



**R 3.06**

**2023 - 2024**

# Architecture des réseaux

**TP n° 5 b**  
**WIFI 2**



**ANNE Jean-François**  
*D'après le cours de M. JEANPIERRE*

# WIFI – 1841

## 1°) Introduction

Le WIFI est un ensemble de protocoles vaste et complexe, pourtant à usage très simple. L'objectif de ce TP est de vous permettre de configurer un routeur 1841 en point d'accès Wifi, et d'y ajouter un soupçon de cryptage.

## 2°) Disclaimer

Ce TP n'est pas strictement égal à celui fait par les autres groupes, car l'architecture de 1941W obéit aux règles des routeurs 'nouvelle génération' et contient un point d'accès complet et indépendant, relié à un routeur 'conventionnel'. Et ceci complique outrageusement la configuration.

Configurer un point d'accès *grand public* est heureusement beaucoup plus simple, grâce en particulier à de nombreux réglages par défaut, et à une interface web mettant les réglages classiques à la portée de tous...

## 3°) Allons-y :

Les Routeurs 1841 possèdent deux *slots* d'extension, qui peuvent contenir toute sorte d'interface réseau. Ceux que vous avez devant vous possèdent une extension HWIC-AP, qui ajoute une interface Wifi aux deux interfaces FastEthernet usuelles. Vous avez donc 3 interfaces réseau disponibles : FastEthernet 0/0, FastEthernet 0/1 et Dot11Radio 0/0/0.

Afin de lisser les différences avec les autres groupes, je vous propose de voir dans un premier temps la notion de pont réseau, même si elle n'est pas à 100% nécessaire à ce TP avec les 1841.

## 4°) Notion de pont (bridge)

Chaque interface réseau peut appartenir à un *bridge-group*. Toutes les interfaces d'un même groupe sont reliées entre elles par un commutateur (switch) virtuel.

Essayez les commandes suivantes :

```
enable
configure terminal
no ip domain-lookup
interface Fast 0/0
    bridge-group 1
    no shutdown
exit
interface Fast 0/1
    bridge-group 1
    no shutdown
exit
bridge irb
bridge 1 protocol ieee
bridge 1 route ip
interface BVI 1
    ip address 192.168.2.1 255.255.255.0
    no shutdown
exit
ip dhcp pool test
    network 192.168.2.0 255.255.255.0
exit
```

Connectez ensuite un PC sur chaque port FastEthernet du routeur, et réinitialisez leur configuration IP.

Quelles sont les adresses IP de chaque PC ?

Testez le ping entre les 2 pc. Que pensez-vous de la variation du TTL entre les 2 machines ?

Dessinez le schéma logique de ce réseau.

### 5°) Configuration d'un réseau « open »

Je vous propose maintenant de configurer l'AP de façon à créer un point d'accès wifi proposant un réseau ouvert.

Depuis le mode configuration de l'AP :

```
interface Dot11Radio 0/0/0
  ip address 10.1.1.1 255.255.255.0
  ssid mon_reseau                               Remplacez le SSID par un nom unique !
  authentication open
  guest-mode
end
```

Avec ces quelques commandes, vous créez un réseau wifi doté d'un SSID « mon\_reseau », public et sans sécurité. `guest-mode` permet l'envoi de trames d'annonce `beacon frames`. Sans elles, le réseau existe mais n'est pas affiché : Seuls ceux qui le connaissent peuvent s'y connecter.

Pouvez-vous voir ce réseau ?

Affichez l'état des interfaces réseau (`show interfaces`). Conclure...

```
interface Dot11Radio 0/0/0
  channel 4
  station-role root
  power local cck 7                               Puissance pour le 802.11b
  power local ofdm 7                             Puissance pour le 802.11g
  power client 7
  speed throughput
  no shutdown
end
```

Ces quelques lignes activent cette interface, choisissent le canal et règlent la puissance d'émission au minimum. Cela devrait limiter les interférences avec le reste de l'IUT, voire avec les autres maquettes de la salle...

Pouvez-vous voir ce réseau ? Pouvez-vous vous y connecter ? Pourquoi ? Corriger ce problème.

Pouvez-vous pinguer l'AP (10.1.1.1) depuis les PCs ? Pourquoi ? Corriger ce problème.

Pouvez-vous pinguer le client wifi depuis les PCs ? Pourquoi ? Corriger ce problème.

### 6°) Configuration d'un réseau WPA-PSK

Je vous propose maintenant d'ajouter un peu de cryptage à votre réseau. Je vous conseille d'effacer préalablement votre réseau wifi précédent, car les conflits sont parfois lourds à gérer (bonnes commandes dans le bon ordre).

```
interface Dot11Radio 0/0/0
  no ssid mon_reseau                             Efface le SSID mon_reseau
  encryption mode ciphers tkip
  ssid ton_reseau
  authentication open
  authentication key-management wpa
  guest-mode
  wpa-psk ascii 0 testtest                       Le mot de passe doit contenir au moins 8
caractères
end
```

Pouvez-vous voir ce réseau ?

Pouvez-vous vous y connecter ?

## 7°) Capture de trames Wifi

Le routeur 1841 n'a pas cette fonctionnalité dans sa version présente.  
Je vais donc vous proposer un exercice un peu différent...

## 8°) Plusieurs SSID simultanés

Vous pouvez placer plusieurs réseaux wifi sur la même borne, mais un seul peut être public (*guest-mode*). Chaque SSID doit être associé à un VLAN. La notion de cryptage doit elle aussi être associée à chaque VLAN...

```
interface Dot11Radio 0/0/0
  no ip address
  encryption vlan 3 mode ciphers tkip
  ssid public
    vlan 2
      authentication open
      exit
  ssid prive
    vlan 3
      authentication open
      authentication key-management wpa
      guest-mode
      wpa-psk ascii 0 testtest           Le mot de passe doit contenir au moins 8
caractères
      exit
  channel 4                             Choisissez un canal différent par
maquette !
  station-role root
  power local cck 7                      Puissance pour le 802.11b
  power local ofdm 7                    Puissance pour le 802.11g
  power client 7
  speed throughput
  no shutdown
  exit
interface Dot11Radio 0/0/0.2
  encapsulation dot1Q 2
  bridge-group 1
  exit
interface Dot11Radio 0/0/0.3
  encapsulation dot1Q 3
  ip address 10.1.1.1 255.255.255.0
end
```

Combien de réseaux voyez-vous ? Pouvez-vous vous connecter sur le réseau « public » ? Sur le réseau « prive » ?

Quelles sont vos adresses IP dans ces deux cas ? Pourquoi ?

Pouvez-vous pinguer les PC (ou les clients depuis les PC) ?

Dessinez le schéma logique incluant les 2 PCs, le Routeur, et les deux clients Wifi (public et privé).

**N'oubliez pas le NETTOYAGE**  
**en fin de séance**