Mantel Nans

Danfakha Abdou

BTS SIO 2

TP LAB 1 : Montage d'un réseau avec un switch L3 et un routeur Cisco

SOMMAIRE

I.Définitions

1.1.Switch de Niveau 3 (L3)

C'est un **commutateur qui possède des fonctionnalités de routage**. Contrairement à un switch classique, il est capable d'interconnecter différents réseaux locaux (VLANs) et de gérer le trafic entre eux sans avoir besoin d'un routeur externe pour chaque saut.

1.2.VLAN (Virtual Local Area Network)

Il s'agit d'un **réseau local virtuel qui permet de segmenter un même commutateur physique en plusieurs réseaux logiques indépendants**. Dans votre TP, vous utilisez les VLANs 10, 20 et 40 pour séparer les flux (utilisateurs A, utilisateurs B et management).

1.3.NAT (Network Address Translation)

C'est le mécanisme configuré sur le routeur pour **traduire les adresses privées de vos VLANs en une seule adresse publique (192.168.211.XXX)**. Cela permet à tous les équipements du réseau local d'accéder à Internet via une interface unique.

1.4.Mode Trunk (802.1Q)

C'est une **configuration de port** (utilisée sur le port Gi1/0/4) **qui permet de faire passer le trafic de plusieurs VLANs sur un seul câble physique**. C'est ce qui permet à votre borne WiFi de gérer plusieurs réseaux (SSID) en même temps.

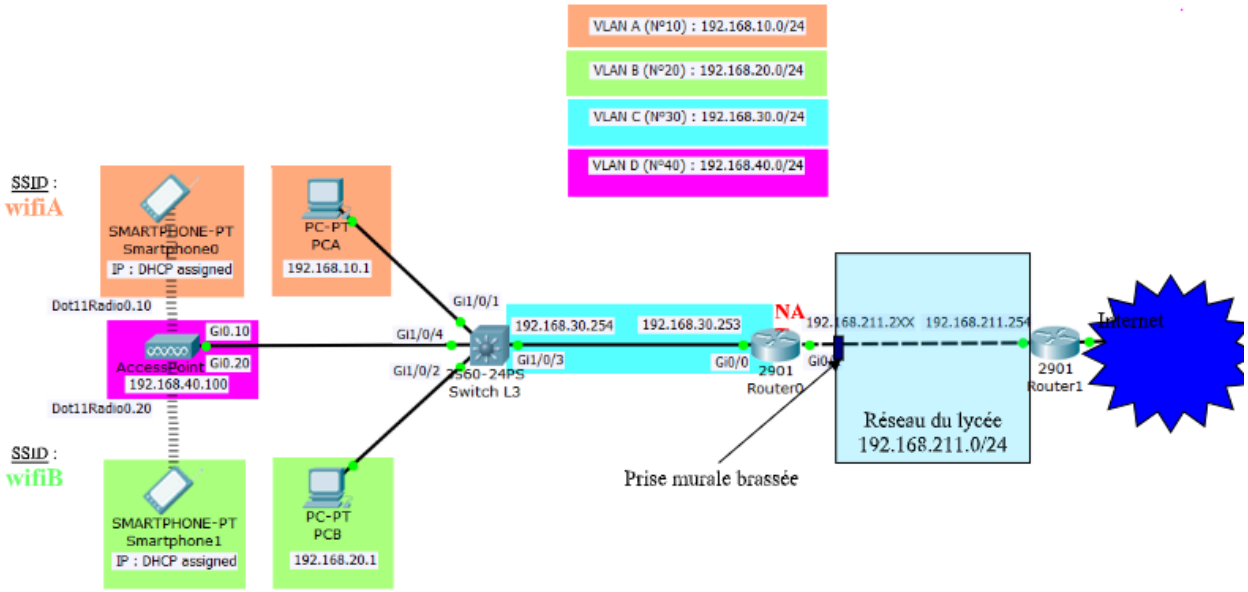
1.5.PoE (Power over Ethernet)

Technologie qui **permet d'envoyer l'alimentation électrique nécessaire à la borne WiFi directement par le câble réseau Ethernet**. Sans un switch compatible PoE, votre borne ne pourrait pas fonctionner sans un bloc d'alimentation externe.

II.Objectif du TP

L'objectif de ce TP est de réaliser le montage et la configuration complète d'une infrastructure réseau segmentée par des VLANs, en utilisant un commutateur de Niveau 3 pour le routage inter-VLAN et un routeur Cisco configuré avec le NAT pour assurer l'accès Internet. Il s'agit également de déployer une borne Wi-Fi autonome capable de gérer plusieurs SSID associés à leurs VLANs respectifs, tout en automatisant l'adressage IP via la mise en place de serveurs DHCP sur le switch-routeur.

III.Schéma de l'infrastructure

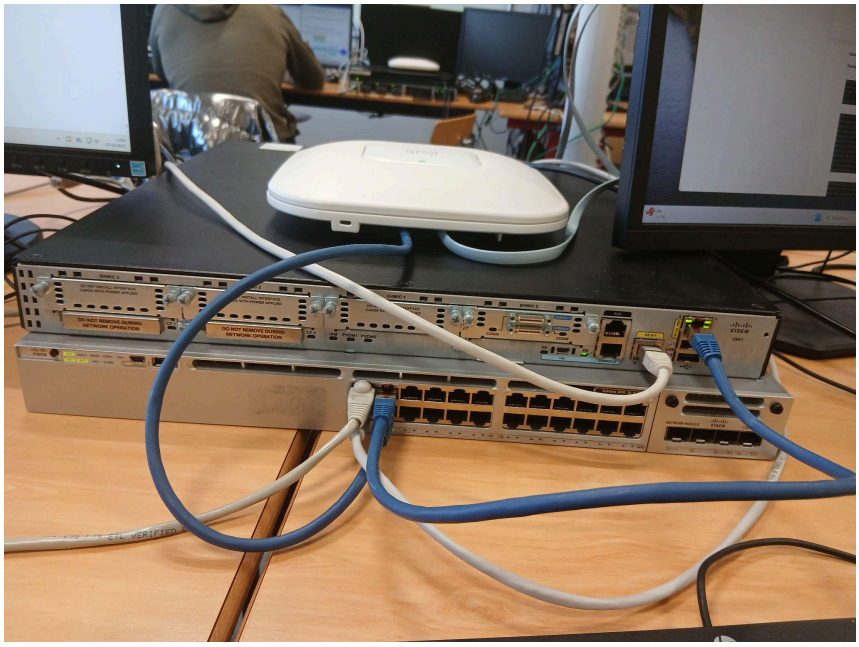


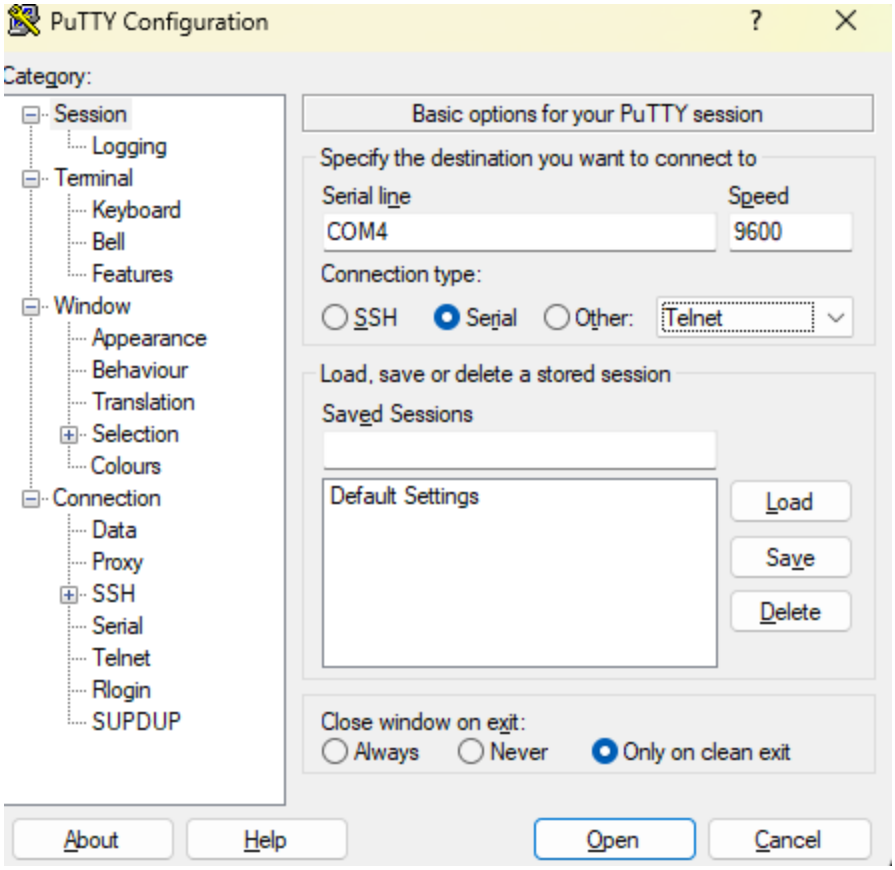
Ce schéma illustre une architecture réseau segmentée en quatre VLANs (10, 20, 30 et 40) où un switch de niveau 3 centralise les connexions filaires (PCA et PCB) et sans fil (borne WiFi) tout en assurant le routage entre ces réseaux. La borne WiFi, alimentée en PoE et configurée via un port Trunk, diffuse deux SSID distincts (wifiA et wifiB) pour intégrer les équipements mobiles dans leurs VLANs

respectifs. Enfin, l'ensemble de la structure est relié à Internet via un routeur Cisco qui assure la traduction d'adresses (NAT) entre le réseau local et le réseau du lycée.

IV.Mise en oeuvre pratique

On a commencé par installer physiquement le matériel en reliant le switch L3 au routeur Cisco et à la borne Wi-Fi, cette dernière étant alimentée directement par le switch grâce au PoE car nous n'avions pas de bloc secteur. Après avoir remis les équipements à zéro pour repartir sur une base propre , on a segmenté le réseau en créant plusieurs VLANs (10, 20, 30 et 40) pour isoler le trafic des différents utilisateurs et de la gestion. Enfin, on a configuré le routeur pour permettre l'accès Internet à tous via le NAT et paramétré la borne pour qu'elle diffuse deux réseaux Wi-Fi distincts (wifiA et wifiB) rattachés à leurs VLANs respectifs.





Maintien du bouton mode, tout en rebrancher l'alimentation

```
Booting...
Interface GE 0 link down***ERROR: PHY link is down

Getting rest of image
Reading full image into memory...Check base package header ...: done = 16384
Getting rest of image
Reading full image into memory....done
Reading full base package into memory...: done = 83293932
Bundle Image
```

Entrer la commande write erase ainsi que delete vlan.dat puis 'reload' pour reboot le switch

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

Après avoir empilé le matériel et relié la borne Wi-Fi au switch L3 via un câble PoE pour l'alimenter directement , nous avons utilisé PuTTY pour configurer les VLANs en ligne de commande. Sur le switch, nous avons créé les réseaux virtuels 10, 20, 30 et 40 , puis assigné chaque port physique (de Gi1/0/1 à Gi1/0/3) à son VLAN correspondant afin d'isoler le trafic des PC et du routeur selon le schéma réseau.

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

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

Pour permettre la communication entre nos différents réseaux, nous avons configuré des adresses IP sur les interfaces virtuelles de chaque VLAN (SVI) afin qu'elles servent de passerelles par défaut pour les PC. Enfin, nous avons activé la fonction de routage sur le switch de niveau 3 avec la commande « ip routing », ce qui autorise enfin les données à circuler librement d'un VLAN à un autre

Affectation adresse IP du à chacun des vlan

192.168.10.254

192.168.20.254

192.168.30.254

Désactiver le pare feu windows

Route par défaut sur switch

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

Configuration des interfaces du routeur

```
Router(config)#int gi0/0
Router(config-if)#ip address 192.168.30.253 255.255.255.0
```

```
Router(config-if)#ip address 192.168.211.173 255.255.255.0
Router(config-if)#
```

```
Router(config)#access-list 1 permit any
Router(config)#int gi0/0
Router(config-if)#ip nat inside

Nov 19 10:29:42.667: %LINEPROTO-5-UPDOWN
ed state to up
Router(config-if)#exi
Router(config)#int gi0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
```

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

Config de l'interface gi1/0/4 du switch pour le vlan 40 de la borne wifi

```
interface GigabitEthernet1/0/4
 switchport mode trunk
!
```

Pour simplifier la connexion des équipements, notamment pour les futurs clients Wi-Fi, nous avons transformé le switch de niveau 3 en serveur DHCP. Nous avons créé des pools d'adresses spécifiques pour chaque VLAN afin que les appareils reçoivent automatiquement une adresse IP, leur masque et l'adresse de leur passerelle dès leur connexion au réseau.

Config dhcp pool

```
ip dhcp pool poolClient
 network 192.168.10.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.10.254
!
ip dhcp pool poolClient2
 network 192.168.20.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.20.254
!
```

Enfin, nous avons configuré le NAT (Network Address Translation) sur le routeur Router0 pour que tous les postes des différents VLANs puissent accéder à Internet. En utilisant l'adresse IP spécifique attribuée à notre groupe (192.168.211.XXX), le routeur traduit désormais les adresses privées internes en une adresse publique autorisée sur le réseau du lycée.

```
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 FCZ160590VE
!
!
!
!
!
!
!
!
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 192.168.211.173 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
```

Pour la partie Wi-Fi, nous avons d'abord isolé la borne dans un VLAN de management (VLAN 40) avec l'adresse IP fixe 192.168.40.100 pour la gérer en toute sécurité. Comme nous n'avions pas de bloc secteur, le switch a fourni l'énergie nécessaire via le câble réseau grâce au **PoE**. Enfin, nous avons configuré deux réseaux sans fil, « wifiA » et « wifiB », pour que les utilisateurs mobiles se connectent directement dans les bons VLANs (10 ou 20) et reçoivent automatiquement leur configuration IP via le serveur DHCP que nous avons mis en place sur le switch.

```
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 192.168.0.0 255.255.0.0 192.168.30.254
!
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
```

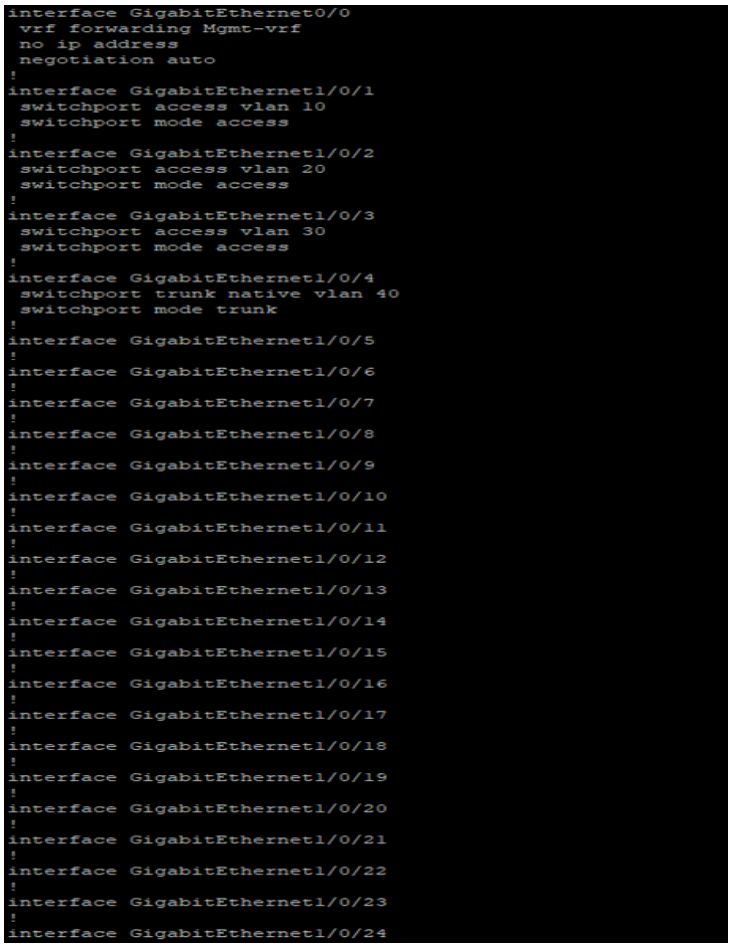
Afin d'automatiser l'attribution des adresses, nous avons configuré le switch L3 en tant que serveur DHCP en créant un « pool » d'adresses pour chaque VLAN. Cette étape est essentielle pour que les futurs clients Wi-Fi des réseaux « wifiA » et « wifiB » obtiennent automatiquement leur adresse IP et les coordonnées de leur passerelle dès leur connexion.

```
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
no aaa new-model
switch 1 provision ws-c3850-24p
!
!
!
!
!
ip routing
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool poolClient
 network 192.168.10.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.10.254
!
ip dhcp pool poolClient2
 network 192.168.20.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.20.254
!
!
qos queue-softmax-multiplier 100
!
!
diagnostic bootup level minimal
spanning-tree mode pvst
spanning-tree extend system-id
hw-switch switch 1 logging onboard message level 3
!
redundancy
 mode sso
!
!
!
class-map match-any non-client-nrt-class
!
!
!
!
```

Pour que les appareils se connectent facilement, nous avons configuré le switch L3 en tant que serveur DHCP. Nous avons créé des pools d'adresses pour chaque VLAN, ce qui permet aux clients Wi-Fi de recevoir automatiquement leur adresse IP, leur masque et l'adresse de leur passerelle dès qu'ils se connectent aux réseaux « wifiA » ou « wifiB ».

```
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
no aaa new-model
switch 1 provision ws-c3850-24p
!
!
!
!
!
ip routing
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool poolClient
 network 192.168.10.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.10.254
!
ip dhcp pool poolClient2
 network 192.168.20.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.20.254
!
!
qos queue-softmax-multiplier 100
!
!
diagnostic bootup level minimal
spanning-tree mode pvst
spanning-tree extend system-id
hw-switch switch 1 logging onboard message level 3
!
redundancy
 mode sso
!
!
!
class-map match-any non-client-nrt-class
!
!
!
!
```

Pour étendre le réseau, nous avons intégré une borne Wi-Fi configurée sur un VLAN de management spécifique (VLAN 40) avec l'adresse IP `192.168.40.100`. Comme nous ne disposions pas de bloc secteur, le switch a alimenté la borne directement via le câble réseau grâce à la technologie PoE. Nous avons ensuite créé deux réseaux sans fil distincts, « wifiA » et « wifiB », rattachés respectivement aux VLANs 10 et 20, pour que les utilisateurs mobiles soient isolés dans les bons réseaux dès leur connexion.



```
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
!
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
```

La capture d'écran suivante montre la console lors de la **réinitialisation matérielle de la borne Wi-Fi**. On y voit le système confirmer que le bouton « MODE » a été maintenu pendant 20 secondes, ce qui déclenche la procédure de récupération pour remettre l'appareil en configuration d'usine. Ce n'est pas un résultat final, mais la preuve que la borne a été correctement « nettoyée » avec son adresse IP par défaut (10.0.0.1) avant que nous ne commencions notre propre configuration.

```
!
interface Vlan1
 no ip address
 shutdown
!
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
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.30.253
!
!
!
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
line vty 5 15
 login
!
wsma agent exec
 profile httplistener
 profile httpslistener
!
wsma agent config
 profile httplistener
 profile httpslistener
!
wsma agent filesys
 profile httplistener
 profile httpslistener
!
wsma agent notify
 profile httplistener
 profile httpslistener
!
!
wsma profile listener httplistener
 transport http
!
wsma profile listener httpslistener
```

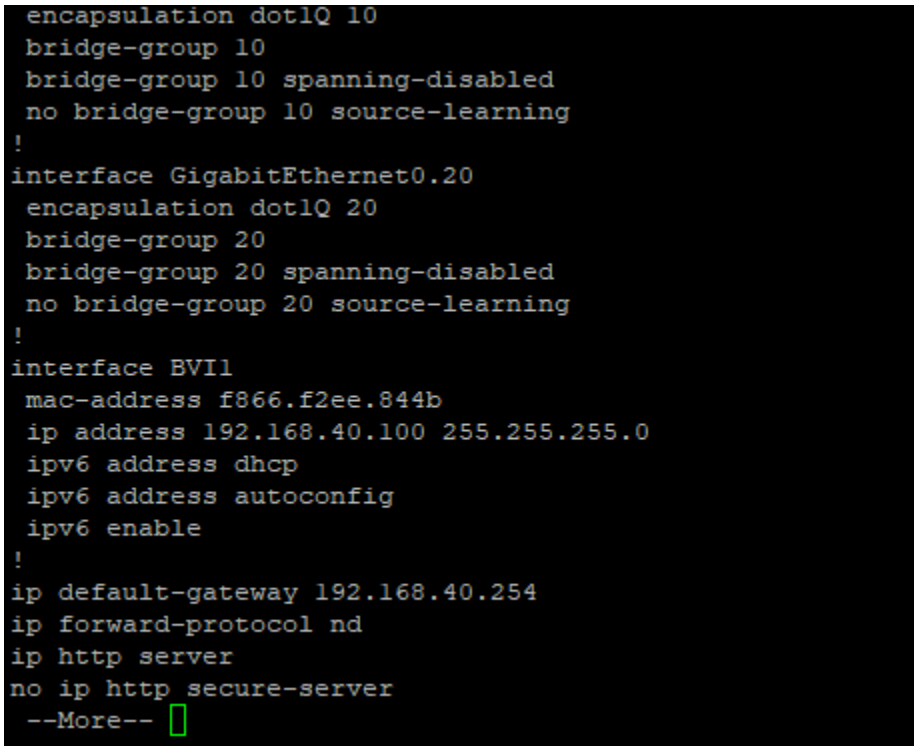
Dans la capture suivante, nous observons la configuration d'une borne Cisco gérant deux réseaux Wi-Fi distincts, wifiA et wifiB, isolés respectivement sur les VLAN 10 et 20. Nous avons sécurisé ces accès avec le protocole WPA2 et configuré l'interface radio pour qu'elle sélectionne automatiquement le canal le moins encombré afin d'optimiser les performances. Ce paramétrage nous permet de segmenter proprement le trafic réseau tout en assurant une liaison stable vers notre infrastructure filaire via les groupes de pontage.

```
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$AbZn$8yomEZ9kY8nxT.IJiQdLC0
!
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 094F471A1A0A19130F0516
!
dot11 ssid wifiB
   vlan 20
   authentication open
   authentication key-management wpa version 2
   mbssid guest-mode
   wpa-psk ascii 7 045802150C2E424F0D1017
!
!
!
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
 --More--
```

Dans la capture suivante, nous observons la partie technique qui fait le pont entre les ondes Wi-Fi et le réseau filaire : nous avons configuré des sous-interfaces spécifiques pour les VLAN 10 et 20 afin de garantir que le trafic reste parfaitement séparé jusqu'au switch. Enfin, nous retrouvons l'interface BVI1 avec l'adresse IP `192.168.40.100`, qui est l'adresse de gestion que nous utilisons pour administrer la borne à distance.

```
 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 f866.f2ee.844b
 ip address 192.168.40.100 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
```

Dans la capture suivante, nous détaillons la configuration des interfaces logiques qui font le pont entre les ondes Wi-Fi et le réseau filaire. Nous avons mis en place des sous-interfaces pour les VLAN 10 et 20 afin de lier chaque SSID à son réseau respectif via des "bridge-groups", garantissant ainsi une isolation totale du trafic. Enfin, nous définissons l'interface de gestion BVI1 avec l'adresse IP `192.168.40.100` et sa passerelle par défaut (`.254`), ce qui nous permet de garder le contrôle sur la borne et de l'administrer à distance.



V.Conclusion

Pour conclure, ce TP a été une réussite puisque toute l'architecture réseau est fonctionnelle. Après avoir configuré le routage, le DHCP et le NAT, nous avons pu vérifier que les différents équipements communiquaient bien entre eux. Le point le plus positif est que la borne Wi-Fi est parfaitement opérationnelle : nous avons réussi à nous connecter aux deux réseaux sans fil (**wifiA** et **wifiB**) et à naviguer sur Internet sans aucun problème.