DHCP & DNS

Préambule

Ce cours vous présente deux des services essentiels du protocole IP à savoir : DHCP et DNS. Cette section aborde le principe de fonctionnement de ces deux applications.

L'automatisation de configuration IP

Lorsque le réseau TCP/IP est constitué d'un grand nombre de machines, la gestion des adresses IP devient quelque peu complexe.

BOOTP

Bootstrap Protocol est un protocole réseau d'amorçage, qui permet à une machine cliente sans disque dur de découvrir sa propre adresse IP, l'adresse d'un hôte serveur, et le nom d'un fichier à charger en mémoire pour exécution. On peut représenter l'amorçage comme une opération se produisant en deux phases :

- Détermination d'adresses et sélection du fichier de démarrage, c'est ici qu'intervient BOOTP
- Transfert du fichier de démarrage, le transfert utilisera typiquement le protocole TFTP.

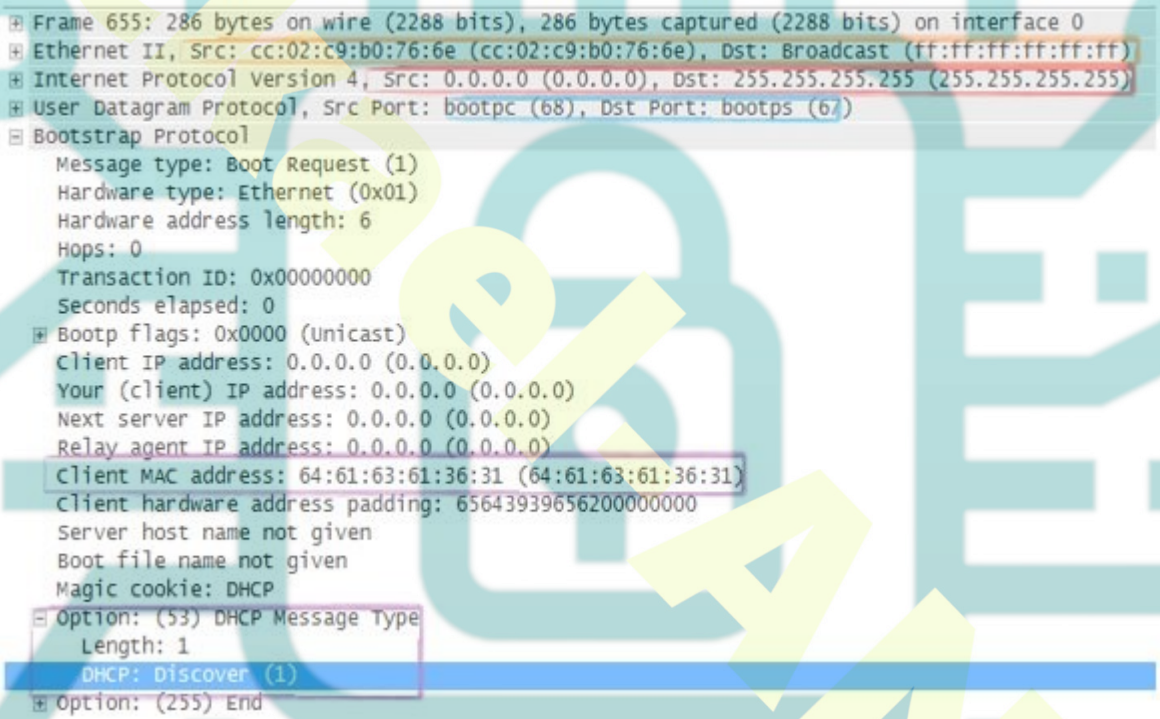
DHCP

Il a été créé au départ comme complément au protocole BOOTP (Bootstrap Protocol) utilisé par certains matériels.

Lors de la configuration du serveur DHCP, il faut indiquer les plages d'adresses qui seront distribuées par le serveur DHCP. En plus de l'adresse IP, le serveur DHCP peut distribuer d'autres paramètres IP tel que : la passerelle, le serveur DNS, le nom de domaine…

Fonctionnement

- Qaund une machine est démarrée, elle n'a aucune information sur sa configuration réseau. Elle envoie alors un broadcast IP associé au message **DHCPDISCOVER** afin de localiser les serveurs DHCP disponibles.
- Le ou les serveurs présents répondent par une diffusion IP associée au message **DHCPOFFER** (qui contient une offre de configuration et l'identification du serveur)
- Le client répond un **DHCPREQUEST** qui indique l'acceptation de l'adresse et l'identification du serveur choisi.
- Le serveur choisi répond alors un **DHCPACK** pour finaliser la transaction.



Message DHCP discover

D'autres questions et réponses sont utilisées par DHCP en fonction des événements :
DHCPNAK (réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau)
DHCPRELEASE (le client libère son adresse IP)

Pour des raisons d'optimisation des ressources réseau, les adresses IP sont délivrées avec une date de début et une date de fin de validité. C'est ce qu'on appelle un "**BAIL**".

Un client qui voit son bail arriver à terme peut demander au serveur une prolongation du bail par un DHCPREQUEST.

De même, lorsque le serveur verra un bail arriver à terme, il émettra un paquet DHCPNAK pour demander au client s'il veut prolonger son bail. Si le serveur ne reçoit pas de réponse valide, il rend de nouveau disponible l'adresse IP.

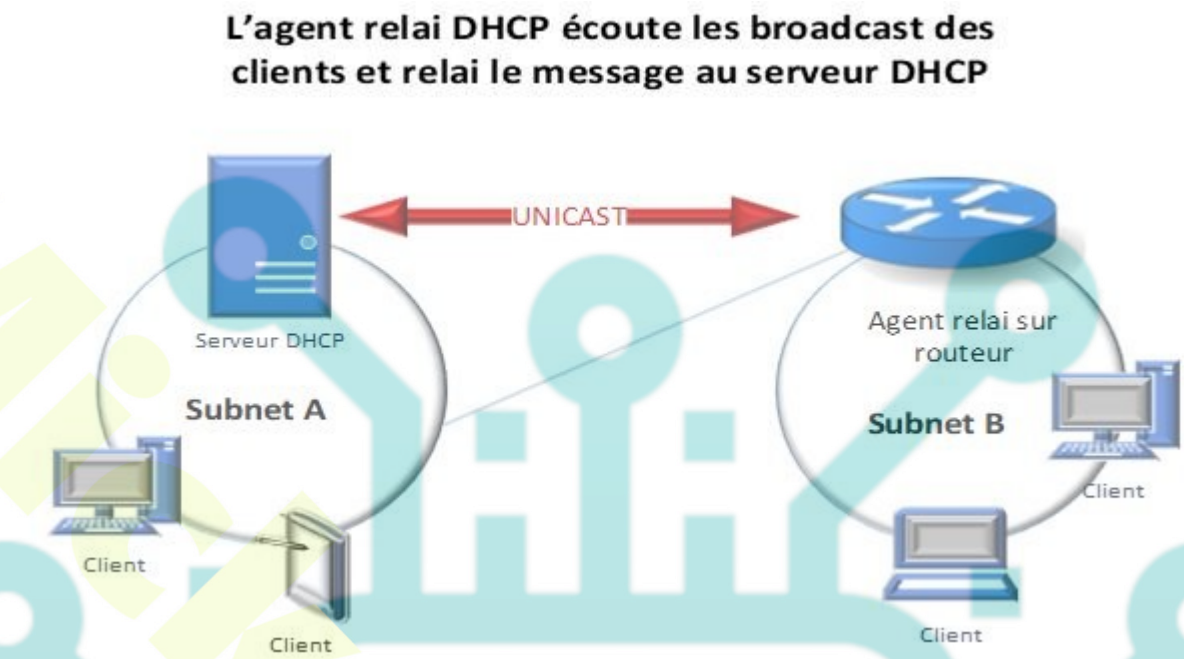
C'est toute la subtilité du DHCP par rapport à BOOTP : on peut optimiser l'attribution des adresses IP en jouant sur la durée des baux.

Messages DHCP v4

Message	Utilisation
DHCPDISCOVER	Diffusion du client pour localiser les serveurs disponibles
DHCPOFFER	Du serveur au client pour répondre au DHCPDISCOVER avec les paramètres de configuration.
DHCPREQUEST	Message client aux serveurs soit (a) qui demande les paramètres à un serveur et décline implicitement les offres de tous les autres, (b) qui confirme la validité des adresses précédemment allouées, par ex : un redémarrage système, ou (c) qui étend le bail sur une adresse réseau en particulier.
DHCPACK	Du serveur au client avec les paramètres de configuration et qui inclut l'adresse réseau déjà attribuée.
DHCPNAK	Du serveur vers le client indiquant que l'adresse d'un client est incorrecte. (par ex : si un client est déplacé sur un nouveau sous réseau) ou que le bail du client a expiré.
DHCPDECLINE	Client vers serveur indiquant que l'adresse réseau est déjà utilisée.
DHCPRELEASE	Client vers serveur libérant l'adresse réseau et annulant le bail.
DHCPINFORM	Client vers serveur, demandant seulement les paramètres de configuration locaux ; le client possède déjà une adresse réseau attribuée de manière externe.

Agent relais

Le service DHCP travaille en diffusion, ce qui implique que les messages DHCP ne passent pas les routeurs. Dans ce cas, il faut utiliser un AGENT RELAI sur les segments réseau qui ne possèdent pas de serveur DHCP (les routeurs fournissent cette option)



A ce moment-là, l'agent relai va se comporter comme un sous-traitant du serveur DHCP. Il va capturer la requête diffusée du client et la transmettre en unicast au serveur.
Le serveur reconnaît l'agent relai (information inclue dans le message DHCP) et transmet la réponse en unicast à l'agent qui lui, la rediffuse au client.

```
⊞ Frame 410: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits)
⊟ Ethernet II, Src: Cisco_43:d8:63 (00:0b:85:43:d8:63), Dst: All-HSRP-routers_02 (00:00:0c:07:ac:02)
  ⊞ Destination: All-HSRP-routers_02 (00:00:0c:07:ac:02)
  ⊞ Source: Cisco_43:d8:63 (00:0b:85:43:d8:63)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 10.10.14.10 (10.10.14.10), Dst: 192.168.200.1 (192.168.200.1)
⊟ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
    Source port: bootps (67)
    Destination port: bootps (67)
    Length: 312
  ⊞ Checksum: 0xd734 [validation disabled]
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x15f9ffb7
  ⊞ Seconds elapsed: 4
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.14.10 (10.10.14.10)
    Client MAC address: IntelCor_35:c2:f0 (a0:88:b4:35:c2:f0)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=12,l=7) Host Name = "8DWP2Q1"
  ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊞ Option: (t=55,l=12) Parameter Request List
```

Message agent relais

Gestions des noms sur IP

Le fichier HOSTS

le fichier host stocke les noms d'hôtes et les adresses IP correspondantes. C'est lui qui est interrogé en premier avant une requête DNS sur les serveurs d'adresse du Web. Ainsi, le fichier host convertit les noms d'hôtes en adresses IP.

Le fichier hosts est situé dans **/etc** sur linux et **c:\windows\system32\drivers**etc sur Windows

Exemple de fichiers HOSTS

```
102.54.94.97 www.google.fr # server Google
38.25.63.10 www.yahoo.fr # server Yahoo
127.0.0.1 localhost #adresse de bouclage
::1 localhost #adresse de bouclage IPv6
```

Le problème avec les fichiers statiques, c'est que dès qu'il y a une modification, il y a nécessité de mise à jour manuelle sur tous les fichiers de tous les ordinateurs. Ainsi, avec l'explosion de la taille des réseaux et de leur interconnexion, il a fallu mettre en place un système de gestion de noms hiérarchisé et plus facilement administrable.

Système DNS

Le DNS propose en quelque sorte les mêmes services qu'un annuaire téléphonique, car il associe un nom à une adresse IP comme un annuaire qui associe un nom à un numéro de téléphone. Comme une personne peut avoir plusieurs numéros de téléphone associés à son nom, un nom DNS peut également avoir plusieurs adresses IP associées.

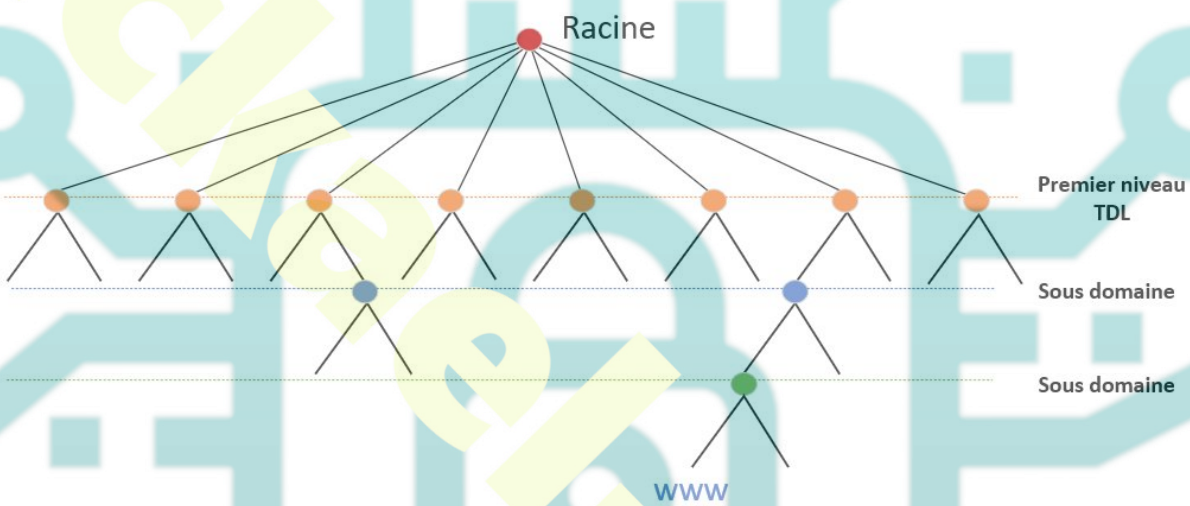
Le système nommé Domain Name System (DNS) mis au point en 1983 est un **annuaire** qui propose :

- Un espace de noms hiérarchique permettant de garantir l'unicité d'un nom dans une structure arborescente.
- Un système de serveurs distribués permettant de rendre disponible l'espace de noms.
- Un système client permettant d'interroger les serveurs afin de connaître l'adresse IP correspondant à un nom.

Le protocole DNS utilise le port UDP 53 lors des requêtes interrogatives et le port TCP 53 lors des transferts de zones.

L'espace de noms

La structure du système DNS s'appuie sur une arborescence dans laquelle sont définis des domaines de premier niveau, rattachés à un nœud racine représenté par un point.



Arborescence DNS

L'ensemble des noms de domaine constitue ainsi un arbre inversé où chaque nœud est séparé du suivant par un point (« . »)

L'extrémité d'une branche est appelée hôte, et correspond à une machine ou une entité du réseau. Le mot domaine correspond au suffixe d'un nom de domaine, à l'exception de l'hôte (www par exemple).

Le nom complet **FQDN** correspond au nom de l'hôte associé au nom de domaine (www.microsoft.com)

Domaine de premier niveau

Domaine spécial
ARPA
Domaine générique non restreint

COM, NET, ORG, INFO

Domaine générique restreint

Un domaine générique restreint est un domaine qui propose des règles aux utilisateurs qui veulent obtenir un sous-domaine dans ce domaine.

BIZ, NAME, PRO

Domaine commandité restreint

Domaine qui confirme le domaine d'activités de l'organisation qui le possède.

GOV – MIL – INT – COOP – MUSEUM – AERO – JOBS – TRAVEL – CAT – MOBI – TEL -ASIA

Domaine national

FR, UK, EU …

Les serveurs de noms

Ils permettent d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau pour un domaine ou plusieurs domaines particuliers.

Chaque domaine possède un serveur de noms de domaine appelé (serveur de nom primaire ou principal), ainsi qu'un serveur de noms secondaire permettant de prendre le relai du serveur primaire en cas d'indisponibilité, de servir de cache ou pour l'équilibrage de charge.

Un serveur correspondant au domaine de plus haut niveau est appelé « serveurs racine ».
Il en existe treize, répartis sur la planète, possédant les noms « a.root-servers.net » jusqu'à « m.root-servers.net ».

Un serveur de noms définit une zone, c'est-à-dire un ensemble de domaines sur lequel il a autorité.

Résolution de nom de domaine

Lorsqu'un client souhaite résoudre un FQDN en adresse IP, une requête est envoyée au premier serveur de noms (appelé « serveur de noms primaire »)
1. Si celui-ci possède l'enregistrement dans son cache, il l'envoie à l'application, dans le cas contraire il interroge un serveur racine.
2. Le serveur de noms racine renvoie une liste de serveurs de noms faisant autorité sur le domaine.

3. Le serveur de noms faisant autorité sur le domaine va alors être interrogé et retourner l'enregistrement correspondant à l'hôte sur le domaine.

https://www.youtube.com/watch?v=cHtQ2O-Di5c

Démo résolution DNS

Type de requêtes

Lorsque la requête est **récursive**, le serveur de noms prend en charge le mécanisme de résolution intégrale en émettant éventuellement lui-même des requêtes vers d'autres serveurs de noms (redirecteur)

Dans le cas d'une requête **itérative**, lorsque le serveur de noms ne gère pas lui-même l'adresse IP demandée, il retourne au résolveur la meilleure réponse qu'il a du serveur de noms le plus proche qui pourrait résoudre la requête.
Le résolveur doit alors à nouveau émettre une demande vers le nouveau serveur de noms qui a été référencé.

Le résolveur procède ainsi de proche en proche de manière itérative afin d'arriver à résoudre le nom du site.
Le client lui, essaye toujours la récursivité.

Types d'enregistrement

Un DNS est une base de données répartie contenant des enregistrements concernant les noms de domaines. Seules sont concernées par la lecture des informations ci-dessous les personnes responsables de l'administration d'un domaine, le fonctionnement des serveurs de noms étant totalement transparent pour les utilisateurs.

Enregistrement	Description
Nom de domaine	Le nom de domaine doit être un nom FQDN
Type A	Établit la correspondance entre un nom canonique et une adresse IP.
Cname	Il permet de faire correspondre un alias au nom canonique
HINFO	Décrit le matériel (CPU) et le système d'exploitation (OS) d'un hôte
MX	Correspond au serveur de gestion du courrier
NS	Correspond au serveur de noms ayant autorité sur le domaine
PTR	Sorte de pointeur vers la zone de recherche inverse Ex. j'ai le nom et je cherche l'adresse IP Utilisé par NSLOOKUP
SOA	Décrit le serveur de nom ayant autorité sur la zone

En raison du système de cache permettant au système DNS d'être réparti, les enregistrements de chaque domaine possèdent une durée de vie, appelée TTL (Time To Live) Elle permet aux serveurs intermédiaires de connaître la date de péremption des informations et ainsi savoir s'il est nécessaire ou non de les vérifier.

Les domaines

Un domaine est un endroit où l'on associe un nom à une adresse IP.

Un domaine représente l'ensemble d'une sous-arborescence à partir d'un nœud donné. Chaque nœud de l'arbre de nommage est un domaine. En dehors de la racine, chaque domaine peut-être considéré comme un sous-domaine pouvant lui-même contenir des sous-domaines.

Les Zones

Pour gérer un domaine DNS, il faut avoir une zone contenant un ou plusieurs domaines.

Une zone DNS est :
soit une zone de recherche directe ou inversée.
soit une zone principale, secondaire ou de stub.

Domaine VS ZONE

Un domaine représente l'ensemble des noms ayant un même suffixe. Une zone représente l'ensemble des noms ayant un même suffixe pour lesquels il n'existe qu'un seul serveur de nom.

Comprendre la différence entre une zone et un domaine est parfois déroutant. Une zone est simplement une portion d'un domaine. Par exemple, le domaine Microsoft.com peut contenir toutes les données de Microsoft.com, Marketing.microsoft.com. Cependant, la zone Microsoft.com contient uniquement des informations pour Microsoft.com et des références aux serveurs de noms faisant autorité pour les sous-domaines.

S'il n'y a pas de sous-domaines, la zone et le domaine sont essentiellement les mêmes. Dans ce cas, la zone contient toutes les données du domaine.

Zone de recherche directe

Une recherche directe est un processus d'interrogation qui recherche le nom affiché du domaine DNS d'un ordinateur hôte pour trouver son adresse IP (enregistrements de ressources de type A).

Zone de recherche inversée

Une recherche inversée est un processus d'interrogation qui recherche l'adresse IP d'un ordinateur hôte pour trouver son nom DNS (s'appuie sur le nom de domaine **in-addr.arpa** et contiennent des enregistrements de ressources de type PTR).

> Une zone peut contenir un ou plusieurs domaine.
> Une zone peut être déléguée.

Une zone principal

C'est une zone sur laquelle on a pleinement autorité (lecture/écriture) **Cette zone peut être directe ou inversée.**
Une zone directe permet de trouver une adresse IP lorsque l'on demande un nom, une zone inversée permet d'obtenir le nom lorsque l'on a l'adresse IP.

Comme le système DNS est comparable à un annuaire, une zone principale est l'annuaire classique, une zone inversée est un annuaire inversé.

Une zone secondaire

C'est une zone sur laquelle on n'a pas pleinement autorité (lecture seule) Elle est utilisée pour les serveurs DNS dit secondaires. L'objectif de l'utilisation de zone secondaire est d'équilibrage de charge et la tolérance aux pannes.

Une zone de STUB

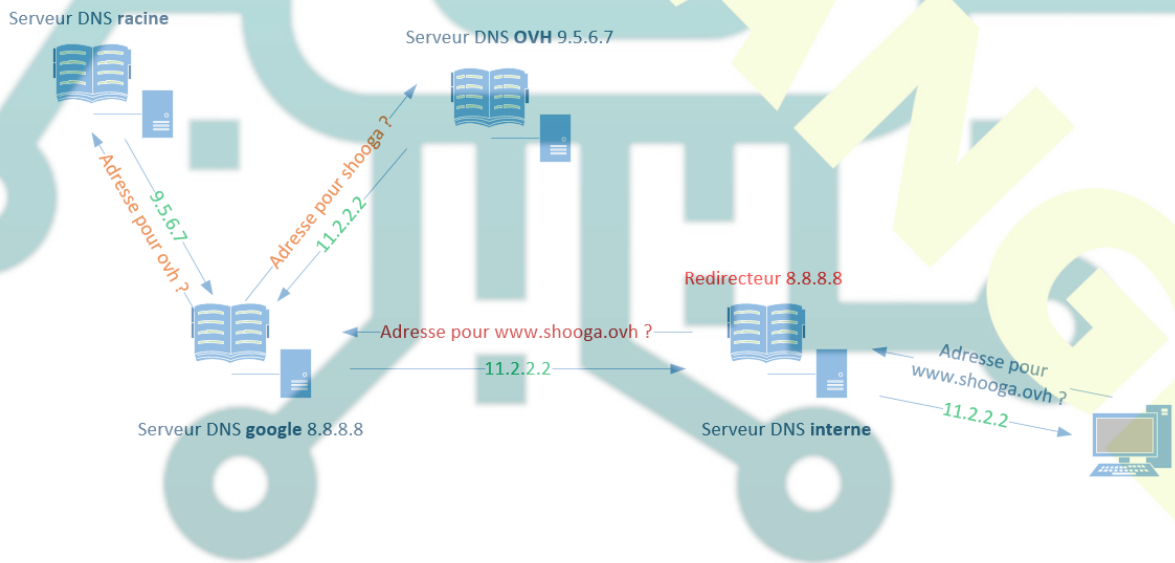
Ce sont des copies d'une zone qui contiennent uniquement les enregistrements de ressources nécessaires à l'identification du serveur DNS faisant autorité pour la zone en question. Une zone de stub contient un sous ensemble des données de la zone qui se compose d'un enregistrement **SOA**, **NS** et **A**.

Redirecteurs

Redirecteur global

Un redirecteur est un serveur DNS (Domain Name System) sur un réseau qui transfère des requêtes DNS pour des noms DNS externes vers des serveurs DNS situés à l'extérieur de ce réseau et cela évite de contacter les serveurs racines.

NB. Les requêtes via un redirecteur sont de types récursives.



Requête DNS avec redirecteur global

Redirecteurs conditionnels

Un redirecteur conditionnel est un serveur DNS sur un réseau qui transfère des requêtes DNS en fonction du nom de domaine DNS mentionné dans la requête.
Par exemple, vous pouvez configurer un serveur DNS de façon à transférer toutes les requêtes qu'il reçoit pour des noms se terminant par sud.societe.com à l'adresse IP d'un serveur DNS spécifique ou aux adresses IP de plusieurs serveurs DNS.

Délégation de zones

Pour des grands domaines, il peut être utile de mettre en place plusieurs serveurs serveurs DNS, chacun gérant sa zone correspondant à son sous-domaine.

Le fonctionnement du DNS est basé sur une **architecture hiérarchique avec une structure en arborescence**. La résolution de nom s'appuie donc sur une base de données distribuée, chaque nœud de l'arbre de nommage ayant autorité sur une zone donnée.
Le serveur faisant autorité sur une zone délègue en général la gestion des sous-domaines créés dans son domaine à d'autres serveurs de nom. On obtient ainsi une hiérarchie de zones dites parentes et de zones dites déléguées.

Exemple

Le serveur de domaine **cola** délègue la gestion de la zone **coca** au serveur1 et la gestion de la zone **pepsi** au serveur2.
Dans le monde internet, les zones sont déléguées selon le schéma de l'arborescence DNS vu plus haut. Les serveurs racines délèguent aux serveurs de premier niveau qui délèguent à leur tour la gestion de domaine d'entreprise à d'autres serveurs.

Le DNS Dynamique

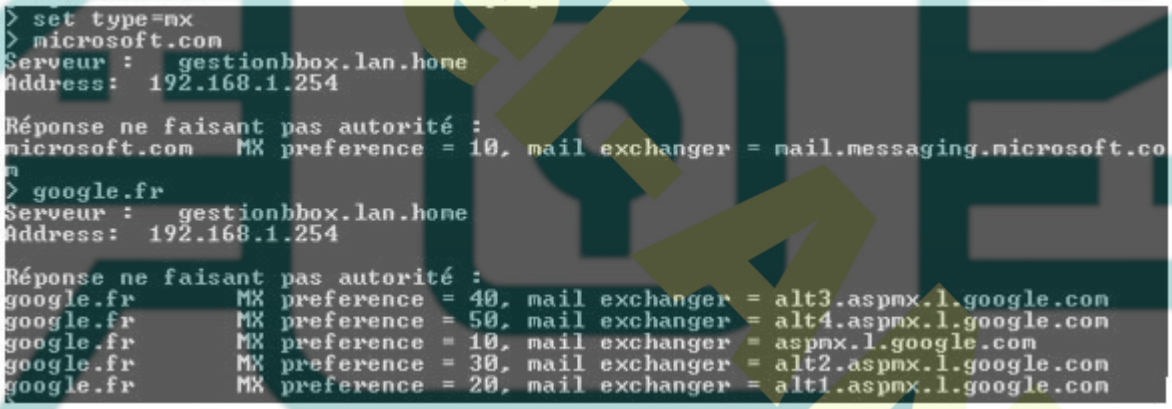
Il existe une nouvelle implantation du DNS qui prend en charge les enregistrements de façon dynamique. Auparavant, le serveur DNS était statique et toute nouvelle entrée dans la base devait se faire manuellement.
Aujourd'hui, les machines peuvent s'inscrire d'elles-mêmes dans le domaine DNS.

Commande nslookup

Cet outil (Windows, Linux) permet l'envoie des requêtes DNS sur un serveur afin de récupérer des informations d'enregistrement.

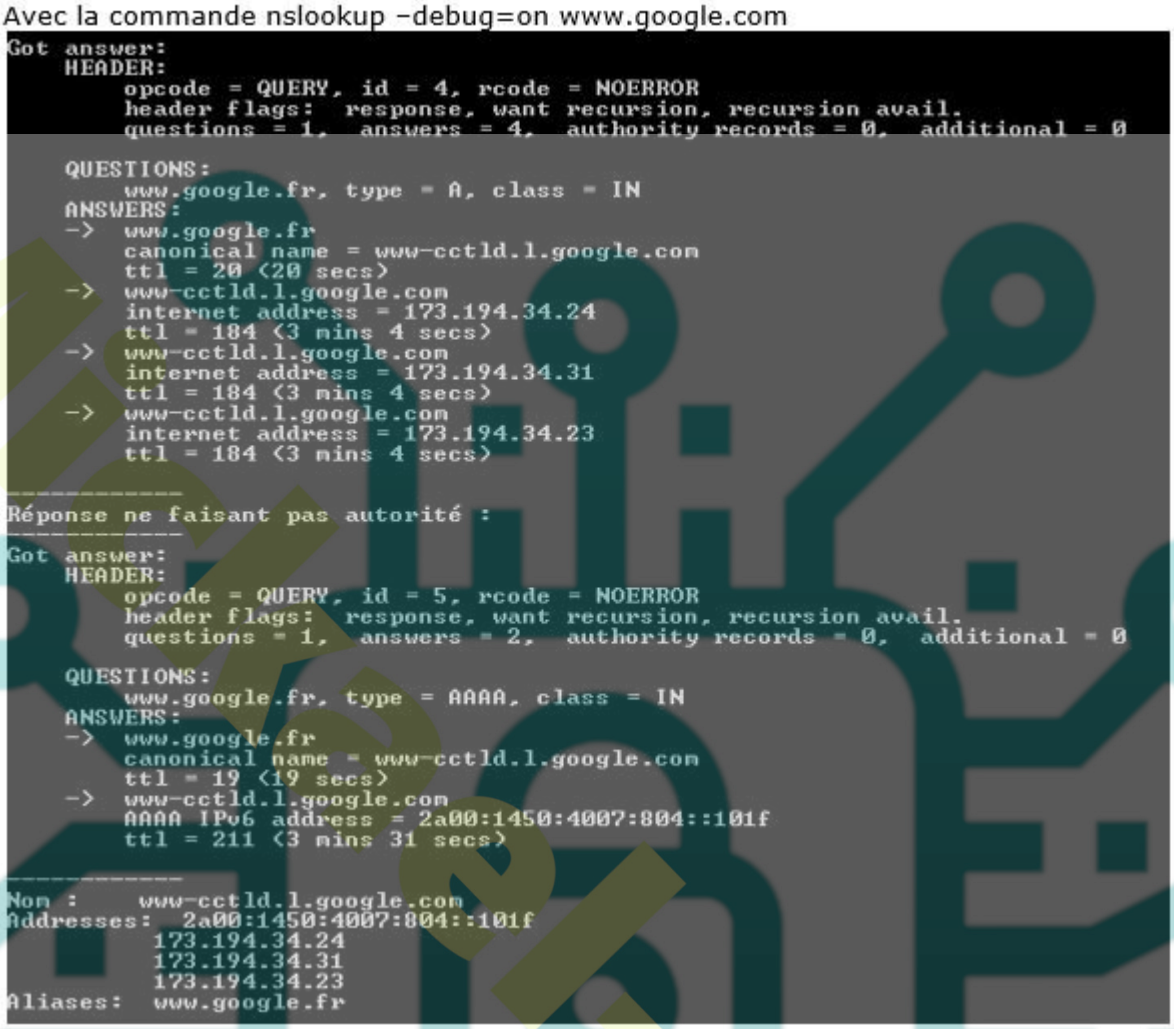
Exemple d'utilisation

Une fois l'outil nslookup démarré, choisir le type de pointage à interroger avec la commande "set type="
Par exemple, pour visualiser un pointage de type mail, inscrire "set type=mx" puis valider.
Indiquer ensuite le domaine à interroger avec la commande microsoft.com par exemple.



A Adresse IPv4
AAAA Adresse IPv6
MX Nom(s) de domaine du serveur de messagerie (Mail Exchanger)
NS Serveur de nom de domaine
PTR Requête « Pointer » (affiche le(s) nom(s) d'hôte sur une adresse IP)
SOA Requête « Start of Authority » (informations sur la gestion de la zone DNS)

Avec la commande nslookup -debug=on www.google.com



La commande DIG (Linux)

Cet outil **dig** (de l'anglais *domain information groper*) est un client en ligne de commandes sous Linux, permettant d'interroger des serveurs DNS. Il est disponible dans le package dnsutils.

Voir les informations d'un domaine

$ dig google.com any

Voir les mx d'un domaine

dig mx google.com +short

Traceroute dig

dig system-linux.eu +trace

Voir les noms des serveurs qui gèrent le domaine google.com

dig NS google.com +short

https://viewdns.info/

Informations sur les domaines