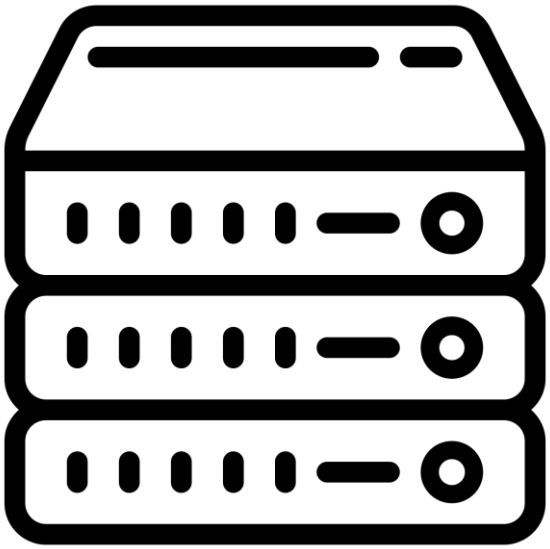


TP - Montage Réseau

Tamara Crétard - 08.12.2025

Sommaire:

1. Contexte

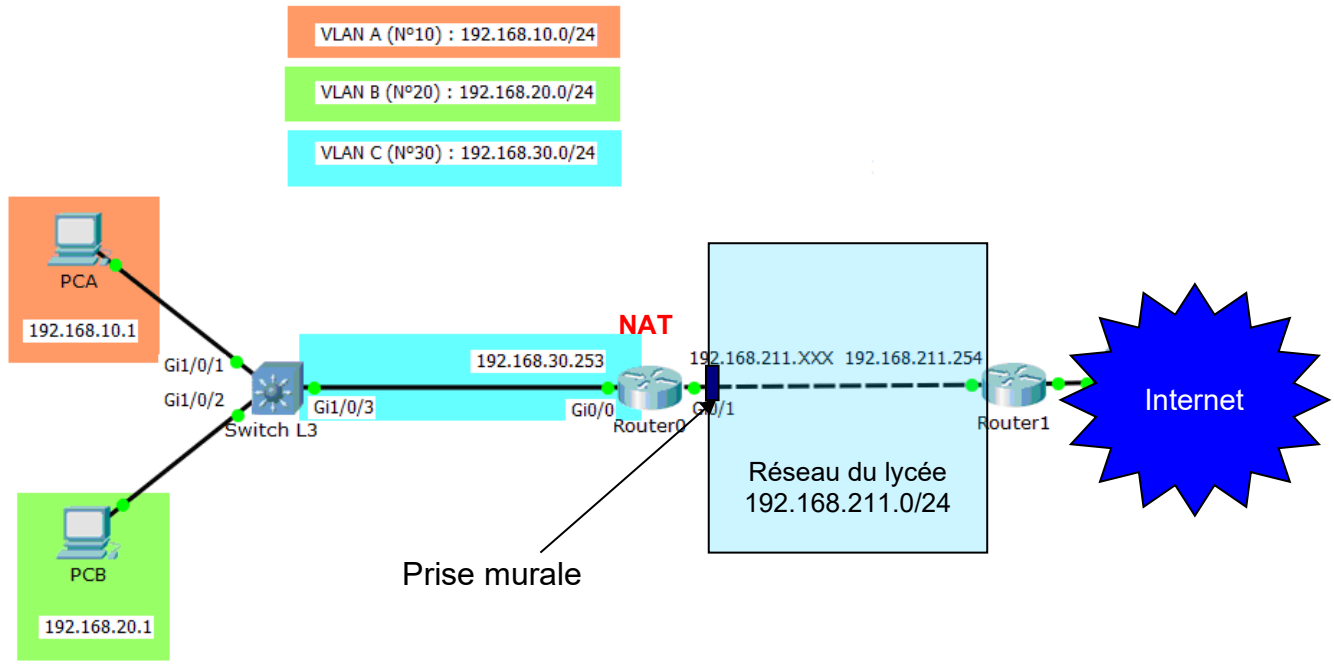
Dans le cadre d'un cours du BTS SIO, l'objectif est d'effectuer le montage et la configuration complète d'un réseau utilisant un switch, un routeur et une borne wifi.

2. Première partie du TP

Dans la première partie du TP, nous avons besoin de deux PC, d'un switch de niveau 3 et d'un routeur:

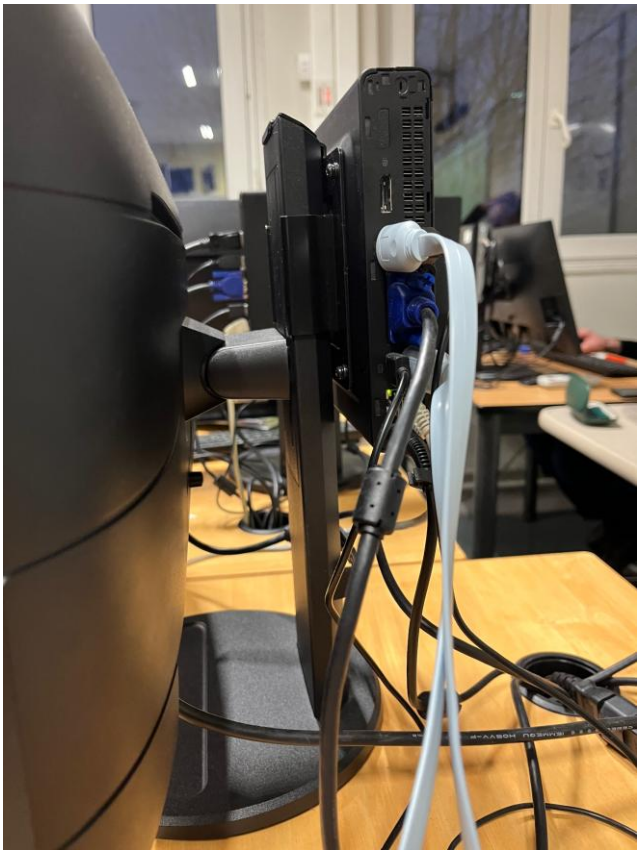
- une machine *PCA* qui aura pour adresse IP 192.168.10.1, dans le VLAN A (n°10)
- une machine *PCB* qui aura pour adresse IP 192.168.20.1, dans le VLAN B (n°20)

Le réseau entre le switch L3 et le routeur sera dans le VLAN C (n°30) et le routeur sera branché à une prise murale brassée.

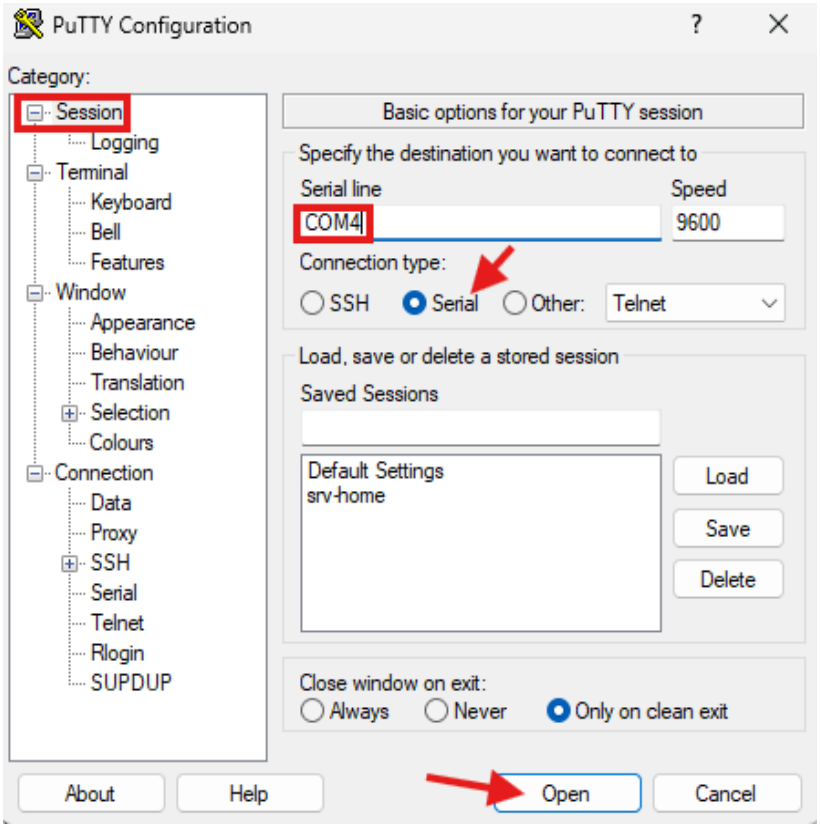


2.1. Configuration du switch de niveau 3

Dans un premier temps, nous allons configurer le switch de niveau 3. Pour cela, il nous faut le switch L3 branché à une prise grâce à un câble d'alimentation et un câble console pour accéder à la console du switch depuis le PC A ou B:



Pour le configurer, il faut utiliser l'application Putty, puis dans "Session" sélectionner le bon port COM après avoir choisi « serial »:



2.1.1. Remise à zéro du switch

Ensuite, il faut mettre à zéro le switch. Pour cela, nous allons suivre la documentation fournie par Cisco. Pour remettre le switch aux valeurs d'usine, la procédure typique est :

- Couper l'alimentation du switch.
- Maintenir le bouton **Mode** enfoncé.
- Rétablir l'alimentation **tout en maintenant** le bouton jusqu'à ce que la LED « SYST » devienne verte solide (ou que les LED commencent à clignoter selon version). uk.genuinemodules.com+1
- Relâcher le bouton : le switch démarre en mode spécial et permet d'effacer le fichier de configuration ou d'ignorer le startup config.

Autrement, il est possible d'utiliser la commande **write erase**:

```
Switch#write erase
```

Ensuite, on sauvegarde la configuration avec **copy run start** :

```
Switch#copy run start
Switch#copy run start
Destination filename [startup-config]
Building configuration...
[OK]
Switch#[OK]
```

Si un mot de passe apparaît, pour le réinitialiser il faut appuyer sur le bouton **mode** quand on rallume le switch. Pour savoir si un mot de passe est nécessaire, il suffit de taper la commande **en**.

2.1.2. Configuration de la partie "Switch" du switch L3

Une fois le switch remis à zéro, nous passons à la configuration de la partie "Switch" du commutateur de niveau 3.

2.1.2.1. Création des VLAN

Tout d'abord, nous nous chargeons de la création des VLAN. Pour cela, nous entrons la commande **en**, puis **conf ter** et pour chaque VLAN, nous entrons **vlan [numéro du VLAN]**, puis **name [nom du VLAN]**:

```
Switch#en
Switch#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name A
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name B
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name C
Switch(config-vlan)#exit
```

2.1.2.2. Configuration des ports physiques

Ensuite, nous configurons les ports physiques du switch. Pour cela, il faut entrer sur chaque port avec **int [port]**, puis entrer **switchport access vlan [numéro du VLAN]** et enfin **switchport mode access**:

```
Switch(config)#int gi1/0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport mode access
Switch(config)#int gi1/0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#switchport mode access
Switch(config)#int gi1/0/3
Switch(config-if)#switchport access vlan 30
Switch(config-if)#switchport mode access
```

2.1.3. Configuration de la partie “Routeur” du switch L3

Après avoir configuré la partie “Switch” du commutateur, nous passons à la configuration de la partie “Routeur”.

2.1.3.1. Activation du routage

Le switch étant un switch de niveau 3, nous activons d’abord le routage avec **ip routing**:

```
Switch(config)#ip routing
```

2.1.3.2. Configuration des interfaces virtuelles

Puis, nous configurons les interfaces virtuelles du switch. Pour cela, il faut entrer sur chaque interface avec **int vlan [numéro du VLAN]**, puis entrer **ip address [passerelle du VLAN] [masque]**:

```
Switch(config)#int vlan 10
Switch(config-if)#ip address 192.168.10.254 255.255.255.0
Switch(config)#int vlan 20
Switch(config-if)#ip address 192.168.20.254 255.255.255.0
Switch(config)#int vlan 30
Switch(config-if)#ip address 192.168.30.254 255.255.255.0
```

A cette étape, si l'on fait **show run**, on obtient:

```
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 30
 switchport mode access
!
interface Vlan10
 ip address 192.168.10.254 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.254 255.255.255.0
!
interface Vlan30
 ip address 192.168.30.254 255.255.255.0
!
```

2.1.3.3. Ajout de la route par défaut

Enfin, nous ajoutons la route par défaut vers internet avec **ip route 0.0.0.0 0.0.0.0 192.168.30.253**:

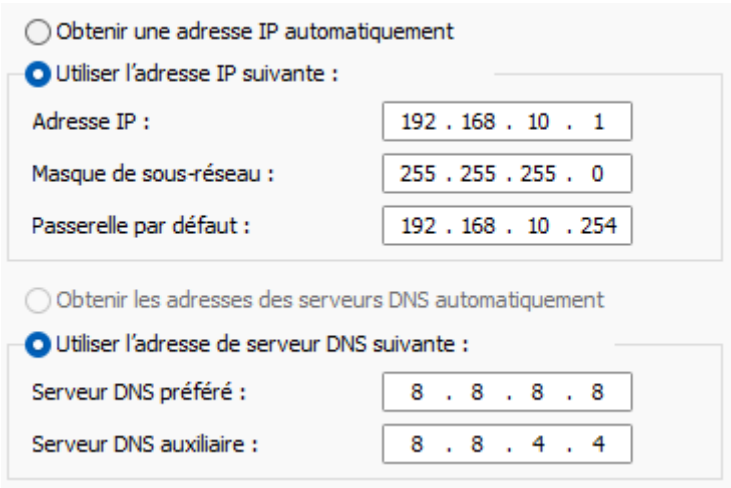
```
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.30.253
```

Après cette étape, nous exécutons à nouveau **copy run start** pour sauvegarder la configuration :

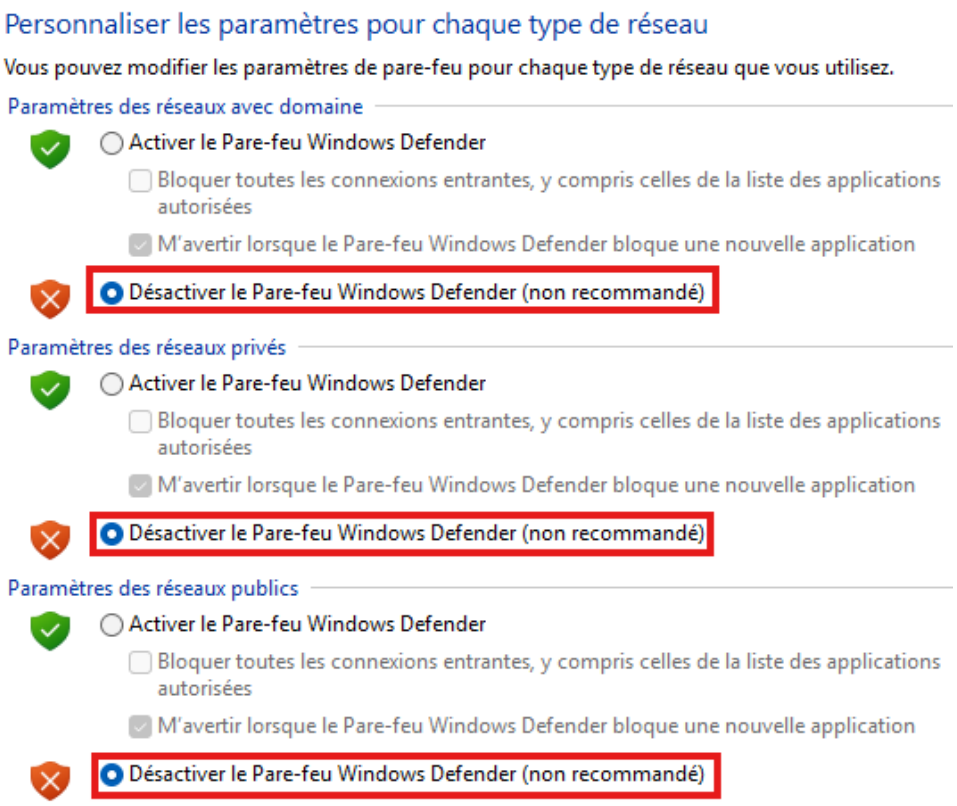
```
Switch>en
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.1.4. Test de la configuration

Pour tester que tout fonctionne, nous changeons la configuration de PCA et PCB pour voir s'ils se pinguent. Pour cela dans le "Panneau de configuration", puis "Réseau et Internet" et "Connexions Réseau", il faut changer l'adresse IP du poste et sa passerelle dans les paramètres avancés de l'adaptateur Ethernet. Par exemple, pour le PC A :



Pour que les deux postes se pinguent, dans le cas du TP, nous désactivons le Pare-feu Windows Defender :



Ensuite, il faut brancher les PC avec un câble Ethernet sur le switch.

Enfin, on ping les machines :

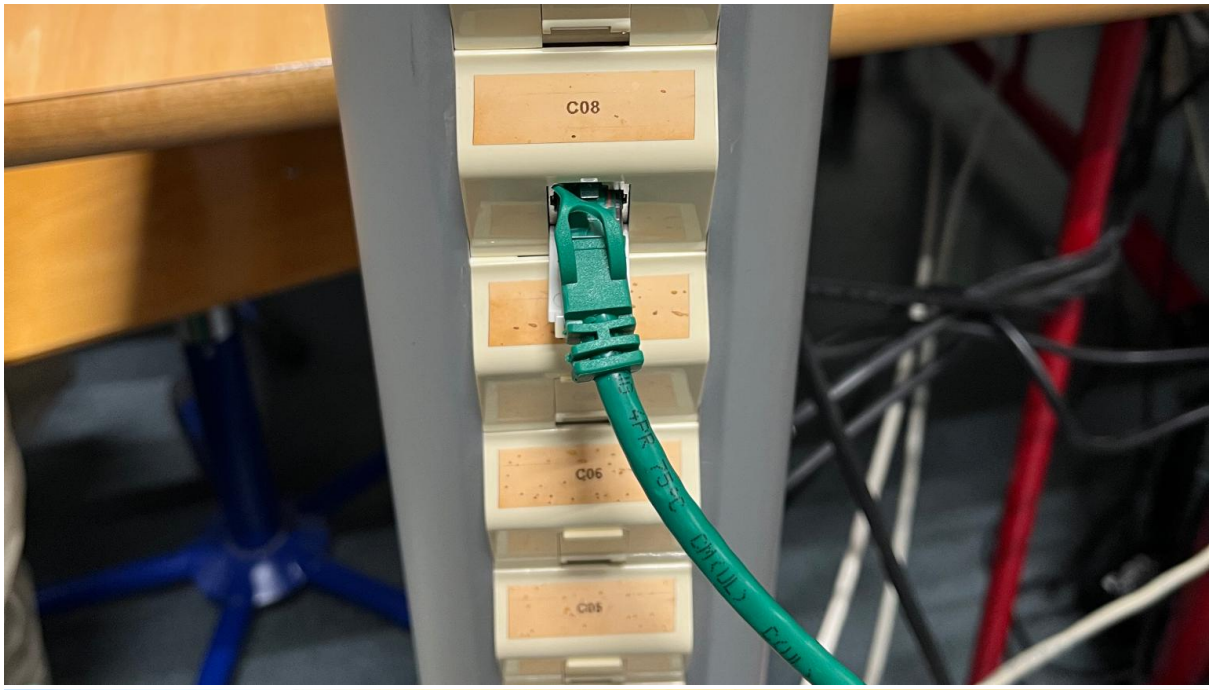
```
PS C:\WINDOWS\System32> ping 192.168.20.1

Envoi d'une requête 'Ping'  192.168.20.1 avec 32 octets de données :
Réponse de 192.168.20.1 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.20.1 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.20.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.20.1 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 192.168.20.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

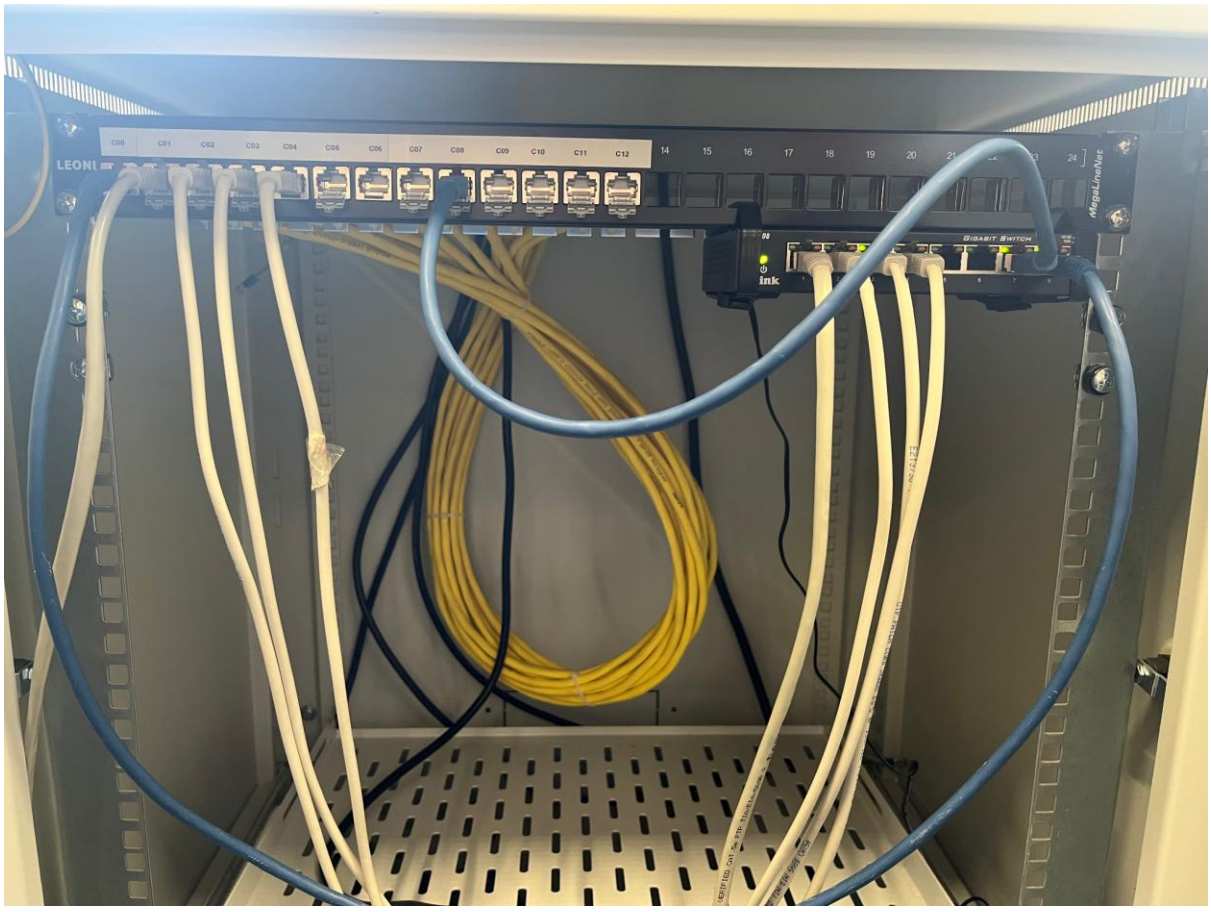
Nous arrivons aussi à pinguer la passerelle :

```
PS C:\WINDOWS\System32> ping 192.168.10.254

Envoi d'une requête 'Ping'  192.168.10.254 avec 32 octets de données :
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=254
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=254
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=254
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=254

Statistiques Ping pour 192.168.10.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

2.2. Configuration du routeur

Dans un deuxième temps, nous allons configurer le routeur. Pour cela, il nous faut le routeur branché à une prise grâce à un câble d'alimentation, à la baie de brassage grâce à un câble Ethernet et il nous faut aussi un câble console pour accéder à la console du switch depuis le PC A ou B. De plus, il faut brancher un câble entre l'interface gi1/0/3 du switch et l'interface gi0/0 du routeur.





Pour configurer le routeur, il faut comme pour le switch, utiliser l’application Putty.

2.2.1. Remise à zéro du routeur

Ensuite, il faut mettre à zéro le routeur. Pour cela, nous allons suivre une certaine procédure.

Tout d'abord, il faut exécuter la commande **write erase**:

```
Router>en
Router#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [con
firm]
[OK]
Erase of nvram: complete
```

Puis, nous entrons la commande **reload**:

```
Router#reload
Proceed with reload? [confirm]

Nov 19 09:48:27.363: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

On répondons ensuite "non", puis "oui" aux questions posées:

```
Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: yes
```

2.2.2. Configuration de la liste de contrôle d'accès (ACL)

Puis, il faut créer une ACL pour autoriser le trafic. Cela se fait avec la commande **access-list 1 permit any**:

```
Router(config)#access-list 1 permit any
```

2.2.3. Configuration du NAT/PAT

Ensuite, nous allons configurer le NAT (Network Address Translation).

Tout d'abord, il faut entrer sur l'interface gi0/0 avec **int gi0/0**. Puis, il faut associer une adresse IP à cette interface avec **ip address 192.168.30.253 255.255.255.0**. Ensuite, il faut indiquer **ip nat inside** (côté réseau privé). Enfin, il faut activer l'interface avec **no shutdown**.

```
Router(config)#int gi0/0
Router(config-if)#ip address 192.168.30.253 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
```

Ensuite, il faut reproduire les mêmes commandes, mais adaptées à l'interface gi0/1. Il faut donc entrer sur l'interface gi0/1 avec **int gi0/1**. Puis, il faut associer une adresse IP à cette interface avec **ip address 192.168.211.175 255.255.255.0**. Ensuite, il faut indiquer **ip nat outside** (côté réseau public/internet). Enfin, il faut activer l'interface avec **no shutdown**.

```
Router(config)#int gi0/1
Router(config-if)#ip address 192.168.211.175 255.255.255.0
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
```

Puis, il faut configurer le PAT (Port Address Translation) avec la commande **ip nat inside source list 1 interface gi0/1 overload**:

```
Router(config)#ip nat inside source list 1 interface gi0/1 overload
```

Enfin, il faut sauvegarder la configuration avec **copy run start**:

```
Router(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.2.4. Ajout des routes

A présent, il faut entrer les différentes routes.

La première route à ajouter est celle par défaut vers internet. Pour cela, il faut exécuter **ip route 0.0.0.0 0.0.0.0 192.168.211.254**:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.211.254
```

Puis, il est nécessaire d'ajouter une route pour chaque VLAN :

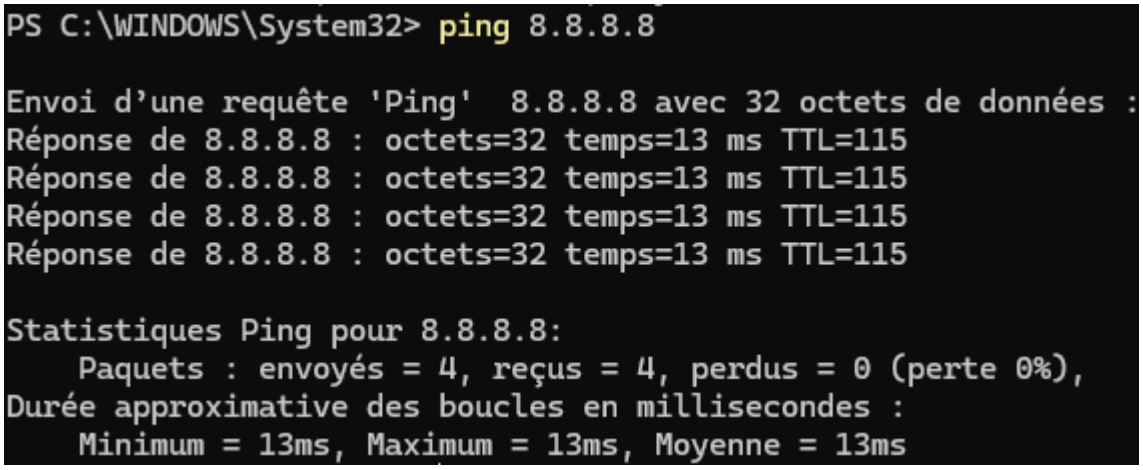
```
Router(config)#ip route 192.168.10.0 255.255.255.0 192.168.30.254
Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.254
Router(config)#ip route 192.168.40.0 255.255.255.0 192.168.30.254
```

Nous faisons encore **copy run start** pour enregistrer la configuration :

```
Router(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.2.5. Test de la configuration

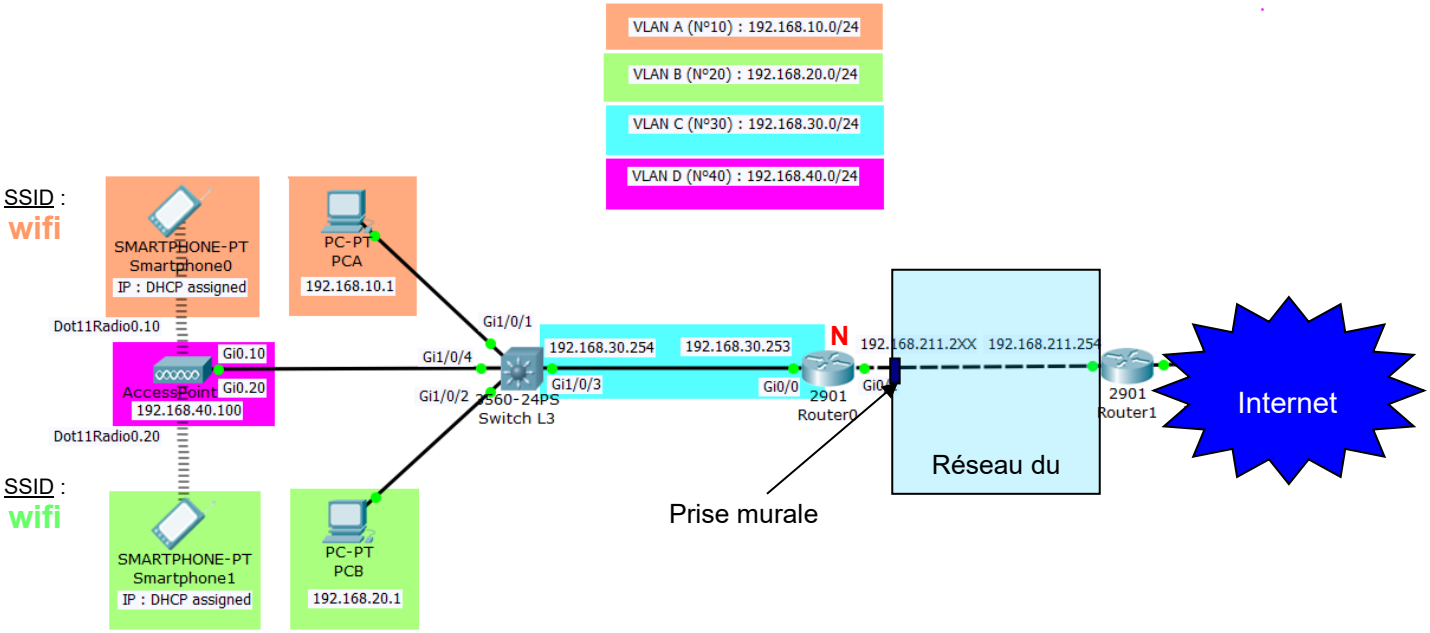
Pour vérifier que tout fonctionne correctement, nous pouvons exécuter **ping 8.8.8.8**. Le ping fonctionne, donc nous avons bien accès à internet:



Dans le cas où le ping ne marche pas, il nous faut regarder si l'on ping notre passerelle.

3. Deuxième partie du TP

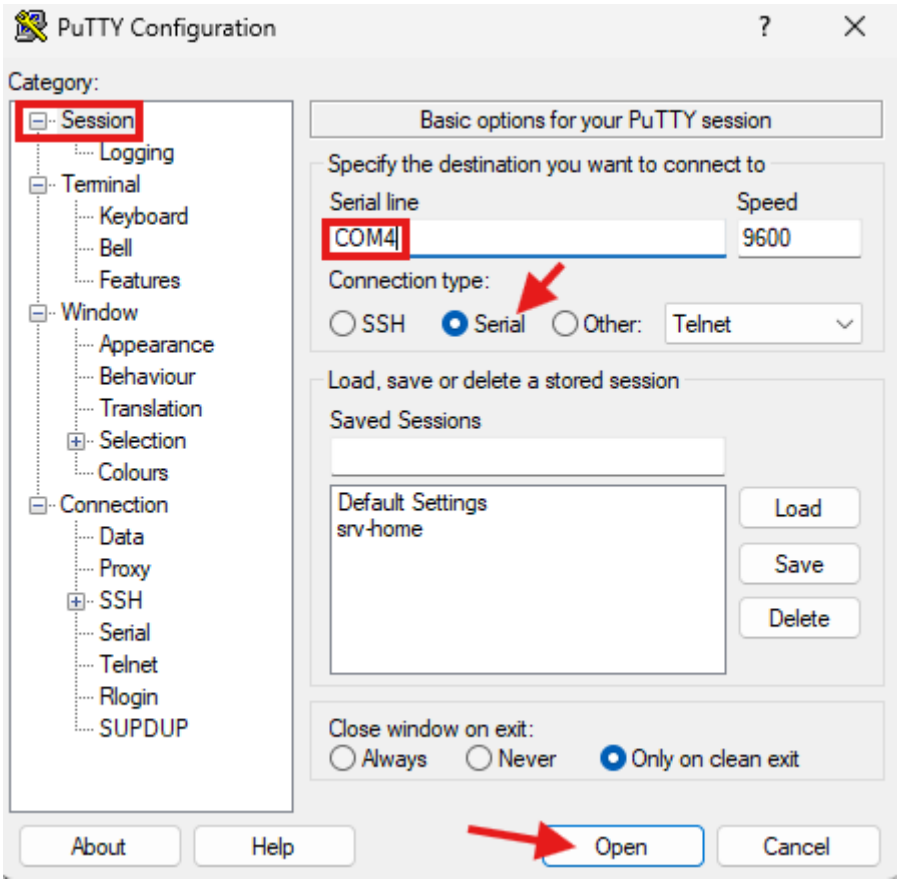
Dans la deuxième partie du TP, nous garderons la même infrastructure que pour la première partie du TP, mais nous ajouterons une bonne Wifi dans un VLAN D (n°40). Cette borne wifi proposera un wifi A et un wifi B. Les dispositifs qui s'y connecteront obtiendront une adresse IP en DHCP, en fonction du wifi A ou B.



3.1. Configuration du switch de niveau 3

Dans un premier temps, nous allons configurer le switch de niveau 3 installé dans la première partie du TP.

Pour le configurer, il faut toujours utiliser l'application Putty, puis dans "Session" sélectionner le bon port COM après avoir choisi « serial »:



3.1.1. Création du VLAN

Tout d'abord, nous nous chargeons de la création du VLAN 40. Pour cela, nous entrons la commande **en**, puis **conf ter**. Ensuite, nous entrons **vlan 40**, puis **name D**, qui est le nom du VLAN:

```
Switch(config)#vlan 40
Switch(config-vlan)#name D
Switch(config-vlan)#exit
```

3.1.2. Configuration de l'interface virtuelle

Puis, nous configurons l'interface virtuelle du switch. Pour cela, il faut entrer sur l'interface avec **int vlan 40**, puis entrer **ip address 192.168.40.254 255.255.255.0**:

```
Switch(config)#int vlan 40
Switch(config-if)#ip address 192.168.40.254 255.255.255.0
```

3.1.3. Configuration du port physique

Ensuite, nous configurons le port physique du switch. Pour cela, il faut entrer sur le port avec **int gi1/0/4**, puis entrer **switchport access vlan 40** et enfin **switchport mode access**:

```
Switch(config)#int gi1/0/4
Switch(config-if)#switchport access vlan 40
Switch(config-if)#switchport mode access
```

3.1.4. Activation du trunk

Etant donné que plusieurs VLAN vont devoir passer par le même port physique, il nous faut activer le mode trunk sur ce port. Pour cela, il faute entrer la commande **switchport mode trunk** puis **switchport trunk native vlan 40**:

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 40
```

Il faut également activer le mode trunk sur le port gi1/0/13, car plusieurs VLAN vont également le traverser. Les commandes sont les mêmes, mais il faut d'abord entrer **int gi1/0/13** pour entrer sur l'interface:

```
Switch(config)#int gil/0/13
Switch(config-if)#switchport trunk native vlan 40
Switch(config-if)#switchport mode trunk
```

Enfin, il faut sauvegarder la configuration avec **copy run start**:

```
Switch(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

3.1.5. Configuration du DHCP

Tout d'abord, il faut créer le pool DHCP pour le VLAN 10 avec la commande **ip dhcp pool pool10**. Ensuite, il faut indiquer le réseau à partir duquel les adresses vont être distribuées avec la commande **network 192.168.10.0 255.255.255.0**. Puis, il faut exécuter la commande **dns-server 8.8.8.8** pour indiquer le serveur DNS, qui sera celui de Google dans notre cas. Enfin, on indique la passerelle par défaut avec **default-router 192.168.10.254**.

```
Switch(config)#ip dhcp pool pool10
Switch(dhcp-config)#network 192.168.10.0 255.255.255.0
Switch(dhcp-config)#dns-server 8.8.8.8
Switch(dhcp-config)#default-router 192.168.10.254
```

On entre ensuite les mêmes commandes en les adaptant au VLAN 20:

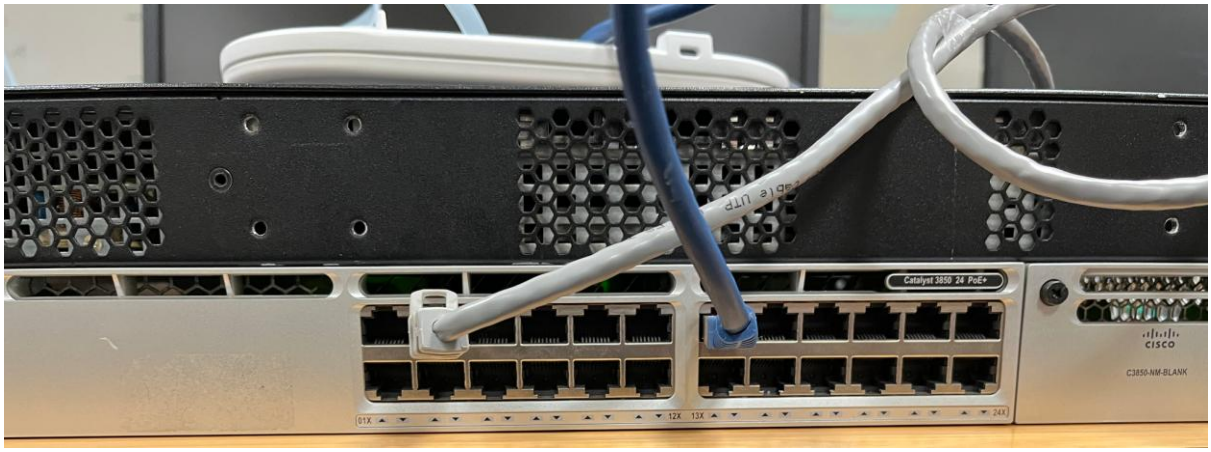
```
Switch(config)#ip dhcp pool pool20
Switch(dhcp-config)#network 192.168.20.0 255.255.255.0
Switch(dhcp-config)#dns-server 8.8.8.8
Switch(dhcp-config)#default-router 192.168.20.254
```

Enfin, il faut sauvegarder la configuration avec **copy run start**:

```
Switch(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

3.2. Configuration de la borne WiFi

Une fois le switch configuré, nous allons configurer la borne WiFi. Pour cela, il faut la brancher à un port du switch (gi1/0/13 dans notre cas, car gi1/0/4 ne fonctionne pas) avec un câble Ethernet. La borne va être alimentée en étant branchée au switch, il n'y a donc pas besoin de câble d'alimentation.



Pour la configurer, il faut comme pour le switch, utiliser l’application Putty.

3.2.1. Remise à zéro de la borne

Ensuite, il faut mettre à zéro la borne. Pour cela, nous allons suivre la documentation fournie par Cisco. Pour remettre la borne aux valeurs d’usine, la procédure typique est :

- Débrancher la borne wifi (si elle est déjà connectée à un switch PoE).
- Connecter le câble console à la borne et au PC, puis lancer Putty.
- Appuyer et maintenir enfoncé le bouton MODE de la borne, puis brancher la borne sur un port du switch PoE.
- Maintenir le bouton MODE enfoncé jusqu'à ce que le voyant d'état devienne orange, puis relâcher le bouton.
- Redémarrer le point d'accès en effectuant un cycle d'alimentation (éteindre puis rallumer).
- Depuis Putty, accéder à la borne avec le nom d'utilisateur et le mot de passe qui sont **Cisco** avec un «**C**» majuscule (sensible à la casse).

3.2.2. Configuration de l'interface virtuelle BVI

D'abord, il faut configurer l'interface virtuelle BVI. Pour cela, il faut entrer sur l'interface avec **int BVI 1**. Puis, assigner une adresse à cette interface avec **ip address 192.168.40.100 255.255.255.0**. Ensuite, il faut activer l'interface avec **no shutdown**. Enfin, il faut définir la passerelle par défaut du dispositif (qui est la dernière adresse utilisable du VLAN D) avec **ip default-gateway 192.168.40.254**.

```
ap#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#int BVI 1
ap(config-if)#ip address 192.168.40.100 255.255.255.0
ap(config-if)#no shutdown
ap(config-if)#exit
ap(config)#ip default-gateway 192.168.40.254
```

3.2.3. Création des SSID sur le point d'accès et mappage d'un SSID à chaque VLAN

Ensuite, il nous faut passer à la création des SSID sur le point d'accès et au mappage d'un SSID à chaque VLAN.

Comme nous souhaitons deux WiFi, il est nécessaire d'exécuter les commandes suivantes pour le WiFi A, puis le WiFi B.

Tout d'abord, il faut entrer **dot11 ssid [nom du wifi]** pour entrer en mode de configuration du SSID spécifié. Puis, entrer **vlan [numéro du vlan]** pour associer le SSID au VLAN. Ensuite, il faut entrer **authentication open** pour spécifier que l'authentification se fait en mode open (pas d'authentification avant le chiffrement WPA) et **authentication key-management wpa version 2** pour activer la gestion des clés WPA version 2 (WPA2). Puis, il faut exécuter **wpa-psk ascii [mot de passe]** pour définir la clé pré-partagée en format ASCII (texte lisible). Enfin, il faut entrer **mbssid guest-mode** pour activer le mode invité pour ce SSID dans la configuration MBSSID.

Pour le Wifi A cela donne:

```
ap(config)#dot11 ssid wifiA
ap(config-ssid)#vlan 10
ap(config-ssid)#authentication open
ap(config-ssid)#authentication key-management wpa version 2
ap(config-ssid)#wpa-psk ascii jesuisenbtssio
ap(config-ssid)#mbssid guest-mode
ap(config-ssid)#exit
```

Pour le Wifi B:

```
ap(config)#dot11 ssid wifiB
ap(config-ssid)#vlan 20
ap(config-ssid)#authentication open
ap(config-ssid)#authentication key-management wpa version 2
ap(config-ssid)#wpa-psk ascii jesuisenbtssio2
ap(config-ssid)#mbssid guest-mode
ap(config-ssid)#exit
```

3.2.4. Configuration de l'interface radio du point d'accès et mappage des SSID à cette interface radio

Ensuite, il nous faut passer à la configuration de l'interface radio du point d'accès et au mappage des SSID à cette interface radio.

Tout d'abord, il faut entrer **int dot11radio0** pour entrer sur l'interface radio. Puis, entrer **mbssid** pour activer le mode Multiple BSSID et permettre de diffuser plusieurs réseaux WiFi (SSID) simultanément sur la même interface radio physique. Ensuite, il faut entrer **encryption vlan 10 mode ciphers aes-ccm** pour configurer le chiffrement pour le vlan 10 et **ssid wifiA** pour créer le WiFi A, c'est le nom que verront les utilisateurs souhaitant se connecter. Puis, il faut exécuter ces deux mêmes commandes, mais pour le Wifi B: **encryption vlan 20 mode ciphers aes-ccm** et **ssid wifiB.** Enfin, il faut entrer **channel least-congested 1 6 11** pour que le canal radio le moins chargé soit sélectionné automatiquement et **no-shutdown** pour activer l'interface radio.

```
ap(config)#int dot11radio0
ap(config-if)#mbssid
ap(config-if)#encryption vlan 10 mode ciphers aes-ccm
ap(config-if)#ssid wifiA
ap(config-if)#encryption vlan 20 mode ciphers aes-ccm
ap(config-if)#ssid wifiB
ap(config-if)#channel least-congested 1 6 11
ap(config-if)#no shutdown
```

3.2.5. Configuration d'une sous-interface Ethernet et d'une sous-interface radio pour chaque VLAN sur le point d'accès

Puis, il nous faut passer à la configuration d'une sous-interface Ethernet et d'une sous-interface radio pour chaque VLAN sur le point d'accès.

Tout d'abord, il faut entrer **bridge [numéro du VLAN] protocol ieee** pour créer un pont utilisant le protocole IEEE (Spanning Tree Protocol). Puis, entrer **bridge [numéro du VLAN] route ip** pour activer le routage pour le pont. Ensuite, il faut entrer **int Dot11Radio0.[numéro du VLAN]** pour entrer sur la sous-interface de l'interface radio et **encapsulation dot1Q [numéro du VLAN]** pour activer le taggage des trames. Puis, il faut exécuter **bridge-group [numéro du VLAN]** pour associer l'interface au pont créé**.** Ensuite, il faut entrer **int Gi0.[numéro du VLAN]** pour entrer sur la sous-interface du port Gigabit Ethernet 0, puis **encapsulation dot1Q [numéro du VLAN]** pour activer le taggage des trames. Enfin, il faut exécuter la commande **bridge-group [numéro du VLAN]** pour associer cette sous-interface au pont créé.

Pour le VLAN 10 cela donne:

```
ap(config)#bridge 10 protocol ieee
ap(config)#bridge 10 route ip
ap(config)#int Dot11Radio0.10
ap(config-subif)#encapsulation dot1Q 10
ap(config-subif)#bridge-group 10
ap(config-subif)#exit
ap(config)#int Gi0.10
ap(config-subif)#encapsulation dot1Q 10
ap(config-subif)#bridge-group 10
ap(config-subif)#exit
```

Pour le VLAN 20:

```
ap(config)#bridge 20 protocol ieee
ap(config)#bridge 20 route ip
ap(config)#int Dot11Radio0.20
ap(config-subif)#encapsulation dot1Q 20
ap(config-subif)#bridge-group 20
ap(config-subif)#exit
ap(config)#int Gi0.20
ap(config-subif)#encapsulation dot1Q 20
ap(config-subif)#bridge-group 20
ap(config-subif)#exit
```

Enfin, il faut sauvegarder la configuration avec **copy run start**:

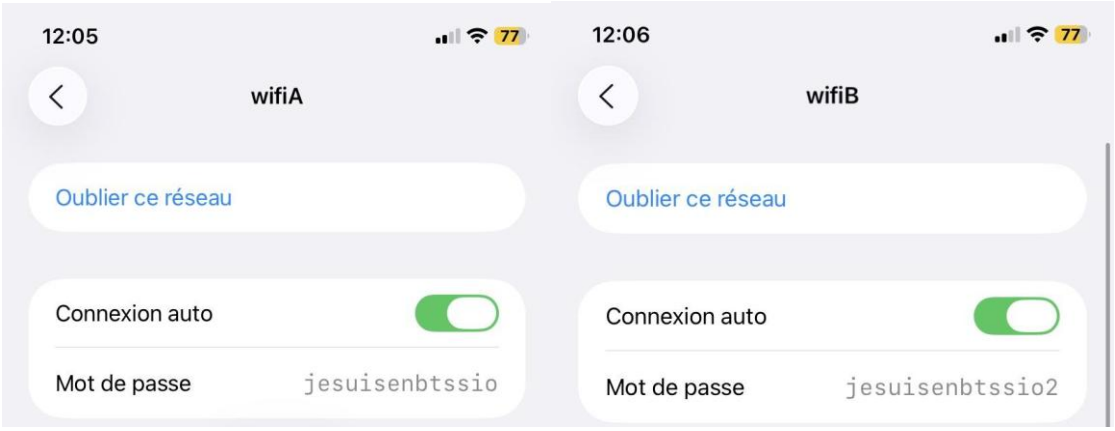
```
ap(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Il ne reste plus qu'à se connecter au WiFi.

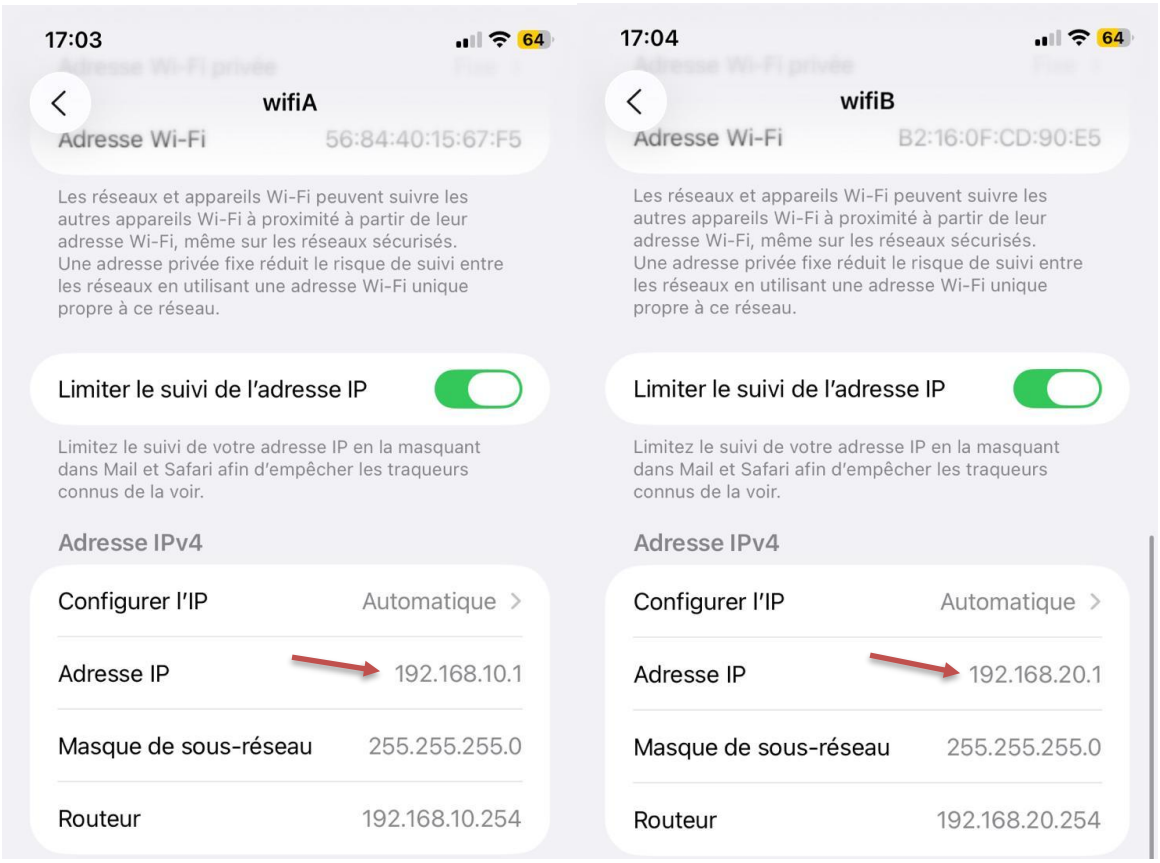
3.2.6. Connexion au WiFi

Pour tester la connexion au WiFi, il suffit de se munir d'un smartphone et de chercher les WiFi disponibles. On observe que les WiFi *wifiA* et *wifiB* apparaissent bien:

Si l'on souhaite s'y connecter, il suffit d'utiliser les mots de passe définis lors de la configuration de la borne:



En se connectant aux WiFi, on peut observer que pour le *wifiA*, on obtient une adresse IP du VLAN 10 et pour le *wifiB,* on obtient une adresse IP du VLAN 20:



4. Annexes

Ayant eu quelques problèmes avec le switch qui n'avait pas sauvegardé sa configuration, garder une trace de celle-ci nous a permis de ne pas perdre de temps et de reconfigurer le switch rapidement. Les annexes suivantes présentent donc les configurations complètes des trois dispositifs utilisés dans ce projet.

4.1. Configuration du switch

```
ip routing
!
ip dhcp pool pool10
 network 192.168.10.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.10.254
!
ip dhcp pool pool20
 network 192.168.20.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.20.254
!
```

```
login on-success log
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1
6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD
230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
       quit
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
redundancy
 mode sso
!
transceiver type all
 monitoring
```

```
!
class-map match-any system-cpp-police-topology-control
  description Topology control
class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data, LOGGING
class-map match-any system-cpp-default
  description Inter FED, EWLC control, EWLC data
class-map match-any system-cpp-police-sys-data
  description Learning cache ovfl, High Rate App, Exception, EGR Exception, NFL SAMPLED DATA, RPF Failed
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-multicast
  description Transit Traffic and MCAST Data
class-map match-any system-cpp-police-l2-control
  description L2 control
class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual
class-map match-any non-client-nrt-class
class-map match-any system-cpp-police-routing-control
  description Routing control and Low Latency
class-map match-any system-cpp-police-protocol-snooping
  description Protocol snooping
class-map match-any system-cpp-police-dhcp-snooping
  description DHCP snooping
class-map match-any system-cpp-police-system-critical
  description System Critical and Gold Pkt
!
policy-map system-cpp-policy
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 negotiation auto
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
```

```
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport trunk native vlan 40
 switchport mode trunk
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
 switchport trunk native vlan 40
 switchport mode trunk
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
```

```
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface TenGigabitEthernet1/1/3
!
interface TenGigabitEthernet1/1/4
!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 192.168.10.254 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.254 255.255.255.0
!
interface Vlan30
 ip address 192.168.30.254 255.255.255.0
!
interface Vlan40
 ip address 192.168.40.254 255.255.255.0
!
ip forward-protocol nd
ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.30.253
!
control-plane
 service-policy input system-cpp-policy
!
line con 0
 stopbits 1
```

```
line aux 0
 stopbits 1
line vty 0 4
 login
line vty 5 15
 login
!
end
```

4.2. Configuration du routeur

```
Current configuration : 1564 bytes
!
! No configuration change since last restart
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ipv6 cef
ip source-route
ip cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
license udi pid CISCO2901/K9 sn FCZ160590VG
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.30.253 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
```

```
interface GigabitEthernet0/1
 ip address 192.168.211.175 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip route 0.0.0.0 0.0.0.0 192.168.211.254
ip route 192.168.10.0 255.255.255.0 192.168.30.254
ip route 192.168.20.0 255.255.255.0 192.168.30.254
ip route 192.168.40.0 255.255.255.0 192.168.30.254
!
access-list 1 permit any
!
control-plane
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

4.3. Configuration de la borne WiFi

```
Current configuration : 3026 bytes
!
! Last configuration change at 00:56:48 UTC Fri Mar 1 2002
version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
logging rate-limit console 9
enable secret 5 $1$60Jf$hRpx2vSyjySoMX3mx6znq0
!
no aaa new-model
no ip source-route
no ip cef
!
dot11 pause-time 100
dot11 syslog
!
dot11 ssid wifiA
   vlan 10
   authentication open
   authentication key-management wpa version 2
   mbssid guest-mode
   wpa-psk ascii 7 0501031C34455D0C1707030118050B
!
dot11 ssid wifiB
   vlan 20
   authentication open
   authentication key-management wpa version 2
   mbssid guest-mode
   wpa-psk ascii 7 130F12011E05172F25263C20262B1C55
!
no ipv6 cef
!
username Cisco password 7 032752180500
!
bridge irb
!
interface Dot11Radio0
 no ip address
 !
 encryption vlan 10 mode ciphers aes-ccm
 !
```

```
 encryption vlan 20 mode ciphers aes-ccm
 !
 ssid wifiA
 !
 ssid wifiB
 !
 antenna gain 0
 mbssid
 channel least-congested 2412 2437 2462
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.10
 encapsulation dot1Q 10
 bridge-group 10
 bridge-group 10 subscriber-loop-control
 bridge-group 10 spanning-disabled
 bridge-group 10 block-unknown-source
 no bridge-group 10 source-learning
 no bridge-group 10 unicast-flooding
!
interface Dot11Radio0.20
 encapsulation dot1Q 20
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 spanning-disabled
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
!
interface Dot11Radio1
 no ip address
 shutdown
 antenna gain 0
 peakdetect
 no dfs band block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
```

```
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.10
 encapsulation dot1Q 10
 bridge-group 10
 bridge-group 10 spanning-disabled
 no bridge-group 10 source-learning
!
interface GigabitEthernet0.20
 encapsulation dot1Q 20
 bridge-group 20
 bridge-group 20 spanning-disabled
 no bridge-group 20 source-learning
!
interface BVI1
 mac-address 1cdf.0f12.fe21
 ip address 192.168.40.100 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
ip default-gateway 192.168.40.254
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
bridge 1 route ip
bridge 10 protocol ieee
bridge 10 route ip
bridge 20 protocol ieee
bridge 20 route ip
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```