namebay
créateur de noms de domaine

BaBA

Les DNS sont nés en 1983 du besoin de remplacer une adresse IP par une forme d'identification de l'application cible plus facile à retenir.

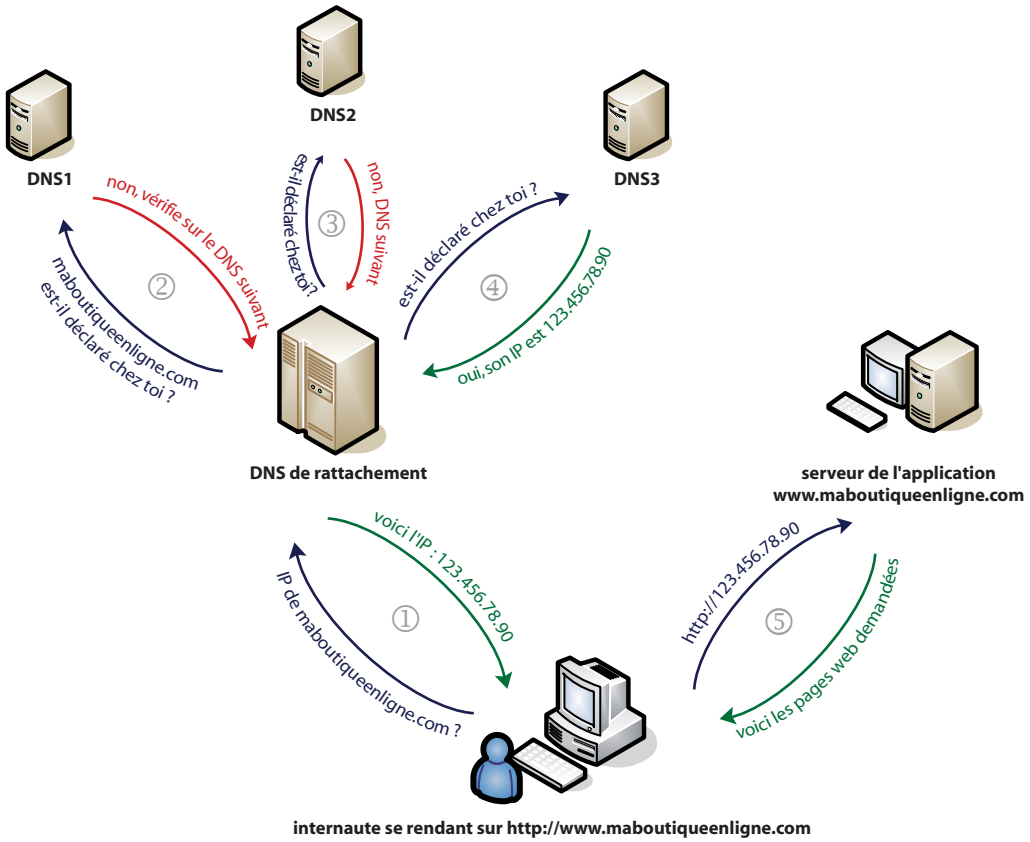
On peut dire que les DNS sont partout, dans une entreprise, chez un hébergeur, chez un fournisseur d'accès Internet, chez un bureau d'enregistrement de noms de domaine (registrar comme Namebay), chez l'exploitant d'une zone (un registre tel que pour le .com, .fr, …). Il en figure même un rudimentaire dans une station de travail sous la forme d'un fichier système dont le nom est « hosts ». Vous pouvez y inscrire vos domaines privés relatifs à votre réseau local domestique par exemple.

Et pourtant, un seul d'entre eux contient l'adresse IP cible associée à un nom de domaine.

Il faut donc qu'un mécanisme de recherche soit mis en œuvre dès qu'un utilisateur tape le nom de domaine de l'application qu'il vise dans la barre de son navigateur (Mozilla, Internet Explorer). C'est ce qu'on veut expliquer le plus simplement possible dans ce qui suit, en gardant à l'esprit que ce mécanisme est mis en œuvre, en complète transparence pour l'utilisateur, sauf quand il n'aboutit pas, ou qu'il est anormalement long.

DNS de rattachement :

Un DNS de rattachement peut avoir un mode de fonctionnement itératif ou récursif. Dans le mode récursif, le DNS de rattachement interroge les serveurs racines, connus de tous les DNS, pour obtenir l'adresse des DNS de zone, eux-mêmes connus des DNS racines. Puis il interroge le premier DNS de zone dans la liste rendue par le DNS racine interrogé, qui lui donne alors l'adresse du DNS autoritaire. L'interrogation du DNS autoritaire permet de récupérer l'adresse IP et de la remettre au navigateur.
Dans le mode itératif, ça fonctionne à peu près semblablement, mais le DNS de rattachement se contente de remettre les résultats intermédiaires au navigateur qui assure alors lui-même l'enchaînement des interrogations.
Voir schéma page 2



Toute station de travail (votre PC) qui possède un raccordement à l'internet, soit dans une entreprise, soit à la maison via un fournisseur d'accès FAI, a été configurée en lui déclarant un DNS de rattachement, celui de l'entreprise ou du FAI généralement.

Après qu'on ait tapé un nom de domaine avec le protocole associé (http, ftp, …) dans la barre d'adressage du navigateur, celui-ci va interroger le DNS de rattachement pour lui demander de résoudre le nom de domaine en adresse IP. Sauf si le DNS de rattachement possède l'information dans son cache (sa mémoire locale), il s'ensuit alors une série d'échanges entre plusieurs DNS pour trouver celui qui possède l'information.

Les types de DNS et leur interrogation

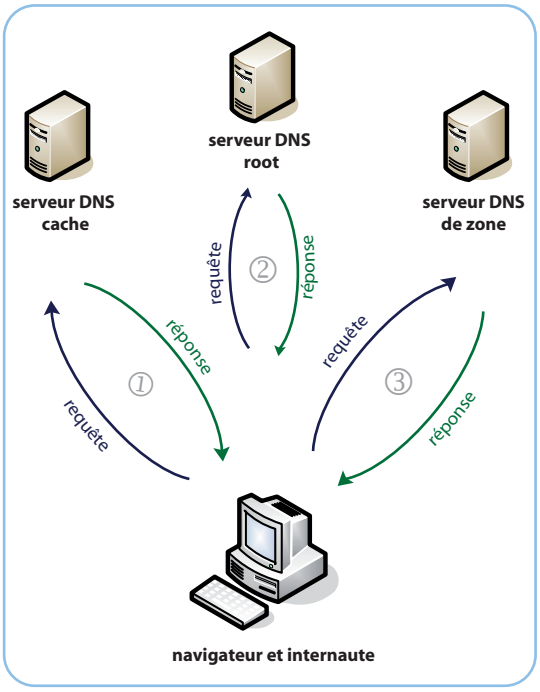
Le DNS qui contient les informations opérationnelles est appelé autoritaire.

Il signale au gestionnaire de la zone (l'extension) au moment de l'enregistrement du nom de domaine qu'il est autoritaire sur ce nom de domaine. Ce gestionnaire va alors consigner l'adresse du serveur autoritaire dans les DNS dits de zone (il peut y en avoir plusieurs pour des raisons de disponibilité ou de performances).

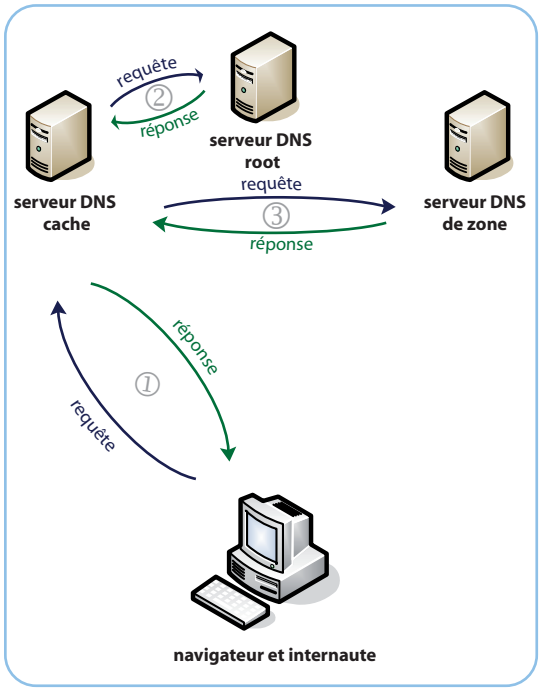
Le réseau Internet possède 13 groupes de serveurs DNS dits racines qui possèdent l'image de tous les DNS de zones, puisque ce sont des registres officiels.
On a défini ci-dessus le type de DNS dit de rattachement. Un DNS de rattachement peut avoir un mode de fonctionnement iteratif ou récursif. Dans le mode récursif, le DNS de rattachement interroge les serveurs racines, qui sont connus de tous les DNS, pour obtenir l'adresse des DNS de zone, qui ne sont connus que des DNS racines. Puis il interroge le premier DNS de zone dans la liste rendue par le DNS racine interrogé, qui lui donne alors l'adresse du DNS autoritaire. L'interrogation du DNS autoritaire permet de récupérer l'adresse IP et de la remettre au navigateur.

Dans le mode iteratif, ça fonctionne à peu près semblablement, mais le DNS de rattachement se contente de remettre les résultats intermédiaires au navigateur qui assure alors lui-même l'enchaînement des interrogations.

MODE ITÉRATIF



MODE RÉCURSIF



Les interrogations sont faites avec le protocole DNS qui a deux commandes principales NSLookUP, et Host. Si le nombre de DNS interrogé est élevé et si le réseau est ralenti, ce peut être une des causes d'attente du chargement de la première page du web appelé.

DNS primaire et secondaire, le cache d'un DNS et la propagation

Un DNS autoritaire est généralement fait d'un serveur primaire qui contient le source des informations et d'un serveur secondaire qui entretient une image de ces informations en se synchronisant périodiquement avec le serveur primaire.

A un nom de domaine est associée une information dite TTL qui est le temps maximal de validité de cette information.

Un DNS de rattachement peut mettre en cache les informations qu'il obtient suite à une demande par les navigateurs. Dans ce cas, la réponse sera rendue très vite au navigateur qui la demande. Mais celle-ci peut devenir obsolète, en particulier, si les informations du DNS autoritaire sont modifiées (changement de l'adresse IP par exemple). Le DNS de rattachement réinterroge les DNS racines à l'expiration du TTL d'un domaine. La propagation d'un changement peut alors prendre la valeur de ce TTL au maximum, selon le moment entre la modification du DNS autoritaire et la dernière mise à jour.

Il devra y avoir propagation de la modification dans le réseau de DNS lors d'un changement d'IP (changement de serveur ou d'hébergeur). Lors d'un transfert de registrar, il n'y aura pas de perturbations si l'adresse IP n'a pas changée.

Les champs du DNS associés à un domaine

Outre ses propriétés dans le réseau, un DNS est une base de données dont les enregistrements sont conçus pour jouer l'ensemble des rôles décrits ci-dessus. A chaque nom de domaine est associé un ensemble d'informations qu'on peut appeler des champs de nature à fournir toutes les informations DNS sur ce nom de domaine. Les principaux champs enregistrés ont les fonctions suivantes :

- Le champ A (comme address record) indique que l'hôte a une adresse IPv4 de 32 bits.
- Le champ AAAA indique au contraire que l'hôte a une adresse IPv6 de 128 bits.
- Le champ CNAME (canonical name record) permet de faire d'un domaine un alias vers un autre. C'est ce champ qui est positionné pour faire une redirection web.
- Le champ MX (mail exchange record) définit les noms de domaines des serveurs de mail associé à ce domaine. L'absence de ce champ correspond à une absence de serveurs mail. On notera que les serveurs de mail peuvent avoir eux-mêmes leurs IP définies par d'autres DNS.
- Le champ PTR (pointer record) est le champ qui définit l'adresse IP associée au nom de domaine.
- Le champ NS (name server record) définit les noms de domaines des serveurs DNS de ce domaine s'ils sont différents des serveurs autoritaires.
- Le champ SOA (Start Of Authority record) définit le serveur DNS autoritaire.

Certains champs peuvent avoir plusieurs valeurs comme le champ MX pour définir une liste de serveurs de messagerie avec un ordre de priorité.