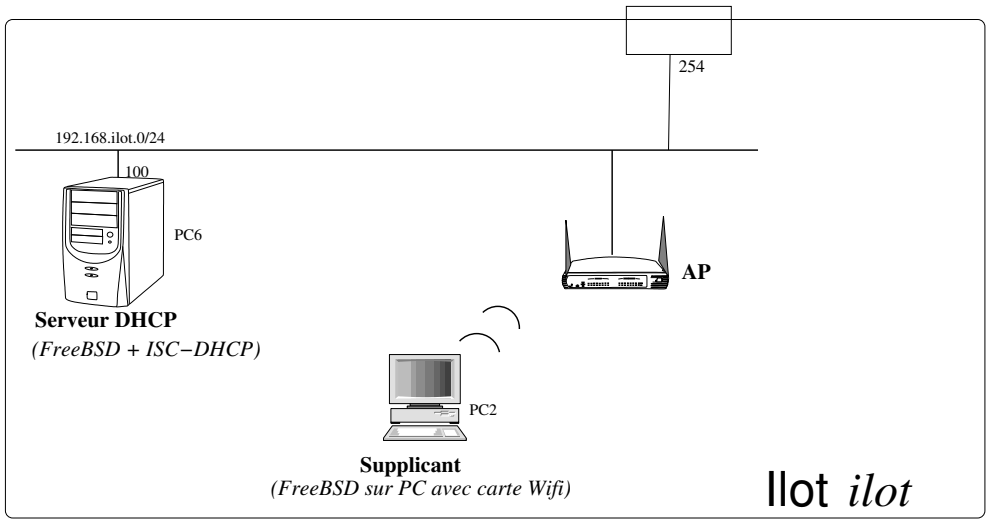
DÉPARTEMENT
Sciences Informatiques

Licence Pro R&S
2012–2013
Chiffrement et authentification
T.T. Dang Ngoc
dntt@u-cergy.fr

TD5 - Wifi, RADIUS, portail captif

Dans un premier temps, vous déploierez sur chaque ilôt la configuration suivante :



Le réseau est pour l'instant autonome (non relié au réseau global).

- votre réseau (privé) a pour adresse 192.168.*ilot*.0/24.
- `PC-6` (192.168.*ilot*.100) est un serveur DHCP chargé d'allouer une adresse IP dynamique aux clients connectés au réseau qui en font la demande.
  - il distribue des adresses sur la plage [192.168.*ilot*.1 − 192.168.*ilot*.50]
  - le routeur par défaut est 192.168.*ilot*.254
  - le serveur DNS à déclarer (mais pas encore atteignable) est : 128.9.0.107
- `PC-2` est une machine qui se connectera au réseau Wi-Fi (vérifiez qu'il comporte bien une carte wifi) par DHCP. Pensez à bien débrancher les câbles réseaux pour ne pas fausser les résultats.
- `AP`x est la borne Wi-Fi servant de point d'accès (AP) à votre réseau. Le SSID que vous utiliserez pour votre ilôt est `ILOT`_*votre_numero_d_ilot*.

1 Chiffrement des communications sans-fil

1.1 Pas de chiffrement

1. Configurez tout d'abord votre réseau sans-fil sans chiffrement (type d'authentification OPEN). Vous configurerez pour cela l'AP ainsi que les paramètres WIFI de votre carte réseau (SSID et authentification : OPEN).

2. Lancez la sonde `wireshark` afin d'intercepter les trames échangées en wifi.
3. Vérifiez l'association de votre carte au réseau.
4. Analysez les trames balises.
5. Utilisez ensuite `dhclient` pour obtenir une adresse IP.
6. Testez l'accès au réseau de distribution (commande ping, accès web, etc.).
7. Vérifiez que les échanges de données passent effectivement en clair. Interceptez les communications sans-fil des autres machines.

1.2 Chiffrement WEP

Vous configurerez à présent votre AP en mode WEP (utilisez une clef de 64 bits) ainsi que votre supplicant.

1. Lancez la sonde `wireshark` afin d'intercepter les trames échangées en wifi.
2. Vérifiez l'association de votre carte au réseau.
3. Analysez les trames balises.
4. Vérifiez que les échanges de données sont effectivement chiffrées par WEP avec l'algorithme RC4.

`aircrack-ng` est un de ces nombreux logiciels exploitant les faiblesses du protocole WEP afin de trouver la clef. À l'aide de ce logiciel :

1. trouvez la clef WEP des autres ilots.
2. interceptez les communications sans-fil des autres machines

1.3 Chiffrement WPA avec clef partagée

1. Configurez à présent votre carte réseau afin d'utiliser WPA-1 sur votre réseau sans-fil avec une clef partagée (Pre Shared Key - PSK).
2. Testez.
3. Lancez la sonde `wireshark` afin d'intercepter les trames échangées en wifi.
4. Analysez les trames balises.
5. Vérifiez que les échanges de données sont effectivement chiffrées par WPA-1 avec l'algorithme RC4 avec le protocole TKIP comme protocole de communication.
6. Configurez à présent votre carte réseau en WPA-2, refaites les mêmes questions et vérifiez que l'algorithme utilisé pour le chiffrement est AES.

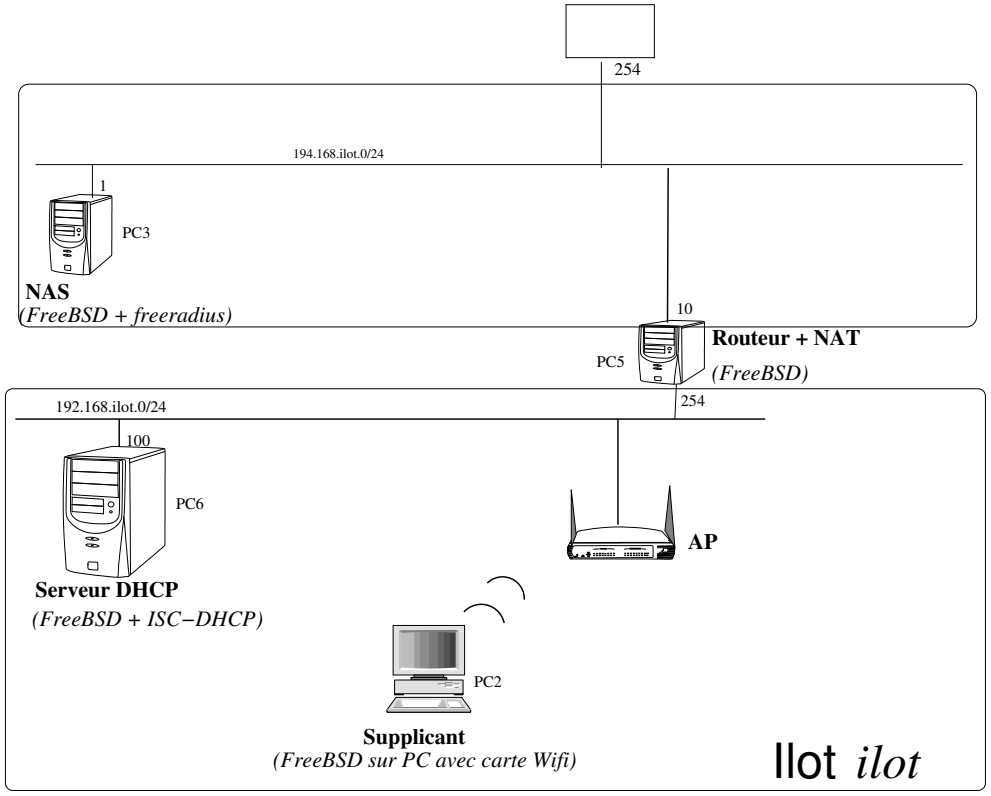
2 Configuration WPA avec serveur d'authentification (NAS)

RADIUS (Remote Authentication Dial-In User Service) permet :
- 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 VLAN, etc.

Nous allons dans cette section utiliser RADIUS afin de permettre l'authentification et le chiffrement de la connexion sans-fil à l'aide d'une clef non partagée, donc propre à chaque utilisateur identifié sur le système.

2.1 Mise en place du serveur RADIUS

Sur `PC-`x`1`, est installé le logiciel `freeradius`. Les fichiers de configuration de ce logiciel se trouvent dans `/usr/local/etc/raddb` (dans d'autres distributions, il pourra se trouver sur `/etc/freeradius`



Adjoignez à présent à votre réseau privé, le réseau de la DMZ 194.168.*ilot*.0/24.

Vous y brancherez et configurerez pour cela les deux machines supplémentaires suivantes :

- `PC-5` (interface interne : 192.168.*ilot*.254 ; interface externe : 194.168.*ilot*.10) est un routeur NAT entre votre réseau privé et le réseau de la DMZ
- `PC-3` (192.168.*ilot*.1) est la machine qui sera de serveur d'authentification réseau (NAS). freeradius y est pour cela installé.

1. Branchez et configurez les interfaces réseaux (n'oubliez pas d'activer sur votre routeur le routage entre les interfaces. Configurez également correctement le NAT).
2. Vérifiez que les accès entre vos 2 réseaux fonctionnent correctement. Essayez par exemple de faire un ping depuis votre serveur DHCP à votre serveur NAS.
3. Testez l'accès réseau de votre supplicant à votre NAS (par ping par exemple). On ne demande pas encore de tester le service d'authentification.

L'authentification RADIUS peut se faire via LDAP, MySQL, `/etc/passwd`, etc. Nous nous contenterons dans un premier temps d'utiliser un simple fichier permettant d'associer des logins d'utilisateurs à des mots de passe en clair.

1. Vous éditerez pour cela le fichier `users` dans lequel vous placerez des entrées.

2. testez ensuite à l'aide de `radclient` depuis une machine du réseau privé (par exemple le serveur DHCP) que votre serveur RADIUS authentifie bien les utilisateurs que vous passerez à la commande
3. enfin, définissez un mot de passe partagé entre le serveur RADIUS et l'AP. Configurez l'AP (et RADIUS) afin d'authentifier les supplicants par RADIUS en WPA-2 Enterprise (802.1x)
4. à l'aide de la commande `wpa_supplicant` en mode debug, vérifiez sur les messages que l'authentification a bien réussi.
5. Lancez la sonde `wireshark` afin d'intercepter les trames échangées en wifi.
6. Analysez les trames balises.
7. Vérifiez que les échanges de données sont effectivement chiffrées.
8. si vous en possèdez un, utilisez un smartphone, tablette ou ordinateur portable, pour tester l'association par WPA via une authentification RADIUS.

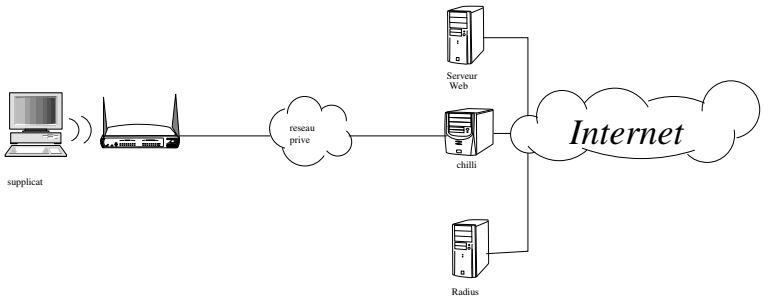
Au lieu d'utiliser un fichier contenant les login/mot de passe en clair de chaque utilisateur, nous allons ne stocker qu'une version haché des mots de passe utilisateur. Ceci, toujours dans le fichier users (la configuration LDAP est vu dans un autre module). Testez à nouveau votre association après authentification.

En utilisant les CA du TP précédent, créez un certificat pour un utilisateur. Placez sa clef privé sur le supplicant et le certificat public sur RADIUS. Reparamétrez RADIUS pour prendre en compte ce type d'authentification. Testez.

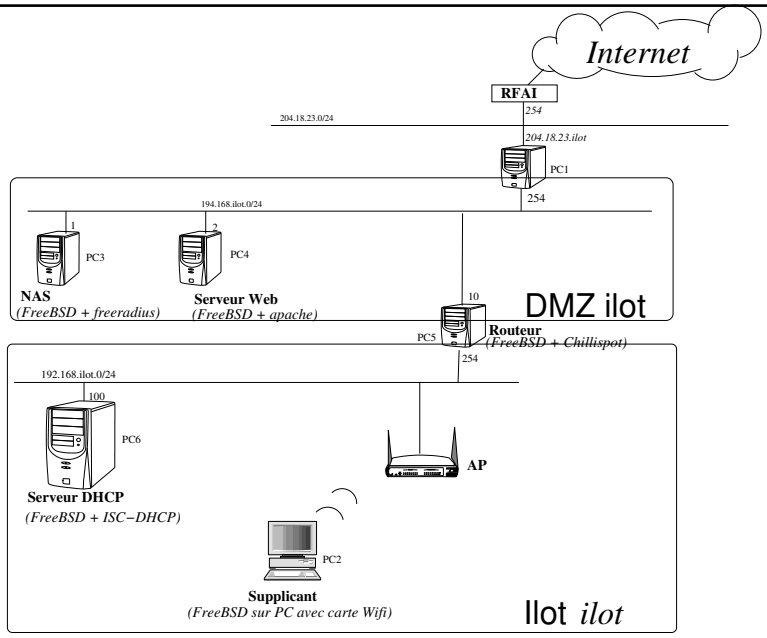
3 Portail captif

Dans certains cas, il peut être utile de laisser les connexions sans-fil ouvertes (mode OPEN, donc sans authentification ni chiffrement) et ne procéder qu'à l'identification et l'authentification du client qu'au moment où celui-ci veut accéder à certaines ressources (par exemple l'accès Internet).

Chillispot (ou sa version coova-chilli) est un tel système. Il se place sur un routeur et interagit avec un serveur RADIUS et un serveur web (qui peuvent être placés sur la même machine) afin de pouvoir permettre l'accès au reste du réseau après authentification.



Rajoutez sur votre réseau les machines :
– `PC-4` (interface : 194.168.*ilot*.2) est un serveur web sur lequel vous configurerez Apache.
– `PC-1` (interface interne : 194.168.*ilot*.254 ; interface externe : 204.18.23.*ilot*) est un routeur entre votre réseau et le réseau du FAI (dont l'adresse est 204.18.23.254)
– le routeur `PC-5` aura à présent le service chillispot qui y sera en plus activé.



Mettez en place le portail captif. Pour cela, vous devrez :

1. reconfigurer l'AP pour être sans authentification (authentification OPEN)
2. configurer `chillispot` sur le routeur afin :
   (a) de rediriger les supplicants vers la page web d'authentification située sur votre serveur web
   (b) d'utiliser le serveur RADIUS comme serveur d'authentification
   (c) de laisser passer ou non les supplicants suivant qu'ils aient ou non réussit leur identification/authentification.
3. configurer votre serveur web afin de :
   (a) distribuer la page web d'authentification
   (b) d'interroger le serveur RADIUS pour authentifier le supplicant
4. testez ensuite votre portail captif.

4 Annexes

4.1 Configuration réseau filaire

4.2 Configuration serveur DHCP

4.3 Configuration réseau sans-fil

- creez l'interface wlan0 (la premiere fois) à partir de votre interface physique.
  `ifconfig wlan0 create wlandev ath0`
  Vous utiliserez par la suite l'interface wlan0.
- `ifconfig nom_interface up scan` pour voir si votre réseau est bien visible
- `ifconfig nom_interface essid ssid_reseau` pour configurer vos paramètres wifi

4.4 Configuration de NAT

Activation de NAT

```
kldload ipfw_nat.ko
ipfw add divert natd all from any to any via <interface extérieure>
natd -interface <interface extérieure>
```

4.5 Configuration du point d'accès (AP)

Votre point d'accès se configure via une interface web.

Pour cela, branchez votre AP à votre réseau de distribution. Regardez l'étiquette collé sous votre AP qui indiquera les paramètres constructeyrs par défaut de votre AP (IP, login/mot de passe administrateur). Au besoin, appuyez sur le bouton "reset".

Configurez la carte réseau de la machine qui configurera l'AP pour y accéder pour le paramétrer puis ouvrez un navigateur à l'URL :
`http://adresse_ip_de_l_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

4.6 Configuration d'un serveur FreeRADIUS

Vous éditerez pour cela le fichier `users` dans lequel vous placerez des entrées suivant la syntaxe suivante :

```
nom_utilisateur User-Password := "mot_de_passe"
                User-Reply-Message := "Bonjour %{User-Name}"
```

(la dernière ligne est facultative).

Vous éditerez 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

}
```

4.6.1 Lancement du serveur FreeRADIUS

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

```
radiusd -xXf -l stdout
```

Explication des options :
- `-x` : mode debug
- `-X` : full debug
- `-f` : mettre le démon en avant-plan
- `-l` *fichier* : où mettre les logs (sur la sortie standard si *stdout*

4.6.2 Utilisation de radclient pour tester un serveur RADIUS

Testez votre serveur freeradius sans la borne :

```
echo "User-Name = hcover, User-Password = toto02" | \
   radclient -x adresse_ip_radius auth mot_de_passe_partage_entre_AP_et_RADIUS
```

4.7 Configuration de l'AP

Vous configurerez l'AP avec les paramètres suivants :

- Wireless →Interface
  - *SSID :* `ILOT_numero_ilot`
  - *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`

4.8 Configuration du supplicant

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 débug 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="ILOT_1"
  scan_ssid=1
  key_mgmt=WPA-EAP IEEE8021X NONE
  eap=MD5
  phase2="auth=MSCHAPV2"
  identity="nom_utilisateur"
  password="mot_de_passe"
}
```

4.9 Configuration du serveur chillispot

chilli.conf

```
radiusserver1 adresse_ip_serveur_radius
radiusserver2 adresse_ip_serveur_radius
radiussecret clefpartage_entre_chilli_et_radius
uamserver url_de_la_page_web_d_authenification
uamsecret mot_de_passe_haché ????
```

Sur le serveur web : /var/www/cgi-bin/hotspotlogin.cgi

```
$uamsecret="xdhhezi"
$uampassword=""
```

4.10 Configuration du serveur web apache