Administration réseau
Résolution de noms
et
attribution d'adresses IP

A. Guermouche

Plan

1. DNS
   - Introduction
   - Fonctionnement
   - DNS & Linux/UNIX
2. DHCP
   - Introduction
   - Le protocole DHCP
   - DHCP & Linux/UNIX

Plan

DNS

Comment relier les adresses IP utilisées pour acheminer les paquets aux noms utilisés par les applications?
→ **DNS** (**D**omain **N**ame **S**ervice)

- Protocole applicatif
- DNS est utilisé par d'autres protocoles applicatifs mais est rarement utilisé directement par l'application
- modèle client/serveur : un émetteur interroge un serveur de noms (serveur DNS)
- port 53/UDP
- RFC 1034, 1035, 2181, ...

Un système centralisé?

Pourquoi pas de DNS centralisé? Un seul serveur contiendrait toutes les correspondances requises par les applications de l'internet

- dimension de l'internet : trop de correspondances à gérer, nombre de requêtes au serveur trop important
- tolérance aux pannes : si le serveur DNS tombe, tout internet aussi
- trafic impossible à supporter par un seul serveur
- délai de réponse : il faut faire en sorte que la réponse soit la plus proche possible du demandeur
- problème lié à la maintenance et aux mises à jour perpétuelles de la base

Un système distribué

Aucun serveur ne connaît les les correspondances nom↔@IP

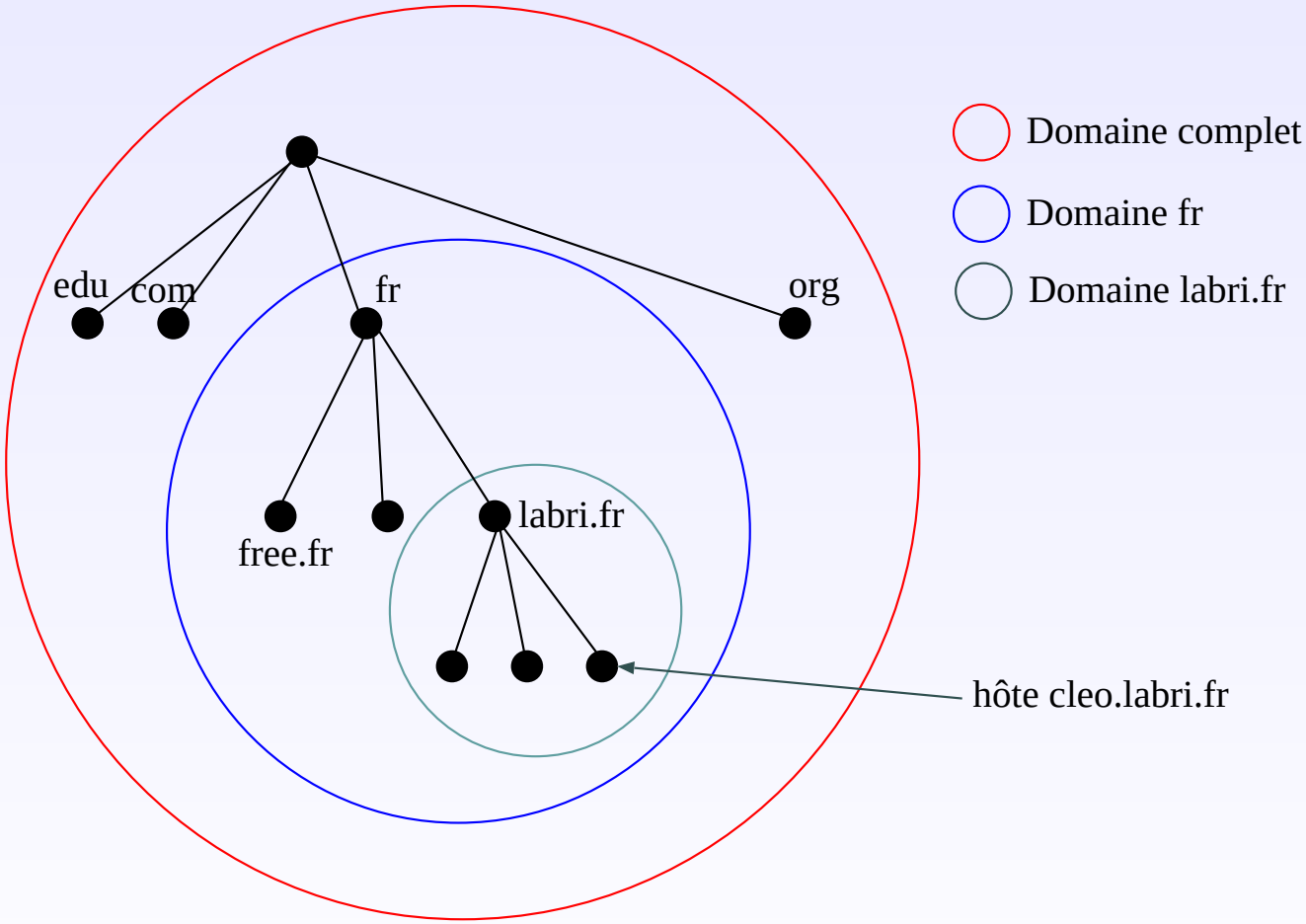
→ si un serveur ne connaît pas une correspondance, il interroge un autre serveur jusqu'à atteindre le serveur détenant l'information

Trois types de serveur DNS :

- ⋆ les serveurs de noms locaux à qui s'adressent les requêtes locales; ils sont en charge de la résolution
- ⋆ les serveurs de noms racine qui sont censés savoir comment se rapprocher de la réponse
- ⋆ les serveurs de noms de source autorisée qui contiennent les correspondances officielles

Domaine DNS (1/2)

Un domaine est un sous-arbre entier de l'espace de "nomage"



Deux nœuds différents peuvent avoir le même nom dans deux domaines différents : `cleo.labri.fr` et `cleo.free.fr`

Domaine DNS (2/2)

Le premier niveau de l'arbre

- Top Level Domain (TLD)
- géré pas l'ICANN (*Internet Corporation for Assigned Names and Numbers*)
- deux types de TLD :
  "generic TLD". `.com`, `.org`, `.gov`, `.net`,...
  "coutries TLD". `.fr`, `.de`, `.uk`,...

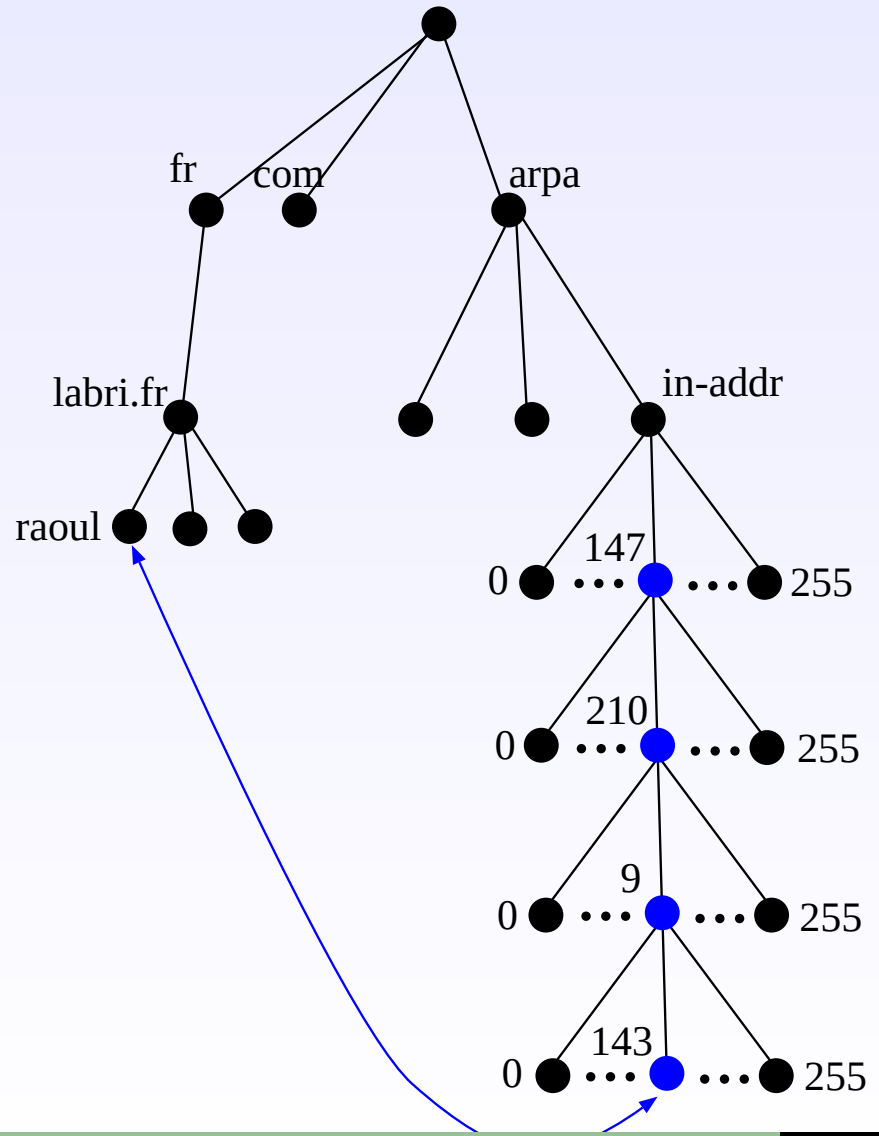
Les autres niveaux sont gérés par des entités "locales" (AFNIC pour `.fr`)

zone DNS :

- Un sous-arbre administré par un organisme qui gère la délégation des noms et sous-domaines de la zone
- Une zone = une administration centralisée avec au moins un serveur DNS (généralement un primaire et un secondaire)
- Une zone doit connaître les serveurs DNS des zones subordonnées

La résolution de noms inverse

- Retrouver le nom canonique à partir de l'adresse IP
- Le domaine `arpa` : un domaine particulier gérer par l'ICANN permettant la résolution inverse
- Résolution inverse : 143.9.210.147.in-addr.arpa ? (pour trouver le nom de la machine dont l'adresse IP est 147.210.9.143)



Les différents types de serveur DNS (1/2)

Les serveurs de noms locaux :

- chaque organisation a un serveur de nom local
  - serveur de noms par défaut de la zone
  - contient parfois les correspondances relatives à la zone de l'organisation
- toutes les requêtes en provenance de cette organisation vont vers ce serveur de noms local

Les serveurs de noms racine :

- il existe 13 serveurs racine dans internet
- chaque serveur DNS local connaît un serveur de noms racine qu'il peut interroger lorsqu'il ne connaît pas une correspondance
- un serveur de nom racine connaît au moins les serveurs de noms de source autorisée du premier niveau (`.fr`, `.com`,...)

Les différents types de serveur DNS (2/2)

Un serveur de noms racine qui ne connaît pas la réponse à une requête interroge un autre serveur de noms le rapprochant de la réponse, généralement le serveur de noms de source autorisée qui connaît la correspondance

Les serveurs de noms de source autorisée :

- chaque hôte est enregistré auprès d'au moins deux *"authoritative servers"* (le primaire et le secondaire) qui stockent son adresse IP et son nom
- un serveur de noms est dit de source autorisée pour un hôte s'il est responsable de la correspondance nom/@IP pour cet hôte (serveur primaire de la zone)
- un serveur de nom local n'est pas forcément de source autorisée de premier niveau (`.fr`,...)

Résolution de noms récursive/itérative

Résolution récursive. la machine qui demande la résolution de nom contacte un serveur DNS et attend que ce dernier lui retourne la réponse désirée.

Résolution itérative. le serveur de noms contacté fournit en réponse le nom d'un autre serveur DNS à contacter pour avancer dans la résolution.

Dans une résolution de nom, certaines requêtes peuvent être itératives, d'autres récursives.

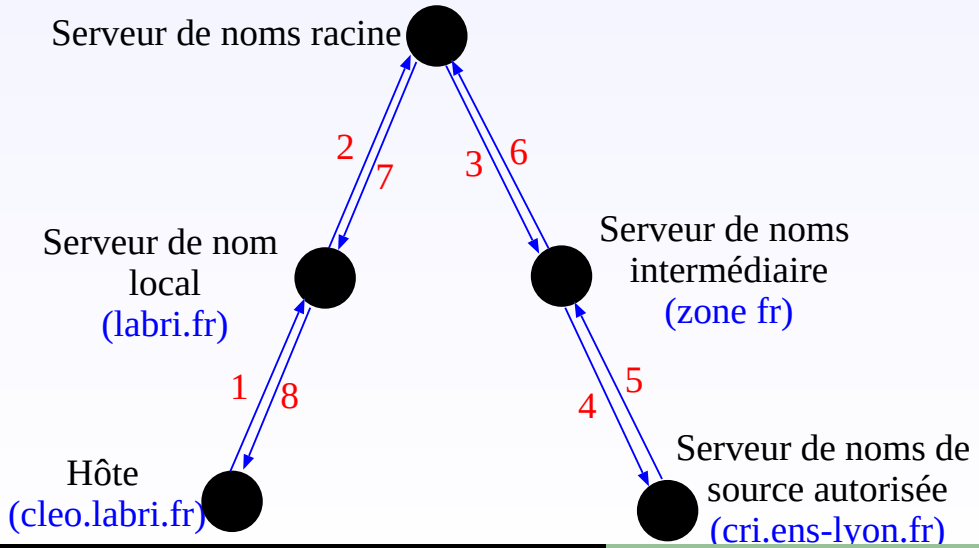
Résolution de noms récursive/itérative

Résolution récursive. la machine qui demande la résolution de nom contacte un serveur DNS et attend que ce dernier lui retourne la réponse désirée.

Résolution itérative. le serveur de noms contacté fournit en réponse le nom d'un autre serveur DNS à contacter pour avancer dans la résolution.

Dans une résolution de nom, certaines requêtes peuvent être itératives, d'autres récursives.

Résolution récursive : `ssh.ens-lyon.fr`→?



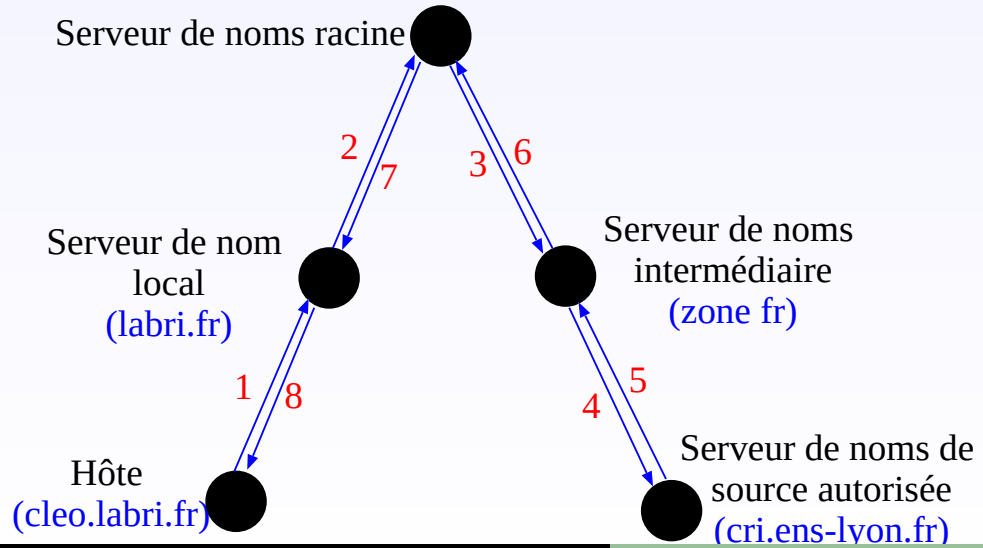
Résolution de noms récursive/itérative

Résolution récursive. la machine qui demande la résolution de nom contacte un serveur DNS et attend que ce dernier lui retourne la réponse désirée.

Résolution itérative. le serveur de noms contacté fournit en réponse le nom d'un autre serveur DNS à contacter pour avancer dans la résolution.

Dans une résolution de nom, certaines requêtes peuvent être itératives, d'autres récursives.

Résolution récursive : `ssh.ens-lyon.fr`→?



Le serveur de noms racine connaît un serveur qui le rapprochera de la réponse (il peut aussi connaître directement le serveur de source autorisée)

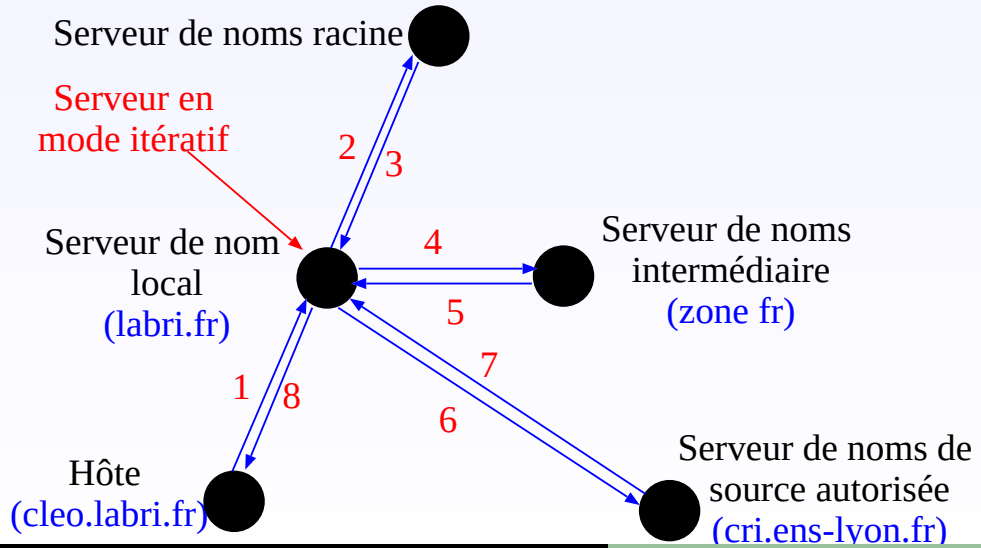
Résolution de noms récursive/itérative

Résolution récursive. la machine qui demande la résolution de nom contacte un serveur DNS et attend que ce dernier lui retourne la réponse désirée.

Résolution itérative. le serveur de noms contacté fournit en réponse le nom d'un autre serveur DNS à contacter pour avancer dans la résolution.

Dans une résolution de nom, certaines requêtes peuvent être itératives, d'autres récursives.

Résolution itérative : `ssh.ens-lyon.fr`→?



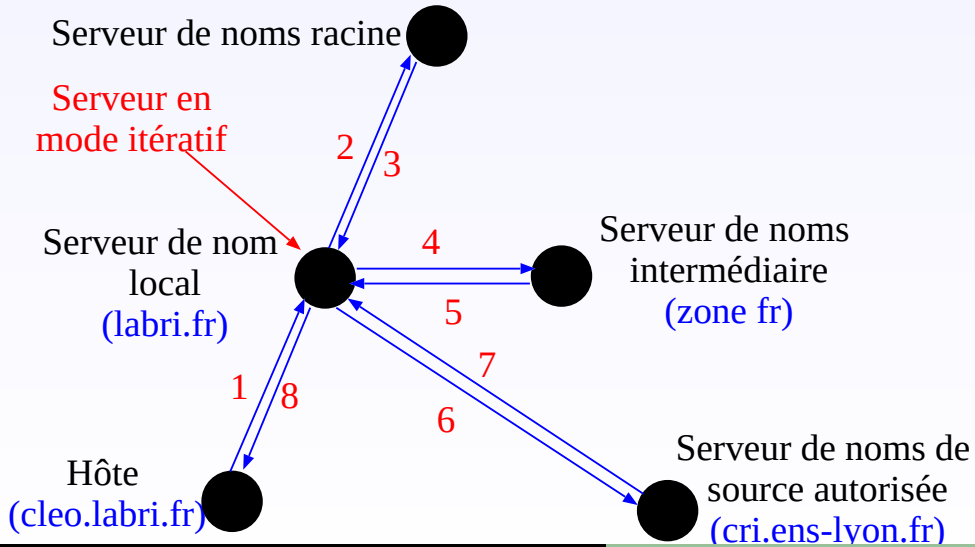
Résolution de noms récursive/itérative

Résolution récursive. la machine qui demande la résolution de nom contacte un serveur DNS et attend que ce dernier lui retourne la réponse désirée.

Résolution itérative. le serveur de noms contacté fournit en réponse le nom d'un autre serveur DNS à contacter pour avancer dans la résolution.

Dans une résolution de nom, certaines requêtes peuvent être itératives, d'autres récursives.

Résolution itérative : `ssh.ens-lyon.fr`→?



généralement toutes les requêtes sont récursives sauf celles entre le serveur local et le serveur racine

⇒ Permet de moins solliciter le serveur racine

Cache DNS

Objectif : Réduire le temps de réponse d'une résolution de nom

- ★ diminuer le nombre de messages DNS nécessaires
- ★ le serveur de noms (quelconque) stocke dans son cache les informations récentes
  - ▸ comme la mémoire n'est pas infinie et que les données peuvent ne plus être valables au bon d'un certain temps, les données "sortent" du cache après un certain temps (TTL d'environ 2 jours)
- ★ Un serveur DNS qui mémorise dans son cache un enregistrement DNS n'a pas autorité dessus

  → spécifie *"no authoritative"* dans la réponse

Les messages DNS (RFC 1034, 1035)

Un message de réponse DNS contient un ou plusieurs RR (*Resource record*)

- l'unité de stockage d'une correspondance dans le cache :
  `(Nom, Type, Classe, TTL, Valeur)`
- `Type` représente le type de l'enregistrement; la signification de `Nom` et `Valeur` dépend de la valeur de `Type`.
  - `Type=A` adresse IPv4
  - `Type=NS` serveur de noms de source autorisée
  - `Type=MX` alias réservé au serveur de mail
  - `Type=PTR` sert à la résolution inverse
  - ...
- `Classe` représente la famille de protocoles; `Classe=1` pour internet (`IN`)
- `TTL` représente la durée de vie de l'entrée dans le cache (en secondes)

Un message de type requête DNS est de la forme :

`(Nom, Type, Classe)`

Clients et Serveur DNS

Côté client :

- le *resolver* est en charge des résolutions de noms à chaque fois que cela est nécessaire
- deux fichiers de configurations :
  - `/etc/resolv.conf`. permet de paramétrer les requêtes DNS effectuées
  - `/etc/host.conf`. permet de configurer les *resolver* (en particulier l'ordre de la résolution) :
    ```
    order hosts,bind,nis
    ```
  - `/etc/nsswitch.conf`. est consulté avant `host.conf` pour la configuration de l'ordre de la recherche
- commandes de test : `host`, `nslookup`, `dig`, ...

Côté serveur : Serveur `BIND` (*Berkeley Internet Name Domain*)

- Le démon répondant aux requêtes est `named`
  - fichier de configuration → `/etc/named.conf`
  - fichiers décrivant les zones administrées stockées dans `/etc/bind/`

Plan

DHCP

DHCP → Dynamic Host Configuration Protocol (RFC 2131)

- Protocole client/serveur
- Le serveur DHCP fournit des paramètres de configuration aux clients (généralement des paramètres nécessaires à la configuration du réseau)
- Permet l'attribution automatique d'adresses IP
- Successeur de BOOTP (protocole d'obtention automatique d'adresse IP utilisé pour les stations *"diskless"*)
- Compatible avec BOOTP

DHCP

DHCP → Dynamic Host Configuration Protocol (RFC 2131)

- Protocole client/serveur
- Le serveur DHCP fournit des paramètres de configuration aux clients (généralement des paramètres nécessaires à la configuration du réseau)
- Permet l'attribution automatique d'adresses IP
- Successeur de BOOTP (protocole d'obtention automatique d'adresse IP utilisé pour les stations *"diskless"*)
- Compatible avec BOOTP

3 méthodes de gestion des adresses IP :

Allocation manuelle. Le serveur DHCP attribue l'adresse IP en se basant sur une table d'adresses MAC prédéfinie

Allocation automatique. Le serveur DHCP attribue de manière permanente une adresse IP (parmi l'ensemble des adresses "libres") à un client

Allocation dynamique. Méthode permettant la réutilisation d'adresses IP (basée sur un mécanisme de "bail")

Protocole DHCP (1/2)

- Protocole utilisant les ports 67/UDP (serveur) et 68/UDP (client)
- Échange de messages entre client et serveurs pour l'attribution d'une adresse IP pour une durée donnée
- Protocole basé sur un mécanisme de *broadcast*
- Utilisation de différents types de messages : `DHCP Discover`, `DHCP Offer`, `DHCP Request`, `DHCP Acknowledge`, `DHCP Inform` et `DHCP Release`

Protocole DHCP (1/2)

- Protocole utilisant les ports 67/UDP (serveur) et 68/UDP (client)
- Échange de messages entre client et serveurs pour l'attribution d'une adresse IP pour une durée donnée
- Protocole basé sur un mécanisme de *broadcast*
- Utilisation de différents types de messages : `DHCP Discover`, `DHCP Offer`, `DHCP Request`, `DHCP Acknowledge`, `DHCP Inform` et `DHCP Release`

DHCP Discover.

- Le client diffuse un message dans le réseau local pour trouver les serveurs disponibles.
- La diffusion est faite vers l'adresse 255.255.255.255.
- De plus Le client peut ajouter sa dernière adresse IP obtenue à l'aide de DHCP.

Protocole DHCP (1/2)

- Protocole utilisant les ports 67/UDP (serveur) et 68/UDP (client)
- Échange de messages entre client et serveurs pour l'attribution d'une adresse IP pour une durée donnée
- Protocole basé sur un mécanisme de *broadcast*
- Utilisation de différents types de messages : `DHCP Discover`, `DHCP Offer`, `DHCP Request`, `DHCP Acknowledge`, `DHCP Inform` et `DHCP Release`

DHCP Offer. Le serveur choisit une configuration pour le client (en se basant éventuellement sur l'adresse MAC contenue dans le message du client)

Protocole DHCP (1/2)

- Protocole utilisant les ports 67/UDP (serveur) et 68/UDP (client)
- Échange de messages entre client et serveurs pour l'attribution d'une adresse IP pour une durée donnée
- Protocole basé sur un mécanisme de *broadcast*
- Utilisation de différents types de messages : `DHCP Discover`, `DHCP Offer`, `DHCP Request`, `DHCP Acknowledge`, `DHCP Inform` et `DHCP Release`

DHCP Request.

- Le client sélectionne une configuration parmi celles qu'il a reçues (paquets `DHCP Offer`) et la diffuse dans le réseau.
- Le client met dans le message l'adresse que le serveur lui a proposée.
- S'il a reçu plusieurs "offres" il spécifie le serveur qu'il a choisi.

Protocole DHCP (1/2)

- Protocole utilisant les ports 67/UDP (serveur) et 68/UDP (client)
- Échange de messages entre client et serveurs pour l'attribution d'une adresse IP pour une durée donnée
- Protocole basé sur un mécanisme de *broadcast*
- Utilisation de différents types de messages : `DHCP Discover`, `DHCP Offer`, `DHCP Request`, `DHCP Acknowledge`, `DHCP Inform` et `DHCP Release`

DHCP Acknowledgement.

- Le serveur confirme l'attribution de l'adresse IP au client (le message contient toutes les informations nécessaires à la configuration plus éventuellement un bail).
- Le client peut configurer son "réseau" à la réception de ce message

Protocole DHCP (1/2)

- Protocole utilisant les ports 67/UDP (serveur) et 68/UDP (client)
- Échange de messages entre client et serveurs pour l'attribution d'une adresse IP pour une durée donnée
- Protocole basé sur un mécanisme de *broadcast*
- Utilisation de différents types de messages : `DHCP Discover`, `DHCP Offer`, `DHCP Request`, `DHCP Acknowledge`, `DHCP Inform` et `DHCP Release`

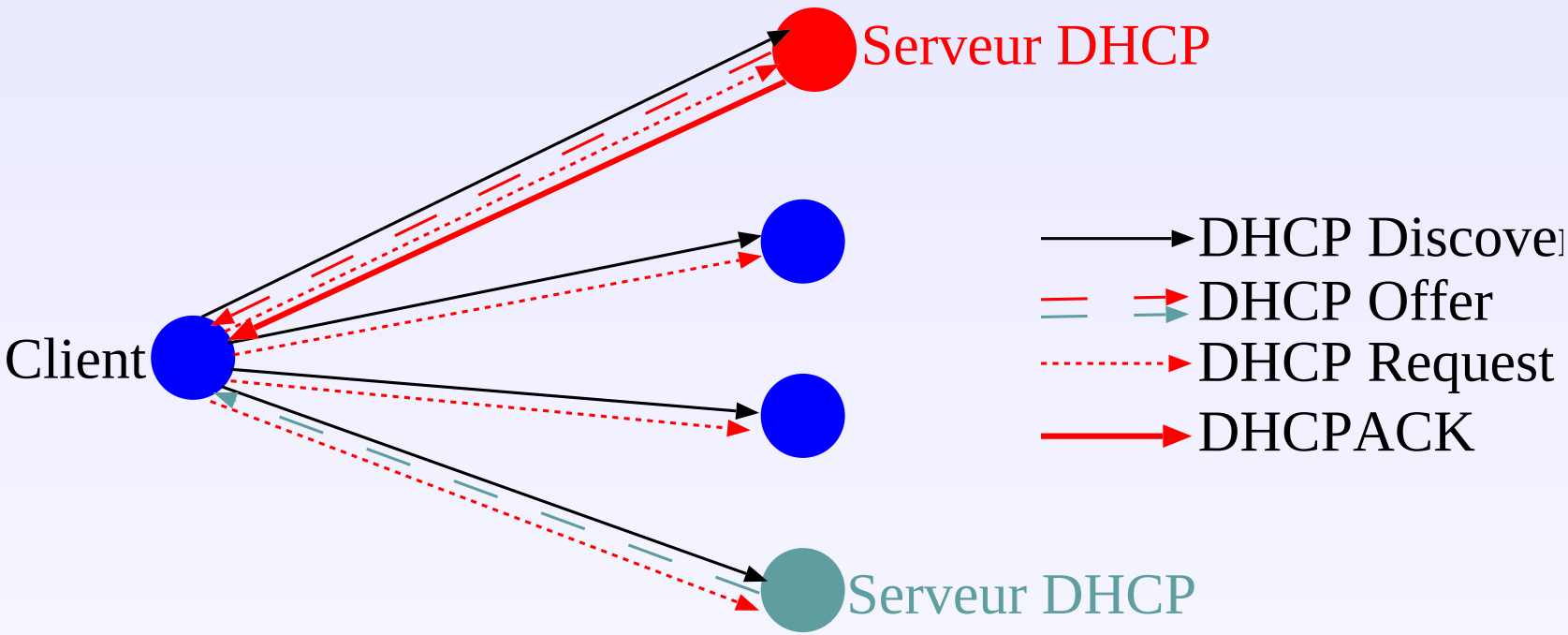
DHCP Inform. Le client demande des informations complémentaires au serveur DHCP (complément par rapport au DHCPACK ou demande spécifique pour une application donnée)

Protocole DHCP (1/2)

- Protocole utilisant les ports 67/UDP (serveur) et 68/UDP (client)
- Échange de messages entre client et serveurs pour l'attribution d'une adresse IP pour une durée donnée
- Protocole basé sur un mécanisme de *broadcast*
- Utilisation de différents types de messages : `DHCP Discover`, `DHCP Offer`, `DHCP Request`, `DHCP Acknowledge`, `DHCP Inform` et `DHCP Release`

DHCP Release. Le client envoie un message au serveur pour libérer son adresse IP. Ce message n'est pas nécessaire (l'adresse IP est récupérée par le serveur lorsque le bail expire et qu'il n'est pas renouvelé)

Protocole DHCP (2/2)



Ordre des messages :

1- DHCP Discover
2- DHCP Offer
3- DHCP Request
4- DHCPACK

DHCP & Linux/UNIX

- DHCPD est le démon qui implémente le serveur DHCP
- Configuration via le fichier `/etc/dhcpd.conf`
  Exemple simple :

```
subnet 192.168.0.0 netmask 255.255.255.0 {
default-lease-time 345600; # bail par défaut
max-lease-time 691200; # bail maximal
option domain-name “domainelocal.com”;
option domain-name-servers 192.168.0.2;
option routers 192.168.0.2;
option broadcast-address 192.168.0.255;
range 192.168.0.20 192.168.0.30;
}
```

- Possibilité d'ajouter dynamiquement les nouveaux hôtes enregistrés via DHCP au DNS (Dynamic DNS en utilisant BIND et DHCPD).
- Configuration du resolver via `/etc/resolv.conf`
- Plusieurs clients DHCP disponibles : `dhclient`, `pump`,...