

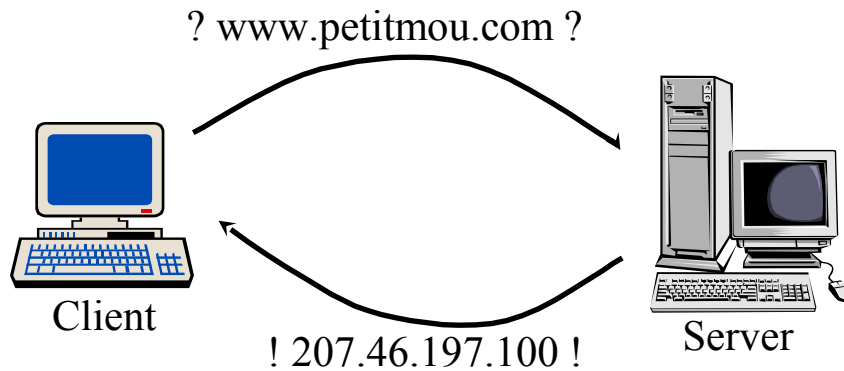
# Niveau 3 – 4 – 7

## DNS – DHCP

# DNS

- Domain Name System (or Service)
- Permet de faire le mapping entre une adresse symbolique (www.petitmou.com) et une adresse IP (207.46.197.100)
- UDP (ou TCP) Port 53
- Notion de FQDN (Fully Qualified Domain Name): « test » vs « test.brussels.petitmou.com »

# DNS – Exemple



Modèle client-serveur !

# DNS – Format du paquet

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Identification																Flags															
Number of questions																Number of answers															
Number of Authority RRs																Number of additional RRs															
Question(s)																															
Answer(s)																															

# DNS – Divers

- Il s'agit donc d'une DB distribuée sur l'internet !
- Quand une application doit transformer un nom symbolique en adresse IP, elle devient un client du DNS.
- Pourquoi une adresse symbolique ? Parce que c'est plus simple à retenir.
- La structure de la DB est hiérarchique ! Les niveaux étant séparés par des points (pingouin.petitmou.com)

# DNS – Notion d'autorité

- Chaque partie du DNS (client, DNS intermédiaire) fait partie d'un arbre et contrôle une partie de cet arbre.
- Un serveur DNS a autorité sur le sous-arbre qu'il contrôle
- Quand un serveur reçoit une demande pour un nom de domaine sur lequel il n'a pas autorité, il envoie la requête au niveau supérieur
- Qui gère les serveurs ? Les registrars !

# DNS – Les top-level domains (TLD)

## Générique (en pleine évolution):

- com (commercial),
- edu (education),
- gov (gouvernement),
- mil (military),
- net (network support center),
- org (autres),
- int (international organisation)
- biz (business)
- info (information)
- name (information personnelles)
- coop (monde coopératif)
- aero (compagnies aériennes et fabricants)
- museum
- xxx (adulte)
- + .jobs, .travel, .cat, .mobi, .tel, .asia

## Par pays (environ 260):

- fr
  - uk
  - be
  - as
  - au
  - eu
  - us ...
- Défini dans ISO 3166
  - Dans certains pays, il est impossible d'avoir un nom '.pays'. Il faut passer par des sous-domaines (.co.uk)

# IDN – Internationalized Domain Name

- Possibilité d'utiliser des caractères non-ascii (éèëêàáâäùçñ etc...)
- Possibilité d'utiliser d'autres alphabets (cyrillique – arabe etc...)
- Utilisation de 'ToAscii' et 'ToUnicode'
- Conversion en PunnyCodes (RFC 3492 - algorithmes)
- Prepend de “xn--”
- Exemple: bücher.ch → xn--bcher-kva.ch



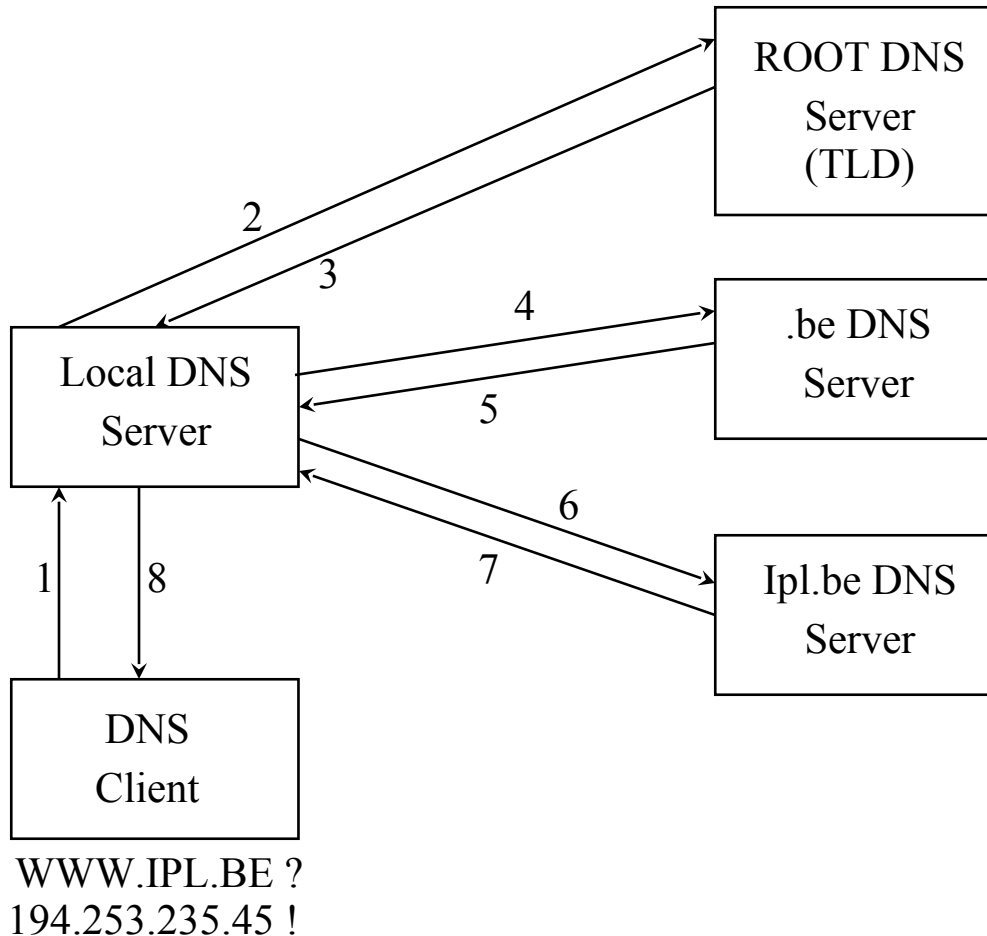
# DNS – Fonctionnement 1

- Utilisation d'un champ 'Identification' pour faire correspondre les réponses aux demandes
- Divers 'flags' pour décrire l'état de la réponse, de savoir si une récursion est possible, si elle est 'autoritaire' ou pas...
- Nombre de requêtes et de réponses dans ce paquet (le nombre de réponses vaut 0 pour une requête et au moins 1 pour une réponse)
- Chaque requête et chaque réponse a un type. Les paquets contiennent un ou plusieurs Ressource Records (RR) qui décrivent ce type.

# DNS – Fonctionnement 2

- Le client envoie une requête à son DNS local.
- Le DNS local n'a pas autorité pour ce nom, il envoie la requête à un 'root (top-level)' DNS
- Le root DNS renvoie l'adresse du sous-domaine au DNS local.
- Le DNS local renvoie la requête au DNS reçu etc...

# DNS – Fonctionnement 3



# DNS – Les root DNS

- a.root-servers.net 198.41.0.4, 2001:503:ba3e::2:30 VeriSign, Inc.
- b.root-servers.net 192.228.79.201 University of Southern California (ISI)
- c.root-servers.net 192.33.4.12 Cogent Communications
- d.root-servers.net 199.7.91.13, 2001:500:2d::d University of Maryland
- e.root-servers.net 192.203.230.10 NASA (Ames Research Center)
- f.root-servers.net 192.5.5.241, 2001:500:2f::f Internet Systems Consortium, Inc.
- g.root-servers.net 192.112.36.4 US Department of Defence (NIC)
- h.root-servers.net 128.63.2.53, 2001:500:1::803f:235 US Army (Research Lab)
- i.root-servers.net 192.36.148.17, 2001:7fe::53 Netnod
- j.root-servers.net 192.58.128.30, 2001:503:c27::2:30 VeriSign, Inc.
- k.root-servers.net 193.0.14.129, 2001:7fd::1 RIPE NCC
- l.root-servers.net 199.7.83.42, 2001:500:3::42 ICANN
- m.root-servers.net 202.12.27.33, 2001:dc3::35 WIDE Project

# DNS – Types

- Chaque query / answer est d'un type particulier:

- A: Address record: nom -> IPv4
- AAAA: Address record: nom -> IPv6
- CNAME: Canonical name: Alias
- MX: Mail exchange: mail servers
- PTR: Pointer: IPv4 -> nom (alias 'reverse', puis inverse de A)
- NS: Name server: serveur DNS du domaine
- SRV: Serveur SIP
- ...

# DNS – TTL

- Les records DNS ont un TTL, afin de pouvoir contrôler la durée de la validité d'un record...
- Plus long: moins de requêtes
- Plus court: plus de requêtes, mais plus de contrôle (vitesse de propagation de changement plus élevée)

# DNS – IPv6

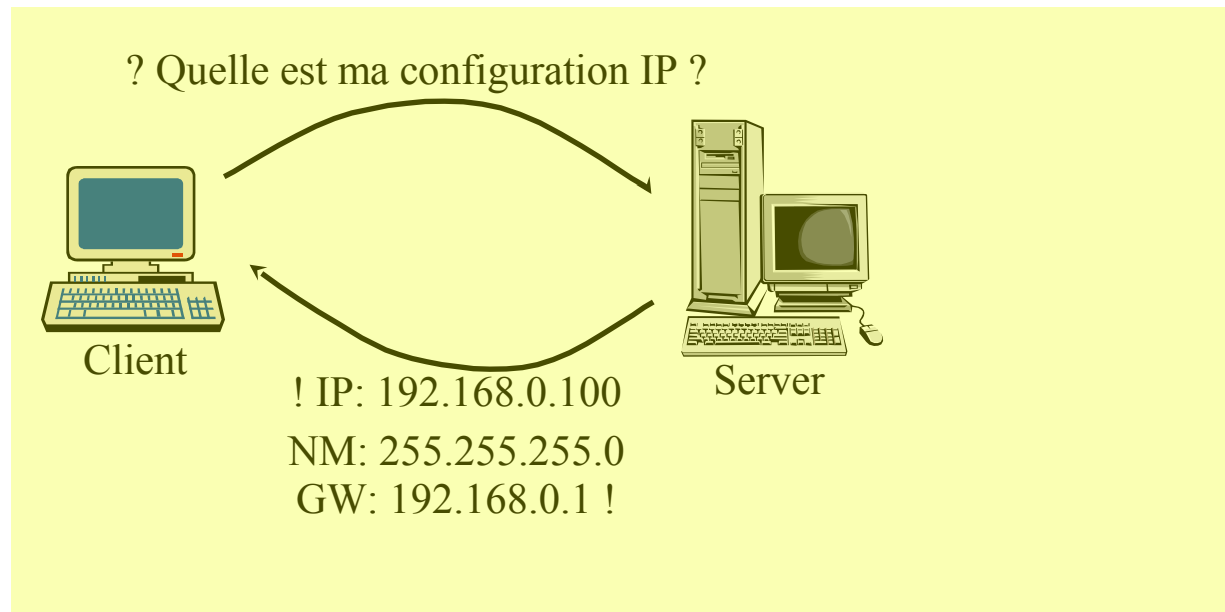
- De nouveaux types de RR ont été définis pour pouvoir renvoyer des adresses IPv6.
- Nouveau type également (AAAA)

# DHCP

- Dynamic Host Configuration Protocol
- RFC 2131. Port UDP 67 (Serveur) et 68 (Client)
- Basé sur une architecture client-serveur
- But: permettre au client d'obtenir automatiquement sa configuration au niveau IP, en la demandant à un serveur
- Basé sur BOOTP (basé sur une configuration manuelle sur le serveur, alors que DHCP offre une possibilité d'allocation d'adresse dynamique)



# DHCP – Exemple



Modèle client-serveur !

# DHCP – Les plus

- Les requêtes DHCP sont des paquets broadcast – les réponses peuvent l'être aussi (flags) ...
- Notion de 'lease': les paramètres sont alloués pour une durée déterminée
- DHCP offre aussi une possibilité de récupération et de réallocation dynamique d'adresse grâce à un mécanisme de leasing

# DHCP – Les plus

- Les requêtes (broadcast) peuvent passer les routeurs (option ‘DHCP helper’ ou ‘BOOTP helper’ ou ‘UDP helper’ sur le routeur)
- Si pas, le serveur doit être dans le même broadcast domain que le client

# Paquet ARP (rappel)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Hardware Type																Protocol type															
Hardware address length									Protocol address length									Opcode													
Source Hardware Address																															
Source Protocol Address																															
Destination Hardware Address																															
Destination Protocol Address																															

# DHCP – Format du paquet

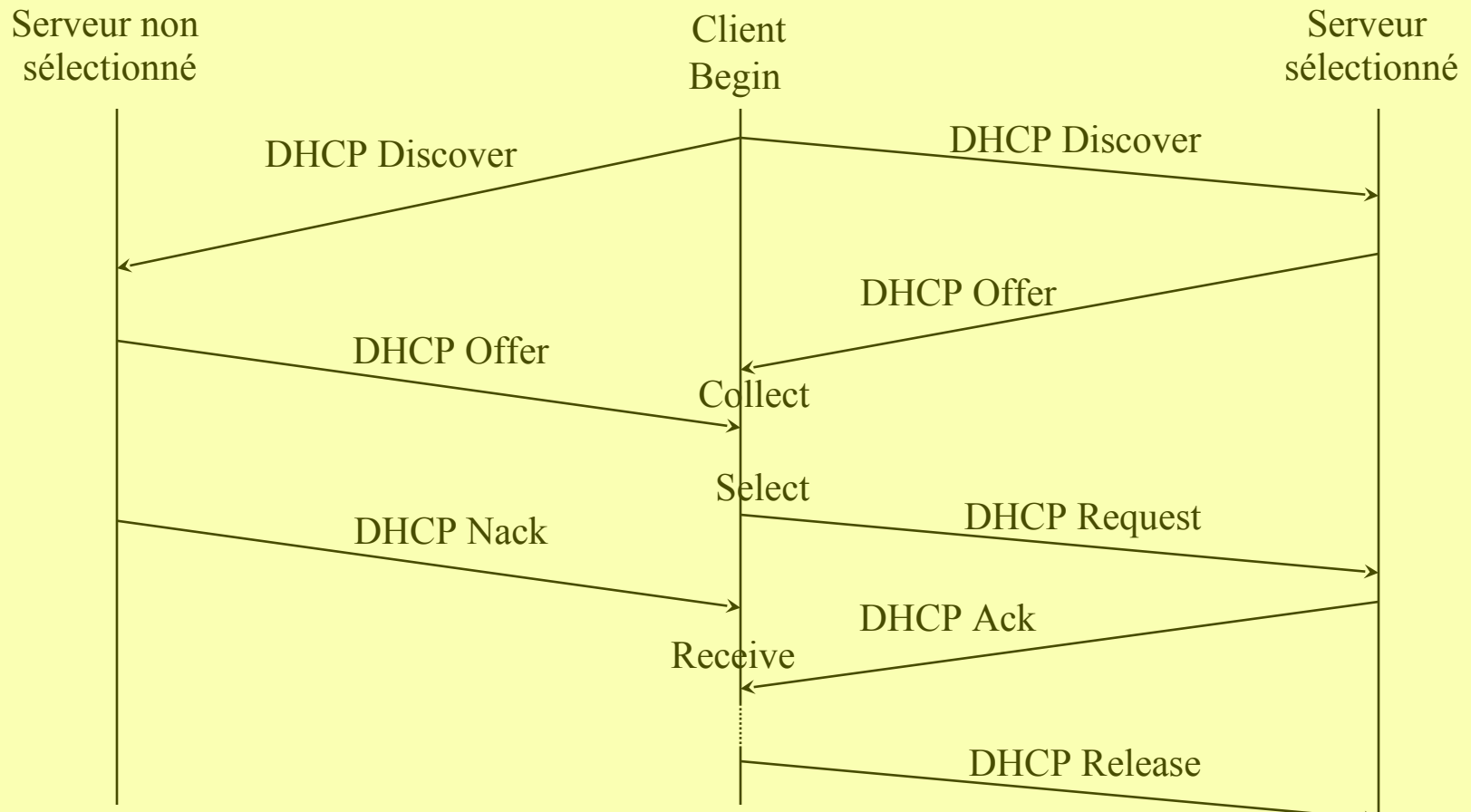
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Opcode	HW Type	HW Address Length	Hop Count
Transaction ID			
Number of seconds		Flags	
Client IP Address			
Your IP Address			
Server IP Address			
Gateway IP Address			
Client HW Address (16 Bytes)			
Server Hostname (64 Bytes)			
Boot Filename (128 Bytes)			
OPTIONS (> 4 Bytes) En particulier: DHCP Message Type			

# DHCP – Les champs

- Opcode: 1 = Bootrequest, 2 = Bootreply
- Filename: 128 Bytes → Limitation !
- Client IP address: utilisé lors du lease (pas pour l'acquisition de l'adresse)
- Your IP address: l'adresse assignée au client par le serveur
- Server IP address: adresse du serveur assignant l'adresse

# DHCP – Fonctionnement



# DHCP – Les messages (référence) – 1

- DHCPDISCOVER: Le client cherche les serveurs
- DHCPOFFER: Les serveurs répondent au client
- DHCPREQUEST: Réponse du client au serveur ou extension du lease
- DHCPRELEASE: Le client annonce au serveur qu'il n'a plus besoin de l'adresse
- DHCPINFORM: Le client informe le serveur qu'il a déjà une adresse



# DHCP – Les messages (référence) – 2

- DHCPACK: Le serveur confirme l'allocation de l'adresse au client
- DHCPNACK: Le serveur indique au client que son adresse est incorrecte ou que son lease est expiré
- DHCPDECLINE: Le client annonce au serveur que l'adresse reçue est déjà utilisée