Service de résolution de noms de domaine

DNS - Domain Name Services

GUINKO Tonguim Ferdinand

IBAM, Université Joseph KI-ZERBO

24 mai 2022

Matériel ayant servi à la conception de ce cours

- http://www.linux-france.org/prj/edu/archinet/systeme/ch30.html
- https://fr.wikipedia.org/wiki/Domain_Name_System
- https://www.ionos.fr/digitalguide/serveur/know-how/resolution-de-noms-quest-ce-quun-serveur-dns/
- https://www.commentcamarche.net/contents/518-dns-systeme-de-noms-de-domaine
- http://mariepascal.delamare.free.fr/IMG/pdf/1_2_CoursDns-2.pdf
- https://cisco.goffinet.org/ccna/services-infrastructure/protocole-resolution-noms-dns/

Sommaire

Domain name service : définition

Pour pouvoir communiquer, chaque machine présente sur un réseau doit avoir un identifiant unique. Avec le protocole IP (Internet Protocole), cet identifiant se présente sous la forme d'un nombre d'une longueur de 32 bits. On parle d'adresses IP. Une adresse IP permet d'identifier une machine sur le réseau.
En IPv4, elles sont représentées sous la forme « - - - . - - - . - - - . - - - », où chaque « groupe » de trois tirets est substituable par un nombre entre 0 et 255 en représentation décimale.
En IPv6, les adresses sont représentées sous la forme « .... : .... : .... : .... : .... : .... : .... : .... », où chaque « groupe » de quatre points est substituable par une valeur hexadécimale de 0000 à FFFF.

Domain name service : définition (2)

Cependant pour un utilisateur, il est difficile de retenir les adresses IP de chaque ordinateur.
Le service de résolution de noms d'hôtes DNS (Domain Name Services), permet d'adresser un hôte par un nom, plutôt que de l'adresser par une adresse IP. C'est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP. C'est pourquoi des mécanismes de résolution de noms ont été mis en place. Un mécanisme de résolution de noms permet de traduire des noms en adresses IP etinversement. Il permet d'établir une corrélation entre des adresses IP et le nom de domaine associé.

Structure d'un nom d'hôte

Nom_d_hôte ou Nom_d_hôte.NomDomaine
Exemple : ns1 ou ns1.foo.org

Domain name service : définition (3)

Le nom de domaine identifie une organisation dans l'internet, comme, par exemple, yahoo.com,ujkz.bf, eu.org. Dans les exemples, nous utiliserons un domaine que l'on considère fictif : «foo.org». Chaque organisation dispose d'un ou plusieurs réseaux. Ces réseaux sont composés de noeuds, ces noeuds (postes, serveurs, routeurs, imprimantes) pouvant être adressés.
Le DNS a les mêmes objectifs qu'un service de renseignement téléphonique. Il met à disposition tous les contacts et les publie sur demande. Pour cela, le système a recours à un réseau international de serveurs DNS qui subdivisent les espaces des noms de domaine de manière indépendante dans des zones administrées. Cela permet une manipulation décentralisée d'informations de noms de domaine.

Domain name service : définition (4)

Chaque fois qu'un internaute enregistre un nom de domaine, une nouvelle entrée est indiquée dans le répertoire compétent. Celui-ci prend la forme d'un enregistrement de ressource (RR pour Resource Record) dans le DNS. La base de données d'un serveur DNS correspond ainsi à une collection de tous les enregistrements de ressources d'une zone d'espace de noms de domaine pour lequel le serveur est responsable.

Domain name service : définition (5)

Quelle différence entre la résolution de noms d'hôtes avec un serveur DNS et les fichiers hosts ?

Avec les fichiers hosts, chaque machine dispose de sa propre base de données de noms. Sur des réseaux importants, cette base de données dupliquée n'est pas simple à maintenir.

Avec un service de résolution de noms, la base de données est localisée sur un serveur. Un client qui désire adresser un hôte regarde dans son cache local, s'il en connaît l'adresse. S'il ne la connaît pas il va interroger le serveur de noms.

Tous les grands réseaux sous TCP/IP, et internet fonctionnent schématiquement sur ce principe.

Domain name service : définition (6)

Avec un serveur DNS, un administrateur n'a plus qu'une seule base de données à maintenir. Il suffit qu'il indique sur chaque hôte, quelle est l'adresse de ce serveur. Ici il y a 2 cas de figures possibles :

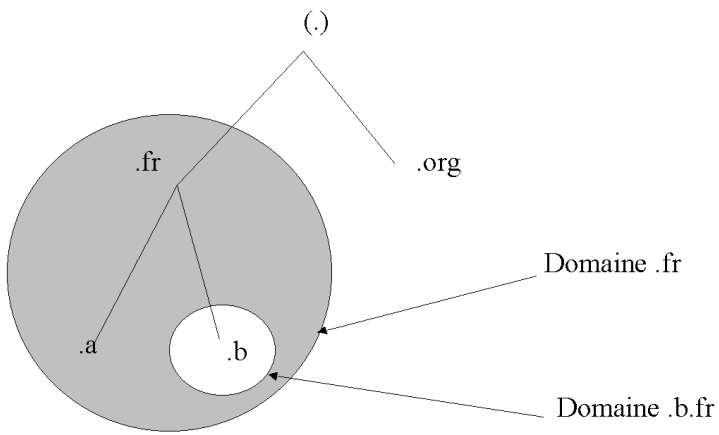
- soit les hôtes (clients) sont des clients DHCP (Dynamic Host Configuration Protocol), cette solution est particulière et n'est pas abordée dans le cadre de ce cours ;
- soit les clients disposent d'une adresse IP statique. La configuration des clients est détaillée dans le cadre de cours.

Domaine : définition

Un domaine est un sous-arbre de l'espace de nommage. Par exemple .COM est un domaine, il contient toute la partie hiérarchique inférieure de l'arbre sous jacente au noeud .COM.
Un domaine peut être organisé en sous domaines. Par exemple .PIRLOUIT.COM est un sous domaine du domaine .COM. Un domaine peut être assimilé à une partie ou sous-partie de l'organisation de l'espace de nommage. Voir la diapositive sur les Domaines, zones et délégations.
Chaque noeud de l'arbre possède une étiquette, *label* en anglais, d'une longueur maximale de 63 caractères.
L'ensemble des noms de domaine constitue ainsi un arbre inversé où chaque noeud est séparé du suivant par un point «.».

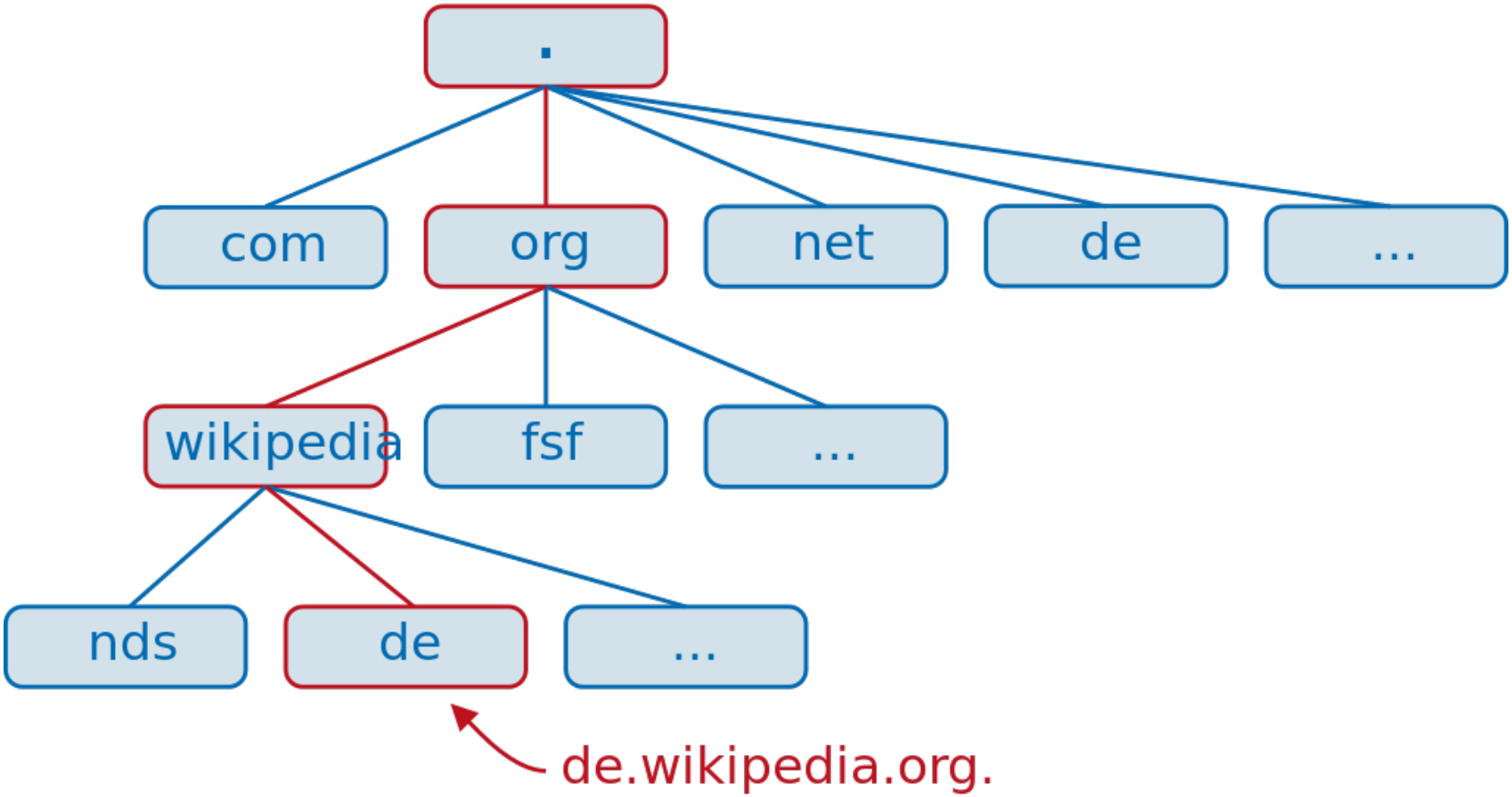
Domaine : définition (2)

L'extrémité d'une branche est appelée hôte, et correspond à une machine ou une entité du réseau. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré, ou le cas échéant dans le sous-domaine. A titre d'exemple le serveur web d'un domaine porte ainsi généralement le nom www.



Un domaine est un sous arbre de l'espace de nommage.

Domaine : illustration



Domaine : récursivité DNS

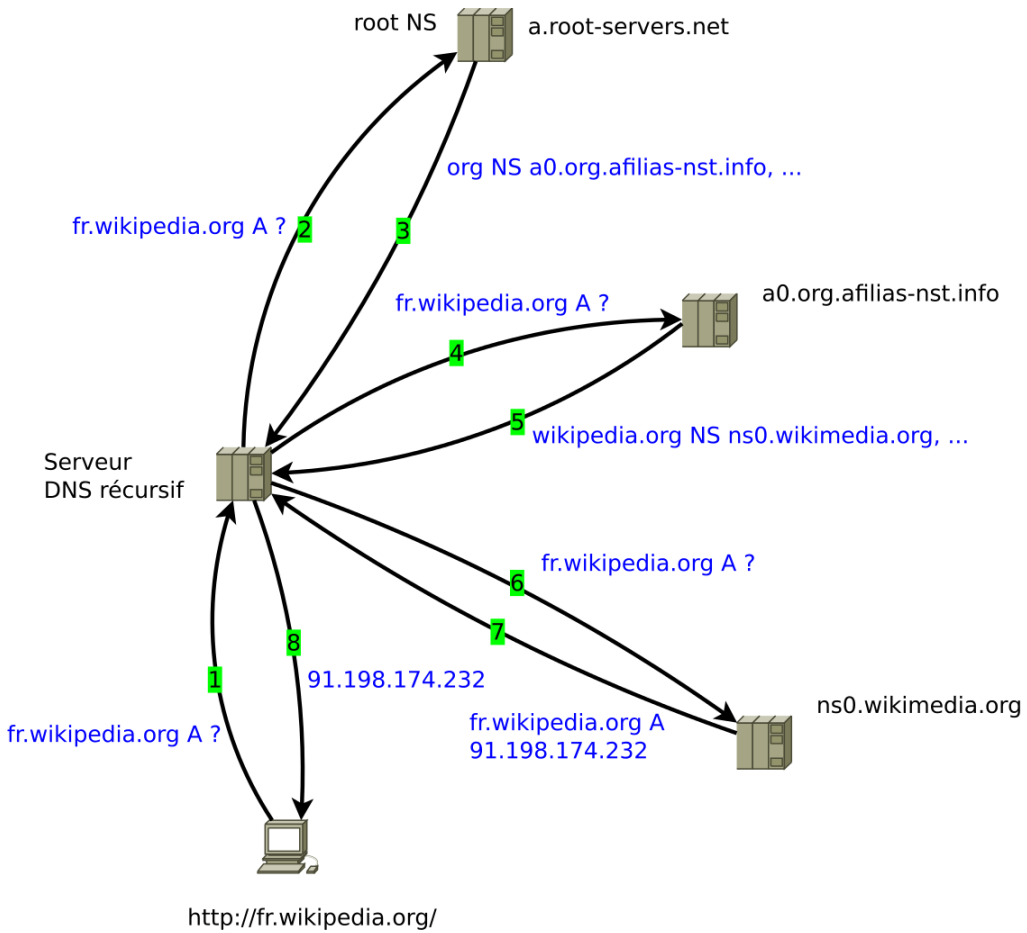


FIGURE – Récursivité DNS

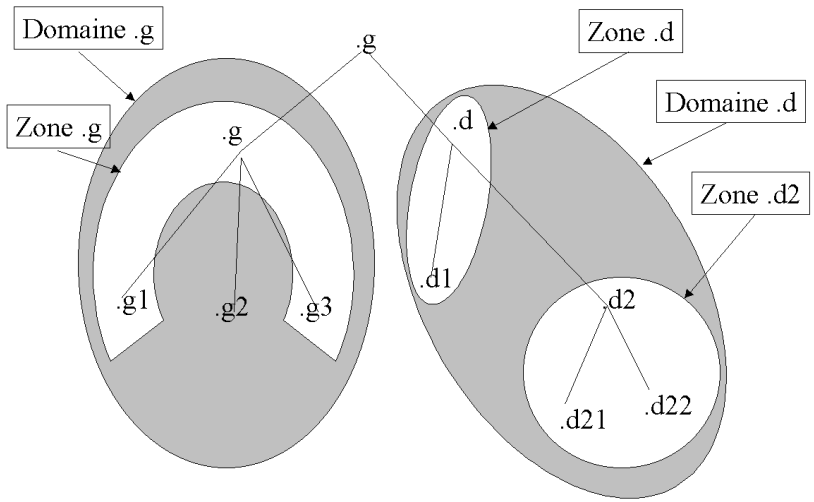
Domaine : récursivité DNS

Description de l'image précédente

Résolution itérative d'un nom dans le DNS par un serveur DNS (étapes 2 à 7) et réponse (étape 8) suite à l'interrogation récursive (étape 1) effectuée par un client (resolver) DNS. (remarque : Le serveur DNS récursif est dit récursif car il accepte ce type de requêtes mais il effectue des requêtes itératives).

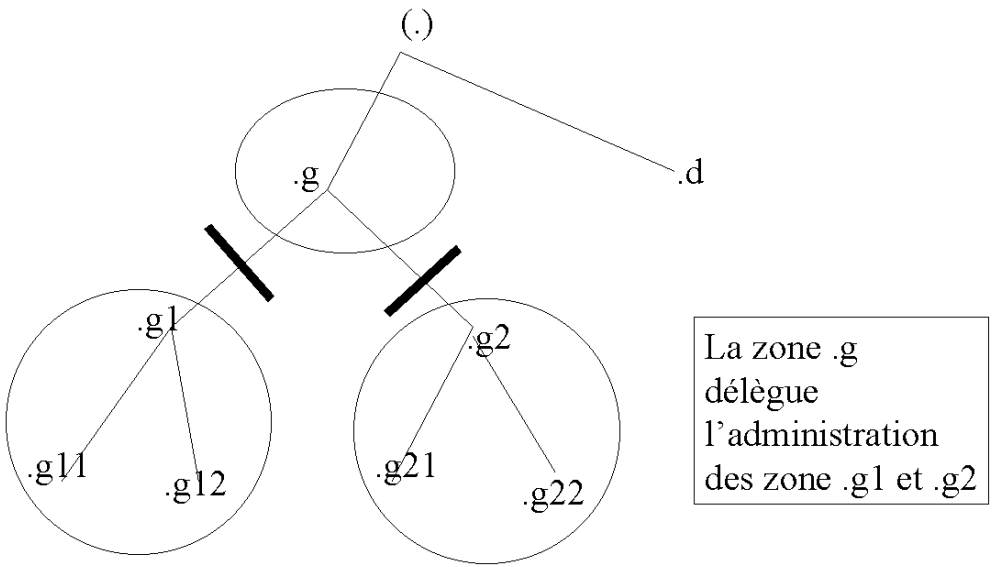
Zone

Une ZONE est une organisation logique ou une organisation administrative des domaines. Le rôle d'une zone est principalement de simplifier l'administration des domaines. Le domaine .COM peut être découpé en plusieurs zones, Z1.COM, Z2.COM ... ZN.COM. L'administration des zones sera déléguée afin de simplifier la gestion globale du domaine.



Délégation

La délégation consiste à déléguer l'administration d'une zone ou une sous-zone aux administrateurs de cette zone.



- La délégation permet de déléguer (décentraliser) l'administration d'une partie de l'espace de nommage d'un domaine.
- Les serveurs de noms disposent de toutes les informations de la zone
- Les serveurs de nom font autorité sur 1 ou plusieurs zones.

Cache

L'organisation d'internet est hiérarchique. Chaque domaine dispose de ses propres serveurs de noms. Les serveurs peuvent être sur le réseau physique dont ils assurent la résolution de nom ou sur un autre réseau. Chaque zone de niveau supérieur (edu, org, bf, fr...) dispose également de serveurs de nom de niveau supérieur.
L'installation du service DNS, installe une liste de serveurs de noms de niveaux supérieurs. Cette liste permet au serveur de résoudre les noms qui sont extérieurs à sa zone. Le serveur enrichit son cache avec tous les noms résolus. Si votre réseau réseau n'est pas relié à internet, vous n'avez pas besoin d'activer cette liste.

Cache (2)

Cette liste est un peu particulière. Elle est fournie avec les distributions. Elle est utilisée par le serveur de noms à l'initialisation de sa mémoire cache. Si vos serveurs sont raccordés à internet, vous pourrez utiliser une liste officielle des serveurs de la racine.

Enregistrements DNS

Un DNS est une base de données répartie contenant des enregistrements, appelés RR (Resource Records), 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.
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*, permettant aux serveurs intermédiaires de connaître la date de péremption des informations et ainsi savoir s'il est nécessaire ou non de la revérifier.

Enregistrements DNS (2)

D'une manière générale, un enregistrement DNS ou la base de données d'une zone ou d'un domaine peut comporte les informations suivantes :

- A record ou address record qui fait correspondre un nom d'hôte à une adresse IPv4 de 32 bits distribués sur quatre octets ex : 123.234.1.2 ;
- AAAA record ou IPv6 address record qui fait correspondre un nom d'hôte à une adresse IPv6 de 128 bits distribués sur seize octets ;
- CNAME record ou canonical name record qui permet de faire d'un domaine un alias vers un autre. Cet alias hérite de tous les sous-domaines de l'original.

Enregistrements DNS : suite liste d'insformation

- MX record ou mail exchange record qui définit les serveurs de courriel pour ce domaine ;
- PTR record ou pointer record qui associe une adresse IP à un enregistrement de nom de domaine, aussi dit "reverse" puisqu'il fait exactement le contraire du A record ;
- NS record ou name server record qui définit les serveurs DNS de ce domaine ;
- SOA record ou Start Of Authority record qui donne les informations générales de la zone : serveur principal, courriel de contact, différentes durées dont celle d'expiration, numéro de série de la zone.

Enregistrements DNS : suite liste d'insformation (2)

- SRV record qui généralise la notion de MX record, mais qui propose aussi des fonctionnalités avancées comme le taux de répartition de charge pour un service donné, standardisé dans la RFC 2782.

Requête DNS

Chaque fois que vous entrez une adresse Web sous la forme d'une URL (Uniform Resource Locator) dans la barre de recherche de votre navigateur, celle-ci renvoie cette demande au résolveur. Il s'agit d'un composant spécial de votre système d'exploitation qui a enregistré des adresses IP déjà chargées dans votre cache et qui fournit à des applications clients si besoin. Si une adresse IP demandée n'est pas présente dans le cache du résolveur, la nouvelle requête DNS est alors transférée au serveur DNS responsable. En règle générale, il s'agit du serveur DNS de votre fournisseur de service Internet. A partir de là, la demande est équilibrée avec la base de données DNS ce qui entraîne une réponse de l'adresse IP (« forward lookup »), si celle-ci est présente.

Requête DNS (2)

Cela permet à votre navigateur de s'adresser de manière claire et uniquement via le Web au serveur Web souhaité. L'alternative est que les adresses IP se traduisent dans la direction opposée avec des noms de domaine respectifs (« reverse lookup »). Si un serveur DNS ne peut pas répondre à une demande en raison de son propre stock de données, il peut alors récupérer les informations correspondantes en partant d'un autre serveur ou transmettre la requête au serveur DNS concerné. On parle dans ce cas de requêtes récursives et de requêtes itératives ainsi qu'il suit :

Requête DNS (3)

- Requêtes récursives : si le serveur DNS ne peut répondre lui-même à une requête, celui-ci récupère les informations désirées sur un autre serveur. Alors, le résolveur rend la requête entière du DNS au serveur affecté. Ce dernier livre au résolveur la réponse dès que le nom de domaine est résolu.
- Requêtes itératives : si un serveur DNS ne peut répondre à une requête, ce dernier répond uniquement avec l'adresse du prochain serveur DNS interrogé. Le résolveur doit s'occuper de ces requêtes de manière indépendante jusqu'à ce que le nom de domaine soit résolu.

Requête DNS (4)

La gestion centrale des informations de domaine dans le DNS est caractérisée par une certaine fiabilité mais aussi par la flexibilité. Si l'adresse IP d'un serveur change, l'utilisateur n'est en général pas prévenu étant donné que le nom de domaine est assigné uniquement à une adresse IP dans la base de données.

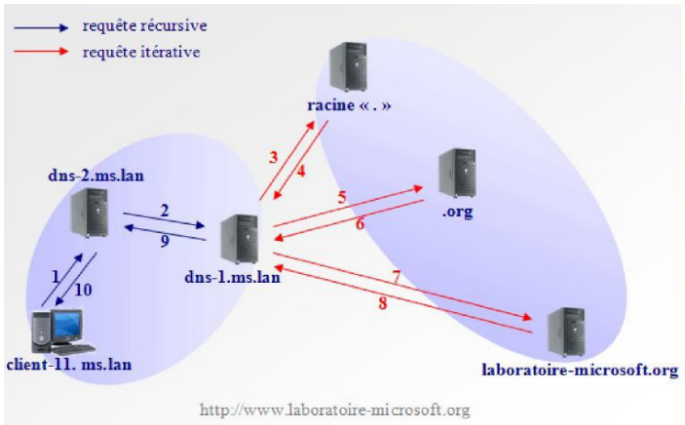


FIGURE – Requête DNS. Exemple 1

Requête DNS (5)

Dans l'exemple ci-dessus, un client nommé CLIENT-11.MS.LAN souhaite accéder au site web du laboratoire Microsoft. La procédure de résolution de nom se passe en plusieurs étapes :

1. L'ordinateur client CLIENT-11.MS.LAN commence par chercher l'adresse IP du serveur Web. Pour cela ilenvoie une requête récursive au premier serveur DNS de sa liste de serveurs DNS soit DNS-2.MS.LAN.
2. Le serveur DNS-2.MS.LAN ne connaît pas la réponse, il envoie donc une requête récursive à DNS-1.MS.LAN qui est le premier serveur DNS de sa liste de redirecteurs.

Requête DNS (6)

3. Dans le cas présent DNS-1.MS.LAN ne connaît pas l'adresse IP recherchée et n'est pas configuré pour utiliser des redirecteurs. Il envoie donc une requête itérative au premier serveur DNS racine parmi saliste d'indications de racine.
4. Le serveur DNS racine ne connaît pas la réponse mais il sait quel serveur DNS fait autorité pour ledomaine org. Il renvoie donc l'adresse IP du serveur DNS faisant autorité pour le domaine ORG à DNS-1.MS.LAN.

Requête DNS (7)

5. Le serveur DNS-1.MS.LAN envoie alors une requête itérative au serveur DNS du domaine ORG.
6. Le serveur DNS du domaine ORG ne connaît pas la réponse et renvoie l'adresse IP du serveur DNSfaisant autorité pour le domaine LABORATOIRE-MICROSOFT au serveur DNS-1.MS.LAN.
7. Le serveur DNS-1.MS.LAN contacte alors le serveur DNS faisant autorité pour la zone LABORATOIRE-MICROSOFT au moyen d'une requête itérative.

Requête DNS (8)

8. Le serveur DNS faisant autorité pour la zone laboratoire-microsoft possède le mappage dans sa zonede recherche directe locale. Il envoie donc l'adresse IP recherché à DNS-1.MS.LAN.DNS-1.MS.LAN transmet la réponse au serveur DNS-2.MS.LAN.
9. Le serveur DNS-2.MS.LAN fait suivre la réponse au client qui peut ensuite joindre le serveur HTTP etafficher le site du laboratoire Microsoft.

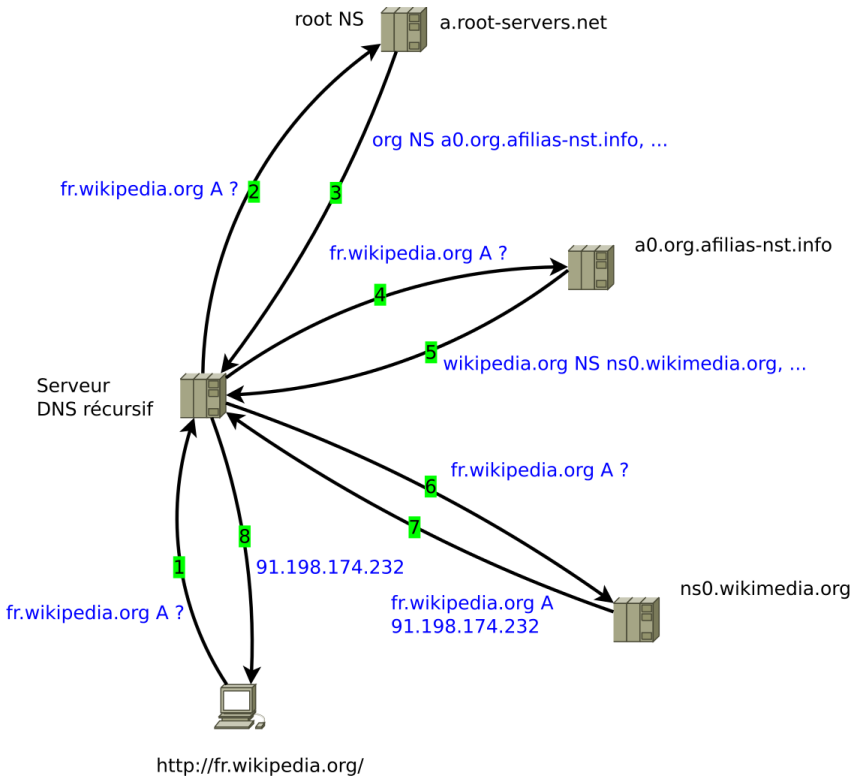


FIGURE – Récursivité DNS.