

- TP 1 -
Wi-Fi – Configuration d'un AP
par Édouard Lumet

Sommaire

1. Point d'accès Wi-Fi.....	3
1.1. Se connecter au point d'accès.....	3
1.2. Limiter l'accès au réseau.....	7
1.3. Jouer sur la performance du réseau.....	7
2. En mode répéteur.....	8

1. Point d'accès Wi-Fi

1.1. Se connecter au point d'accès

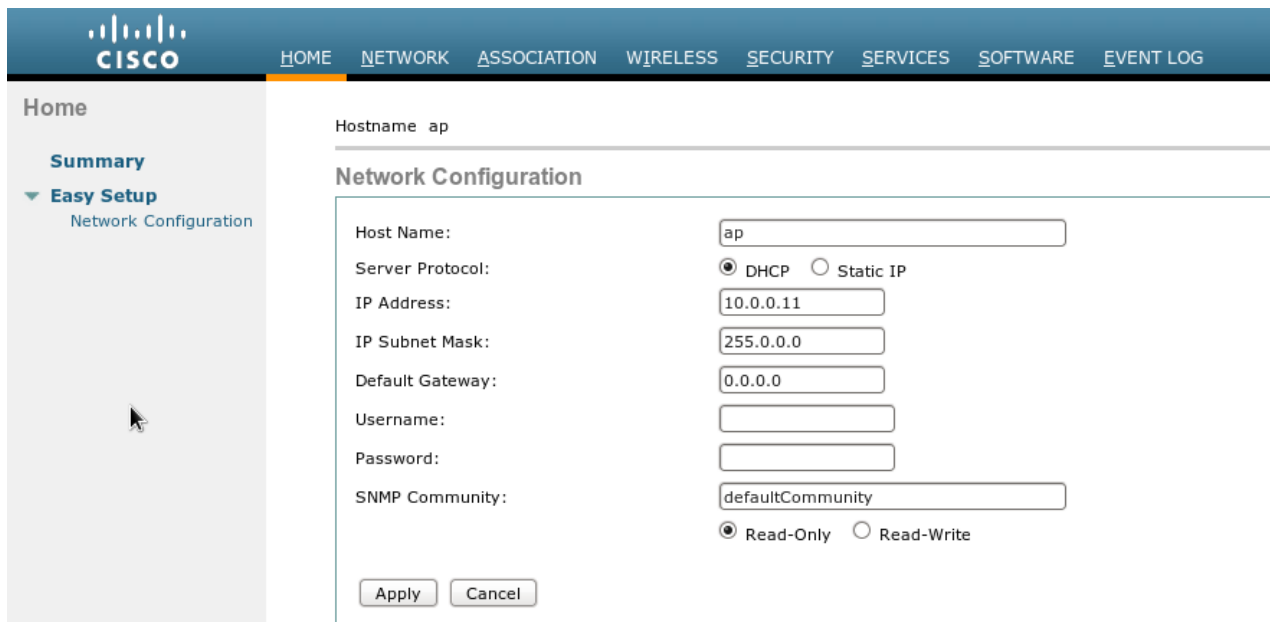
1. Pour commencer, il faut installer un serveur DHCP et le configurer pour que l'AP obtienne une adresse IP puis y accéder. Sous Fedora, on exécute **sudo yum update** puis **yum install dhcp**. Ensuite, on modifie le fichier `/etc/dhcp/dhcpd.conf` en ajoutant :

```
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 trouvons précédemment sur l'AP, on configure un SSID pour l'interface radio (2,4GHz) :

Radio Configuration

Radio 2.4GHz

SSID :

Broadcast SSID in Beacon

VLAN : No VLAN Enable VLAN ID: (1-4094) Native VLAN

Security :

Role in Radio Network :

Optimize Radio Network :

Aironet Extensions:

Channel:

Power:

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

The screenshot shows the Cisco configuration page for the 'Radio0-802.11N 2.4GHz' interface. The 'SETTINGS' tab is active. Under 'Network Interfaces: Radio0-802.11N 2.4GHz Settings', the 'Enable Radio' checkbox is checked, and the 'Current Status (Software/Hardware)' is 'Disabled' with a red arrow pointing down. The 'Operating Mode' is set to 'Mixed'.

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 :

No.	Time	Source	Destination	Protocol	Length	Info
18	0.351038	c0:c9:76:1e:37:b6	Cisco_77:75:30	802.11	48	Authentication, SN=2102, FN=0, Flags=.....
20	0.351789	Cisco_77:75:30	c0:c9:76:1e:37:b6	802.11	48	Authentication, SN=3717, FN=0, Flags=.....
22	0.353413	c0:c9:76:1e:37:b6	Cisco_77:75:30	802.11	135	Association Request, SN=2103, FN=0, Flags=....., SSID=TheWirelessRedUnicorn
24	0.355413	Cisco_77:75:30	c0:c9:76:1e:37:b6	802.11	142	Association Response, SN=3718, FN=0, Flags=.....
26	0.356414	Cisco_77:75:30	c0:c9:76:1e:37:b6	802.11	51	Action, SN=3719, FN=0, Flags=.....
29	0.358920	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
30	0.359161	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
31	0.359391	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
32	0.359641	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
33	0.360016	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
34	0.361016	c0:c9:76:1e:37:b6	Cisco_77:75:30	802.11	51	Action, SN=2104, FN=0, Flags=.....
36	0.361411	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
37	0.369646	10.0.0.11	224.0.0.1	IGMP	98	V2 Membership Query, general
45	0.466665	0.0.0.0	224.0.0.251	IGMP	87	V2 Membership Report / Join group 224.0.0.251
53	0.526260	::	ff02::1:ff1e:37b6	ICMPv6	119	Neighbor Solicitation for fe80::c2c9:76ff:fe1e:37b6
55	0.537500	::	ff02::16	ICMPv6	131	Multicast Listener Report Message v2
57	0.537614	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general

No.	Time	Source	Destination	Protocol	Length	Info
55	0.537500	::	ff02::16	ICMPv6	131	Multicast Listener Report Message v2
57	0.537614	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
58	0.538865	::	ff02::16	ICMPv6	126	Multicast Listener Report Message v2
61	0.539487	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
63	0.540387	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
66	0.542388	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
71	0.613273	0.0.0.0	255.255.255.255	DHCP	395	DHCP Discover - Transaction ID 0x250ce28
73	0.613864	0.0.0.0	255.255.255.255	DHCP	390	DHCP Discover - Transaction ID 0x250ce28
77	0.628204	0.0.0.0	224.0.0.251	IGMP	87	V2 Membership Report / Join group 224.0.0.251
121	1.352792	Cisco_b6:2e:28	c0:c9:76:1e:37:b6	WLCCP	102	U, func=UI; SNAP, OUI 0x004096 (Cisco Wireless
136	1.519538	fe80::c2c9:76ff:fe1e::ff02::16	ff02::16	ICMPv6	126	Multicast Listener Report Message v2
137	1.519913	fe80::c2c9:76ff:fe1e::ff02::2	ff02::2	ICMPv6	106	Router Solicitation from c0:c9:76:1e:37:b6
140	1.616741	10.0.0.1	10.0.0.13	DHCP	380	DHCP Offer - Transaction ID 0x250ce28
142	1.676174	10.0.0.1	10.0.0.13	DHCP	380	DHCP ACK - Transaction ID 0x250ce28
177	2.115169	10.0.0.13	224.0.0.251	MDNS	177	Standard query PTR %9E5E7C8F47989526C98CD95D2
179	2.117190	10.0.0.13	224.0.0.251	MDNS	172	Standard query PTR %9E5E7C8F47989526C98CD95D2
180	2.117197	10.0.0.13	224.0.0.251	IGMP	87	V2 Membership Report / Join group 224.0.0.251

20	0.351789	Cisco_77:75:30	c0:c9:76:1e:37:b6	802.11	48	Authentication, SN=3717, FN=0, Flags=.....
22	0.353413	c0:c9:76:1e:37:b6	Cisco_77:75:30	802.11	135	Association Request, SN=2103, FN=0, Flags=....., S
24	0.355413	Cisco_77:75:30	c0:c9:76:1e:37:b6	802.11	142	Association Response, SN=3718, FN=0, Flags=.....
26	0.356414	Cisco_77:75:30	c0:c9:76:1e:37:b6	802.11	51	Action, SN=3719, FN=0, Flags=.....
29	0.358920	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
30	0.359161	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
31	0.359391	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
32	0.359641	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
33	0.360016	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
34	0.361016	c0:c9:76:1e:37:b6	Cisco_77:75:30	802.11	51	Action, SN=2104, FN=0, Flags=.....
36	0.361411	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general
37	0.369646	10.0.0.11	224.0.0.1	IGMP	98	V2 Membership Query, general
45	0.466665	0.0.0.0	224.0.0.251	IGMP	87	V2 Membership Report / Join group 224.0.0.251
53	0.526260	::	ff02::1:ff1e:37b6	ICMPv6	119	Neighbor Solicitation for fe80::c2c9:76ff:fe1e:37b6
55	0.537500	::	ff02::16	ICMPv6	131	Multicast Listener Report Message v2
57	0.537614	10.0.0.11	224.0.0.1	IGMP	101	V2 Membership Query, general

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

> Frame 20: 48 bytes on wire (384 bits), 48 bytes captured (384 bits)
 > Radiotap Header v0, Length 18
 > IEEE 802.11 Authentication, Flags:
 Type/Subtype: Authentication (0x0b)
 > Frame Control: 0x0080 (Normal)
 Duration: 218
 Destination address: c0:c9:76:1e:37:b6 (c0:c9:76:1e:37:b6)
 Source address: Cisco_77:75:30 (0c:27:24:77:75:30)
 BSS Id: Cisco_77:75:30 (0c:27:24:77:75:30)
 Fragment number: 0
 Sequence number: 3717
 > IEEE 802.11 wireless LAN management frame
 > Fixed parameters (6 bytes)
 Authentication Algorithm: Open System (0)
 Authentication SEQ: 0x0002
 Status code: Successful (0x0000)

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.

Filter: wlan.addr == c0:c9:76:1e:37:b6 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
282	4.054168	c0:c9:76:1e:37:b6	Broadcast	802.11	207	Probe Request, SN=2118, FN=0, Flags=....., SSID=Broadcast

Frame 282: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits)

- ▶ Radiotap Header v0, Length 18
- ▼ IEEE 802.11 Probe Request, Flags:

 - Type/Subtype: Probe Request (0x04)
 - ▶ Frame Control: 0x0040 (Normal)
 - Duration: 0
 - Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source address: c0:c9:76:1e:37:b6 (c0:c9:76:1e:37:b6)
 - BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
 - Fragment number: 0
 - Sequence number: 2118

- ▼ IEEE 802.11 wireless LAN management frame

 - ▼ Tagged parameters (165 bytes)

 - ▶ Tag: SSID parameter set: Broadcast
 - ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
 - ▶ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
 - ▶ Tag: Extended Capabilities
 - ▼ Tag: Vendor Specific: Microsof: WPS

 - Tag Number: Vendor Specific (221)
 - Tag length: 120
 - OUI: 00-50-f2 (Microsof)
 - Vendor Specific OUI Type: 4
 - Type: WPS (0x04)
 - ▶ Version: 0x10
 - ▶ Request Type: Enrollee, Info only (0x00)
 - ▶ Config Methods: 0x4288
 - ▶ UUID E
 - ▶ Primary Device Type
 - ▶ RF Bands: 2.4 and 5 GHz (0x03)
 - ▶ Association State: Not associated (0x0000)
 - ▶ Configuration Error: No Error (0x0000)
 - ▶ Device Password ID: PIN (default) (0x0000)
 - ▶ Manufacturer: WIKO
 - ▶ Model Name: FEVER
 - ▶ Model Number: FEVER
 - ▶ Device Name: l5460
 - ▶ Vendor Extension

 - ▶ Tag: Vendor Specific: Wi-FiAll: P2P

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 est 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 un 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.

```

▼ IEEE 802.11 wireless LAN management frame
  ▼ Fixed parameters (4 bytes)
    ▶ Capabilities Information: 0x0421
      Listen Interval: 0x0004
  ▼ Tagged parameters (89 bytes)
    ▶ Tag: SSID parameter set: TheWirelessRedUnicorn
    ▶ Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    ▶ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▶ Tag: Supported Channels
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: Extended Capabilities
    ▶ Tag: Vendor Specific: Microsoft: WMM/WME: Information Element
  
```

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 :

The screenshot shows the Cisco IOS configuration interface for the 'Radio0-802.11N 2.4GHz' interface. The 'Role In Radio Network' section is highlighted with a red box, and the 'Repeater' option is selected. The 'Root Parent MAC 1 (optional)' field is also highlighted with a red box and contains the value '0c27.2477.4c10'. Other configuration options include 'Operating Mode: Mixed', 'Enable Radio: Enable', 'Current Status (Software/Hardware): Disabled', 'Beacon Privacy Guest-Mode: Disable', 'Beacon Period: 100', 'Max. Data Retries: 64', 'Fragmentation Threshold: 2346', 'Root Parent Timeout: 0', and 'Data Beacon Rate (DTIM):'. The interface also shows a 'Close Window' button and a status bar at the bottom indicating 'En attente de 10.0.0.11...'.

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

Hostname ap

Association					
Clients: 0			Infrastructure clients: 1		
View: <input checked="" type="checkbox"/> Client <input checked="" type="checkbox"/> 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.