R 3.06

2023 – 2024

Architecture des réseaux

TP n° 5 a
WIFI

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

WIFI – 1941W

1°) Introduction

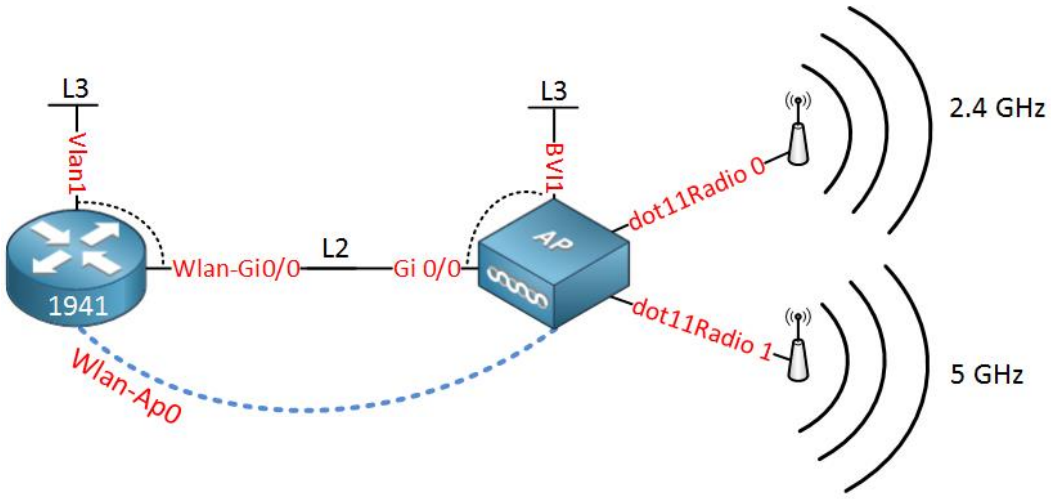
Le WIFI est un ensemble de protocoles vaste et complexe, pourtant à usage très simple. L'objectif de ce TP est de vous permettre de configurer un routeur 1941 en point d'accès Wifi, et d'y ajouter un soupçon de cryptage.

2°) Disclaimer

Ce TP va vous paraître outrageusement compliqué, car le système choisi par Cisco pour les routeurs *nouvelle génération* consiste à associer un routeur de couche 3 *classique* à un point d'accès de couche 2 complet. Du coup, monter un point d'accès *standard* conjugue 3 problèmes simultanés : Le routage, le wifi, et *la communication entre les deux plateformes* ! Bien sûr le cryptage ajoute un 4° niveau de problèmes…
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 :

Tout d'abord, voici un schéma explicatif de la structure interne du routeur :



(c) Rene Molenaar - http://networklessons.com/wireless/cisco-1941w-wireless-configuration-example

Vous pouvez y ajouter 2 interfaces de niveau 3 GigabitEthernet 0/0 et 0/1, les deux ports réseau externes.
Le problème principal de cette configuration est que le point d'accès n'est qu'un appareil de niveau 2, c'est-à-dire un commutateur (switch). La seule interface de niveau 3 (IP) est BVI1 (Bridge Virtual Interface 1). C'est elle qui va permettre la communication avec le routeur, à l'aide d'un switch interne (marqué L2 sur le schéma ci-dessus).

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 Gig 0/0
  bridge-group 1
  no shutdown
  exit
interface Gig 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 /24
    exit
```

Connectez ensuite un PC sur chaque port Gigabit du routeur.
Quelles sont les adresses IP de chaque PC ?
Testez le ping entre les 2 pc. Que pensez-vous du TTL ?
Dessinez le schéma logique de ce réseau.

5°) Configuration du point d'accès (AP)

Pour configurer le point d'accès, vous devez d'abord l'activer, et lui donner une adresse IP. Celle-ci ne sera utilisée qu'en interne dans le routeur. Elle peut donc être quelconque.

```
  interface wlan-ap 0
    ip address 1.2.3.4 255.255.255.0
    no shutdown
    exit
  interface vlan 1
    ip address 10.1.1.1 255.255.255.0
    no shutdown
  end
  service-module wlan-ap 0 session
```

Cette dernière commande redirige la console vers l'AP interne, via l'adresse IP que vous venez de régler.
Pour revenir au routeur, tapez *Control-Shift-6 x*. Vous restez sur le routeur jusqu'à taper une commande vide. Vous pouvez aussi entrer la commande *disconnect* pour quitter définitivement l'AP.
Le mot de passe par défaut de l'AP est cisco/cisco.
Le point d'accès possède un IOS proche de celui d'un switch, aussi vous devriez y être à l'aise rapidement…

```
  configure terminal
  no ip domain-lookup
  int GigabitEthernet 0
    bridge-group 1
    exit
  bridge irb
  interface BVI 1
    ip address 10.1.1.2 255.255.255.0
    no shutdown
  end
  ping 10.1.1.1
```

Ces quelques commandes vous permettent de configurer le pont interne au routeur permettant la communication entre ce dernier et son point d'accès. Le VLAN 1 du routeur est ainsi doté d'une IP, 10.1.1.1 et l'interface virtuelle de l'AP d'une IP 10.1.1.2, associée au port interne de l'AP dans le routeur. Le ping devrait donc fonctionner.
Pouvez-vous pinger les PC depuis l'AP ? Pouvez-vous ping l'AP depuis les PC ? Pourquoi ?
Corrigez la configuration de façon à ce que cela fonctionne.

6°) 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 :

```
  dot11 ssid mon_reseau                    Remplacez le SSID par un nom unique !
    authentication open
    guest-mode
    exit
```

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 ? Pouvez-vous vous y connecter ?
Affichez l'état des interfaces réseau (*show interfaces*). Conclure…

Il est donc maintenant nécessaire d'associer ce réseau wifi à une interface radio. Votre AP en possède 2 : Dot11Radio 0/1. La première permet de communiquer sur la bande de 2.4GHz, alors que la seconde travaille sur celle des 5GHz. Je vous encourage à prendre celle des 5GHz, car plus de canaux y sont disponibles et le 1811 ne peut travailler que sur la bande des 2.4GHz… Elle risque donc d'être plus occupée…

```
  interface Dot11Radio 1
```

```
    ssid mon_reseau
    channel 36              least-congested = le moins utilisé
    station-role root
    bridge-group 1
    power local 8
    power client 8
    speed throughput
    no shutdown
    end
```

Ces quelques lignes associent le réseau de SSID *mon_reseau* à cette interface, choisit le canal et règle 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.

7°) 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).

```
  dot11 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
    exit
  interface Dot11Radio1
    encryption mode ciphers tkip
    ssid ton_reseau
    power local 8
    power client 8
    channel 40
    station-role root
    bridge-group 1
    no shutdown
    end
```

Pouvez-vous voir ce réseau ? Pouvez-vous vous y connecter ?

8°) Changement d'adresse

Quels paramètres ci-dessus faudrait-il modifier si l'on voulait changer l'adresse IP du réseau Wifi ?

9°) Capture de trames Wifi (Bonus)

La capture de trames Wifi est difficile car il faut tout d'abord être associé à un AP, et donc d'avoir entré le bon mot de passe. Votre machine ne reçoit alors que des trames Ethernet classiques. Heureusement il existe quelques solutions permettant de passer outre… La suite logicielle AirCrack est la plus connue. Wireshark propose aussi une extension (payante) airPcap. Heureusement, le routeur Cisco propose un service de détection d'intrusion : CWIDS.
Il faut pour cela reconfigurer votre point d'accès en mode scanner :

```
  interface Dot11Radio1
    station-role scanner
    channel <freq>        Vous ne pouvez espionner qu'un seul canal à la fois
    monitor frames endpoint ip address <ip> port <port> truncate 2312
    end
```

Vous allez alors recevoir sur le PC désigné par son IP des trames UDP qui incluent un entête de 28 octets et une ou plusieurs trames IEEE 802.11. Vous pouvez aussi lancer un serveur (*netcat*) UDP écoutant sur le port que vous avez choisi pour éviter les trames ICMP d'erreur…
Lancez donc Wireshark, capturez des trames, puis sélectionnez l'une des trames émises par le routeur.
Faites alors un clic-droit sur le champ « data », puis decode-with « cwids » (Cisco Wireless Intrusion Detection System).
Bon courage pour l'analyse des trames !

N'oubliez pas le NETTOYAGE en fin de séance