Administration et sécurité des réseaux

Chapitre 2

Les protocole DHCP, DNS, FTP et SMTP fonctionnement, mise en place et sécurisation

Partie 1 :

DHCP (Dynamic Host Configuration Protocol)

- Objectifs
- Fonctionnement
- Configuration et options
- Attaques
- Sécurisation

Rôle d'un service DHCP

- **Rôle:**
  - Distribue d'une façon dynamique des adresses IP à des clients pour une durée déterminée.
  - Evite l'affectation manuelle à chaque hôte d'une adresse IP statique, ainsi que tous les paramètres dont il a besoin pour utiliser le réseau
- **Exemple d'utilisation: chez les FAI.**
  - Le fournisseur d'accès alloue une adresse IP de son réseau le temps de la liaison. Cette adresse est libérée, donc de nouveau disponible, lors de la fermeture de la session.
- **Contraintes:**
  - Tous les nœuds critiques du réseau (serveur de nom, passerelle par défaut, serveur de mail…etc) ont une adresse IP statique sinon problèmes de gestion

Avantage de DHCP

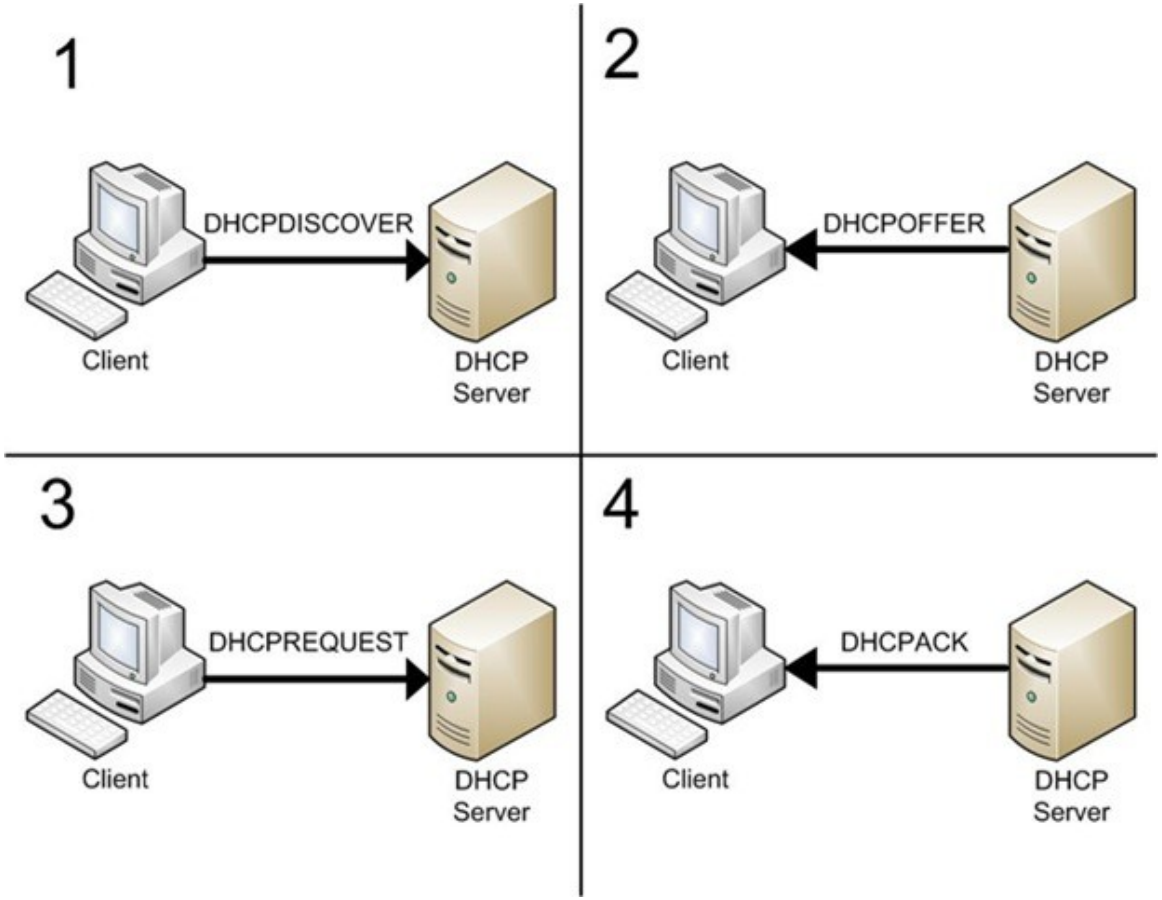
- **Configuration fiable et simple de réseaux TCP/IP**
- **Minimisation du risque de conflits d'adresses**
- **Les postes itinérants sont plus faciles à gérer (PC portable)**
- **L'économie des adresses IP:**
  - Exemple: Les FAI disposent d'un nombre d'adresses limité.
  - Avec DHCP, seules les machines connectées en ligne ont une adresse IP.
- **Contrôle centralisé de l'utilisation des adresses IP.**
- **Le changement de la valeur d'un paramètre au niveau du serveur DHCP (exemple: passerelle par défaut) est pris en compte par tous les clients du serveur ➔ changement facile**
  - Dans le cas de l'adressage statique, il faudrait reconfigurer toutes les machines manuellement .

Le protocole DHCP

- **RFC 1533 et 1534**
- **Extension de BootP**
- **Se base sur les protocoles UDP et IP**
- **Fonctionne en mode client serveur**
  - Le client demande une adresse IP (une configuration automatique)
  - Le serveur dispose d'une pool d'adresses à louer
  - Le serveur fournit/loue l'adresse IP (configuration) pendant un temps limité appelé bail (lease)

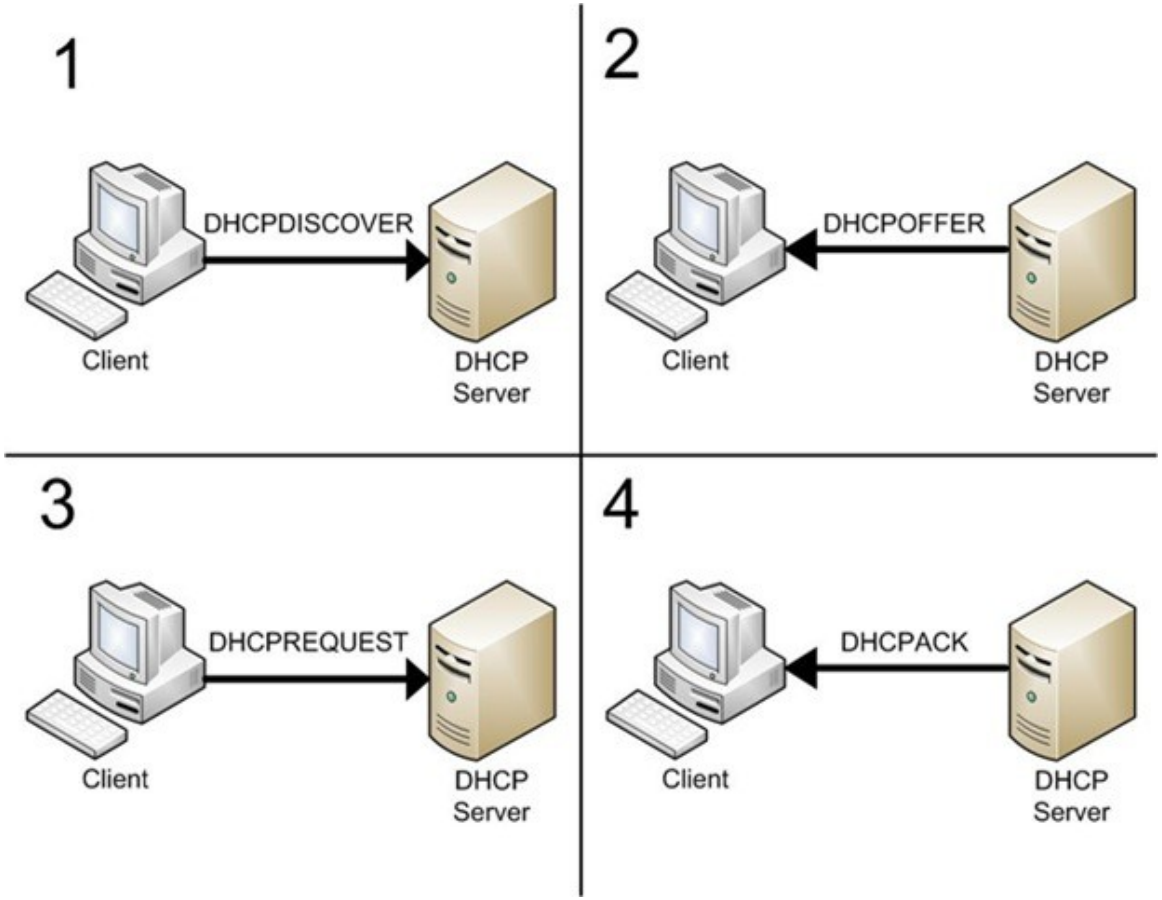
Attribution de configuration IP

- **Le client émet un message de demande de bail IP (DHCPDISCOVER) envoyé par diffusion sur le réseau avec adresse IP source 0.0.0.0, adresse IP destination 255.255.255.255 et son adresse MAC.**



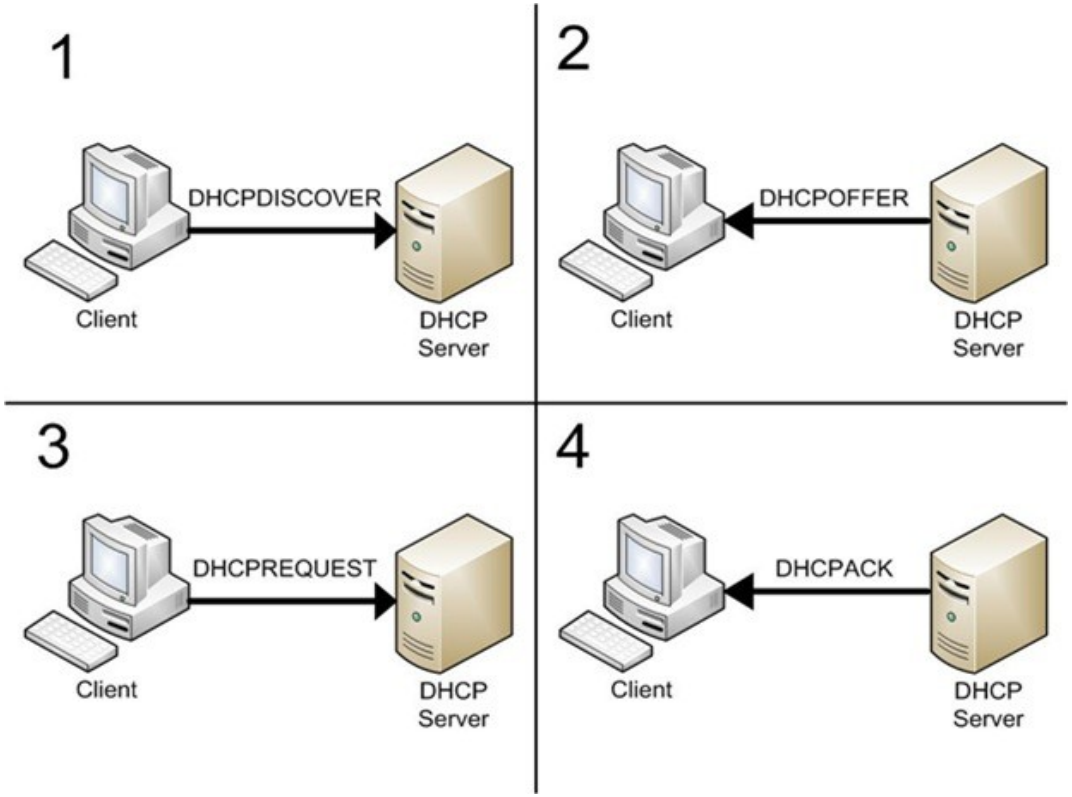
Attribution d’adresse IP

- **Les serveurs DHCP répondent en proposant une adresse IP avec une durée de bail et l'adresse IP du serveur DHCP (DHCOFFER)**



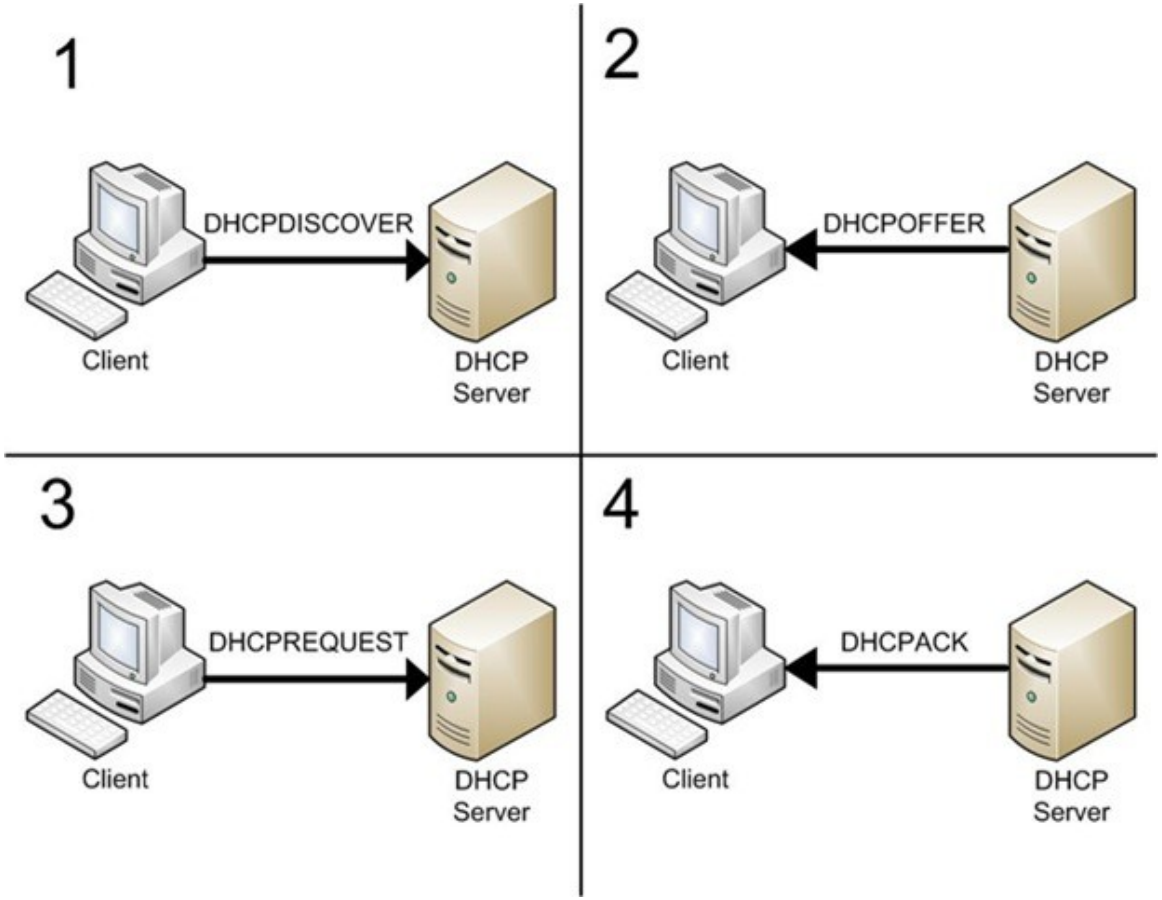
Attribution d’adresse IP

- **Le client sélectionne la première adresse IP reçue (s'il y a plusieurs serveurs DHCP) et envoie une demande d'utilisation de cette adresse au serveur DHCP (DHCPREQUEST). Son message envoyé par diffusion 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.**

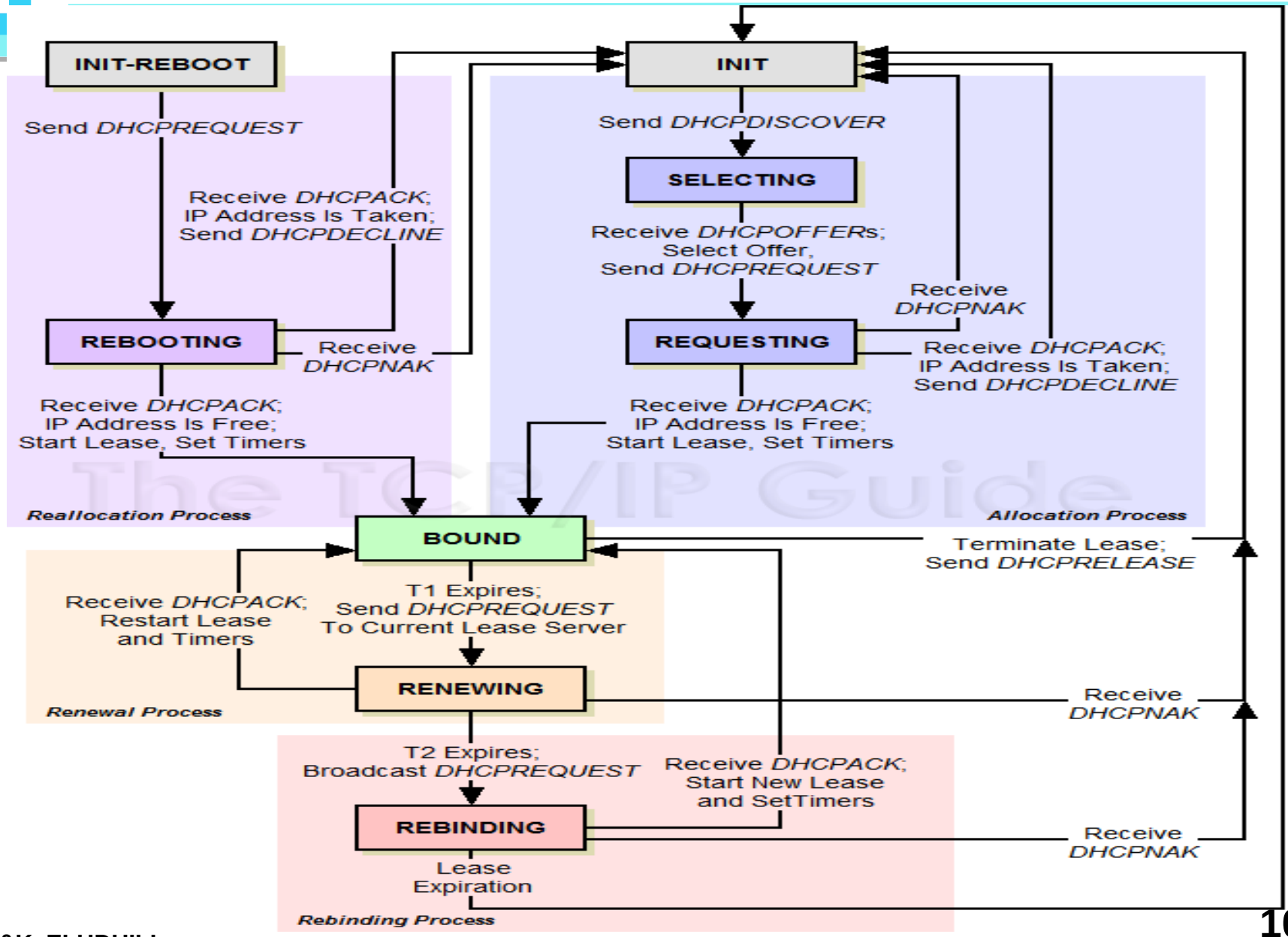


Attribution d’adresse IP

- **Le serveur DHCP accuse réception de la demande et accorde l'adresse en bail (DHCPACK), les autres serveurs retirent leur proposition.**



L'automate de DHCP

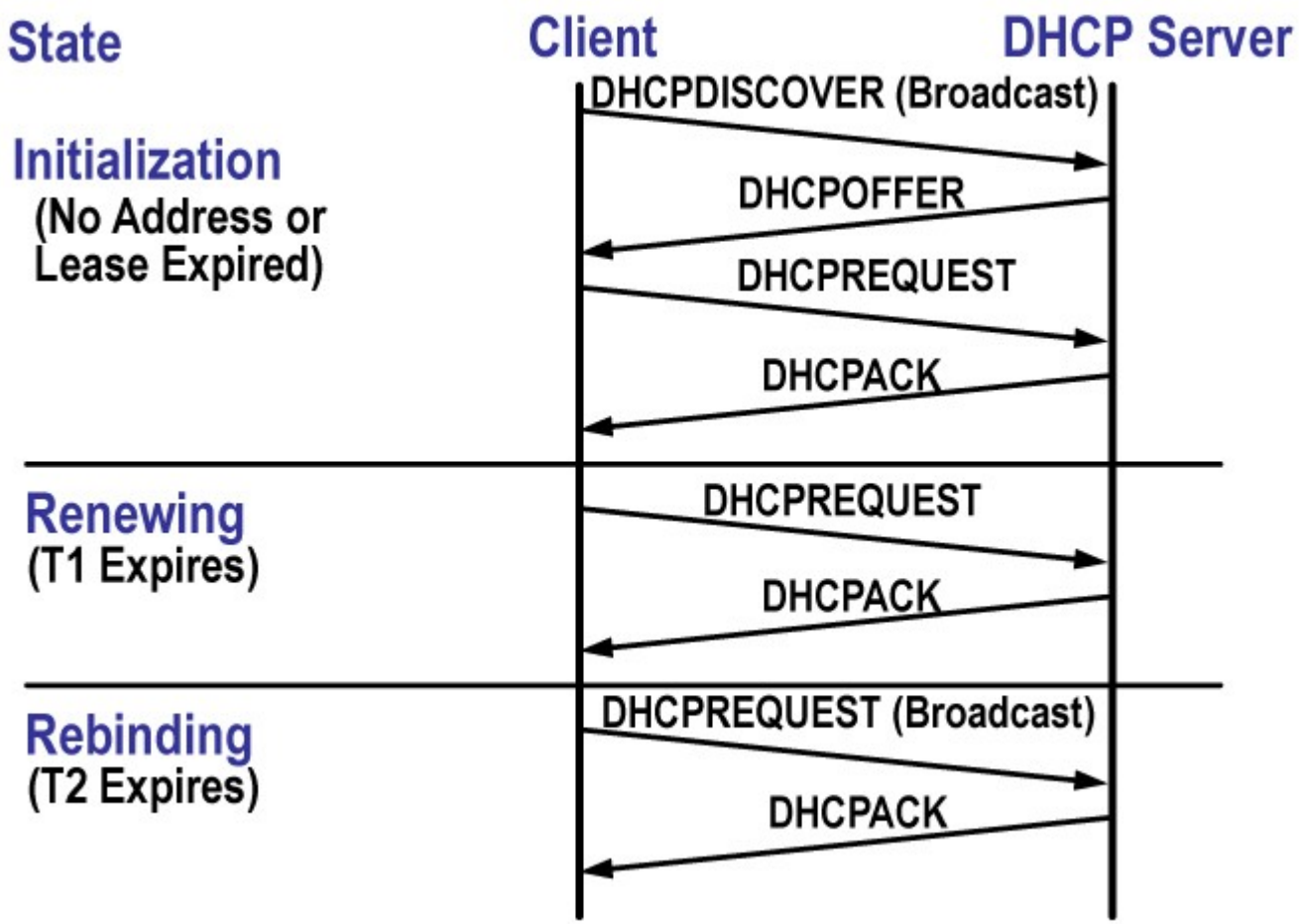


Renouvellement de bail IP

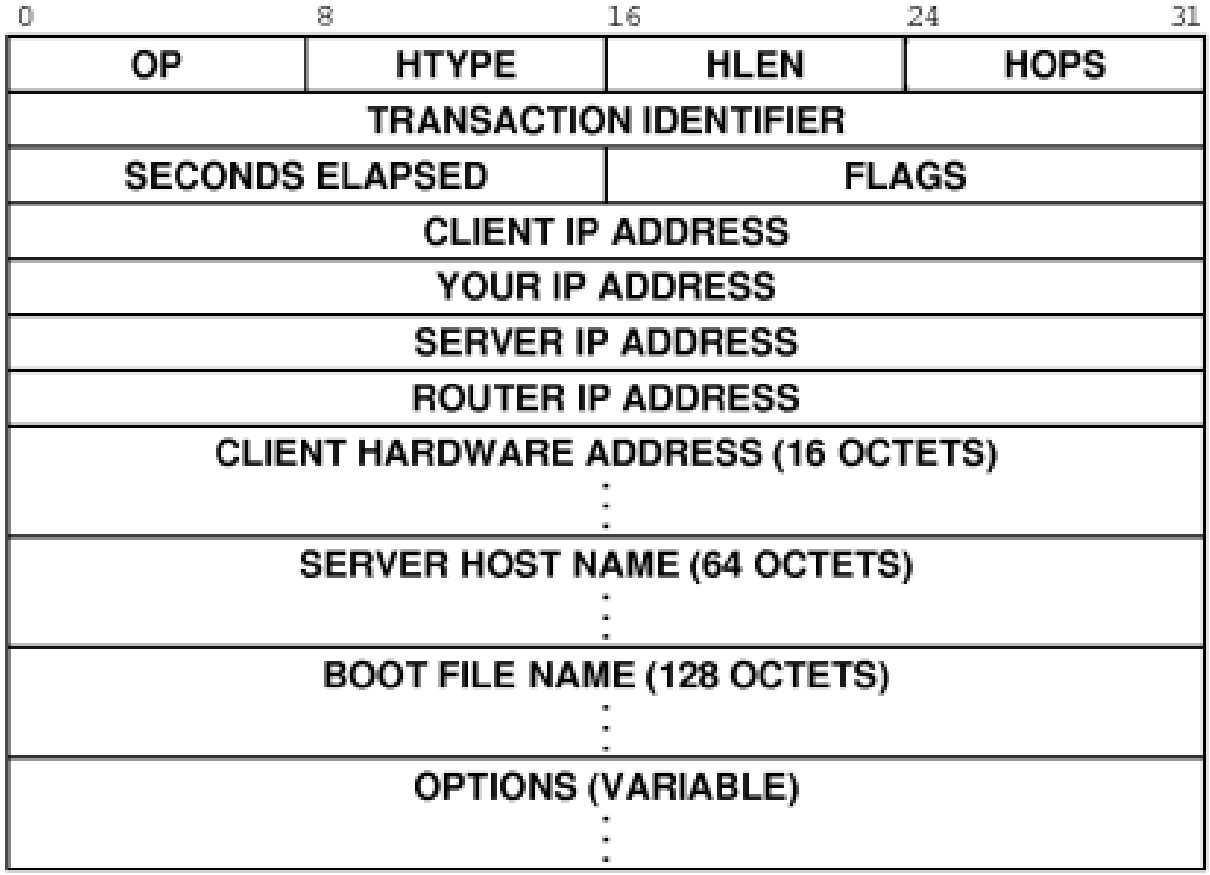
- Lorsqu'un client redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine, en émettant un DHCPREQUEST.
- En cas d’échec, le client continue à utiliser la même adresse IP s‘i le bail n’a pas encore expiré.
- Les clients DHCP d'un serveur DHCP Windows (NT/2000) tentent de renouveler leur bail lorsqu'ils ont atteint 50% de sa durée par un DHCPREQUEST. Si le serveur DHCP est disponible il envoie un DHCPACK avec la nouvelle durée et éventuellement les mises à jour des paramètres de configuration.
- Si à 50% le bail n'a pu être renouvelé, le client tente de contacter l'ensemble des serveurs DHCP (diffusion) lorsqu'il atteint 87,5% de son bail, avec un DHCPREQUEST, les serveurs répondent soit par DHCPACK soit par DHCPNACK (adresse inutilisable, étendue désactivée...).
- Lorsque le bail expire ou qu'un message DHCPNACK est reçu le client doit cesser d'utiliser l'adresse IP et demander un nouveau bail (retour au processus de souscription). Lorsque le bail expire et que le client n'obtient pas d'autre adresse la communication TCP/IP s'interrompt.

- Remarque : Si la demande n'aboutit pas et que le bail n'est pas expiré, le client continue à utiliser ses paramètres IP.

Echange de messages DHCP



Format du message DHCP



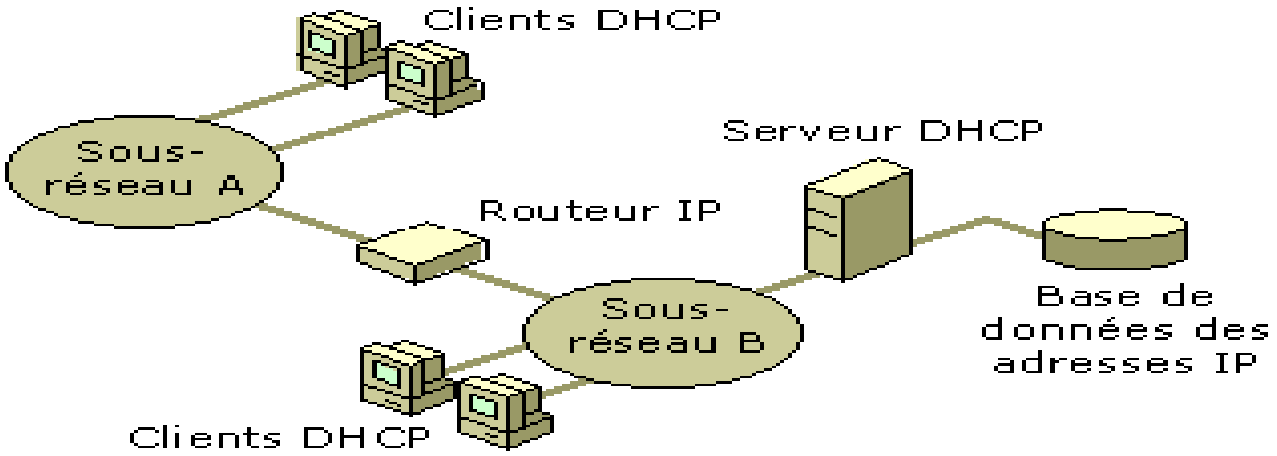
Format du message DHCP

- op : vaut 1 pour BOOTREQUEST (requête client), 2 pour BOOTREPLY (réponse serveur)
- htype : type de l'adresse hardware (adresse MAC, par exemple. Voir Rfc 1340)
- hlen : longueur de l'adresse hardware (en octet). C'est 6 pour une adresse MAC
- hops : peut être utilisé par des relais DHCP
- xid : nombre aléatoire choisi par le client et qui est utilisé pour reconnaître le client
- secs : le temps écoulé (en secondes) depuis que le client a commencé sa requête
- flags : flags divers

Format du message DHCP

- ciaddr : adresse IP du client, lorsqu'il en a déjà une
- yiaddr : la (future ?) adresse IP du client
- siaddr : adresse IP du (prochain) serveur à utiliser
- giaddr : adresse IP du relais (passerelle par exemple) lorsque le serveur n’est pas dans le même réseau physique
- chaddr : adresse hardware du client
- sname : champ optionnel. Nom du serveur
- file : nom du fichier à utiliser pour le boot
- options : Champ réservé pour les options (RFC 2132).

Le relais DHCP



- Lorsque le serveur DHCP n'est pas sur le même réseau physique que les clients: nécessité d'un relais DHCP
- Le relais fait passer les messages DHCP d'un réseau à un autre
- Un routeur doit être configuré pour jouer le rôle d'un relais DHCP

Les options du protocole

- Le passage de paramètres (nom de la machine...) se fait par l'intermédiaire d'options.
- Les options sont documentées dans la RFC 2132.
- Chaque option porte un numéro qui l'identifie.
- Il est possible d'envoyer plusieurs options dans le même message DHCP.
- Dans tous les cas, on doit toujours finir la zone d'options par une option 255 (end).
- Le format des options est le suivant :

Octet 1	Octet 2	Données
Code de l'option	Longueur champ de données	…

Quelques options utiles

- 1 Masque
- 3 Routeur
- 4 Serveur de temps
- 5 serveur de noms
- 6 serveur du domaine
- 10 serveur d’impression
- 15 nom du domaine
- 28 adresse de diffusion
- 66 serveur TFTP
- 255 end

Inconvénients de DHCP

- **Les trames de diffusion pour obtenir les adresses chargent le réseau.**
- **Risque de graves goulots d'étranglement sur le réseau lors des démarrages synchronisés.**

  →L'administrateur doit donc réfléchir à l'organisation de son réseau.

- **Nécessité d'un équipement serveur pour chaque zone de diffusion**

  → Compromis nombre de serveurs/ zone de diffusion

Config. d’un réseau en DHCP

- Attribuer aux serveurs des adresses IP statiques
- Organiser les clients en catégories
- Affecter à chaque catégorie une pool d’adresses dynamiques
- Configurer le maximum d’options dans le serveur
- Bien dimensionner la durée du bail pour un compromis charge réseau/validité
- Faire le choix entre utiliser un relais ou plusieurs serveurs distincts

Analyse d'une capture DHCP avec wireshark

DHCP: mise en ouevre
(sous linux Fedora)

Mise en œuvre DHCP (linux Fedora)

- Identité :
  - Type : service standalone
  - Ports : 67 (serveur), 68 (client)
  - Démon : /etc/init.d/dhcpd
  - Fichier de configuration : /etc/dhcpd.conf
  - Fichiers gérés par dhcpd(dans /etc ou /var/state/dhcp):
  - dhcpd.leases → contenant les baux en cours
  - dhcpd.leases~ → contenant les baux précédant .
  - Remarque: Pour certaines versions, ces fichiers ne sont pas créées lors de l'installation ➔ executer:

    touch /var/state/dhcp/dhcpd.leases

Mise en œuvre DHCP

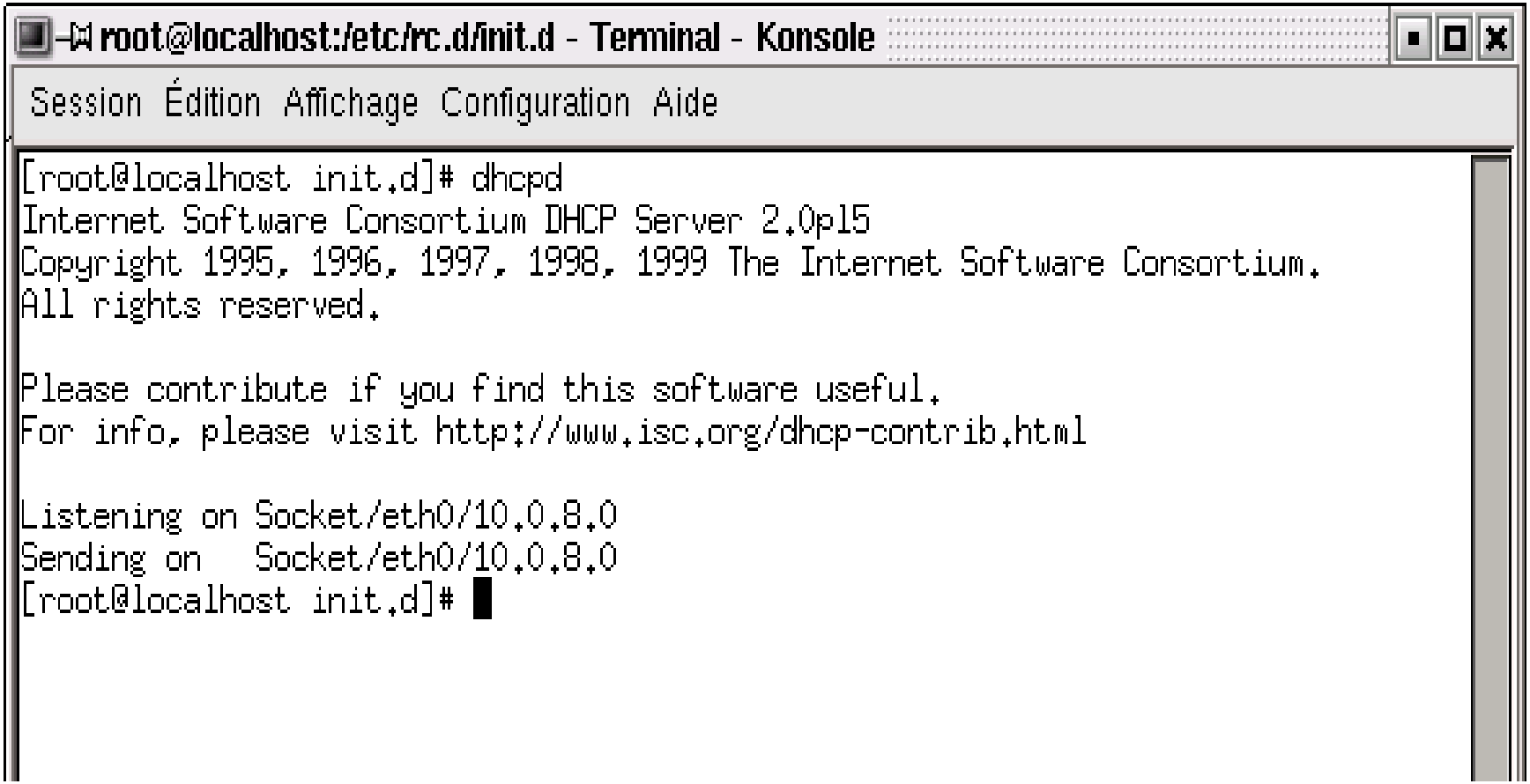
```
# Sample dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

ddns-update-style ad-hoc;

# option definitions common to all supported networks...
option domain-name "linuxhelp.ca";

# Your name servers. You can normally find these in
# your /etc/resolv.conf file. These will be distributed to all DHCP
# clients.
option domain-name-servers 10.1.1.1, 65.39.196.215, 65.39.192.130;

default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# Configuration for an internal subnet.
subnet 10.1.1.0 netmask 255.255.255.0 {
  range 10.1.1.2 10.1.1.25;
  option domain-name-servers 10.1.1.1, 65.39.196.215, 65.39.192.130;
  option domain-name "linuxhelp.ca";
  option routers 10.1.1.1;
  option broadcast-address 10.1.1.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

Mise en œuvre DHCP

- **max-lease-time** : durée maximale du bail que dhcp peut fournir (max une semaine) selon la durée demandée par le client
- **default-lease-time:** durée du bail utilisé (1 jour) si le client ne spécifie pas une durée dans sa demande
- **option subnet-mask** : definie le net mask.
- **option domain-name-servers** : liste des adresse IP des serveurs DNS
- **option domain** : le domaine par défaut
- **option lpr-servers** : liste les adresses des serveurs d'impression
- **option routers** : liste les routeurs du sous réseau du client
- **range** : Definie la plage d'addresses

Mise en œuvre DHCP

- Invoquer le démon /usr/sbin/dhcpd par la commande dhcpd



Commande démon dhcpd

dhcpd [interfce] [-p port] [-f] [-d] [-q] [-cf config-file] [-lf lease-file]

- **Options**
  - -p: specifier le port udp sur lequel le processus reste en écoute des demandes.
  - -f : le processus dhcpd sera lancer en avant plan.
  - -d : pour lancer le processus en mode deboguage (plus d'information sur le traffic dhcp).
  - -cf :specifier le fichier de configuration.
  - -q: les information d'entete sera omise lors du démarrage du démon(version ,copyright...)
  - -lf :spécifier un fichier .lease

- Pour lancer automatiquement le service dhcp lors de démarage ajouter /etc/sbin/dhcpd dans :

  /etc/rc.d/rc.local

- Lancer avec le script dhcpd sous /etc/rc.d/init.d

  dhcpd [start|stop|status……]

DHCP CLIENT sous linux

- Configurer le client

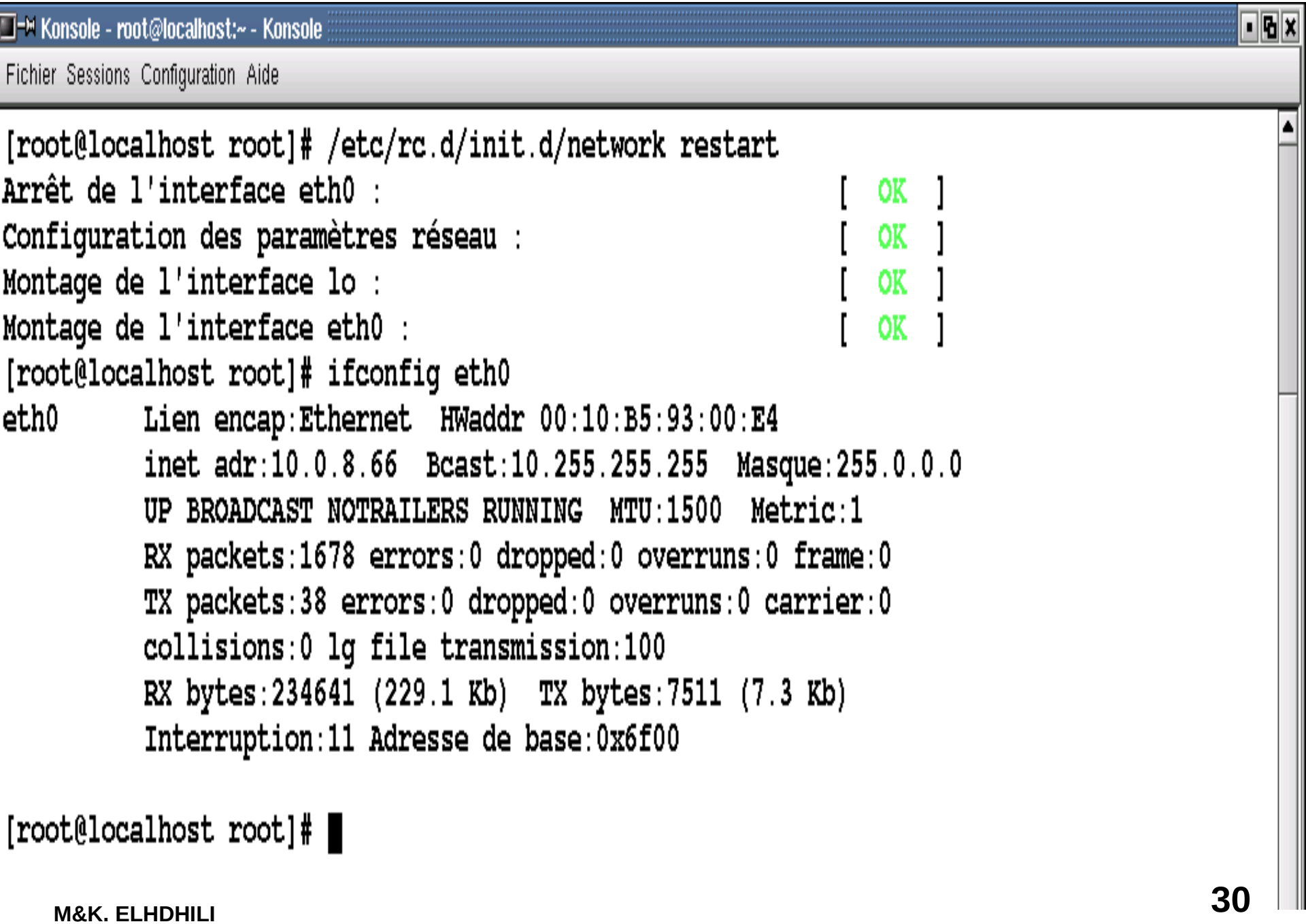
  - configurer l'interface eth0 comme client dhcp (version red hat)
  - Modifier:/etc/sysconfig/network-scripts/ifcfg-eth0
  - Relancer les service réseau /etc/rc.d/init.d/network start

Avant

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=10.255.255.255
IPADDR=10.0.8.4
NETMASK=255.0.0.0
NETWORK=10.0.0.0
ONBOOT=yes
```

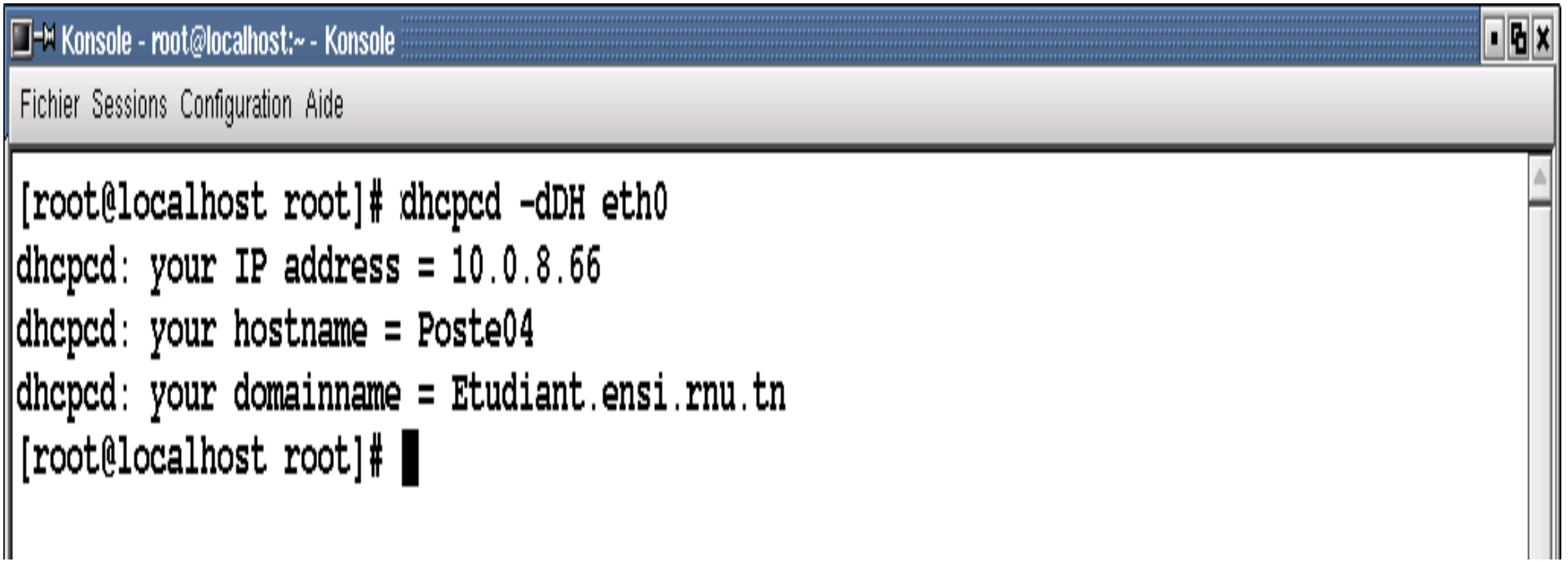
Aprés

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```


Konsole - root@localhost:~ - Konsole
Fichier Sessions Configuration Aide
[root@localhost root]# /etc/rc.d/init.d/network restart
Arrêt de l'interface eth0 : [OK]
Configuration des paramètres réseau : [OK]
Montage de l'interface lo : [OK]
Montage de l'interface eth0 : [OK]
[root@localhost root]# ifconfig eth0
eth0 Lien encap:Ethernet HWaddr 00:10:B5:93:00:E4
inet adr:10.0.8.66 Bcast:10.255.255.255 Masque:255.0.0.0
UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
RX packets:1678 errors:0 dropped:0 overruns:0 frame:0
TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 lg file transmission:100
RX bytes:234641 (229.1 Kb) TX bytes:7511 (7.3 Kb)
Interruption:11 Adresse de base:0x6f00
[root@localhost root]#

Démon client dhcpcd

- Permet d'intéragir avec le serveur dhcpd
- invoquer le démon /usr/sbin/dhcpcd par la commande dhcpcd



Commande client dhcpcd

dhcpcd [-dknrBCDHRT] [-t timeout]

[-c filename] [-h hostname] [-l leasetime]

[-s [ipaddr]] [interface]

- **Options**

-k : mettre à fin le bail .

-n : renouvellement .

-B : demander une réponse par le serveur en broadcast

-t timeout : temps d'attente d'une réponse du serveur (par défaut 60seconde).

Commande client dhcpcd (suite)

-c filename : pour que dhcpcd exécute le fichier après avoir configurer l'interface .

-H : forcer dhcpcd à affecter au hostname celui reçu par le serveur .

-D : forcer dhcpcd à affecter à domainename celui reçu par le serveur .

-l leasetime : la durée du bail recommandée par le client .

Démon client dhcpcd (suite)

- **Le démon dhcpcd gère et créé des fichiers tels que:**

  - ✓ **var/run/dhcpcd-eth0.pid :**_ image mémoire contient le pid du processus dhcpcd .

  - ✓ **/etc/dhcp/dhcpcd-eth0.info :**_contient les information obtenus par le serveur dhcp (avec eth0 est l'interface cliente dhcp) .

Démon client dhcpcd (suite)

- **/etc/resolv.conf :**_ce fichier est crée par dhcpcd quand le client reçoit **dns** et **domainename options** ,l'ancien fichier renommé en **/etc/resolv.con.sv** pour restauration en cas de problème dû à dhcpcd.

- **/etc/dhcp :**contient les fichiers que crées le démon dhcpcd .

DHCP- attaques

- Deux principale attaques:
  - Épuisement d'adresse IP (DHCP starvation)
  - Faux serveurs DHCP

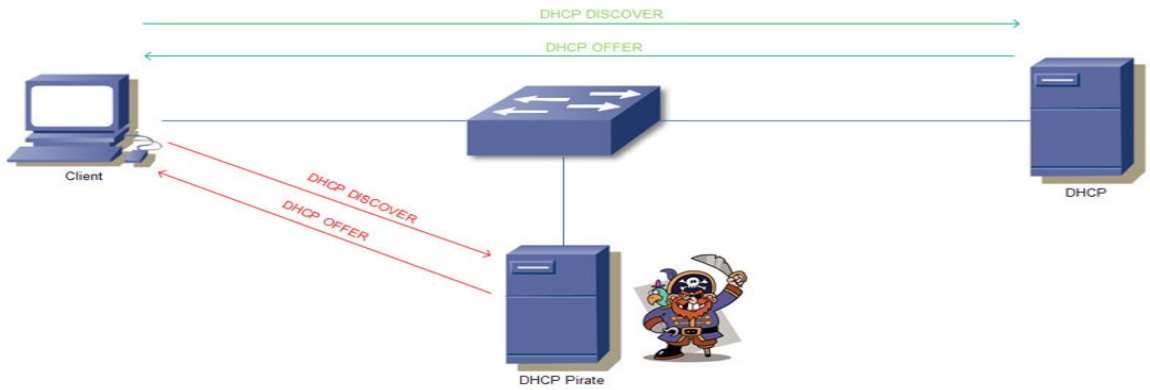
DHCP- attaques

Epuisement d'adresse IP (DHCP starvation)

- Vulnérabilité:
  - Les requêtes DHCP ne sont pas authentifiées.
- Attaque:
  - L'attaquant inonde le serveur avec des messages **DHCPREQUEST** afin de réserver toutes les adresses IP disponibles. L'attaquant doit utiliser une nouvelle adresses MAC pour chaque requête.
- Risque: Dénis de service.
- Contre mesures:
  - Limiter le nombre d'adresses MAC permises sur un port donné.
  - Authentification

Faux serveurs DHCP

- ***Vulnérabilité:*** ***Les requêtes DHCP ne sont pas authentifiées.***
- ***Attaque:*** ***L'attaquant prend le rôle d'un serveur DCHP.***
  - L'attaquant répond avec un DHCPOFFER en donnant de fausses paramètres IP à l'utilisateur
    - *Fausses adresses IP et réseau*
    - *Faux routeur par défaut*
      - L'adresse de l'attaquant si celui veut voir tout le trafic de la victime.
  - L'attaquant peut effectuer un déni de service sur le serveur légitime afin qu'il n'interfère pas avec cette attaque.



Faux serveurs DHCP

- ***Risque:***
  - Dénis de service.
  - Divulgation d'informations sensibles (p.ex. mots de passe) qui ne devraient pas être envoyées sur un port.

- ***Contre mesures:***
  - DHCP snooping : Défense contre le DHCP spoofing
    - *Implémenté dans certains commutateurs CISCO*
    - *Mettre en place une liste de ports sur le commutateur sur lequel se trouvent les "trusted dhcp server".*
    - ➔ *Limite l'impact de l'attaque*

Chapitre 2 : Mise en place et sécurisation de services réseau

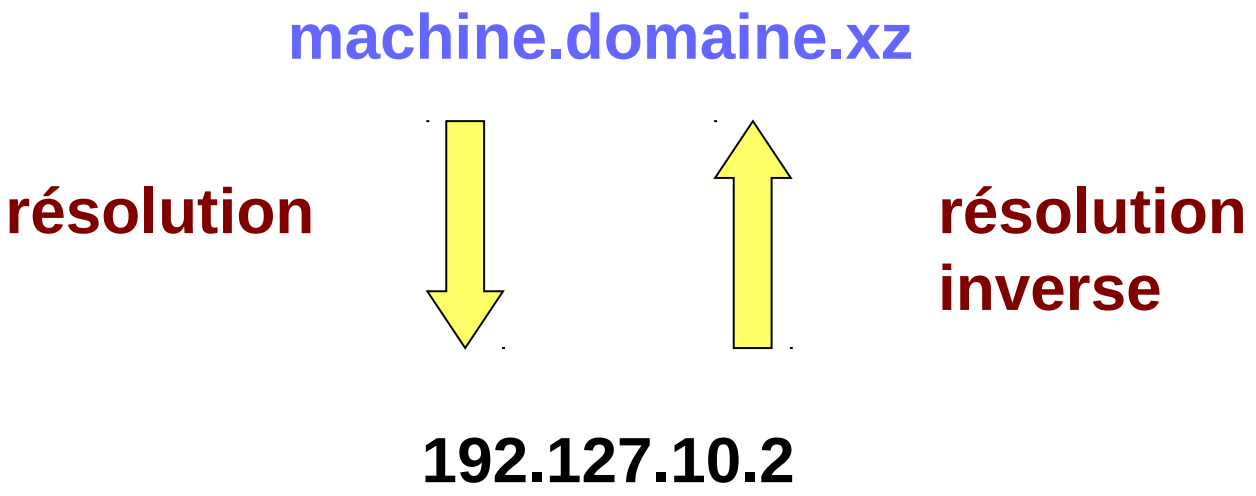
Partie 2 :

DNS (Domain name service)

- Objectifs
- Fonctionnement
- Configuration et options
- Attaques
- Sécurisation

DNS: fonctionnalités

- Assurer la conversion entre les noms d'hôtes et les adresses IP.

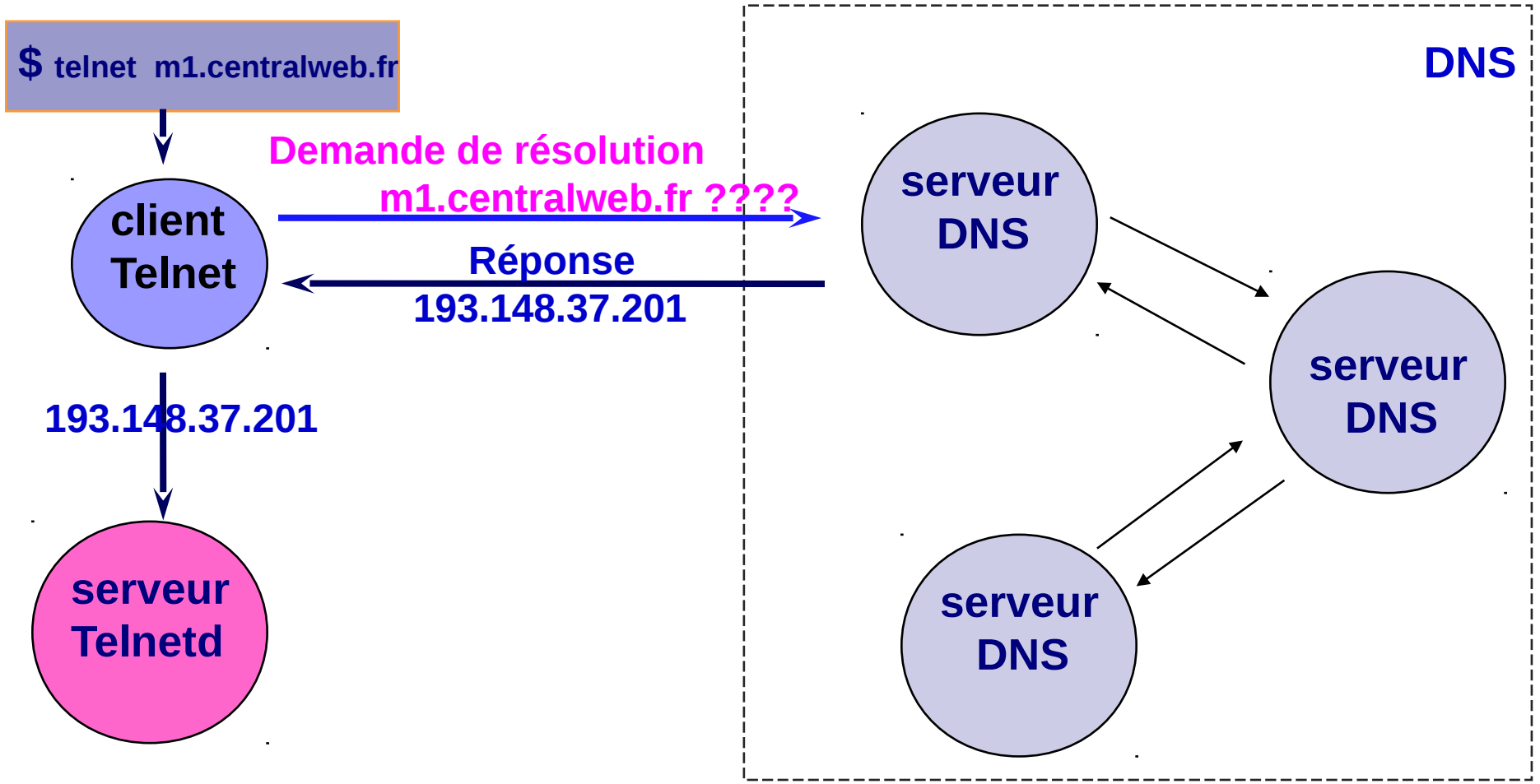


- Exemple:
  - Le nom www.yahoo.fr correspond à l'adresse IP 192.95.93.20 de la machine www sur le réseau yahoo.fr

Plan

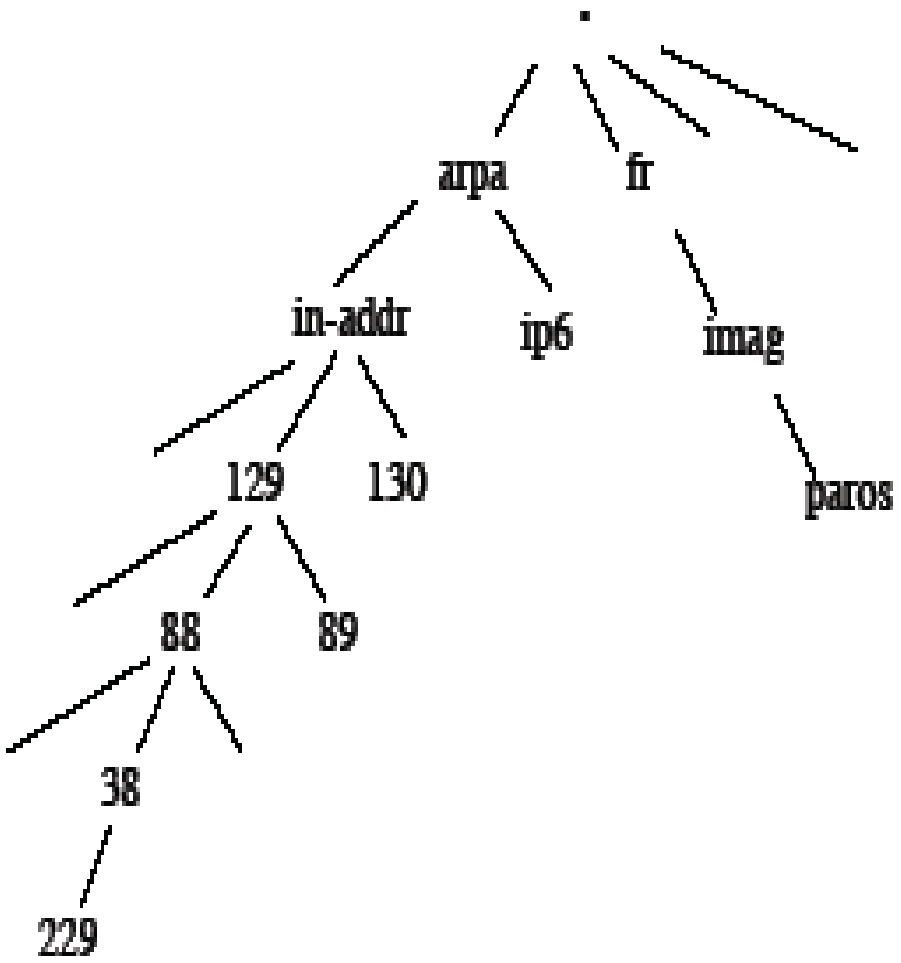
- Fonctionnalités du DNS
- Résolutions de noms et résolution inverse
- Types de serveurs de noms
- Entête DNS
- Analyse de datagrammes DNS
- Mise en œuvre de DNS
- Attaques et sécurisation

DNS: résolution de noms



DNS: Résolution de noms inverse

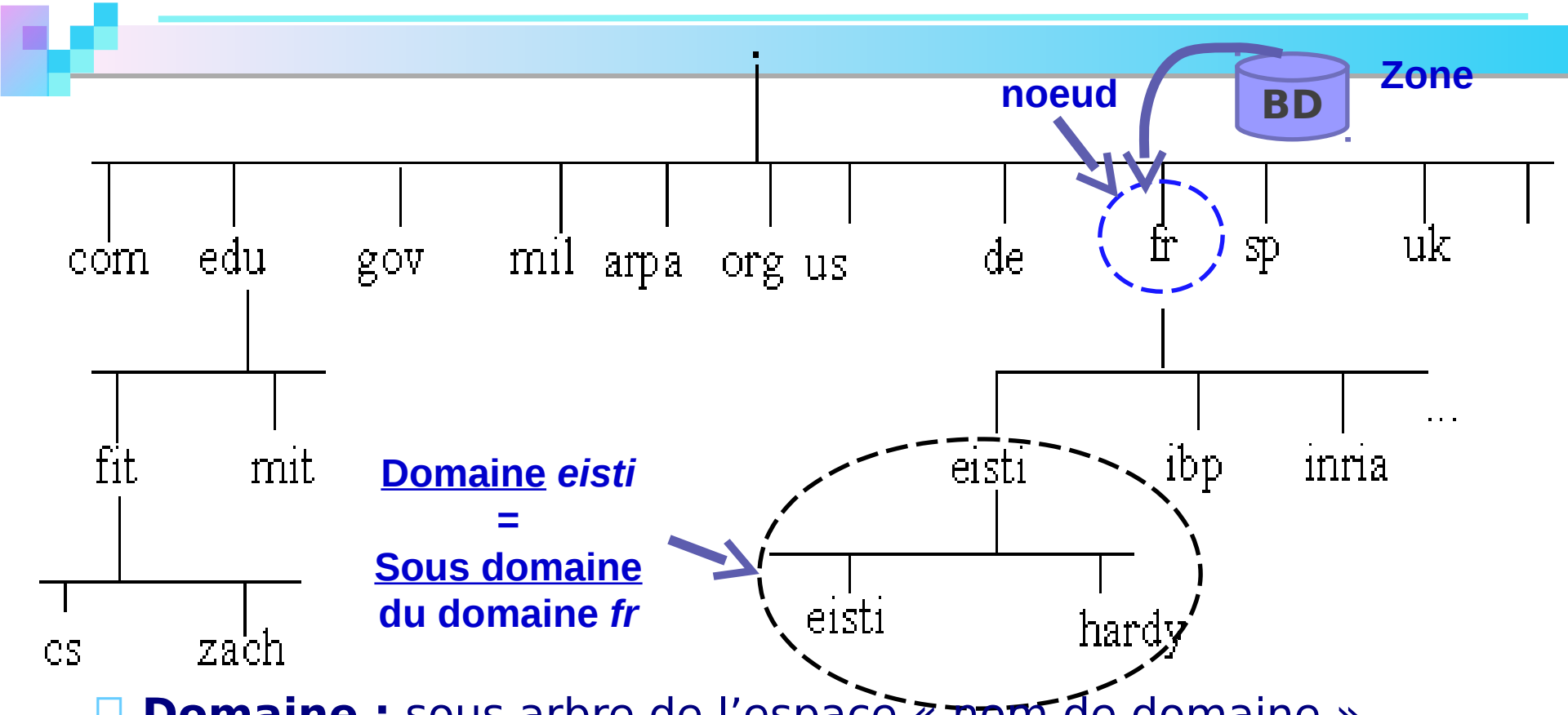
- Trouver le nom à partir de l'adresse
- Même principe que pour les noms
- Chaque octet de l'adresse IP est vue comme un sous domaine.
- Un domaine particulier ***: arpa***
- Sous domaines
  - ***in-addr*** pour les adresses IPV4
  - ***ip6*** pour les adresses IPV6



Exemple: **paros.imag.fr**

229.38.88.129.in-addr.arpa

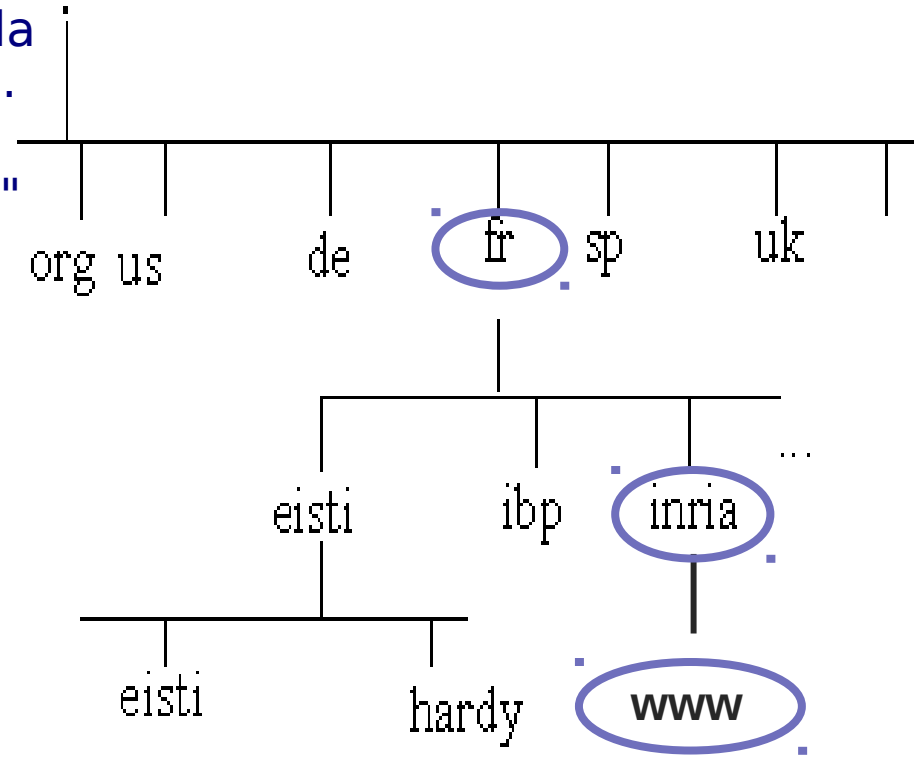
Terminologies



- **Domaine :** sous arbre de l'espace « nom de domaine »
- **Zone :** contient les données propres à une partie de l'espace « nom de domaine » sous l'autorité d'un serveur de noms (SOA: *start of a zone of authority ou sphere of authority)*.
- **Délégation:** Transfert de la responsabilité d 'une zone à une ou plusieurs de ses sous-zones.

Sémantique des noms

- Le nom qualifié ou complet (FQDN) d'une machine se lit en partant de la feuille et en remontant dans l'arbre.
- Chaque niveau est séparé par un "."
- Le domaine racine n'a pas de nom et par convention est appelé "."
- Chaque niveau de l'arborescence garantie que les noms de ses fils soient uniques.
- Un nom de domaine est constitué par une suite de noms séparés par des points.



➔ www.inria.fr

Les Serveurs de noms

Un serveur de noms

- Enregistre les données propres à une partie de l'espace nom de domaine dans une zone.
- Possède l'autorité administrative sur cette zone.
- Peut avoir autorité sur plusieurs zones.

Les Serveurs de noms

Types de serveurs de noms:

- **Serveur primaire (maître)**:
  - contient l'original des données sur la zone dont il a l'autorité administrative
- **Serveur cache (forwarding)** :
  - Relaye des requêtes vers d'autres serveurs
  - Garde en cache les résultats les plus récents pour un temps de réponse meilleur
- **Serveur secondaire (esclave)** :
  - Seconde automatiquement le serveur de noms maître
  - Interroge périodiquement le serveur de nom primaire et met à jour les données

Serveurs de Noms (suite)

- **La redondance permet la défaillance éventuelle du primaire et du (des) secondaire(s).**
- **Il y a un serveur primaire et généralement plusieurs secondaires**
- **Un serveur de nom peut être primaire pour une (des) zone(s) et secondaire pour d'autre(s).**
- **Serveurs racine (décrits dans /var/named/named.ca)**
  - Environ 15 serveurs de nom répartis dans le monde
  - Connaissent tous les serveurs de premier niveau ***: .tn , .fr, .com***, ...
  - Serveur origine (ou primaire, ou maitre) géré **par IANA/ICANN** (*IANA* — Internet Assigned Numbers Authority, ICANN-Internet Corporation for Assigned Names and Numbers)
  - Serveurs MIROIRS (ou secondaire, ou esclave)

Entête DNS

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
identificateur de la requête (recopié dans la réponse)															
qr	opcode				aa	tc	rd	ra	Z			rcode			
QDCOUNT nombre d'entrées dans la section question															
ANCOUNT nombre d'entrées (RR) dans la section réponse															
NCOUNT nombre d'entrées (NS) dans la section réponse															
ARCOUNT nombre d'entrées (RR) dans la section additionnel															

qr: question (0) ou réponse (1)

Opcode:

- 0 - Requête standard (Query)
- 1 - Requête inverse (Iquery)
- 2 - Status d'une requête serveur (Status)
- 3-15 - Réservé pour des utilisations futurs

- **aa** : réponse d'une autorité
- **tc** : message tronqué
- **rd** : récursion désiré
- **ra** : récursion acceptée
- **Z:** utilisation futur
- **rcode**: type de réponse

Entête DNS (suite)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
identificateur de la requête (recopié dans la réponse)															
qr	opcode				aa	tc	rd	ra	Z			rcode			
QDCOUNT nombre d'entrées dans la section question															
ANCOUNT nombre d'entrées (RR) dans la section réponse															
NCOUNT nombre d'entrées (NS) dans la section réponse															
ARCOUNT nombre d'entrées (RR) dans la section additionnel															

- **rcode:** indique le type de réponse.
  - 0 - Pas d'erreur
  - 1 - Erreur de format dans la requête
  - 2 - Problème sur serveur
  - 3 - Le nom n'existe pas
  - 4 - Non implémenté
  - 5 - Refus
  - 6-15 - Réservés

Les RR (Resource Records)

- La base de données des serveurs de noms = ensemble de RR répartis en classes
- La seule classe implémenté: Internet (IN)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Nom: Nom du domaine où se trouve le RR															
Type (2octets): type de donnée utilisées dans le RR															
Classe ((2octets): famille de protocoles ou un protocole (IN: Internet)															
TTL(4octets): durée de vie des RRs (utilisé lorsque les RR sont en cache)															
longueur: longueur des données suivantes															
Données: Données identifiant la ressource															

Les RR (champs type)

Entrée	Valeur	Désignation
A	01	Adresse de l'hôte
NS	02	Nom du serveur de noms pour ce domaine
MD	03	Messagerie (obselete par l'entrée MX)
MF	04	Messagerie (obselete par l'entrée MX)
CNAME	05	Nom canonique (Nom pointant sur un autre nom)
SOA	06	Début d'une zone d'autorité (informations générales sur la zone)
MB	07	Une boite à lette du nom de domaine (expérimentale)
MG	08	Membre d'un groupe de mail (expérimentale)
MR	09	Alias pour un site (expérimentale)
NULL	10	Enregistrement à 0 (expérimentale)
WKS	11	Services Internet connus sur la machine
PTR	12	Pointeur vers un autre espace du domaine (résolution inverse)
HINFO	13	Description de la machine
MINFO	14	Groupe de boite à lettres
MX	15	Mail exchange (Indique le serveur de messagerie. Voir [Rfc-974] pour plus de détails
TXT	16	Chaîne de caractère

Le DNS Côté Client

- **Le client demande une adresse IP ou la résolution d'un nom par une requête UDP (ou TCP) sur le port 53 (“domain”)**

- **Liste des serveurs de noms à contacter : /etc/resolv.conf :**

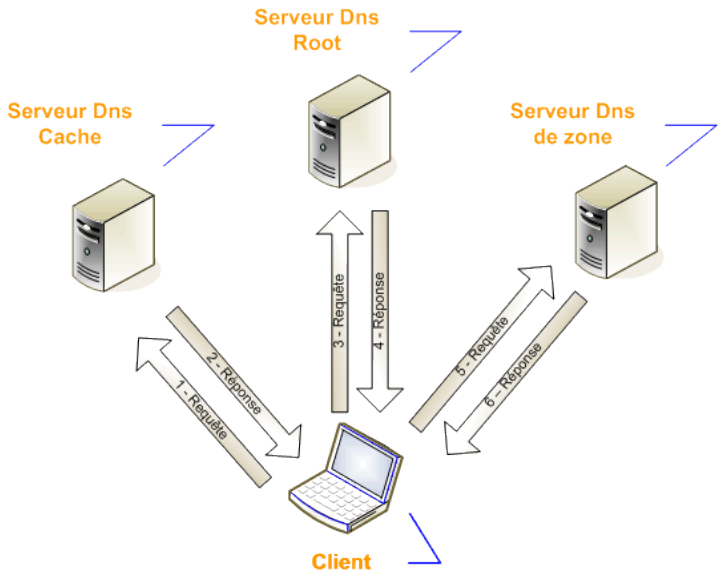
search <nom_domaine>

nameserver <@_IP du serveur>

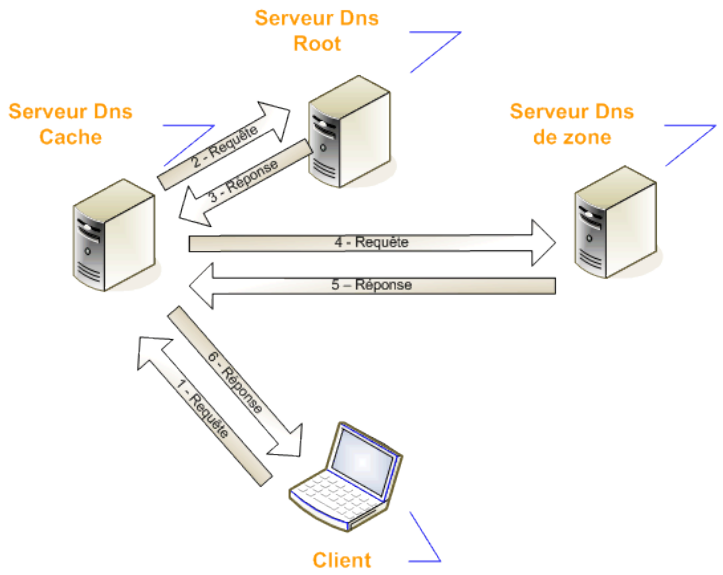
- **Peut être mis à jour lors de la configuration dynamique de l'interface (DHCP)**
  - Indiquer **PEERDNS=no** dans le fichier de configuration de l'interface pour empêcher les modifications automatiques de /etc/resolv.conf

Le Serveur DNS

- Le serveur reçoit la requête
- Mode récursif: Si le serveur n'a pas de réponse, il demande au serveur racine ou fait suivre la requête (pour le cas d'un serveur cache)
- Mode itératif: Le serveur sollicité prend le rôle de résolveur



Mode itératif



Mode Récursif

source des figures: www.frameip.com

Analyse de datagrammes DNS

DNS: mise en ouevre

Profil du Service DNS

- **Implémentation la plus courante : Bind**
- **Paquetages : *bind, bind-utils, caching-nameserver***
- **Démons : /etc/ini.d/named**
- **Ports : 53 udp, 53 tcp**
- **Configurations : /etc/named.conf et /var/named/***

Configuration de BIND

- **Le fichier de configuration par défaut est /etc/named.conf**
  - Lu par named (le démon de BIND) au démarrage
  - Directives de configuration :
    - déclaration de zones, options, listes de contrôle d'accès, etc.
  - Les commentaires peuvent être de type C, C++ ou shell
  - On peut spécifier des réseaux avec la notation réseau/masque
  - Les directives de configuration de BIND se terminent toujours par un point-virgule

/etc/named.conf : Options Globales

- **Se déclarent avec la directive « options » :**

```
options {
directory "/var/named";          //base de données
forwarders {203.50.0.137;};     //serveur racine à contacter
allow-query {192.100.100/24;};  // machines autorisées
allow-transfer {192.100.100/24;};     //serveurs caches autorisés
};
```

Déclaration des zones

- Se déclarent avec la directive « zone »
- Les fichiers de zones sont placés par défaut dans /var/named/.
- Les noms de fichiers sont arbitraires.
- Chaque zone directe doit avoir une zone de résolution inverse sauf la zone racine.
- Zone racine : "."

```
zone "." {
 type hint;   //relative a internet
file "named.ca"; }; //fichier zone
```

Déclaration des zones

- **Zones Maîtres (primaires)**

```
zone " infcom.rnu.tn" {
type master;          // serveur maître (primaire)
file « infcom.rnu.tn.zone"; }; // fichier de zone
```

- **Zones Esclaves (secondaires)**

```
zone " infcom.rnu.tn " {
type slave;
masters { 192.100.100.1; };
file " infcom.rnu.tn.zone"; };
```

Déclaration des zones

Zones de Résolution Inverse

- **Le nom de zones se termine par un domaine spécial : .in-addr.arpa**

```
zone "10.100.172.in-addr.arpa" {
type slave;
masters { 172.100.10.1; };
file "172.100.10.zone"; };
```

Zones Spéciales

- **Zone racine : pas de résolution inverse**
- **Zone de *loopback* : "0.0.127.in-addr.arpa »**

```
zone "0.0.127.in-addr.arpa" {
    type master;
    file "0.0.127"; }; //fichier zone
```

Fichiers de Zones

- **fichiers de zones = Base de données du services DNS**
  - contiennent la déclaration des machines appartenant à la zone.
  - se trouvent généralement dans /var/named/
  - Commencent par $TTL (*time to live* ou durée de vie)
  - La première *définition de ressource* est le *début d'autorité* (SOA) de la zone
  - Définitions de Ressource (*Resource Record* ou RR)

Syntaxe : *[domain] [ttl] [class]* <type> <rdata>

- ***[domain]*** spécifier le domaine ou utiliser le domaine courant
- ***[ttl]*** temps de conservation en cache
- ***[class]*** classification de définition (généralement **IN**)
- **<type>** type de définition (**SOA, MX, A,** etc)
- **<rdata>** données spécifiques à la définition

SOA (*Start Of Authority*)

- **Tout fichier de zone doit avoir un SOA**

```
@ IN   SOA   ns.redhat.com.      root.redhat.com. (
2001042501 ; //numéro de série
300 ; //rafraîchissement
60 ; //nouvelle tentative
1209600 ; //expiration
43200 ; //durée de vie minimale pour les réponses négatives )
```

- **Les valeurs ne s'expriment pas obligatoirement en secondes**

Autres ressources

- **NS (*name server* ou serveur de noms)**
- **Il doit y avoir une définition NS pour chaque serveur de noms maître ou esclave d'une zone**
- **Les définitions NS pointent sur tout serveur esclave qui doit être consulté par le serveur de noms du client si le serveur maître est indisponible**
  - **@ IN NS ns.redhat.com.**
  - **redhat.com. IN NS ns1.redhat.com.**

Autres ressources

- Les définitions A associent un nom de machine à une adresse IP
  - mail IN A 192.100.100.3
  - login.redhat.com. IN A 192.100.100.4
- Les définitions CNAME fournissent des alias d'adresses
  - pop IN CNAME mail
  - ssh IN CNAME login.redhat.com.
- Les définitions PTR associent une adresse IP à un nom de machine
  - 3.100.100.192.in-addr.arpa IN PTR mail.redhat.com.
- MX associe un domaine à une machine chargée de gérer le courrier de ce domaine
  - redhat.com. IN MX 5 mail.redhat.com.
- HINFO fournit des informations supplémentaires sur les machines
  - mail IN HINFO i686 Linux-2.0.36

Exemple complet : déclaration d'un serveur maitre pour une zone

- **Scénario :**
  - Poste3 est une machine du réseau qui veut se déclarer maitre pour une zone regroupant les machines poste5 et poste6.

- **Seront crées :**
  - Déclaration de la zone directe et inverse pour la nouvelle zone (exemple : zone3)
  - Fichier de résolution directe : /var/named/poste3.zone
  - Fichier de résolution inverse : /var/named/0.0.10.5.in-addr.arpa

/etc/named.conf :

```
                    /*les options globales par défauts sont conservées*/
                /* les 3 zones suivantes sont existantes et à ne pas modifier */
zone "." in {
      type hint;
      file "named.ca";
  };
  zone "localhost" in {
      type master;
      file "localhost.zone";
  };
  zone "0.0.127.in-addr.arpa" in {
      type master;
      file "named.local";
  };
 /* les 2 zones suivantes servent à déclarer poste3 maitre pour « zone3 » */
   // zone directe :
         zone "zone3" in {
        type master;
        file "poste3.zone";
  };
  // zone inverse :
         zone "0.0.10.in-addr.arpa" in {
        type master;
        file "0.0.10.5.in-addr.arpa";
         };
```

/var/named/poste3.zone : fichier de zone directe

```
$TTL 1W
@  IN SOA   poste3.zone3.   root.poste3.zone3. (
                  42          ; serial
                  2D          ; refresh
                  4H          ; retry
                  6W          ; expiry
                  1W )        ; minimum

zone3.          IN    NS          poste3.zone3.
poste3.zone3.                IN    A          10.0.0.5
poste5.zone3.                IN    A          10.7.7.8
poste6.zone3.                IN    A          10.10.10.15
```

/var/named/0.0.10.5.in-addr.arpa : fichier de zone inverse

```
$TTL 1W
@  IN SOA       poste3.zone3.   root.poste3.zone3. (
                42          ; serial
                2D          ; refresh
                4H          ; retry
                6W          ; expiry
                1W )            ; minimum

0.0.10.in-addr.arpa.        IN   NS        poste3.zone3.
5.0.0.10.in-addr.arpa.      IN   PTR            poste3.zone3.
8.7.7.10.in-addr.arpa.      IN   PTR            poste5.zone3.
15.10.10.10.in-addr.arpa.       IN   PTR            poste6.zone3.
```

Utilitaires BIND

- **On trouve dans le paquetage *bind-utils* plusieurs utilitaires pratiques, dont :**
  - **host** : pour recueillir des informations sur une machine ou un domaine **host -a ns.redhat.com**
    - **host -al redhat.com**
  - **dig** : pour envoyer des requêtes directement au serveur de noms **dig @ns redhat.com any**

- **BIND échouera au lancement dans le cas d'erreurs de syntaxe**
- **named-checkconf : vérifie la syntaxe de /etc/named.conf**
- **named-checkzone : vérifie un fichier de zone spécifique**

Outils de résolution de noms

- **Dig: remplace la commande nslookup**
  - Syntaxe:

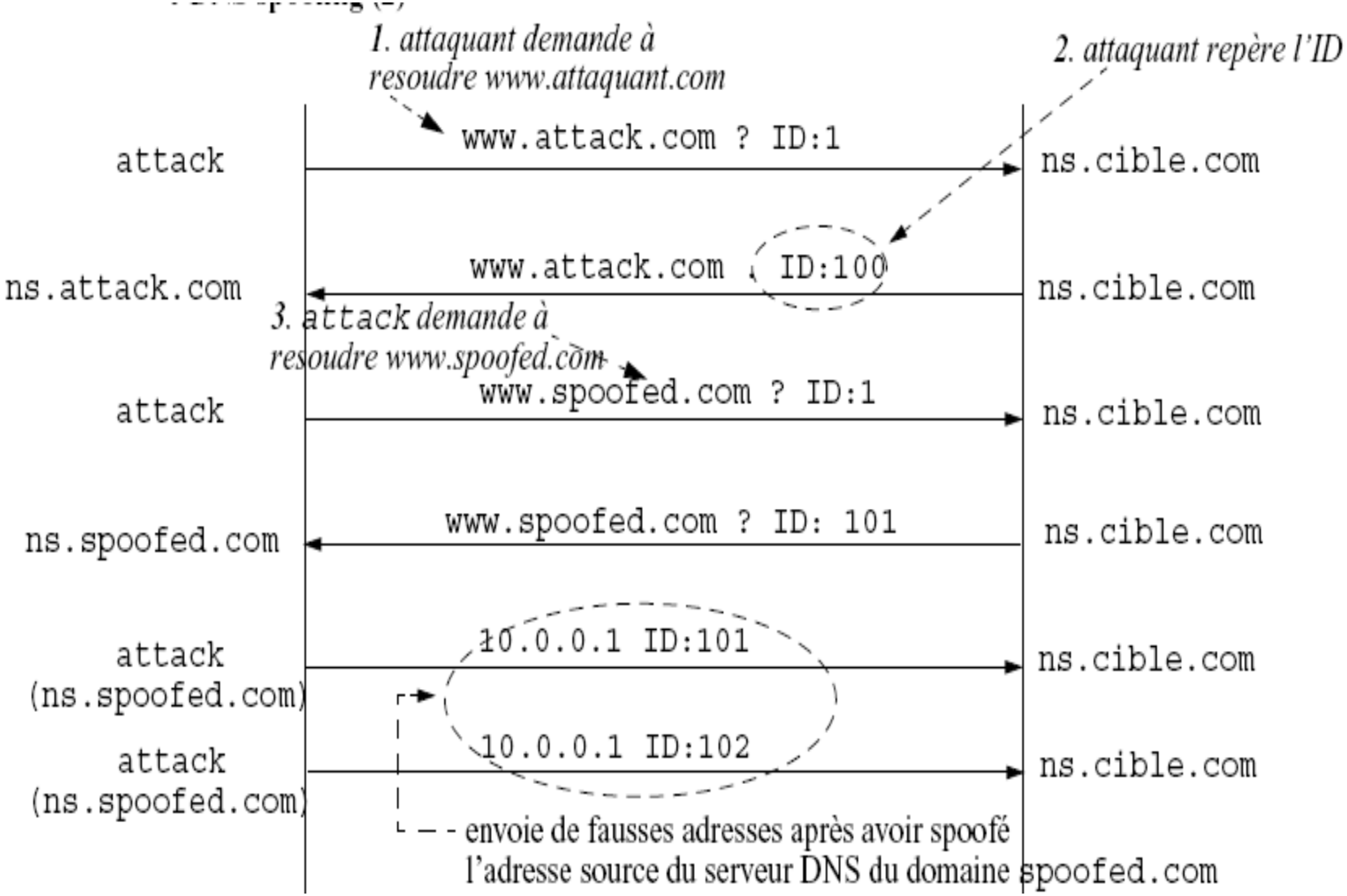
    dig hosname

    dig –i @IP
  - Requiert un nom de domaine qualifié (FQDN)
- **host**
  - Non-interactif seulement
  - L'IP de serveur n'a pas besoin d'être résolvable
- **nslookup (déconseillé)**

Attaque DNS spoofing

- ***Serveurs DNS envoient régulièrement des requêtes du type :***
  - DNS Query (Quelle est l'adresse de www.abc.tn?)
- ***Serveurs DNS reçoivent alors des réponses du type***
  - DNS Answer (www.abc.tn → → 195.93.66.41)
- ***Ces réponses ne sont pas authentifiées (pas de cryptographie)***
- ***Bien que:***
  - L'entête DNS contient un numéro permettant d'associer une réponse à une question (16 bits). **Mais**, ce numéro peut être deviné!
  - Port UDP du client DNS (16 bits) **Mais**, le client peut être amené à toujours utiliser le même port pour faciliter la configuration du pare-feu.
- ***→ Il est simple de forger une réponse malicieuse à une question légitime***
  - ***DNS spoofing (cache poisoning)***

Attaque DNS cache poisoning



Attaque DNS cache poisoning

- cette attaque nécessite que attack contrôle le serveur DNS **ns.attack.com**

et qu'il sait prédire les numéros de séquence DNS de **dns.cible.com**

1. **attack** envoie une requête DNS pour le nom www.attack.com au serveur DNS du domaine **cible.com**
2. le serveur DNS relaie la demande au DNS du domaine **attack.com**;

==> ainsi attack peut sniffer la requête pour récupérer l'ID

3. attack falsifie @ IP associée à un nom de machine, www.spoofed.com,et émet ensuite une requête de résolution pour **www.spoofed.com** vers **ns.cible.com**;

==> **ns.cible.com** relaie la requête en l'envoyant à **ns.spoofed.com**

4. attack envoie réponses DNS falsifiées à sa propre requête en se faisant passer pour **ns.spoofed.com** (plusieurs réponses pour avoir plus de chances de tomber sur le bon ID)

=>le cache DNS de **cible.com** est donc corrompu

Attaque DNS cache poisoning

- ***Vulnérabilité:***
  - Les messages DNS ne sont pas authentifiés.
- ***Attaque:***
  - L'attaquant envoie de faux messages à un serveur DNS local.
    - *Réponse qui spécifie un nom de domaine différent que celui demandé ➔ à ignorer*
    - *Réponse qui spécifie un serveur DNS appartenant à un domaine différent de celui demandé ➔ douteux*
    - *Réponse contenant une adresse suspecte (frauduleuse)*
- ***Risque:***
  - Redirection du trafic légitime

Attaque DNS cache poisoning

- ***Sécurisation:***
  - ***Configuration du serveur DNS pour qu'il ne résolve directement que les noms de machine du réseau sur lequel il a autorité.***
  - ***Autorisez seulement machines internes à demander la résolution de noms de domaines distants.***
  - ***Mise à jour des logiciels assurant le service DNS***