PROMÉO
BEAUVAIS

PPE-1

INFRASTRUCTURE RÉSEAU

Pauline JIMENEZ
BTS SIO 26

pauline.jimenez.etude@gmail.com

https://pjimenez.promeo-capnumerique.fr/?page_id=177

SOMMAIRE :

Situation initiale

L’entreprise JIM dispose actuellement d’un réseau entièrement filaire, sans segmentation logique entre les différents services.

Cette architecture limite la mobilité des employés et ne permet pas une gestion optimisée du réseau.

L’entreprise souhaite mettre en place une infrastructure Wi-Fi interne afin de permettre aux collaborateurs de se déplacer sur le site tout en restant connectés au réseau.

Comment déployer et administrer une borne point d’accès autonome afin d’intégrer un réseau Wi-Fi interne sécurisé et segmenté au sein de l’infrastructure existante ?

Problématique

La problématique est donc la suivante :

Comment déployer et administrer une borne point d'accès autonome afin d'intégrer un réseau Wi-Fi interne sécurisé et segmenté au sein de l'infrastructure existante ?

Matériel

Pour ce projet nous aurons besoin :

- Un routeur Cisco
- un switch Cisco
- un point d'accès wifi autonome
- Un ordinateur portable
- Un ordinateur Fixe

Résumé

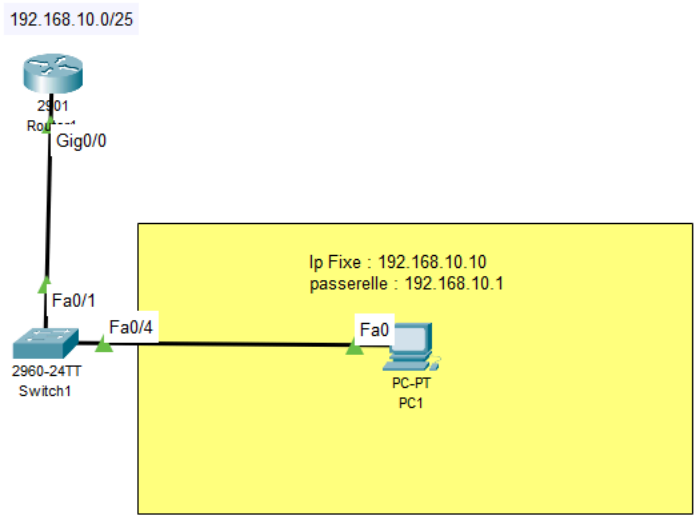
L'ordinateur fixe représente tous les PC de l'entreprise branchés en filaire.

L'ordinateur portable représente les nouveaux ordinateurs portable des employé pour se déplacer dans les bureaux et sur site.

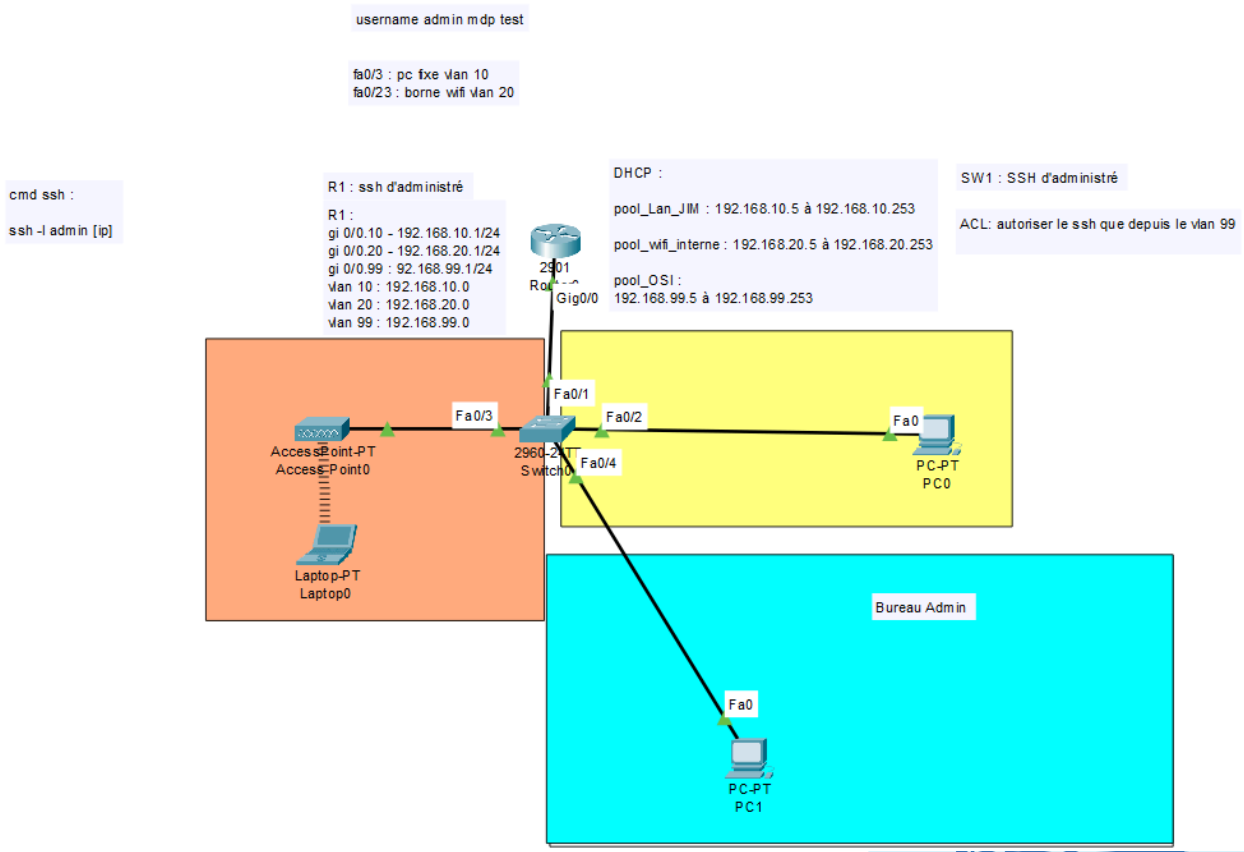
VLAN	NOM	RESEAU	PASSERELLE	UTILISATION
10	Lan_JIM	192.168.10.0	192.168.10.1	PC filaire
20	WIFI_JIM	192.168.20.0	192.168.20.1	Laptop
99	OSI	192.168.99.0	192.168.99.1	administration réseau

Schéma :

- Avant Intervention :



- Après Intervention :



Solution

Configuration du routeur :

Première étape : créer des interfaces virtuelles sur le routeur pour créer nos vlan, ici on utilisera la méthode router-on-Stick.

Deuxième étape : créer le DHCP sur le routeur pour les trois vlan.

Troisième étape : Administrer le SSH sur le routeur.

Quatrième étape : créer une ACL pour n'autoriser que le SSH depuis le VLAN OSI

Cinquième étape : créer les VLANS sur le commutateur pour associer les interfaces virtuelles du routeur aux VLAN du commutateur

Créer l'ACL sur le commutateur pour n'autoriser que le VLAN OSI à accéder en SSH aux équipements

Créer les liaisons : La liaison entre R1 et SW1 seront en mode trunk. Les liaisons entre SW1 et le point d'accès sera en mode accès.

Configurer le point d'accès autonome :.

attribuer une adresse sur l'interface BVI 1
se connecter à la page web
créer le SSID pour se connecter au LAN de manière sécurisée
configurer le SSH

Conclusion

Test :

PC WIFI reçoit une adresse IP via le DHCP
IP : 192.168.20.x
Passerelle : 192.168.20.1

PC connecté en filaire reçoit une adresse IP via le DHCP
IP : 192.168.10.x
Passerelle : 192.168.10.x

Ping PC VLAN10 ↠ PC WIFI VLAN20 : OK

Connexion SSH depuis VLAN10 : refusée
Connexion SSH depuis VLAN99 : autorisée

Depuis l'intervention dans l'entreprise JIM les employés peuvent désormais utiliser des ordinateurs portables et se connecter au réseau via le Wi-Fi tout en conservant l'accès aux ressources internes.

Annexe

Configuration du Routeur :

Confiig de base

```
conf t
hostname R1
exit
banner motd “attention zone interdite”
Service password-encryption
line console 0
password test
login
enable password test
line vty 0 15
password test
login
```

Configuration ssh :

```
ip domain name lan.jim
ip ssh version 2
crypto key generate rsa 1024
username admin priviledge 15 secret test
line vty 0 4
transport input ssh
login local
```

Création des interfaces virtuelles :

```
Conf t
interface gigabitethernet 0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
no shutdown
exit
interface gigabitethernet 0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
no shutdown
exit
interface gigabitethernet 0/0.99
encapsulation dot1q 99
ip addres 192.168.99.1 255.255.255.0
no shutdown
exit
```

activer l’interface physique :

```
interface gigabitetherneto/0
no shutdown
```

attribution d’un ip de management :

```
interface vlan 99
ip address 192.168.99.2 255.255.255.0
no shutdown
```

configuration du DHCP :

```
dhcp service
ip dhcp pool LAN_JIM
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
ip dhcp pool WIFI_JIM
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
ip dhcp pool OSI
network 192.168.99.0 255.255.255.0
default-router 192.168.99.1

ip dhcp excluded-address 192.168.10.1 192.168.10.5
ip dhcp excluded-address 192.168.20.1 192.168.20.5
ip dhcp excluded-address 192.168.99.1 192.168.99.5
```

Configuration d’ACL pour le SSH

```
access list 10 permit 192.168.99.0 0.0.0.255
line vty 0 4
access class 10 in
```

Annexe

Configuration du Switch :

Confiig de base

```
conf t
hostname SW1
exit
banner motd “attention zone interdite”
Service password-encryption
line console 0
password test
login
enable password test
line vty 0 15
password test
login
```

Configuration ssh :

```
ip domain name lan.jim
ip ssh version 2
crypto key generate rsa 1024
username admin priviledge 15  secret test
line vty 0 4
transport input ssh
login local
```

Création de vlan :

```
Conf t
vlan 10
name Lan_JIM
exit
vlan 20
name Wifi
exit
vlan 99
name OSI
exit
```

attribution d’un ip de management :

```
interface vlan 99
ip address 192.168.99.2 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.1
```

configuration des interfaces

```
conf t
interface fastethernet 0/1
switchport mode trunk
swicthport trunk allowed vlan 10,20,99
no shutdown
exit

interface fastethernet 0/22
switchport mode access
swicthport access vlan 10
no shutdown
exit

interface fastethernet 0/23
switchport mode access
swicthport acces vlan 20
no shutdown
exit

interface fastethernet 0/21
switchport mode access
swicthport acces vlan 99
no shutdown
exit
```

Configuration d’ACL pour le SSH

```
access list 10 permit 192.168.99.0 0.0.0.255
line vty 0 4
access class 10 in
```

Annexe

Configuration Cisco Aironet 1130AG

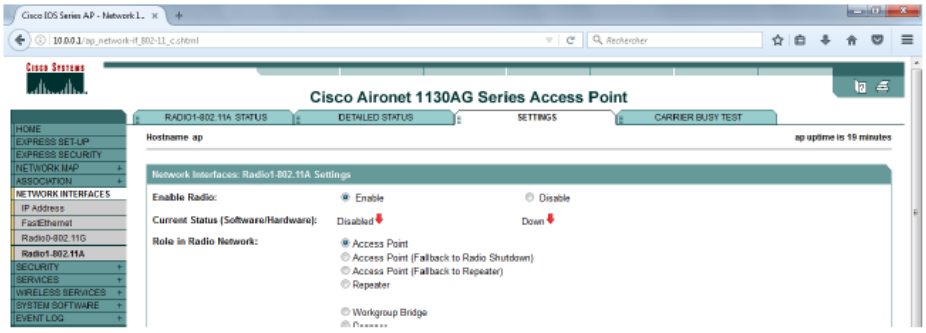
Config de base :

hostname ap1
Line console 0
login
password
enable password
service password-encryption

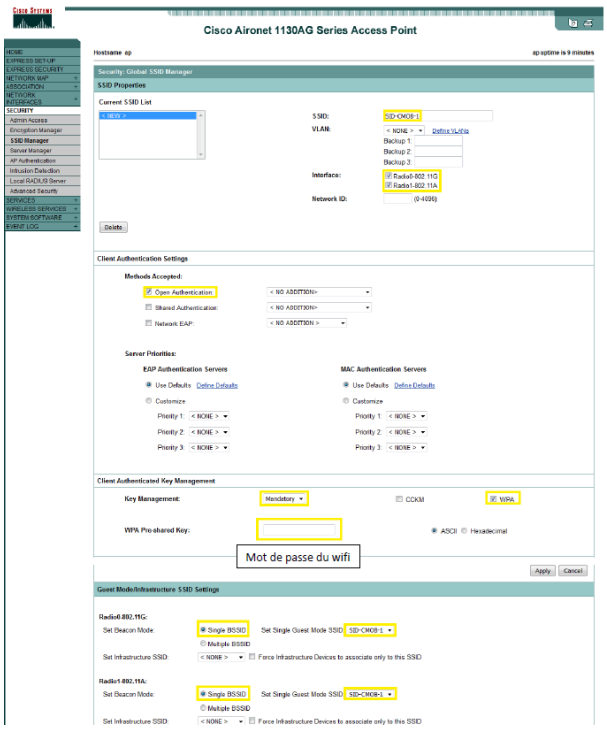
Config de l'interface BVI 1

interface BVI1
 ip address 192.168.99.3 255.255.255.0
 no ip route-cache

Activation des interfaces radio :



Création du SSID :



Config en ligne de commande :

dot11 ssid PPE_interne
 authentication open
 authentication key-management wpa
 guest-mode
 infrastructure-ssid optional
 wpa-psk ascii 7 031451020B0A2F4954

Positionner le SSID sur les interaces radio :

interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 ssid PPE_interne
 station-role root
 beacon privacy guest-mode
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled

ANNEXE

Configuration complète du routeur :

```
R1#sh running-config
Building configuration...

Current configuration : 2410 bytes
!
! Last configuration change at 05:58:18 UTC Mon Feb 16 2026
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable password 7 120D000406
!
no aaa new-model
memory-size iomem 5
!
!
!
!
!
!
!
!
!
!
ip dhcp excluded-address 192.168.10.1 192.168.10.5
ip dhcp excluded-address 192.168.20.1 192.168.20.5
ip dhcp excluded-address 192.168.99.1 192.168.99.5
!
ip dhcp pool LAN_JIM
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
!
ip dhcp pool WIFI_JIM
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
!
ip dhcp pool OSI
 network 192.168.99.0 255.255.255.0
 default-router 192.168.99.1
!
!
!
ip domain name jim.lan
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
!
license udi pid CISCO1941/K9 sn FCZ1545C1UJ
```

```
username admin privilege 15 password 7 120D000406
!
redundancy
!
!
!
!
!
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/0.99
 encapsulation dot1Q 99
 ip address 192.168.99.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 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
!
interface FastEthernet0/1/0
 no ip address
!
interface FastEthernet0/1/1
 no ip address
```

```
interface FastEthernet0/1/1
 no ip address
!
interface FastEthernet0/1/2
 no ip address
!
interface FastEthernet0/1/3
 no ip address
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
access-list 10 permit 192.168.99.0 0.0.0.255
!
control-plane
!
!
banner motd ^C attention zone interdite^C
!
line con 0
 password 7 071B245F5A
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class 10 in
 login local
 transport input ssh
!
scheduler allocate 20000 1000
!
end
```

ANNEXE

Configuration complète du switch :

```
! Last configuration change at 02:59:49 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
enable password 7 044F0E151B
!
username admin password 7 120D0004064B1C16233D2D2436312516474756
no aaa new-model
system mtu routing 1500
!
!
ip domain-name lan.jim
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
!
!
!
!
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20,99
 switchport mode trunk
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
```

```
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
!
interface Vlan99
 ip address 192.168.99.2 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
access-list 10 permit 192.168.99.0 0.0.0.255
!
!
line con 0
 password 7 111D1C1603
 login
line vty 0 4
 access-class 10 in
 password 7 03105E1812
 login
 transport input ssh
line vty 5 15
 login
!
end
```

ANNEXE

Configuration complète du point d'accès :

```
ap1#sh running-config
Building configuration...

Current configuration : 1786 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap1
!
logging rate-limit console 9
enable secret 5 $1$eGye$p.bcM1Y75qnRF8HDQPZVQ1
!
no aaa new-model
ip domain name jim.lan
!
!
no dot11 syslog
!
dot11 ssid PPE_interne
   authentication open
   authentication key-management wpa
   infrastructure-ssid optional
   wpa-psk ascii 7 031451020B0A2F4954
!
dot11 network-map
!
!
username bob privilege 15 secret 5 $1$ZmsW$Vr40Ka5Q6Ojn0cHABg4ZX0
!
!
ip ssh version 2
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid PPE_interne
 !
 station-role root
 beacon privacy guest-mode
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
```

```
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid PPE_interne
 !
 station-role root
 beacon privacy guest-mode
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid PPE_interne
 !
 no dfs band block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.168.20.3 255.255.255.0
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
snmp-server community ppe RO
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
 login local
 transport input ssh
!
end
```