DNS: Domain Name System

Plan

- **Introduction**
- **Bases universelles du DNS**
  - Les domaines de top niveau
  - La séparation en zones
  - Les composants d'une zone
  - La résolution itérative et récursive
- **Installation et configuration du serveur DNS**

Problématique

- Sur un réseau comme Internet une machine (ou un service) peut être identifiée par :
  - –Un Nom d'hôte
  - –Une adresse logique (IP)
- •En général, les utilisateurs ne connaissent que le nom des machines ou des services avec lesquels ils veulent communiquer.
- –Exemple pour un serveur web : www.univ-batna.dz
- •Les machines n'établissent leur communication qu'à l'aide de leurs adresses IP
- •Comment résoudre les noms de machines en adresses IP ?

Méthodes de Résolution du client

1. **A l'aide du fichier hosts.**

2. **En utilisant le service de résolution de noms : DNS (Domain Name System).**

Le fichier hosts Se retrouve sur tous les systèmes d'exploitation mettant en œuvre TCP/IP

- **Windows NT/2000/XP/Seven/8 : %system%\System32\Drivers\etc**
- **Linux : dans le dossier /etc**
- **Mac OS X : /etc**

Le fichier HOSTS

- Fichier éditable avec n'importe quel éditeur de textes
- Chaque entrée (ligne) contient une association IP-Nom de machine

- 193.194.69.34 www.univ-batna.dz
- 216.58.210.227 www.google.dz

Il existe une entrée par défaut :

- 127.0.0.1 localhost

Le fichier HOSTS

- •Avantages :
  - •Modifiable facilement
  - •Rapide (traitement local)
- Inconvénients :
  - •Difficile à mettre à jour pour Internet
  - •Pas de centralisation de l'information
  - •Informations non vérifiables

DNS : Domain Name System

- Les noms DNS sont appelés des URL (Uniform Resource Locator)
- •Une adresse URL est composée d'au minimum trois parties:
  - –Le Top-Level-Domain ou TLD (ex : fr)
  - –Le Second-Level-Domain (ex : src3)
  - –Le nom de l'hôte ou du service (www)
- Elle peut être complétée par des "Sub-Level-Domain" qui viennent s'intercaler entre le nom de l'hôte et le TLD
- Un nom de domaine ou d'hôte ne peut excédé 63 caractères
-
- Il ne peut y avoir plus de 127 niveaux de domaines.

DNS : Domain Name System

- L'ensemble des noms de domaine constitue un arbre inversé où chaque nœud est séparé du suivant par un point (".")
- Le nom absolu ou FQDN (Fully Qualified Domain Name) correspond à l'ensemble du nom de la machine terminé par un point final symbolisant la racine de cet arbre. (ex : www.univ-batna.dz.)
- La longueur maximale d'un nom FQDN est de 255 caractères.

- **Le DNS est une base de données distribuées**
  - utilisée par les applications réseaux pour effectuer les correspondances d'adresses IP et noms de machines sur l'Internet
  - **Exemple:**

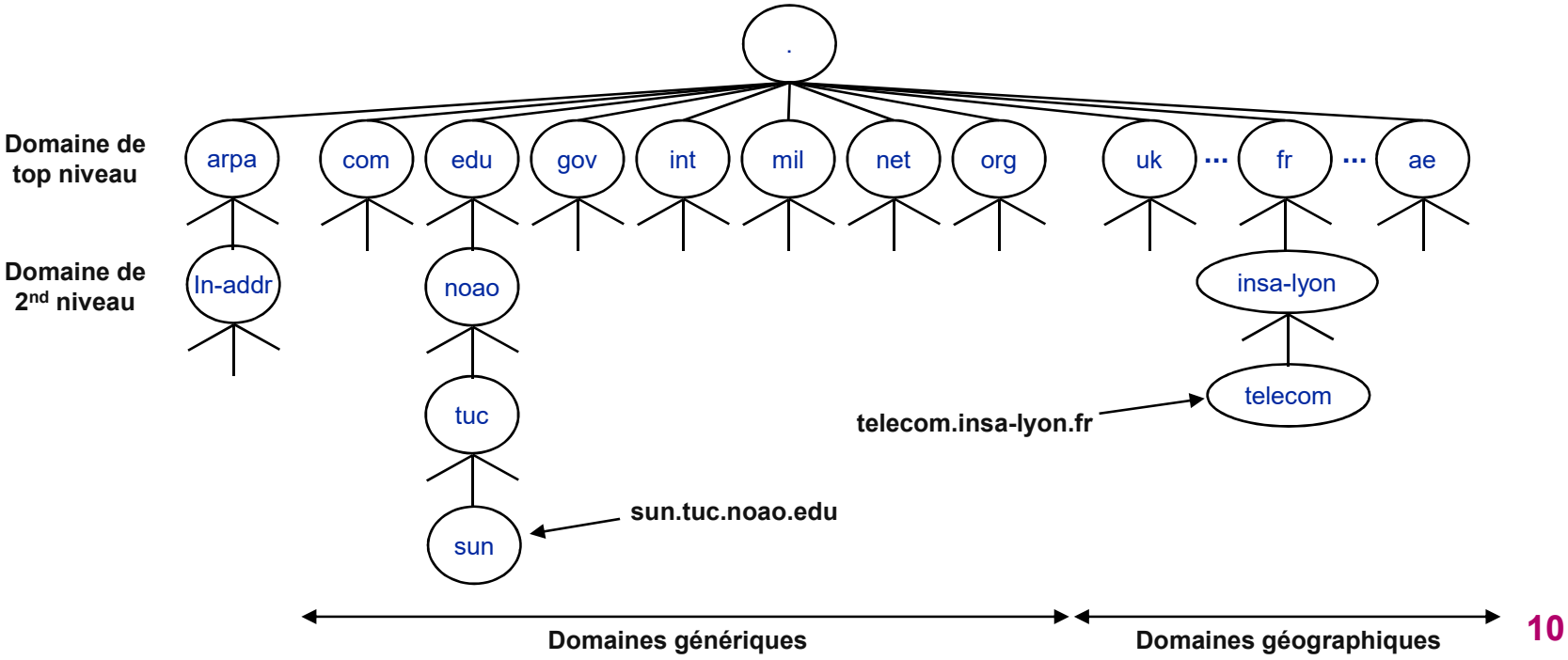
    Chaque site (département universitaire, campus, société, …) maintient sa propre **BD** d'informations et exécute un **Serveur** que les autres systèmes de l'Internet (**Clients**) peuvent interroger.

- **L'accès au DNS s'effectue à travers un Résolveur**
  - le **résolveur** est intégré au noyau du système d'exploitation
  - on accède au **résolveur** à travers des fonctions de librairies C ou Java intégrées à l'application lorsqu'elle est construite
  - le résolveur contacte un ou plusieurs serveurs de noms pour établir une correspondance (fonction de résolution)

- **RFC1034 :** spécifie les concepts et facilités procurés par le DNS
- **RFC1035 :** détaille l 'implémentation et la spécification
- **BIND** (Berkeley Internet Name Domain) est l'implémentation la plus couramment utilisée du DNS (le serveur est appelé **named**)

Bases universelles du DNS

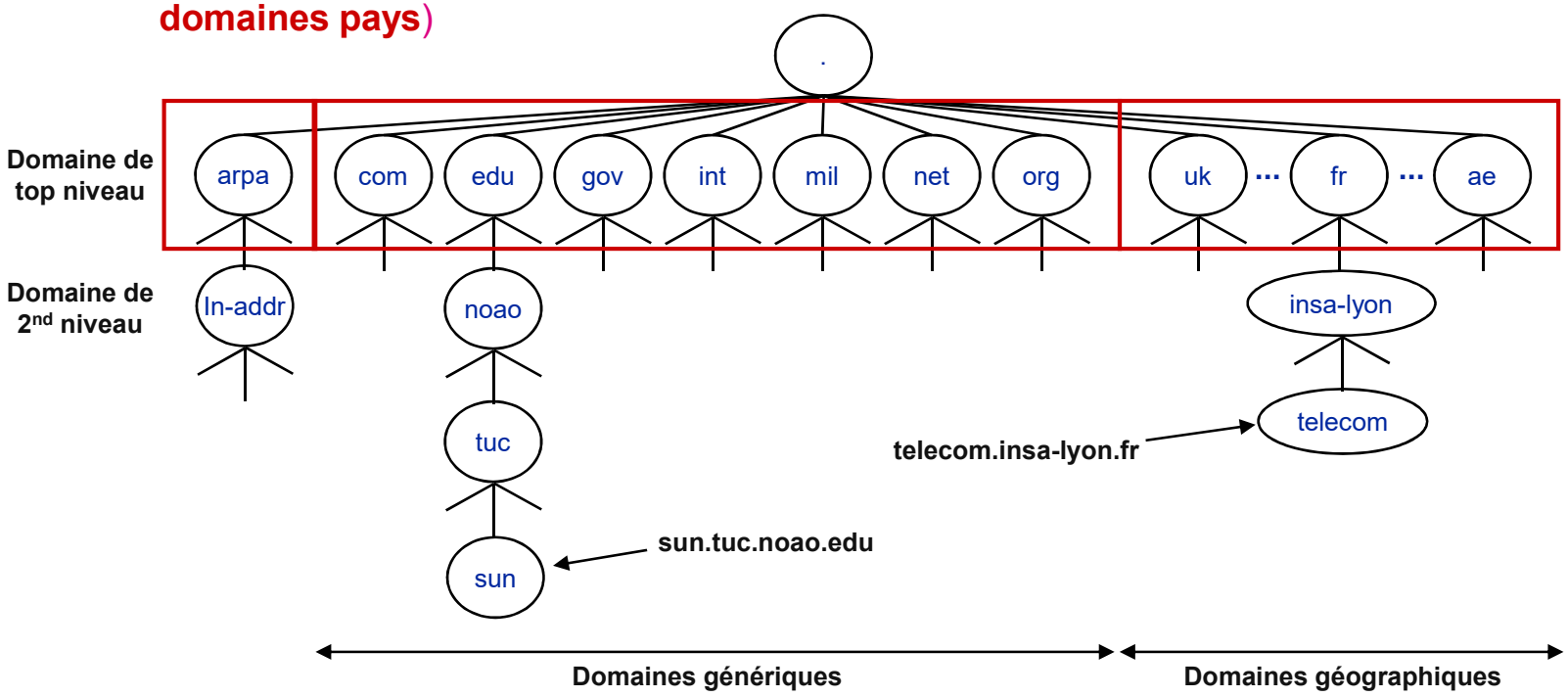
- **L'espace de noms DNS est hiérarchique** (équivalent au système de fichiers Unix)
  - chaque nœud a un label comprenant jusqu'à 63 caractères
  - la racine est un nœud spécial avec un label nul
  - aucune différence entre MAJUSCULES et minuscules
  - le nom de domaine de n'importe quel nœud de l'arbre est le résultat de la concaténation des labels à partir de nœud jusqu'à la racine
  - **exemple:** telecom.insa-lyon.fr



Les domaines de top niveau

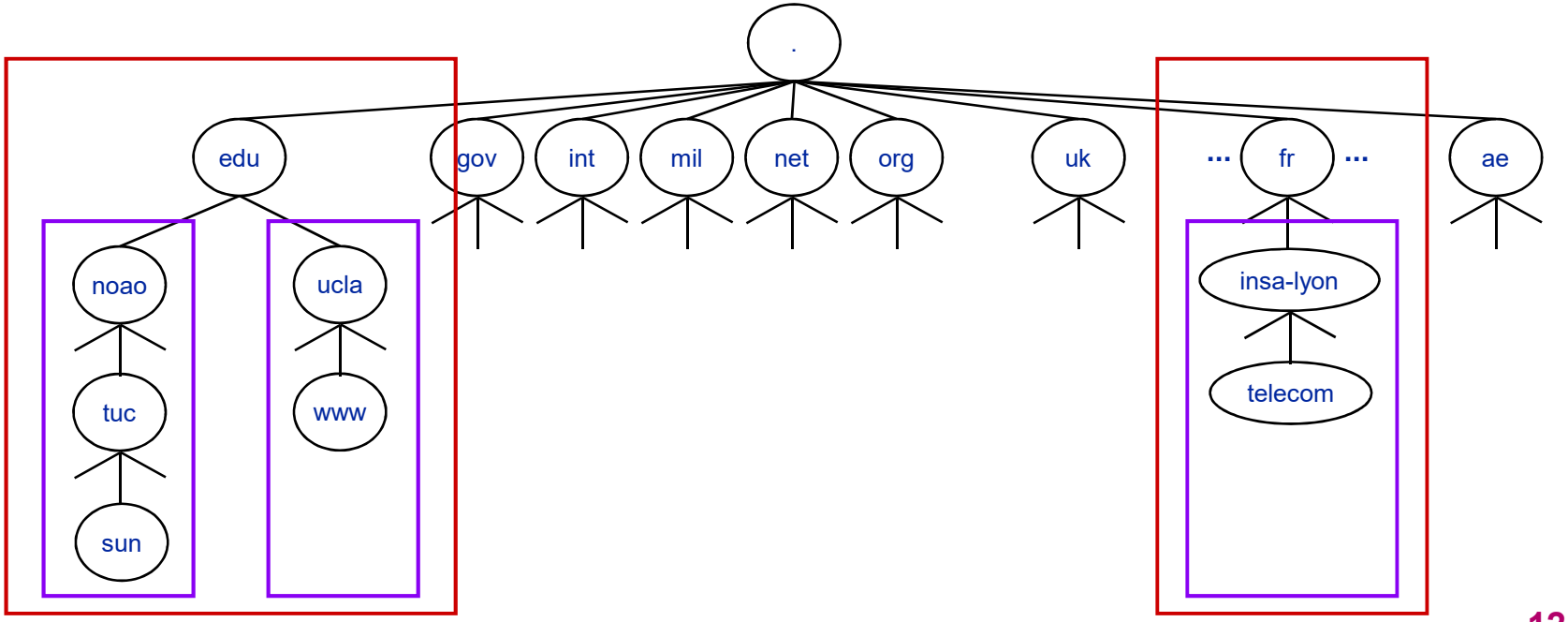
- **Les domaines de niveaux supérieurs sont divisés en 3 zones**
  - la **zone arpa** est un domaine spécial pour les correspondances d'adresses IP vers noms (géré par l'interNIC)
  - les sept domaines sur 3 caractères sont appelés **domaines génériques** (ou **domaines organisationnels**)
  - tous les domaines sur 2 caractères (codes pays ISO 3166) sont appelés **domaines géographiques** (ou **domaines pays**)

Domaine	Description
com	organisations commerciales
edu	institutions éducatives
gov	organisations gouvernementales US
int	organisations internationales
mil	militaire US
net	réseau
org	autres organisations



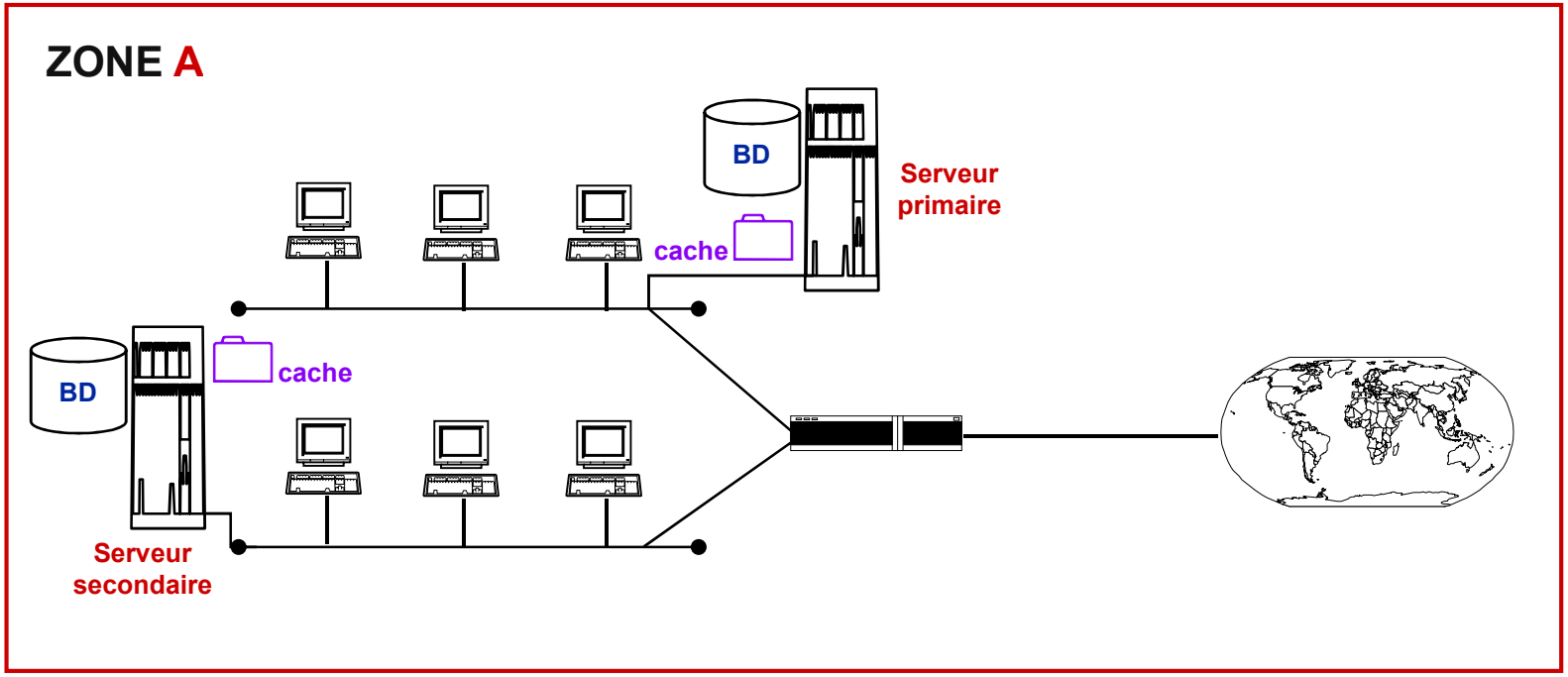
La séparation en zones

- **Une zone est un sous-arbre DNS administré séparément.**
- **Chaque zone est subdivisée en plusieurs sous-zones etc. …**
  - chaque sous-zone est administrée par une autorité séparément (administration hiérarchique)
- **Chaque racine de zone administre un serveur de noms**
  - la base de données du serveur de noms est mise à jour, par l'administrateur du DNS, à chaque introduction d'un nouveau système (machine) ayant une adresse IP et un nom



Les composants d'une zone

- **Une zone = 1 seule autorité administrative.**
- **Un serveur primaire**
  - charge les informations de résolutions à partir de fichiers stockés sur le disque
- **Un ou plusieurs serveurs secondaires**
  - récupèrent des copies de ses fichiers pour le recouvrement en interrogeant le primaire sur une base régulière (toute les 3h ou 4h en moyenne (fixée par l 'autorité))
- **Des caches**



Fonctionnement de DNS

- Le service est formé de deux composants :

- Le résolveur
- Le serveur DNS

LE RESOLVEUR

- C'est le client DNS.
- Il est installé en même temps que TCP/IP.
- Son rôle consiste à transmettre les requêtes des applications au serveur DNS et à récupérer les réponses.
- Il doit donc connaître l'adresse IP des serveurs DNS à interroger.

LE RESOLVEUR

PARAMETRAGE DU RESOLVEUR :

- Sous Linux : fichier /etc/resolv.conf
  Commande hostname et fichier HOSTS pour le nom local de la machine

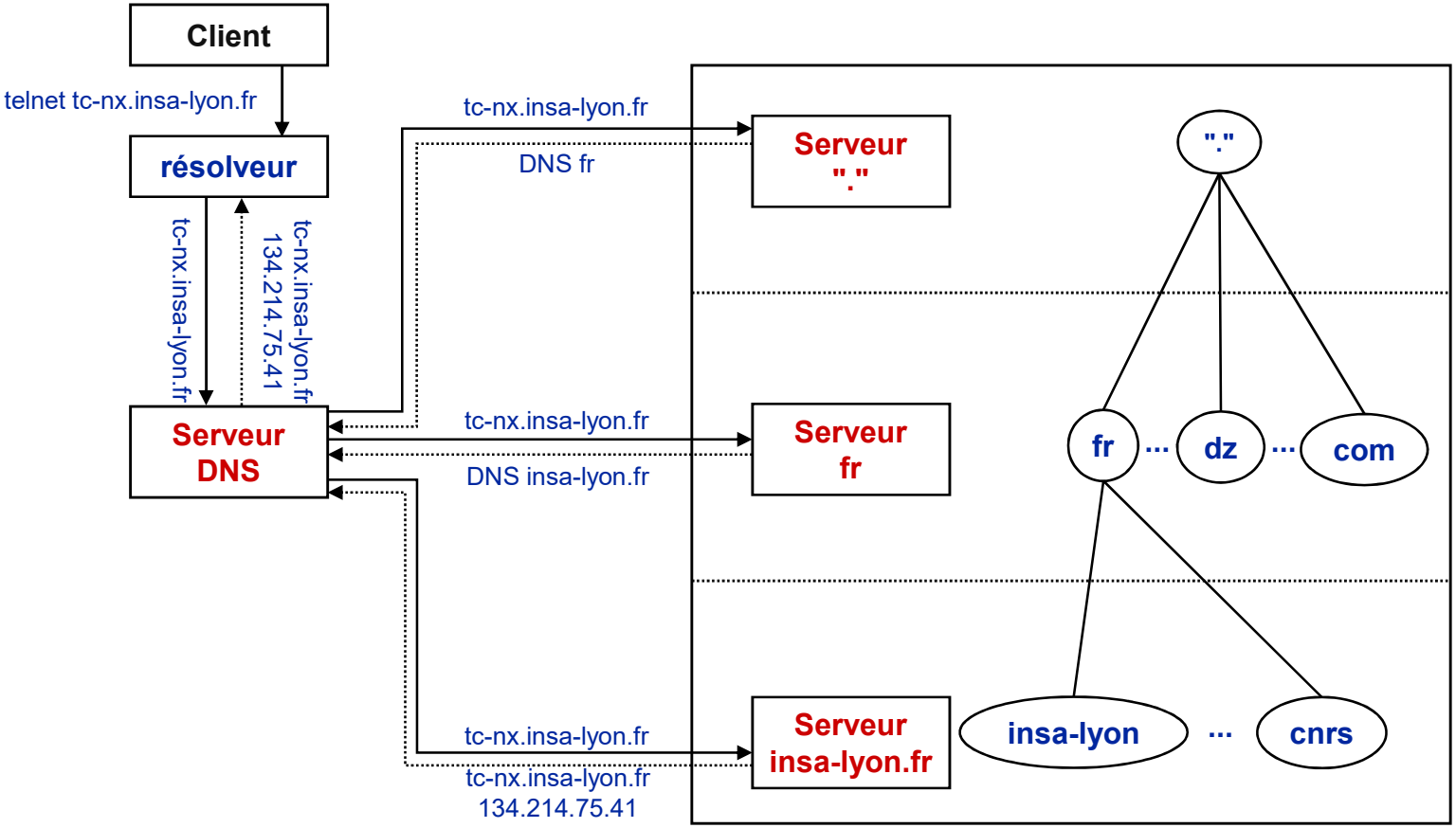
- Sous Windows : Dans les propriétés avancées de TCP/IP.

La résolution

- **Que fait le serveur lorsqu'il est interrogé pour une résolution ?**
- **Solution**
  - chaque serveur de noms doit savoir contacter les serveurs de noms racines (com, edu, fr, uk, …)
  - ces @IP des serveurs racines vont constituer les fichiers de configuration du serveur primaire
  - les serveurs racines connaissent ensuite les @IP et noms de chaque serveur de nom secondaire
- **Processus itératif (requête itérative)**
- **Processus récursif (requête récursive)**
- **Note:** la liste courante des serveurs racines se trouve sur les sites FTP anonymes ftp.rs.internic.net et nic.ddn.mil
  Le fichier s'appelle netinfo/root-servers.txt

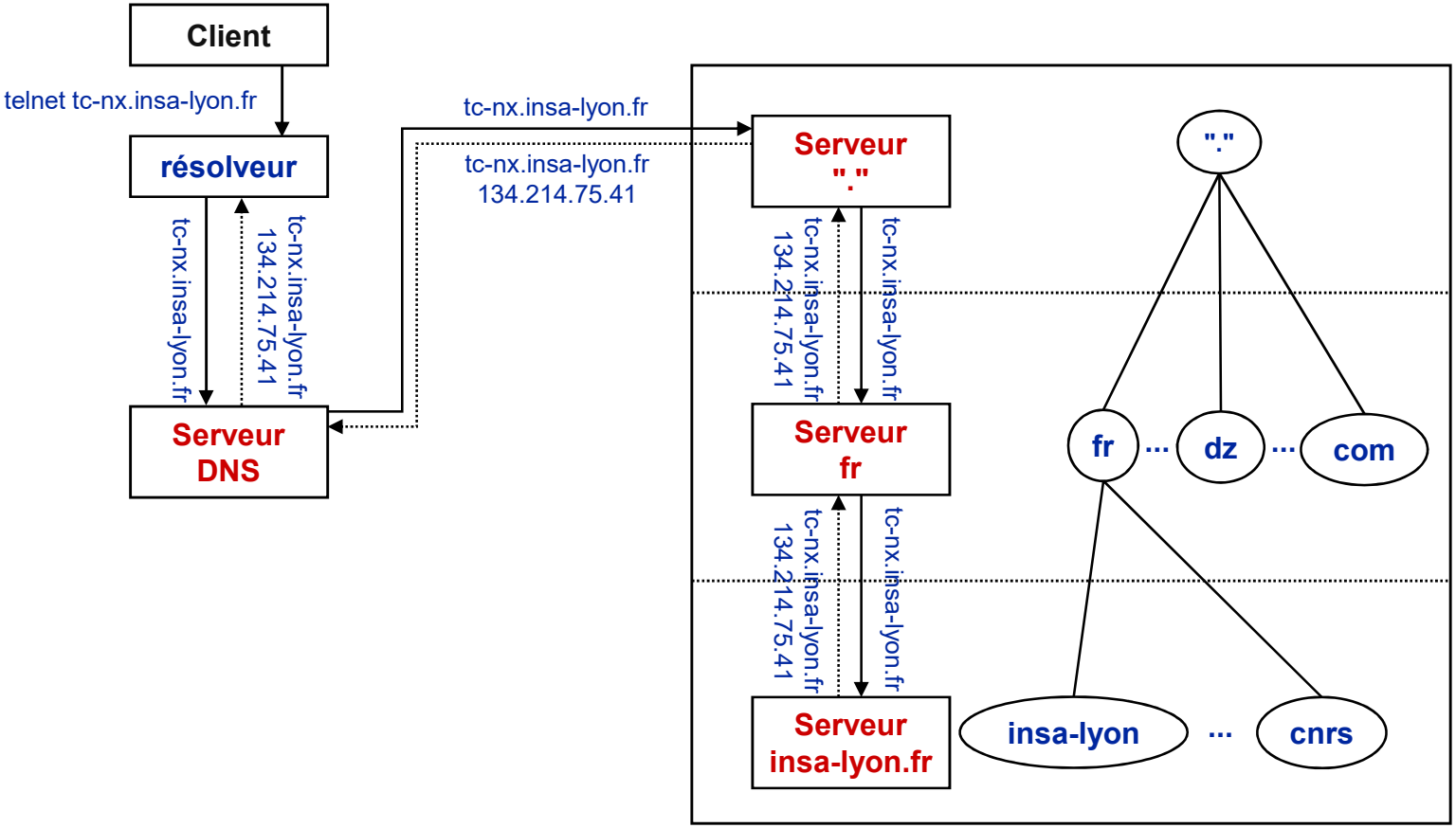
La résolution itérative

- Le serveur de noms demandeur doit contacter la racine
- Le serveur racine donne au serveur demandeur une adresse d'un autre serveur de noms à contacter, etc. …



La résolution récursive

- Le serveur de noms demandeur doit contacter la racine
- Le serveur racine demande la résolution au serveur du sous-domaine juste en dessous de la hiérarchie
- etc. …



UDP ou TCP ?

- **Un serveur DNS fonctionne sur le port 53**
- **Les clients et Serveurs DNS supportent à la fois UDP et TCP pour le transport.**
- **UDP est utilisé de façon primaire**
- **TCP est utilisé uniquement lorsque:**
  - la réponse à la requête est reçue tronquée
  - le serveur secondaire récupère au démarrage la base de données de noms à partir du serveur primaire
  - au rafraîchissement du serveur secondaire (par intervalle de fréquence donné)
- **Un exemple de client DNS sous Unix:** nslookup

```
[C:\Documents and Settings\intel>nslookup
Serveur par dÚfaut :  google-public-dns-a.google.com
Address:  8.8.8.8

> www.univ-batna.dz
Serveur :  google-public-dns-a.google.com
Address:  8.8.8.8
Nom :    univ.univ-batna.dz
Address:  193.194.69.34
Aliases:  www.univ-batna.dz

> mail.univ-batna.dz
Serveur :  google-public-dns-a.google.com
Address:  8.8.8.8
Nom :    mail.univ-batna.dz
Address:  193.194.69.43

> www.google.fr
Serveur :  google-public-dns-a.google.com
Address:  8.8.8.8

Nom :    www.google.fr
Address:  216.58.210.195

> www.google.dz
Serveur :  google-public-dns-a.google.com
Address:  8.8.8.8

Nom :    www.google.dz
Address:  216.58.210.227
```

SERVEUR DNS

PARAMETRAGE DU SERVEUR DNS :

- Le système DNS est basé sur une base de données répartie.
- Chaque serveur est responsable des noms et des adresses IP appartement à un domaine d'adressage particulier (ex : iim.net)
- Si un serveur n'est pas en mesure de résoudre un nom, il doit être capable de transmettre la requête à un serveur capable de l'exécuter.

ZONE D'AUTORITE

- Chaque serveur DNS est responsable d'une zone d'autorité
- Cette zone correspond à son espace de dénomination (ex : Un serveur à autorité sur la zone iim.net)
- Cette zone contient les noms et les adresses IP de toutes les machines et services du domaine géré

TYPE DE SERVEURS DNS

- **Primaire:** C'est sur ce serveur que sont effectuées les mises à jours. C'est le serveur principal de la zone

- **Secondaire:** Ce serveur possède une copie du fichier de zone du serveur primaire. Il ne peut être qu'interrogé et n'accepte aucune mises à jour directes

- **"Cache-Only" :** Ce serveur ne dispose d'aucune zone d'autorité. Son rôle consiste uniquement à transmettre les demandes issues des clients vers les serveurs d'autorités et à enregistrer les informations pour pouvoir les réutiliser. Il accélère ainsi les requêtes suivantes portant sur les mêmes noms de machines.

SERVEUR DNS

L'installation d'un serveur DNS nécessite un système d'exploitation de type Unix/Linux ou Windows Serveur :

- Sous Windows, le serveur DNS est exécuté comme un service. Il est paramétrable à l'aide d'une interface graphique.

- Sous Linux, il est nécessaire d'installer un "package". Le plus connu est BIND9. Son paramétrage se fait généralement en éditant les fichiers textes de configuration, mais peut aussi être fait à l'aide de l'outil Webmin

SERVEUR DNS

- Que ce soit sous Windows ou Linux, la configuration des serveurs DNS est construite autour de plusieurs fichiers :

- named.conf ou named.boot Contient la description des zones et le rôle du serveur sur celles-ci
- Des fichiers .rev et .hosts qui contiennent la description de chaque zone

named.conf.local

```
zone "dom99.net" IN {
type master;
 file "dom99.hosts";
 };

zone “99.168.192.in-addr.arpa" {
 type master;
 file "dom99.rev";
 };

zone "a203.net" {
type slave ;
masters {172.16.0.1;} ;
file "a203.hosts" ;
} ;

zone "dom20.net" {
type slave ;
masters {192.168.20.2;} ;
file "dom20.hosts" ;
} ;
```

Zone primaire pour le domaine dom99.net

Zone inverse pour le réseau 192.168.99.0

Zone secondaire pour le domaine a203.net
Le serveur maitre se trouve à l’adresse 172.16.0.1

Zone secondaire pour le domaine dom20.net
Le serveur maitre se trouve à l’adresse 192.168.20.2

Fichier de zone

```
$TTL 86400
dom99.net. IN SOA debian.dom99.net. root.dom99.net (
123;
604800;
86400;
2419200;
86400 );
dom99.net.          IN NS debian.dom99.net.
dom99.net.          IN MX 100 debian.dom99.net.
debian.dom99.net.           IN A 192.168.99.2
poste.dom99.net.            IN A 192.168.99.3
www                 IN CNAME debian.dom99.net.
ftp                 IN CNAME debian.dom99.net.
mail                IN CNAME debian.dom99.net.
```

- $TTL 86400 Durée (en s) de conservation des enregistrements dans le cache (sans relire le fichier)
- IN Désigne la classe utilisée pour nommés les enregistrements dans la base (IN=INTERNET)
- SOA Enregistrement désignant la zone décrite dans ce fichier. Les valeurs numériques désignent le n° de série du fichier suivi de délais de mise à jour pour les serveurs secondaires.
- NS (NAME SERVER) : Désigne le serveur DNS gérant la zone
- MX (MAIL EXCHANGE) : Désigne le serveur de messagerie du domaine
- A (ADDRESS) : Désigne l'adresse IP d'une machine
- CNAME (COMMON NAME) : Désigne un alias pouvant se substituer au nom de la machine.
- PTR (POINTER): Désigne le nom d'une machine en partant de son adresse IP (inversée)

DNS et IP Dynamique

Problématique :

- **Comment associer l'ip publique de votre connexion ADSL à un nom de domaine ?**
- **Pourquoi le faire ?**
- **Héberger vos services réseaux (web, ftp,mails)et les rendre accessibles depuis Internet.**
- **Accéder à vos serveurs à distance.**

DNS et IP Dynamique

Solution:

- **Utiliser un service de DNS Dynamique**
- **Ces services souvent disponibles sur vos "BOX" permettent d'avoir une zone DSN mise à jour automatiquent via :**
  - **•Un utilitaire fournit par le prestataire.**
  - **•Un script**
  - **•Des API vous permettant de développer votre propre système de mise à jour.**

- **Quelques services connus :**
  - **•DynDNS**
  - **•NoIP**
  - **•DtDNS**
  - **•DyDNS**
  - **•FreeDNS**