TP réseaux
Wireless Fidelity

Pascal Sicard

1 Avant-propos

Les questions auxquelles il vous est demandé de répondre sont indiquées de cette manière.

Il sera tenu compte de la clarté et de la concision de la rédaction des réponses lors de la correction des comptes-rendus.

Si vous désirez conserver *temporairement* une trace de vos travaux, vous pouvez créer un répertoire personnel sur le disque dur des PCs que vous utilisez. Attention, chaque station dispose de son propre disque. Il n'y a aucune garantie de conservation de vos données sur ces machines.

2 Introduction

Ce TP illustre les réseaux radio utilisant la norme IEEE 802.11, autrement dit les réseaux sans fil Wifi.

2.1 Topologies

Un réseau WIFI est identifié par un ***ESSID*** (Extended Service Set Indentifier) abrégé ***SSID***, désigné par une chaine de caractères.

Il existe plusieurs possibilités de topologies de réseau Wifi. La première utilisée habituellement pour la couverture d'un bâtiment (type "infrastructure"), consiste à placer des bornes dites ***points d'accès***, les machines utilisateurs se connectent ensuite à la borne la plus proche. Ces bornes permettent en général de se relier à un réseau filaire,

0. Version 8 janvier 2022

Ethernet par exemple, elles s'apparentent alors à des ***ponts Wifi/Ethernet*** (voir la figure 1).

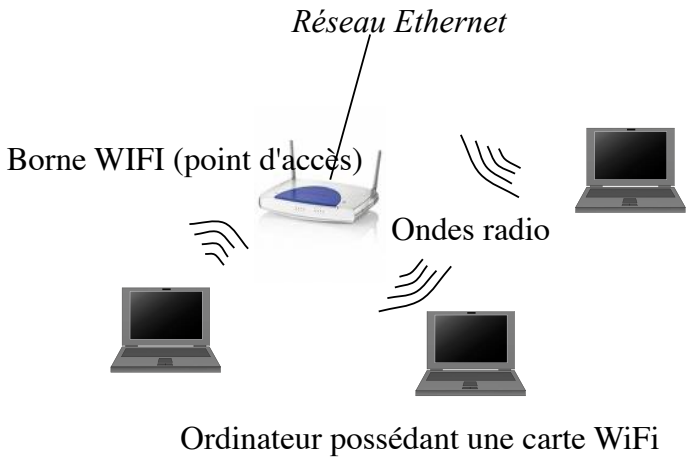

FIGURE 1 – Topologie en mode infrastructure à base de point d'accès

Tous les paquets passent alors par le point d'accès (similaire à un switch). En cas de plusieurs points d'accès accessibles pour un même réseau (même SSID), la carte WIFI choisi le plus proche en testant les performances du réseau physique. En cas de plusieurs réseaux accessibles (SSID différents), l'utilisateur peut choisir le réseau auxquel il veut se raccorder.

Il est aussi possible de ne pas utiliser de point d'accès, on parle d'infrastructure point à point ou ***Adhoc***. Les cartes sont configurées dans un mode particulier et l'échange des paquets se fait directement entre machines utilisateurs (voir la figure 2).

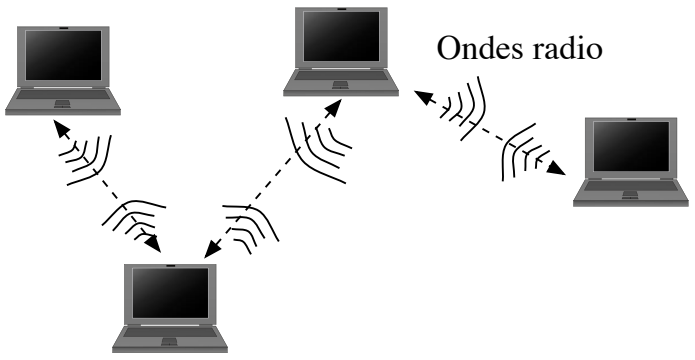

FIGURE 2 – Topologie en mode Adhoc

2.2 Plages de fréquences

2.2.1 Bande 2,4 Ghz

Dans cette bande, il est possible d'utiliser différentes plages de fréquences radio, 13 canaux en Europe (14 aux Etats Unis) ont été définis. La figure 3 montre la répartition des ces canaux et leurs recouvrements. Le choix de ces canaux est laissé à l'utilisateur. En particulier il est judicieux de choisir des canaux indépendants pour la configuration de borne d'accès proches.

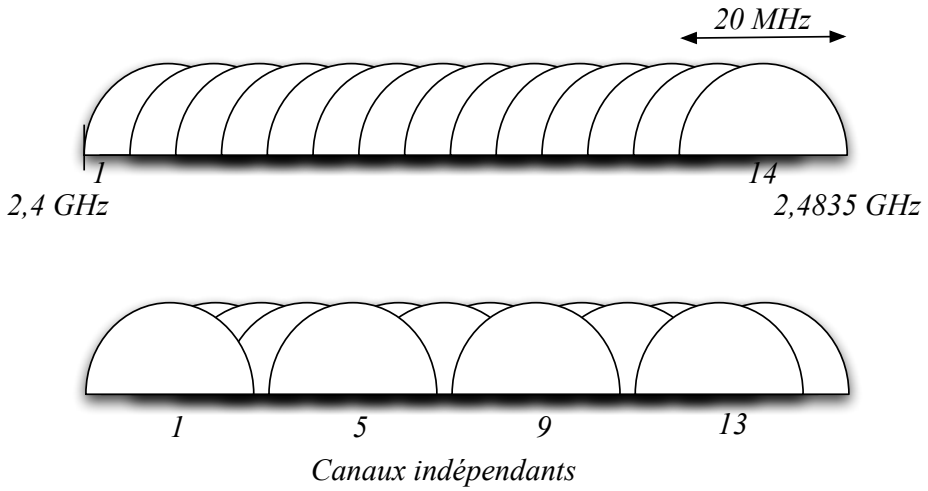

FIGURE 3 – Canaux radio des réseaux WIFI

2.2.2 Bande 5 Ghz

Pour le déploiement des dernières normes de réseaux WIFI (IEEE 802.11n et IEEE 802.11ac) des fréquences dans cette bande sont autorisées en France depuis 2008.
En Europe il y a 19 canaux (36 à 64) possibles. Ces canaux ne sont pas superposés et ils peuvent être regroupés par 2 pour le IEEE 802.11n et par 2, 4 ou 8 pour le IEEE 802.11ac.

3 Expérimentations

3.1 Configuration d'une interface en mode station

Sous Free-BSD il est possible de connaitre le nom de l'interface physique WIFI à l'aide de la commande :
sysctl net.wlan.devices.

Quel est le nom de l'interface WIFI présente sur les PCs ?

Il faut pour la configurer définir une une interface virtuelle :
ifconfig *wlan0* ***create wlandev*** *iwm0* ***up***

Cette commande crée une interface virtuelle de nom *wlan0* basée sur l'interface WIFI physique *iwm0*.

On peut à tout moment supprimer cette nouvelle interface par :
ifconfig wlan0 destroy

Il est possible une fois une interface WIFI mise en marche, d'obtenir la liste des réseaux WIFI à l'aide de la commande :
ifconfig *wlan0* ***scan***

1. *Affichez les réseaux WIFI accessibles.*
2. *Sur quels canaux le réseau wifi-campus est il présent ?*
3. *Pourquoi le réseau wifi-campus apparait il sur différents canaux ?*
4. *Wifi-campus est il accessible dans la norme 802.11ac ?*

Vérifiez l'état de l'interface WIFI par :
ifconfig wlan0.

1. *A quel réseau la carte WIFI s'est elle associé ?*
2. *Quelle est la norme WIFI utilisée par l'interface WIFI présente ? Avec quel débit physique ?*
3. *L'interface WIFI possède t-elle une adresse IP ?*

On peut définir le SSID de rattachement (ou de définition en cas de point d'accès) :
ifconfig *wlan0* ***ssid*** *MonSSID*
Essayez de vous associer à d'autres réseaux visibles. Est ce possible ? Conclusions ?

On peut définir le canal utilisé par la carte WIFI :
ifconfig *wlan0* ***channel*** *NoChannel* ***ssid*** *MonSSID*
Attention il faut changer en même temps de *ssid* pour que le changement du channel soit possible.

1. *Essayez de changer le canal utilisé pour accéder au réseau wifi-campus. Quel intérêt ?*
2. *Est ce possible sur le canal 40 ?*

3.1.1 Différents modes de fonctionnement existants

Une interface WIFI peut être configurée dans différents modes :
— ***sta*** : mode *station*, permet à l'ordinateur de se connecter à un réseau à base de bornes d'accès.
— ***ap*** : mode *acces point* permet à à l'ordinateur de devenir un point d'accès WIFI.
— ***adhoc*** : mode *adhoc* permet à à l'ordinateur de se connecter à d'autres machines en mode Adhoc.
— ***monitor*** : mode moniteur, permettant de capturer des paquets sans se connecter à un point d'accès.

On peut connaître les différents modes d'utilisation supportés pour l'interface WIFI présente sur les PCs par :
ifconfig *wlan0 list caps*

Dans quel mode la carte WIFI présente s'est elle configurée ?

On peut changer de mode par la commande *ifconfig wlan0 wlanmode modechoisi*

A priori il n'est pas possible de changer de mode pour ces interfaces.

3.1.2 Attribution d'une adresse IP

L'interface WIFI n'a pas d'adresse IP. Pour en récupérer une sur le réseau *wifi-campus*, il est possible de lancer un client DHCP par ***/sbin/dhclient wlan0***.

1. *Observez les paquets circulant sur le réseau WIFI au moment du lancement du client DHCP. Retrouvez les informations de configuration.*
2. *Vérifiez que la machine possède maintenant une adresse IP, une route par défaut (netstat -rn) via l'interface WIFI et un serveur DNS (/etc/resolv.conf).*
   ***Attention** si une route par défaut existe déjà via une autre interface le client DHCP ne la change pas, il faut donc la supprimer au préalable.*
3. *Avez vous accès à Internet ?*

3.1.3 Authentification par login

Il n'est toujours pas possible d'accéder à l'extérieur via *wifi-campus*, il reste à s'authentifier auprès du réseau. Sur ce réseau l'authentification est possible via l'accès au site WEB ***portail-captif.grenet.fr***.

Après authentification vérifier votre accès à Internet.

3.1.4 Configuration via le fichier de configuration

Ces configurations peuvent être effectuées au moment du boot de la machine, il suffit pour cela de modifier le fichier système *rc.conf* :
wlans_iwm0="wlan0"
create_args wlan0= "wlanmode sta"
ifconfig_wlan0="DHCP"

La dernière ligne permet de lancer un client DHCP.

Ce n'est pas la peine d'essayer, la manip est dangereuse, une erreur de syntaxe dans ce fichier et la machine peut ne plus booter correctement, passez plutôt à la suite.

3.2 Observations de paquets

1. *Capturez les paquets émis lors d'un ping www.google.com.*
2. *Observez l'entête de niveau liaison de données des paquets, quelles différences avec une entête Ethernet ?*
3. *Les données circulant sur le réseau sont elles chiffrées ?*
4. *Essayez un accès à wikipedia via un navigateur.*
   - *Les données circulant sur le réseau sont elles chiffrées ?*
   - *A quel niveau ?*
   - *Quel est le protocole de sécurisation utilisé ? Rappelez brièvement son fonctionnement.*
   - *Peut-on accéder à un site web http. Essayez. Conclusions ?*

3.3 Utilisation d'un routeur Cisco

3.3.1 Configuration d'un point d'accès

La figure 4 décrit le point d'accès inclus dans les routeurs Cisco 800. Il faut configurer et paramétrer l'interface radio appelée ***Dot11Radio*** (0 ou 1).
Puis il faut configurer l'interface Ethernet ***GigabitEthernet 0 (GE0)*** du point d'accès. Cette interface Ethernet est relié à l'interface d'un switch interne qui est lui même relié à l'interface du routeur proprement dites ***VLAN1***.

L'interface ***wlan-ap 0*** permet **seulement** de configurer le module point d'accès à partir du routeur (voir commande ***service-module*** plus loin). Elle n'intervient donc pas dans le réseau composé du point d'accès et du switch inclus dans le routeur. Il faut malgré tout lui affecter une adresse réseau pour pouvoir configurer l'AP.

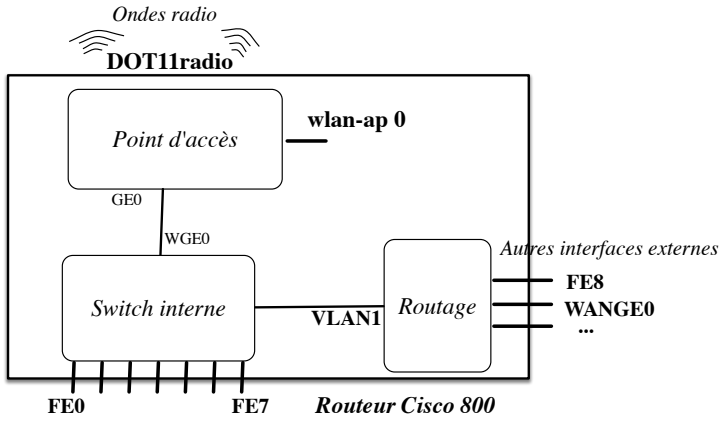

FIGURE 4 – Architecture du point d'accès

Configuration du point d'accès (AP) :

1. Configuration de l'interface Ethernet permettant de configurer l'AP depuis le routeur :
   — ***interface*** *wlan-ap 0*
   — Attribution d'une adresse : ***ip address*** *adresse netmask*
   Attention, l'adresse attribuée devra être une adresse non utilisée par ailleurs (en particulier la plage d'adresse du réseau Point d'accès-switch), une adresse privée autre fait très bien l'affaire.

   — Mise en marche de l'interface : ***no shutdown***

2. Configuration de l'interface Radio de l'AP
   — Il faut tout d'abord ouvrir une session avec le module radio via l'interface *wlan-ap* :
   service-module wlan-ap 0 session (au premier niveau de commande).

   On se retrouve alors dans le module AP avec toutes les commandes habituelles du système CISCO (***enable, configure terminal*** ...).

   — Un *Username* et *password* sont demandés : **cisco** ou **Cisco** dans les deux cas.

   — On peut ensuite configurer l'interface radio :
   configuration terminal puis ***interface*** *dot11radio 0*

   — Définition du SSID : ***ssid*** *nomssid*

   — Dans le mode configuration de SSID (attention la complétion ne marche plus ici), inhiber l'authentification :***authentication open***

   — Passage en mode invité (affichage de SSID dans les paquets Beacon) :
   guest-mode

— Mise en marche de l'interface (après être sortie du mode *ssid*) : ***no shutdown***

— Choix d'un canal : ***channel*** *NoChannel* ou ***channel least-congested***.

— Pour sortir de la session avec le module radio :
ctrl-shift 6 puis x
Puis au prompt du routeur : ***disconnect*** ou ***exit***

— On peut connaitre la liste des ordinateurs connectés au point d'accès WIFI par *show dot11 association*

(a) Vérifiez sur un PC par un scan des réseaux WIFI que le nouveau réseau apparait.
(b) Faire en sorte que deux PCs puissent communiquer entre eux via ce réseau WIFI. On utilisera des adresses privées.
(c) Tester la connectivité et mesurez le débit possible entre les deux machines utilisateurs à l'aide des deux outils udpmt et tcpmt. .

3.3.2 Accès à Internet

Pour l'instant les PCs reliés au point d'accès peuvent communiquer entre eux mais ils n'ont pas accès à l'extérieur.
Il faut pour cela

— Configurer l'interface VLAN1 pour pouvoir connecter le réseau WIFI à d'autres réseaux via le routeur (voir figure 5).
Pour l'interface VLAN 1, on choisit une adresse privée dans la même plage que les PCs connectés à votre réseau WIFI.
  — ***interface*** *vlan 1*
    — Attribution d'une adresse : ***ip address*** *adresse netmask*
    — Mise en marche de l'interface : ***no shutdown***

  Après la configuration de *vlan 1* vérifiez que vous pouvez "pinguer" le routeur à travers le réseau WIFI.
— Relier le routeur Cisco à l'extérieur via le réseau filaire du bâtiment.

  On choisit pour cela une interface Ethernet du routeur non relié au swicth interne (donc autre que FE0 à FE7). Il reste à trouver une adresse publique pour cette interface. On peut prendre une des adresses IP attribuées habituellement à l'interface *em0* d'un des PCs de la plateforme, c'est une adresse publique, il n'y a pas de NAT dans le bâtiment.

  Essayez un *ping 8.8.8.8* sur le routeur. Remédier au problème si cela ne fonctionne pas.

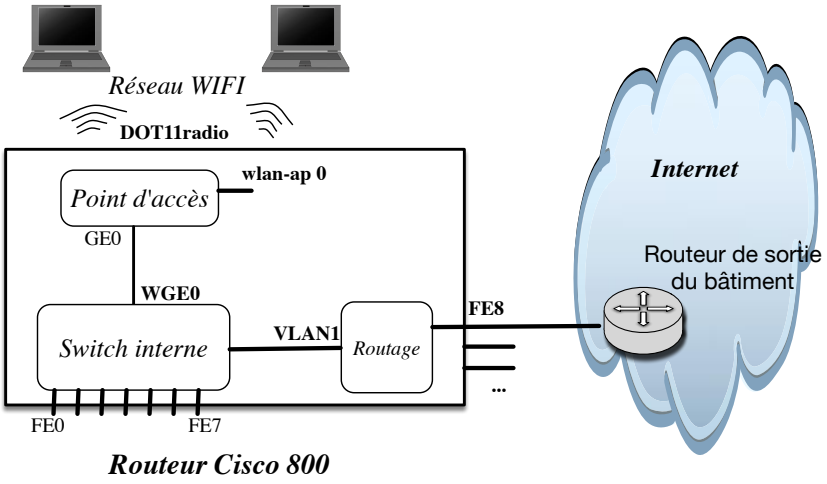

FIGURE 5 – Accès à l'extérieur depuis le routeur Cisco

1. *Les machines reliées au réseau WIFI peuvent elles communiquer avec l'extérieur ? Faites les configurations nécessaires et testez.*
2. *Comment faire en sorte que le DNS fonctionne sur les PCs ? Faites les configurations nécessaires et testez.*

3.4 Sécurisation du réseau WIFI

Si il vous reste du temps...

Nous allons configurer le point d'accès pour mettre en place une de ces méthodes pour l'authentification et le chiffrement des messages. Il existe différentes méthodes de chiffrement/authentification, plus ou moins sûre : WPA, WEP... avec différentes options (clés statiques, dynamiques, utilisation du protocole EAP...).
Voici un exemple de configuration.

1. Configuration du point d'accès sur le routeur
   - Configuration de l'interface radio :
     interface *dot11radio 0*

   - Chiffrement :
     - ***encryption key*** *NombreCle* ***size*** *TailleCle Cle* ***transmit-key*** où
       - *TailleCle* peut être ***40bit*** ou ***128bit***.
       - *Cle* doit être une chaine de 10 (resp. 26) caractères hexadécimaux pour une clé de 40 bits (resp. 128 bits).
       - L'option ***transmit-key*** spécifie que le point d'accès distribue la clé de chiffrement.

— Exemple : ***encryption key 1 size 40bit 0123456789 transmit-key***
— Puis ***encryption mode wep mandatory***
Obligation d'utiliser le chiffrement WEP.

2. Configuration sur les PCs
La commande suivante active un chiffrement WEP avec la clé de 40 bits *0x0123456789*
ifconfig wlan0 wepmode on wepkey 0x0123456789

Pour enlever le chiffrement ***wepmode off***

1. *Mettez en place tout d'abord le chiffrement des données sur le réseau WIFI précédent.*
2. *Observez les paquets lors de l'échange de données entre deux ordinateurs connectés au réseau WIFI. A quel niveau (protocole) se fait le chiffrement ?*
3. *Mettez en place une authentification et un chiffrement WPA sur le réseau WIFI.*
Pour cela trouvez les documentations nécessaires sur le WEB.
Observez les paquets échangés au moment de la connexion.

Documentations sur le chiffrement et l'authentification sur un réseau WIFI :
`https://www.freebsd.org/doc/handbook/network-wireless.html`
`https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/wifi/WiFi_Book/wifi_interface.pdf`
`https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html#wp1035522`

3.5 Rappels NAT

Pour que la translation d'adresse marche sur un routeur CISCO :

1. Il faut désigner les interfaces mise en jeu pour le NAT.
Dans le niveau de commande `configure interface`, il faut tout d'abord configurer les deux interfaces utilisées par le NAT en entrée : `inside` (Intranet) et et en sortie : `outside`(externe) :
ip nat inside — ***outside*** suivant l'interface.
2. Il faut définir l'ensemble des adresses qui vont subir la translation. Pour cela on peut par exemple utiliser une liste d'accès qui autorise toutes les adresses du réseau interne. Exemple : `access-list 7 permit 192.168.0.0 0.0.255.255`
3. On spécifie d'utiliser cette *access-list* pour la translation d'adresse :
ip nat inside source list `7` ***interface*** `interfacesortie` ***overload***
où `interfacesortie` est l'interface de sortie du NAT.