LE WIFI

<https://www.youtube.com/watch?v=RglTaUWXDIs>

Tout savoir sur le wifi - 20 min.

Le wifi permet de connecter tous les appareils domestiques sans fil et de leur donner l’accès à Internet.

Normes de communication sans fil par la IEEE.

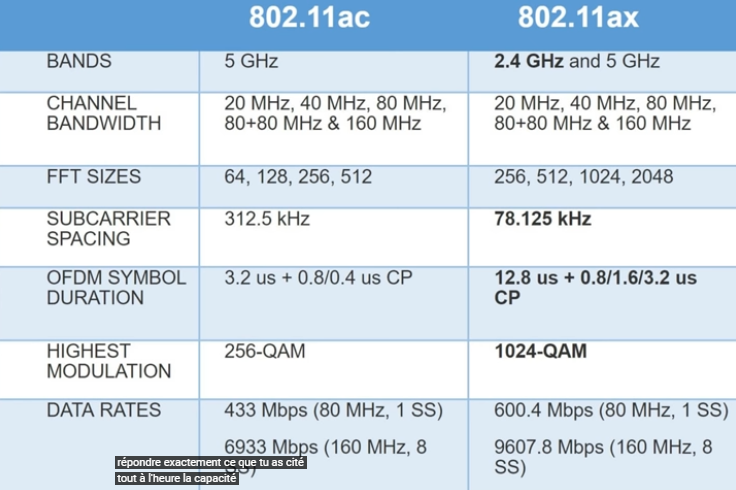
Wi Fi Alliance : wifi5, wifi6

Il faut avoir des wifis de plus en plus puissant car de plus en plus de périphériques et c’est l’accès principal à internet et à l’information aujourd’hui.

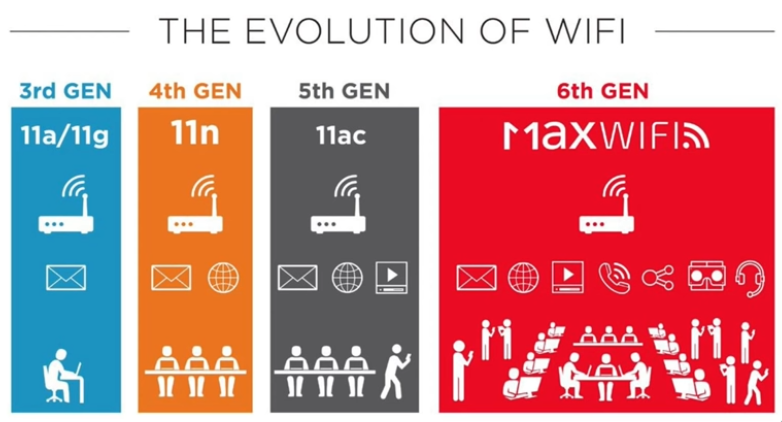
Wifi puissance d'environ 100 mW. Normes CE - pas de danger aux ondes.

ANFR - Agence Nationale des Fréquences.

Le wifi6 ?? La dernière évolution du wifi.



802.11ac = wifi 5 /// 802.11ax = wifi 6



Le wifi 2.4GHz et 5GHz ne traversent toujours pas les murs, ils ne sont pas conçus pour ça.

h[ttps://www.youtube.com/watch?v=ijFIqCeABIM](https://www.youtube.com/watch?v=ijFIqCeABIM)

Comment fonctionne le wifi ? Le tout sur les réseaux sans fil

Relier deux ordinateurs : le plus simple par câble

Sans fil :

> Infrarouge sur de courtes distances avec des équipements proches et alignés

> Ondes radios comme le Bluetooth [2.4GHz ; 2.4835 GHz]

Transféré dans toutes les directions avec 1 Mbit/s avec des ondes omnidirectionnelles qui traversent les obstacles courants + faible consommation adaptée aux périphériques.

Portée de 1 à 30 m.

>Le WiFi : norme 802.11b, Wireless Fidelity. Équipement wifi à l’origine ou ajout par module. Le wifi utilise la même bande passante que le Bluetooth découpé en 13 canaux en Europe pour plus d’efficacité. La portée du Wifi se situe entre 30 et 50 m, avec un débit supérieur : 5.5Mbits/s (selon la version). Permet la création de LAN : Local Area Network. Réseau local ou les ordinateurs sont connectés ensemble par Ethernet souvent, par câble RJ45, branchés sur un routeur. Il achemine les données sur chaque machine. Une borne wifi peut tenir le même rôle pour des communications sans fil.

Le WLAN : Wireless LAN est un LAN sans fil.

Un pirate peut détruire des données, déposer des virus, obtenir des informations privées.

Le réseau local peut être surchargé.

Sécurité du réseau : SSID Service Set Identifier. Il faut le renommer et empêcher la diffusion du nom. Le filtrage d’adresse MAC (Media Access Control) permet de contrôler les membres du réseau.

Les données peuvent être cryptées à l’aide d’une clé WEB (Wired Equivalent Privacy).

Seuls les équipements possédant la même clef peuvent communiquer. L’envoyer crypte les données avant l’envoi et le récepteur les décrypte.

* fort, le WPA (Wifi Protected Access) demande une authentification avec une clé de cryptage qui est modifiée régulièrement.

https://www.youtube.com/watch?v=LsyfJc83SQo

Voici comment fonctionne le Wi-fi

Racine du Wifi dans les années 1940. Etalement de spectre par bande de fréquence.

Années 1980s.

1ère version du code 802.11

Utilise les ondes radios

2.4 - rapide + loin.

/!\ Interférences avec les autres appareils domestiques

23 canaux sur la 5 GHz.

<https://www.youtube.com/watch?v=YSl6bordSh8>

Ports et protocoles : l’essentiel en 5 min

Socket = @IP + N°Port

@IP : détermine l’unique machine destinataire

N°port : détermine l’application concernée

Ports [0 ; 1023] reconnus // ports [1024 ; 49151] enregistrés // ports [49152 - 65535] dynamiques et/ou privés utilisés pour des services privés, personnalisés.

Un protocole applicatif est attribué à chaque port (syntaxe, règles transport, réception etc).

Les protocoles applicatifs s’appuient sur les protocoles de transport.

HTTP - SMTP DNS - DHCP

TCP UDP

IP

<https://www.youtube.com/watch?v=26jazyc7VNk&t=0s>

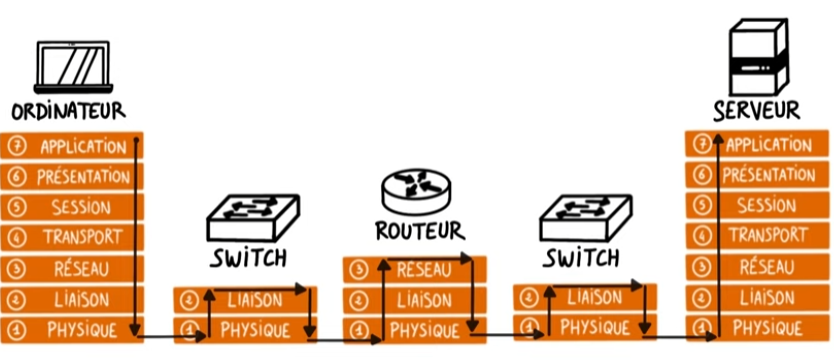
Comprendre les modèles OSI et TCP/IP

TCP : fiabilité des données ~~

UDP : temps réel ~~

=> modèle TCP/IP Application (Protocoles dhcp, ftp, dns etc.) / Transport (TCP/ UDP) / Internet (IPs) / Accès réseau (MAC, ethernet, wifi, etc)

En tête, encapsulation, etc.



<https://www.youtube.com/watch?v=9UMvyfT4V_Y>

Comment fonctionne Internet ?

Les données dans le monde circule par un énorme réseau mondial de fibre optique. (data centers, etc.).

Les smartphones, ou tout autre appareil connecté, avec ou sans fil, peut se connecter par des données cellulaires ou par borne Wi-Fi, mais rejoint forcément ce réseau de fibre.

Un serveur sert à faire parvenir des données. La transmission entre le serveur et la machine : Identification unique grâce à l’adresse IP. DNS ⇔ adresses IP.

NEXT : <https://www.youtube.com/watch?v=K9nfeF6-0Fw>



LE NFC

Les cartes sans contact sont de plus en plus présentes dans notre environnement.

En effet, en mai 2016 en France la NFC représente :

* 11,5 millions de smartphone utilisant cette technologie.
* 41.4 millions (soit 61%) cartes bancaires équipé du NFC.
* une progression de 183% en 1 an par rapport à mai 2015 ( en un an)

Cette croissance se traduit grâce à une grande simplicité de cette technologie pour l'usager. Un grand nombre d'usages nouveaux comme les cartes de transport, de badges d'entreprise, de cartes de fidélité, de clés de voiture ou de chambre d'hôtel, les jeux en réseau et le paiement, tout cela par un simple geste.

## **Définition NFC/RFID (Champ d’application)**

## **Technologie RFID**

La technologie de la RFID est basée sur l'émission de champ électromagnétique.

**Système RFID** : Un système RFID (Radio Fréquence Identification) se compose de transpondeurs (aussi nommés étiquettes, marqueurs, tags, identifiants...) et d'un ou plusieurs interrogateurs (aussi nommés coupleurs, base station...).

**Interrogateurs RFID** : Ce sont des dispositifs actifs, émetteurs de radiofréquences qui vont activer les tags qui passent devant eux en leur fournissant l'énergie dont ils ont besoin pour fonctionner.

Outre de l'énergie pour l'étiquette, l'interrogateur envoie des commandes particulières auxquelles répond le tag. L'une des réponses les plus simples possibles est le renvoi d'une identification numérique.

La fréquence utilisée par les interrogateurs est variable selon le type d'application visé et les performances recherchées.

**Tag RFID** : C'est un dispositif récepteur, que l'on place sur les éléments à tracer (objet, animal...). Ils sont munis d'une puce contenant les informations et d'une antenne pour permettre les échanges d'informations.

* Classe 0 et classe 1 : tags passifs à lecture seule (on ne peut que lire l'identifiant unique du tag)
* Classe 2 : tags passifs à fonctions additionnelles (écriture mémoire)
* Classe 3 : tags passifs assistés par batterie ; Classe 4 : tags actifs. Communication large-bande du type « peer-to-peer»
* Classe 5 : interrogateurs. Alimentent les tags de classe 0, 1, 2 et 3. Communiquent avec les tags de classe 4.

Le principe de base d'identification repose sur le fait que chaque transpondeur possède son identifiant unique UID (Unique ID) fréquemment codé sur 32 bits et qui est stocké en zone mémoire à lecture seule.

## **Technologie NFC**

La communication en champ proche (Near Field Communication : NFC) est une technologie de communication sans-fil à courte portée et haute fréquence, permettant l'échange d'informations entre des périphériques jusqu'à une distance d'environ 10 cm. Cette technologie est une extension de la norme ISO/CEI 14443 standardisant les cartes de proximité utilisant l’identification par radiofréquence (Radio Frequency Identification : RFID), qui combinent l'interface d'une carte à puce et un lecteur au sein d'un seul périphérique. Le système NFC est donc une application utilisant la technologie RFID à 13,56 MHz destiné à la reconnaissance mutuelle à très courte distance ( de 0 à 20 cm), avec un débit de 212 kbits/s. L’une des différence notable avec la technologie RFID est que cette technologie est prévu pour transiter des données autres qu’un UID unique par badge.

Les champs d'application de cette technologie sont notamment les systèmes de paiement et les communications entre dispositifs électroniques tels que téléphones cellulaires, PCs, PDAs, téléviseurs, consoles de jeu, etc. Les avantages de cette technologie sont une identification mutuelle entre dispositifs, et sa très courte distance d'utilisation qui rend peu probable le piratage ou brouillage de la communication sans que l’opérateur ne s'en rende compte.

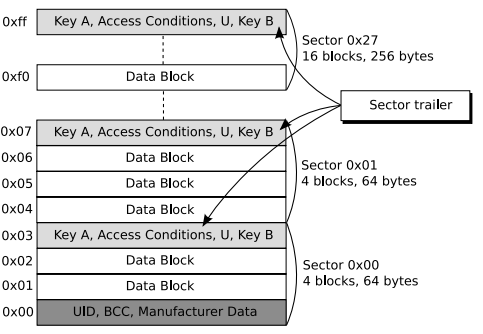
Les différents types de NFC : **Mifare**, **Mifare** classic, **Mifare** DESFire EV1 et EV2, **Mifare** Plus, Ultralight …

## Cartes MIFARE

Nous revenons maintenant en détail sur les cartes MIFARE.

### Structure logique des cartes MIFARE Classic

Les cartes MIFARE Classic sont essentiellement composées d’une puce de mémoire EEPROM qui possède la particularité d’ouvrir une communication sécurisée. Cette communication permet de réaliser des opérations de base : lire, écrire, incrémenter et décrémenter. Ces actions peuvent être effectuées sur cette mémoire. La mémoire de l'étiquette est divisée en secteurs. Chacun de ces secteurs est divisé en Blocs de 16 octets. Le dernier bloc de chacun de ces secteurs s'appelle le “sector trailer” et stocke deux clés secrètes ainsi que les conditions d’accès correspondant à ce secteur.  
  
Pour effectuer une opération sur un Bloc spécifique, le lecteur doit d'abord s'authentifier sur le secteur contenant ce bloc. Les conditions d’accès de ce secteur contenues dans le « sector trailer » déterminent la clé A ou B qui doit être utilisée. La figure 1 montre un schéma de la structure logique de la mémoire d'une étiquette MIFARE Classic.



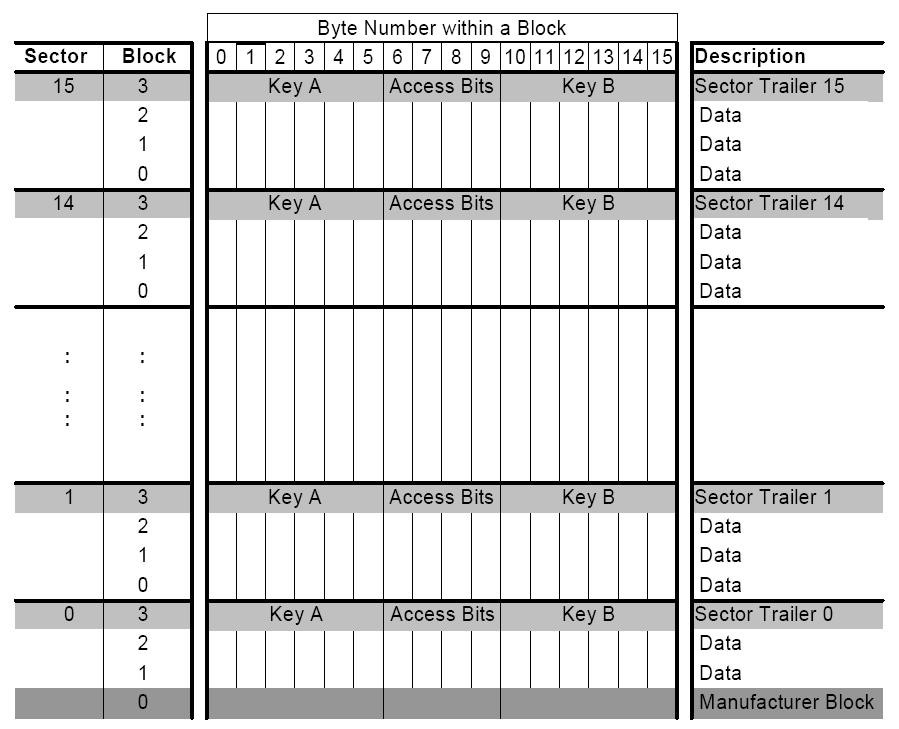
**Image 2 : Conditions d’accès aux secteurs**

### Récapitulatif

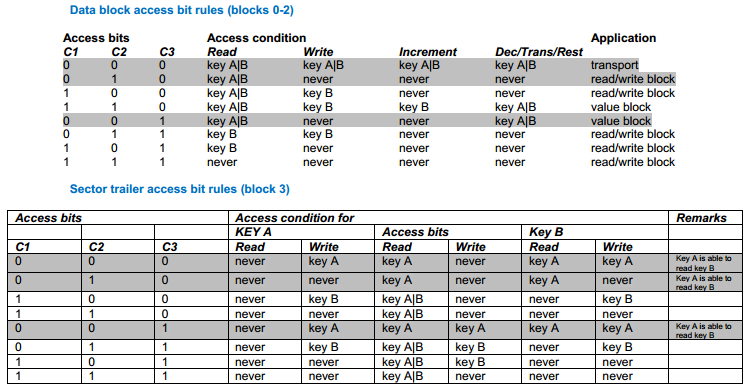
Le premier bloc du secteur 0, contient l'UID, BCC qui sont des données du fabricant (en lecture seule).

1. Chaque secteur contient 64 octets
2. Chaque bloc contient 16 octets.
3. Le dernier bloc de chaque secteur (“trailer”) contient les clés A et B qui permettent de définir les conditions d’accès.
4. Les conditions d’accès déterminent les permissions de chaque bloc.

Voici la structure globale d’une carte MIFARE Classic 1K :



**Image 3 : Structure de la MIFARE Classic 1K**



**Image 4 : Bits d’accès et permissions des blocs**

Le schéma ci-dessus correspond à la documentation technique qui définit selon la valeur des clés les permissions de chaque bloc.

## **failles NFC**

Le clonage / spoofing :

Grâce à la longue portée de la technologie RFID, le clonage et le spoofing peuvent être très facilement effectués, un simple lecteur peut récupérer les données d’une carte et en créer alors une copie très aisément. Pour de cas des cartes Mifare uniquement. En effet d’autres cartes incluant un chiffrement ne permettent pas de les cloner. (ex: Mifare DESFire)

* La destruction de la carte / Altération des données :

La puce RFID est très vulnérable aux champs électromagnétiques, de plus si la carte dispose d’une protection en plastique peu épaisse, elle peut facilement être endommagé par une pression légère, un choc thermique, une humidité trop importante.

* Attaques par relais

Une attaque par relais est une attaque utilisant deux matériels :

- Un lecteur longue distance qui servira à récupérer les informations à distance.

- Un émetteur “fantôme” longue distance

Un lecteur situé jusqu'à 50 mètres de la carte de l'utilisateur pourrait récupérer les données contenues dans cette carte. Puis un émetteur pirate, après avoir reçu les informations de la carte pourrait envoyer les informations au lecteur original autant de fois que nécessaire et à longue distance. Tout cela sans que l’utilisateur ne puisse s’en apercevoir en vue de la distance maximale de 50 mètres.

* Attaques Man In The Middle :

Tout comme une attaque Man In The Middle standard sur un réseau, l’attaque Man In The Middle consiste à avoir un appareil malveillant placé au centre entre le lecteur et le badge. Celui-ci récupérera les données tout en laissant croire que lecteur qu’il accède directement à la carte sans “intermédiaire malveillant”.

* Attaques cryptographiques :

Si des données cryptées sont stockées dans une puce RFID il faut prendre un compte que la faible mémoire de ses puces empêche un cryptage suffisant, en effet une puce RFID standard comme celle contenue dans les passeports a été démontrée vulnérable à des attaques par bruteforce avec un ordinateur basique.

En seulement deux heures une puce peut être décrypté et son contenu récupéré.

* Cartes faillibles :

Certaines cartes comme la “Mifare classic 1k” ne possèdent qu’un simple chiffrement , les information sont déchiffrables simplement et rapidement. Ce qui as pour conséquence de laisser le code lisible pour un éventuel attaquant. De ce fait, il est possible de cloner ou modifier le contenu comme vu ci-dessus.

III - Etude des sécurités actuelles

La technologie NFC est aujourd’hui présente partout dans le monde. Elle offre plus de sécurité que la RFID dû à sa courte portée (<10cm).

Il faut donc définir les moyens de protection existants contre les différentes failles de sécurité que comportent ces cartes “sans contact”.

**Le choix du type de carte :**

* **Mifare Classic et Classic EV1**

Elle offre 1024 octets pour la 1K, et 4096 octets pour la 4K pour le stockage de données, répartis sur 16 secteurs. Chaque secteur est protégé par deux clés différentes, “A” et “B”.

Le protocole de sécurité propriétaire NXP (crypto-1), est utilisé pour l'authentification et le chiffrement.

Grâce à leur fiabilité et leur faible coût, elles sont utilisées comme porte-monnaie électronique, cartes d’identité d’entreprise, billetterie ou pour le contrôle d’accès.

Le chiffrement de la Mifare Classic a été compromise : le temps actuel pour calculer ces clés est de 6 secondes.

La version **Mifare Classic EV1** a été créé afin d’améliorer la sécurité, la performance et la durabilité :

-Générateur de clés aléatoire (car les anciennes ne dépendent que de la durée d'allumage de la carte)

-Gestion de l’ID aléatoire (sur 7 octets)

-Vérification de l’authenticité de la carte

-Augmentation de la robustesse de l’ESD (des composants électroniques)

-Vitesse d’écriture de 200.000 cycles (au lien de 100.000 cycles)

* **Mifare Ultralight et Ultralight EV1**

Possède seulement 512 bits de mémoire (64 octets - 16 pages de 4 octets), sans sécurité cryptographique.

Ces puces sont tellement bon marché, qu'ils sont souvent utilisés comme billets jetables.

Ne fournit que des sécurités de base : 1 seule fois programmable (OTP bits : One-Time Programmable) avec une fonction de verrouillage pour empêcher la ré-écriture des pages de mémoire.

La version **Mifare Ultralight EV** intègre des options de sécurité supplémentaire comme :

-1024 bits mémoire pour l’utilisateur

-OTP, compteurs configurables pour une meilleure sécurité

-3 compteurs indépendants “24-bit-one-way” pour arrêter le rechargement

-Protection de l’accès aux données par un mot de passe de 32 bits

-Fonction de vérification d’authenticité de signature afin de prévenir la contrefaçon de billets

La **Mifare Ultralight C** est rétrocompatible avec la Mifare Ultralight, ce qui permet une intégration facile dans les infrastructures existantes mais dispose en plus d’une authentification intégrée avec Triple DES.

Utilisées principalement pour des billets de voyage, des tickets de transport publics, des billets d'événement, ou encore des cartes de fidélité.

* **Mifare DESFire**

Quatre différentes :

-une avec seulement Triple-DES et 4 Ko de stockage

-trois avec AES (2, 4 ou 8 Ko de stockage, voir DESFire EV1)

Elle est vendue pré-programmée avec le système d'exploitation "MIFARE DESFire", et offre bien plus de fonctionnalités et de sécurité que les MIFARE Classic.

En 2010, NXP a annoncé l’arrêt du Mifare DESFire après avoir introduit la Mifare DESFire EV1 fin 2008.

La Mifare DESFire a été cassé en octobre 2011 par les chercheurs de l'Université Ruhr Bochum.

**Mifare DESFire EV1**

Compatible avec les versions précédentes.

Disponible avec 2 Ko, 4 Ko et 8 Ko de mémoire.

-Prise en charge d'un ID aléatoire

-Prise en charge d'un chiffrement 128-bit AES

-Le matériel et le système d'exploitation sont certifiés Common Criteria au niveau EAL 4+ utilisée dans les transports publics, la gestion des accès, les cartes fidélité et les micropaiement.

**Mifare DESFire EV2**

Annoncée publiquement en mars 2016.

Compatible avec les versions précédentes.

-MIsmartApp permet d’offrir ou de vendre de l’espace mémoire pour des applications supplémentaires de tiers sans avoir à partager de clés secrètes.

-Transaction MAC (Message authentication codes) pour authentifier les transactions par des tiers

-”Virtual Card Architecture” pour la protection de la vie privée

-Vérification de proximité contre les attaques relais (rejouer

**Etude des outils existant**

<https://github.com/nfc-tools>

<http://nfc-tools.org/index.php?title=Main_Page>

<http://tools.kali.org/kali-metapackages>

# Réalisation du projet

## Configuration Raspberry

Nous avons commencé par réaliser la configuration réseau dans le but de s’adapter à plusieurs cas d’usages.

Cette configuration est commentée dans le but de comprendre à quoi sert chaque partie :

auto lo

iface lo inet loopback

#DHCP

auto eth0

allow-hotplug eth0

iface eth0 inet dhcp

#IP statique Ethernet Direct ou réseau domestique

auto eth0:1

allow-hotplug eth0:1

iface eth0:1 inet static

address 192.168.1.253

netmask 255.255.255.0

auto eth0:2

#IP statique salle CDAISI

allow-hotplug eth0:2

iface eth0:2 inet static

address 192.168.11.253

netmask 255.255.255.0

#Connexion point d’accès Vincent

allow-hotplug wlan0

auto wlan0

iface wlan0 inet dhcp

wpa-ssid "AndroiAP"

wpa-psk "e3d9ec17b63a"

#En ajoutant un module USB -> ethernet

auto eth1

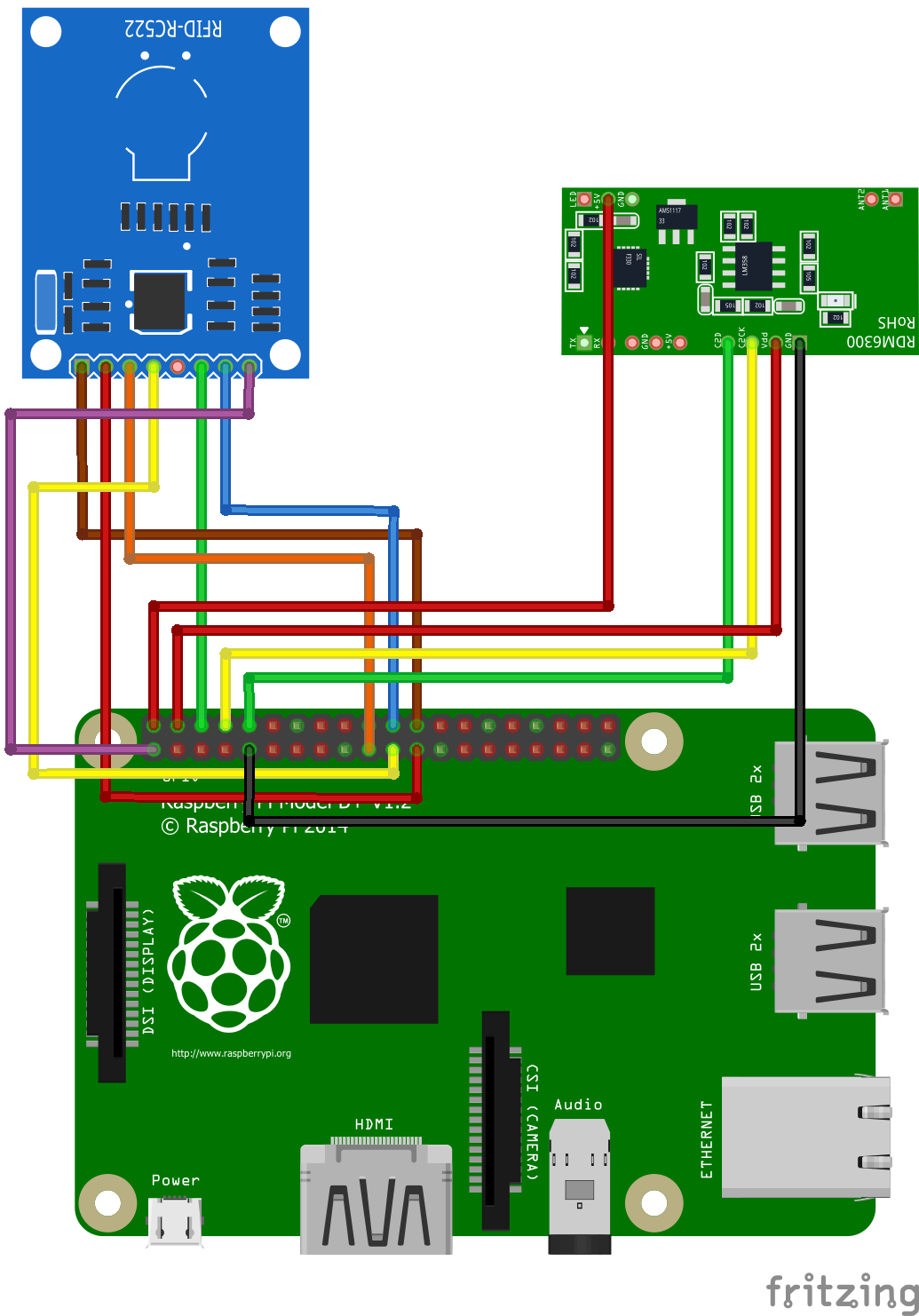
allow-hotplug eth1

iface eth1 inet static

address 192.168.1.253

netmask 255.255.255.0

Nous avons ensuite câblé les modules de la façon suivante :



**Image 7 : Schéma de câblage de la Raspberry et ses modules**

Pour tester les lecteurs nous utilisons les scripts suivants :

* Pour le lecteur RFID RDM6300 125 kHz :

def read\_rfid():

ser = serial.Serial("/dev/ttyAMA0")

ser.baudrate = 9600

data = ser.read(14)

ser.close()

data = data.replace("\x02", "" ) #On enlève le bit de start

data = data.replace("\x03" , "" ) #On enlève le bit de stop

return data

print "En attente d'une carte..."

#Lecture 125 kHz

for i in range(1):

try:

id = read\_rfid()

print id

time.sleep(0.1)

except:

"Impossible de lire le tag"

* Pour le lecteur RFID RC522 13,56 MHz :

# Hook the SIGINT

signal.signal(signal.SIGINT, end\_read)

# Create an object of the class MFRC522

MIFAREReader = MFRC522.MFRC522()

print "appuyez sur Ctrl-C pour arrêter."

# La boucle permet de récuperer l'UID et d'utiliser des clé A et/ou B pour lire le contenu d'une carte MIFARE

while continue\_reading:

# Scan des cartes

(status,TagType) = MIFAREReader.MFRC522\_Request(MIFAREReader.PICC\_REQIDL)

# Si la carte est détecté

if status == MIFAREReader.MI\_OK:

print "Carte détectée"

# Obtenir l'UID de la carte

(status,uid) = MIFAREReader.MFRC522\_Anticoll()

# Si nous avons l'UID nous continuons

if status == MIFAREReader.MI\_OK:

# Afficher UID

print "Lecture de l'UID : "+str(uid[0])+","+str(uid[1])+","+str(uid[2])+","+str(uid[3])

# This is the default key for authentication

key = [0xFF,0xFF,0xFF,0xFF,0xFF,0xFF]

# Select the scanned tag

MIFAREReader.MFRC522\_SelectTag(uid)

# Authenticate

status = MIFAREReader.MFRC522\_Auth(MIFAREReader.PICC\_AUTHENT1A, 8, key, uid)

# Check if authenticated

if status == MIFAREReader.MI\_OK:

MIFAREReader.MFRC522\_Read(8)

MIFAREReader.MFRC522\_StopCrypto1()

else:

print "Erreur d'authentification"