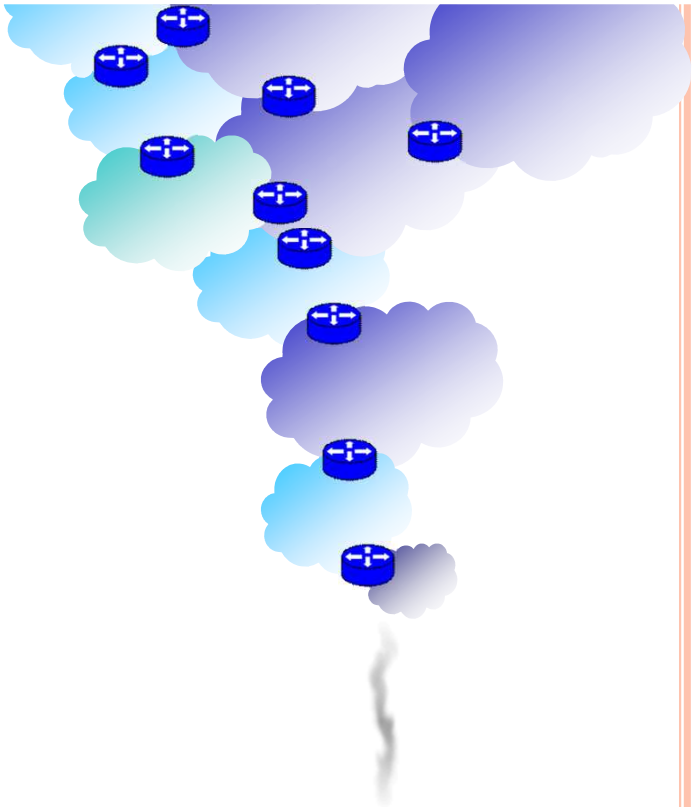


D'INTERNET AU RÉSEAU DOMESTIQUE

Chapitre 5

Plan Chapitre 5 – D'Internet au réseau Domestique

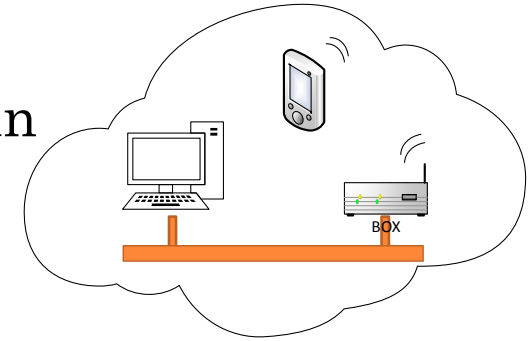
- 5.1 – Vue d'ensemble d'Internet
  - Architecture d'Internet
  - Hiérarchie et vocabulaire
  - Différence entre client et serveur
  - Besoins
- 5.2 – Le réseau domestique
  - Architecture
  - Besoins
- 5.3 – DHCP
  - Répond à quel besoin?
  - Principe et protocole
- 5.4 – NAT
  - Répond à quel besoin?
  - Mise en oeuvre
- 5.5 – DNS
  - Répond à quel besoin?
  - Domaine et hiérarchie
  - Protocole et mise en oeuvre

5.1 Vue d'ensemble du réseau

- Introduction via un dessin en cours de:
  - La notion d'AS
  - La hiérarchie dans les AS (tiers 1, tiers 2-3)
    - Un AS est client d'un autre
  - Le positionnement des clients et leur accès => FAI
  - Les communications
    - entre clients directes
    - entre clients serveurs (notion de Fournisseur de Services ou Fournisseur de Contenus)
    - entre clients en passant par des serveurs (exemple du mail)
  - Le besoin de configurer les machines:
    - DHCP dans un réseau local (exemple pour un serveur)
    - PPP pour un accès ADSL

5.2 Le réseau domestique

- Home Network
  - Plusieurs équipements avec chacun une adresse IP
  - Des technologies:
    - Ethernet
    - Wifi



- Quelles adresses IP pour les équipements?
  - Le FAI ne donne qu'une adresse publique
  - Utilisation de quelle type d'adresses?
  - Besoin de communiquer avec Internet
- Communiquer avec un serveur?
  - Nom =/= adresse IP!
- Sécuriser

5.3 DHCP
OBJECTIFS

- Dynamic Host Configuration Protocol
  - Protocole du monde IETF
  - RFC 2131, RFC 1533

- Objectifs
  - Configuration Automatique et Dynamique d'IP sur une machine
    - Adresse IP de l'interface
    - Masque
    - Passerelle par défaut
    - DNS
  - Installation d'un OS au boot via l'extension de BOOTP [RFC 1542]

5.3 DHCP
Comment? (1)

- Protocole utilisant UDP en mode client / serveur
  - Port 67 en écoute
  - Mais : « Comment obtenir une configuration en utilisant le réseau que l'on veut configurer? »

- Utilisation du broadcast
  - Au niveau IP
  - Au niveau de la technologie sous-jacente (ex: Ethernet)

5.3 DHCP
Comment? (2)

- La configuration classique

5.3 DHCP
Le Bail

- Qu'obtient-on?
  - Adresse IP mais pas que…
  - Masque, adresse de diffusion
  - Options IP, TCP, ...
  - Adresses de routeur, serveur DNS, serveur de temps, impression, …
  - Nom de domaine, …
- Notion de bail (lease) DHCP
  - Allocation pour une durée donnée
    - éventuellement infini
  - Nécessité d 'actualiser régulièrement
    - permet de détecter les arrêts
  - Abandon explicite du client (dhclient –r)

5.3 DHCP

Autre cas

- Refus de configuration

- Libération de bail

5.3 DHCP

Format des message

op	htype	hlen	hops
xid			
secs		flags	
ciaddr			
yiaddr			
siaddr			
giaddr			
chaddr (16 bytes)			
sname (64 bytes)			
file (128 bytes)			
options			

5.4 LE NAT
OBJECTIFS

- Network Address Translation
  - Traduction d'adresse
    - Ici Source
    - Mais peut aussi être faite sur la destination

- Objectifs du sNAT dans un *home network*
  - Pouvoir permettre à des machines du réseau
  - De communiquer avec Internet
  - Alors qu'elles sont en adressage privé

5.4 LE NAT
COMMENT?

- Transformation à la volée des adresses sources
  - Aussi appelé la Mascarade (*Masquerade*)
  - Mais
    - besoin de tables de correspondance
    - besoin d'une adresse publique
  - Sous linux
    - Iptables –t nat

- Mais seulement les adresses, est-ce suffisant?
  - Illustration via l'exemple de la box

5.4 NAT
Bilan

- Avantages
  - Permet d'augmenter le nombre
    - d'utilisateurs d'Internet
    - d'équipements dans Internet
  - Quid d'une forme de sécurité?
    - C'est plutôt faux
- Désavantages
  - *Middlebox*
    - Pas de communication entrante
    - Besoin de mécanismes ou d'ouvertures de ports fixes
  - Complexité

5.5 LE DNS
OBJECTIFS

- Problème: Mémoriser des adresses IP
  - Analogie numéro de téléphone
  - L'être humain préfère les noms

- Correspondance?
  - Statique
    - Fichier host ou host.txt
    - Problème de la maintenance de la liste
  - Annuaire dynamique
    - Centralisé ou distribué?

- Domain Name Server/System

5.5 LE DNS
GÉNÉRALITÉS

- Annuaire distribué
  - nom symbolique <-> adresse IP
  - chaque domaine gère sa partie

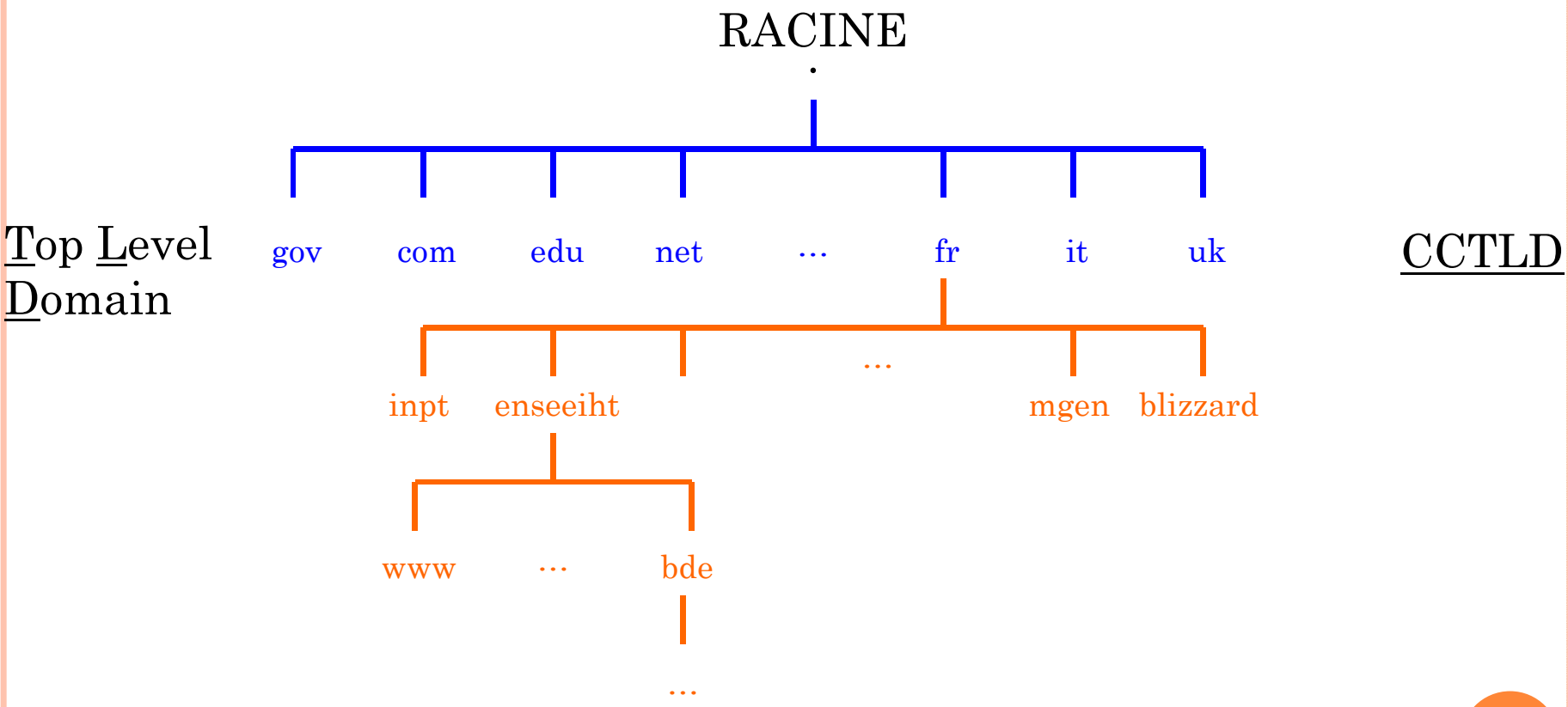
- Définition
  - d 'un protocole de communication [RFC 1034] [RFC 1035]
  - d 'une politique de délégation [RFC 1591]
  - RFC 6895 et des centaines…
  - https://www.isc.org/community/rfcs/dns/

- Fondé sur
  - Une organisation de l'espace
  - Un système de serveurs hiérarchisés
  - De nombreux clients appelés resolver

- Deux parties
  - Un protocole de communication
  - Une politique de répartition des noms de domaines

5.5 LE DNS

ORGANISATION DE L'ESPACE DES NOMS (I)



5.5 LE DNS

ORGANISATION DE L'ESPACE DES NOMS (II)

- Fully Qualified Domain Name
  - www.enseeiht.fr. = Nom absolu
  - www = hôte (serveur web)
  - Profondeur maximale = 127 niveaux
  - 255 caractères max

- Notion de zone
  - Ex: enseeiht.fr
  - Peut être subdivisée (bde.enseeiht.fr)
  - Deux ou plus serveurs de noms DNS par zone
    - Primaire
    - Secondaire(s)

5.5 LE DNS

SERVEURS DE NOMS DNS

- Les Serveurs Racines
  - 13 serveurs racine au monde de a.root-servers.net » à « m.root-servers.net »
  - Gérés par 12 entités
  - Et répartis physiquement sur beaucoup de serveurs (virtualisation)
  - http://www.root-servers.org/
  - Un serveur DNS racine comme k-root reçoit plus de 40000 requêtes à la seconde (https://www.ripe.net/analyse/dns/k-root/#stats)
- Serveurs de domaine
  - Autorité sur une zone
  - Déclaré au serveur de domaine directement supérieur
- Logiciel
  - Plus commun = BIND (*Berkeley Internet Name Domain*)

5.5 LE DNS

RESOLVERS

- Définition
  - Processus client qui contacte les serveurs de noms

- Rôles
  - Dialogue avec le serveur de nom
  - Interprétation des réponses
  - Restituer l'information au logiciel appelant
  - Mise en place d'un système de cache local

5.5 LE DNS

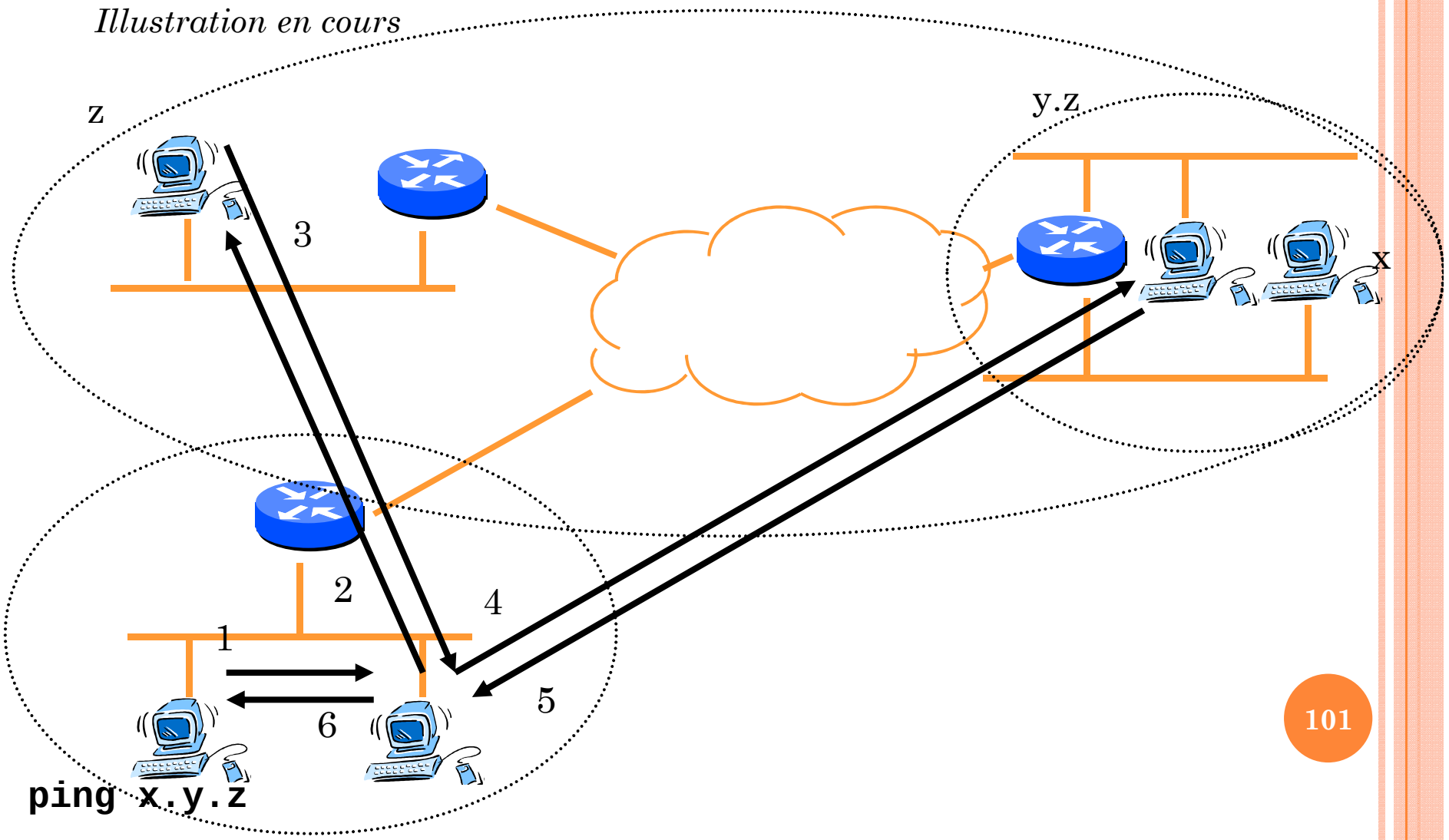
LE PROTOCOLE (I)

- Messages
  - Questions
  - Réponses
  - Utilisation d'UDP
  - Port d'écoute 53
- Principe
  - Renvoyer le message au serveur DNS le plus apte à répondre
- Deux modes d'interrogation des serveurs
  - Itératif
    - Envoie de l'info la plus détaillée dont le serveur dispose
  - Récursif
    - Serveur prend en charge la suite des requêtes
  - Dépendant du serveur interrogé
    - Notion de serveur maître
    - Couplage des modes

5.5 LE DNS

LE PROTOCOLE (II)

Illustration en cours



5.5 LE DNS

LES MESSAGES

identification	flags
nb of questions	nb of answers
nb of authority RRs	nb of add. RRs
questions	
answers	
authority	
additionnal	

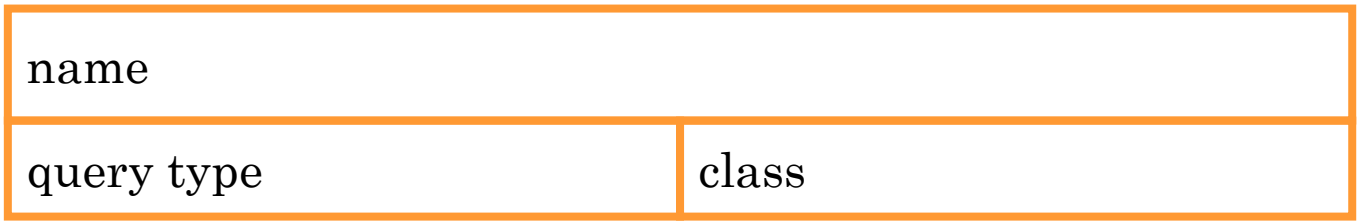
5.5 LE DNS

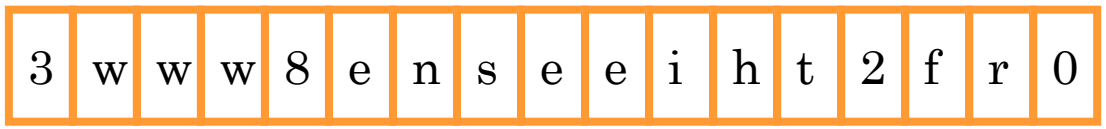
LES MESSAGES

- Q : 0 = requête
- opcode 0 = standard, 1 = inverse
- AA = authoritative
- TC = truncated
- RD = recursion desired
- RA = recursion available

5.5 LE DNS

LES MESSAGES





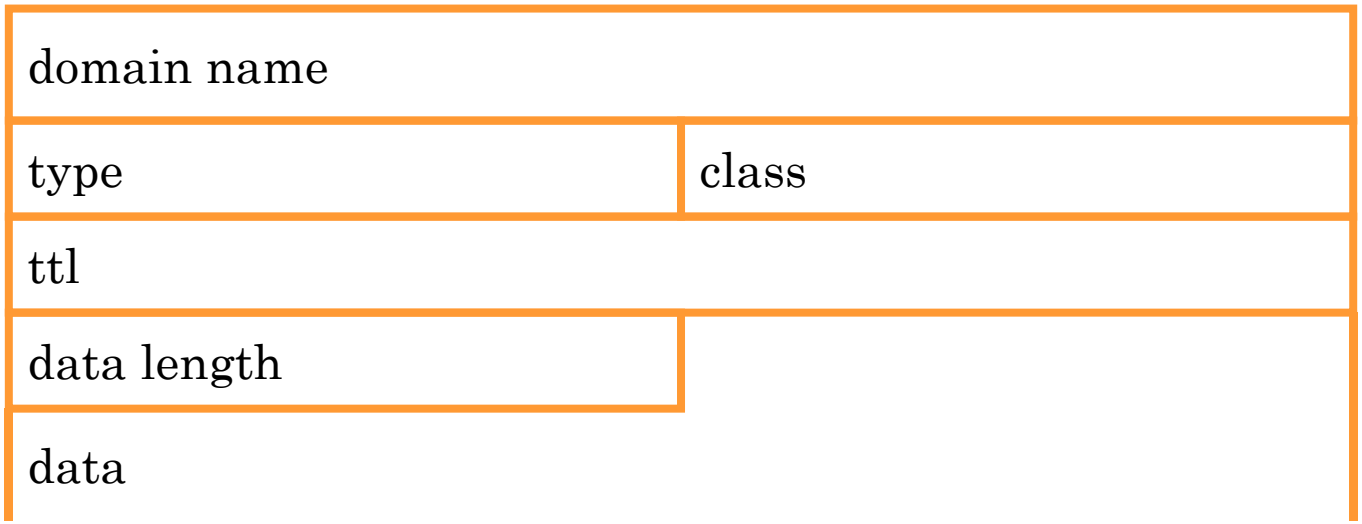
5.5 LE DNS

LES QUESTIONS

Query type	**Signification**
A	Adresse IP
NS	Serveur de nom
CNAME	Nom canonique
PTR	Noms d ’une adresse
HINFO	Informations
MX	Serveur mail

5.5 LE DNS

LES ENREGISTREMENTS (RESSOURCE RECORD)



1.2 – Domain Name Server

DNS et sécurité

- Point critique d'Internet
  - DNS permet de faire association
    - nom symbolique
    - Adresse IP
  - Faux DNS = Fausse réponse
- Points faibles
  - Aucune préoccupation de sécurité
  - Interception et forge
  - Déni de service
- Solutions
  - DNSSEC
  - Ne pas se référer à n'importe quel DNS!