**03 COURS SERVEUR DHCP ET SERVEUR DNS**

1. **Le serveur DHCP**

Comme vous le savez, l'adresse IP permet d'identifier une machine sur un réseau. Dans le cas d'un réseau IP, cette adresse est indispensable pour pouvoir communiquer avec les autres machines du réseau.

Il existe **deux méthodes pour obtenir une adresse IP** :

* Soit c'est vous qui la configurez (méthode manuelle),
* Soit c'est un serveur qui vous la donne (méthode dynamique).

La méthode manuelle pose quelques problèmes de prime abord.

* Pour qu'une machine puisse communiquer avec ses voisines, son adresse IP devait se trouver dans le même réseau que les autres machines. Pour sortir du réseau local, il faut que notre machine connaisse l'adresse de la passerelle. Cela fait déjà quelques informations dont il faut avoir connaissance quand vous branchez votre ordinateur à un réseau local.
* Autre problème, comment vous assurez-vous que l'adresse IP que vous choisissez n'est pas déjà utilisée par une autre machine sur le réseau ?

On se rend donc bien compte qu'il serait bien d'avoir un mécanisme rapide et fiable pour adresser les machines d'un réseau. C'est là qu'entre en jeu **le protocole DHCP**.

La première fonction d'un serveur DHCP (*Dynamic Host Configuration Protocol*) est de **fournir des adresses IP** (associées à un masque) aux machines en faisant la demande.

Si vous avez configuré votre carte réseau pour récupérer son adresse IP automatiquement, votre machine va chercher à contacter un serveur DHCP susceptible d'être présent sur votre réseau local.

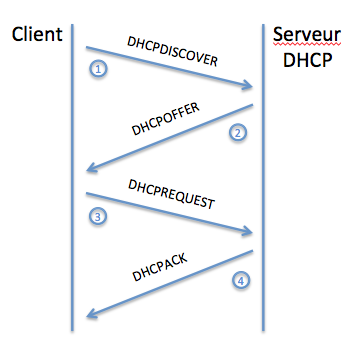
- La trame permettant de trouver un serveur DHCP est une trame "DHCPDISCOVER", comme c'est un broadcast, le serveur DHCP doit obligatoirement se trouver **dans le même réseau** que la machine. Les routeurs (qui délimitent les réseaux) séparent les domaines de broadcast et en général, ne relaient pas.

- Une fois que notre serveur DHCP reçoit le DHCPDISCOVER, il va renvoyer une proposition, c'est un DHCPOFFER. Il va proposer une adresse IP, un masque ainsi qu'une passerelle par défaut et parfois un serveur DNS (étudié dans le prochain paragraphe).

- Le client (votre machine) répond par un DHCPREQUEST. Celui-ci est aussi envoyé en broadcast et sert à prévenir quelle offre est acceptée.

- Le serveur DHCP dont l'offre a été acceptée valide la demande et envoie un DHCPACK qui valide l'allocation du bail.

On parle en effet de "bail", car cette attribution d'adresse IP a une durée limitée. Une fois expiré, il faut redemander une adresse IP.



Toutefois, lors d'un renouvellement, notre machine ne va pas refaire toute la procédure en commençant par un DHCPDISCOVER. On repart directement du DHCPREQUEST. Les serveurs DHCP conservent en mémoire les adresses qu'ils ont distribuées, associées aux adresses MAC. Ainsi, vous constatez que vous conservez parfois très longtemps la même adresse IP, même si votre bail a sûrement été renouvelé plusieurs fois.

1. **Le serveur DNS**

Nous savons, que l’adresse IP permet aux machines de communiquer entre elles.

Cependant, notre cerveau n'est pas fait pour retenir des séries de chiffres comme 104.20.55.240. On aimerait mieux avoir à retenir des noms comme openclassrooms.com.

Le DNS (Domain Name System) est un protocole indispensable au fonctionnement d'Internet, non pas du point de vue technique, mais du point de vue de son utilisation. Il est inconcevable aujourd'hui d'utiliser des adresses IP en lieu et place des noms des sites web pour naviguer sur Internet.

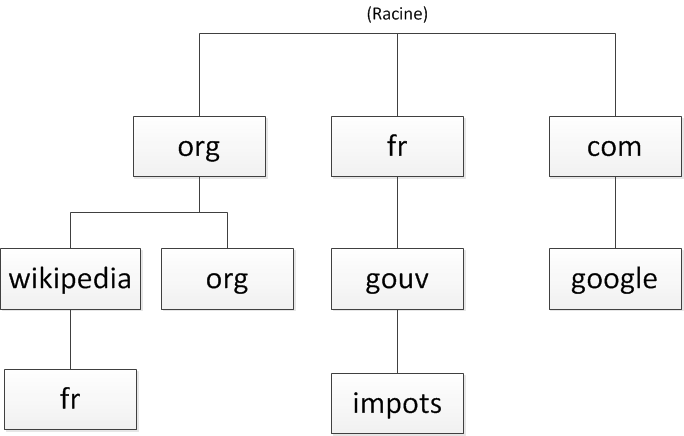
Un nom de domaine se décompose en plusieurs parties. Prenons l'exemple suivant : **www.google.com.** Chaque partie est séparée par un point.

**www.google.com :** En partant de la droite, on trouve d’abord l'extension ; on parle de Top Level Domain (TLD). Il existe des TLD nationaux (fr, it, de, es, etc.) et les TLD génériques (com, org, net, biz, etc.).

**www.google.com** : Il existe une infinité de possibilités pour la deuxième partie. Ici, google est un sous-domaine de com.

**www.google.com** La troisième partie est exactement comme la seconde. On y retrouve généralement le fameux "www". **www** peut soit être un sous-domaine de google.com, mais dans ce cas il pourrait y avoir encore des machines ou des sous-domaines dans ce domaine, soit être directement le nom d'une machine. Ici c’est une machine. On peut bien entendu ajouter autant de troisièmes parties que nécessaire.

Voici une toute petite partie de l'arborescence des noms Internet :



Chaque "partie" est appelée label et l'ensemble des labels constitue un FQDN : Fully Qualified Domain Name. Ce FQDN est unique.

Dans l'architecture du service DNS, chaque label est responsable du niveau directement en dessous et uniquement de celui-ci. La racine est responsable du domaine .com, le .com de google.com et google.com de www.google.com, etc. Bien entendu, Google veut gérer lui-même le domaine google.com. L'organisme qui gère le domaine .com délègue donc la gestion de ce nom de domaine à google.

Ainsi, chaque personne qui veut posséder un domaine sur Internet peut l'acheter, mais devra ensuite gérer un serveur DNS pour publier ses adresses.

Nous savons donc que le DNS est organisé sous forme d'une grosse arborescence, et que chaque partie de l'arborescence peut être gérée par la personne qui la possède.

Mais comment fait-on pour savoir qui possède telle ou telle partie et où sont stockées les informations que l'on recherche ?

Imaginez que vous entrez www.siteduzero.com dans votre navigateur. Lorsque vous entrez ce nom, votre machine doit commencer par le résoudre en une adresse IP.

Vous allez donc demander une résolution au serveur DNS que vous avez reçu par le DHCP.

Celui-ci a deux moyens pour vous fournir la réponse :

* Il connaît lui-même la réponse ;
* Il doit la demander à un autre serveur, car il ne la connaît pas. En effet, chaque serveur DNS étant responsable d'un domaine ou d'un petit nombre de domaines, la résolution consiste à aller chercher la bonne information sur le bon serveur.

Pour obtenir cette résolution, notre serveur va procéder de façon rigoureuse et commencer par là où il a le plus de chance d'obtenir l'information, c'est-à-dire au point de départ de notre arborescence.

Il va demander aux serveurs racine l'adresse IP de www.siteduzero.com. Mais comme les serveurs racine ne sont pas responsables de ce domaine, ils vont le rediriger vers un autre serveur qui peut lui donner une information et qui dépend de la racine, le serveur DNS de com.

Il demande ensuite au serveur DNS de com l'adresse IP de www.siteduzero.com. Mais comme auparavant, le serveur com renvoie l'adresse IP du serveur DNS qui dépend de lui, le serveur DNS de siteduzero.com.

Enfin, il demande au serveur DNS de siteduzero.com l'adresse IP de www.siteduzero.com et là, ça marche : le serveur de siteduzero.com connaît l'adresse IP correspondante et peut la renvoyer.

On dit qu'un serveur fournissant la résolution d'un nom de domaine sans avoir eu à demander l'information à quelqu'un d'autre fait **autorité**.

Les serveurs DNS utilisent un système de **cache** pour ne pas avoir à redemander une information de façon répétitive, mais ils ne font pas autorité pour autant, car l'information stockée en cache peut ne plus être valide après un certain temps.

Le DNS sait faire la résolution inverse, c’est-à-dire retrouver le nom associé à l’IP.

Cependant, c'est relativement peu utilisé, sauf parfois pour des raisons de sécurité.

*La gestion internationale des noms de domaine*

Même si le système DNS n'est pas indispensable au fonctionnement d'Internet, il en est un élément incontournable.

Le système de noms de domaine est géré par un organisme américain appelé l'ICANN. Il est responsable de la gestion des 13 serveurs racine du DNS. Ces 13 serveurs connaissent les adresses IP des serveurs DNS gérant les TLD (les .fr, .com; org, etc.)

En fait, après plusieurs attaques sur les serveurs racine, on a mis en place un système qui duplique les 13 serveurs en différents endroits d'Internet, sur plus de 1000 serveurs.

C'est l'ICANN qui autorise la création d'une nouvelle extension, comme le .post en 2012 ou l'utilisation de caractères non-latins (arabes, chinois, japonais, etc.), il y a quelques années.

L'ICANN délègue ensuite les domaines TLD à divers organismes. Pour l'Europe, c'est le RIPE qui délègue lui-même à l'AFNIC la responsabilité du domaine .fr (ainsi que des extensions correspondantes à la France d'outre-mer) ; pour le domaine .com, c'est VeriSign qui s'en occupe. Les labels inférieurs correspondent généralement à des sites ou à des entreprises, et la gestion du nom de domaine leur revient.