2018

Radio Club de l'Avesnois F6KTN

Réseaux Ethernet et connectivités

Introduction 4

Généralités 5

Support physique de la liaison éthernet 5

Vitesses de transmission 6

Adresses IP 6

Adresses IP V4 6

Adresses IP V6 6

Masque de réseau 7

Exemples de réseaux 9

réseau simple reliant deux périphériques 9

Réseau en parallèle (Ethernet partagé) 10

Réseau par un HUB 10

Réseau commuté par un switch 11

Adresse de passerelle 11

Intercommunication 12

Interconnexion de deux réseaux : le routeur 13

La « box », un routeur particulier 14

Exemple d'architecture réseau simple 15

Site embarqués 16

Adresses IP dynamiques et serveur DHCP 16

Notion de nom d'hôte 17

Serveur DNS 18

Cartes Ethernet de contrôle des réseaux 19

Adresse MAC 19

Sous Windows : 19

Sous Raspbian : 19

Configuration des Adresses IP et DNS sous Windows 21

Configuration des adresses IP et DNS sous raspbian 22

Configuration du Wifi d'un routeur 22

Détermination de l'origine de la non connectivité internet 23

Structure d'une trame Ethernet 24

Protocoles et ports 24

Protocole TCP 25

Protocole UDP 25

URL, adresse de site et nom de domaine ____ *25*

Attribution d'une adresse internet ____ *26*

Adresse WAN publique ____ 26

Adresse WAN privée ____ 27

Attribution d'une adresse dynamique réservée ____ *27*

Routage et redirection de ports ____ *28*

Redirection automatique des ports : le protocole UpnP ____ 29

Les réseaux virtuels privés (VPN) ____ *29*

Le Wifi ____ *30*

Bande 2,4 GHz ____ 30

Bande 5 GHz ____ 31

Le Bluetooth ____ *31*

Annexes ____ *32*

Réglage du wifi sur Raspbian ____ 32

IP fixe sur Raspbian ____ 32

Glossaire ____ *33*

Introduction

Cette présentation montre le matériel utilisé dans le cadre de l'utilisation et de l'élaboration de réseaux éthernet, ainsi que de leurs adressages. Certains des protocoles utilisés dans la cadre de la liaison éthernet y sont également décrits.

Frédéric F1IWQ

Généralités

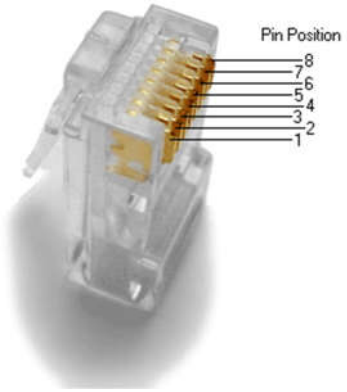
L'interconnectivité entre différents périphériques communiquant par réseau Ethernet est assurée par le protocole IP. Chaque périphérique possède une « adresse IP » qui lui est propre.

Support physique de la liaison éthernet

La couche matérielle de la liaison éthernet a d'abord existé sous forme de câble coxial. Actuellement, elle est assurée par du câble double paire torsadée par paires et blindée.

La liaison éthernet utilise le protocole CSMA/CD : protocole d'accès multiple avec détection de collision. Tous les utilisateurs du réseau peuvent émettre à n'importe quel moment sous réserve que la ligne soit libre. Après une communication entre deux utilisateurs, un temps de repos aléatoire est lancé pour qu'un tiers puisse transmettre pendant ce temps, sinon la communication reprend.

La liaison physique utilise en général des connecteurs RJ45, avec des câbles de 120 ohms, selon les normes RS422/RS485. (liaison série différentielle asynchrone)



Câblage en norme T568B	
1.blanc/orange :	TX D1+
2.orange	TX D1-
3.blanc/vert	RX D2+
4.bleu	
5.blanc/bleu	
6.vert	RX D2-
7.blanc/brun	
8.brun	

En cas d'utilisation de POE (alimentation via ethernet), une tension continue de 48V est superposée d'une part sur les paires TX et d'autre part sur les paires RX.

Les câbles éthernet sont catégorisés:

cat 1: applications de téléphonie bande passante 300-3400 Hz
cat 2: applications jusqu'à 1 Mb/s
cat 3: applications type ethernet 10 Mb/s sur 100 mètres
cat 4: applications type token-ring 16 Mb/s
cat 5: applications type ethernet 100 Mb/s sur 100 mètres
cat 5e: applications type ethernet 2,5 Gb/s sur 100 mètres (10 Gb/s sur 30 mètres)
cat 6: applications type ethernet 5 Gb/s sur 100 mètres (10 Gb/s sur 55 mètres)
cat 6a : applications type ethernet 10 Gb/s sur 100 mètres
cat 7: applications type ethernet 100 Gb/s

Vitesses de transmission

Type	Vitesse	Distance
10BASE-T	10 Mb/s	100m
100BASE-TX	100 Mb/s	100m
100BASE-FX	100 Mb/s	412 m - 2 km
1000Base LX	1000 Mb/s	3,55 km

La vitesse de transmission entre deux ports ethernet est limitée à la vitesse la plus basse des deux ports. En règle générale, les PC sont dotés de ports 1Gb/s. Les switches et routeurs existent en ports 100M ou 1Gb/s suivant les références.

Adresses IP

Il existe deux types d'adresses IP

Adresses IP V4

V4 car sur 4 octets soit 32 bits. Elle est exprimée par 4 nombres en décimal. Exemple : 192.168.1.1
Les parties à gauche de l'adresse IP sont l'adresse réseau.
Les parties à droite sont l'adresse de l'hôte (le périphérique).
La limite entre ces deux parties dépend du masque réseau.

Le problème des adresses IP V4 sur internet est leur limitation.

Adresses IP V6

Les adresses IP V6 ont été créées à cause de la limitation des adresses IP V4.
V6 car sur 16 octets soit 128 bits : Elle est représentée par 8 groupes de 2 octets **hexadécimaux** soit 16 octets :
Exemple : 2001:0db8:0000:85a3:0000:0000:ac1f:8001

Autre notation :
`fe80::8c79:7ab:73ea:9943`
:: signifie de remplir avec autant de 0 pour avoir 128 bits (soit 16 octets), c'est un raccourci pour ne pas écrire les 0. Dans l'adresse ci dessus, on a 5 fois un groupe de 16 bits. Cette adresse est donc :
128 – (3 x 16) = 48 bits soit 6 octets soit 3 mots
`fe80:`**`0:0:0`**`:8c79:7ab:73ea:9943.`

Autre exemple :
`FE80::1234:1` : on a 3 groupes de 16 bits
128 - (3x16) = 80 bits soit 10 octets soit 5 mots. L'adresse est donc
`Fe80:0:0:0:0:0:1234:1`

On ne peut pas utiliser deux fois le double deux points :: dans une adresse IP.

Le masque réseau utilise le / ou le %

exemple : `fe80::8c79:7ab:73ea:9943%11`

%11 signifie un masque à 11 bits.

Certains systèmes d'exploitation ne supportent pas les IP V6 de base (comme Win XP).

Vous trouverez d'autres informations sur l'adresse IP V6 à ce lien

Masque de réseau

En IP V4, le masque réseau permet de dissocier l'adresse réseau de l'adresse hôte. Le masque réseau est un filtre appliqué aux adresses IP par l'intermédiaire d'une fonction logique ET. Le masque est exprimé par 4 nombres en décimal. Exemple : 255.255.255.0
Cela signifie que les 3 premiers octets à gauche d'une adresse ip sont l'adresse du réseau, et que le dernier octet à droite représente l'adresse de l'hôte.

Exemple 1:
adresseIP = 192.168.1.15
masque= 255.255.255.0 : 8 bits à 0 donc $2^8 = 256$
L'adresse réseau est 192.168.1.0
L'adresse du périphérique sur ce réseau est 15. Ce réseau peut gérer 255 hôtes.

Exemple 2 :
adresseIP1 = 10.13.120.17
adresseIP2 =10.13.121.17
masque = 255.255.254.0 : 9 bits à 0 donc $2^9 = 512$
L'adresse réseau est 10.13.120.0
L'adresse du périphérique1 sur ce réseau est 0.17.
L'adresse du périphérique2 sur ce réseau est 1.17.
On a ici un réseau qui peut gérer 511 hôtes.

Notez qu'une adresse IP peut se noter avec son masque. Exemple :
192.168.1.16/24 signifie que le masque défini pour cette adresse IP utilise 24 bits de masquage, soit 1111 1111 1111 1111 1111 1111 0000 0000 ou encore 255,255,255,0

donc :
192.168.1.16/24

signifie :

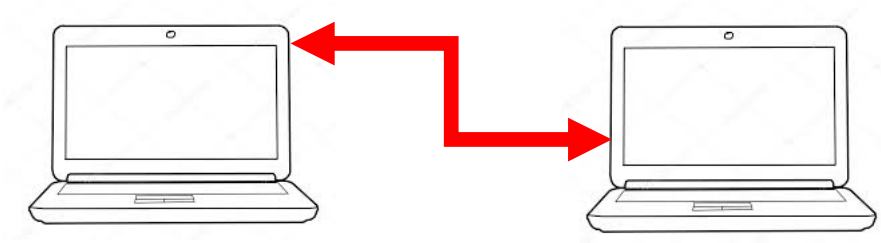
192.168.1.16
255.255.255.0

Les adresses IP attribuées ici à chaque périphérique l'ont été manuellement. On parle d'**adresses IP statiques.**

Exemples de réseaux

réseau simple reliant deux périphériques

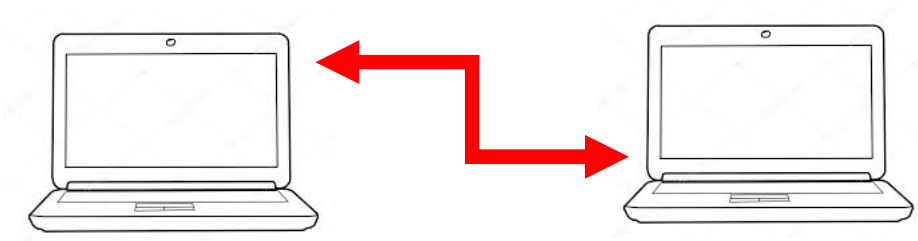
Ce type de réseau entre deux machines est réalisé simplement avec un câble éthernet. A l'origine il fallait utiliser un câble croisé (transmetteurs vers récepteurs). Depuis longtemps, les cartes ethernet des ordinateurs et autres dispositifs reconnaissent l'état des lignes RX et TX et inversent les signaux automatiquement.



192.168.1.10
255.255.255.0

192.168.1.12
255.255.255.0

Soient deux PC avec les adresses IP et de masque positionnées comme ci-dessus.
La communication entre les deux ordinateurs est possible car ils sont situés sur le même réseau d'adresse 192.168.1.0.

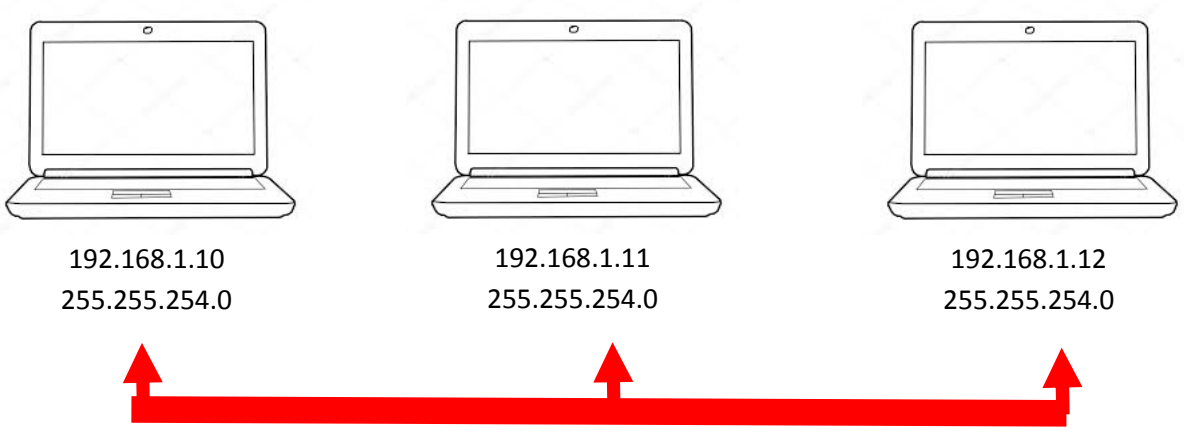


192.168.1.10
255.255.254.0

192.168.0.10
255.255.254.0

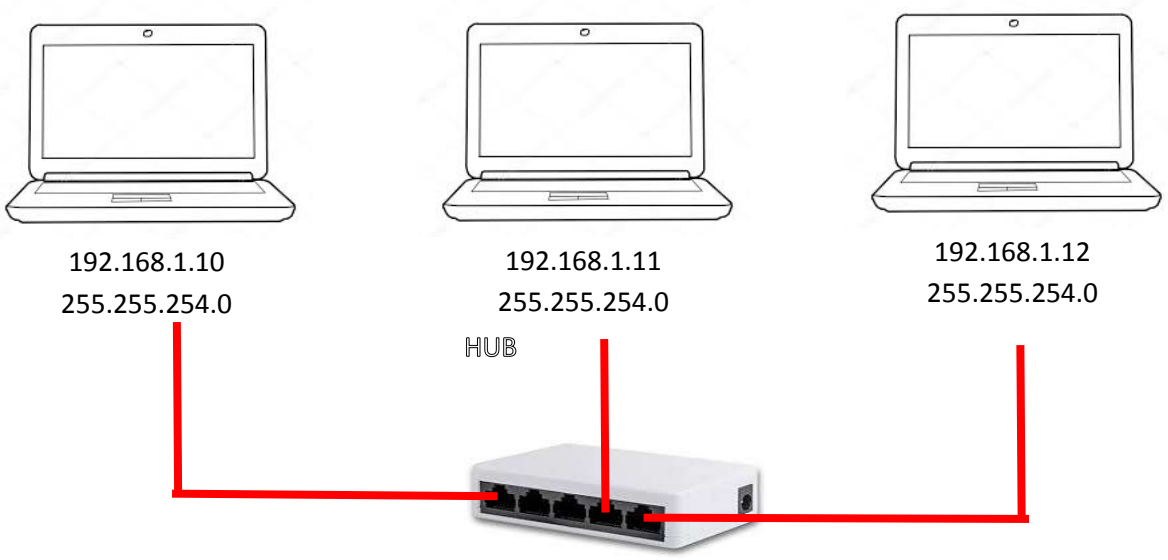
Soient deux PC avec les adresses IP et de masque positionnées comme ci-dessus.
La communication entre les deux ordinateurs est possible car ils sont situés sur le même réseau d'adresse 192.168.0.0 ou 192.168.1.0. Par contre un PC ayant l'adresse 192.168.3.10 appartient à un troisième réseau.

Réseau en parallèle (Ethernet partagé)



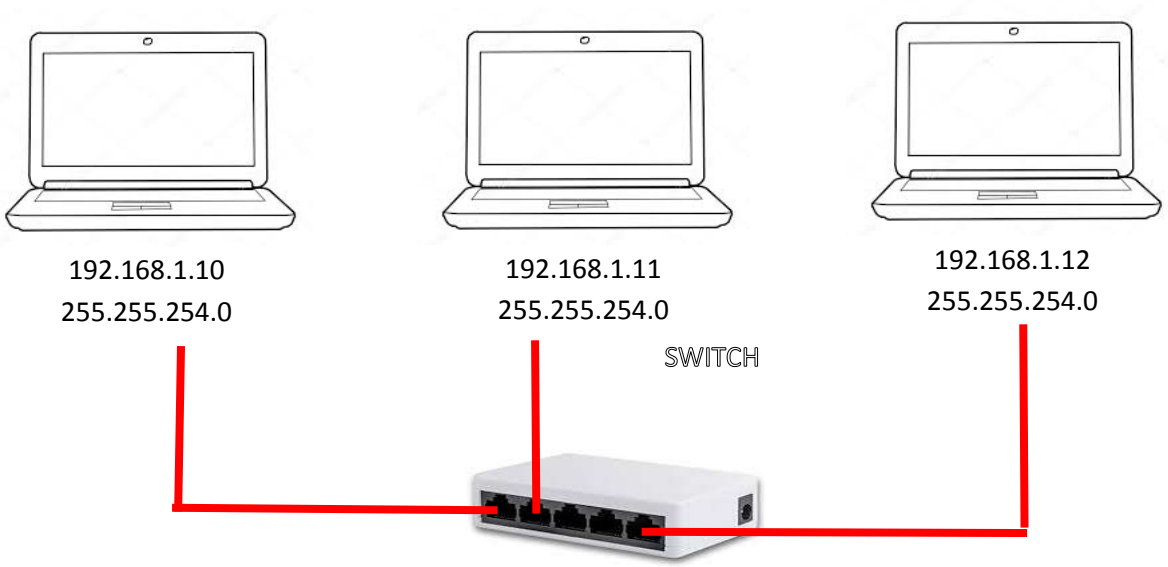
Dans ce réseau en étoile, les PC sont en parallèle. Une information transmise par un ordinateur est transmise sur le réseau et elle est partagée par tous les utilisateurs du réseau. Toute la bande passante est utilisée par les 3 PC.

Réseau par un HUB



Un Hub permet de raccorder plusieurs hôtes sur le même réseau. La gestion du réseau est la même que précédemment. Un message émis sur le PC1 vers le PC2 sera véhiculé sur tout le réseau, et donc vers le PC3, même s'il ne lui est pas destiné. Ainsi, une seule liaison de PC1 vers PC2 utilise toute la bande passante du réseau.

Réseau commuté par un switch



Un switch permet également de raccorder plusieurs hôtes sur le même réseau. La gestion du réseau est commutée. Un message émis sur le PC1 vers le PC2 sera véhiculé **uniquement** sur les ports du switch sur lesquels sont branchés PC1 et PC2, et donc pas vers le PC3. Ainsi la bande passante est partagée et optimisée. Contrairement à un hub, un switch gère une table de routage. D'autre part, il n'y a plus de temps de collision à gérer car il n'y a que deux communicants entre 2 ports.

Un switch peut être paramétrable (*manageable*). Dans ce cas, il reçoit une adresse ip.

Attention :
un switch n'est pas un routeur
un hub n'est pas un switch

Adresse de passerelle

La passerelle est l'équipement qui réalise la « passerelle » entre le réseau LAN et le réseau WAN. Elle dispose, comme le routeur d'une adresse IP. Comme en général, le routeur est la passerelle, l'adresse de la passerelle est l'adresse du routeur. Elle permet aux équipements de savoir vers quelle adresse IP renvoyer une adresse demandée qui ne se trouve pas sur le LAN, mais sur le WAN.

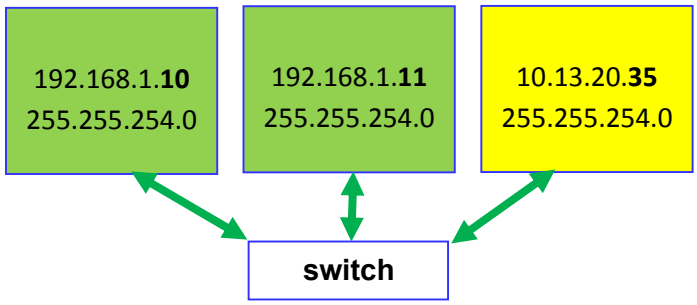
L'adresse de passerelle n'est pas nécessaire en cas d'absence du routeur.

Chaque équipement connecté sur un réseau recevra donc 2 adresses et un masque :
L'adresse IP de l'équipement, le masque réseau et l'adresse de la passerelle. Ces adresses sont par convention énumérés dans cet ordre pour un équipement.

Exemple :
192.168.1.15
255.255.255.0
192.168.1.1

Intercommunication

On connecte trois équipements sur un switch, dont une des adresses IP n'a pas la même classe que les deux premières :



Les adresses IP 1.10 et 11.11 pourront communiquer ensemble, mais ne pourront pas communiquer avec l'adresse IP 20.35, car il s'agit d'une classe d'adresse différente c'est à dire d'un réseau différent. Pour faire communiquer deux réseaux différents, il faut utiliser un routeur.

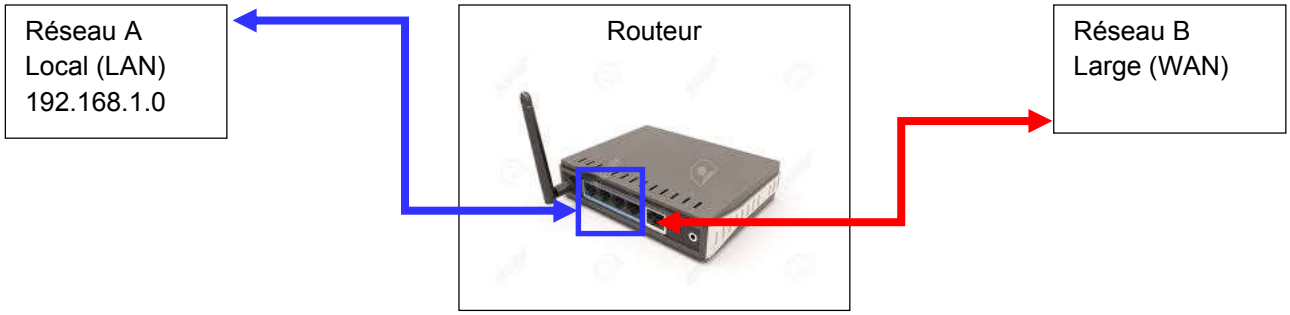
Cette situation survient lorsque l'on veut connecter plusieurs équipements sur le réseau internet (WAN). Le réseau internet brasse des adresses IP très différentes, de 1.1.1.1 à 255.255.255.255. Il est donc très possible que les adresses IP des équipements du réseau local (LAN) soient déjà utilisées sur le réseau WAN. Le routeur permet de faire la liaison entre les deux réseaux en **routant** les adresses.

Les adresses IP du réseau LAN d'appellent adresses IP **privées**. Elles ne sont pas visibles depuis internet.

Les adresses IP du réseau internet sont appelées des adresses IP **publiques**.

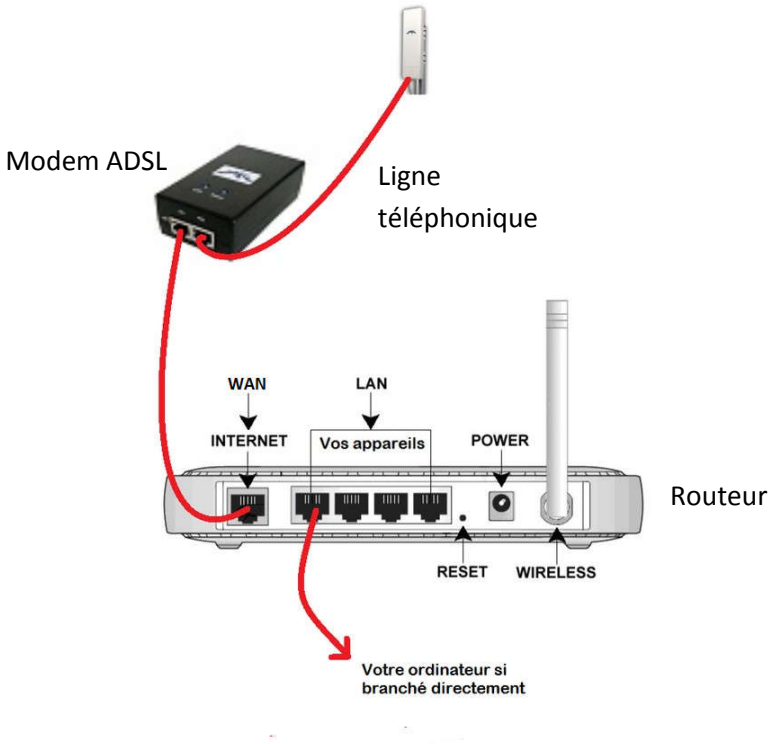
Interconnexion de deux réseaux : le routeur

On souhaite faire connecter deux réseaux, on utilise un routeur :



Le routeur comporte un switch qui route le LAN sur plusieurs ports ethernet identifiés en tant que tel. Il comporte, en plus du switch, un port ethernet WAN qui « translate » les messages entre les ports LAN et le port WAN. Le routeur, peut comporter également, un modulateur WIFI, GSM (3G, 4G), satellite, fibre ou ADSL. Dans ce cas, il s'appelle « BOX »

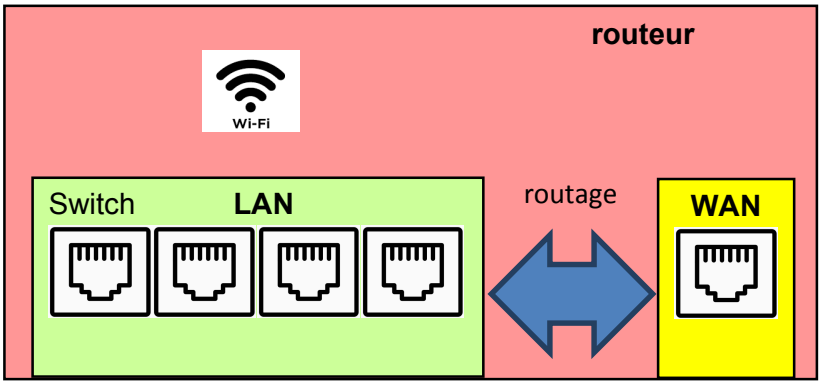
Le WAN est le port sur lequel on branche le réseau large (internet).



LAN = Local Adapter Network = Port réseau local
WAN = Wide Adapter Network = Port réseau large

Un routeur est paramétrable, et **doit** être paramétré à la première mise sous tension pour définir les règles d'appartenance au réseau et les tables de routage. Le routeur a une adresse ip propre sur le réseau.

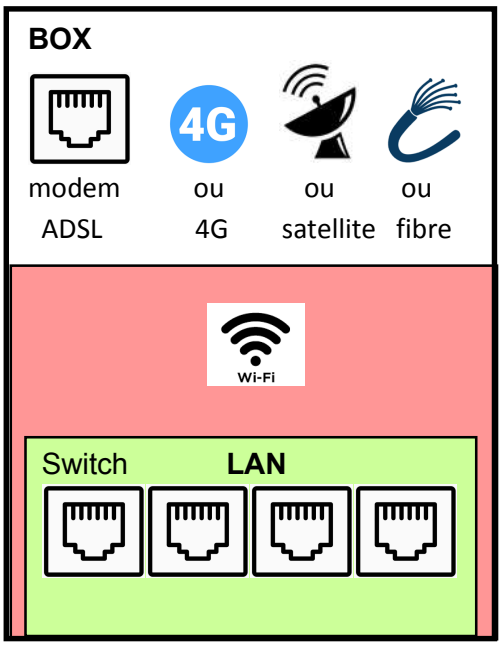
Un routeur se reconnaît d'un switch car le routeur a toujours quelques ports LAN qui constituent son switch, **et** un port WAN. Le découpage fonctionnel d'un routeur est montré ci-dessous.



Un routeur est constitué d'un switch doté d'un certain nombre de ports LAN, d'un port WAN et d'une logique de routage entre les deux réseaux. Il peut également recevoir un modem Wifi associé aux ports LAN.

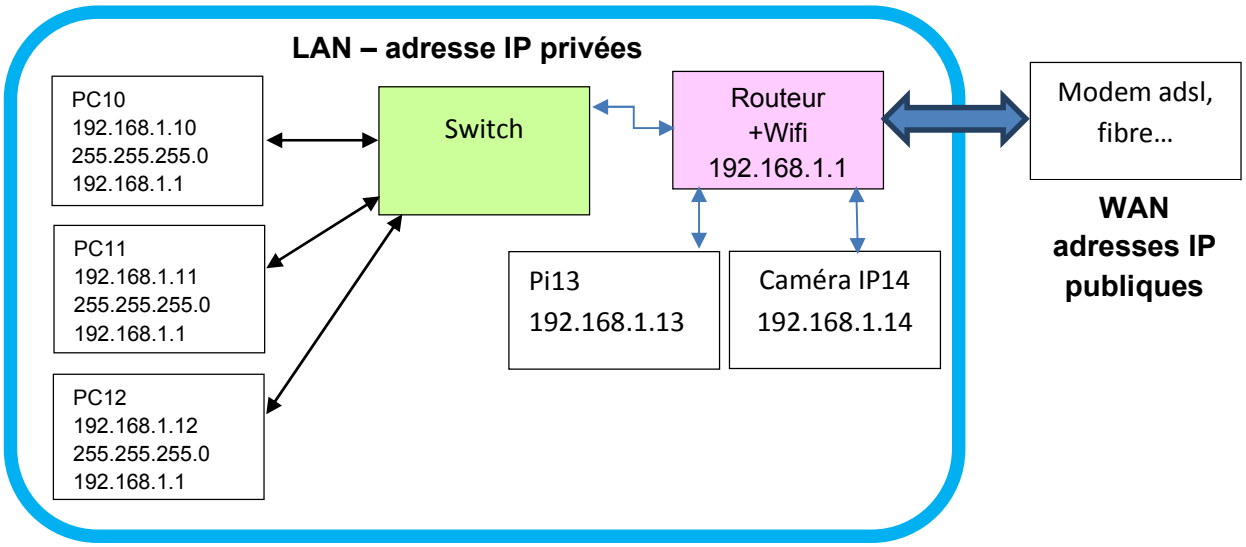
La « box », un routeur particulier

Une « box » est constituée d'un routeur (hors WAN) et donc d'un switch, et suivant le type, d'un modem ADSL, satellite, fibre ou GSM. Le découpage fonctionnel d'une « box » est montré ci-dessous. Une « box » est souvent dotée de capacités de stockages étendus comme la présence d'un disque dur.



Le wifi est vu par le routeur comme des adresses IP vues sur le réseau connecté au LAN.

Exemple d'architecture réseau simple



Commandes Dos ou Pi pour tester les équipements :

pour savoir si un équipement est connecté au réseau local ou au réseau global, utiliser la commande **ping** :

Exemple, depuis l'équipement PC11, taper la commande ping 192.168.1.10 qui permet de pinguer PC10. On peut aussi pinger 192.168.1.12 ou même un équipement sur le WAN.

Sur un pi, le ping est permanent. Utiliser ctrl C pour arrêter la commande.

```
U:\>ping 10.13.136.159

Envoi d'une requête 'Ping'  10.13.136.159 avec 32
Réponse de 10.13.136.159 : octets=32 temps<1ms TTL
Réponse de 10.13.136.159 : octets=32 temps<1ms TTL
Réponse de 10.13.136.159 : octets=32 temps<1ms TTL
Réponse de 10.13.136.159 : octets=32 temps<1ms TTL

Statistiques Ping pour 10.13.136.159:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

La commande ci dessus teste l'équipement 10.13.136.159. Celui-ci a répondu en 1 ms.

Les adresses IP du réseau privé ne sont pas visibles depuis internet.
Pour qu'un équipement communique avec internet, le routeur doit établir les liens entre le WAN et le LAN.

Site embarqués

Les switchs manageables et les routeurs sont configurables par l'intermédiaire d'un site internet embarqué. Ils sont atteignables par l'intermédiaire d'un navigateur internet.

Par exemple pour configurer un routeur dont l'adresse IP LAN est 192.168.1.1, vous tapez cette adresse dans la barre d'adresses de votre navigateur :

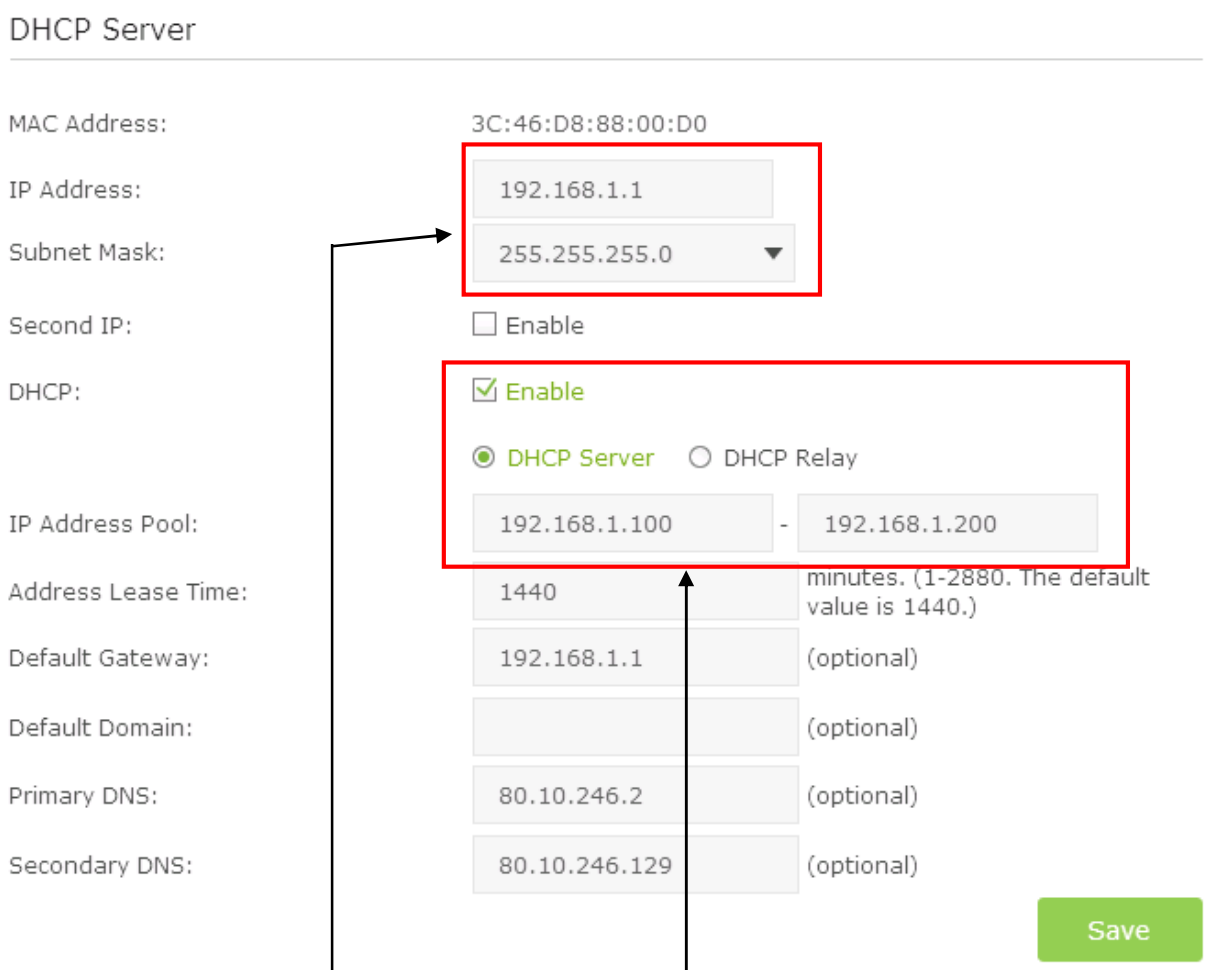
Vous êtes dans le site internet embarqué de votre routeur.

Adresses IP dynamiques et serveur DHCP

Toutes les affectations d'adresses IP que l'on vient de voir ont été faites manuellement, on les appelle adresses IP statiques. Il est néanmoins possible d'affecter des adresses IP de manière automatique sans avoir à les renseigner. On les appelle alors adresses IP dynamiques, elles sont obtenues depuis le routeur par le protocole DHCP.

Lorsqu'on n'a pas renseigné d'adresse IP dans un équipement et qu'on le connecte au routeur, ce dernier lui attribue une adresse IP, un masque et son adresse de passerelle automatiquement. Le routeur se paramètre car il est possible de lui imposer une plage d'adresses dans laquelle il choisira d'attribuer les adresses IP.

Voici un exemple de page de configuration du service DHCP d'un routeur :



L'adresse IP du routeur est 192.168.1.1, et son masque est 255.255.255.0.
Il peut donc gérer 255 périphériques sur son LAN.

Le serveur DHCP est validé (enabled) et il attribue les adresses 192.168.1.100 à 200, le masque 255.255.255.0 et la passerelle (gateway) 192.168.1.1 aux périphériques qui sont connectés sur son port LAN à la mise sous tension.

Il est possible d'utiliser des adresses IP fixes sur un réseau doté d'un serveur DHCP. Les IP fixes seront bien entendu choisies en dehors de la plage des adresses du serveur DHCP.

Notion de nom d'hôte

Un nom d'hôte permet d'associer une adresse IP un nom. Il est ainsi beaucoup plus facile de retenir un nom qu'une adresse, surtout sur le réseau mondial. Par exemple, l'adresse IP WAN 172.217.19.238 correspond à l'hôte `google.com`. Ainsi, au lieu de taper ping 172.217.19.238, on tape ping google.com : (à condition d'avoir un serveur DNS connecté – voir plus loin)

```
>ping google.com

Envoi d'une requête 'ping' sur google.com [172.217.19.238]

Réponse de 172.217.19.238 : octets=32 temps=39 ms TTL=49
Réponse de 172.217.19.238 : octets=32 temps=48 ms TTL=49
```

```
Réponse de 172.217.19.238 : octets=32 temps=37 ms TTL=49

Statistiques Ping pour 172.217.19.238:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 37ms, Maximum = 48ms, Moyenne = 41ms
```

Serveur DNS

Le système « sait » que google.com a pour adresse IP 172.217.19.238. La façon dont le système reçoit l'adresse IP en fonction d'un nom d'hôte s'appelle le service DNS. (DNS=Domain Name Server)

Lorsque l'on tape le nom d'un site internet dans la barre d'adresse d'un navigateur (on appelle ce nom un nom de domaine), votre ordinateur va interroger un service DNS dont il connaît l'adresse IP.

Evidemment, pour solliciter le serveur DNS, il faut connaître son adresse IP. Celui-ci est fourni automatiquement par votre FAI (Fournisseur d'Accès Internet) lors de votre connection, mais vous pouvez en utiliser un autre, bien que certains FAI bloquent l'accès aux DNS tiers.

Dans un système informatique, on peut définir deux adresses IP de servers DNS, le primaire et le secondaire.

Plusieurs cas sont à considérer sur une machine :

- Si elle est en IP fixe, il faudra obligatoirement renseigner le serveur DNS (au minimum un, au maximum deux).
- Si elle est en IP dynamique (DHCP) on peut soit :
    a) renseigner manuellement le serveur DNS en indiquant son adresse IP comme si on était en IP fixe (cas ci dessus)
    b) obtenir automatiquement le serveur DNS depuis votre FAI. Quelque fois, cette obtention ne fonctionne pas, et il faut indiquer manuellement un DNS.

Exemples de DNS de différents FAI :

FAI	DNS primaire	DNS secondaire
Darty	212.99.2.8	195.167.224.150
Free	212.27.40.240	212.27.40.241
Google	8.8.8.8	8.8.8.4
Orange	80.10.246.2	80.10.246.129
OpenDNS	208.67.222.222	208.67.220.220

Notez que OpenDNS possède une fonction d'anti-fishing.

Le serveur DNS n'est utile que si on souhaite connecter le périphérique à Internet.

Cartes Ethernet de contrôle des réseaux

Sur un PC, chaque port Ethernet possède une carte de contrôle, de même que pour le WIFI. Voici un exemple de PC disposant de 4 cartes :

2 ports Ethernet
1 Wifi 2,4 GHz
1 Wifi 5 GHz

Il est nécessaire de configurer ces 4 cartes pour accéder aux différents réseaux. Hormis l'adresse IP qui sera utilisée pour chaque réseau, chacune des cartes possède une adresse MAC.

Adresse MAC

Cette adresse mac est une adresse attribuée de façon unique dans chaque carte réseau au niveau mondial et permet d'identifier la carte. Ces adresses sont attribuées par constructeur. Il existe un catalogue d'adresses MAC permettant d'identifier le matériel et son constructeur. Ainsi, tout appareil connecté ethernet dispose d'une adresse MAC (téléphone, tablette, ordinateur, pi, console de jeux...)

L'adresse MAC a la forme de 6 octets hexadécimaux. Exemple : `5E:FF:56:A2:AF:15`

Sous Windows :
Pour voir l'adresse MAC des cartes de l'ordinateur, taper en ligne de commande `ipconfig /all`
Chaque carte est listée. L'adresse MAC apparaît à la ligne « Adresse physique ».

```
U:\>ipconfig /all

Configuration IP de Windows
   Nom de l'hôte . . . . . . . . . . . . : xxxxxx
   Suffixe DNS principal . . . . . . . . : xxxxxx
   Type de noeud. . . . . . . . . . . . . : Pair-Pair
   Routage IP activé . . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . . : Non

Carte Ethernet Connexion au réseau local :
   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Intel(R) 82567LM-3 Gigabit Network
   Adresse physique . . . . . . . . . . . : 84-2B-2B-9E-1B-71
   DHCP activé. . . . . . . . . . . . . . : Oui
```

Sous Raspbian :
Taper ifconfig dans la console :

```
pi@raspberrypi:~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1349:8f0f:19ae:1683  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:ef:00:27  txqueuelen 1000  (Ethernet)
        RX packets 16271  bytes 942484 (920.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12745  bytes 5206898 (4.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Certains réseaux identifient l'utilisateur non pas par l'adresse IP, mais par l'adresse MAC, qui constitue le plus bas niveau d'identification possible puisqu'il est matériel. Néanmoins, certains logiciels (ex : TmacV6) permettent de « changer » son adresse MAC de façon logicielle temporaire ou permanente pour contourner la protection.

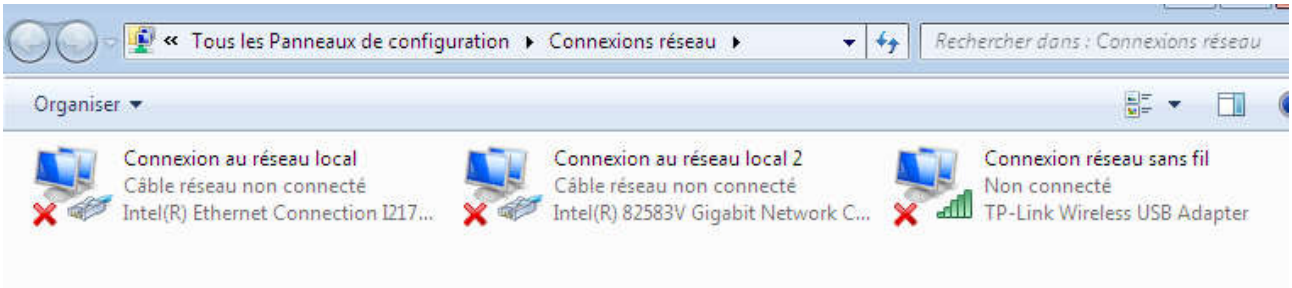
Configuration des Adresses IP et DNS sous Windows

W7 : Panneau de configuration / Centre réseau et partage / modifier les paramètres de la carte

ou

taper en ligne de commande : `control netconnections` ou
`control ncpa.cpl` (suivant version de windows)

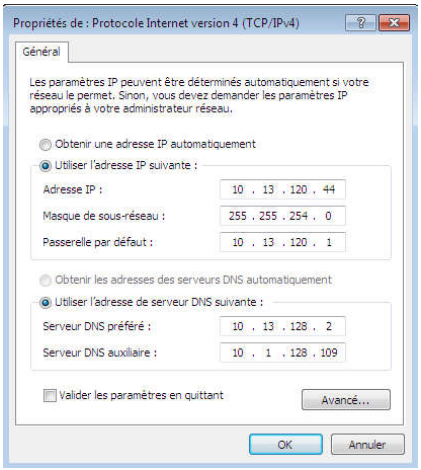
Vous arrivez sur l'écran de gestion de vos connexions réseaux. On peut trouver :



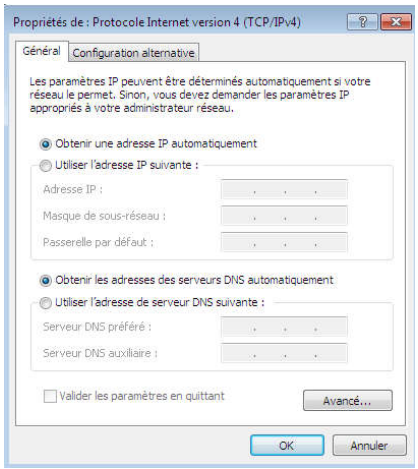
Connexion au réseau local : carte du premier premier port Ethernet
Connexion au réseau local 2 : carte du deuxième port Ethernet
Connexion au réseau sans fil : carte WIFI

On peut également trouver d'autres connexions, si un logiciel spécifique en a créé ; par exemple des VPN.

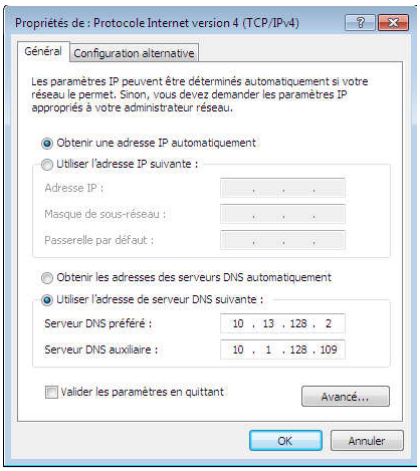
Pour configurer le LAN de la première carte (premier port) Ethernet, faire un clic droit sur l'icône du réseau local, propriétés, et sélectionner Protocole internet V4 (IPv4)



configuration en IP fixe et DNS préréglés



configuration en DHCP et obtention automatique des DNS



configuration en DHCP et DNS préréglés

Configuration des adresses IP et DNS sous raspbian

Concerne l'interface eth0 (la liaison filaire ethernet)
Il faut éditer le fichier /etc/dhcpcd.conf. Dans l'exemple ci-dessous, l'adresse ip de l'équipement est 192.168.1.100 (static ip address), l'adresse de la passerelle est 192.168.1.1 (static routers), l'adresse du serveur DNS est la passerelle, ou le DNS de google (domain_name_servers).

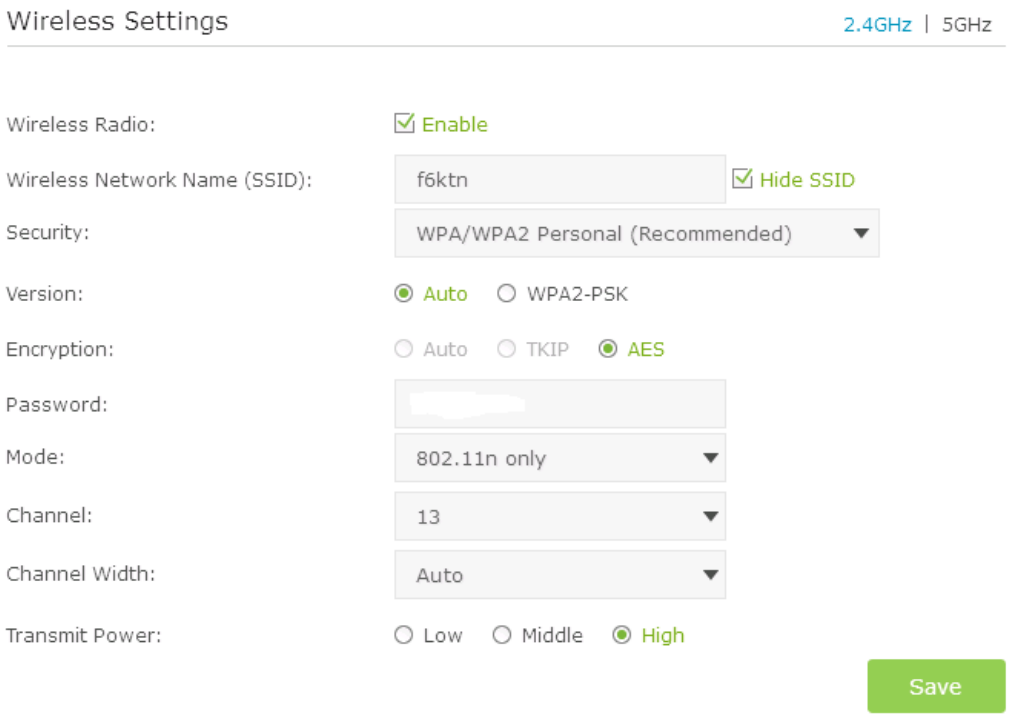
```
# Example static IP configuration:
interface eth0
static ip_address=192.168.1.100/24
# static ip6_address=fd51:42f8:caae:d92e::ff/64
static routers=192.168.1.1
static domain_name_servers=192.168.1.1 8.8.8.8
```

Configuration du Wifi d'un routeur

La configuration d'un réseau wifi d'un routeur nécessite le positionnement de quelques paramètres. Le wifi sera normalement dans la même plage d'adresses que le réseau LAN du routeur. Le réseau wifi peut être utilisé sur la bande 2,4 GHz ou sur la bande 5 GHz. Cette dernière permet une vitesse et une bande passante supérieure qu'en 2,4 GHz.

SSID : nom du réseau Wifi. Il peut être diffusé ou non diffusé, ce qui améliore la sécurité.
Cryptage : La liaison wifi peut être cryptée ou non. Il est nécessaire dans ce cas de définir une clé de cryptage.

Voici ci dessous l'exemple du réseau wifi « f6ktn ». Son SSID est caché, ce qui lui permet de rester invisible en cas de recherche des réseaux wifi.
Les réseaux ne diffusant pas leur SSID apparaîtront sous le libellé « autre réseau ». Pour s'y connecter, il faudra connaître à l'avance leur SSID.

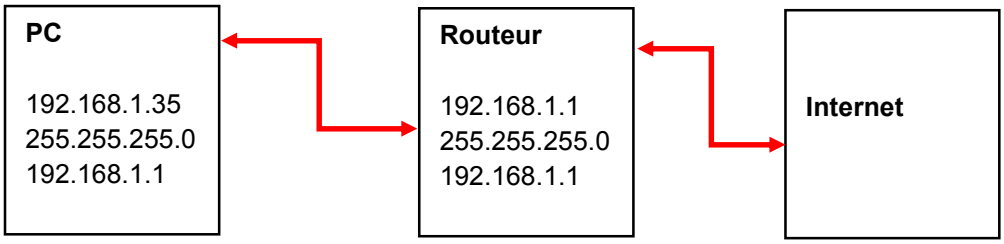


Un réseau wifi comporte, comme le réseau filaire, un serveur DHCP. Il est donc possible d'utiliser des IP fixes ou dynamiques sur des clients Wifi.

Détermination de l'origine de la non connectivité internet

Il arrive d'avoir une liaison Ethernet connecté au LAN et au WAN, mais qu'internet « ne marche pas ».

Exemple de configuration



1. Vérifier la liaison du PC au routeur

```
ping 192.168.1.1
```

Si non ok, vérifier la configuration IP du PC, s'assurer de la compatibilité des adresses et la liaison au routeur.

2. Vérifier la connexion du PC à internet (au travers du routeur)

```
ping 172.217.19.238
```

Si non ok, vérifier la connexion du routeur à internet

3. Vérifier la connexion du PC à un serveur DNS (au travers du routeur)

```
ping google.com
```

Si non ok, vérifier la configuration DNS du PC. Certains FAI ne distribuent pas le DNS de façon automatique au routeur, et il faut alors l'indiquer dans le routeur. Côté PC il faut mettre le DNS à l'adresse du routeur.

Pour se connecter à internet standard, il est nécessaire d'avoir la connectivité IP et être connecté à un serveur DNS pour pouvoir assurer la résolution des noms de domaine.

Pour se connecter aux réseaux internet « superposés » (Deepweb, I2P, Freenet...), les serveurs DNS ne sont pas nécessaires (mais ils sont utilisables pour atteindre des sites de l'internet standards) car il n'y a pas de moteur de recherche pour ces réseaux. On utilise directement l'adresse URL du site à atteindre (qui est une codification de l'adresse IP)

Structure d'une trame Ethernet

Une trame Ethernet peut comporter différentes structures. Voici un exemple dont le détail est fourni ci-dessous :

Sync	7 octets 0xAA + 1 octet 0xAB
SFD	1 octet AB – Marqueur de début de la trame
Mac Destination	6 octets
Mac Source	6 octets
protocole	2 octets – type du protocole

Suit une zone de longueur variable appelée datagramme

Checksum	2 octets

Structure du datagramme dans la cadre d'une trame de transmissions de données :

Entête IP
Entête UDP :
- port source
- port destination
- longueur
- Checksum
- données

Protocoles et ports

Une communication ethernet est toujours associée à un numéro de port, en fonction du protocole utilisé. Le protocole dépend de la fonctionnalité que l'on souhaite réaliser. Le regroupement de l'adresse IP et du port s'appelle un *socket*. Certains ports sont réservés par le système ou par des organisations.

Exemples de ports et de protocoles standards :

protocole	**description**	**port**
http	protocole « internet » standard http://	80
https	protocole internet crypté : https://	443
ssh (telnet crypté)	commandes et terminal en ligne cryptés	22
ftp	transfert de fichiers	20/21
Telnet	commandes et terminal en ligne	21/23
Smtp	service d'échange de courriers entre deux serveurs	25
pop3	protocole client / serveur pour accéder au courrier d'une machine distante	110
dns		53
http	port alternatif du http	8080

Nous avons parlé du site internet embarqué dans le routeur pour le configurer. Certains éléments du routeur sont atteignables par telnet en ligne de commande. On peut par exemple rebooter un routeur par une ligne de commande telnet qui utilise le port 21 ou 23 en standard.

Il y a bien d'autres protocoles existants. Vous pouvez utiliser vos propres ports si vous souhaitez par exemple que deux programmes que vous avez écrits doivent communiquer ensemble sur deux processeurs différents, connectés par ethernet.

Pour atteindre un port sur une adresse ip, on tape : adresse_ip :port
Par exemple : 192.168.1.100:22
Ici le port 22 sur l'adresse ip 192.168.1.100

http://site.fr est équivalent à site.fr:80

Il existe plusieurs protocoles d'échange de données sur éthernet ; mais les deux plus importants sont TCP et UDP.

Protocole TCP

TCP est un protocole connecté utilisé pour échanger de grandes quantités de données. L'envoi de données est garanti par un accusé de réception et un réenvoi le cas échéant. Les ports FTP (21), SSH (22), Telnet (23), SMTP (25), HTTP (80), POP3 (110) utilisent le protocole TCP.

Protocole UDP

UDP est un protocole non connecté idéal pour échanger de petites quantités d'informations de type demande-réponse. Il ne demande pas d'accusé de réception des trames, qui ne seront pas renvoyées si elles sont perdues. Par exemple les flux audio et vidéos utilisent le protocole UDP.

URL, adresse de site et nom de domaine

Un peu de vocabulaire sur les termes utilisés dans les techniques de réseaux.

Une **URL** est une adresse internet. C'est donc une **adresse de site**.

Un **nom de domaine** est un nom attribué à un serveur et donc à une adresse ip.

Exemples :

free.fr
orange.fr } sont des noms de domaine.

forum.free.fr
free.fr/bienvenue } sont des pages spécifiques du nom de domaine free.fr

Le nom de domaine du l'url « forum.free.fr/sujet/65787 » est free.fr

Autres exemples :

paypal.com est un nom de domaine.
paypal.com.payement.com est une url, dont le nom de domaine est payement.com. Cette URL ne vous dirigera donc pas sur paypal.com mais sur le site payement.com, probablement un site pirate.

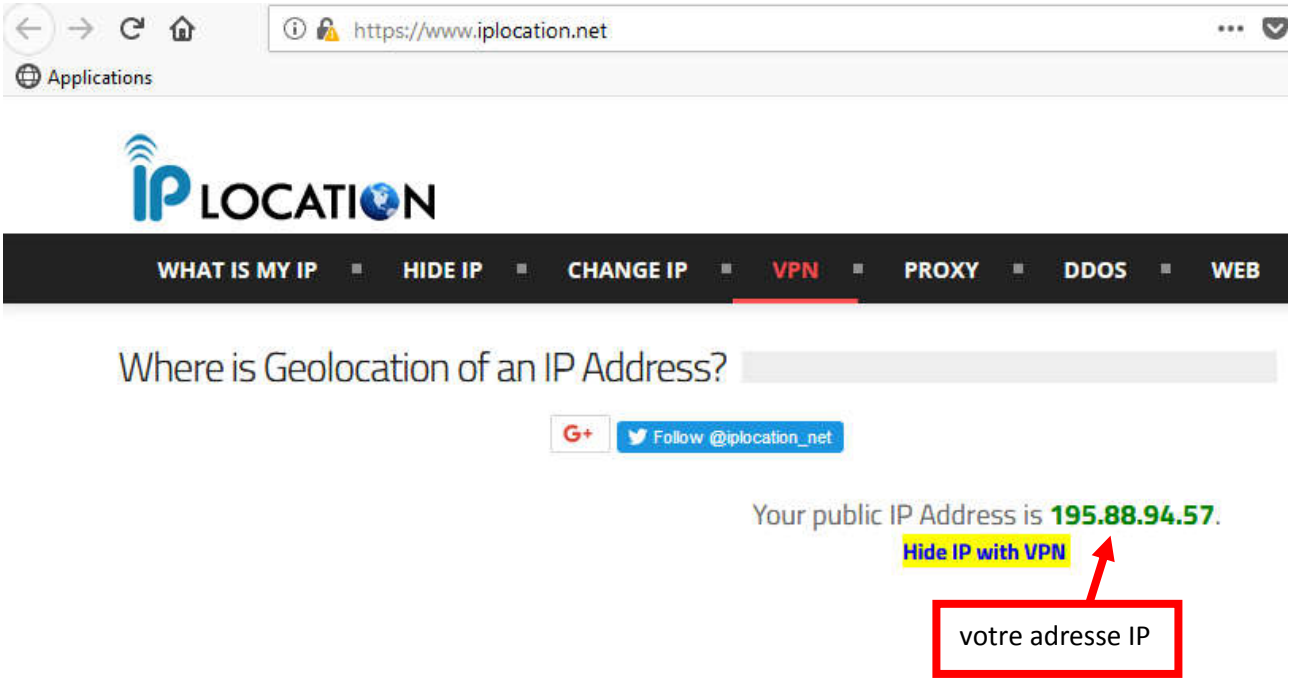
Le nom de domaine est associé à une adresse IP. Exemple free.fr =212.27.48.10
C'est le serveur DNS qui renvoie l'adresse IP en fonction du nom de domaine.

Attribution d'une adresse internet

Lorsque votre FAI vous donne une adresse IP lorsque vous connectez votre routeur sur internet, il vous attribue une adresse IP dans le WAN. Cette adresse IP peut être fixe ou dynamique.

Votre routeur, dans l'une de ses pages, vous indique l'adresse IP WAN (internet) sous laquelle vous êtes visible depuis internet.

Un autre moyen pour connaître son adresse IP est de consulter un site internet spécialisé comme iplocation.net, qui vous donne en plus votre localisation :



L'adresse IP de votre FAI, en plus d'être statique ou dynamique, peut être de deux types : privée ou publique. Le fait que votre adresse WAN soit publique ou privée dépend de votre FAI.
Exemples : Free distribue des adresses IP publiques
En GSM, Orange, Bouygues et SFR attribue des adresses IP privées.

Adresse WAN publique

Une adresse WAN publique signifie que vous êtes connecté en direct sur le réseau internet. La liaison pourra accepter une liaison entrante initiale depuis un tiers (quelqu'un pourra se connecter

chez vous), et vous pourrez par exemple contrôler vos caméras depuis internet lorsque vous êtes absent.

Adresse WAN privée

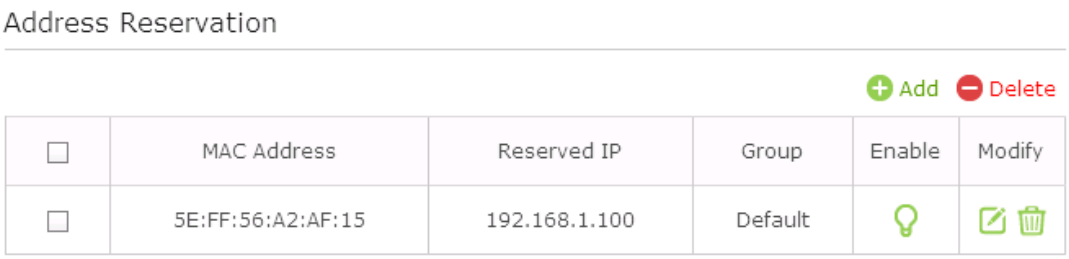
Une adresse WAN privée signifie que vous n'êtes pas connecté en direct sur le réseau internet. Votre réseau WAN est en réalité connecté sur le LAN du routeur qui se situe chez votre FAI. La liaison ne pourra pas accepter des liaisons entrantes depuis un tiers (personne ne pourra se connecter chez vous), et vous ne pourrez pas contrôler vos caméras.

Pour savoir si vous utilisez une adresse WAN publique ou privée, il faut contrôler l'adresse IP WAN dans le routeur, et l'adresse IP WAN de votre connexion sur internet en consultant un site spécialisé. Si elles sont identiques, vous utilisez une adresse publique, sinon vous utilisez une adresse privée.

Attribution d'une adresse dynamique réservée

Lorsqu'un routeur distribue une adresse IP dynamique par le protocole DHCP à un périphérique qui se connecte, cette adresse IP n'est pas prévisible. Il est donc difficile de connaître à priori à l'avance quelle sera son adresse IP. Il est malgré tout possible de réserver dans le routeur une adresse IP par équipement, en fonction de l'adresse MAC. Cet équipement ainsi réservé aura donc toujours la même adresse IP, bien qu'il soit attribué par le DHCP.

Voici ci-dessous un exemple de réservation de périphérique DHCP dans un routeur.

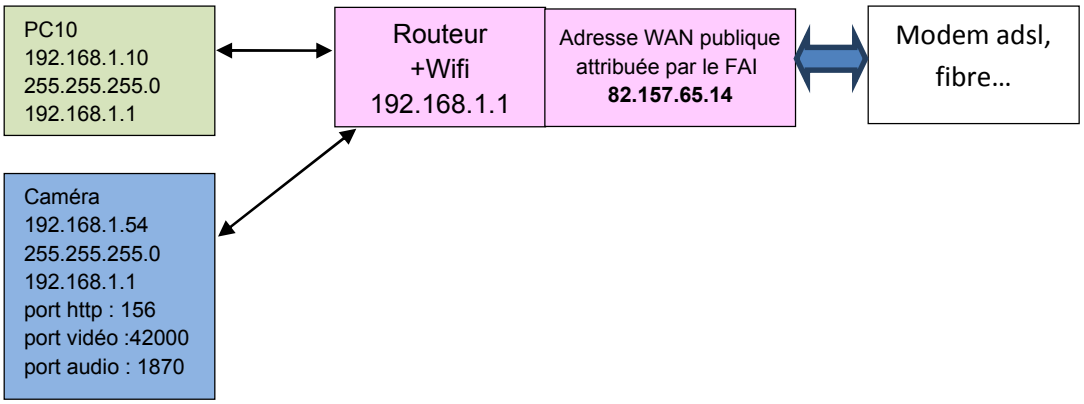


Le périphérique dont l'adresse mac est 5E:FF:56:A2:AF:15 a été réservé en 192.168.1.100. La configuration IP de ce périphérique doit être sur DHCP (attribution automatique d'une adresse IP). Lorsque le routeur verra se connecter ce périphérique, il va interroger son adresse MAC. Si elle correspond à une de ses adresses réservées dans cette table, il attribuera l'adresse en conséquence.

Routage et redirection de ports

Nous avons vu que les adresses IP du réseau privé ne sont pas visibles depuis internet. Inversement, pour qu'un équipement communique avec internet, le routeur doit établir les liens entre le WAN et le LAN. Lors de la connexion d'un dispositif utilisant un port non standard, il faut manuellement l'indiquer au routeur dans sa table de routage.

Exemple :



L'adresse WAN publique, visible depuis internet est 82.157.65.14.

Par défaut, le routeur établit des liens pour certains ports normalisés dont le port HTTP (80), https (443) et les ports de messagerie 25/110. C'est pourquoi il est possible de connecter internet depuis un PC sur le LAN sans ouvrir des ports supplémentaires dans le routeur.

On supposera que le FAI distribue des adresses IP publiques à ses clients.

On connecte une caméra IP dont les caractéristiques sont données dans le schéma ci-dessus. Comme l'adresse IP192.168.1.54 fait partie du LAN, elle n'est pas connectable depuis internet. Pour la rendre connectable, il faut créer un routage dans le routage par ce qu'on appelle une table de translation d'adresses (NAT en anglais : *network address translation*). L'adresse IP de la caméra se « reroutée » vers un autre port que l'on déclarera dans la NAT. Le tableau de routage est différent sur les différentes marques de routeur. Voici un exemple sur une « box » free.

redirection de ports

port	protocole	Destination	port
156	tcp	192.168.1.54	156
42000	udp	192.168.1.54	42000
1870	udp	192.168.1.54	1870

Cela signifie qu'un flux qui arrive sur le port 156 du routeur sera redirigé vers le socket 192.168.1.54 :156 (le port de commande http de la caméra). Il faut faire la même chose pour le flux audio et vidéo de la caméra.

Ensuite, pour se connecter à la caméra, on tape l'URL suivante dans la barre d'adresses :

82.157.65.14:156

Vous êtes alors connecté à votre caméra.

Redirection automatique des ports : le protocole UpnP

UpnP est un protocole « plug and play » qui permet de connecter des périphériques éthernet sur un réseau avec ouverture automatique des ports entre le routeur et le périphérique, sans avoir à effectuer la configuration de redirection comme vus précedemment. Pour pouvoir utiliser ce service, le routeur ET le périphérique doivent être compatibles UpnP.

Les réseaux virtuels privés (VPN)

Les réseaux virtuels privés, également appelés tunnel vpn, sont des « tuyaux sécurisés » entre un équipement connecté et un serveur distant.

Une liaison entre deux équipements finaux utilisant internet n'est pas fiable, car un tiers peut intercepter les liaisons. Lorsque le protocole utilisé est « http » c'est-à-dire non sécurisé (port 80), le contenu n'est pas crypté et il est transmis en clair. Lorsque le protocole utilisé est « https » (port 443), le contenu est crypté mais l'adresse IP source et destination ainsi que l'URL sont visibles, ne garantissant pas la confidentialité de la transmission. De plus le HTTPS peut être décrypté à postériori.

Le VPN utilise un serveur distant qui encapsule les trames de trafic entre le destinataire et l'expéditeur (et inversement). Ainsi, si le protocole HTTPS est utilisé, un 2ème cryptage est appliqué à la transmission, cryptant également les entêtes des paquets.

Les protocoles utilisés dans le tunneling peuvent être PPTP, L2F, L2TP et IPSec.

La mise en œuvre de VPN sur un ordinateur client nécessite en général l'installation d'un programme créant une connexion supplémentaire sur la carte réseau. Il est en général nécessaire de souscrire un abonnement à un service VPN. Certains sont gratuits mais ont un volume limité.

Il existe aussi des programmes qui installent et qui configurent un VPN gratuitement. Par exemple SOFTEtherVPN Client Manager. Lorsque la liaison est établie, vous entrez sur internet depuis un point d'accès de ce VPN dont vous choisissez le pays de connexion. Vous pourrez ainsi apparaître comme connecté depuis n'importe quel pays dans le monde. Attention : SoftEtherVPN surencrypte les trames au détriment du volume. Attention donc au volume consommé suivant votre FAI.

Le Wifi

Le wifi est une technologie permettant d'interfacer un réseau éthernet sur un réseau radio. Une carte réseau wifi dispose des mêmes attributs qu'une carte Ethernet : Adresse MAC, adresse IP, masque, passerelle, DNS. Des options de sécurité permettent de crypter les liaisons :

- cryptage WEP : facilement piratable, à ne pas utiliser
- cryptage WPA TKIP : comporte des failles de sécurité
- cryptage WPA2 AES : sécurité plus robuste

ces cryptages sont associés à des mots de passe de connexion.

Une des caractéristique d'un réseau wifi est de diffuser son identifiant, que l'on appelle SSID. il permet d'identifier un réseau WIFI parmi d'autres. Cet ID est alphanumérique et peut être rempli au choix.

Pour se connecter à un réseau WIFI, il est nécessaire de connaître son SSID **et** son mot de passe.

Afin d'augmenter la sécurité, il est possible de ne pas diffuser le SSID. Il apparaîtra lors du SCAN de l'environnement wifi sous le nom « autre réseau ».

Bande 2,4 GHz

Bande passante par canal : 22 MHz. Un canal occupe donc en fait 3 canaux du fait de la superposition des canaux adjacents. La vitesse maximale est de 52 Mbits/s. Elle descend avec l'éloignement de la station de base avec le carré de la distance.
Les fréquences du WIFI en 2,4 GHz sont :

canal	Fréquence en MHz
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

Noter que la fréquence 2,45 MHz est celle des fours à micro-ondes.

Bande 5 GHz

Les vitesses de base sont de 450 Mbits/s (en norme N). Les canaux adjacents peuvent être regroupés par 2, 4 ou 8 pour augmenter le débit jusque 2 Gbits/s (Norme AC wave 2)

canal	Fréquence en MHz	canal	Fréquence en MHz
36	5180	124	5620
40	5200	128	5640
44	5220	132	5660
48	5240	136	5680
42	5260	140	5700
56	5280	144	5720
60	5300	149	5745
64	5320	153	5765
100	5500	157	5785
104	5520	161	5805
108	5540	165	5825
112	5560		
116	5580		
120	5600		

Le Bluetooth

Cette technologie permet de connecter des équipements avec la technologie IP, mais avec un débit et des puissances beaucoup plus faibles.

Le débit est de 1 Mbits/s. Selon les version de bluetooth, il peut monter à 10 Mbits/s.
L'avantage du Bluetooth est sa faible consommation puisque sa puissance est beaucoup plus faible que le wifi. Il est donc mieux adapté à des appareils portables sur batterie qui en limite la décharge.

Les canaux bluetooth s'étalent de 2402 à 2480 MHz. Le bluetooth utilise la structure de maître et d'esclave. Un maître peut être maître d'un autre maître qui dispose de ses propres esclaves.

le bluetooth peut s'utiliser sous différentes forme. En voici deux parmi d'autres : **RFCOMM** qui émule un port série (COMx) avec tous les signaux RS232 (Txd Rxd, Rts,Cts ..) , **BNEP** qui fournit un fonctionnement similaire au wifi.

Annexes

Réglage du wifi sur Raspbian

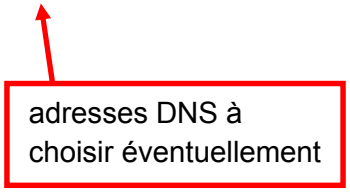
```
sudo nano /etc/wpa_supplicant/wpa_supplicant.conf

network=
{
    ssid="ssid du wifi"
    psk="clé de cryptage"
    key_mgmt=WPA-PSK
}
```

IP fixe sur Raspbian

```
sudo nano /etc/dhcpcd.conf

# Example static IP configuration:
interface eth0
static ip_address=192.168.1.100/24
# static ip6_address=fd51:42f8:caae:d92e::ff/64
static routers=192.168.1.1
static domain_name_servers=192.168.1.1 8.8.8.8
```



Glossaire

FAI	Fournisseur d'accès à internet
DHCP	Protocole d'obtention d'une adresse IP dynamique
DNS	Protocole d'obtention d'un serveur de noms de domaines = résolution de noms
NAT	Table de translation d'adresse dans le routeur
WAN	Réseau « large » (internet) Peut désigner aussi le réseau WIFI
LAN	Réseau local privé
VPN	Réseau privé virtuel
MAC	Adresse MAC : adresse physique d'une carte réseau (ethernet, wifi ou bluetooth)
UpnP	Protocole permettant la translation d'adresse et l'ouverture des ports automatiques d'un équipement pour qu'il soit visible sur le WAN.
Socket	Regroupement d'une adresse IP et d'un port

Liste des présentations disponibles

1. Introduction au DMR et au TETRA
2. Composants radio-électriques passifs particuliers
3. Mesures complexes en hautes fréquences
4. Adaptations d'impédances
5. Réseaux Ethernet et connectivités
6. Complément sur les adaptations d'impédances
7. Lignes de transmissions
8. Foudres, surtensions et protections
9. Cavités duplexeurs et montages à cavités