Internet sans fil : concepts, technologies et architectures

Rémy Grünblatt 2022

Informations

La majorité de ce TP peut s'effectuer plutôt facilement sous Linux, mais avec plus de difficulté sous Windows et probablement encore plus sous OSX. Pour faciliter le déroulement de ce TP, il est proposé d'utiliser un système d'exploitation dédié sous la forme d'un système *live*, c'est-à-dire un système exécutable sans installation nécessaire. Des clefs USB sur lesquelles sont pré-installés différents outils ainsi que la distribution Ubuntu sont disponibles auprès de votre chargé de TP. N'hésitez pas à demander de l'aide pour booter le système sur vos machines.

Information: Merci de bien penser à ramener ces clefs USB à la fin du TP.

Partage du Medium (30 minutes)

Important: Il est plus que conseillé de vous coordonner avec les autres groupes de TP, sous peine de fausser vos mesures.

Un point d'accès Wi-Fi est disponible dans la salle de TP. Il possède deux SSID, "NET4104-2.4G" et "NET4104-5G", qui fonctionnent respectivement sur la bande des 2.4GHz et la bande des 5GHz. Ces points d'accès fonctionnent en mode OPEN (sans chiffrement). Votre but dans cette première partie est de mettre en place un protocole qui permet d'illustrer l'efficacité (ou non) du mécanisme de partage du medium (on le rappelle, il s'agit de CSMA/CA) vers ce point d'accès, en fonction du nombre de stations connectées à ce point d'accès. Pour vous aider dans votre tâche, plusieurs serveurs Iperf3 fonctionnent sur ce point d'accès, et écoutent sur l'adresse IP "192.168.1.1" et les ports 5201, 5202, 5203, 5204 et 5205. Iperf3 est un logiciel qui permet d'effectuer différentes mesures liées aux réseaux IP, en particulier de débit au niveau des couches TCP et UDP. Iperf3 fonctionne sur un modèle client-serveur, on pourra l'installer en utilisant (par exemple) la commande `apt install iperf3` en root. On pourra par exemple essayer de déterminer comment la capacité totale du réseau évolue en fonction du nombre de stations connectées et envoyant des données au point d'accès, ou encore le taux de perte de paquets.

Information: Il est possible d'installer iperf3 (ainsi que d'autres outils orientés réseaux) sur vos smartphones fonctionnant sous Android et iOS en installant la boîte à outils de Hurricane Electric, l'application gratuite "he.net - Network Tools".

Attention, l'interface est un peu trompeuse, il faut rentrer les options de iperf3 dans le champs d'input, par exemple "-c 192.168.1.1" pour lancer l'équivalent de "iperf3 -c 192.168.1.1".

Propagation et Qualité de Service (45 minutes)

Important: Il est plus que conseillé de vous coordonner avec les autres groupes de TP pour choisir quelles mesures sont intéressantes à effectuer, et éviter de les effectuer aux mêmes endroits, en même temps.

Une carte des bâtiments est disponible auprès de votre chargé de TP. En vous inspirant du premier exercice, établir un protocole permettant d'illustrer la qualité de service en fonction de la distance au point d'accès. De même, ce protocole devra permettre d'illustrer la ou les différences de propagation en fonction de la fréquence et de l'environnement du point d'accès (distance, obstacle, ...).

Information: Sous Linux, on peut utiliser la commande `iw` pour obtenir des informations sur sa carte Wi-Fi et sur la connexion courante. En particulier, on pourra utiliser `iw dev` ou `iw dev <device> station dump` pour obtenir des informations sur le nombre de paquets envoyés, reçus, la puissance en réception, ou le débit de transmission.

Monitoring, DNS et WPA2 Entreprise (30 minutes)

Il est possible d'écouter le medium (le spectre) pour observer quelles sont les données qui y sont échangées (sous réserve de pouvoir les décoder, i.e. ne pas être trop loin de l'émetteur par exemple). En particulier, certaines cartes Wi-Fi possèdent un mode de fonctionnement appelé mode « monitor » qui permet de recevoir l'ensemble des trames Wi-Fi captée, et non uniquement celles destinées à notre machine. C'est un outil très intéressant pour comprendre le fonctionnement des protocoles.

Important: Il n'est souvent pas possible de placer sa carte en mode monitor tout en restant connecté à un autre réseau. Ainsi, n'exécutez pas les commandes suivantes si vous souhaitez rester connectés à un réseau Wi-Fi.

Sous Kali Linux (et sous Linux en général), les commandes suivantes peuvent être utilisées pour mettre la carte Wi-Fi en mode monitor:

```
# Cette commande tue les processus ayant la main sur l'interface Wi-Fi
airmon-ng check kill
# Cette commande relance l'interface <interface> en mode monitor
```

```
airmon-ng start <interface>
# Cette commande supprime le mode monitor de l'interface <interface>
airmon-ng stop <interface>
```

Une fois l'interface en mode monitor, lancez Wireshark et activez la « barre d'outils sans-fils » (Onglet View) qui permet d'afficher un menu de sélection du canal sur lequel la carte écoute, ainsi que de sélection de la largeur de bande écoutée.

Écoute de requêtes DNS

Connectez l'un de vos appareil (par exemple un téléphone portable) au point d'accès disponible dans la salle, et ouvrez un navigateur web, puis visitez un site web. Quelles requêtes observez vous ? Quelles données arrivez vous à extraire depuis l'ordinateur qui est en mode monitor ? Essayez d'activer DNS-Over-HTTPS sur votre appareil (possible dans Firefox, possiblement dans d'autres navigateurs web) ; arrivez vous à voir le contenu des requêtes ?

Illustration du processus de connexion WPA 2 Entreprise (PEAP, MSCHAPv2)

Connectez l'un de vos appareil (par exemple un téléphone portable) au réseau eduroam. Quelles requêtes observez vous ? Quelles données arrivez vous à extraire depuis l'ordinateur qui est en mode monitor ?

Réseau Ad-Hoc / Mesh (?? minutes)

En plus du mode « infrastructure » (pour se connecter à un point d'accès) et le mode « monitor » que l'on vient de voir, certaines cartes supportent le mode « ad-hoc » qui permet d'établir des réseaux sans point d'accès, directement entre différentes STA. Ce mode est aussi connu sous le nom de mode « P2P ».

Information: Pour vérifier si votre carte supporte le mode P2P, il est possible d'utiliser la commande `iw phy` pour vérifier les modes de fonctionnement valides des interfaces ("valid interface combinations")

Pour placer la carte en mode ad-hoc:

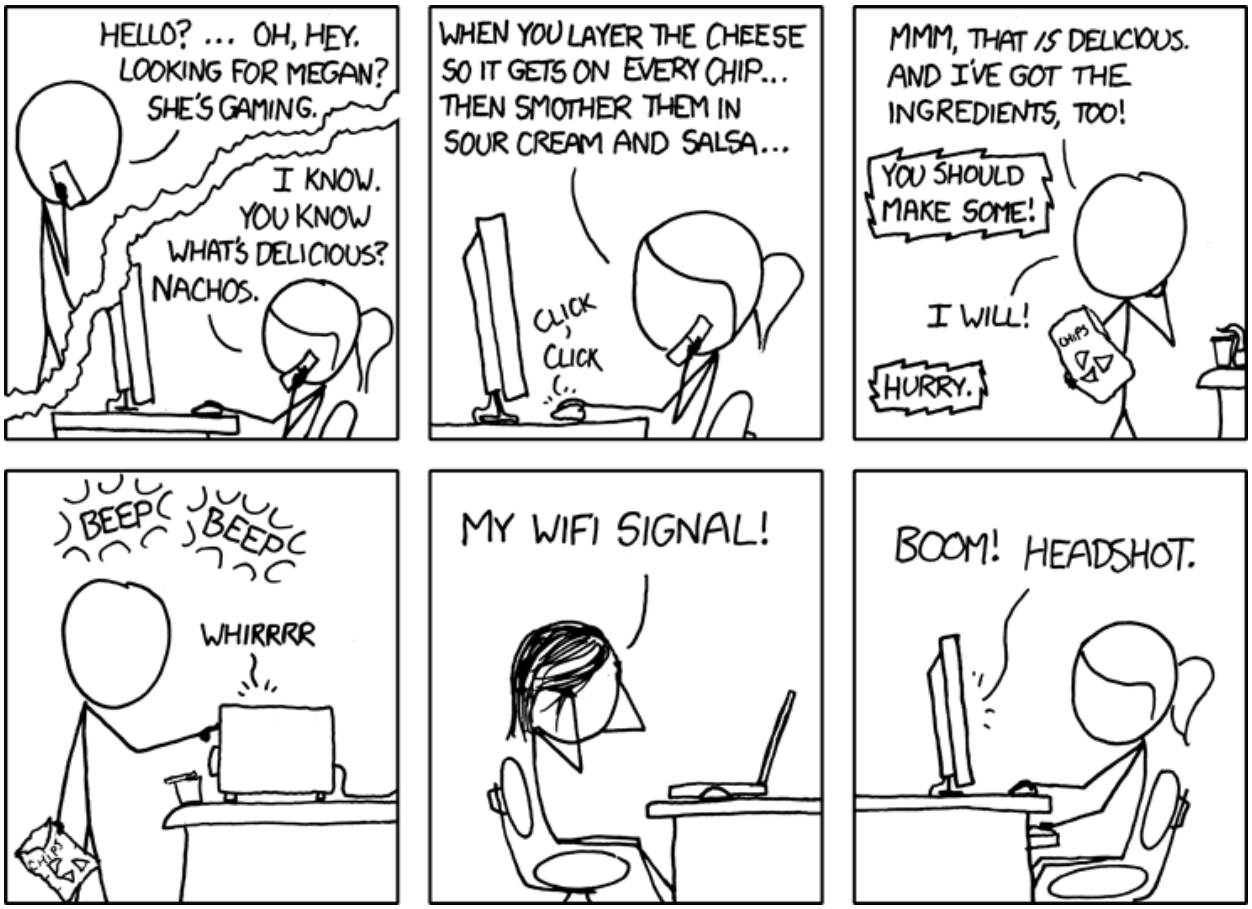
1. S'assurer qu'aucun programme n'utilise le Wi-Fi. On peut utiliser par exemple :
   `airmon-ng check kill`
2. Placer l'interface en mode Ad-Hoc (IBSS) :
   `iw dev <interface> set type ibss`
3. Rejoindre un IBSS :
   `iw <interface> ibss join <SSID> <Fréquence>`
   Par exemple : `iw wlp1s0 ibss join NET4104 2437`

Warning: Un réseau ad-hoc fonctionne déjà dans la salle sur la fréquence 2.437GHz (canal 6), en 20 MHz, un réseau IP en 10.0.0.0/24 où 10.0.0.1 est une adresse déjà utilisée

Information: Vous pouvez suivre l'état de la "connexion" à un réseau ad-hoc dans le journal des messages du noyau, accessible par la commande `dmesg`. Le mode IBSS n'étant pas beaucoup utilisé / testé, il peut arriver que votre carte ne le supporte pas ou le supporte mal, et qu'elle « crashe », ce qui est aussi visible dans ce même journal.

Le fait de rejoindre un BSS n'implique pas d'obtenir une adresse IP, ou d'établir une connexion au niveau IP. Il faut donc ensuite configurer vos interfaces pour qu'elles possèdent chacune une adresse IP (par exemple, dans la plage `10.0.0.0/24`, attention aux doublons !), configurer une route signifiant que ce subnet est disponible directement sur l'interface ("on-link"). Une fois que cela a été fait, tentez de lancer des pings avec d'autres machines du réseau.

Pour aller plus loin, tentez d'utiliser le logiciel babel (`babeld`) pour gérer automatiquement l'ajout de routes et permettre de faire des communications multi-sauts (au niveau IP, et radio) de manière transparente.



XKCD #654 – CC-BY-NC-2.5