IUT de La Rochelle

Université La Rochelle

- TP 1 -
Wi-Fi – Configuration d'un AP

par Édouard Lumet

IT La Rochelle

iut réseaux & télécoms

Sommaire

1. Point d'accès Wi-Fi

1.1. Se connecter au point d'accès

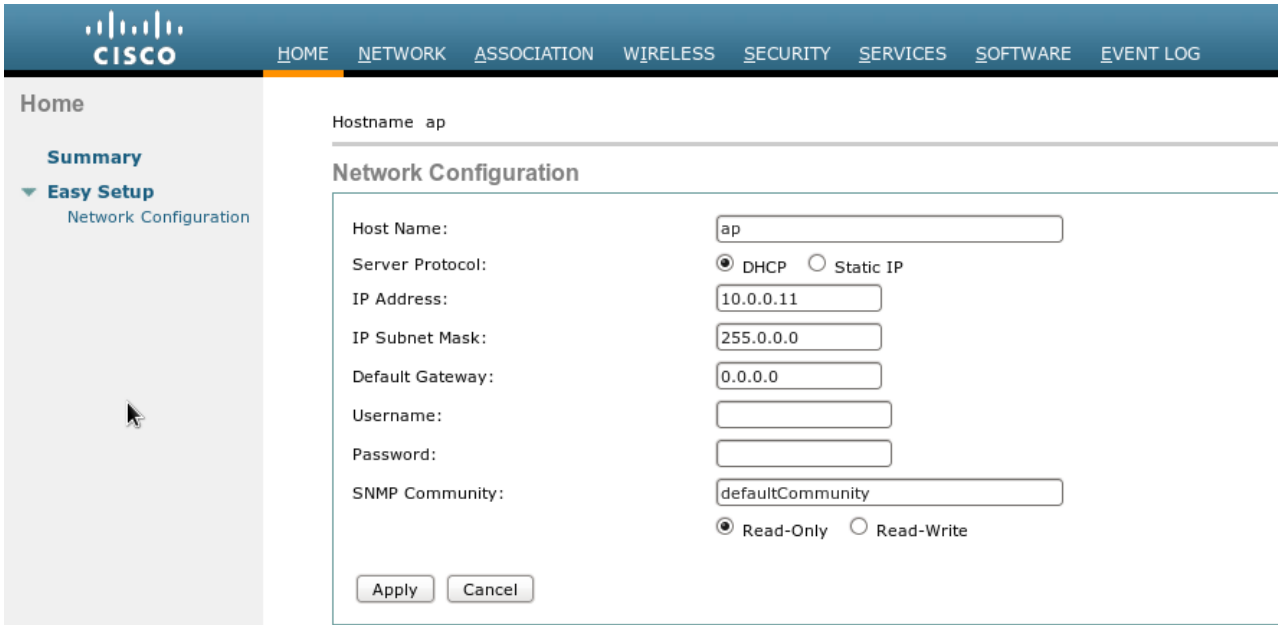
1. Pour commencer, il faut installer un serveur DHCP et le configurer pour que l'AP obtienne une adresse IP puis y accéder. Sous Fedora, on exécute **sudo yum update** puis **yum install dhcp**. Ensuite, on modifie le fichier /etc/dhcp/dhcpd.conf en ajoutant :

```
subnet 10.0.0.0 netmask 255.0.0.0 {
        range 10.0.0.10 10.0.0.20 ;
}
```

   On ajoute alors une adresse à l'interface eth1 via la commande **sudo ifconfig eth1 10.0.0.1/24** puis on redémarre le serveur dhcp : **sudo service dhcpd restart**. Après avoir connecté l'AP à l'interface eth1 et l'avoir électriquement branché, le serveur DHCP lui attribue une adresse IP.

   NB : pour connaître l'adresse IP attribuée, on exécute **sudo service dhcpd status**.

2. En tapant 10.0.0.11 dans firefox, on arrive sur l'interface de gestion de l'AP (login/pwd : cisco/Cisco).



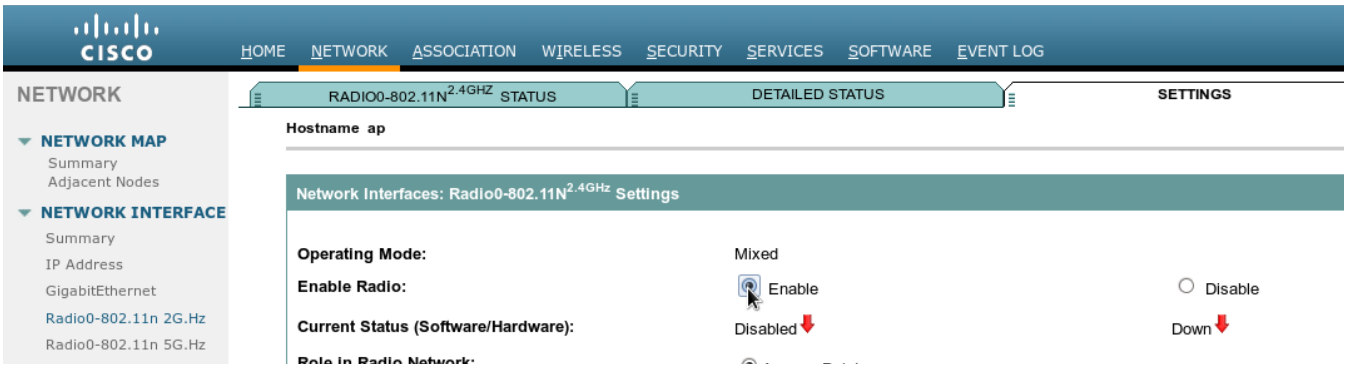
3. Le hostname est 'ap'. On pouvait s'y attendre car c'est celui qui était indiqué dans **service dhcp status**. Ensuite, avec Wireshark on peut voir des paquets révélant l'adresse MAC : *voir page suivante*

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_b6:2e:28	CDP/VTP/DTP/PAgP/UDLD	CDP	371	Device I
2	0.827958	Cisco_b6:2e:28	Cisco_b6:2e:28	LOOP	60	Reply
3	10.827942	Cisco_b6:2e:28	Cisco_b6:2e:28	LOOP	60	Reply
4	20.827994	Cisco_b6:2e:28	Cisco_b6:2e:28	LOOP	60	Reply
5	30.827976	Cisco_b6:2e:28	Cisco_b6:2e:28	LOOP	60	Reply
6	40.828028	Cisco_b6:2e:28	Cisco_b6:2e:28	LOOP	60	Reply

L'adresse MAC de l'AP est 0C:27:27:B6:2E:28. Le protocole CDP est un protocole propriétaire Cisco (Cisco Discovery Protocol).

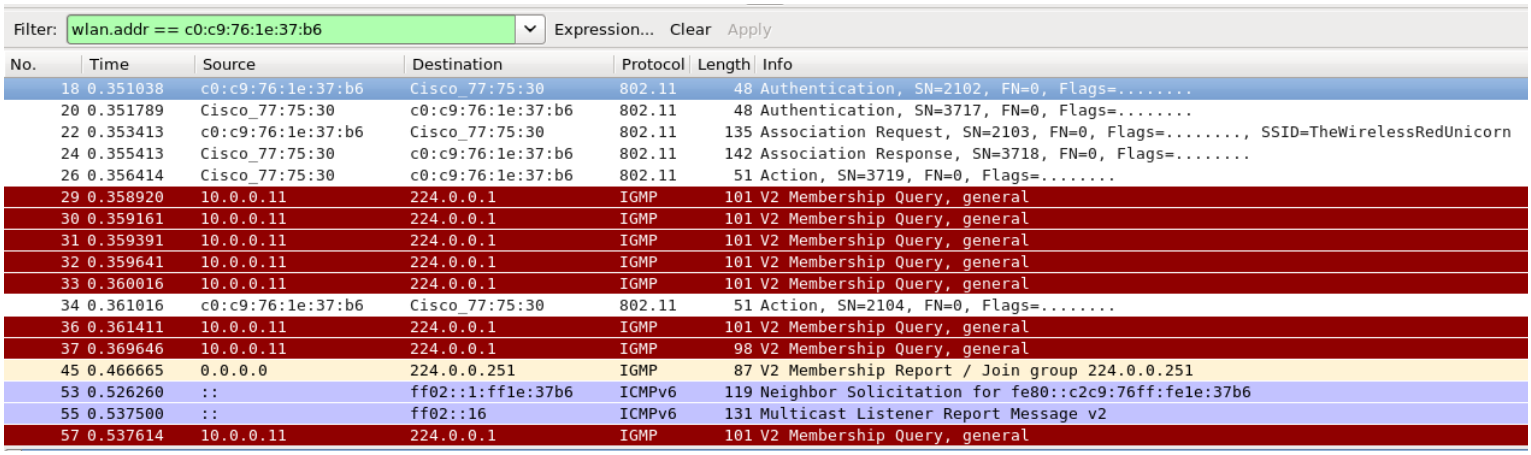
4. Dans l'écran où nous nous trouvions précédemment sur l'AP, on configure un SSID pour l'interface radio (2,4GHz) :

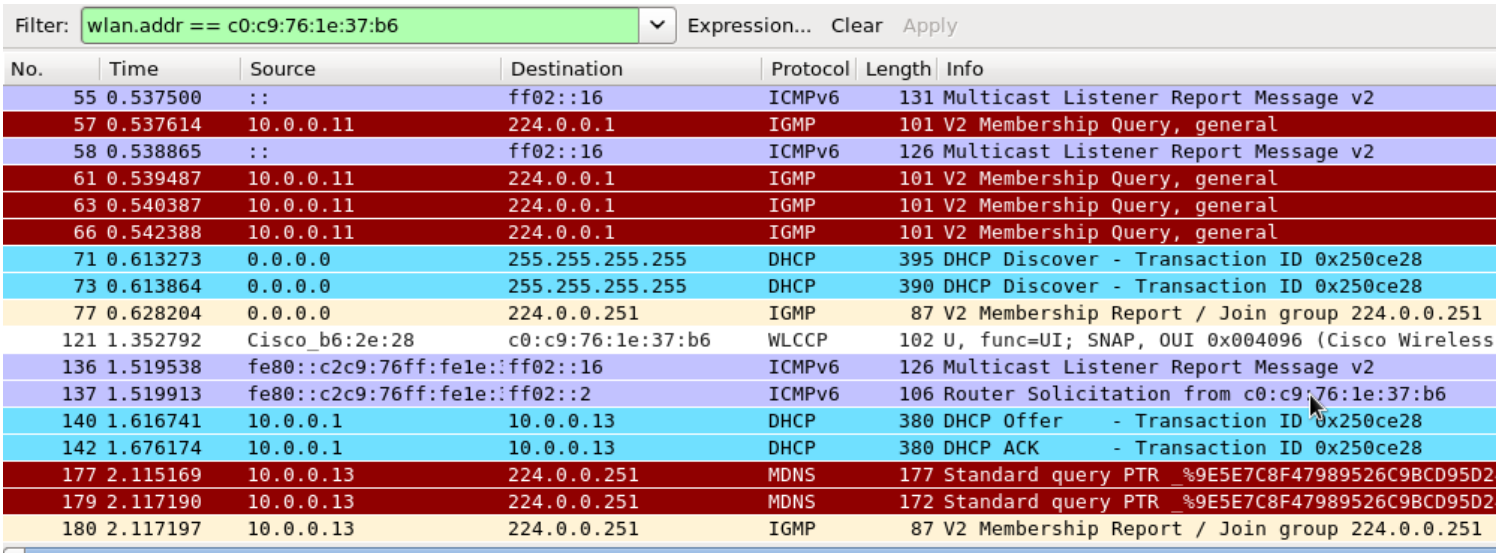
Il faut ensuite activer l'interface radio : NETWORK > sous NETWORK INTERFACE : Radio 2GHz puis onglet SETTINGS :

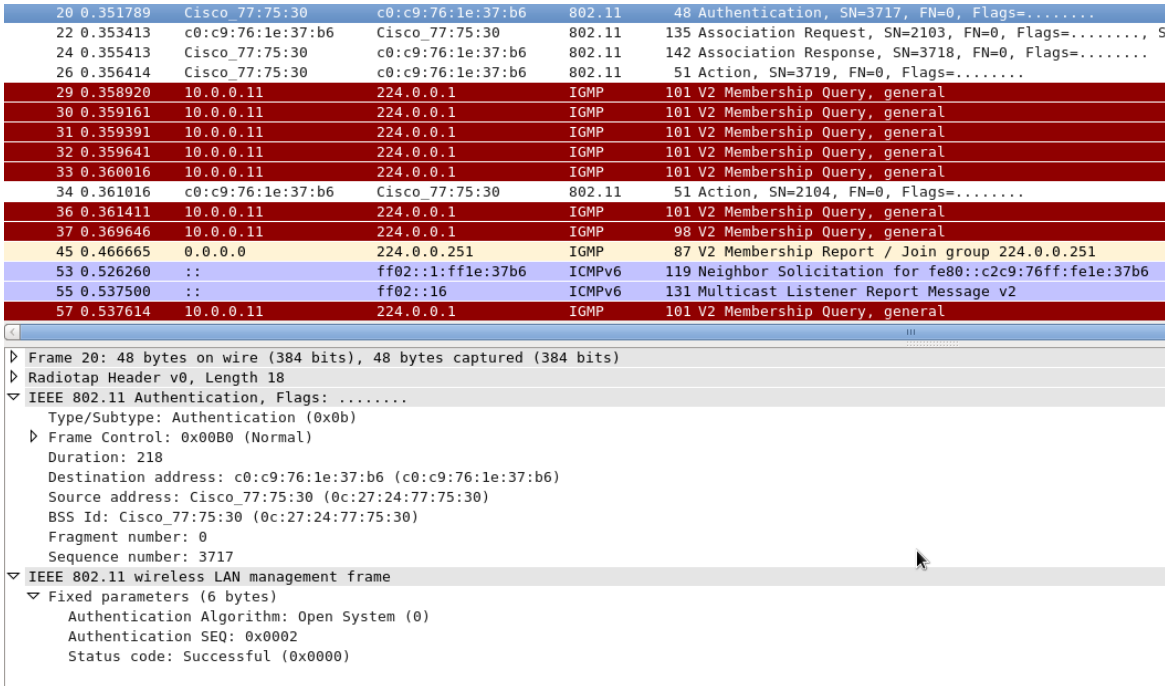


Il faut enfin cliquer sur 'Apply' en bas de page.

5. On observe ce qui passe sur le réseau à l'aide de Wireshark en mode promiscuous lorsque l'on est connecté à notre réseau Wi-Fi :



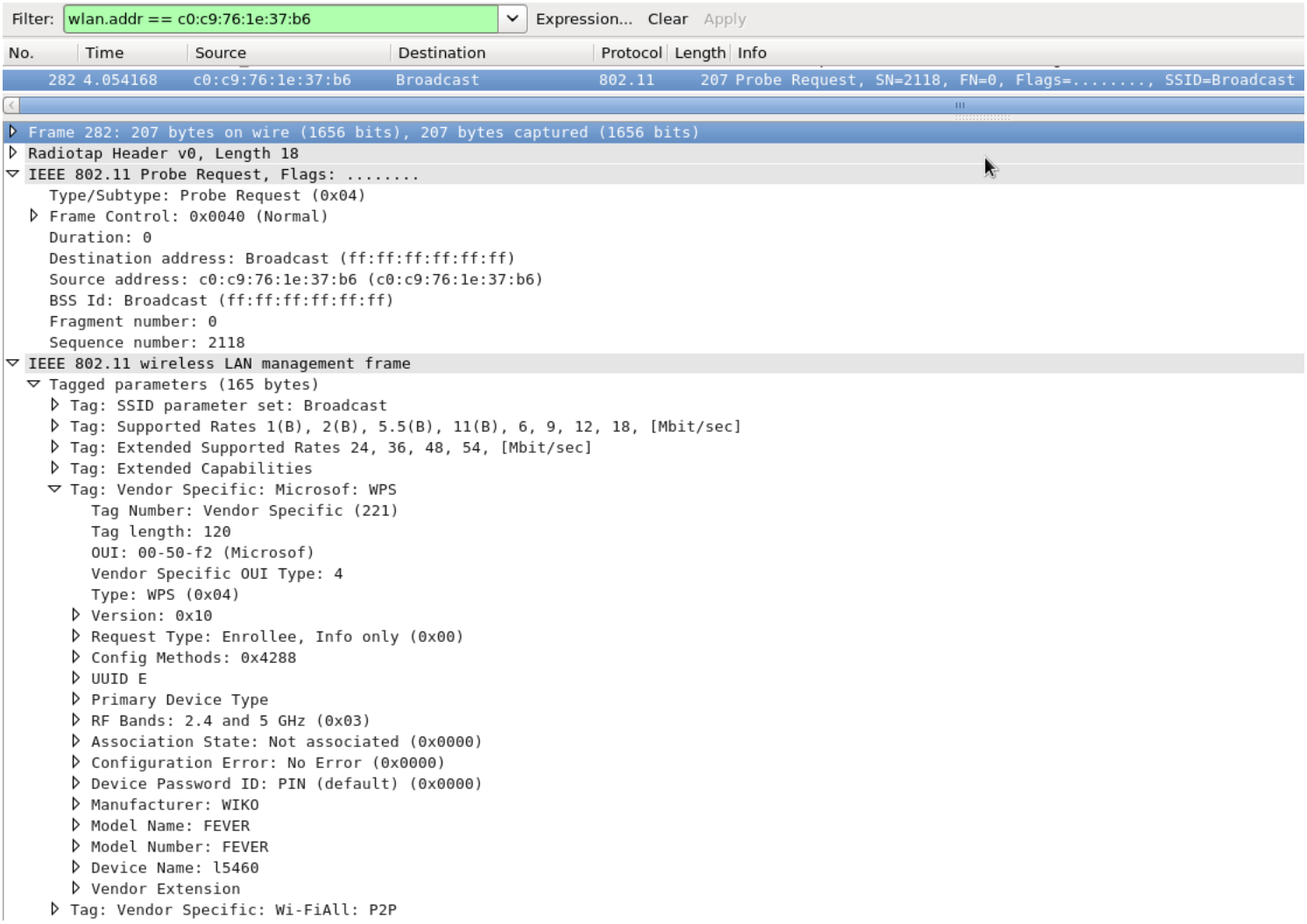




On filtre les trames avec l'@ MAC de notre machine par exemple pour plus de lisibilité. On voit les différentes étapes : authentification, association, échanges DHCP. De plus, on voit dans les messages d'authentification que le réseau est ouvert.

6. Pour tester la connectivité Web, il faut mettre en place routage et NAT sur le PC sous Fedora. En revanche, on peut tester facilement le ping entre le PC et un autre équipement connecté par exemple.

7. Avec Wireshark, on écoute en mode monitor puis on se connecte au réseau Wi-Fi avec un autre équipement.



On peut voir que l'équipement envoie un message Probe (Probe Request) pour démarrer une authentification puis une association. On peut voir dans le message que plusieurs informations sont transmises dont notamment la marque et le modèle de l'équipement. Ici, on peut voir le nom et le modèle de mon smartphone quand je me suis connecté à mon réseau (WIKO FEVER).

1.2. Limiter l'accès au réseau

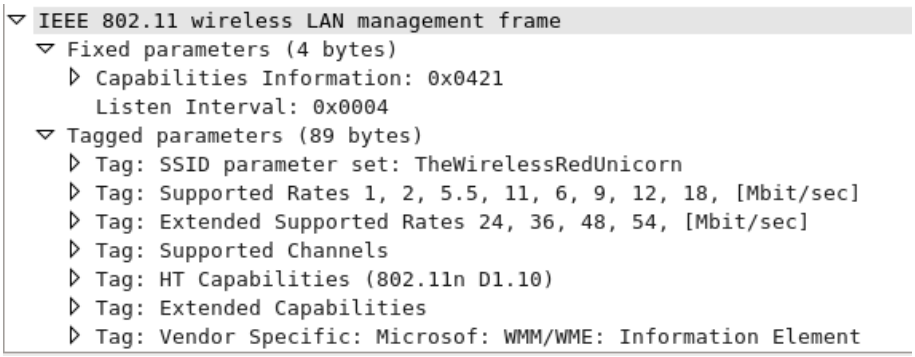
Plusieurs options sont possibles pour limiter l'accès au réseau. Une des options consiste à filtrer sur la base d'adresses MAC via une liste noire ou une liste blanche. Le principe d'une liste noire est d'accepter toutes les adresses MAC sauf celles indiquées dans cette liste. Pour la liste blanche c'est le contraire. Cependant, comme nous l'avons vu avec Wireshark en mode monitor, il facile de voir de nombreuses informations sans être connecté au réseau Wi-Fi visé. Il suffirait simplement de repérer l'adresse MAC d'une machine pouvant se connecter au réseau est d'usurper son adresse.

Un autre moyen très simple est de stopper la diffusion du SSID via les beacon émis par l'AP. Ceux-ci ne sont plus transmis et le réseau n'est plus visible. En revanche, il est aisé de récupérer le SSID du réseau Wi-Fi via les requêtes Probe envoyées par les équipements de connectant à ce réseau.

On peut également restreindre l'accès avec une authentification chiffrée à l'aide d'une clé. On peut ici configurer deux types de sécurité : WEP et WPA. Pour rappel, WEP est très vulnérable car il utilise un chiffrement symétrique RC4 reconnu « cassé » depuis de nombreuses années et CRC pour l'intégrité qui est algorithme linéaire. WPA, associé à CCMP, est quant à lui beaucoup plus fort car il utilise le chiffrement symétrique AES et n'emploie plus CRC.

1.3. Jouer sur la performance du réseau

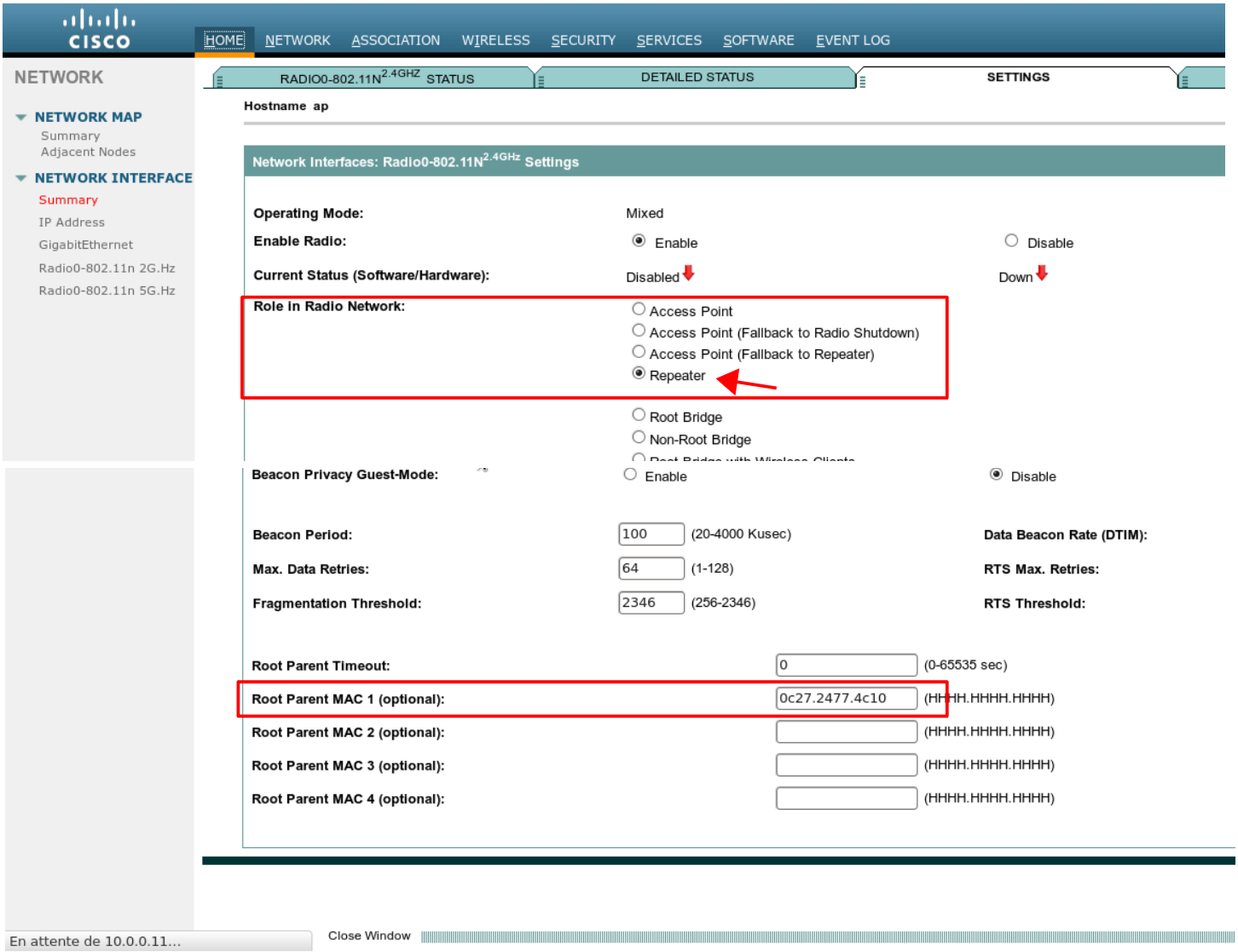
Il est possible de régler différents paramètres affectant la performance du réseau. On peut par exemple modifier le débit entre 1 et 54 Mbit/s, sachant que le débit de 1 Mbit/s est toujours utilisé. En effet, c'est à ce débit fixe que sont transmis les messages tels que RTS, CTS, etc, dans le cadre de CSMA/CA (évitement de collision). On peut aussi faire varier la puissance d'émission de la borne. Un autre paramètre qu'il peut être intéressant de modifier est la période d'envoi des beacons par l'AP. En effet, ces messages ayant pour but d'informer les utilisateurs de la présence du réseau Wi-Fi avec notamment le SSID, les débits possibles etc, réduisent le débit utile sur le support.



Ces paramètres sont typiquement visibles dans un beacon. Le SSID apparaît ainsi que les débits supportés. On remarque aussi la norme employée, qui est ici 802.11n.

2. En mode répéteur

13. Avant de configurer le mode répéteur, on s'assure que les deux AP ont les mêmes paramètres de sécurité.
14. On note ensuite l'adresse MAC de **l'interface radio** de l'AP que l'on souhaite répéter (= AP répété). L'autre AP, celui qui répète est nommé répéteur.
15. Il faut commencer par configurer le répéteur en mode infrastructure. Dans SECURITY > SSID Manager. On crée alors un SSID avec le nom du SSID répété. Ensuite, on sélectionne ce SSID dans le menu déroulant Set Infrastructure SSID.
16. On configure maintenant l'interface radio de l'AP répéteur en mode répéteur puis on renseigne l'adresse MAC de **l'interface radio** de l'AP répété dans un champ Root Parent MAC pour indiquer au répéteur qui est le répété :



17. On vérifie sur l'AP répété que le répéteur est connecté :

Hostname ap

Association					
Clients: 0			Infrastructure clients: 1		
View: ☑ Client ☑ Infrastructure client					
Radio0-802.11N$^{2.4GHz}$					
SSID panda17 :					
Device Type	**Name**	**IP Address**	**MAC Address**	**State**	**Parent**
WGB-client	ap	10.0.0.11	bc16.65b6.2e28	Associated	self

À noter que l'on ne peut pas modifier le débit sur un seul AP, sous peine de ne plus pouvoir contacter l'AP répéteur. En effet, nous avons fait l'expérience et une fois que le débit est différent sur les deux AP, le répéteur devient injoignable. En revanche, il est possible de configurer des puissances différentes sans aucun soucis.