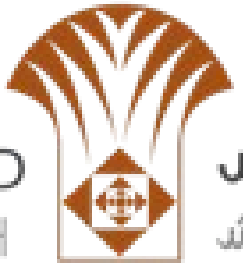


UNIVERSITE CADI AYYAD
MARRAKECH

جامعة القاضي عياض
مراكش

ENSA
Safi

Administration Réseau Avancée sous GNU/Linux

Mohammed Madiafi
Département Informatique, Réseaux et Télécoms

DNS

- 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.

DNS

- 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.
- Deux cas sont possibles :
  - L'adresse du serveur DNS est renseignée de manière statique dans les fichiers de configuration.
  - L'adresse du serveur DNS est affectée par un serveur DHCP.

DNS
Domain Name Server

- Le service DNS = service de résolution de noms de domaine.
- Il permet d'adresser un hôte par un nom, plutôt que de l'adresser par une adresse IP.
- Structure d'un nom d'hôte :
  - NomHôte**.**NomDomaine
  - serveur**.**ensas.ma

Domaine

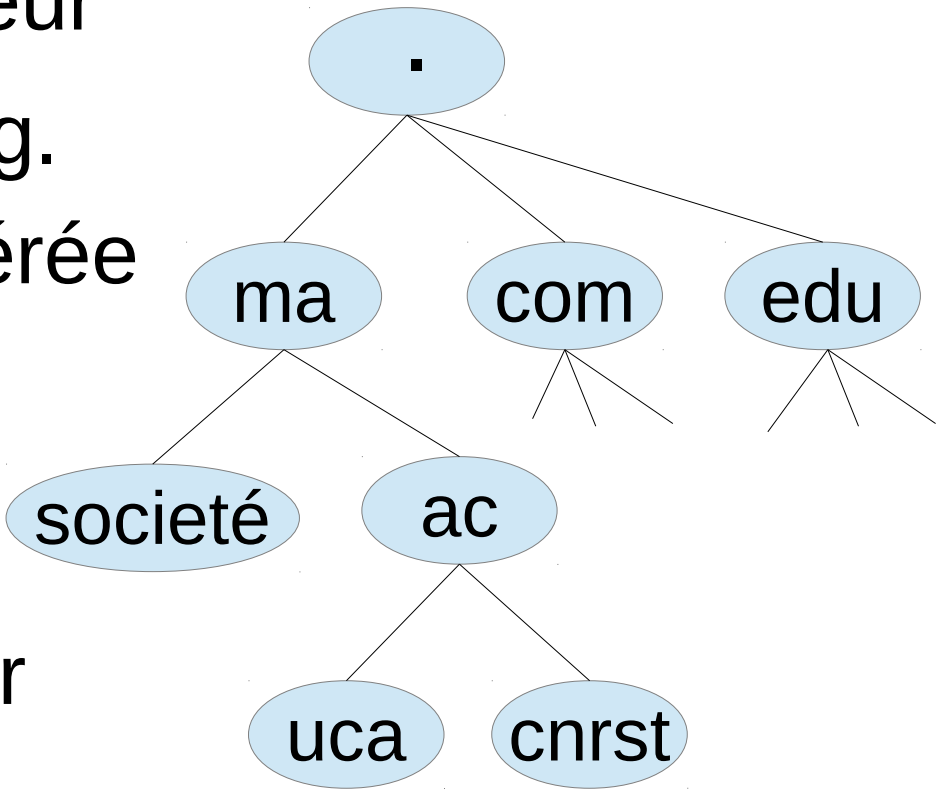
- Un domaine est un sous-arbre de l'espace de nommage.
  - Exemple : .com est un domaine, il contient toute la partie hiérarchique inférieure de l'arbre sous jacente au noeud .com.
- Un domaine peut être organisé en sous domaines.
  - Exemple : .google.com est un sous domaine du domaine .com.

Nom de domaine

- Le nom de domaine identifie une organisation dans l'internet
  - Exemple : google.fr, yahoo.com, etc.
- Chaque organisation dispose d'un ou plusieurs réseaux. Ces réseaux sont composés de noeuds (postes, serveurs, routeurs, imprimantes) pouvant être adressés.
  - Exemple : « ping serveur.ensas.ma » permet d'adresser la machine qui porte le nom d'hôte « serveur », dans le domaine (organisation) « ensas.ma ».

Zones DNS

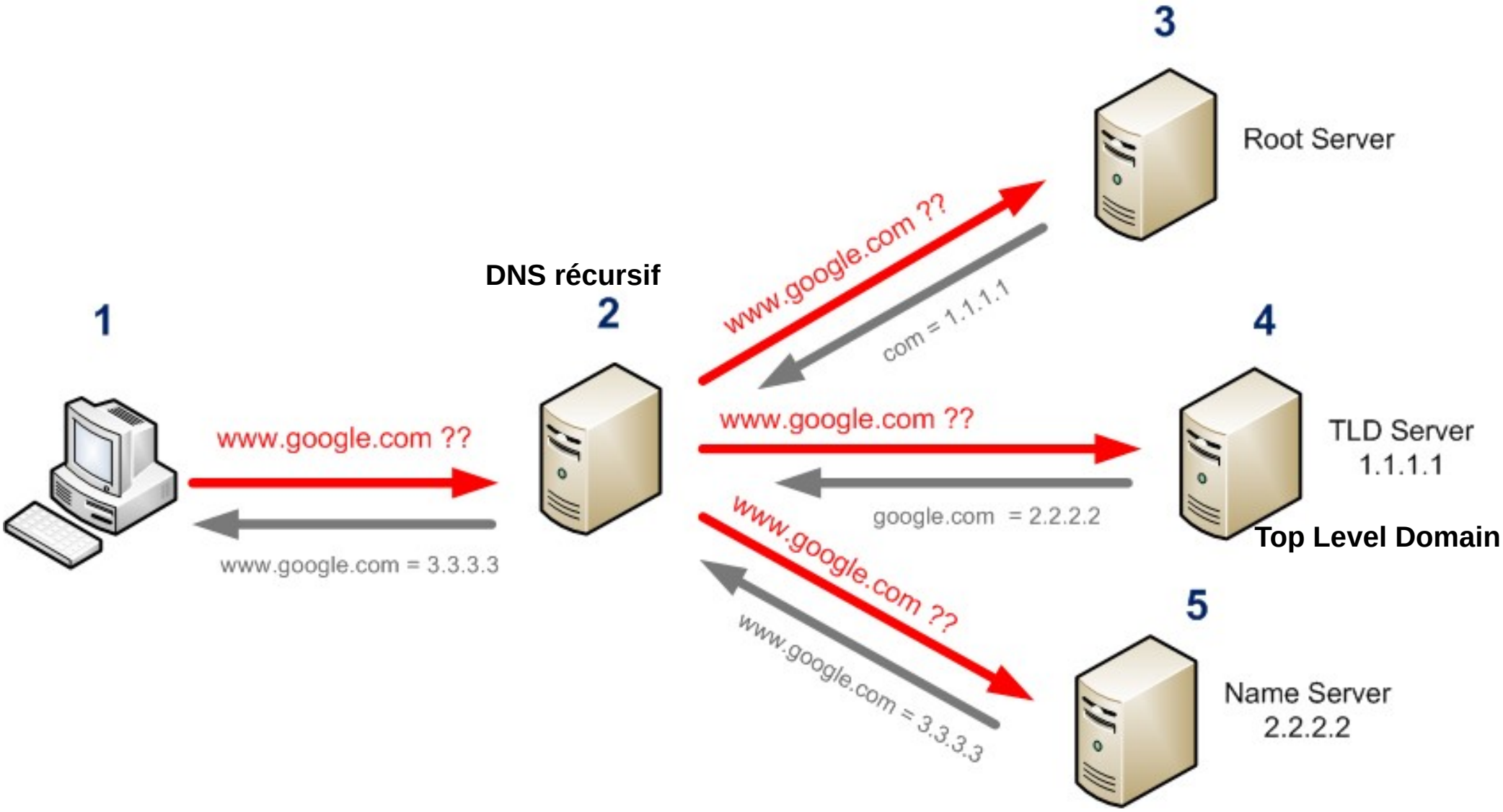
- Chaque niveau de l'arborescence DNS est une zone DNS.
- La zone « . » est la racine qui contient tous les niveaux de niveau supérieur
  - tels que com, ma, fr, org.
- Chaque zone peut être gérée par un serveur.
  - Le serveur hébérgeant les données de la zone « ac » est consulté pour résoudre tout nom se terminant par « ac.ma ».



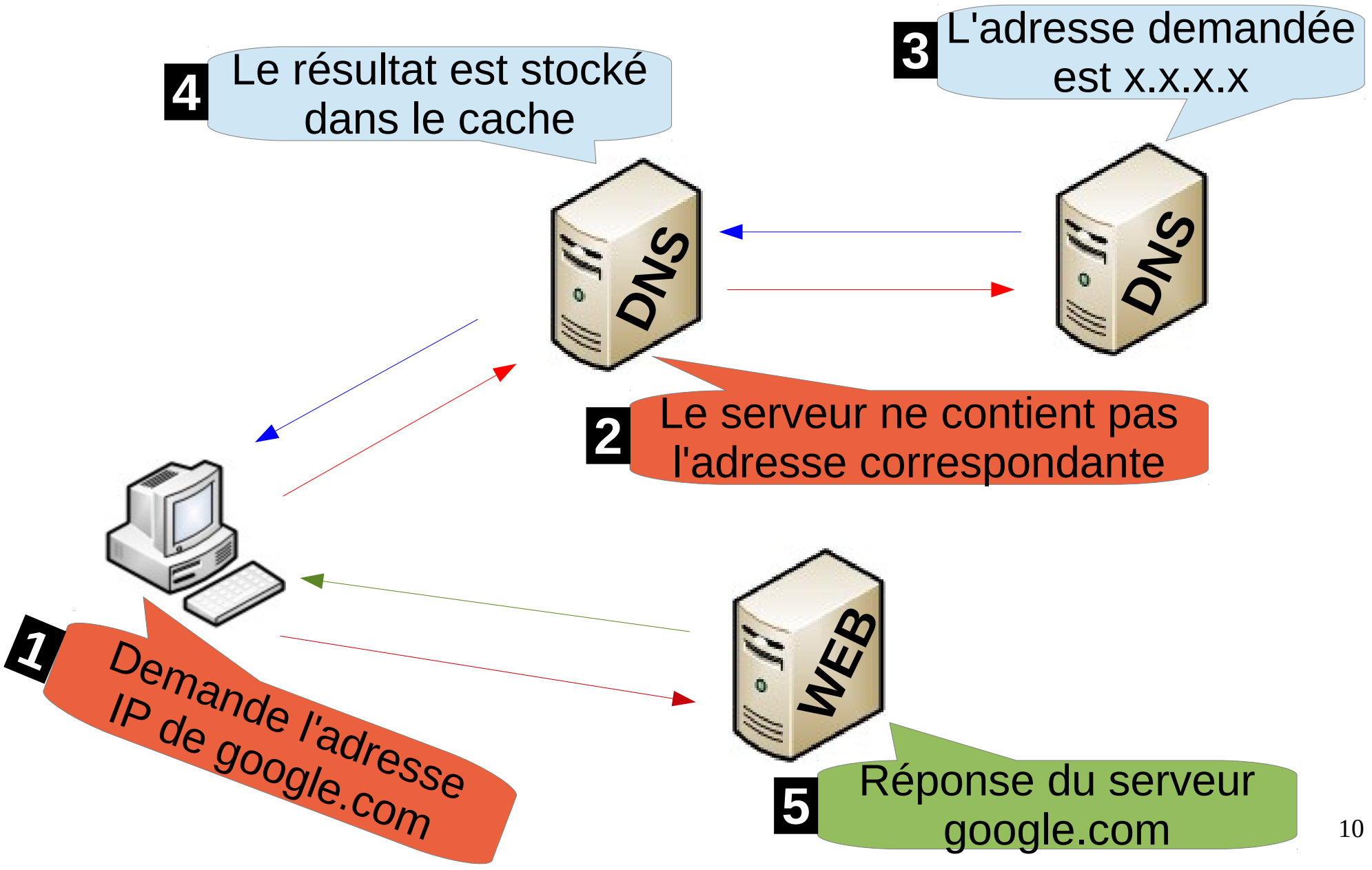
Mécanisme de résolution de noms

- Une application demandant une résolution de nom s'adresse au « resolver » du système d'exploitation.
- Le resolver envoie une requête à un serveur DNS local référencé dans un fichier de configuration.
- Si le serveur interrogé dispose de l'information demandée, il répond directement.

Mécanisme de résolution de noms



Mécanisme de résolution de noms



Enregistrements

- Les enregistrements sont des informations permettant de correspondre un nom à une adresse IP ou à une autre information.
- Dans les fichiers de configuration d'un serveur DNS, on utilise des noms de domaines pleinement qualifiés (FQDN : Fully Qualified Domain Name)
  - Exemple : « www.google.com. » : www est représenté par un enregistrement dans la zone google.com. La présence du point après com est obligatoire.

Enregistrement de type A

- L'enregistrement qui fait correspondre une adresse IP à un nom.
  - www.google.com est un enregistrement de A dans la zone google.com.
  - Il correspond au serveur Web hébérgeant la page d'accueil google.
- Syntaxe :
  - www IN A 196.12.217.53

Enregistrement de type AAAA

- Fait correspondre un nom à une adresse IPv6
- Syntaxe :
  - www IN AAAA
    2001:670 :12:234a:24:16bb:ab21:1234

Enregistrement de type PTR

- Un enregistrement PTR permet de faire l'inverse de A.
- C'est à dire la résolution inverse.
- Il existe dans des zones particulières nommées « in-addr.arpa »
- Syntaxe : Zone 168.192.in-addr.arpa
  - 9.10 IN PTR serveur1.domaine.fr

    (ça veut dire que l'adresse de serveur1.domaine.fr) est 192.168.9.10.

Enregistrement de type CNAME

- CNAME : Canonical Name
- Ceci permet de correspondre à un nom un autre nom ou alias.
- Syntaxe :
  - Serveur1 IN CNAME imprimantes

Enregistrement de type MX

- MX (MAIL EXCHANGE) : Indique le serveur de messagerie pour le domaine
- Ça permet de faire savoir à des agents de transfert de messagerie quel est le serveur destinataire final d'un courrier.
- Syntaxe : Zone domaine.fr
  - mail IN MX 192.168.9.100

    (un message envoyé à une adresse se terminant par @domaine.fr sera dirigé au serveur mail.domaine.fr)

Enregistrement de type SOA

- SOA (START OF AUTHORITY) : Détermine le serveur ayant la responsabilité de la zone.
- Toute zone fonctionnelle a un enregistrement SOA.
- Syntaxe :
  - Domaine.fr. IN SOA ns.hebergeur.fr

Enregistrement de type NS

- NS (NAME SERVER) : indique les serveurs de noms pour la zone.
- Toute zone fonctionnelle a au moins un enregistrement NS.
- Syntaxe :
  - Domaine.fr. IN NS ns.hebergeur.fr

BIND
Berkeley Internet Name Domain

- Le paquet logiciel « bind » comporte le démon « named » qui répond aux requêtes DNS.
- Sur le client, il existe un ensemble de bibliothèques permettant la résolution de nom en intérogeant un serveur DNS.
  - dig
  - nslookup
  - host

Installation

- Côté serveur :
  - apt-get install bind9
- Côté client :
  - apt-get install dnsutils

Exemple de zone directe

- $TTL 86400
- pas.net. IN SOA serv.pas.net. root.pas.net. (
  2 ;serial
  604800 ;refresh
  86400 ;retry
  2419200 ;expire
  86400 ;negative)
- pas.net. IN NS serv.pas.net.
- serv.pas.net. IN A 192.168.9.100
- web IN CNAME serv.pas.net.

Exemple de zone directe

- Numéro de série (serial) : Identifie la version de la zone ; quand on modifie le fichier de zone, on incrémente ce numéro. Le format conseillé est le suivant : YYYYMMDDxx.
- Rafraîchissement (refresh) : intervalle en secondes destiné au serveur secondaire pour rafraîchir son fichier de zone (nombre décimal entier sur 8 chiffres).

Exemple de zone directe

- Tentatives (retry) : intervalle en secondes avant de recontacter le serveur principal en cas d'échec de la demande de rafraîchissement.
- Expiration (expire) : indique le temps en secondes, au bout duquel un serveur secondaire doit éliminer toutes les informations de zone s'il n'a pas pu contacter le serveur (cette valeur doit être élevée).

Exemple de zone inverse

- $TTL 86400
- 168.192.in-addr.arpa. IN SOA serv.pas.net. root.pas.net. (

  2 ;serial

  604800 ;refresh

  86400 ;retry

  2419200 ;expire

  86400 ;negative)
- 168.192.in-addr.arpa. IN NS serv.pas.net.
- 100.9 IN PTR serv.pas.net.

Configuration (côté client)

- /etc/resolv.conf
  - Nameserver 1.1.1.1
  - Nameserver 2.2.2.2
  - Nameserver 3.3.3.3