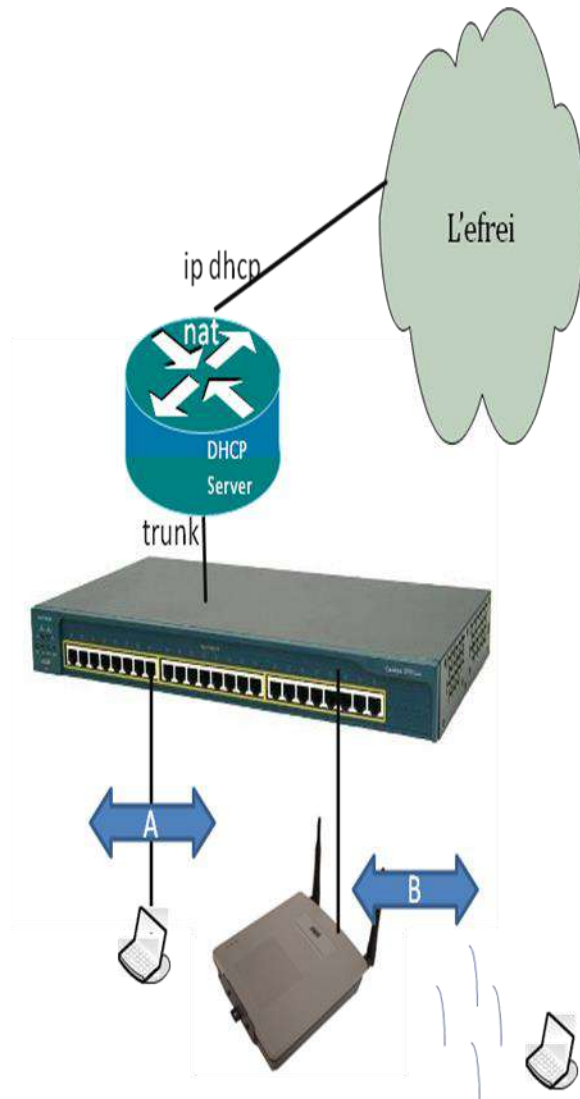


Intégrer un acces wifi pour l'internet dans un réseau d'entreprise**Information :**

Le but de ce TP est d'inclure un PA dans un réseau, on le configurant sur un VLAN, et permettre aux stations mobiles d'accéder à Internet, tout en protégeant le reste du réseau.

Le schéma

Matériel : Un routeur, Un switch, Un PA, des PCs



Logiciels :

Logiciel SolarWinds TFTP server
Logiciel Mib browser
Logiciel Analyseur Wireshark
Logiciel putty

Configuration Aironet, router et switch voir les annexes.

Dans toutes les étapes toutes les configurations seront faites en mode console IOS, voir les annexes.

Etape 1

Faire un plan d'adressage.

Les questions ou les précisions à apporter à ce schéma?

A faire valider par le formateur

Etape 2 (adressage statique)

Après reset configurer Aironet en mode ligne de commande et invalider l'accès web pour des problèmes de sécurité et d'efficacité

Le configurer , en mode authentification Open, SSID votre prénom.

Configurer les postes, puis vérifier l'interopération PA.

Etape 3 (adressage statique)

Configurer le point d'accès pour pouvoir y accéder en telnet

Y accéder depuis un PC, la liaison est elle sécurisée ?

Configurer le PA pour pouvoir y accéder en SSH (putty)

Y accéder depuis un PC, la liaison est elle sécurisée ?

Etape 4 (adressage DHCP)

Configurer le service DHCP sur le router pour permettre aux clients de se connecter.

Configuration du switch

Configuration router

Etape 5

Test connectivité générale quand on est en DHCP

Etape 6

Test verification accès Internet

Etape 7

Sauvegarde des configuration router, switch et PA en utilisant le serveur TFTP servi

Etape 8

Après reset configurer l'aironet en mode authentification WAP, SSID votre nom .

Etape 9

Bloquer le trafic entre les deux réseaux A et B

Annexe : Mise en œuvre aironet

- Réinitialisation à faire systématique au début TP, et entre chaque changement de configuration, la procédure:
Couper le courant, puis à la remise du courant appuyer une dizaine de seconde sur le bouton reset (mode)
- Initialisation du point d'accès

```
ap #conf t
ap(config)#no ip domain-lookup
ap(config)#int bvi1
ap(config-if)#ip address 192.168.10.10 255.255.255.0
ap(config-if)#no shutdown
ap(config-if)#exit
ap(config)#int f 0
ap(config-if)#ip address 192.168.10.11 255.255.255.0
ap(config-if)#no shutdown
ap(config-if)#exit
ap(config)#exit
ap #show ip interface brief
```

ANNEXE :Configuration de base

```

ap #conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#dot11 ssid surf
ap(config-ssid)#guest-mode
ap(config-ssid)#authentication open
ap(config-ssid)#exit
ap(config)#interface dot11Radio 0
ap(config-if)#ssid surf
ap(config-if)#no shutdown
*%LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*%DOT11-6-FREQ_SCAN: Interface Dot11Radio0, Scanning frequencies for 29 seconds
*%DOT11-6-FREQ_USED: Interface Dot11Radio0, frequency 2437 selected
*%LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up
*%DOT11-6-ASSOC: Interface Dot11Radio0, Station 000e.35be.47bf Associated
KEY MGMT[NONE]
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [surf] :
MAC Address      IP address      Device          Name           Parent         State
000e.35be.47bf 192.168.10.252  unknown        -              self           Assoc
ap#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ap#copy running-config tftp:
Address or name of remote host []? 192.168.10.252
Destination filename [ap-config]? ap-config-aironet1231G-leplussimple
!!
1227 bytes copied in 1.227 secs (1000 bytes/sec)
ap#

```

ANNEXE : Configuration WPA

```
ap#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#dot11 ssid celeste
ap(config-ssid)#authentication open
ap(config-ssid)#authentication key-management wpa
ap(config-ssid)#wpa-psk ascii margeride
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
ap(config)#interface dot11Radio 0
ap(config-if)#encryption mode ciphers tkip
ap(config-if)#ssid celeste
ap(config-if)#no shutdown
ap(config-if)#
* %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
* %DOT11-6-FREQ_SCAN: Interface Dot11Radio0, Scanning frequencies for 19
seconds
* %DOT11-6-FREQ_USED: Interface Dot11Radio0, frequency 2417 selected
* %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state
to up
* %DOT11-7-AUTH_FAILED: Station 000e.35be.47bf Authentication failed
* %DOT11-7-AUTH_FAILED: Station 000e.35be.47bf Authentication failed
* %DOT11-7-AUTH_FAILED: Station 000e.35be.47bf Authentication failed
* %DOT11-6-ASSOC: Interface Dot11Radio0, Station 000e.35be.47bf Associated
KEY_MGMT[WPA PSK]
```

ANNEXE : Configuration SSH et DHCP

```

ap#conf terminal
ap(config)#username hello password 2101
ap(config)#line vty 0 4
ap(config-line)#transport input all
ap(config-line)#login local
ap(config)#line console 0
ap(config-line)#login local

```

Pour changer le password sur enable

```

ap(config)#enable secret 2101

```

Validation SSH

```

ap#conf terminal
ap(config)#ip domain name alain
ap(config)#crypto key generate rsa
The name for the keys will be: ap.alain
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
ap(config)#
*Mar  1 00:17:45.588: %SSH-5-ENABLED: SSH 1.99 has been enabled
ap(config)#

```

EXEMPLE DECLARATION DU SERVEUR DHCP

```

IP DHCP POOL 20
NETWORK 192.168.20.0 255.255.255.0
DEFAULT-ROUTER 192.168.20.254
IP DHCP POOL 10
NETWORK 192.168.10.0 255.255.255.0
DEFAULT-ROUTER 192.168.10.254
!
IP DHCP EXCLUDED-ADDRESS 192.168.20.250 192.168.20.254

```

QQ COMMANDES UTILES

```

R2#SH IP DHCP BINDING

```

BINDINGS FROM ALL POOLS NOT ASSOCIATED WITH VRF:

IP ADDRESS	CLIENT-ID/ HARDWARE ADDRESS/ USER NAME	LEASE EXPIRATION	TYPE
10.10.20.101	0100.0D9D.4B38.07	SEP 11 2007 02:43 PM	AUTOMATIC
10.10.30.100	0100.1125.119D.12	SEP 11 2007 02:41 PM	AUTOMATIC

```

R2#

```

```

R2#clear ip dhcp binding *

```

ANNEXE : Exemple configuration VLAN Switch Router

```
Switch# vlan database
Switch(vlan)# vlan 2 name vlan_admin
Switch(vlan)# vlan 3 name vlan_wifi

Switch#conf t
Switch(config)#interface fastEthernet 0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2

Switch#conf t
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all

Router(config)#interface ethernet 0/1
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface ethernet 0/1
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface Ethernet0/1.10
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 192.168.10.254 255.255.255.0
Router(config-subif)#exit

Router(config)#interface Ethernet0/1.20
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.100.254 255.255.255.0
Router(config-subif)#exit
```

ANNEXE : Exemple configuration router avec NAT

```
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.8.1

Router#conf t
Router(config)#access-list 10 permit 192.168.0.0 0.0.255.255
Router(config)#ip nat inside source list 10 interface Ethernet 0/0 overload

Router(config)#interface ethernet 0/0
Router(config-if)#ip nat outside

Router(config)#interface ethernet 0/1.10
Router(config-subif)#ip nat inside
Router(config-subif)#exit

Router(config)#interface ethernet 0/1.20
Router(config-subif)#ip nat inside
Router(config-subif)#exit
```

ANNEXE : Interdire traffic entre 192.168.20.0 et 192.168.10.0

```
access-list 100 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

interface FastEthernet0/1.10
ip access-group 100 out
```

Feuille de validation

Date:

Membre du group :

Si ok le responsable TP signe à chaque étape validée

Etape 1

Etape 2

Etape 3

Etape 4

Etape 5

Etape 6

Etape 7

Etape 8

Etape 9