Système DNS et Résolution de noms de domaine

Système DNS : présentation, fonctionnement et administration

BTS SIO – Bloc n°2 : Administration des systèmes

PLAN DU COURS

I. DNS : Problématique et origines

- Pour pouvoir communiquer, chaque machine présente sur un réseau doit avoir un identifiant unique.
- Sur un réseau physique, une machine est identifiée de façon unique par une adresse MAC associée à la carte réseau et attribuée par le fabricant.
- Sur un réseau logique (IP) ou Internet une machine est identifiée de manière unique par une adresse IP (v4 ou v6).
- Cependant pour un utilisateur/administrateur réseau, il est impensable de retenir les adresses IP de chaque ordinateur.
  → 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 et inversement.

I. DNS : Problématique et origines

- Au départ, chaque machine stockait localement les mappages noms / adresse IP.
  → un mappage est une correspondance/lien entre un nom et une adresse IP,
  → soit via des **fichiers de configuration** (hosts) ou soit via des **systèmes de tables** tels que NetBIOS ((dédié au réseau regroupant des machines Windows),
  → bien que toujours en place sur certains réseaux → systèmes parfois jugés obsolète voire supplantés par le système DNS.
- Au début (1970-1984) : un annuaire complet dans un fichier texte (/etc/hosts sous Unix) :
  → Adresse Nom1 Nom2 Nom3
  → Cohérence des noms par diffusion du fichier entre les machines.
- Aujourd'hui, ce fichier est encore utilisé pour l'annuaire du système en local.

I. DNS : Problématique et origines

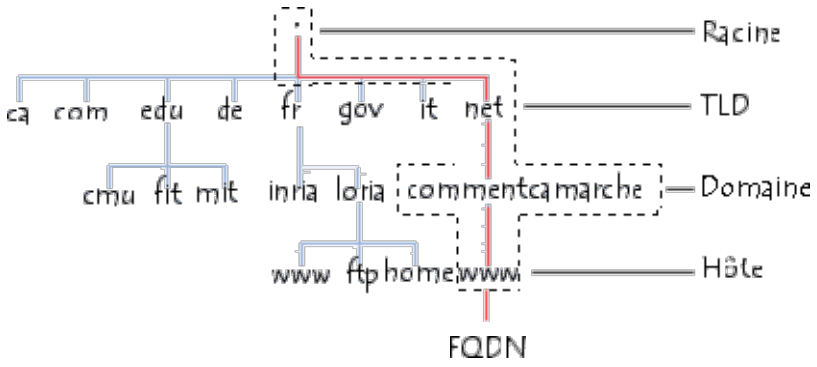
- Ces systèmes présentent les inconvénients :
  - Un système basé sur des fichiers répartis et partagés entre les machines présentait un problème de lenteur (lors des transferts) au niveau du réseau et de lourdeur lors de la maintenance et l'administration et la configuration des hôtes (machines):
    → à chaque ajout de machines dans le réseau ou bien à chaque modification de la configuration d'une machine, il faut éditer manuellement le fichier contenant les mappages noms / adresse IP et le paramétrer.
  - De plus, le réseau nécessitait un système de dénomination automatisé pour résoudre les problèmes techniques et de personnel

II. DNS : Introduction

- Un nouveau système a été créé, le DNS, basé sur le protocole IP.
  - → D'abord, conceptualisé par des chercheurs de l'université de Standford, dans les années 70.
  - → Puis, implémenté par 4 étudiants de l'université de Berkeley sur un système Unix appelé « Bind », dans les années 80.
- Le système de nom de domaine (DNS) fournit une correspondance de noms entre des ressources de plusieurs types :
  - → machines (serveurs, postes de travail),
  - → périphériques réseaux (imprimantes réseaux),
  - → applications, base de données,
  - → équipements réseaux (routeurs, parefeu), …
- C'est un système hiérarchique, redondant et distribué :
  - → Arborescence (arbre inversé, comme un système de fichiers) ;
  - → Chaque site/organisation est maître de ses données (dans son domaine) ;
  - → Dynamique : mise à jour automatique entre serveurs DNS locaux, de domaines et racines.

II. DNS : Introduction

- Exemple de la structure du système DNS :



II. DNS : Introduction

- Le DNS a été créé en 1983 (RFCs 1034 et 1035), modifié, mis à jour, et amélioré par une multitude de RFCs: 2181, …
- Le système DNS introduit une convention de nommage hiérarchique des domaines qui commence par :
  - ❑ un domaine **racine** appelé ".".
  - ❑ les domaines situés directement sous le domaine racine sont appelés **domaines de premier niveau (TLD – Top Level Domain)**,
    - →représentent souvent la localisation géographique (pays **ccTLD country code TLD** : .fr, .be, .eu, .uk, .us …) ou le type de service (.info, .org, .gov, .mail, .com, …).
  - ❑ les **domaines de second niveau** sont disponibles pour les entreprises et les particuliers (cisco.com, microsoft.fr, google.fr, amazon.uk, …).
  - ❑enfin, une **multitude de sous domaines peuvent être créés à l'intérieur d'un domaine de second niveau** (education.gouv.fr, …), jusqu'à 127 niveaux.

II. DNS : Introduction

- Les domaines de premier niveau sont gérés par l'ICANN (Internet Corporation for Assigned Names and Number) :
  →attribution des noms de domaine mondialement.

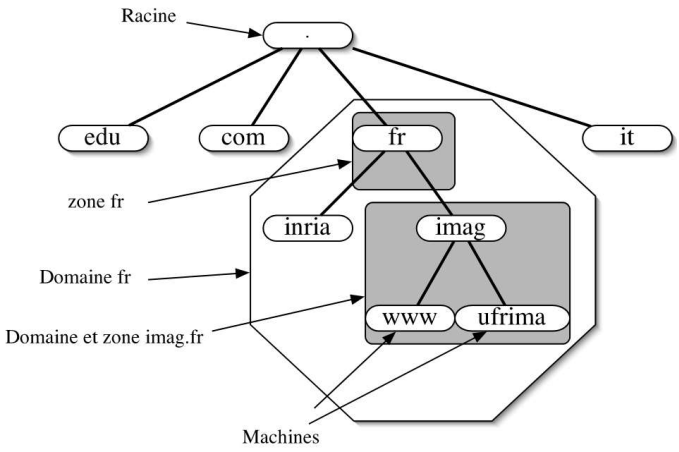
- Les domaines de second niveau sont distribués et gérés par d'autres sociétés comme l'InterNIC (une filiale le l'ICANN) ou bien l'AFNIC (Association Française pour le Nommage Internet en Coopération) qui gère le domaine « .fr ».

III. DNS : Concept de résolutions de noms

- L' espace de nommage a besoin d' être hiérarchisé pour évoluer à grande échelle.
- L' idée est de nommer les objets sur la base de :
  - l'endroit (au sein d' un pays, d'une organisation, ensemble d' organisations, d'une société, ensemble de sociétés, etc ...) : **.fr**
  - l'unité (département, service, cellule, ...) dans cet endroit (organisation dans un ensemble d'organisations, etc ...) : **gouv.fr**, **education.gouv.fr**
  - l'objet au sein de l' unité (nom de personne, d'une machine, d'un périphériques dans une société) : **www.lgtbaimbridge.fr, srvad.ville-abymes.fr, jdupont.ville-abymes.fr, srvnas.ville-abymes.fr**
- Informations accessibles grâce au DNS :
  - Adresses IP (V4 ou V6) en fonction du nom : résolution directe,
  - Nom en fonction de l'adresse IP : résolution inversée,
  - Adresse de relais de messagerie électronique : pour transférer les emails entre les différents domaines.

IV. DNS : Terminologie

- Hiérarchique par domaine : *www.imag.fr*



IV. DNS : Terminologie

- Hiérarchique par domaine : *www.imag.fr*
  - ❑ hôte (machine) « www » dans le domaine « imag » lui-même dans le domaine « fr »
  - ❑ on omet en général la racine (le point) à la fin : www.imag.fr.
- Un **domaine** est la partie de l'arborescence à partir du nœud portant son nom :
  - → Exemple : domaine « fr », arborescence à partir du nœud « fr »
- On parle de **sous-domaine** pour un domaine inclus dans un autre :
  - → Exemple : « imag.fr » est un sous domaine du domaine « fr ».

IV. DNS : Terminologie

- Une **zone** : c'est la base de données associée à un nœud.
- Le contenu des bases de données associées aux zones :
  - ❑ Noms/Adresses des serveurs de la zone (plusieurs serveurs DNS → disponibilité du service DNS.
    - →Exemples :
      - **racine**, liste des serveurs des domaines de premiers niveaux.
      - « .fr » : liste des adresses des serveurs des sous-domaines de « .fr »
  - ❑Noms/Adresses des machines de ce domaine.

IV. DNS : Terminologie

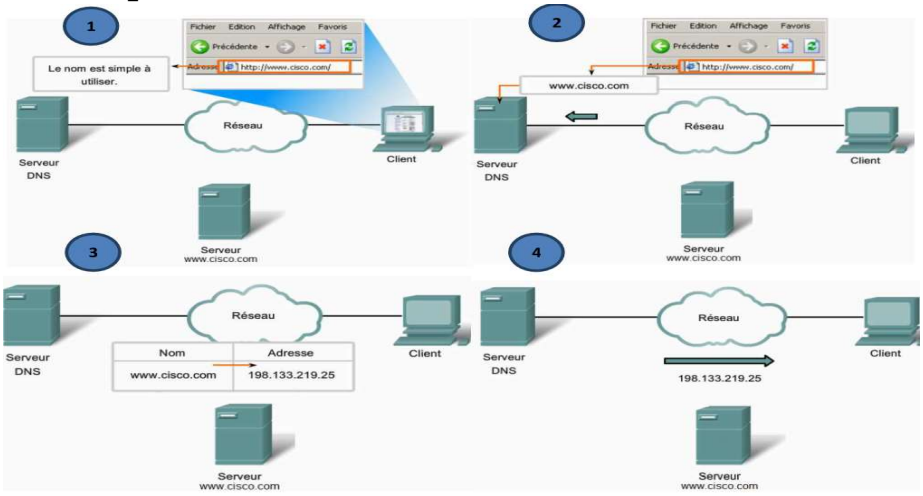
- Le nom de domaine « *www.imag.fr* » est un nom de domaine pleinement qualifié (FQDN Full Qualified Domain Name) :
  - ❑ FQDN = Nom d'hôte . Nom de domaine (ou suffixe dns) ;
  - ❑Le « . » point, représente la « concaténation» : joindre deux chaînes de caractères (accoler)

V. DNS : Protocoles

- Application client/serveur.
- Pour les échanges, voici les ports utilisés :
  - ❑ par UDP quand c'est possible, pour les requêtes courtes pour des raisons d'efficacité.
  - ❑ sinon par TCP (transfert de zones).
  - ❑ Port serveur = 53, port client > 1023
  - ❑ échange « serveur » à « serveur » protocole transport UDP : port 53 à 53.
  - ❑ échange « serveur » à «client » protocole transport TCP : > 1023 à 53.

VI. DNS : Principe de fonctionnement

- Principe de résolution de noms de domaines :



VI. DNS : Principe de fonctionnement

- Principe de résolution de noms de domaines :
  1. L'utilisateur de l'ordinateur client veut visualiser une page web sur le serveur web « www.cisco.com ». L'utilisateur tape donc « www.cisco.com » dans la barre d'adresse url de son navigateur.
  2. L'ordinateur client demande à son serveur DNS : quelle est l'adresse IP du serveur ayant pour nom «www.cisco.com » ?

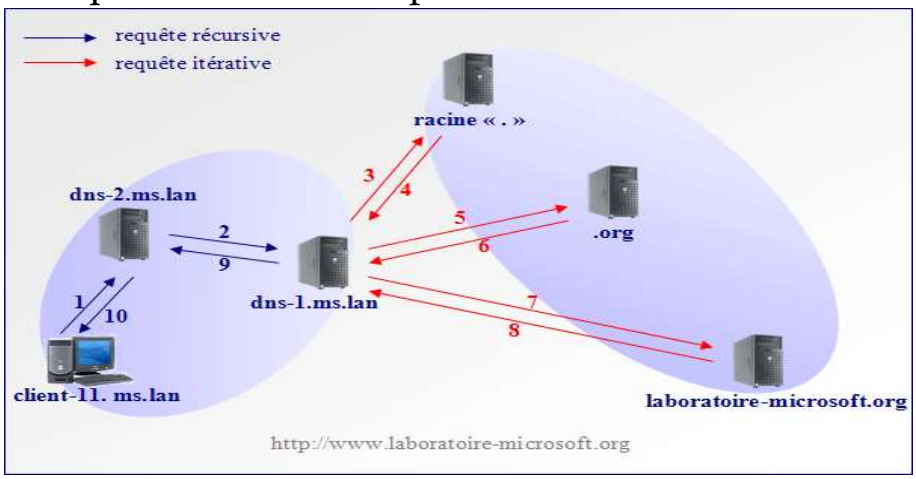
     Remarque : le port d' écoute du serveur DNS est le port n°53
  3. Le serveur DNS recherche dans sa base constituée de fichiers configurés afin d'associer le nom du serveur www.cisco.com, à son adresse IP.
  4. Une fois une correspondance trouvée, l'adresse IP est renvoyée au client pour que celui-ci puisse l'utiliser dans ses requêtes adressées au serveur. L'ordinateur client envoie donc sa requête de visualisation de page web, au serveur d'adresse IP 198.133.219.25.

VI. DNS : Principe de fonctionnement

- Un serveur DNS peut recevoir deux types de requêtes DNS :
  - ❑ les **requêtes récursives** sont des requêtes DNS envoyées entre les postes clients et les serveurs DNS du réseau local voire les serveurs DNS du FAI.
    - →Les serveurs DNS du réseau local jouent à la fois le rôle de serveurs DNS mais aussi de client DNS car ils font la résolution de noms de domaines des requêtes provenant des postes clients mais ils envoient aussi des requêtes DNS vers les autres serveurs DNS disponibles sur Internet.
  - ❑ les **requêtes itératives** se font entre le serveur DNS local ou du FAI vers les autres serveurs DNS présents sur le réseau Internet et chargés de mettre en œuvre la résolution de noms avant de retourner les réponses DNS à savoir les adresses IP vers les postes clients.

VI. DNS : Principe de fonctionnement

- Un serveur DNS peut recevoir deux types de requêtes DNS – Exemple :



VI. DNS : Principe de fonctionnement

- Un serveur DNS peut recevoir deux types de requêtes DNS - 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 il envoie une requête récursive au premier serveur DNS de sa liste de serveurs DNS soit « dns-2.ms.lan ».
  2. Le serveur « dns-2.ms.la »n 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.
  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 sa liste d'indications de racine.

VI. DNS : Principe de fonctionnement

- Un serveur DNS peut recevoir deux types de requêtes DNS – Exemple (suite) :
  4. Le serveur DNS racine ne connaît pas la réponse mais il sait quel serveur DNS fait autorité pour le domaine « .org ». Il renvoie donc l'adresse IP du serveur DNS faisant autorité pour le domaine « org » à « dns-1.ms.lan ».
  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 DNS faisant 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.

VI. DNS : Principe de fonctionnement

- Un serveur DNS peut recevoir deux types de requêtes DNS – Exemple (suite) :
  8. Le serveur DNS faisant autorité pour la zone « laboratoire-microsoft » possède le mappage dans sa zone de recherche directe locale. Il envoie donc l'adresse IP recherché à « dns-1.ms.lan ».
  9. « dns-1.ms.lan » transmet la réponse au serveur « dns-2.ms.lan ».
  10. Le serveur « dns-2.ms.lan » fait suivre la réponse au client qui peut ensuite joindre le serveur HTTP et afficher le site du laboratoire Microsoft.

VI. DNS : Principe de fonctionnement

- En d'autres termes, un serveur DNS peut recevoir deux types de requêtes DNS :
  - une **requête récursive** : lorsqu'un serveur DNS reçoit une requête récursive, il doit donner la réponse la plus complète possible. C'est pourquoi le serveur DNS est souvent amené à joindre d'autres serveurs de noms dans le but de trouver la réponse exacte.
  - une **requête itérative** : Lorsqu'un serveur reçoit une requête itérative, il renvoie la meilleure réponse qu'il peut donner sans contacter d'autres serveurs DNS (c'est-à-dire en consultant uniquement sa propre base de données).

VII. DNS : Types d'enregistrement

- On distingue plusieurs types d'enregistrements de ressources :

```
$TTL    1600
@       IN      SOA     debvirt.maison.mrs. root.debvirt.maison.mrs. (
                        2009012901      ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          1600 )        ; Negative Cache TTL
;
@         IN    NS      debvirt.maison.mrs.
@         IN    A       192.168.0.254
debvirt   IN    A       192.168.0.254
test1     IN    A       192.168.0.1
test2     IN    CNAME   test1
test3     IN    CNAME   irp.nain-t.net.
```

VII. DNS : Types d'enregistrement

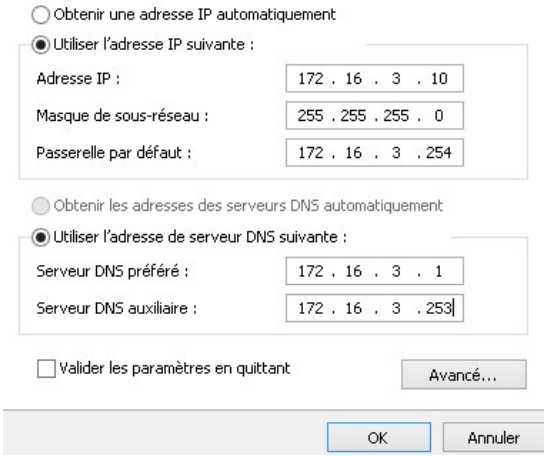
- Les mappages nom d'hôte / adresse IP et adresse IP / nom d'hôte sont appelés enregistrements de ressources.
- Voici la liste des principaux types :
  - SOA (Start Of Authority) : spécifie des informations relatives à l'administrateur du domaine (nom du serveur primaire suivi du mail de l'administrateur). Il contient le nom d'hôte et l'adresse IP du serveur DNS qui héberge actuellement la zone DNS principale. Il y a un seul enregistrement SOA par zone DNS. C'est le premier enregistrement crée dans une zone DNS.
  - A : Les enregistrements de ressources A (pour Adresse d'hôte) sont des mappage entre un nom d'hôte et une adresse IPv4. Ils représentent généralement la majorité des enregistrements de ressources des zones de recherches directes.
  - AAAA : Les enregistrements de ressources de ce type sont des mappages entre un nom d'hôte et une adresse IPv6 (adresse IP d'une longueur de 128 bits).

VII. DNS : Types d'enregistrement

- Voici la liste des principaux types :
  - CNAME : les enregistrement de ressources de type CNAME (Canonical NAME ou nom canonique) sont des mappages entre un nom d'hôte et un autre nom d'hôte. Ils permettent de créer des alias pour un nom d'hôte donné (c'est-à- dire d'associer plusieurs noms d'hôte à une même machine).
  - MX : les enregistrements de ressources de type MX (Mail eXchanger) identifient les serveurs de messagerie. Chaque serveur de messagerie doit aussi disposer d'un enregistrement de ressource A. Il est possible de donner une priorité différente à chaque enregistrement MX.
  - NS : les enregistrements de ressources de type NS (Name Server ou serveur de nom) identifient les serveurs DNS de la zone DNS. Ils sont utilisés dans le cadre de la délégation DNS.

VIII. DNS : Configuration postes « clients »

- Exemple de configuration d'un ordinateur client :



VIII. DNS : Configuration postes « clients »

- <u>Explications :</u>
- Serveur maître, principal
  → sur lequel sont faites les modifications par l'administrateur,
  → il est à l'origine de l'autorité sur une zone (SOA : Start Of Autority).
- Serveur esclave, secondaire
  → interroge et récupère régulièrement les bases de données depuis le serveur maître,
  → peut posséder un cache pour minimiser les requêtes.
- Une réponse à une interrogation peut être faite par un serveur primaire ou secondaire
- Un serveur peut être secondaire pour certaines zones et primaire pour d'autres.

SYSTÈME DNS ET RESOLUTION DE NOMS DE DOMAINES

FIN