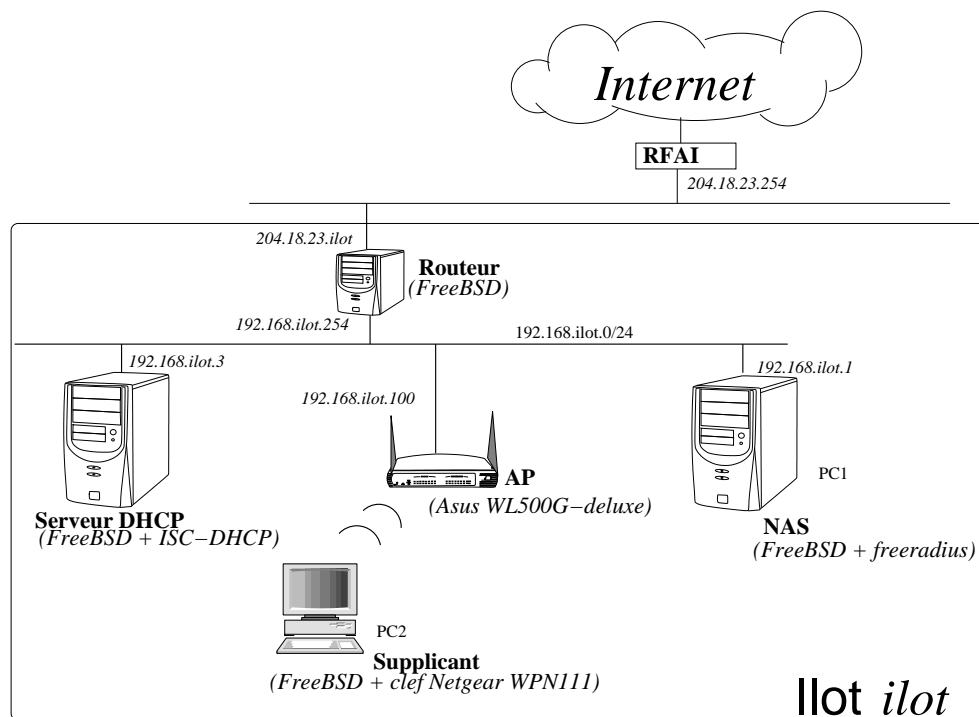


TD 5 - Wifi / Radius

Vous déployerez la salle en IPv4 de la manière suivante :



Dans chaque ilôt x , vous gèrerez les réseaux $192.168.x.0/24$. Les machines :

- APx est la borne Wi-Fi servant de point d'accès (AP) à votre réseau.
- $PC-1$ est le serveur d'authentification.
- $PC-2$ est une machine se connectant au réseau Wi-Fi (pour cela, vous utiliserez la clef USB Wi-Fi qui vous sera fournie).
- $PC-3$ est un serveur DHCP chargé d'allouer une adresse IP dynamique aux clients connectés au réseau qui en font la demande.
- $PC-6$ serviront de routeur entre votre réseau et le réseau $204.18.23.0/24$.

1 Sur le réseau de distribution (DS)

1.1 Configuration des routeurs PC6

Configurez les en tant que routeurs NAT.

Configuration de chaque interface du routeur :

```
ifconfig nom_interface inet adresse_IP netmask masque_reseau
```

Paramétrage indiquant le passage des paquets entre les interfaces :

```
sysctl -w net.inet.ip.forwarding=1
```

Activation de NAT

```
ipfw add divert natd all from any to any via <interface extérieure>
natd -interface <interface extérieure>
```

1.2 Serveur DHCP sur les PC3

Il vous est demandé d'installer un serveur DHCP sur le réseau 192.168.numero_ilot.0/24.

Configurez le serveur DHCP de la manière suivante : dans /usr/local/etc/dhcpd.conf

```
subnet <adresse reseau> netmask <masque> {
    range <debut plage reseau> <fin plage reseau>;
    default-lease-time <bail en seconde par default>;
    max-lease-time <bail maximal en secondes> ;
    option subnet-mask <masque> ;
    option routers <adresse reseau> ;
    option domain-name-servers <adresse du serveur de nom> ;
}
```

Puis lancez le serveur dhcpd (en tapant dhcpd).

Lancez le programme client dhclient sur une machine connectée au réseau pour obtenir votre adresse IP dynamiquement et tester la bonne marche de votre serveur DHCP.

1.3 Configuration de l'AP

Votre AP est un Asus WL 500 G-Deluxe. Il se configure via une interface web.

Pour cela, branchez votre AP à votre réseau de distribution. Ouvrez un navigateur à l'URL :
http://adresse_ip_de_l_AP.

Par défaut constructeur, les paramètres de votre AP sont

- Adresse IP : 192.168.1.1
- login : admin
- mot de passe : admin

Si votre AP avait été configuré autrement (par des étudiants précédents par exemple), vous pouvez réinitialiser votre AP aux paramètres défaut constructeur en utilisant le bouton situé à l'arrière de votre AP.

Configurez votre AP sur le réseau de distribution :

- IPConfig → LAN :
 - *Get IP automatically* : No
 - *IP address* : 192.168.numero_ilot.100
 - *Subnet Mask* : 255.255.255.0
 - *Default Gateway* : 192.168.numero_ilot.6
- System Setup : Access point

1.4 Configuration du supplicant

Le supplicant est le PC2 qui sera connecté au réseau via une liaison sans-fil (pensez bien à débrancher votre câble réseau afin de ne pas fausser les résultats).

A l'aide de la commande `ifconfig -a`, vérifiez que votre interface wi-fi est bien reconnue par votre système.

A l'aide de la commande `ifconfig nom_interface_wifi scan`, listez la liste des réseaux WI-FI accessibles par votre interface.

2 Configuration WEP

Vous configurerez tout d'abord votre AP en mode WEP.

- *SSID* : MASTER_MA_ILOT_num_ilot
- *Authentication Method* : Open System or Shared Key
- *WEP Encryption* : WEP-64 bits
- *Passphrase* :
- *WEP Key 1* :
- *Key Index* : 1

Testez l'accès au réseau sans-fil :

- `iflist nom_interface scan` pour voir si votre réseau est bien visible
- `ifconfig nom_interface essid ssid_reseau key clef_wep` pour configurer vos paramètres wifi
- Utilisez ensuite `dhclient` (ou configurez une adresse statique IP manuellement à l'aide de la commande `ifconfig`) et testez l'accès au réseau de distribution.

3 Configuration WPA avec serveur d'authentification (NAS)

RADIUS (Remote Authentication Dial-In User Service) permet de :

- d'authentifier un utilisateur distant, suivant de multiples modes plus ou moins sécurisés, allant du simple fichier texte à l'annuaire LDAP, en passant par une base de données de type SQL,
- d'enregistrer des informations sur chaque « login »,
- de renvoyer au demandeur des paramètres variés pouvant, suivant le cas, être une configuration IP, un numéro de LAN virtuel etc.

3.1 Mise en place du serveur RADIUS

Sur PC-*x1*, est installé le logiciel `freeradius`. Les fichiers de configuration de ce logiciel se trouvent dans `/etc/freeradius` (suivant les installations, il peut également se trouver sur `/usr/local/etc/raddb`)

L'authentification peut se faire via LDAP, MySQL, `/etc/passwd`, etc. Nous nous contenterons dans ce TP d'utiliser un simple fichier permettant d'associer des logins d'utilisateurs à des mots de passe en clair. Vous éditez pour cela le fichier `users` dans lequel vous placerez des entrées suivant la syntaxe suivante :

```
nom_utilisateur User-Password == "mot_de_passe"
```

Vous éditez également le fichier `clients.conf` en y ajoutant l'entrée suivante :

```
client 192.168.numero_ilot.0/24 {
    secret          = mot_de_passe_partage_entre_AP_et_RADIUS
    shortname       = ilot\_num_ilot
}
```

Vous lancerez le démon radius en mode debug avec la commande suivante :

```
freeradius -xyz -l stdout
```

ou

```
radiusd -xyz -l stdout
```

3.2 Configuration de l'AP

Vous configurerez l'AP avec les paramètres suivants :

- Wireless →Interface
 - *SSID* : MASTER.M1_ILOT_numero_ilot
 - *Channel* : 1
 - *Wireless Mode* : auto
 - *Authentication Method* : WPA
 - *WPA Encryption* : TKIP
- Wireless →Radius Setting
 - *Server IP address* : 192.168.numero_ilot.100
 - *Server Port* : 1812
 - *Connection Secret* : mot_de_passe_partage_entre_AP_et_RADIUS

3.3 Configuration du supplicant

Programme de gestion d'accès aux réseaux sans-fil Nous utiliserons comme gestionnaire d'accès au réseau sans-fil, le programme `wpa_supplicant` dont le fichier de configuration se trouve à `/etc/wpa_supplicant.conf`.

Le lancement du programme `wpa_supplicant` en mode debug se fait avec la commande suivante :

```
wpa_supplicant -dd -c /etc/wpa_supplicant.conf -i nom_interface_wifi
```

Dans le fichier `/etc/wpa_supplicant.conf`, vous configurerez

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
```

```
network={
    ssid="MASTER_M1_ILOT1"
    scan_ssid=1
    key_mgmt=WPA-EAP IEEE8021X NONE
    eap=MD5
    phase2="auth=MSCHAPV2"
    identity="nom_utilisateur"
    password="mot_de_passe"
}
```

Vous lancerez ensuite `wpa_supplicant` en mode débog pour tester.

Vérifiez sur les messages que l'authentification a bien réussi. Durant toute la phase de test, il vous est conseillé d'utiliser `ethereal` entre l'AP et le supplicant ainsi qu'entre l'AP et Radius afin de reconstituer le dialogue échangé.