Impact de IEEE 802.11 sur les couches supérieures

Introduction

Ce travail s'étale sur deux séances de TP. Les étudiants s'organisent en binômes. Il est évalué sous la forme d'un seul compte rendu par binôme reprenant les expérimentations menées au cours des 2 séances. Il sera remis au plus tard une semaine après la dernière séance. L'évaluation prendra en compte la rigueur et l'exhaustivité de l'investigation et privilégiera le qualitatif au quantitatif.

L'objectif est de mettre en œuvre un certain nombre de configurations (et de variantes de ces configurations) et d'évaluer les performances associées. Le travail qui vous est demandé est « ouvert » en ce sens qu'il ne s'agit pas de répondre à un ensemble de questions prédéfinies mais d'avoir une réelle démarche d'ingénierie visant à mettre en évidence l'impact des couches MAC et PHY de 802.11 sur les couches supérieures et en particulier sur la couche transport.

Pour cela il est mis à votre disposition:

- du matériel WiFi
    - STA Linksys WMP600N (http://www.linksysbycisco.com/EU/en/products/WMP600N)
    - AP Linksys WRT160NL (http://www.linksysbycisco.com/EU/en/products/WRT160NL)
- des PC Linux fixes
    - Distribution : Debian
    - Wireless Tools : v29-1.1 (http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html)

Les configurations

Vous devrez mettre en oeuvre les configurations suivantes:

- une configuration « ad hoc ».
- une configuration « infrastructure »
- une connexion ethernet entre deux BSS

Les outils logiciels

Au-delà des « wireless tools », les outils qui sont mis à votre disposition pour analyser le trafic et mesurer le débit sur l'interface air:

- un « sniffer » pour l'interface air : kismet (http://www.kismetwireless.net/)
- un analyseur de protocoles : wireshark (http://www.wireshark.org/)
- un outil de mesure de débit sur la couche transport : iperf (http://dast.nlanr.net/Projects/Iperf/). Un tutorial : http://www.openmaniak.com/fr/iperf.php

Quelques éléments de réflexion

Les architectures WiFi déployées seront déconnectées du réseau de l'ESIEE.

Ce travail nécessite une grande coordination entre les groupes pour ce qui concerne:

- la planification des canaux radio
- le plan d'adressage IP
- l'utilisation des ressources matérielles

Une série d'expérimentation vous est proposée. Les initiatives personnelles tendant à s'écarter de la simple mise en œuvre seront valorisées. Dans cet esprit et sans aucune exhaustivité, voilà quelques pistes qu'il est possible explorer:

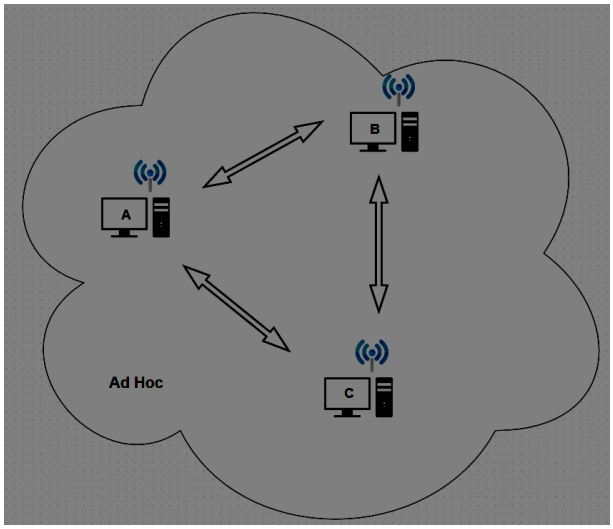
- la mise en place d'architectures avancées
- l'analyse de trames
- la mesure de couverture

Une étude paramétrique peut être conduite sur les éléments suivants :

- les options de configuration élémentaires de la couche MAC
- les caractéristiques de la couche PHY

Exp 1 : Déploiement Ad-Hoc et mesure de performances

Utiliser les commandes iwlist et iwconfig pour établir une architecture ad-hoc.



Une machine établit le réseau

Les autres machines s'y associent. Maximiser la distance entre les machines.

Utiliser un plan d'adressage IP permettant de vérifier la connectivité de chaque machine avec les autres participants du réseau

S'assurer que les conditions d'un débit utile maximal sont réunies. Vérifier la conformité avec les ordres de grandeur théoriques

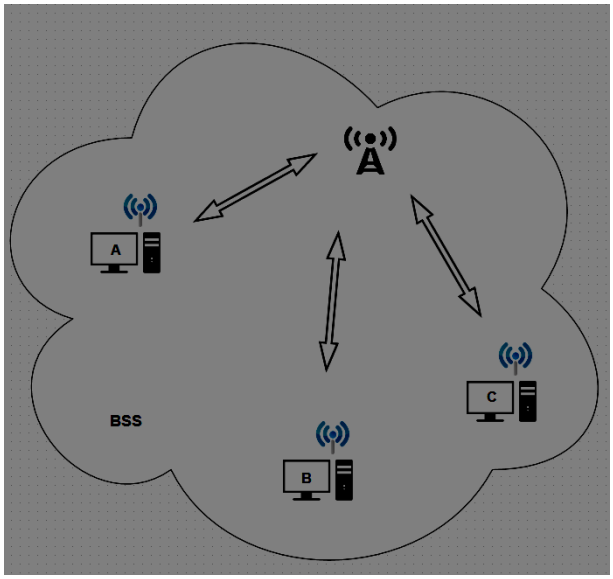
Établir une connexion simultanée entre deux paires de machines et vérifier l'impact sur le débit utile.

Déconnecter une antenne et recommencer l'expérience.

Comparer les résultats entre deux machines proches et deux machines distantes. Le résultat est-il dépendant de la couche physique utilisée ?

Exp 2 :Déploiement BSS

Utiliser les commandes iwlist et iwconfig pour paramétrer les cartes réseau. Utiliser un navigateur web pour paramétrer le point d'accès. Portez une attention particulière au canal radio choisi.



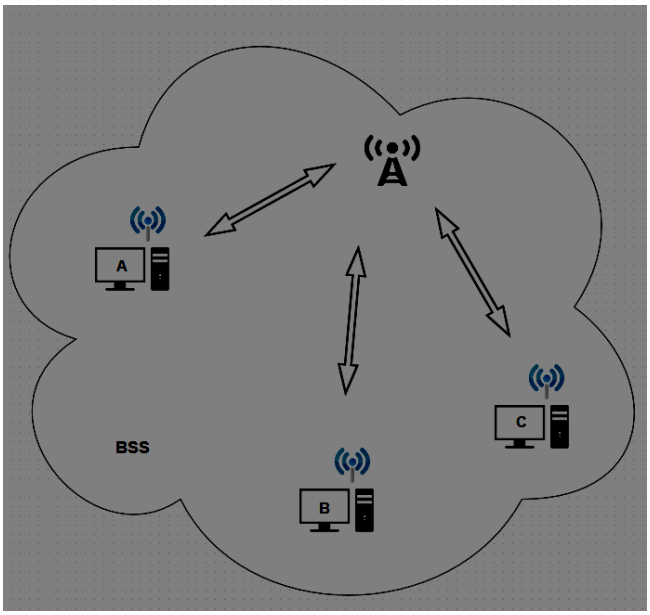
Utiliser un plan d'adressage IP permettant de vérifier la connectivité de chaque machine avec les autres participants du réseau.

Effectuer une mesure de débit rapide pour vérifier que le débit utile observé est bien cohérent avec les paramétrages choisis.

Exp 3 :Surcharge réseau

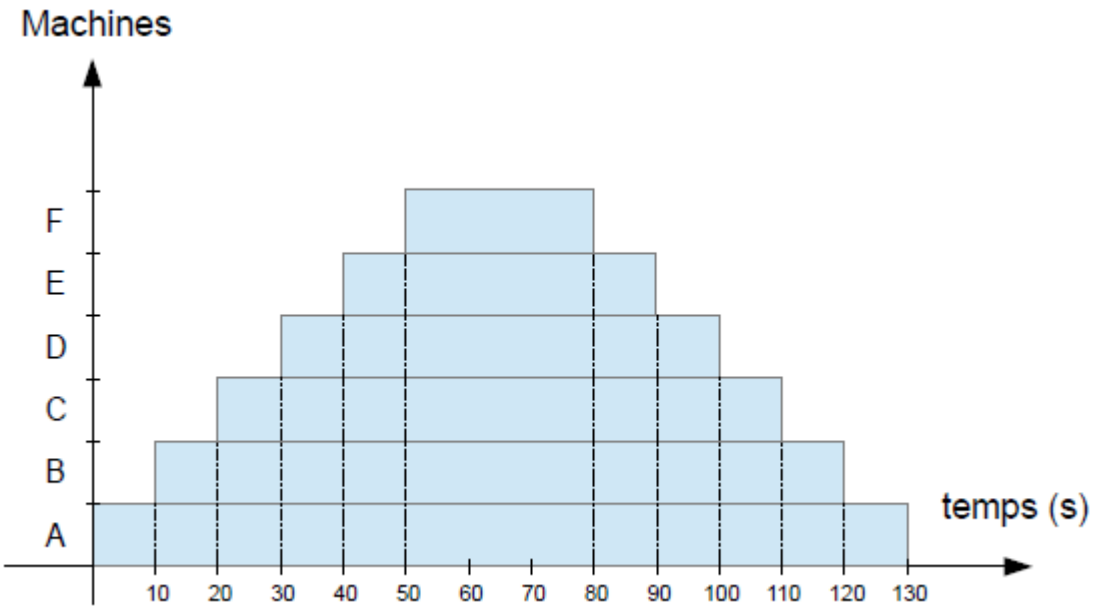
Une possibilité de mesurer la surcharge réseau est la suivante.

Déployer un BSS sur un canal radio peu perturbé comportant 6 machines A, B, C, D, E et F hébergeant chacune un client iperf

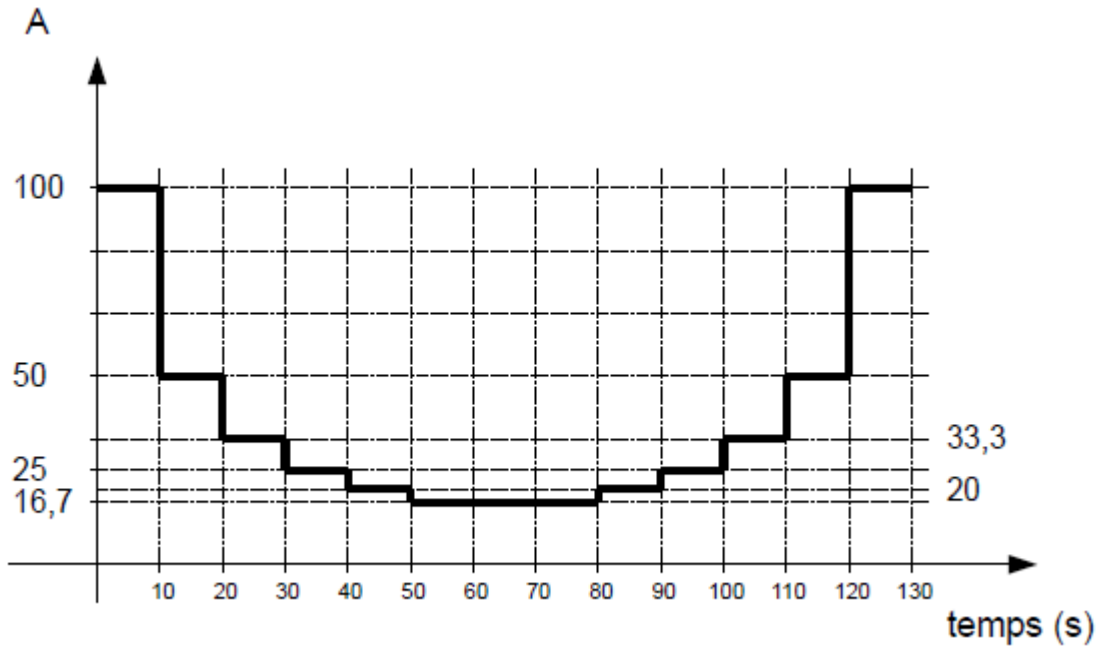


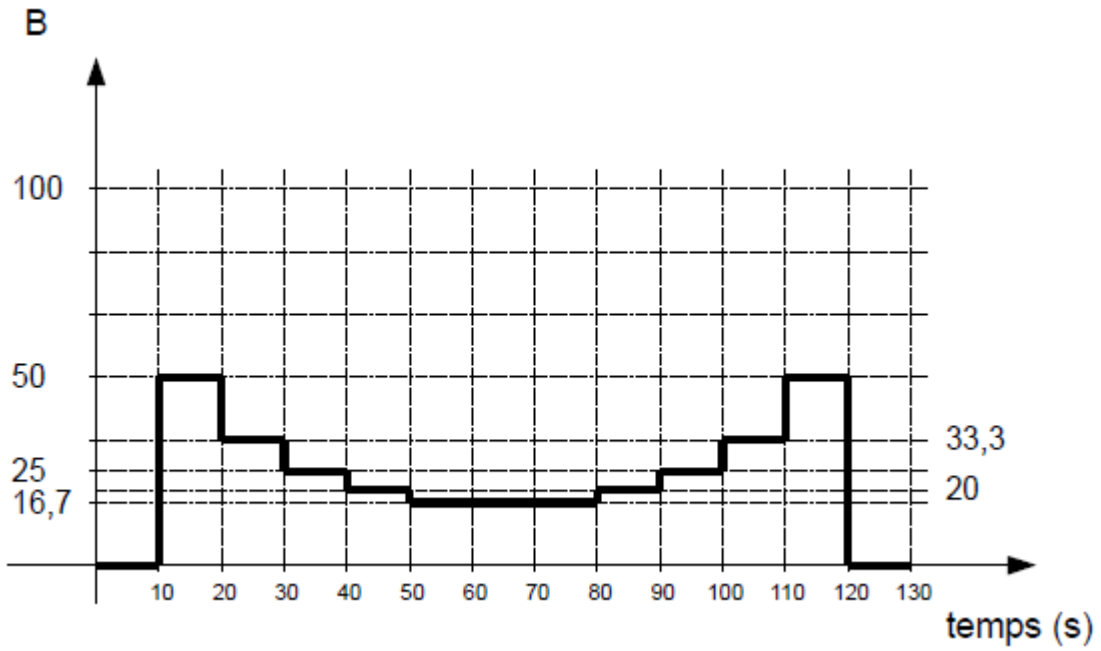
Une machine est connectée en Ethernet filaire au point d'accès et héberge un serveur iperf

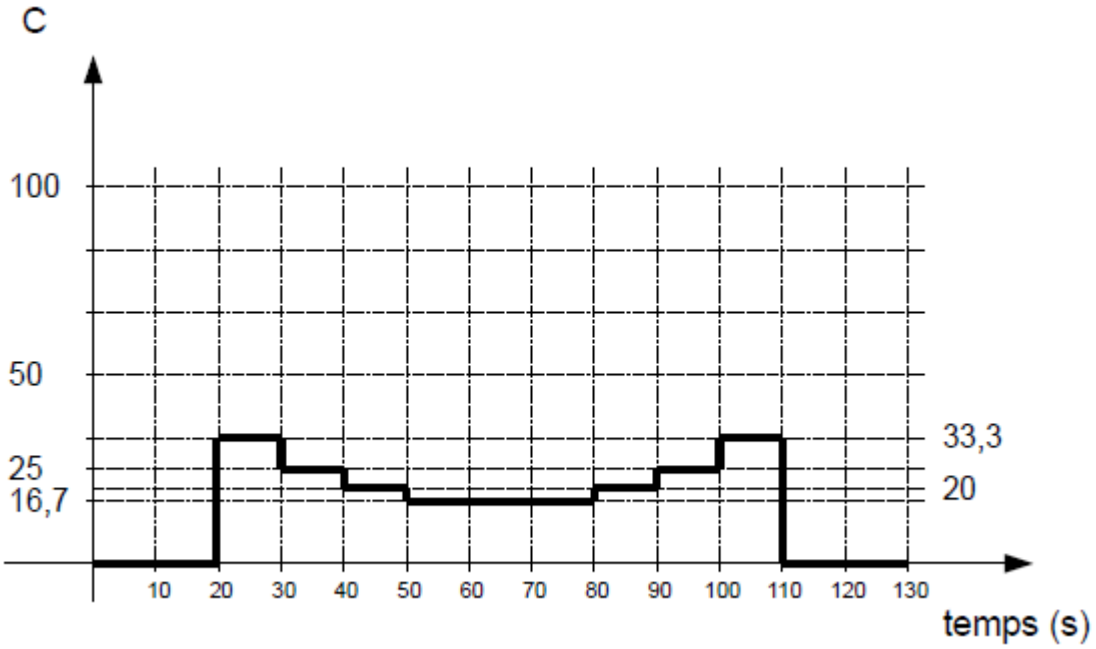
Chaque machine va communiquer à son tour suivant le schéma temporel suivant :

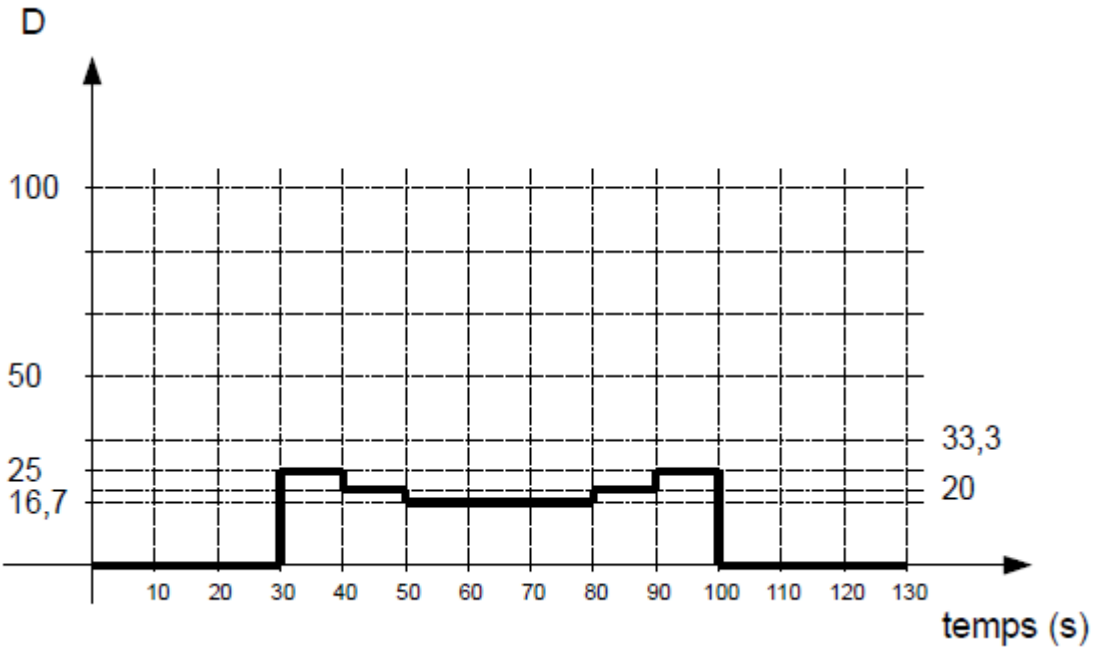


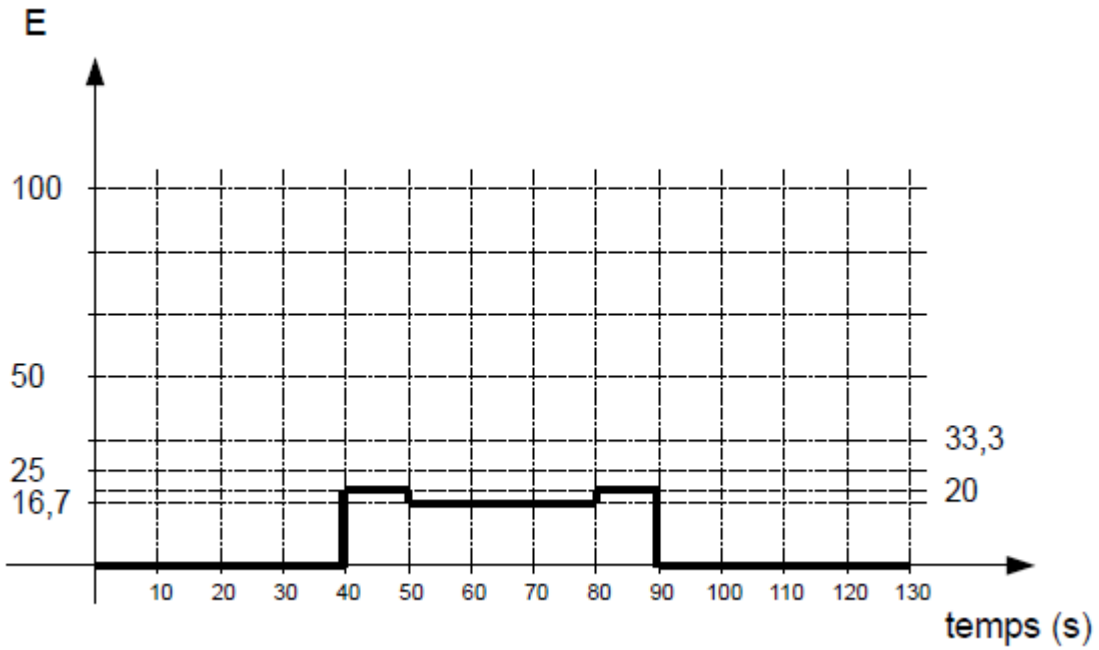
Les diagrammes théoriques de répartition du débit nominal sont les suivants.

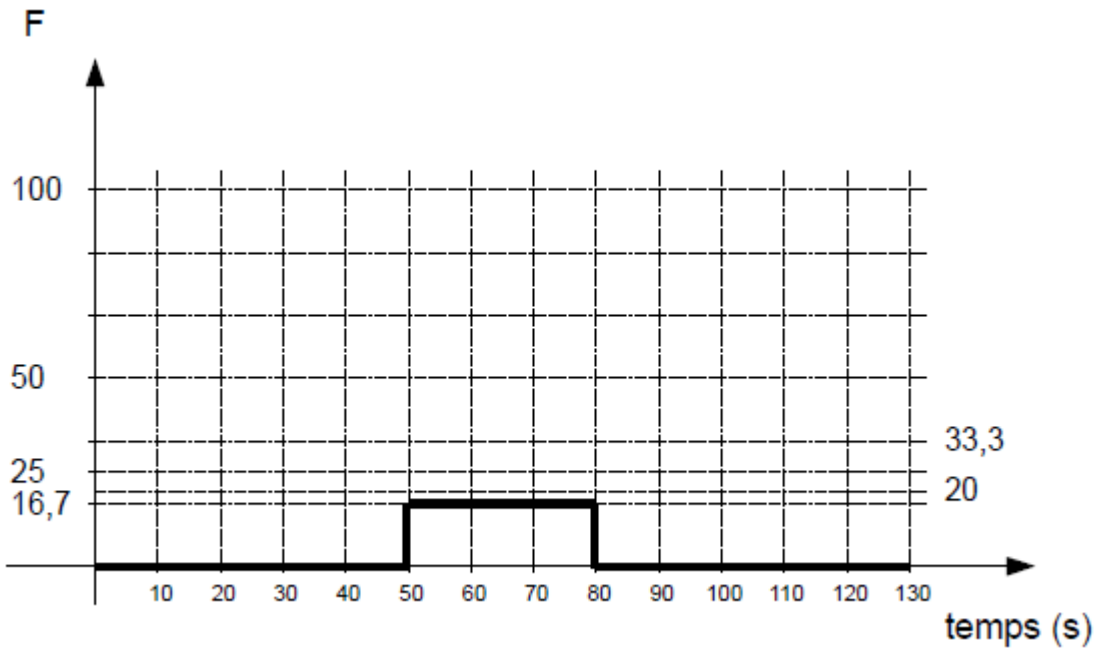





C
100
50
25
16,7
33,3
20
10 20 30 40 50 60 70 80 90 100 110 120 130
temps (s)


D
100
50
25
16,7
33,3
20
10 20 30 40 50 60 70 80 90 100 110 120 130
temps (s)





Tracer pour chaque machine le débit réel observé.

Tracer l'enveloppe globale du débit servi dans le BSS et évaluer les écarts avec la valeur théorique. Qualitativement, interpréter les éventuels écarts constatés.

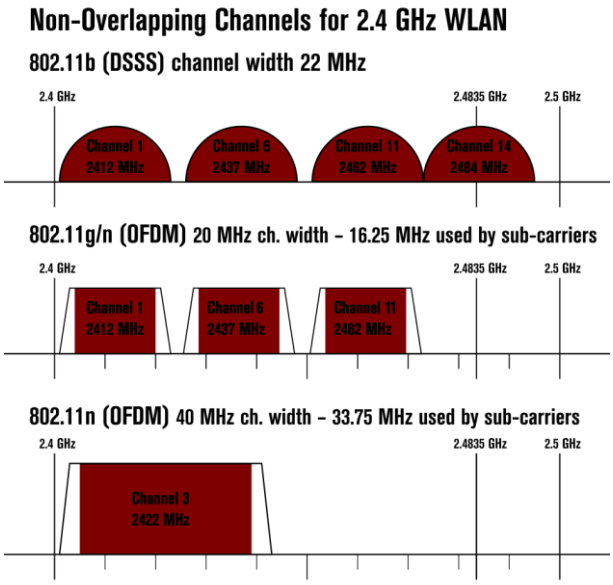
Le milieu ouvert dans lequel s'effectue l'expérimentation ainsi que le caractère non déterministe de l'accès d'une machine à la ressource conduit à des résultats dont il est essentiel de mesurer la reproductibilité. Reproduire deux autres fois l'expérimentation précédente, de façon à disposer de trois réalisations de l'expérience globale.

La conclusion de votre étude devra faire apparaître les valeurs min, moyenne et max des débits mesurés dans chacun des intervalles.

Exp 4 : Recouvrement de canal

Déployez deux architecture BSS, chacune comprenant au moins deux stations. Mettez en place ce qui est nécessaire à la mesure de débit entre les deux stations d'un même BSS.

Le plan de fréquence ci dessous rappelle qu'il y a seulement 3 canaux indépendants.



De façon synchrone, effectuez une mesure de débit sur 30 s entre chaque paire de machine dans les situations suivantes.

Canal BSS 1	Canal BSS 2
1	1
2	1
3	1
4	1
5	1
6	1

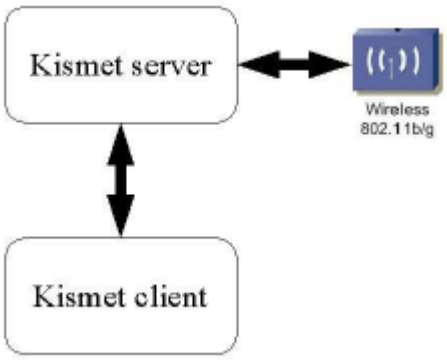
Présentez les résultats obtenus sous forme graphique. Pour estimer la reproductibilité de la mesure, reproduire deux autres fois l'expérimentation précédente, de façon à disposer de trois réalisations de l'expérience globale.

La conclusion de votre étude devra faire apparaître les valeurs min, moyenne et max des débits mesurés dans chacun des intervalles.

Annexe A : la capture de trames

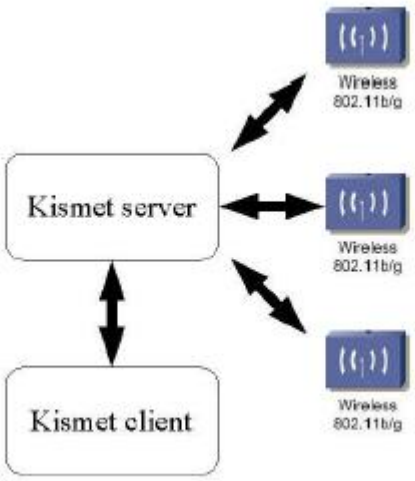
La capture de trames s'effectue avec une station de mesure équipée d'une interface radio et d'un logiciel permettant de stocker les informations recueillies. Le logiciel utilisé est Kismet (http://www.kismetwireless.net/)

Kismet possède une architecture client-serveur dont le schéma synoptique trés simplifié est présenté ci dessous.

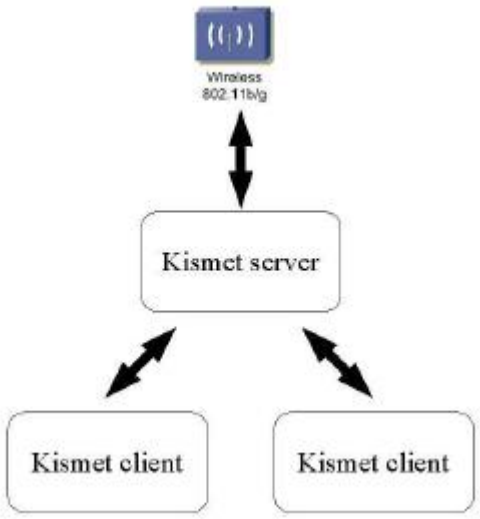


L'architecture trés modulaire de kismet autorise chacune des trois composantes à être hébergées ou pas sur une même plateforme matérielle. Ceci conduit aux conséquences suivantes:

plusieurs interfaces radio peuvent être connectées au serveur. Dans la terminologie kismet, une telle interface radio déportée est appelée un drone. La connexion se fait par Ethernet filaire ou avec une deuxième interface radio coté drone, utilisant un canal différent de celui utilisé pour la capture.



Plusieurs clients peuvent être simultanément connectés au serveur. La connexion se fait par Ethernet filaire ou avec une interface radio, utilisant un canal différent de celui utilisé pour la capture.



C'est dans cette dernière configuration que l'on se placera.

La configuration du serveur

Le serveur se démarre avec la commande kismet_server. Seules les options qui ne peuvent pas être passées en ligne de commande seront définies dans le fichier de configuration kismet.conf présent dans le répertoire /etc/kismet. On observera en particulier:

la définition de la source de capture

```
# Sources are defined as:
# source=sourcetype,interface,name[,initialchannel]
# Source types and required drivers are listed in the README.
# The initial channel is optional, if hopping is not enabled it can be used
# to set the channel the interface listens on.
# YOU MUST CHANGE THIS TO BE THE SOURCE YOU WANT TO USE
source=none,none,addme
```

la définition des clients autorisés à se connecter au serveur:

```
# People allowed to connect, comma seperated IP addresses or network/mask
# blocks.  Netmasks can be expressed as dotted quad (/255.255.255.0) or as
# numbers (/24)
allowedhosts=127.0.0.1
```

le filtrage éventuel des paquets[1]:

```
# Packet filtering options:
# filter_tracker - Packets filtered from the tracker are not processed or
#            recorded in any way.
# filter_dump -    Packets filtered at the dump level are tracked,
displayed,
#            and written to the csv/xml/network/etc files, but not
#            recorded in the packet dump
# filter_export -  Controls what packets influence the exported CSV,
network,
#            xml, gps, etc files.
# All filtering options take arguments containing the type of address and
```

[1]Le filtrage peut également être effectué à posteriori avec Ethereal, avec l'inconvénient de manipuler des fichiers de grande taille.

```
# addresses to be filtered.  Valid address types are 'ANY', 'BSSID',
# 'SOURCE', and 'DEST'.  Filtering can be inverted by the use of '!' before
# the address.  For example,
# filter_tracker=ANY(!00:00:DE:AD:BE:EF)
# has the same effect as the previous mac_filter config file option.
# filter_tracker=...
# filter_dump=...
# filter_export=...
```

la validation ou non la capture des trames beacon:

```
# Do we log beacon packets or do we filter them out of the dumpfile
beaconlog=true
```

La configuration du client

Le client se démarre avec la commande kismet_client. Les options sont détaillées dans le fichier de configuration kismet_ui.conf présent dans le répertoire /etc/kismet. On observera en particulier la définition du serveur auquel le client est connecté:

```
# Server to connect to (host:port)
host=localhost:2501
```

La capture proprement dite

Kismet démarre l'enregistrement des données dès son lancement. Le nombre de trames interceptées pouvant être important, il est conseillé de synchroniser l'acquisition et l'initialisation des échanges que l'on souhaite observer.

Le contrôle de kismet se fait au clavier avec quelques commandes simples dont la liste est donnée par un simple appui sur la touche “h”. Les principales sont:

```
c: liste des clients du réseau courant
L: verrouillage sur le canal du réseau courant
i: informations détaillées sur le réseau courant
s: tri des réseaux détectés
r: graphe des paquets capturés
a: statistiques
p: type des paquets capturés
x: retour à la fenêtre principale
Q: terminer Kismet
```

L'analyse des trames

Par défaut, kismet stocke les informations recueillies dans le répertoire /var/log/kismet dans les fichiers de type:

Kismet-MM-DD-YYYY-i.csv: environnement radio au format CSV (comma separated value)

Kismet-MM-DD-YYYY-i.dump: paquets capturés au format binaire

Kismet-MM-DD-YYYY-i.network: environnement radio au format texte

Kismet-MM-DD-YYYY-i.xml: environnement radio au format XML

i représente le numéro de l'enregistrement et MM-DD-YYYY la date du jour. Il sera prudent de renommer ces fichiers immédiatement après capture pour faciliter leur gestion.

Le fichier dump peut être relu par Wireshark (http://www.wireshark.org/). Il sera surement nécessaire de filtrer les paquets capturés pour n'afficher que ceux concernés par l'expérimentation en cours.

Plan indicatif du compte rendu

AdHoc

Schéma fonctionnel, description de l'architecture utilisée, distance approximative entre les équipements radio, etc...

Paramétrage des composants du réseau

Description complète de l'expérimentation (pour la rendre reproductible)

Processus de calibration et analyse de la reproductibilité des résultats obtenus

Présentation et analyse des résultats par comparaison avec la calibration de référence.

Présentation et analyse des résultats dans des contextes différents (charge réseau, recouvrement de canal, interférences, étude paramétrique, etc...)

Les graphes devront rappeler dans leur titre les principales caractéristiques de la manip (paramétrage radio, type d'expérimentation, condition, etc...)

Infrastructure

Schéma fonctionnel, description de l'architecture utilisée, distance approximative entre les équipements radio, etc...

Paramétrage des composants du réseau

Description complète de l'expérimentation (pour la rendre reproductible)

Processus de calibration et analyse de la reproductibilité des résultats obtenus

Présentation et analyse des résultats par comparaison avec la calibration de référence.

Présentation et analyse des résultats dans des contextes différents (charge réseau, recouvrement de canal, interférences, étude paramétrique, etc...)

Les graphes devront rappeler dans leur titre les principales caractéristiques de la manip (paramétrage radio, type d'expérimentation, condition, etc...)

Architecture étendue

Schéma fonctionnel, description de l'architecture utilisée, distance approximative entre les équipements radio, etc...

Paramétrage des composants du réseau

Description complète de l'expérimentation (pour la rendre reproductible)

Processus de calibration et analyse de la reproductibilité des résultats obtenus

Présentation et analyse des résultats par comparaison avec la calibration de référence.

Présentation et analyse des résultats dans des contextes différents (charge réseau, recouvrement de canal, interférences, étude paramétrique, etc...)

Les graphes devront rappeler dans leur titre les principales caractéristiques de la manip (paramétrage radio, type d'expérimentation, condition, etc...)