

# **Interconnexion de multiples drones**

## **« AR Parrot »**

*Rowier Nicolas pour UCL/ICTEAM/INMA*

8/12/2014

# 1 Cahier de charges

## 1.1 Objectifs

Les 3 objectifs sont :

- La possibilité de connecter 5 drones et qu'ils puissent communiquer entre-eux.
- De permettre un flux vidéo à 30 images par seconde pour chaque drone.
- D'éviter les connexions accidentelles.

## 1.2 Contraintes

- Modifier le moins possible le logiciel embarqué sur le drone, afin de récupérer facilement les paramètres d'usine.
- Ne pas interférer avec les infrastructures sans fil du service "Infrastructures des réseaux" (SRI).
- Respecter la réglementation en terme de puissance d'émission, la limite actuelle est de 100mw dans la bande des 2.4GHz.

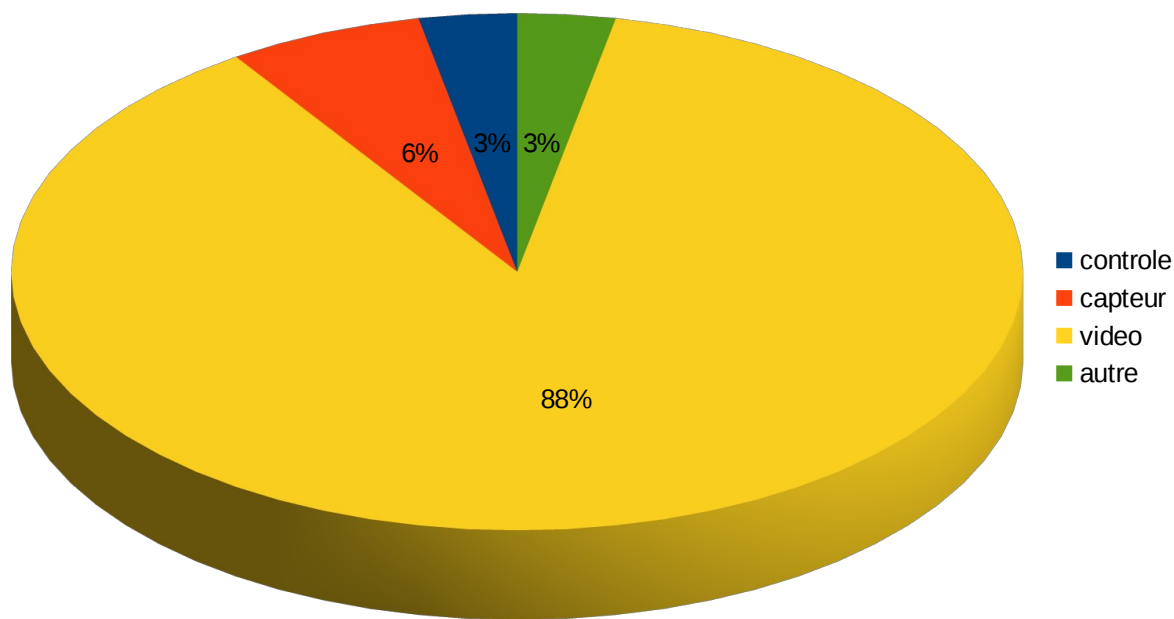
# 2 Analyse préliminaire

## 2.1 Topologie actuelle

Le drone se comporte comme un point d'accès sans chiffage entre l'ordinateur ou le smartphone qui s'y connecte. Ce qui ne permet pas de connecter plusieurs drones entre-eux.

Les applications clients des drones ne permettent pas de changer l'adresse IP dans leur configuration. L'interface de programmation des drones n'est pas prévue pour une utilisation simultanée de plusieurs drones.

## 2.2 Analyse du trafic entre un drone et le PC client



Lors d'un scénario de décollage/atterrissage utilisant la camera dorsale, la bande passante pour un débit total de 1.22Mbit/s est répartie entre :

- Le contrôle, commande de pilotage du drone : protocole « freeciv » (UDP/5556), 0.03 Mbit/s, du PC (client) vers le drone (serveur).
- Les capteurs, données de navigation : protocole « sgi-esphhttp » (UDP/5554), 0.07Mbit/s, du drone vers le PC.
- La vidéo : protocole « personnel-agent » (TCP/5555), 1.06Mbit/s, du drone vers le PC.
- Autres : 0.004Mbit/s

Les données entre guillemet sont le type de trafic détecté par « Wireshark », le logiciel d'analyse de flux réseaux.

**En cas de modification des fonctionnalités le débit peu varier.**

Lors de la première analyse 70 % du trafic était non identifié, le débit totalisait 5Mbit/s. Il s'est avéré que certains processus tournaient en tâche de fond sur l'ordinateur du laboratoire. Le logiciel générant le plus de trafic parasite était Dropbox (3,5Mbit/s).

Pour les analyses futures, il est recommandé de :

- Désactiver Dropbox ainsi qu'un maximum de protocole de découverte réseaux. Le plus simple est d'avoir un système fraîchement installé ce qui limitera fortement le problème.
- Minimiser le nombre de machines raccordées au routeur, diminue le risque d'avoir du trafic parasite.

## 3 Analyse

### 3.1 Le routeur et son système

Pour le choix du routeur, le cahier des charges suivant a été suivi :

- Peu coûteux.
- Compatible wifi N en 2.4GHz, comme les drones.
- Rapidement disponible.
- Compatible Openwrt : Afin d'avoir les fonctions nécessaires à la sécurisation de l'installation comme le filtrage des « adresses MAC » et la possibilité de masquer le nom du réseau. La version 14 du « firmware » est recommandée afin de garantir une durée de vie importante à ce travail mais elle n'est pas indispensable.
- Le modèle choisi est le TPlink « TL-WR841N ».

### 3.2 Le wifi et la sécurité

- La bande de fréquence est limitée au 2.4GHz et seuls 3 canaux qui ne s'entrecroisent pas sont disponibles. Un seul sera utilisé : si nous utilisons deux fréquences tous les routeurs du réseau de l'UCL dans la zone passeront sur le dernier canal disponible, ce qui générera des collisions et limitera la bande passante pour les utilisateurs connectés dans la zone.
- Le réseau du routeur wifi est configuré comme un routeur classique : Les drones se connectent comme des clients, soit la topologie inverse de celle par défaut afin de pouvoir connecter plusieurs drones (clients) en utilisant une seule fréquence et un seul routeur.
- L'adressage de l'ensemble est statique : Grâce au script de configuration, un même drone récupère la même adresse IP, ce qui évite d'ajouter un service de distribution d'adresse et favorise la simplicité.
- Afin de favoriser les performances, aucun chiffrement ne sera utilisé. Le nom du réseau sera masqué et les « adresses MAC » seront filtrées.

Cette approche n'est pas optimale une personne dans la zone de couverture peut sniffer le réseau afin d'obtenir le nom du réseau et usurper l'adresse MAC d'un drone. Cependant c'est la solution la plus légère : Elle garantit donc une bande passante maximale et une latence minimale car les données ne sont pas chiffrées.

## 4 Mise en œuvre

### 4.1 Obtenir les informations et configurer les drones

#### Collecte des informations

Afin de pouvoir autoriser un drone à se connecter au routeur, il faut d'abord récupérer son « adresse MAC » et le nom de son réseau, cette étape est à recommencer pour chaque drone :

- Débranchez la carte réseau filaire de votre ordinateur pour éviter un conflit d'adressage entre le routeur wifi et le drone.
- Connectez-vous avec votre ordinateur au réseau du drone ici « ardrone\_08286 », le réseau des drones commence toujours par « ardrone\_ », notez le nom du réseau afin de pouvoir l'ajouter à l'outil de configuration par la suite.
- Recueillir « l'adresse MAC » du drone :

```
#Connexion au drone
telnet 192.168.1.1
#Affiche les paramètres de la carte réseau sans fil du drone.
ifconfig ath0
```

- L' « adresse MAC » sera affichée dans le champ « hwaddr », notez-la afin de pouvoir l'autoriser dans le routeur par la suite :

```
ath0      Link encap:Ethernet  HWaddr 90:03:B7:2A:DF:11
          inet addr:192.168.1.1  Bcast:192.168.1.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6739 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22947 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:731621 (714.4 KiB)  TX bytes:1555330 (1.4 MiB)
```

## Configuration d'un drone « autoconfarparrot »

Cette étape permet de configurer le drone en mode client à l'aide d'un script, il fonctionne exclusivement sous Linux :

- Copiez le script ci-dessous dans un fichier de votre répertoire de travail avec comme nom « autoconfarparrot » :

```
#!/bin/bash
conf_path="./"
#current setting
cur_essid=$(iwconfig wlan0 | grep ESSID | cut -d\" -f2)
cur_ip="192.168.1.1"
#ap setting
essid="drone"
#check curent essid
if [[ $cur_essid != *"ardrone"* ]] ; then
    echo ardrone not detected
    exit 1
fi
#check connection
if ping $cur_ip -c1 -q
then
    #load setting
    if [ ! -e "$conf_path$cur_essid" ]
    then
        echo Create a $conf_path$cur_essid file with ip address
    fi
    ip=$(cat "$conf_path$cur_essid")
#configure
telnet $cur_ip << EOF
killall udhcpd;    iwconfig ath0 mode managed essid $essid;
ifconfig ath0 $ip netmask 255.255.255.0 up;
EOF
fi
```

- Avant de lancer script, vous devez toujours être connecté au drone et connaître le nom de son réseau sans fil.
- Dans le répertoire où se situe le script, il va falloir créer un fichier avec le nom du réseau sans fil du drone (« ardrone\_008286 » dans l'exemple). Cette opération est à faire une seule fois par drone.
  - Ce fichier de configuration contient l'adresse IP attribuée au drone.
  - L'adresse IP doit être dans la plage 192.168.1.x : x étant le numéro unique attribué au drone, il peut prendre toutes valeurs sauf :
    - Celle qui sont déjà utilisées.
    - 1 et 2 qui sont les adresses par défaut des drones.
    - 253 qui est l'adresse de l'ordinateur.
    - 254 qui est l'adresse du routeur wifi.
- Le moyen le plus simple de créer ce fichier est de lancer la commande suivante dans le même dossier que le script :

```
# Syntaxe de la commande
#cat « 192.168.1.x » > le_nom_du_wifi_drone
# Exemple pratique
cat « 192.168.1.3 » > ardrone_008286
```

- Lancez le script pour effectuer les changements :

```
#Lance le script
bash ./autoconfarparrot
```

- Déconnectez votre ordinateur de ce réseau sans fil, s'il ne l'a pas fait automatiquement.
- Répétez l'ensemble des opérations pour chaque drone (Tout le chapitre 4.1).

Si vous redémarrez le drone ou changez sa batterie, il faut se reconnecter au drone et relancer le script.

## 4.2 Configuration d'un routeur

- A chaque interaction avec une page l'interface web, il faut cliquer sur « save » en bas de page, sauf mention contraire.
- Le routeur ne peut pas être connecté au réseau de l'UCL sans accord des gestionnaires du réseau.

### Choix du matériel

Le choix d'un routeur adapté est indispensable au bon fonctionnement de l'ensemble :

- Référez-vous au site suivant pour les modèles supportés : <http://wiki.openwrt.org/toh/start> ainsi qu'au point 3.1 (de ce document) pour les critères de sélection du modèle actuel : le TPlink « TL-WR841N ».
  - Privilégiez du matériel compatible avec la dernière version d'openwrt (14) et les marques disponibles en Europe (Linksys, Netgear, TPlink, Asus ...).
  - Un modèle plus performant (CPU > 600MHz et plus de 64Mo de mémoire) est plus adaptés au « monitoring ».
- En suivant le lien à coté du routeur (sur le site de Openwrt), vous tomberez sur une mine d'information et le lien vers le « firmware » adapté au modèle.
- Téléchargez ce « firmware ».

### Remplacement du « firmware » d'origine

Afin d'accéder aux fonctions avancées du routeur et d'avoir une configuration standardisée une mise à jour du logiciel du routeur est nécessaire :

- Rendez-vous dans l'interface par défaut du routeur dans la section permettant la mise à jour du « firmware ». Souvent cette section est dans un menu « maintenance », ceci est propre à chaque fabricant, parfois même à chaque modèle.
- Sélectionnez le « firmware » téléchargé et lancez l'opération de mise à jour.
- Si ça ne fonctionne pas, l'usage de « tftp » est une bonne option, mais trop longue à détailler dans ce document. Référez-vous à la documentation officielle : <http://wiki.openwrt.org/doc/howto/generic.flashing.tftp>



## Configuration initiale du routeur

La configuration initiale est faite en « telnet » afin de définir un mot de passe et d'optimiser les performances du routeur ainsi que d'éviter les interférences avec le script d'auto-configuration des drones.

- Raccordez un câble entre le routeur et votre ordinateur, vous recevrez automatiquement une adresse IP.
- Le mot de passe est défini et tous les services inutiles sont désactivés via les commandes suivantes :

```
#Établit une connexion avec le routeur
telnet 192.168.1.1

#Définir le mot de passe administrateur afin d'éviter les
connexions non autorisées
passwd

#Désactive le filtrage des données
/etc/init.d/firewall disable

#Désactive les tâches planifiées
/etc/init.d/cron disable

#Désactive la distribution d'adresse IP qui interfère avec le
script d'auto configuration des drones.
/etc/init.d/odhcpd disable
/etc/init.d/dnsmasq disable

#Désactive les accès non chiffrés, il faudra utiliser ssh à
l'avenir.
/etc/init.d/telnet disable

#Désactive la mise à jour automatique de l'heure (en cas de
monitoring il est conseillé de ne pas désactiver cette
fonctionnalité)
/etc/init.d/sysntpd disable

#redémarre le routeur
reboot
```

## Connexion à l'interface du routeur

Après le redémarrage du routeur vous pouvez commencer les opérations ci-dessous.

Dans un premier temps, il est nécessaire de permettre à votre ordinateur de se connecter au routeur sans fil :

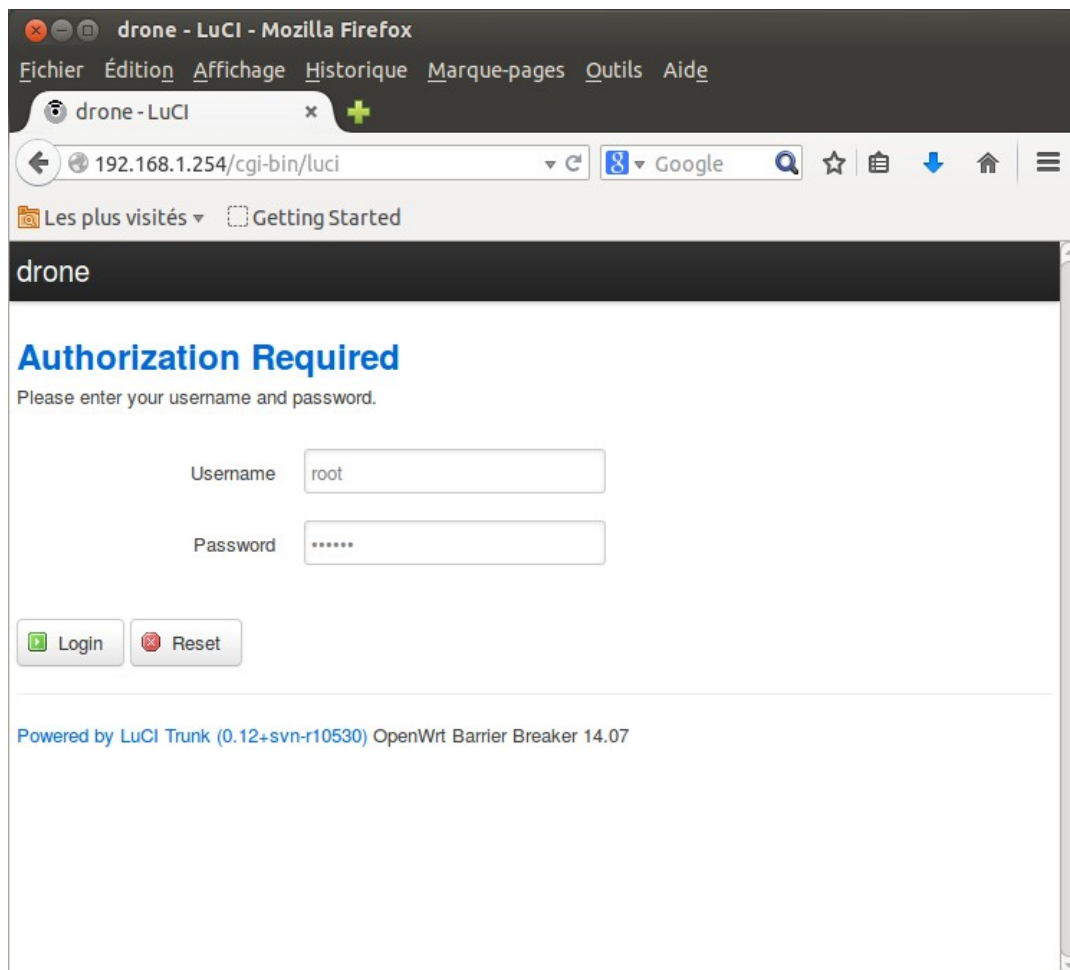
- Désactiver le « Network Manager » d 'Ubuntu : Clic sur l'icône du réseau dans la barre supérieure > Décochez « Activer le réseau ».

Dans un terminal, configurez votre carte réseau :

```
#Configuration en ligne de commande  
sudo ifconfig eth0 192.168.1.253
```

L'objectif de l'interface web du routeur est d'accéder aux paramètres de configuration facilement :

- Tapez l'adresse IP du routeur « 192.168.1.1 » dans le cas d'un routeur dont le « firmware » vient d'être remplacé. « 192.168.1.254 » dans le cas du routeur pré-configuré.
- La page de connexion suivante s'affiche :



- Introduisez le login « root » et le mot de passe introduit à l'étape précédente ou « cocoon » dans le cas du routeur pré-existant.

## Changement de l'adresse IP

La configuration de l'adresse sur le routeur permettra de s'y connecter, « 192.168.1.1 » étant utilisé par défaut sur beaucoup d'équipement, il vaut mieux la changer :

- Allez dans le menu : « Network » > « Interfaces ».

drone - Interfaces - LuCI - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils Aide

drone - Interfaces - L... x



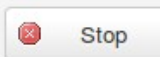




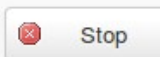


192.168.1.254/cgi-bin/luci/;stok=b8f96380841 Google

Les plus visités Getting Started

drone Status System Network Logout AUTO REFRESH ON

### Interfaces

#### Interface Overview

Network	Status	Actions
<b>LAN</b>  br-lan	<b>Uptime:</b> 0h 11m 15s <b>MAC-Address:</b> C4:6E:1F:93:53:BC <b>RX:</b> 67.36 KB (664 Pkts.) <b>TX:</b> 166.18 KB (621 Pkts.) <b>IPv4:</b> 192.168.1.254/24 <b>IPv6:</b> FD1C:E533:1A43:0:0:0:1/60	 Connect  Stop  Edit  Delete
<b>WAN</b>  eth1	<b>Uptime:</b> 0h 0m 0s <b>MAC-Address:</b> C4:6E:1F:93:53:BD <b>RX:</b> 0.00 B (0 Pkts.) <b>TX:</b> 0.00 B (0 Pkts.)	 Connect  Stop  Edit  Delete
<b>WAN6</b>	<b>MAC-Address:</b>	

- Cliquez sur « Edit » en face de « Network » section « LAN », vous verrez la page suivante :

drone - Interfaces - LuCI - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils Aide

drone - Interfaces - L... x

192.168.1.254/cgi-bin/luci/stok=b8f96380841 Google

Les plus visités Getting Started

drone Status System Network Logout AUTO REFRESH ON

IPv4: 192.168.1.254/24  
IPv6: FD1C:E533:1A43:0:0:0:1/60

Protocol Static address

IPv4 address 192.168.1.254

IPv4 netmask 255.255.255.0

IPv4 gateway

IPv4 broadcast

Use custom DNS servers

IPv6 assignment length 60

Assign a part of given length of every public IPv6-prefix to this interface

IPv6 assignment hint

- Dans le champ « ipv4 address », définissez l'adresse à : « 192.168.1.254 ».

Le plus simple est d'utiliser l'adresse « 192.168.1.254 » pour rester cohérents avec l'ensemble de ce document.

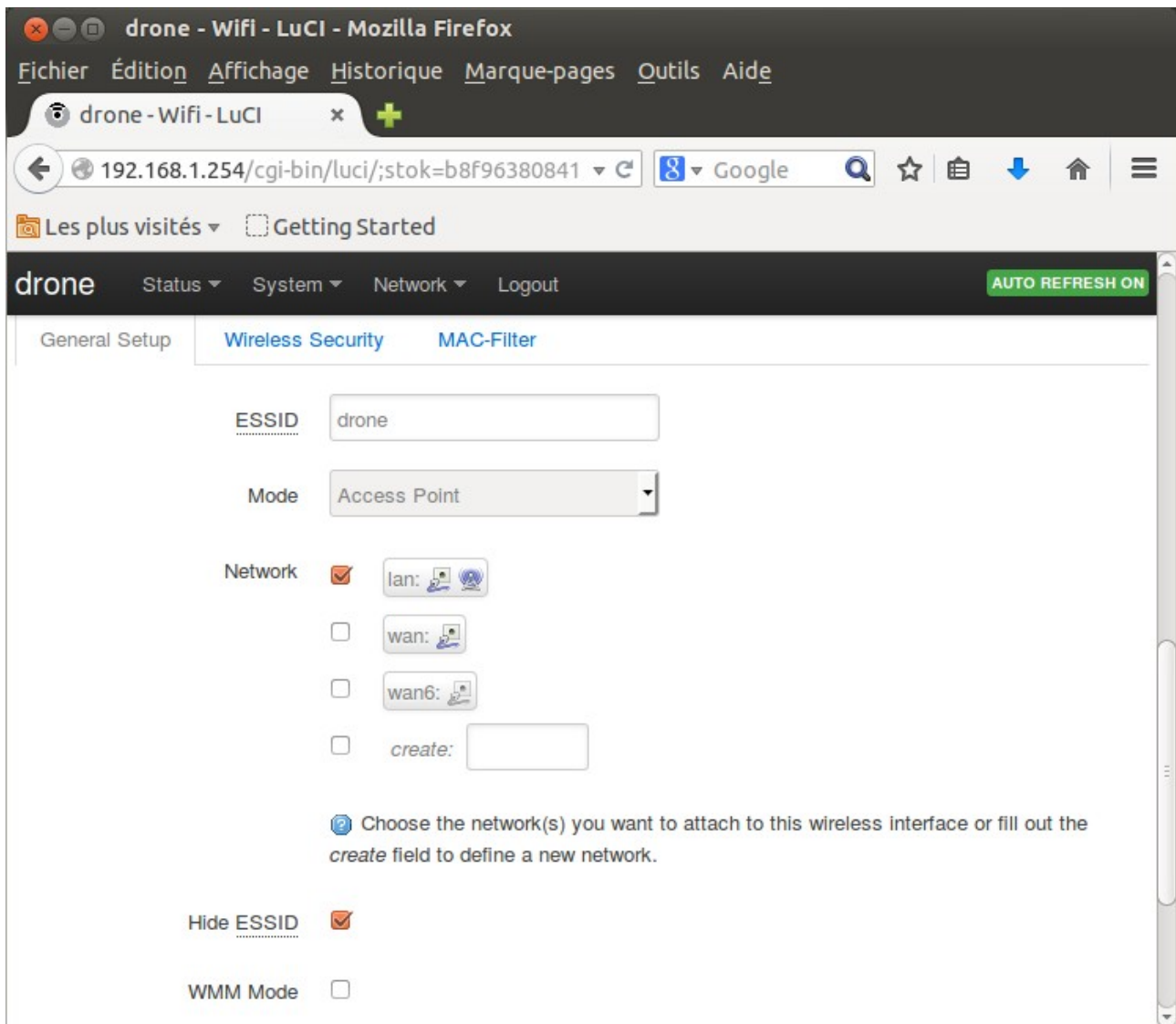
## Configuration du réseau Wifi

Afin que les drones puissent se connecter au réseau sans fil, il faut configurer celui-ci :

- Allez dans le menu : « Network » > « Wifi ».

The screenshot shows the LuCI web interface in a Mozilla Firefox browser. The address bar shows the URL `192.168.1.254/cgi-bin/luci/stok=b8f96380841`. The interface has a top navigation bar with links for **drone**, **Status**, **System**, **Network**, and **Logout**, along with an **AUTO REFRESH ON** button. The main content area is titled **Wireless Overview** and displays the configuration for the **Generic MAC80211 802.11bgn (radio0)** interface. It shows the channel as 11 (2.462 GHz) and the bitrate as ? Mbit/s. Below this, it indicates the SSID is **drone**, the mode is **Master**, the BSSID is **C4:6E:1F:93:53:BC**, and encryption is **None**. There are buttons for **Scan**, **Add**, **Disable**, **Edit**, and **Remove**. The **Associated Stations** section below shows a table with columns for SSID, MAC-Address, IPv4-Address, Signal, Noise, RX Rate, and TX Rate, but it currently displays *No information available*. At the bottom, it mentions the interface is powered by **LuCI Trunk (0.12+svn-r10530)** and **OpenWrt Barrier Breaker 14.07**. A status bar at the very bottom indicates **En attente de 192.168.1.254...**

- Cliquez sur « Add » en face du contrôleur, si vous avez deux contrôleurs, utilisez le contrôleur qui contient « BGN » dans sa description, c'est la bande de fréquence utilisée par les drones.



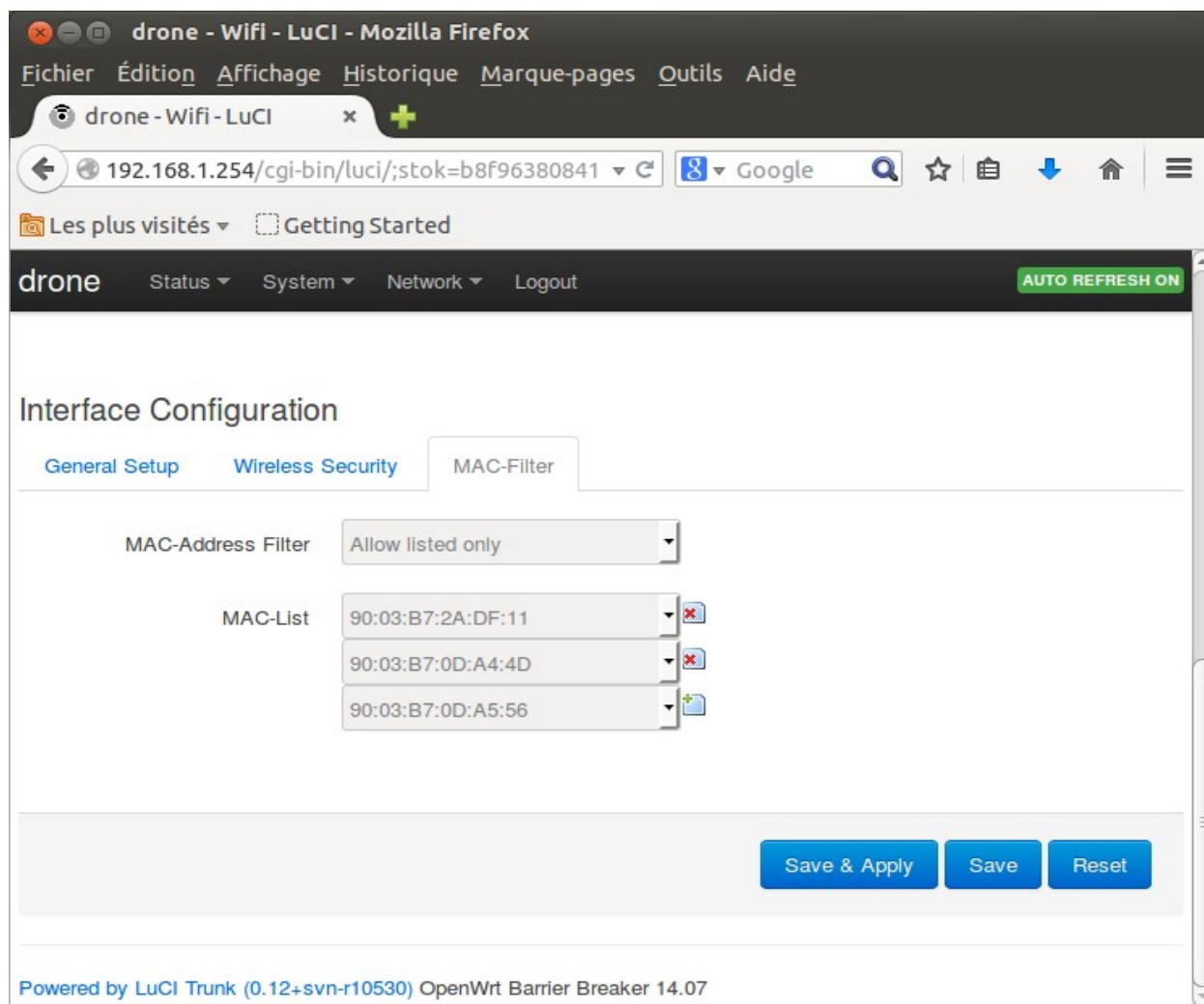
- Configurez le champ « essid » sur « drone » pour attribuer un nom au réseau, cochez la case « hide essid », pour masquer le nom du réseau.
- Retournez dans le menu « Network » > « Wifi ».
- En face du réseau « Drone », un bouton « Enable » apparaît. Cliquez dessus pour activer le réseau.

La bande passante étant partagée en wifi je vous recommande de connecter votre ordinateur via un câble afin de la préserver au maximum.

## Limitation des « adresses MAC »

Cette configuration évite qu'un client non autorisé qui aurait « deviné » le nom du réseaux se connecte au routeur sans fil :

- Si ce n'est pas déjà fait, connectez-vous avec votre navigateur internet au routeur.
- Allez dans le menu « Network » > « Wifi ».
- Dans ce menu en face du réseau drone, cliquez sur « edit ».
- Cliquez sur l'onglet « Mac Filter », l'écran suivant apparaît :



- Dans la liste « MAC address filter », choisissez « Allow listed only », ce qui autorisera uniquement les adresses listées.
- Dans la « MAC-List », Ajouter les « adresses MAC » des drones que vous avez collectés au point 4.1 (de ce document), afin de les autoriser.

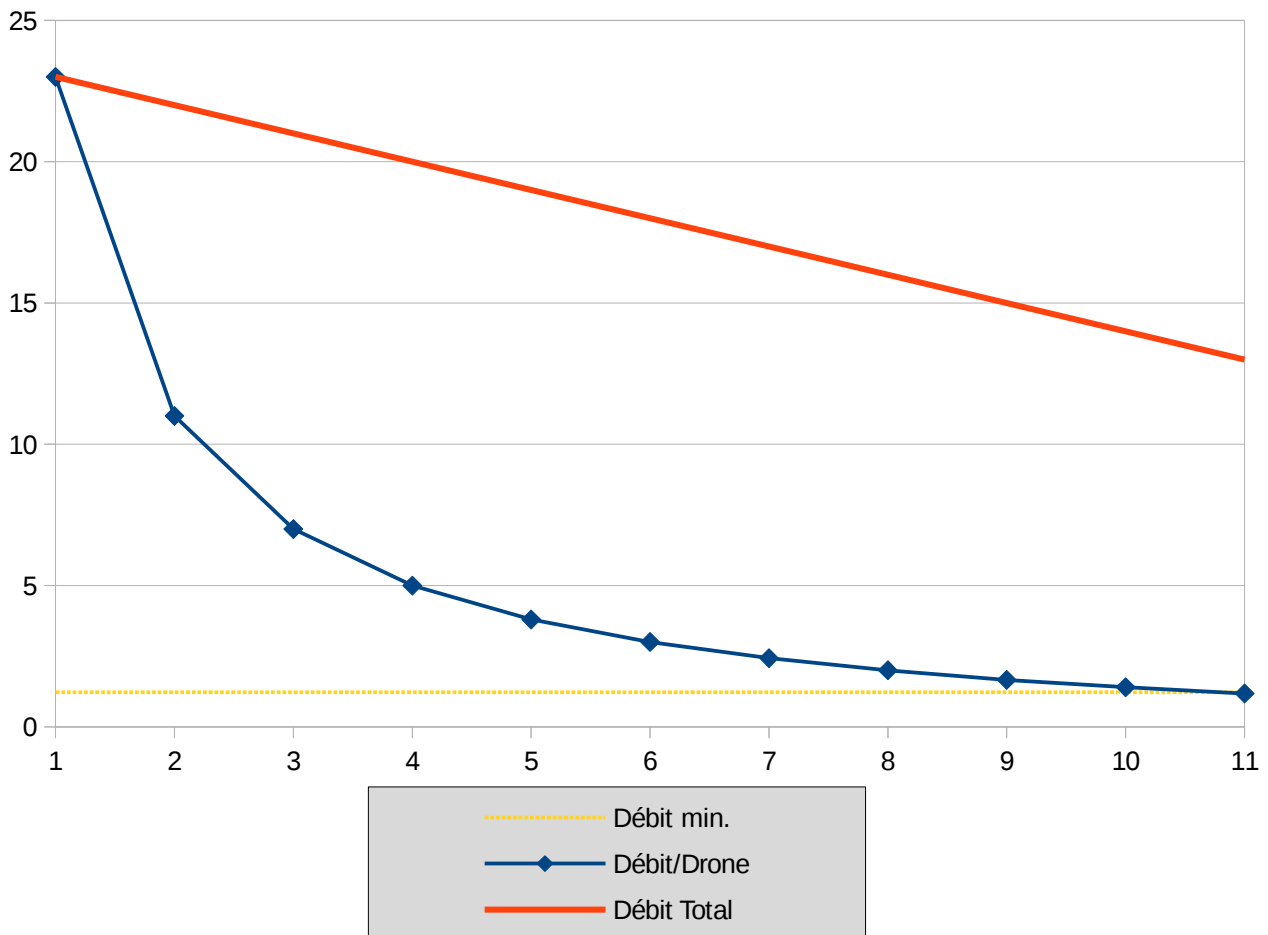
Cliquez sur « save & apply », le drone va prendre son « adresse IP » définitive si ce n'est pas encore le cas et appliquer les changements.

## 5 Benchmark et Validation

Ces tests ont été effectués en intérieur sur une petite surface, les 4 drones étaient à moins de 5 mètres de la borne (le débit diminue avec la distance).

La latence ne varie que très peu en fonction du nombre de drones connectés et ce même quand on les utilise, la latence est comprise entre 2 et 5ms.

Le débit lui varie beaucoup en fonction du nombre de drones en parallèle, ce graphique représente les variations :



Le test de débit simultané a eu lieu sur 4 drones, pour chaque drone ajouté on perd 1Mbit/s de la bande passante totale et ce de façon linéaire, ce qui a permis d'extrapoler le graphique. Au dessus de 10 drones, les 1.22Mbit/s ne seront plus disponibles ce qui peut engendrer de la latence et des coupures.



## 6 Conclusion

Aucune modification définitive n'a été effectuée sur les drones, elles sont totalement réversibles, au démarrage les drones reprennent leur configuration d'usine. La configuration spécifique est effectuée par un script, ce qui permet de ne pas avoir besoin de modifier le logiciel embarqué, de gagner du temps et de pouvoir facilement identifier les drones. L'inconvénient de cette approche est de devoir reconfigurer les drones à chaque démarrage et donc à chaque changement de batterie (environ deux minutes sont nécessaires).

Les drones peuvent communiquer entre-eux via la machine qui gère le pilotage. La limitations de bande passante limite le nombre de drone à 10 dans une petite pièce d'un point de vue théorique, en pratique les tests ont été fait avec 4 drones et extrapolé. La partie de bande passante consommée par le contrôle et les capteurs est faible (9%), comparé à la vidéo (86%), il y a peu de risque que le scénario influe sur le débit total. La vidéo a une occupation de bande passante linéaire, que les mouvements soient rapides ou lents. En cas de modification, il est intéressant de refaire les mesures de débit pour que les mesures collent parfaitement au contexte principalement sur les points suivants :

- Nouveau local : Il peut y avoir des interférences avec des réseaux sans fil existants ou un débit moindre sur une surface plus étendue.
- Compression vidéo : La modification de l'algorithme de compression peu changer la bande passante utilisée et la façon dont elle est utilisée (linéarité).
- De nouvelles fonctionnalités : Si la caméra frontale est utilisée, si de nouveaux capteurs sont ajoutés ou utilisés, la consommation de bande passante sera plus importante.

Le nom du réseau sans fil est masqué et empêche quelqu'un qui n'en connaît pas le nom de s'y connecter involontairement, ce mécanisme est doublé d'un filtrage par « adresse MAC », qui demande des compétences complémentaires pour être contourné et empêche définitivement les connections accidentelles. Seule une fréquence sans fil est utilisée à une puissance de 100mW, ce qui en laisse deux au réseau sans fil de l'UCL et évite des interférences, le tout dans le respect de la législation.

D'après les applications clients, le flux vidéo est à 30fps (image par seconde). Certaines documentations mentionnent une limite à 15fps, elle semble ne plus être d'actualité ou erronée. L'API des drones a posé quelques soucis pour établir plusieurs connexions simultanées. Les étudiants se sont occupés de cet aspect.

## 7 Améliorations

- Traduction du présent document en anglais.
- Optimisation :
  - Différents algorithmes de compression vidéo sont disponibles, il serait intéressant de mesurer les performances de compression, les résultats avec opencv ainsi que la linéarité de chacun.
  - Détection automatique des drones en configuration d'usine : Ce serait pratique lors des changements de batterie et pour un déploiement encore plus rapide. Actuellement il faut se connecter à chaque drone manuellement à tour de rôle puis lancer l'outil de configuration.
    - Depuis un ordinateur : Ceci demande de faire attention aux interférences avec le « network manager » d'Ubuntu, qui désactive l'alimentation du wifi quand on désactive le gestionnaire.
    - Depuis un routeur : Il faut un routeur de plus pour éviter les déconnexions, le plus pratique est de programmer un bouton en façade pour lancer l'opération automatiquement sans ordinateur.
- L'API : Actuellement une modification rapide faite par les étudiants permet la connexion à plusieurs drones. Si l'usage du multi drones est prolongé, il serait intéressant de faire des tests plus en profondeur pour faciliter les développements futurs et éviter des comportements imprévus.
- Topologie : Actuellement elle est adaptée à couvrir de petites surfaces pour des drones pilotés par une machine. Une topologie point à point peu être plus adapté dans les cas suivants :
  - Besoin d'une faible latence entre les drones, sans que les communications passent par l'ordinateur.
  - Une plus grande surface de couverture est nécessaire.
- Sécurité : Le chiffrement WEP peut être ajouté et géré matériellement, ce qui limite les pertes de performances.

Cette norme de sécurité n'est pas totalement sûre mais elle l'améliore.

## 8 Remerciements

Au département INGI, plus particulièrement à :

- Pierre Reinbold : Pour m'avoir conseillé lors de la relecture du script de configuration.
- Olivier Bonaventure : Pour m'avoir aidé à valider la topologie réseau et donné des conseils pour l'analyse des flux.

Au département INMA, plus particulièrement à :

- Etienne Huens : Pour m'avoir amené à faire ce travail et avoir relu ce rapport.
- Francois Wielant : Pour l'encadrement du projet sur le terrain, la relecture et la correction de ce rapport.
- Julien Hendrickx : Pour le management du projet et l'organisation de celui-ci.

Aux étudiants en électromécanique, plus particulièrement à :

- Florent Vanhijfte et Briec de Radigues : Pour leur participation et leur connaissance de l'API, sans qui ce travail aurait pris plus de temps ou n'aurait pas eut lieu.

## 9 Lexique

Adresse Mac : Adresse unique identifiant une carte réseau. (

[http://fr.wikipedia.org/wiki/Adresse\\_MAC](http://fr.wikipedia.org/wiki/Adresse_MAC) )

Adresse IP : Adresse identifiant de manière unique une machine sur un réseau. (

[http://fr.wikipedia.org/wiki/Adresse\\_IP](http://fr.wikipedia.org/wiki/Adresse_IP) )

Api : Interface de programmation ( [http://fr.wikipedia.org/wiki/Interface\\_de\\_programmation](http://fr.wikipedia.org/wiki/Interface_de_programmation) )

Bande passante : Volume de données pouvant transiter sur un réseau pendant un temps donné.

Broadcast : Un message part d'une machine vers l'ensemble des machines du réseau. (

[http://fr.wikipedia.org/wiki/Broadcast\\_%28informatique%29](http://fr.wikipedia.org/wiki/Broadcast_%28informatique%29) )

Essid ou ssid : Nom d'un réseau wifi. ( [http://fr.wikipedia.org/wiki/Service\\_set\\_identifier](http://fr.wikipedia.org/wiki/Service_set_identifier) )

Firmware : Logiciel interne au routeur. ( <http://fr.wikipedia.org/wiki/Firmware> )

Latence : Temps nécessaire au transit d'un paquet de la source à la destination. (

[http://fr.wikipedia.org/wiki/Latence\\_%28informatique%29](http://fr.wikipedia.org/wiki/Latence_%28informatique%29) )

Monitoring : Le monitoring permet de surveiller différents paramètres dans le temps (tel la bande passante et la latence dans le cas présent).

Network manager : Outils de gestion des connexions réseaux. ( <http://doc.ubuntu-fr.org/network-manager> )

Openwrt : C'est un firmware alternatif permettant d'étendre les fonctionnalités d'un routeur à moindre coût. ( <http://fr.wikipedia.org/wiki/OpenWrt> )

Telnet : Protocole de contrôle distant non chiffré. ( <http://fr.wikipedia.org/wiki/Telnet> )

TFTP : Protocole léger permettant le transfert de fichiers. (

[http://fr.wikipedia.org/wiki/Trivial\\_File\\_Transfer\\_Protocol](http://fr.wikipedia.org/wiki/Trivial_File_Transfer_Protocol) )

# Table des matières

1Cahier de charges.....	2
1.1Objectifs.....	2
1.2Contraintes.....	2
2Analyse préliminaire.....	2
2.1Topologie actuelle.....	2
2.2Analyse du trafic entre un drone et le pc client.....	3
3Analyse.....	4
3.1Le routeur et son système.....	4
3.2Le wifi et la sécurité.....	4
4Mise en œuvre.....	5
4.1Obtenir les informations et configurer les drones.....	5
Collecte des informations.....	5
Configuration d'un drone « autoconfarparrot ».....	6
4.2Configuration d'un routeur.....	8
Choix du matériel.....	8
Remplacement du « firmware » d'origine.....	8
Configuration initiale du routeur.....	9
Connexion à l'interface du routeur.....	10
Changement de l'adresse IP.....	11
Configuration du réseau Wifi.....	13
Limitation des « adresses MAC ».....	15
5Benchmark / Validation.....	16
6Conclusion.....	17
7Améliorations.....	18
8Remerciements.....	19
9Lexique.....	20