Les services d'annuaire
DHCP et DNS

Christian Bulfone
christian.bulfone@gipsa-lab.fr
www.gipsa-lab.fr/~christian.bulfone/MIASHS-L3

Master MIASHS L3
Année 2024/2025

Notion d'annuaire

- Définition
  - Tout service permettant d'obtenir des informations à partir d'une base, centrale ou répartie
- Apporte un confort non négligeable
  - aux utilisateurs (DNS)
  - à l'administrateur réseau (DHCP)
- Peuvent généralement être gérés
  - soit par plusieurs serveurs simultanément
  - soit par un serveur principal et par un ou plusieurs serveurs secondaires qui en prennent le relais en cas de défaillance

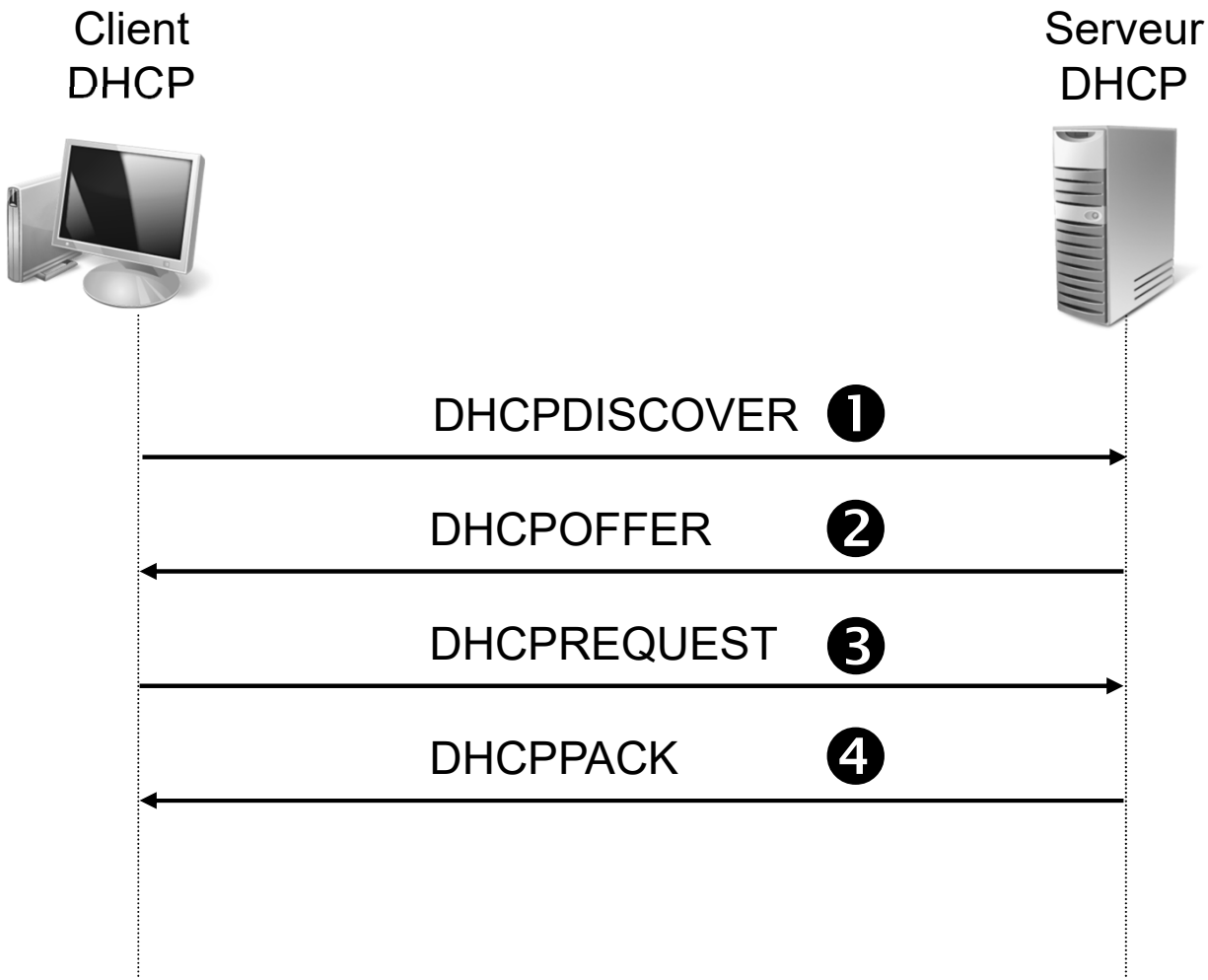
DHCP

- *Dynamic Host Configuration Protocol* (RFC 2131)
- Conçu comme une extension du protocole BOOTP (*Bootstrap Protocol*)
- Protocole fonctionnant en client/serveur
- S'appuie sur UDP (ports 67 et 68)
- Permet la configuration automatique des paramètres TCP/IP (adresse IP, masque, gateway …) des différents hôtes du réseau

Méthodes d'allocation des adresses

- 3 méthodes d'allocation
  - **Allocation manuelle** : attribution par le serveur DHCP d'une adresse IP définie par l'administrateur
  - **Allocation automatique** : attribution automatique par le serveur DHCP d'une adresse IP dans un pool d'adresses disponibles
  - **Allocation dynamique** : attribution par le serveur DHCP d'une adresse IP d'un pool d'adresses définies pour une certaine durée (bail)

Configuration d'un client DHCP



Configuration d’un client DHCP

❶ Le client (d’adresse IP inconnue 0.0.0.0) envoie une requête DHCPDISCOVER en broadcast (255.255.255.255) dans laquelle il insère son adresse MAC

❷ Les serveurs DHCP répondent en proposant une adresse IP avec une durée de bail et leur adresse IP de serveur (DHCOFFER)

❸ Le client sélectionne la première adresse IP (s'il y a plusieurs serveurs DHCP) reçue et envoie en broadcast une demande d'utilisation de cette adresse au serveur DHCP (DHCPREQUEST)

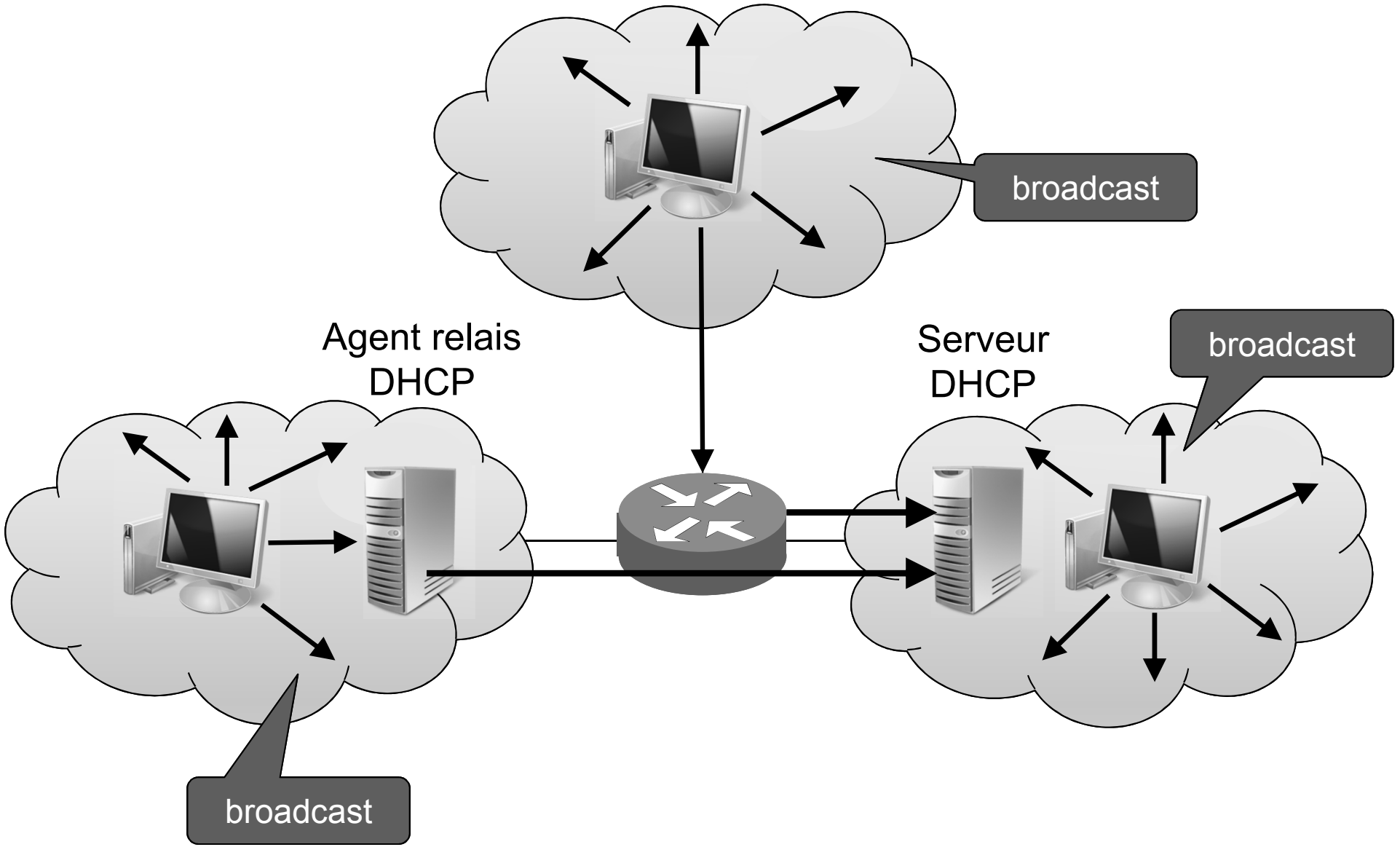
- Le message comporte l'identification du serveur sélectionné qui est informé que son offre a été retenue
- Tous les autres serveurs DHCP retirent leur offre et les adresses proposées redeviennent disponibles (allocation dynamique)

❹ Le serveur DHCP accuse réception de la demande et accorde l'adresse en bail (DHCPACK), les autres serveurs retirent leurs propositions

DHCP relais

- Les clients contactant les serveurs DHCP par *broadcast*, en présence de (sous-)réseaux routés, un serveur DHCP doit théoriquement être installé par (sous-)réseau
- Un routeur prenant en charge la RFC 1542 peut faire office d'agent de relais DHCP c'est-à-dire relayer les broadcast dans chaque sous-réseau
- Dans le cas contraire une machine serveur peut être configurée comme agent de relais DHCP
  - L'agent doit connaître l'adresse du serveur DHCP mais ne peut pas être lui-même client DHCP
  - Les demandes des clients DHCP sont relayées vers le serveur DHCP par l'agent qui transmettra les offres aux clients

DHCP relais

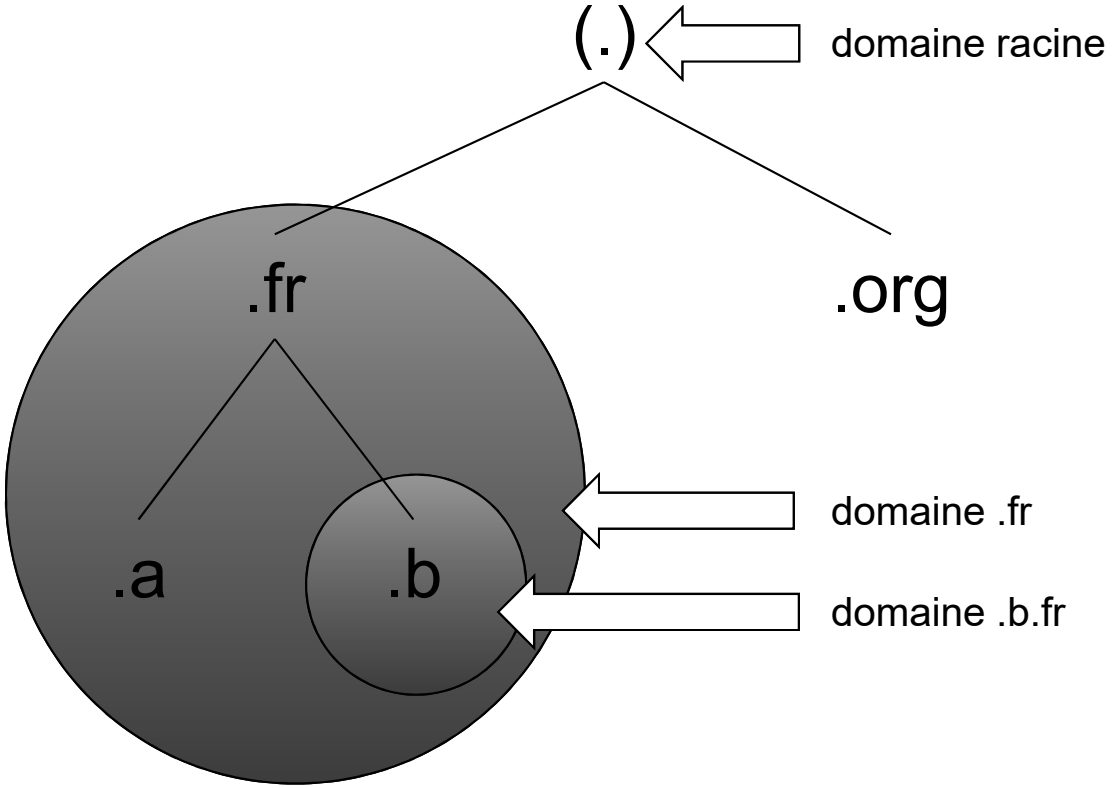

broadcast
Agent relais
DHCP
Serveur
DHCP
broadcast
broadcast

Le DNS

- Le *Domain Name System* est l'annuaire le plus ancien et certainement le plus utilisé
  - Conçu en 1983 à la demande de la DARPA
- Permet de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresse IP
- Construit sous la forme d'une structure arborescente

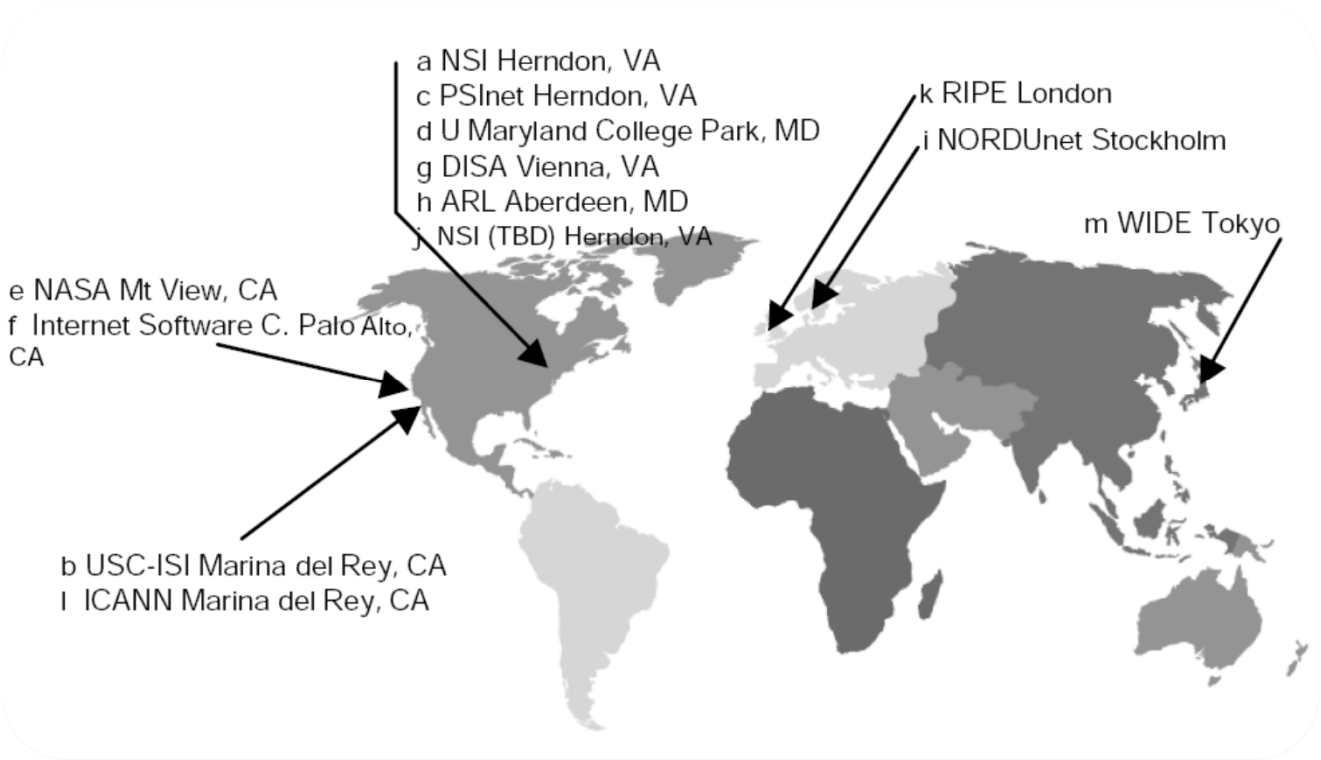
Notion de domaine

- Un « domaine » est un sous-arbre de l'espace de nommage
  - Le sommet, la racine est représentée par un « . »
  - Un domaine peut être organisé en sous domaines



Notion de domaine

- Les 13 serveurs racine sont gérés par des organisations différentes
  - 2 européennes, 1 japonaise et 10 américaines
  - Certains serveurs DNS racine sont en fait de grosses grappes de serveurs utilisant *anycast* (technique d'adressage et de routage permettant de rediriger les données vers le serveur informatique le "plus proche" ou le "plus efficace" selon la politique de routage)



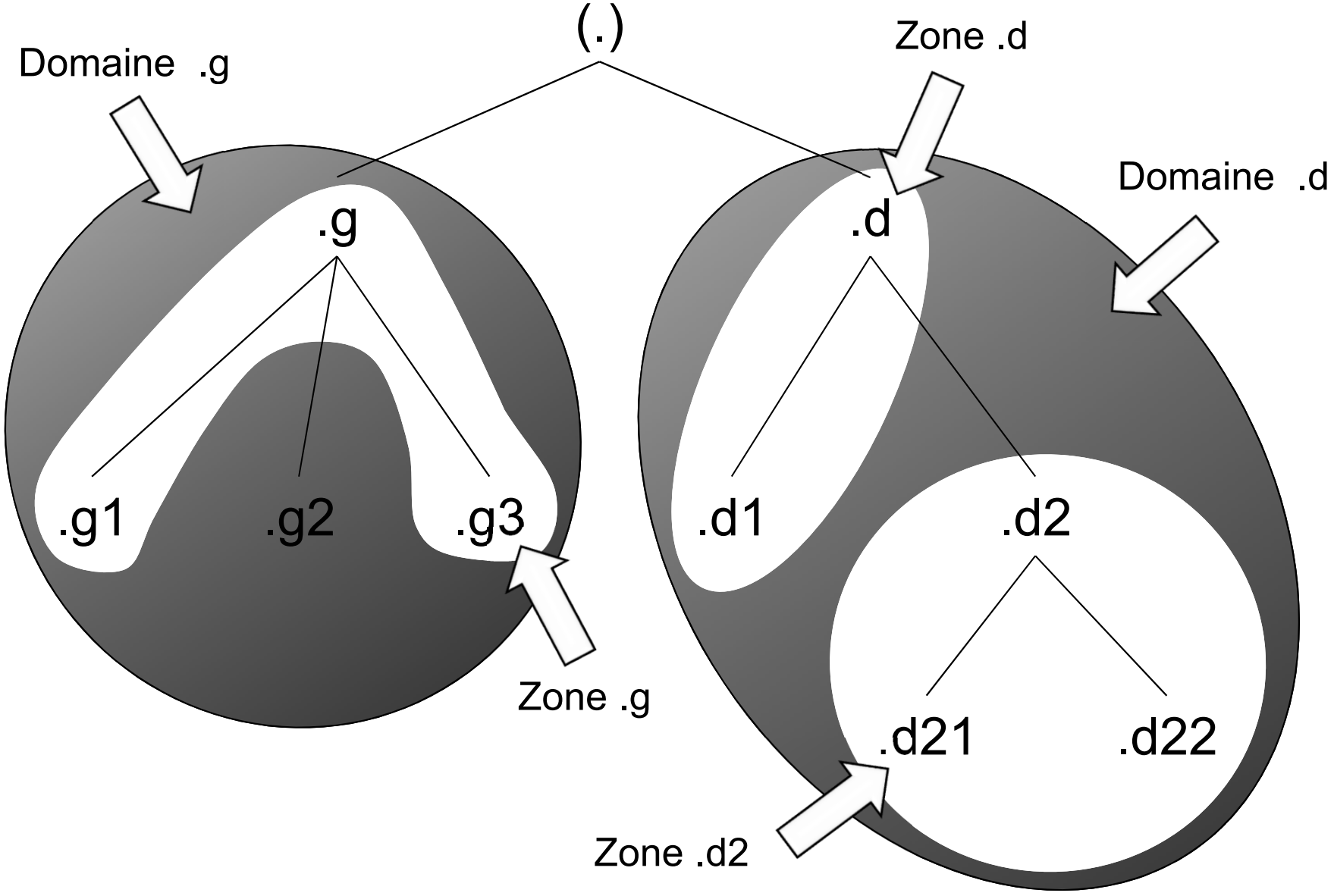
Notion de domaine

- Les domaines se trouvant immédiatement sous la racine sont appelés *domaine de premier niveau* (TLD : *Top Level Domain*)
- Les noms de domaines ne correspondant pas à une extension de pays sont appelés des *domaines génériques* (*generic TLD*)
  - org, com, …
- Les noms correspondant à des codes de pays sont appellés ccTLD (*country code TLD*)
  - fr, be, ch, …

Notion de zone et de délégation

- Une « zone » est une organisation logique (plus précisément une organisation administrative) des domaines
  - Le rôle d'une zone est principalement de simplifier l'administration des domaines
  - L'administration des zones est **déléguée** afin de simplifier la gestion globale du domaine

Domaines et zones DNS



Délégation de zones

- Consiste à déléguer l'administration d'une zone (ou une sous-zone) aux administrateurs de cette zone
- Les serveurs de noms disposent de toutes les informations de la zone
- Les serveurs de noms font **autorité** sur une ou plusieurs zones

En résumé …

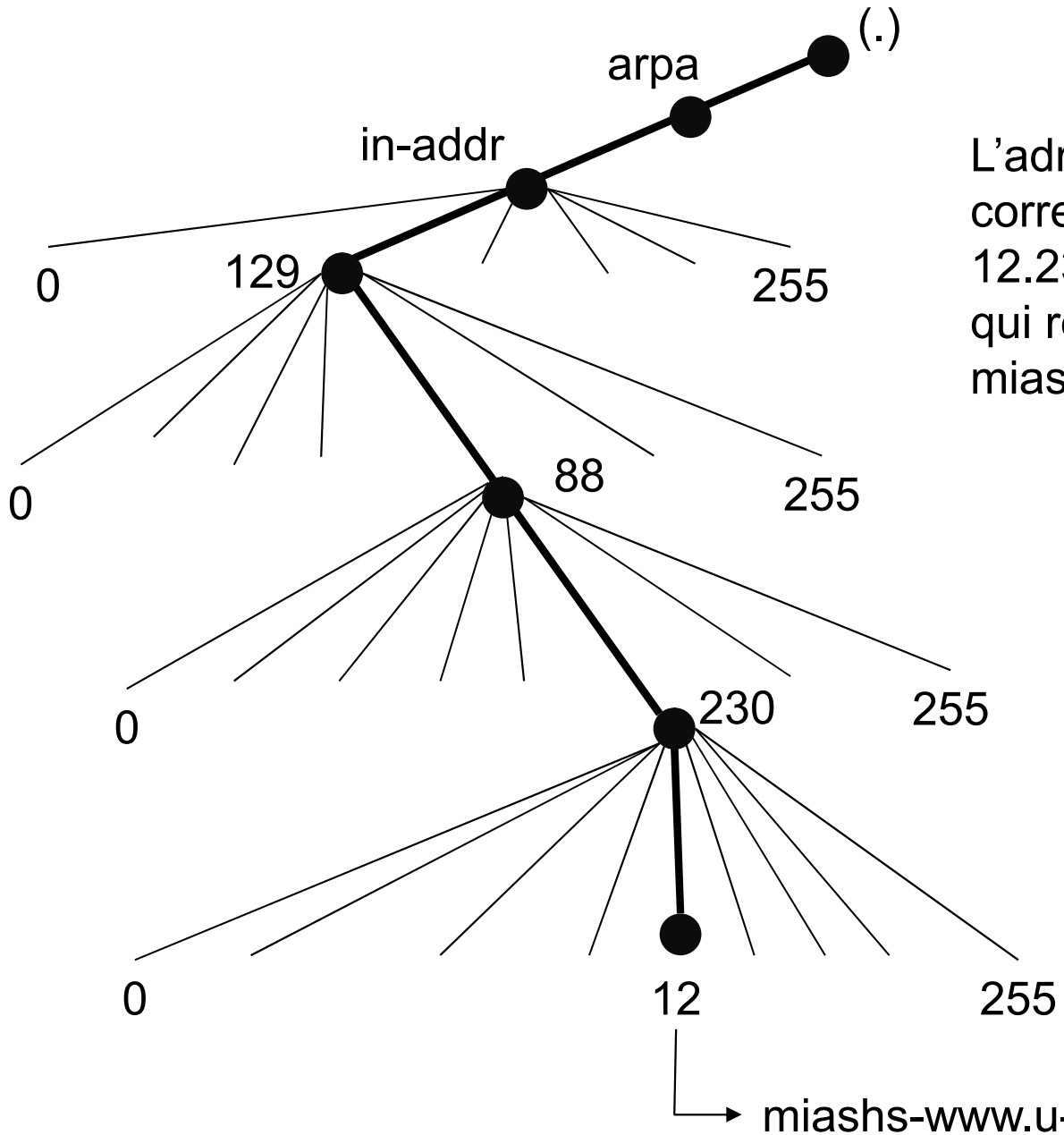
- Un domaine est une organisation de l'espace de nommage
  - Il peut être attaché à un domaine parent, et/ou peut avoir un ou plusieurs sous-domaines enfants
- Les zones correspondent à des organisations administratives des domaines
- L'organisation de l'espace de nommage est complètement indépendante de l'implantation géographique d'un réseau ou de son organisation physique
- Les seules machines connues au niveau de l'espace de nommage, sont les serveurs de nom « déclarés »
  - Ces informations sont accessibles par des bases de données « whois »

Le domaine in-addr.arpa

- Le principe de la résolution de noms, consiste à affecter un nom d'hôte une adresse IP
  - On parle de résolution de noms directe
  - Un *Fully Qualified Domain Name* (FQDN), ou *Nom de domaine pleinement qualifié* est un nom de domaine écrit de façon absolue et ponctué par un point final (**`miashs-www.u-ga.fr.`**)

- Le processus inverse existe qui permet, pour une adresse IP, de fournir le nom correspondant
  - On parle de résolution de noms inverse ou reverse
  - Une zone particulière in-addr.arpa existe permettant la résolution inverse d'adresse IP

Le domaine in-addr.arpa



L'adresse IP 129.88.230.12 correspond au sous-domaine 12.230.88.129.in-addr.arpa qui renvoie le nom qualifié miashs-www.u-ga.fr

Cache DNS

- Quand un hôte doit résoudre un nom, il s'adresse à un ou plusieurs serveurs de noms dits *récursifs*
  - Parcourent la hiérarchie DNS et font suivre la requête à un ou plusieurs autres serveurs de noms pour fournir une réponse
- Pour optimiser les requêtes ultérieures, les serveurs DNS récursifs gardent en mémoire (*cache*) la réponse d'une résolution de nom
  - Cette information est conservée pendant une période (*Time to live)* et associée à chaque nom de domaine

Serveurs primaires / secondaires

- Un nom de domaine peut utiliser plusieurs serveurs DNS
  - Généralement au moins deux : un **primaire** et un **secondaire**
  - Possibilité d'avoir plusieurs serveurs secondaires
- L'ensemble des serveurs primaires et secondaires font **autorité** pour un domaine
  - la réponse ne fait pas appel à un autre serveur ou à un cache
- Les serveurs récursifs fournissent des réponses qui ne sont pas nécessairement à jour, à cause du cache mis en place.
  - ➔réponse ne faisant pas autorité (*non-authoritative answer*)

Principaux types d'enregistrement

- SOA (*Start Of Authority*)
  - indique l'autorité sur la zone. Ces enregistrements contiennent toutes les informations sur le domaine (délai de mise à jour des bases de données entre serveurs de noms primaires et secondaires, nom du responsable du site)
- NS (*Name Server*)
  - donnent les adresses des serveurs de noms pour le domaine
- A (*Adresse*) ou AAAA
  - permettent de faire correspondre un nom d'hôte respectivement à une adresse IPv4 de 32 bits distribués sur quatre octets, et à une adresse IPv6 de 128 bits sur seize octets
- MX (*Mail eXchanger*)
  - servent pour déclarer les serveurs de messagerie
- CNAME (*Canonical Name*)
  - permettent de définir des alias sur des noeuds existants
- PTR (Pointeur)
  - permettent la résolution de noms inverse dans le domaine in-addr.arpa.