Les Services Réseaux

Université Assane Seck
UFR Sciences et technologie
Département Informatique

1 Le service de noms (DNS)

1 Le service de noms (DNS)

Introduction

- La communication entre les hôtes sources et destinations via Internet nécessite que chaque hôte dispose d'une adresse IP valide
- Cependant, les milliers adresses IP v4, notamment ceux utilisées par les serveurs sur internet, ne sont pas simples à retenir pour les utilisateurs
- Le service de gestion des noms **(DNS, Domain Name Service)** est fondamental sur l'Internet : il permet d'associer des noms à des adresses IP (et vice versa)
- Ce qui permet de saisir www.yahoo.fr en lieu et place de 217.12.3.11.

Introduction

- Le DNS (Domain Name System) est une base de données distribuée s'appuyant sur UDP (Port 53)
- Le DNS est une base de données distribuée basée sur le modèle relationnel client/serveur
- La partie cliente, le **solveur (resolver)**, est chargée de résoudre la correspondance entre le nom symbolique de l'objet et son adresse réseau
- Introduit un nommage hiérarchique et la notion de domaine
- Chaque noeud de la hiérarchie peut être un domaine ou sous-domaine de nommage

Avantages DNS

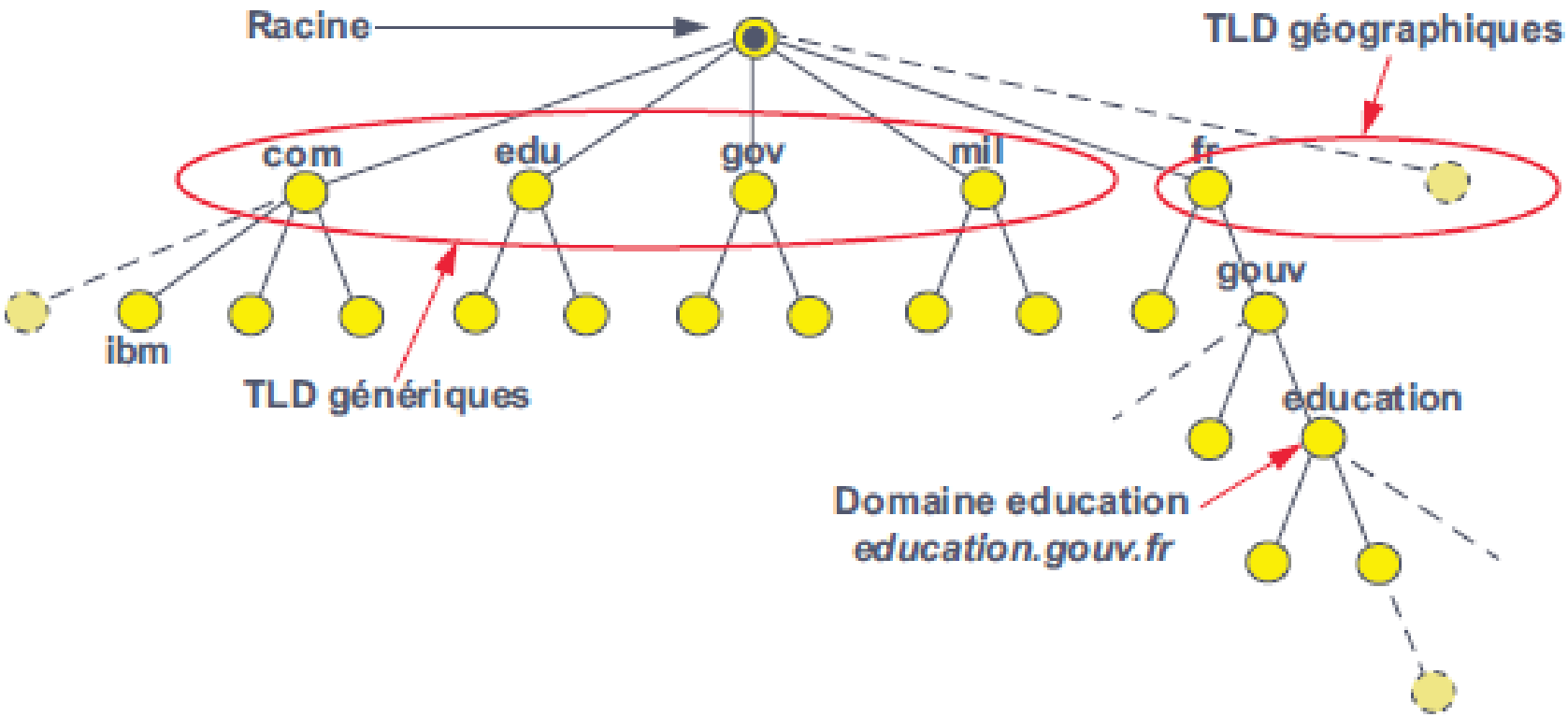
DNS présente les avantages suivants

- gestion simplifiée du nommage (nommage hiérarchique) ;
- délégation et répartition des responsabilités d'attribution de noms et d'administration par domaine de nommage ;
- duplication possible de la base (notion de serveur maître ou primaire et de serveur secondaire),
- le serveur secondaire pouvant répondre à une requête si le serveur principal est occupé.
- La mise à jour se fait uniquement sur le serveur maître avec réplication automatique des données modifiées sur le serveur secondaire ;
- indépendance vis-à-vis d'un constructeur, les resolvers DNS sont, en principe, disponibles sur tous les environnements TCP/IP

L'espace de nommage

- Les noms sont organisés selon une structure arborescente hiérarchique (arbre inversé) appelée espace de nommage
- La racine est au sommet, son nom de domaine est vide, elle est symbolisée par un point (•)
- Le nombre de niveaux est limité à 127
- Un nom ne peut dépasser 255 caractères et chaque niveau est limité à 63 caractères

L'espace de nommage



L'espace de nommage

- Le premier niveau est composé de **TDL, Top Level Domain**
- Deux types de TLD
  - Les TDL génériques:.com, .org, .gov, .net, .biz, .edu
  - Les TLD goégraphiques: .fr, .sn, .uk
- Les sous-domaines sont souvent la désignation des entreprises ou des institutions : univ-zig.sn, adie.sn
- Il peut y avoir des sous-sous-domaines à plusieurs niveaux :
- Le premier composant d'un nom désigne le hôte
  - www.ucad.sn => machine www du domaine ucad.sn
- Une machine est désignée en indiquant l'arborescence complète de son nom **(FQDN, Fully Qualified Domain Name)**

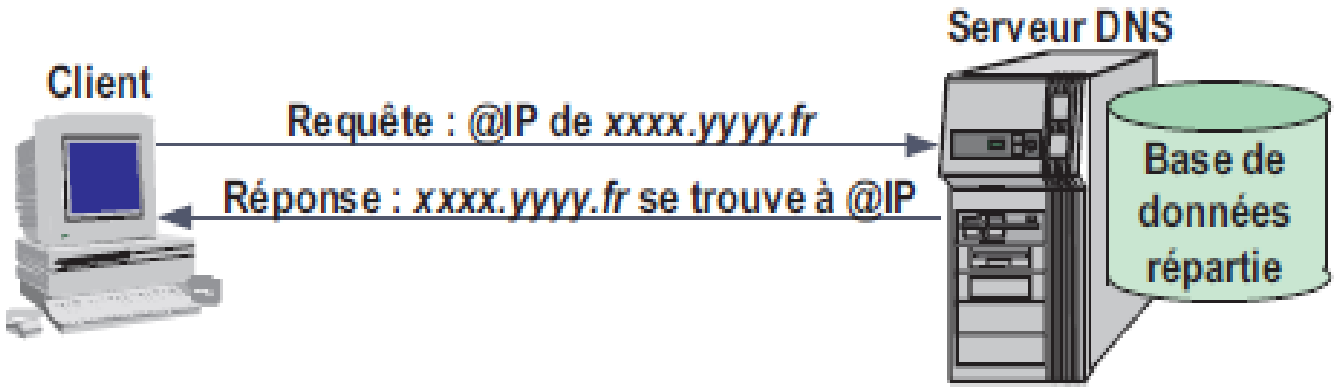
L'espace de nommage

Quelques exemples

- **com**, organisations commerciales, en principe possédant des implantations sur plusieurs domaines géographiques (ibm.com) ;
- **edu**, établissements d'enseignement (réservé aux établissements des USA, mit.edu) ;
- **gov**, établissements gouvernementaux (USA, nsf.gov) ;
- **mil**, organisations militaires américaines (USA, army.mil) ;
- **net**, organisations du réseau Internet (bull.net) ;
- **org**, organisations non commerciales et non gouvernementales (ong.org) ;
- **int**, organisations internationales (onu.int) ;

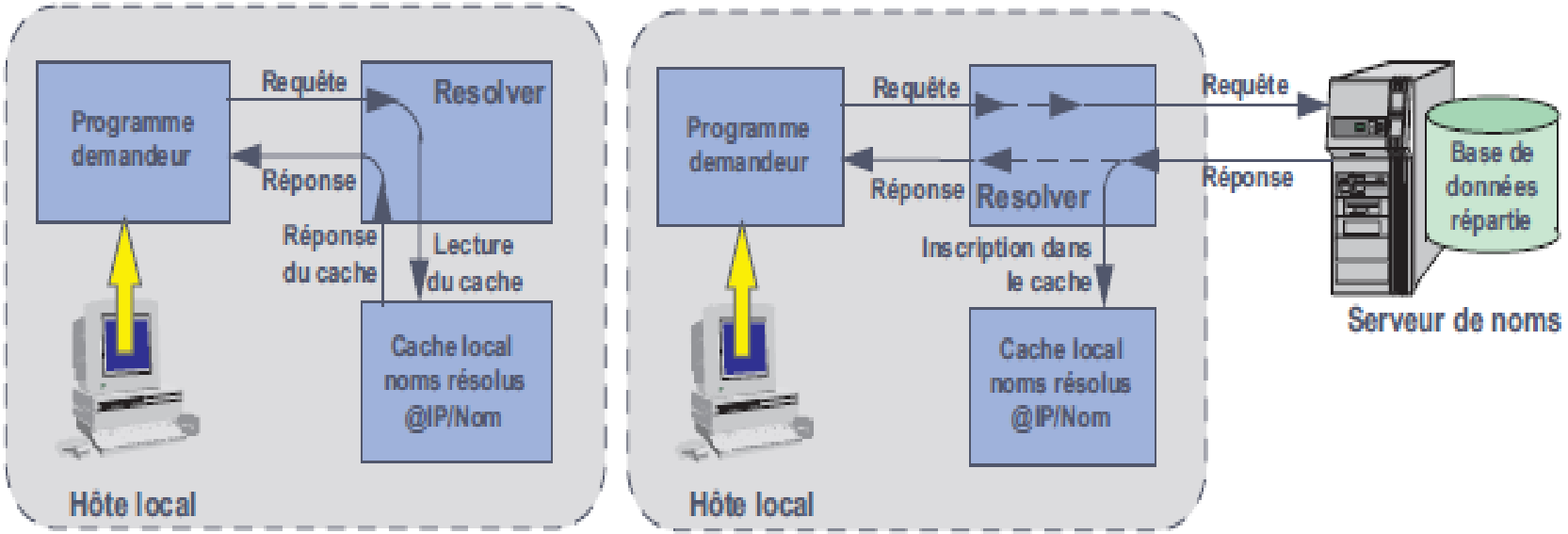
La résolution de nom

- Le client DNS ou solveur (resolver) est un programme de type daemon
- Sur sollicitation d'un programme demandeur, il est chargé d'émettre les demandes et de traduire les réponses



- A la configuration d'une station IP, on lui fournit son nom de domaine, l'adresse de son serveur local de noms et, éventuellement, une liste ordonnée de serveurs de noms
- Le client solveur interroge le serveur de noms local
- Sinon il interroge le serveur de niveau supérieur (recherche récursive)

La résolution de nom



Les types de serveurs

- Les résolvers récursif
  - Un résolveur récursif (également appelé récurseur DNS) est le premier arrêt d'une requête DNS
  - Agit comme un intermédiaire entre un client et un serveur de noms DNS
  - Chaque organisation a un serveur de nom local
  - Il contient les correspondances relatives à la zone de l'organisation
  - Toutes les requêtes en provenance de cette organisation vont vers ce serveur de nom local
  - La plupart des internautes utilisent un résolveur récursif fourni par leur FAI

Les types de serveurs

- Les serveurs de noms racine DNS
  - Existe 13 serveurs racines dans le monde : NASA, DoD, ICANN, Verisign
  - Accepte une requête de résolveur récursif qui inclut un nom de domaine
  - Répond en dirigeant le résolveur récursif vers un serveur de noms TLD, en fonction de l'extension de ce domaine (.com, .net, .org, etc.)
  - Les serveurs de noms racine sont supervisés par Internet Corporation for Assigned Names and Numbers (ICANN)

Les types de serveurs

- Les serveurs de noms TLD
  - Conserve les informations de tous les noms de domaine qui partagent une extension de domaine commune
  - Exemple: Un serveur de noms TLD .com contient des informations pour chaque site web qui se termine par ’.com’
  - L’IANA divise les serveurs TLD en deux groupes principaux :
    - Domaines génériques de premier niveau : .com, .org, .net, .edu et .gov.
    - Domaines de premier niveau de code de pays : .uk, .us, .ru et .jp.

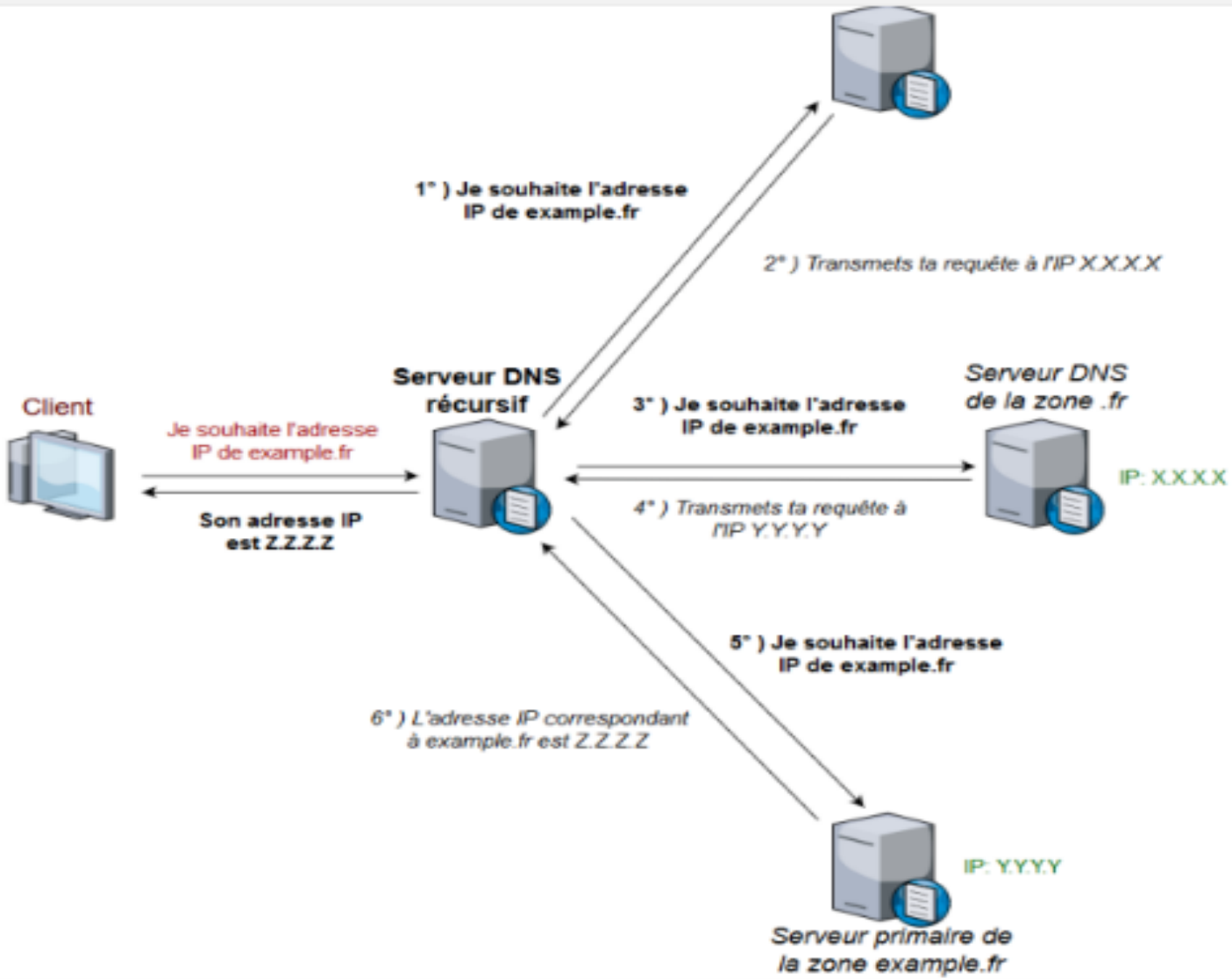
Les types de serveurs

- Les types de serveurs de noms faisant autorité
  - Chaque hôte est enregistré auprès d'au moins deux « authoritative server» (le primaire et le secondaire) qui stockent son adresse IP et son nom
  - Un serveur de nom est dit de source autorisée pour un hôte s'il est responsable de la correspondance nom/@IP pour cet hôte
  - Un serveur de nom local n'est pas forcément de source autorisée de premier niveau (.fr, .sn)

Les types de serveurs

- Le cache DNS
  - Réduire le temps de réponse d'une résolution de nom
  - Le serveur de nom stocke dans son cache les informations récentes (TTL d'environ 2 jours)
  - Un serveur DNS qui dispose d'un cache n'a pas autorité dessus : « no authoritative server»

Les types de serveurs



Principe et fonctionnement du serveur primaire

- Un serveur primaire fait autorité sur le contenu d'une zone
- Un serveur secondaire, normalement hébergé sur une autre machine
- Il se contente de proposer une copie de la zone primaire, qu'il met à jour régulièrement
- Chaque zone peut contenir différents types d'enregistrements (Resource Records)

Principe et fonctionnement du serveur primaire

Les types d'enregistrements

- **A**: attribution d'une adresse IPv4
- **CNAME**: définition d'un alias
- **MX**: définition d'un serveur de courrier électronique
  - Chaque enregistrement MX a une priorité associée
  - Le serveur de plus haute priorité porte le nombre le plus petit
- **PTR**: correspondance adresse IP vers nom
  - Elle est stockée dans une zone dédiée à la résolution inverse
  - Exemple 1.168.192.inaddr.arpa pour toutes les adresses du réseau 192.168.1.0/24
- **AAAA**:correspondance nom vers adresse IPv6
- **NS**:correspondance nom vers serveur de noms
  - Chaque domaine doit compter au moins un enregistrement NS

Configuration d'un serveur DNS privé sous Linux

- Le logiciel serveur de nom de référence, Bind, est développé par l'ISC (Internet Software Consortium, ou consortium du logiciel Internet)
- Debian le fournit dans le paquet bind9
- Trois fichiers à configurer principalement
  - Le fichier ***/etc/bind/named.conf.local***: contient la déclaration des zones
  - Le fichier ***/etc/bind/db.nom_domaine***: contient les correspondances @IP Noms
  - Le fichier ***/etc/bind/db.@IP_Réseau***: Contient la résolution inverse Noms @IP

Configuration d'un serveur DNS privé sous Linux

Exemple de fichier de déclaration ***/etc/bind/named.conf.local***

```
zone "falcot.com" {
        type master;
        file "/etc/bind/db.falcot.com";
        allow-query { any; };
        allow-transfer {
                195.20.105.149/32 ; // ns0.xname.org
                193.23.158.13/32 ; // ns1.xname.org
        };
};

zone "interne.falcot.com" {
        type master;
        file "/etc/bind/db.interne.falcot.com";
        allow-query { 192.168.0.0/16; };
};

zone "168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168";
        allow-query { 192.168.0.0/16; };
};
```

Configuration d'un serveur DNS privé sous Linux

Exemple de fichier de déclaration */etc/bind/db.nom_domaine*

```
; Zone falcot.com
; admin.falcot.com. => contact pour la zone: admin@falcot.com
$TTL    604800
@       IN      SOA     falcot.com. admin.falcot.com. (
                        20040121        ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
; Le @ fait référence au nom de la zone («falcot.com.» en l'occurrence)
; ou à $ORIGIN si cette directive a été employée
;
@       IN      NS      ns
@       IN      NS      ns0.xname.org.

interne IN      NS      192.168.0.2

@       IN      A       212.94.201.10
@       IN      MX      5 mail
@       IN      MX      10 mail2

ns      IN      A       212.94.201.10
mail    IN      A       212.94.201.10
mail2   IN      A       212.94.201.11
www     IN      A       212.94.201.11

dns     IN      CNAME   ns
```

Configuration d'un serveur DNS privé sous Linux

Exemple de fichier de déclaration ***/etc/bind/db.@IP_Réseau***

```
        IN      NS      ns.interne.falcot.com.

; 192.168.0.1 -> arrakis
1.0     IN      PTR     arrakis.interne.falcot.com.
; 192.168.0.2 -> neptune
2.0     IN      PTR     neptune.interne.falcot.com.

; 192.168.3.1 -> pau
1.3     IN      PTR     pau.interne.falcot.com.
```