Fiche de révisions - protocoles et réseaux

Rédigé par : Jimmy Paquereau

1. Préliminaire

Au travers des précédents chapitres, nous avons abordés les notions d'architectures client-serveur ou encore de service d'authentification. Il vient que ces notions n'ont de sens que dans le cadre d'un réseau, à savoir dès lors que des machines informatisées peuvent communiquer entre elles.

Quoique nous ayons étudié ces concepts, nous l'avons fait en faisant abstraction de notions liées aux réseaux. En outre, afin que des ordinateurs et autres appareils interagissent les uns avec les autres, il faut encore que les conditions soient réunies afin qu'ils puissent le faire. Et pour ce faire, il faut tout à la fois des infrastructures matérielles et logicielles.

Dans ce chapitre, nous tâchons d'éclaircir la situation en définissant des notions de réseau et quelques autres notions fondamentales que nous avons jusqu'à maintenant éludées ou brièvement entrevues.

2. Réseau et sous-réseau

2.1. Définition

Un réseau informatique est un ensemble d'appareils informatisés :
o interconnectés entre eux au moyens de divers liaisons filaires (câbles, exemple : câble Ethernet) ou non filaires (exemple : wifi) ;
o interconnectés entre eux via des matériels « intermédiaires » (exemple : commutateur (switch) ou routeur) assurant l'acheminement des messages à bon port ;
o comportant des ressources logicielles leur permettant d'échanger des informations au travers des liaisons.

2.2. Adresse MAC

Tout d'abord, on notera que **tout matériel est identifié de manière unique par ce qu'on appelle une adresse MAC**. **On parle encore d'adresse physique**. Celle-ci n'a aucun rapport avec une adresse IP ! Elle est constituée d'une partie permettant d'identifier de manière unique le constructeur de l'appareil (sur 3 octets) et d'une autre permettant d'identifier de manière unique l'appareil parmi ceux du constructeur (sur 3 octets).

Rappel :
- **bit** : un bit correspond à un 0 ou à un 1 (en binaire). Ce sont les « chiffres binaires » (on parle de digit) ;
- **octet** : un octet est une succession de 8 bits (exemple : 10101010). C'est un nombre, mais un nombre écrit en binaire. Si, en décimal, on a $158 = 1x10^2+5x10^1+8x10^0$, en binaire, on a $(110)_2 = 1x2^2+1x2^1+0x2^0=6$. La notation $(110)_2$ se lit « 110 base 2 ». Et oui, binaire signifie tout simplement « en base 2 ».

2.3. Adresse IP et masque de sous-réseau

Au sein d'un réseau local d'entreprise (LAN, *Local Area Network*), **une adresse IP v4 permet d'identifier de manière unique un matériel sur un sous-réseau**. **Elle est constituée de 4 nombres allant de 0 à 255**. Ici, nous ne parlerons que d'adresse IP v4. Ainsi, sans ambiguïté, on dira plus simplement adresse IP.
On l'écrit usuellement en notation décimale de la manière suivante : X.X.X.X (où X est un nombre compris entre 0 et 255). Exemple : 192.168.1.254.

Le **masque de sous-réseau** est une information, s'apparentant également à une adresse IP, permettant d'identifier, par calcul, l'adresse IP du réseau auquel est rattaché le matériel (partie réseau) et la partie hôte de l'adresse IP. Le masque de sous-réseau s'écrit exactement de la même manière qu'une adresse IP (exemple : 255.255.255.0).

En effet, une adresse IP est constituée de deux parties :
o la **partie réseau** (adresse IP réseau) indiquant le réseau de rattachement du matériel ;
o la **partie hôte**, identifiant effectivement le matériel sur le réseau local (en fait, sur le sous-réseau).
On notera qu'un réseau local peut très bien n'être constitué que d'un seul sous-réseau.

Exemple : 192.168.1.28 (masque : 255.255.255.0)
Partie réseau : 192.168.1.0
Partie hôte : 0.0.0.28
Ce qui signifie : le poste qui à l'adresse IP 192.168.1.28 appartient au sous-réseau 192.168.1.0 et il s'agit de l'hôte « numéroté » 0.0.0.28.

Pour aller plus loin

Calcul de la partie réseau et de la partie hôte.

o configuration : 192.168.16.72/26 (c'est le couple adresse IP + masque de sous-réseau) ;
o adresse IP : 192.168.16.72 ;
o masque de sous-réseau : 255.255.255.192 (abrégé /26, explication fournie ci-dessous) ;

Ecrivons l'adresse IP et le masque de sous-réseau en binaire.

o 255 = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = $1x2^7 + 1x2^6 + 1x2^5 + 1x2^4 + 1x2^3 + 1x2^2 + 1x2^1 + 1x2^0$
Soit en binaire : 11111111 (on a pris tous les 1 devant les puissances de 2)
On note $(255)_{10} = (11111111)_2$ (se lit : 255 base 10 égal 11111111 base 2)
o 192 = 128 + 64 = $1x2^7 + 1x2^6 + 0x2^5 + 0x2^4 + 0x2^3 + 0x2^2 + 0x2^1 + 0x2^0$
D'où : $(192)_{10} = (11000000)_2$
o $(168)_{10} = (128 + 32 + 8)_{10} = (10101000)_2$
o $(16)_{10} = (00010000)_2$ (en guise d'exercice, vérifiez !)
o $(72)_{10} = (01001000)_2$ (en guise d'exercice, vérifiez !)

Finalement, l'IP et le masque s'écrivent en binaire :

o masque de sous-réseau : 11111111.11111111.11111111.11000000 (soit 26 bits à 1, d'où le fameux /26) ;
o adresse IP : 11000000.10101000.00010000.01001000

A présent, le calcul effectif de la partie réseau de l'IP à partir de son masque :
o l'opération à utiliser est un ET logique (booléen) entre le masque et l'IP ;
o en logique booléenne, le ET s'écrit « . » ou « x » (multiplication booléenne) ;
o table de vérité : 1.1 = 1 ; 1.0 = 0 ; 0.1 = 0 ; 0.0 = 0 ;

11111111.11111111.11111111.11000000
11000000.10101000.00010000.01001000
o la partie réseau est donc : ----------
11000000.10101000.00010000.01000000
= **192.168.16.64** (en décimal)

Quant à la partie hôte, on la trouve comme suit :
o autant de 0 que de 1 dans le masque de sous-réseau ;
o puis la partie restante de l'adresse IP ;

11111111.11111111.11111111.11000000
11000000.10101000.00010000.01001000
o la partie réseau est donc : ----------
00000000.00000000.00000000.00001000
= **0.0.0.8** (en décimal)

Conclusion : si la partie réseau et la partie hôte sont très faciles à identifier avec un masque en /8 (255.0.0.0), /16 (255.255.0.0) ou /24 (255.255.255.0), cela n'a rien d'immédiat dans les autres cas.

2.4. Sous-réseau

C'est bien beau tout cela ! Mais finalement, qu'est-ce que c'est un sous-réseau ? **Un sous-réseau, c'est un ensemble de matériel informatisés :**
o reliés à un commutateur ;
o possédant le même masque de sous-réseau ;
o et communiquant entre eux au moyen des protocoles ARP et Ethernet

3. Procotole ARP

3.1. Commutateur

Le commutateur, ou *switch*, est l'élément central d'un sous-réseau et les hôtes du sous-réseau s'adressent à lui en utilisant le protocole ARP. Eventuellement, plusieurs commutateurs peuvent être reliés entre eux. On retrouve typiquement les commutateurs dans des **baies de brassage**, c'est-à-dire dans des « armoires » dans lesquelles parviennent de multiples câbles Ethernet. L'embout de chaque câble (le connecteur RJ45) vient s'insérer dans un port du commutateur. En ce sens, un commutateur est un pont multiports (un pont est également un matériel réseau). En pratique, un commutateur possède plus de fonctionnalités que celles que nous évoquons ci-après.

Exemple de switch

Symbole

3.2. Protocole ARP

Nous l'avons déjà vu, un protocole est basé sur l'émission/réception de messages. C'est en quelque sorte un mode et des modalités de discussion. **Les messages du protocole ARP sont appelés les paquets ARP**. La transmission filaire (sur les câbles) de ces messages est réalisée au moyen du **protocole Ethernet**. Nous y reviendrons plus loin.

Le protocole ARP est un protocole permettant à un hôte d'un sous-réseau de demander l'adresse MAC d'un autre hôte du sous-réseau ou plus généralement du réseau local.

Les deux messages du protocole ARP sont l'**ARP request** (demande ARP) et l'**ARP reply** (réponse ARP).

Fonctionnement

Une « demande ARP » est un message transmis par un émetteur au commutateur. Ce message consiste à demander l'adresse MAC d'un destinataire dont l'émetteur fournit l'adresse IP. Plusieurs cheminements sont alors possibles :

1. L'adresse IP fournie appartient au même sous-réseau :
o si le commutateur connaît l'adresse MAC en question, il la retourne directement à l'émetteur au moyen d'un message ARP reply ;
o au contraire, s'il ne connaît pas cette adresse, il retransmet cette demande sur tous ces ports à l'exception de celui correspondant à l'émetteur. Alors, si une machine se reconnaît (elle a l'adresse IP fournie), elle fait connaître son adresse MAC en retournant un message ARP reply au commutateur, lequel le retransmet à l'intéressé.

2. L'adresse IP fournie n'appartient au même sous-réseau :
o si le commutateur connaît l'adresse MAC en question, il la retourne directement à l'émetteur au moyen d'un message ARP reply ;
o au contraire, s'il ne connaît pas cette adresse, il retransmet cette demande sur tous ces ports à l'exception de celui correspondant à l'émetteur. Malheureusement, aucune machine ne se reconnaît car l'adresse IP fournie est celle d'une machine se trouvant sur un autre sous-réseau. Mais, potentiellement, le routeur (s'il y a un routeur évidemment) répond par un message ARP reply en précisant son adresse MAC. On parle alors de proxy ARP. En quelque sorte, le routeur se « faisant passer pour » le matériel en question. Pourquoi ? Parce que le routeur fait également partie du sous-réseau du matériel recherché et connaît ce matériel. En effet, nous verrons plus loin qu'un routeur peut être connecté à plusieurs sous-réseaux.

Une fois qu'un hôte a connaissance de l'adresse MAC du matériel avec lequel il souhaite communiquer, il est enfin capable de transmettre ses données au bon matériel en utilisant le protocole Ethernet.

Par ailleurs, les matériels (dont le commutateur) conservent en fait **un cache ARP** qu'ils mettent à jour. Ce cache ARP, ou table ARP, est une table de correspondance ou chaque entrée de la table (chaque ligne) associe entre autre l'adresse IP d'un matériel du sous-réseau à son adresse MAC.

3.3. Protocole Ethernet

Le protocole Ethernet est un protocole dit de couche « liaison de données ». Cela signifie qu'il décrit la circulation de l'information au niveau du câble, ce qui relève de l'électronique et du traitement du signal (au même titre que le protocole Wifi). Les messages du protocole Ethernet sont **appelés les trames Ethernet**.

Ce qu'on retiendra, c'est que ce protocole existe et est utilisé par le commutateur.

3.4. Rôle du commutateur

Dans son cache ARP, le commutateur conserve également le port sur lequel le matériel est connecté. **Lorsqu'il reçoit une trame Ethernet, le commutateur est capable de la retransmettre à l'intéressé. En conclusion, le commutateur commute ! C'est-à-dire qu'il retransmet les trames et paquets à l'intéressé**. **On parle de diffusion unicast**.

Plus encore, un commutateur est capable d'effectuer des **diffusions broadcast**. **Dans le cas d'un commutateur, une diffusion broadcast consiste à retransmettre un message à l'ensemble des hôtes du sous-réseau**. Il existe des adresses IP dites **adresses IP de diffusion** (**adresses de broadcast**)**. Chaque sous-réseau possède une adresse IP de diffusion**. En somme, cette adresse IP permet à un matériel de transmettre, via un commutateur, des informations à l'ensemble des matériels du sous-réseau. Comme évoqué précédemment, c'est le commutateur qui se charge de la diffusion.

Exemple : sur le sous-réseau 192.168.1.0/24, l'adresse IP de broadcast est 192.168.1.255. Le « /24 » correspond au masque de sous-réseau et signifie 255.255.255.0. Sur le sous-réseau 10.0.5.0/8, l'adresse IP de broadcast est 10.255.255.255. Le « /8 » correspond au masque de sous-réseau 255.0.0.0.

En résumé, **un commutateur permet à des machines d'un sous-réseau de communiquer entre elles**.

3.5. Concentrateur

Les **concentrateurs** (**hub**) ne sont plus ou quasiment plus utilisés. Ils se comportent un peu comme les commutateurs, à ceci près qu'ils ne savent faire que de la diffusion. Autrement dit, un concentrateur fonctionne comme suit : si un matériel lui envoie une trame, il diffuse, c'est-à-dire qu'il pollue le sous-réseau. Tous les matériels du sous-réseau reçoivent la trame. Et chaque matériel vérifie si oui ou non la trame le concerne.

4. Routeur et communication entre sous-réseaux

Maintenant que nos matériels informatisés parviennent à communiquer sur un sous-réseau, il convient de pouvoir faire communiquer entre eux des matériels provenant de sous-réseaux distincts. **Un routeur permet entre autre d'assurer la communication entre appareils appartenant à des sous-réseaux, voire des réseaux distincts**. En particulier, une box est en outre un routeur.

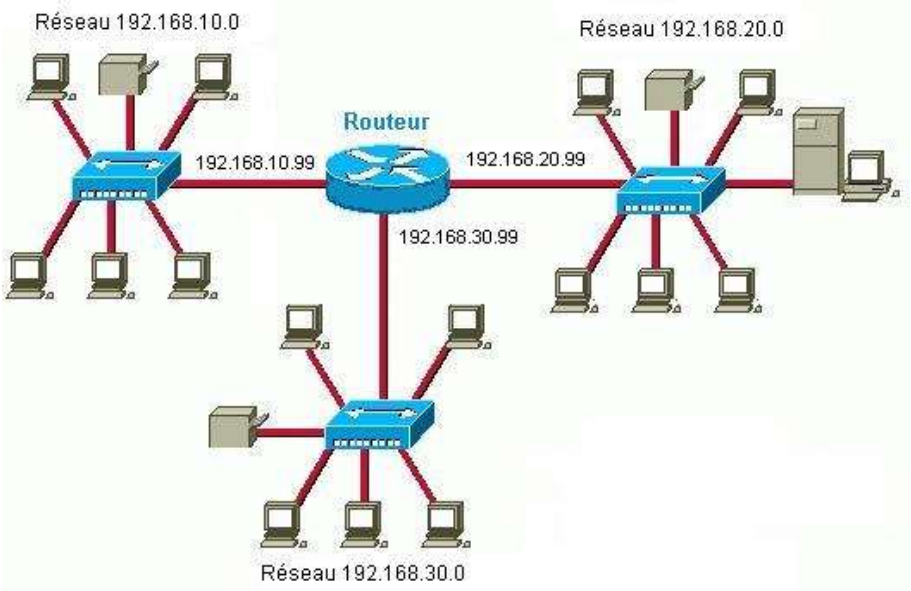
Le routeur assure **le routage** de messages qu'on appelle les **paquets IP** :
o vers l'intérieur du réseau, c'est-à-dire entre sous-réseaux ;

o à destination de l'extérieur, par exemple sur internet, au moyen de divers algorithmes (algorithmes de routage, de contrôle de congestion ou encore de contrôle de flots).

De même qu'un commutateur, un routeur possède en général plusieurs ports. En revanche, **un routeur possède typiquement plusieurs adresses IP**, potentiellement une part port. Chaque port peut être :
o relié à un sous-réseau d'un réseau local ou non ;
o relié à un autre routeur.

Un routeur peut ainsi appartenir à plusieurs sous-réseaux et/ou réseaux locaux et/ou réseaux.

Pour un matériel d'un sous-réseau donné, l'adresse IP, parmi les adresses IP du routeur, rattachée au même sous-réseau que ce matériel, s'appelle l'**adresse IP proxy** ou encore la **passerelle**. **C'est via la passerelle qu'un matériel peut communiquer avec un matériel situé sur un sous-réseau voire un réseau autre que le sien**.



On conclura en faisant remarquer qu'un réseau local est un ensemble de sous-réseaux reliés entre eux par un routeur.

5. Réseau et internet

5.1. Catégories de réseaux

Jusqu'à maintenant, nous n'avons parlé que de réseau local, plus exactement de sous-réseaux, sans se préoccuper du monde extérieur. Or, une société peut très bien être constituée de plusieurs sites, et par conséquent de plusieurs réseaux locaux.

Très vite, un réseau est constitué de plusieurs réseaux, de plusieurs réseaux locaux, de plusieurs sous-réseaux. Et tous ces réseaux doivent potentiellement communiquer entre eux (parfois même outre Atlantique). Ainsi, on distingue plusieurs genres de réseaux :
o les **LAN (*Local Area Network*)** ou réseaux locaux d'entreprise, précédemment évoqués ;
o les **MAN (*Metropol Area Network*)** ou réseaux métropolitains, lesquels interconnectent des LAN via divers procédés logiciels et matériels que nous n'étudierons pas ;
o les **WAN (*Wilde Area Network*)** ou réseaux étendus, lesquels interconnectent des réseaux à l'échelle d'un pays, d'un continent voire de la planète, au moyen de procédés que nous n'étudierons pas non plus ;
o INTERNET, qui est un cas particulier de WAN, que nous étudierons un peu.

5.2. Adresses IP publiques et adresses IP privés

Toute machine connectée à un réseau local (exemple : réseau d'entreprise, réseau domestique…) possède une adresse IP, plus exactement une **adresse IP privée**. On parle d'**adresse IP non routable**, sous-entendu non routable en-dehors du réseau local. En effet, il est impossible de communiquer en-dehors du réseau local (exemple : internet) en utilisant son adresse IP privée, ces fameux couples adresse IP / masque de sous-réseau que nous avons évoqués précédemment.

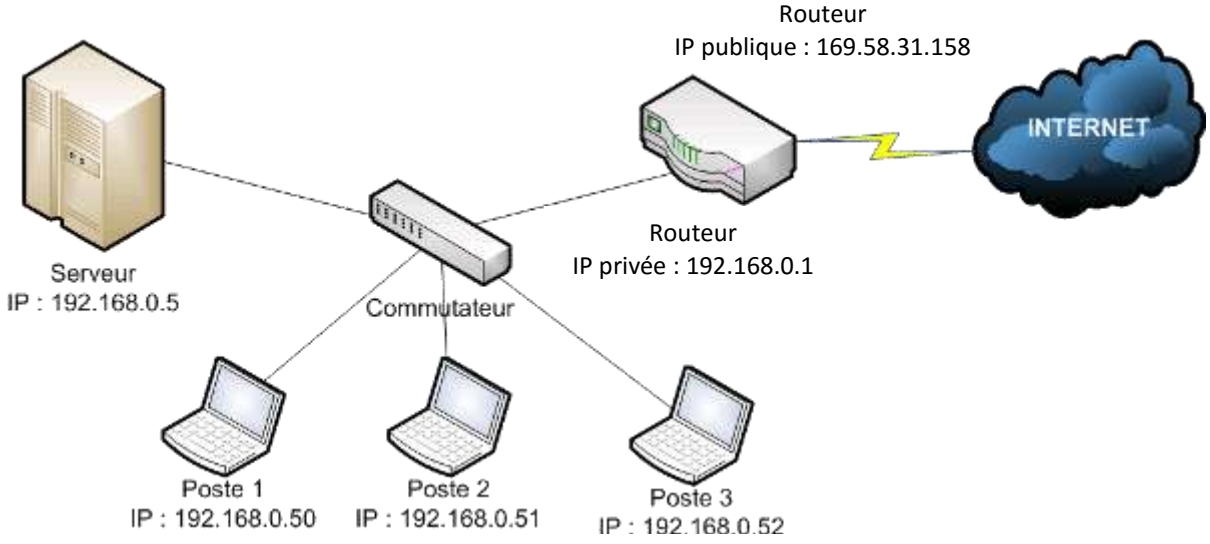
Plus exactement, il existe des plages d'adresses IP privées :
o 192.168.0.0 à 192.168.255.255 (soit 2^{16} adresses) ;
o 172.16.0.0 à 172.31.255.255 (soit 2^{20} adresses) ;
o 10.0.0.0 à 10.255.255.255 (soit 2^{24} adresses).

Les autres adresses IP, à l'exception des adresse de broadcast et quelques autres adresses, sont appelées adresses IP publiques. Il s'agit d'adresses IP routables.

Or, il est bien souvent nécessaire que les matériels de réseaux locaux distincts puissent communiquer entre eux ou encore qu'un matériel puisse communiquer avec un serveur distant possédant une **adresse publique**. Pour ce faire, on utilise **des routeurs NAT**.

5.3. Routeur NAT

Un routeur NAT (*Network Adress Translation*) permet de faire communiquer une machine d'un sous-réseau, et donc ayant une adresse IP privée, avec l'extérieur. Pour ce faire, il utilise des mécanismes dit de traduction d'adresses. L'un des mécanismes communément utilisé est le *port forwarding*, encore appelé l'*NAT masquerade*. En simplifié, le principe du *port forwarding* est le suivant :
o une machine émet un paquet IP à destination de l'extérieur via le routeur. Cet appareil est l'émetteur. Le paquet IP contient entre autre l'adresse IP de l'émetteur ;
o le routeur reçoit le paquet IP ;
o le routeur remplace l'adresse IP de l'émetteur par son adresse IP publique. Il change également une autre information du paquet IP, appelée numéro de port de l'émetteur. Il retient le numéro du port et l'adresse IP associée ;
o le routeur fait suivre le paquet IP sur le réseau extérieur ;
o le routeur reçoit la réponse (un autre paquet IP), incluant le numéro de port qu'il a indiqué. Il est le destinataire du paquet IP reçu. Il retrouve l'adresse IP du vrai destinataire ;
o le routeur remplace l'adresse IP de destination par celle du vrai destinataire ;
o le routeur fait suivre le paquet IP sur le réseau interne.



5.4. DNS

5.4.1. Domaine et sous-domaine

Un nom de domaine est un espace de noms (*name space*) normalisé (norme RFC 1034). Plus simplement, **un nom de domaine est une dénomination attachée à un matériel informatisé possédant au moins une adresse IP publique. A un même matériel informatisé peuvent très bien être attachés plusieurs noms de domaine**. On parle d'espace de noms dans le sens ou un nom de domaine est destiné à permettre, du moins à faciliter l'accès à des ressources nommées d'un matériel informatisé.

Exemples de nom de domaine : com, fr, youtube.com, google.com, wikipedia.fr…

Ces noms de domaine, vous les côtoyez au quotidien en surfant sur internet lorsque vous saisissez des URLs (exemple : http://www.allocine.fr) dans la barre d'adresse de votre navigateur (exemple : Google Chrome).

De fait, quoique l'on ne s'en aperçoive pas nécessairement**, les noms de domaine sont traduits en adresse IP par des appareils appelés serveur DNS (Domain Name System) communiquant entre eux au moyen du protocole DNS**.

Le système de noms de domaine est hiérarchique et on parle de sous-domaine. Par exemple, « youtube.com » est un sous-domaine de « com », « fr.wikipedia.org » est un sous-domaine « wikipedia.org » qui est lui-même un sous-domaine d « org ».

Il importe de bien comprendre que les noms de domaines ne sont pas le propre du web ! Un nom de domaine peut très bien permettre : d'accéder à un serveur sans avoir à en connaître l'adresse IP, de se connecter à un serveur de fichier, de se connecter à un serveur mail… C'est en général les serveurs qui possèdent un ou plusieurs noms de domaine.

5.4.2. URL et URI

Une URL (*Uniform Resource Locator*) est un chemin, basé sur un nom de domaine, lequel permet d'accéder à une ressource. Les URL sont bien entendu normalisées elles-aussi.

Une URL est constituée d'un nom de domaine et, le cas échéant, d'une URI (*Uniform Resource Identifier*) permettant d'identifier la ressource demandée.

Syntaxe simplifiée d'une URL	Exemple
protocole://nom_de_domaine/uri	https://fr.wikipedia.org/wiki/Théorème_de_Taylor **Protocole** : http **Nom de domaine** : fr.wikipedia.org **URI** : /wiki/Théorème_de_Taylor

De multiples protocoles, ont recours aux URL : HTTP, FTP/SFTP, GIT, SVN, WebDav, LDAP…

6. DHCP

DHCP (*Dynamic Host Configuration Protocol*) est un protocole particulièrement utilisé pour l'attribution dynamique d'adresses IP. En effet, dans bien des cas, on ne se préoccupe guère de l'adresse IP du matériel informatique sur le réseau local auquel il est connecté, pourvu qu'il ait une adresse IP ! Dans ce cas, on utilise des adresses IP dynamiques. **Une adresse IP dynamique est une adresse IP qu'un serveur DHCP a attribué à un matériel informatique du réseau local suite à une demande d'adresse IP**.

Dans un réseau domestique, c'est la box qui fait office de serveur DHCP. Et oui, encore et toujours la box !
Une adresse IP dynamique est attribuée pour une durée donnée. On parle de bail. Une fois que le bail a expiré, le matériel informatique effectue une nouvelle demande d'adresse IP.

Cependant, il est tout à fait possible d'attribuer manuellement une adresse IP à un matériel informatique. On parle alors d'**adresse IP manuelle**.

Enfin, il advient qu'il ne soit pas commode que certains matériels changent continuellement d'adresse IP. Prenez une imprimante ! Vous venez de configurer une connexion à une imprimante sur votre ordinateur. Après quelques jours, l'imprimante change d'adresse IP. Ca y est ! Vous êtes obligé de reconfigurer la connexion à l'imprimante.

Pour solutionner le problème, un serveur DHCP est également capable d'allouer des adresses IP statiques. **Une adresse IP statique est une adresse propre à un matériel donnée. Cette adresse IP ne varie pas dans le temps** (exemple d'utilisation : serveurs, imprimantes, badgeuses…). Bien entendu, il est également possible d'utiliser une adresse IP manuelle au lieu d'une adresse IP statique. La différence majeure, c'est que toutes les adresses IP statique peuvent être configurées sur un serveur DHCP tandis que les adresses IP manuelles doivent être configurées sur chaque matériel informatique, ce qui ne facilite pas le travail d'administration réseau.