan)#
SW1(config-vlan)#name PROFS
SW1(config-vlan)#
SW1(config-vlan)#exit
```

Retournons dans le switch 1 puis créons les différents VLANs comme stipulait dans le contexte du TP.

1. **Mode de configuration terminal**
2. **vlan [numéro]**
3. **name [nom_du_vlan]**

Attribution des ports au VLAN correspondant

SW1

```
SW1(config)#int fa0/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
SW1(config-if)#exit
SW1(config)#
SW1(config)#int fa0/6
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
SW1(config-if)#exit
```

SW1

```
SW1(config)#int fa0/8
SW1(config-if)#switchport mode a
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 3
SW1(config-if)#exit
SW1(config)#
SW1(config)#int fa0/10
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 3
SW1(config-if)#exit
```

SW2

```
SW2(config)#int fa0/7
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 2
SW2(config-if)#exit
SW2(config)#
SW2(config)#int fa0/9
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 3
SW2(config-if)#exit
```

SW2

```
SW2(config)#int fa0/11
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 1
SW2(config-if)#exit
SW2(config)#
SW2(config)#int fa0/12
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 4
SW2(config-if)#exit
```

Après avoir créé les VLANs, affectons les ports des équipements informatiques au VLAN correspondant avec les commandes :

- **switchport mode access** : configure le port en mode « access », ce qui signifie qu'il ne transportera qu'un seul VLAN.
- **switchport access vlan** : Attribue un VLAN au port connecté.

Attribution du mode trunk entre les switchs et le routeur

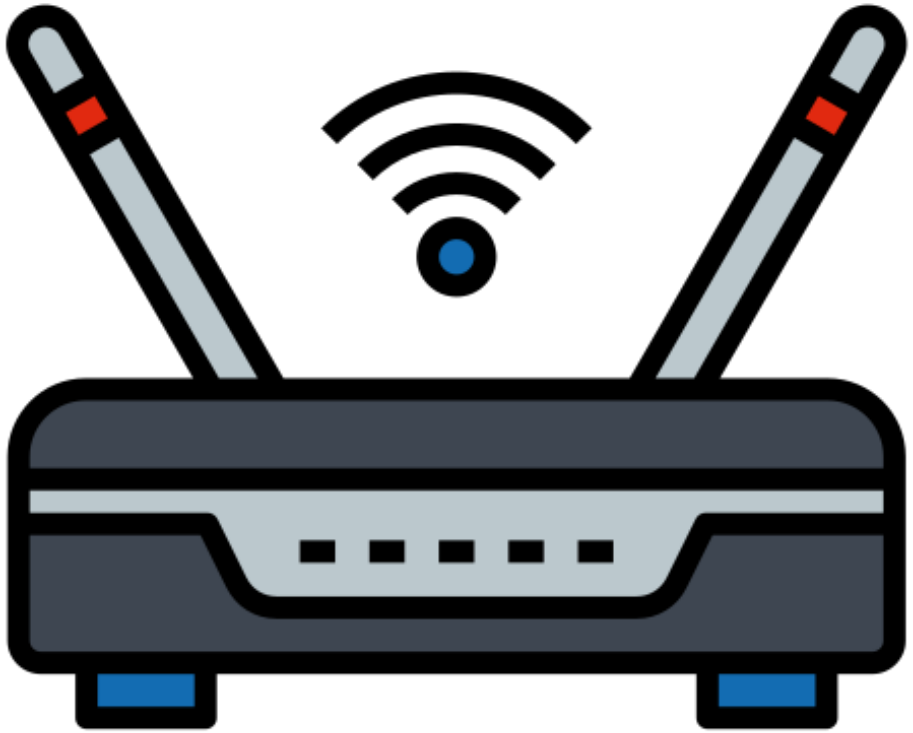
SW1

```
SW1(config)#int fa0/1
SW1(config-if)#
SW1(config-if)#switchport mode trunk
SW1(config-if)#
SW1(config-if)#exit
SW1(config)#
SW1(config)#int fa0/24
SW1(config-if)#
SW1(config-if)#switchport mode trunk
SW1(config-if)#
SW1(config-if)#exit
```

SW2

```
SW2(config)#int fa0/24
SW2(config-if)#
SW2(config-if)#switchport mode trunk
SW2(config-if)#
SW2(config-if)#exit
```

Puis, affectons également les ports en mode trunk sur les interfaces correspondantes.



Sur le routeur

Configuration du routeur

1

```
Router>en
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#int fa0/0
Router(config-if)#
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

2

```
Router(config-if)#int fa0/0.2
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#
Router(config-subif)#ip address 192.168.2.254 255.255.255.0
Router(config-subif)#
Router(config-subif)#no shutdown
```

3

```
Router(config)#int fa0/0.3
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up

Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#
Router(config-subif)#ip addr 192.168.3.254 255.255.255.0
Router(config-subif)#exit
```

4

```
Router(config-if)#int fa0/0.4
Router(config-subif)#
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#
Router(config-subif)#ip addr 192.168.4.254 255.255.255.0
Router(config-subif)#
Router(config-subif)#no shutdown
```

Allons dans le CLI du routeur puis allons dans l'interface 0/0 (comme indiquait sur la topologie du réseau), activons-la avec un « **no shutdown** » et créons les sous interfaces virtuelles sur l'interface 0/0, par exemple :

1. **int fa0/0.[n°vlan]**
2. **encapsulation dot1Q [n°vlan]**
3. **ip addr [passerelle_du_vlan] [masque_du_vlan]**
4. **no shutdown**

Mise en place des plages d'exclusions IP pour le DHCP

```
Router(config)#ip dhcp excluded-address 192.168.2.4 192.168.2.9
Router(config)#
Router(config)#ip dhcp excluded-address 192.168.2.21 192.168.2.254
Router(config)#
Router(config)#ip dhcp excluded-address 192.168.3.4 192.168.3.9
Router(config)#
Router(config)#ip dhcp excluded-address 192.168.3.21 192.168.3.254
Router(config)#
Router(config)#ip dhcp excluded-address 192.168.4.2 192.168.4.9
Router(config)#
Router(config)#ip dhcp excluded-address 192.168.4.21 192.168.4.254
```

Ensuite, nous souhaitons n'avoir que les plages 10 à 20 de disponible pour le DHCP alors nous exclurons toutes les adresses en dehors avec la commande :

- **ip dhcp excluded-address [ip_debut] [ip_fin]**

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

La commande « **ip dhcp pool VLAN** » permet de créer un pool DHCP sur le VLAN correspondant afin de distribuer automatiquement les adresses IP aux appareils du réseau VLAN attribué.

Ensuite avec la commande « **network [adresse_réseau_vlan] [masque_vlan]** », nous définissons la plage d'adresse du réseau utilisée par le DHCP (**ex** : 192.168.2.0/24 va attribuer automatiquement sur les adresses de 192.168.2.1 à 192.168.2.254 hors exclusion).

Enfin, la commande « **default-router [passerelle]** » permet de faire communiquer le VLAN à d'autres réseaux.

Création d'une liste de contrôle d'accès (ACL) sur le routeur

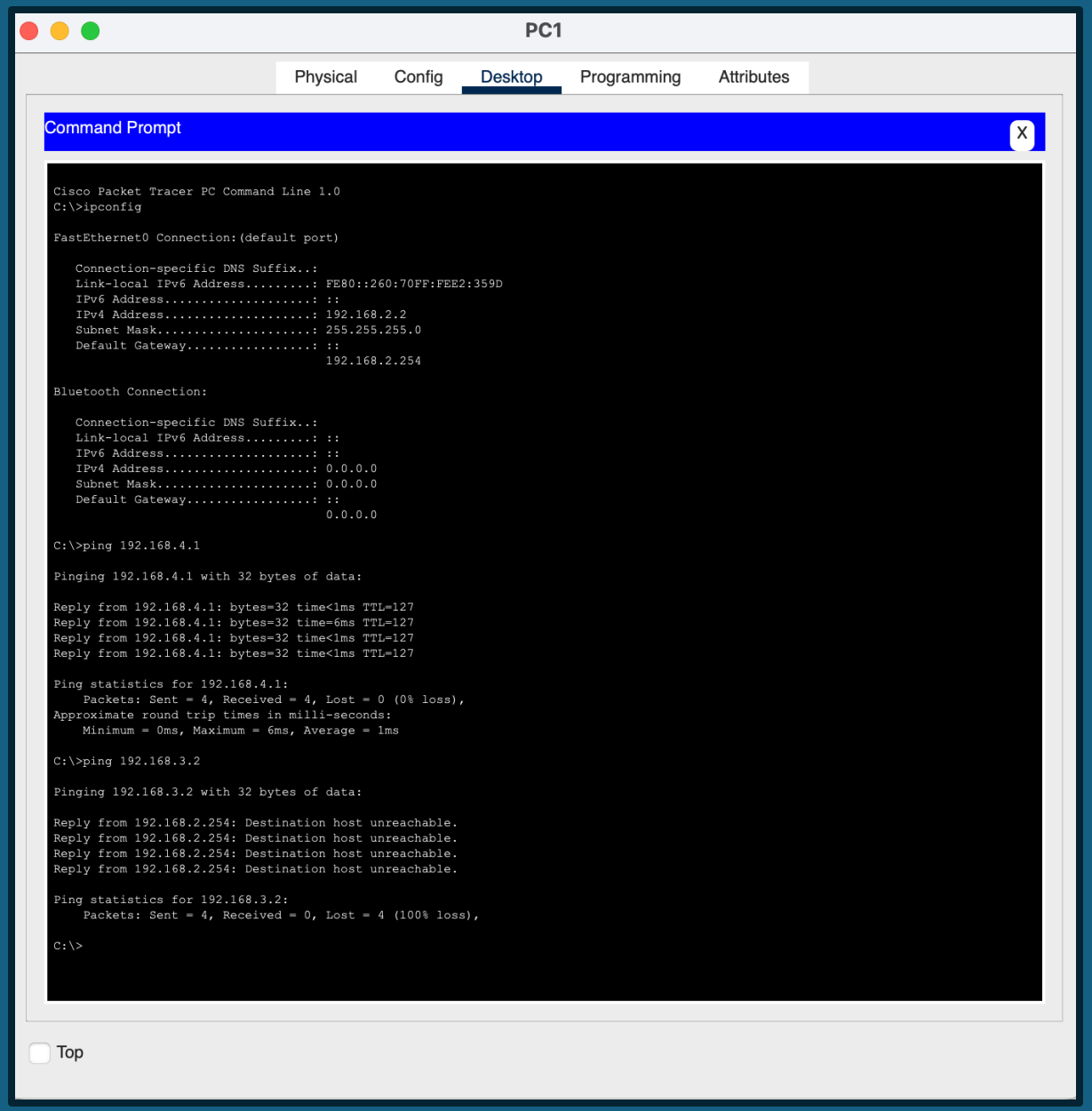
```
Router(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255
Router(config)#
Router(config)#access-list 100 deny ip any any
Router(config)#
Router(config)#int fa0/0.2
Router(config-subif)#
Router(config-subif)#ip access-group 100 in
Router(config-subif)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Comme vu précédemment dans le contexte du TP, nous souhaitons que seulement le VLAN 2 puisse communiquer avec l'imprimante du VLAN 4.

Nous instaurerons dans ce cas précis une liste de contrôle d'accès sur le routeur avec les commandes :

- **access-list [n°100 à 199] permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255** : permet à l'adresse réseau du VLAN 2 d'accéder au réseau du VLAN 4. Le masque définit une plage d'adresses de **.0** à **.255**.
- **access-list [n°] deny ip any any** : bloque tout le reste du trafic IP qui ne correspond pas à la règle de la liste (ici **100**).
- **int fa0/0.2** : on appliquera la règle ACL sur la sous-interface du VLAN 2.
- **ip access-group [n°_liste] in** : applique la liste sur le trafic entrant de l'interface fa0/0.2.

Test de ping



Enfin, testons la communication d'un poste dans le VLAN 2 (par exemple: **PC1**) vers l'imprimante du VLAN 4 (**192.168.4.1**).

Comme nous pouvons le constater, les deux équipements peuvent communiquer ensemble.

De plus en essayant de ping un équipement du VLAN 3 (**PC4**) toujours depuis le **PC1** (du VLAN 2), celui-ci échoue et nous dit que l'hôte est inatteignable.

En conclusion, nous avons pu mettre en place une communication interVLAN, un pool DHCP ainsi que des restrictions avec l'ACL.