

Mettre en place simplement un PA WiFi - 802.11

On mettra le PA sur le réseau du labo en DHCP, les postes se connecteront au PA et obtiendront une adresse en DHCP, et pourront accéder à internet.

Le schéma

Matériel : Un PA, Un PC éventuellement des smartphones

Logiciels :

Logiciel SolarWinds TFTP server

Logiciel Mib browser

Logiciel putty

Configuration Aironet et switch voir les annexes.



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

Etape 1 Connectique

Faire Addressage.

A faire valider par le formateur

Etape 2

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.

Puis vérifier l'accessibilité du poste windows.

Etape 3

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

Faire les mêmes vérifications windows

Etape 4

Configurer le point d'accès pour y accéder en telnet (putty).

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

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

Etape 6

Sauvegarde des IOS du switch et PA en utilisant le serveur TFTP serveur.

Envoyer la configuration à efrei.alt.tp@gmail.com

Etape 7

Configuration SNMP, puis faire un test avec MIB browser

Lire avec le MIB browser les variables contact, location et les interfaces réseaux, faire une étude.

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)#
```

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
```

ANNEXE : Exemple configuration snmp sur AP

```
ap(config)#snmp-server community public R0
ap(config)#snmp-server community private RW
ap(config)#snmp-server host 192.168.100.10 public
ap(config)#snmp-server host 192.168.100.10 private
ap(config)#snmp-server enable traps
ap(config)#snmp-server contact Bond
ap(config)#snmp-server location mI6
```

Lire avec le MIB browser les variables contact, location et les interfaces réseaux, faire une étude.

Feuille de validation

Dés votre arrivée remplir date et heure, membre du groupe, faire signer le responsable de TP.

Date et heure démarrage TP:

Membre du group :

Si ok le responsable TP signe à chaque étape validée

Etape 1

En terme d'architecture réseau quel est le rôle du PA

Etape 2**Etape 3****Etape 4****Etape 5****Etape 6****Etape 7**